Contributions to Quantum Probability

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Tobias Fritz

aus Weissach im Tal

Bonn, April 2010

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Referent: Prof. Dr. Matilde Marcolli (California Institute of Technology/Bonn)

2. Referent: Prof. Dr. Sergio Albeverio (Bonn)

Tag der Promotion: 25.6.2010

Erscheinungsjahr: 2010

Contents

Acknowledgements. This work would have been impossible without the excellent research conditions within the IMPRS graduate program at the Max Planck Institute for Mathematics. Always highly useful was the instant advice provided constantly by my supervisor Matilde Marcolli. I have greatly enjoyed stays at the University of Magdeburg with Dirk Oliver Theis, and at the Centre for Quantum Technologies in Singapore with Andreas Winter. Many of the ideas presented in this thesis originated from or have been tested in uncountably many discussions with numerous people.

Chapter 1

On the existence of quantum representations for two dichotomic measurements

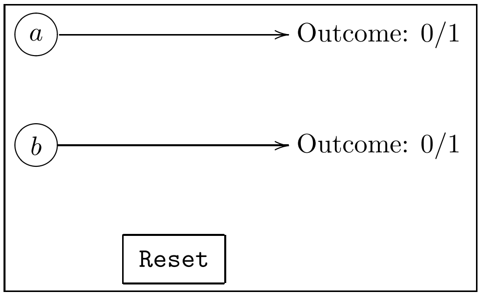
1.1 Introduction

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 also that the experimenter can conduct two different types of measurement—call them a and b—each of which is *dichotomic, i.e.* has the possible outcomes 0 and 1. In this chapter, such a system will be referred to as the "black box figure 1.1".

The experimenter can conduct several repeated measurements on the same system—like first a, then b, and 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. Thereby, he will obtain his results in terms of estimates for probabilities of the form

$$P_{a,b,a}(1,0,0) \tag{1.1.1}$$

Figure 1.1: A black box with two dichotomic measurements and an initialization button.



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

Now suppose that the experimenter finds out that the measurements a and b are always repeatable, in the sense that measuring one of them consecutively yields always the same result 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 are each 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 like (1.1.1) can be calculated from this data by the usual rules of quantum mechanics.

Question 1.1.1. Which conditions do these probabilities $P_{\cdot}(\cdot)$ 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. Physically, the constraints turn out to be so unexpected that an intuitive explanation of their presence seems out of reach.

A variant of this problem has been studied by Khrennikov [Khr09], namely the case of two observables a and b with discrete non-degenerate spectrum. In such a situation, any post-measurement state is uniquely determined by the outcome of the directly preceding measurement. Hence in any such quantum-mechanical model, the outcome probabilities of an alternating measurement sequence $a, b, a, \ldots$ form a Markov chain, meaning that the result of any intermediate measurement of a (respectively b) depends only on the result of the directly preceding measurement of b (repectively a). Furthermore, by symmetry of the scalar product $|\langle\psi|\varphi\rangle|^2 = |\langle\varphi|\psi\rangle|^2$, the corresponding matrix of transition probabilities is symmetric and doubly stochastic. In the case of two dichotomic observables, non-degenarcy of the spectrum is an extremely restrictive requirement; in fact, a dichotomic observable is necessarily degenerate as soon as the dimension of its domain is at least 3. It should then not be a surprise that neither the Markovianness nor the symmetry and double stochasticity hold in general, making the results presented in this chapter vastly more complex than Khrennikov's.

Summary. This chapter is structured as follows. Section 1.2 begins by generally studying a dichotomic 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 1.3 goes on by settling notation and terminology for the probabilities in the black box figure 1.1 and describes the space of all conceivable outcome probability distributions for such a system. The main theorem describing the quantum region within this space is stated and proven in section 1.4. The largest part of this section is solely devoted to the theorem's technical proof; some relevant mathematical background material on moment problems can be found in the appendix 1.10. Section 1.5 then studies projections of the space of all conceivable outcome probabilities and mentions some first results on the quantum region therein; these finite-dimensional projections would mostly be relevant for potential experimental tests. Section 1.6 continues by proving that every point in the whole space of all conceivable outcome probability distributions has a model in terms of a general probabilistic theory. As described in section 1.7, determining the quantum region for a higher number of measurements or a higher number of outcomes should be expected to be very hard. Section 1.8 mentions some properties that experiments comparing quantum-mechanical models to different general probabilistic models should have. Finally, section 1.9 briefly concludes the chapter.

Acknowledgements. I want to thank Andrei Khrennikov for organizing a very inspiring conference “Quantum Theory: Reconsideration of Foundations 5” in Växjö. During discussions, I have received useful input from Cozmin Ududec, who encouraged me to think about iterated measurements in general probabilistic theories, as well as from Ingo Kamleitner, who suggested the quantum dot experiment described in section 1.2. I have also highly profited from conversations with Fabian Furrer and Wojciech Wasilewski. Finally, this work would not have been possible without the excellent research conditions within the IMPRS graduate program.

Notation and terminology. Given a projection operator p, its negation is written as $\overline{p} \equiv 1-p$. In order to have a compact index notation for p and $\overline{p}$ at once, I will also write $p^1 = p$ and $p^0 = \overline{p} = 1 - p$, which indicates that p^1 is the eigenspace projection corresonding to the measurement outcome 1, while p^0 is the eigenspace projection corresponding to the measurement outcome 0.

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 1.4 and in the appendix.

Finally, $\{0,1\}^* \equiv \cup_{n\in\mathbb{N}}\{0,1\}^n$ is the set of all binary strings of arbitrary length.

1.2 Preliminary observations

Before turning to the general case, this section presents some results about outcome probabilities for the measurement sequence a, b, a and reveals some unexpected constraints for quantum-mechanical models. One may think of the two 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 dichotomic 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. initially, it conducts a measurement of the projection operator $|\psi_i\rangle\langle\psi_i|$ and starts over in case of a negative result, and

- postselects with respect to a state $|\psi_f\rangle$ i.e., it finally conducts a measurement of the projection operator $|\psi_f\rangle\langle\psi_f|$ and starts all over from the beginning in case of a negative result.

In between the pre- and the postselection, the experimenter measures the dichotomic observable b. For simplicity, the absence of any additional dynamics is assumed.

This kind of situation can only occur 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

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

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

Proposition 1.2.1. *In such a situation, the condition $\langle\psi_i|\psi_f\rangle = 0$ implies that the two outcomes of b have equal probability, independently of any details of the particular quantum-mechanical model:*

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

Note that such a pre- and postselected dichotomic quantum measurement would therefore be a perfectly unbiased random number generator.

Proof. The proof of proposition 1.2.1 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

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

This equals the probability of measuring $b=1$ and successful postselection, so that both conditional probabilities equal 1/2. □

As 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

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

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

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

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

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

Take the intermediate dichotomic measurement to be given by opening one of the boxes and checking whether the particle is there. This 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 in a way similar to the optical realization of the original Aharanov-Vaidman thought experiment [KJR04] or by 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 1.2.1 also shows that the following more general statement is true:

Proposition 1.2.2. *(a) Given any discrete 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.

So what does all this imply for quantum-mechanical models of the black box figure 1.1? 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:

$$\boxed{P_{a,b,a}(0,0,1) = P_{a,b,a}(0,1,1)} \tag{1.2.1}$$

Similar relations can be obtained from 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 dichotomic 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 (1.2.1) vanish.

1.3 Probabilities for two dichotomic repeatable measurements

In the situation of figure 1.1, 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:

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

and

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

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. In the rest of this chapter, the probabilities of the form $P_{a,b,a,\ldots}$ will be denoted by P_a for the sake of brevity, while similarly P_b stands for the probabilities determining the second stochastic process $P_{b,a,b,\ldots}$.

Since total probability is conserved, it is clear that for every finite binary string $r \in \{0,1\}^*$,

$$\begin{aligned} P_a(r) &= P_a(r,0) + P_a(r,1) \\ P_b(r) &= P_b(r,0) + P_b(r,1) \end{aligned} \tag{1.3.1}$$

A probability assignment for the P_a's and P_b's is called *admissible* whenever the probability conservation laws (1.3.1) hold.

1.4 Classification of probabilities in quantum theories

Now let us assume that the black box figure 1.1 does have a quantum-mechanical description and determine all the constraints that then have to hold for the probabilities P_a and P_b.

The final results will be presented right now at the beginning. 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 string $r \in \{0,1\}^n$, 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. The single letter r and the sequence $r_1, \ldots, r_n$ are interchangeable notation for the same binary string.

The overline notation $\overline{r}$ stands for the inverted string, 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 1.4.1. *A quantum-mechanical description of the black box figure 1.1 exists if and only if the outcome probabilities satisfy the following constraints:*

- *For every $r \in \{0,1\}^{n+1}$ and $i \in \{a,b\}$, the probabilities*

$$P_i(r_1, \ldots, r_{n+1})$$

only depend on i, $s = s(r)$ and r_1; denote this value by $F_{i,r_1}(n,s)$.

- *For every $r \in \{0,1\}^n$,*

$$P_a(r) + P_a(\overline{r}) = P_b(r) + P_b(\overline{r}).$$

- *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]

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

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

- *Using the coefficients*

$$c_{n,k} = (-1)^k \binom{-1/2}{k} - (-1)^{k-n} \binom{-1/2}{k-n}$$

[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

$$\begin{aligned}V_{x,\pm}(n) = & \sum_{k=0}^{\infty} c_{n,k} C_1(k,k) \\ & \pm \sqrt{F_{a,+}(n,n)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} C_2(n+k-1,n-1)\right)^2} \\ V_{z,\pm}(n) = & \sum_{k=0}^{\infty} c_{n,k} C_2(k,0) \\ & \pm \sqrt{F_{a,+}(n,0)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} C_1(n+k-1,k)\right)^2},\end{aligned}$$

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

$$\left(\sup_n V_{x,-}(n),\ \sup_n V_{z,-}(n),\ \inf_n V_{x,+}(n),\ \inf_n V_{z,+}(n)\right) \qquad (1.4.1)$$

has to lie in the convex region $\mathcal{C} \subseteq \mathbb{R}^4$ *characterized in proposition 1.10.2.*[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 $\mathcal{H}$. Upon pulling back the black box's 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 dichotomic 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 figure 1.1.

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

$$\mathcal{A}_2 \cong \left\{ f : [0,1] \overset{\text{cont.}}{\longrightarrow} M_2(\mathbb{C}) \,\middle|\, f(0),\, f(1) \text{ are diagonal} \right\}$$

where the universal pair of projections is given by

$$\begin{aligned} a(t) &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{\mathbb{1}_2 + \sigma_z}{2} \\ b(t) &= \begin{pmatrix} t & \sqrt{t(1-t)} \\ \sqrt{t(1-t)} & 1-t \end{pmatrix} = \frac{1}{2}\mathbb{1}_2 + \sqrt{t(1-t)}\,\sigma_x + \left(t - \frac{1}{2}\right)\sigma_z \end{aligned}$$

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 algebra of matrix-valued continuous functions $\mathscr{C}([0,1], M_2(\mathbb{C}))$ to the subalgebra $\mathcal{A}_2$. Hence for the purposes of the proof of theorem 1.4.1, there is no need to distinguish between $\mathcal{A}_2$ and $\mathscr{C}([0,1], M_2(\mathbb{C}))$.

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

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 dichotomic strings $r = (r_i)_{i=1}^{n+1}$. Every such outcome r has an associated Kraus operator which is given by

$$H_r = a^{r_1} b^{r_2} a^{r_3} \ldots \tag{1.4.2}$$

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

$$\begin{aligned} P_a\left(r_1, \ldots, r_{n+1}\right) &= \rho\left(H_r H_r^\dagger\right) \\ &= \rho\left(a^{r_1} b^{r_2} a^{r_3} \ldots a^{r_3} b^{r_2} a^{r_1}\right) \end{aligned} \tag{1.4.3}$$

Now follows the main observation which facilitates all further calculations.

Lemma 1.4.2. *We have the following reduction formulas in $\mathcal{A}_2$:*

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

Proof. Direct calculation. □

As a consequence, one finds that the measurement outcome probabilities (1.4.3) have the form

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

where s is the number of switches in the dichotomic string $r_0, \ldots, r_n$; 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 1.4.3. *The probabilities $P_a\left(r_1, \ldots, r_{n+1}\right)$ only depend on the number of switches contained in the dichotomic sequence $r_1, \ldots, r_{n+1}$. The same holds for the $P_b\left(r_1, \ldots, r_{n+1}\right)$.*

A particular instance of this is equation (1.2.1).

Remark 1.4.4. Moreover, this observation is actually a *consequence* of the conditional statement of proposition 1.2.2(b). Due to that result, it is clear that the equations

$$P_a(r_1, \ldots, r_k, 0, 0, 1, r_{k+3}, \ldots, r_{n+1}) = P_a(r_1, \ldots, r_k, 0, 1, 1, r_{k+3}, \ldots, r_{n+1})$$

$$P_a(r_1, \ldots, r_k, 1, 0, 0, r_{k+3}, \ldots, r_{n+1}) = P_a(r_1, \ldots, r_k, 1, 1, 0, r_{k+3}, \ldots, r_{n+1})$$

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, 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_1, mention of r will be omitted from now on. Instead, the dependence on r will be retained by considering all expressions as functions of n, r_1 and s, with $s \in \{0, \ldots, n\}$.

The two possible values of the initial outcome r_1 as well as the initial type of measurement are indicated by subscripts:

$$\begin{aligned}
P_a(0, r_2, \ldots, r_{n+1}) &= F_{a,0}(n,s)\\
P_a(1, r_2, \ldots, r_{n+1}) &= F_{a,1}(n,s)\\
P_b(0, r_2, \ldots, r_{n+1}) &= F_{b,0}(n,s)\\
P_b(1, r_2, \ldots, r_{n+1}) &= F_{b,1}(n,s)
\end{aligned}$$

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

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

But actually instead of using these sequences of probabilities, the patterns are easier to spot when using the new variables

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

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

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

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 somewhat reminiscient of the CHSH correlations. In these terms,

$$\begin{aligned} C_1(n,s) &= \rho\left(t^{n-s}(1-t)^s \underbrace{\left[\sqrt{t(1-t)}\,\sigma_x + t\sigma_z\right]}_{\vec{v}_1(t)\cdot\vec{\sigma}}\right) \\ C_2(n,s) &= \rho\left(t^{n-s}(1-t)^s \underbrace{\left[-\sqrt{t(1-t)}\,\sigma_x + (1-t)\sigma_z\right]}_{\vec{v}_2(t)\cdot\vec{\sigma}}\right) \end{aligned}$$

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 $\mathscr{C}([0,1],M_2(\mathbb{C}))$ 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 1.4.1 is a consequence of theorem 1.10.3 as applied to

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

1.5 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.

Question 1.5.1. Given numerical values for a finite subset of the probabilities $P_\cdot(\cdot)$, how can one decide whether a quantum-mechanical representation of these probabilities exists?

Clearly, such a representation 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 1.4.1. 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 an infinite-dimensional vector space down to a finite-dimensional one can be notoriously hard to compute.

Question 1.5.1 is a close relative of the truncated Hausdorff moment problem (see e.g. [Wid41, 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—and then calculating the corresponding points in the truncation, and finally taking 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 $[0,1]$. Since global phases are irrelevant, $|\psi\rangle$ can be assumed to be given by

$$|\psi\rangle = \left(\begin{array}{c} \cos\theta \\ e^{i\lambda}\sin\theta \end{array} \right).$$

In conclusion, the pure states are parametrized by the numbers $t_0 \in [0,1]$, $\lambda \in [0,2\pi]$ and $\theta \in [0,2\pi]$. In any given truncation, this determines an algebraic variety, whose convex hull coincides with the quantum region in that truncation. This reduces the problem 1.5.1 to the calculation of the convex hull of an algebraic variety 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 1.5.2. *A quantum-mechanical representation 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 (1.4.1) that this condition is necessary. To see that it is sufficient, recall the equations

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

which have been used in the proof of theorem 1.4.1. 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 1.10.1 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.

1.6 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 figure 1.1. 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 two sections, this shows that—for systems with two dichotomic 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

$$\mathrm{tr}(\rho) = 1 \quad \forall \rho \in \Omega \tag{1.6.1}$$

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,

$$V = \Omega_0 - \Omega_0. \tag{1.6.2}$$

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 1.6.1. As an example of this machinery, one may take density matrices as normalized states and completely positive trace-nonincreasing 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 dichotomic measurement is then implemented by two operations $a, \overline{a} : V \to V$ which are idempotent,

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

and complementary in the sense that the operation $a + \overline{a}$ preserves the trace. Physically, the operation a takes place whenever the dichotomic measurement has the outcome 1, whereas $\overline{a}$ happens in the case that the dichotomic measurement has the outcome 0.

Proposition 1.6.2. *Under these assumptions,* $a\overline{a} = \overline{a}a = 0$.

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

$$\mathrm{tr}(\overline{a}a(\rho)) = \mathrm{tr}(a(\rho)) - \mathrm{tr}(aa(\rho)) = 0,$$

which proves $\overline{a}a = 0$ by (1.6.1). The other equation works in exactly the same way. □

The interpretation of this result is that, when a has been measured with outcome 1, then the opposite result $\overline{a}$ will certainly not occur in an immediately sequential measurement, and vice versa. In this sense, the measurement of a vs. $\overline{a}$ is repeatable.

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

Theorem 1.6.3. *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 1.4: 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 needs to consider the unital $\mathbb{R}$-algebra freely generated by formal variables v_a, $v_{\overline{a}}$, v_b, $v_{\overline{b}}$, subject to the relations imposed by the above requirements. Hence the definition is this,

$$\begin{aligned}\mathcal{A}_{gp} = \Big\langle v_a, v_{\overline{a}}, v_b, v_{\overline{b}} \mid \quad & v_a v_{\overline{a}} = v_{\overline{a}} v_a = v_b v_{\overline{b}} = v_{\overline{b}} v_b = 0, \\ & v_a^2 = v_a,\ v_{\overline{a}}^2 = v_{\overline{a}},\ v_b^2 = v_b,\ v_{\overline{b}}^2 = v_{\overline{b}} \Big\rangle_{\mathtt{\mathbb{R}Alg}}\end{aligned}$$

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". This definition guarantees that any finite product of generators can be reduced to one of the form

$$v_{a^{r_1}} v_{b^{r_2}} v_{a^{r_3}} \ldots \qquad \text{or} \qquad v_{a^{r_1}} v_{b^{r_2}} v_{a^{r_3}} \ldots\ .$$

These expressions, together with the unit $\mathbb{1}$, form a linear basis of $\mathcal{A}_{gp}$.

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

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

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

$$\rho\left(x(v_a + v_{\overline{a}})\right) = \rho(x), \quad \rho\left(x(v_b + v_{\overline{b}})\right) = \rho(x) \tag{1.6.3}$$

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 functional is defined to be

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

so that a state is normalized if and only if $\rho(1) = 1$. Thereby the state space Ω is defined.

Now for the definition of the operators a, $\overline{a}$, b, $\overline{b}$, which should map Ω_0 to itself. Given an unnormalized state $\rho \in \Omega_0$, they produce a new state which is defined as

$$\begin{aligned} a(\rho)(x) &\equiv \rho(v_a x) \\ \overline{a}(\rho)(x) &\equiv \rho(v_{\overline{a}} x) \\ b(\rho)(x) &\equiv \rho(v_b x) \\ \overline{b}(\rho)(x) &\equiv \rho(v_{\overline{b}} x) \end{aligned}$$

Since $v_a^2 = v_a$, it follows that $a^2 = a$, and similarly it follows that $\overline{a}^2 = \overline{a}$, $b^2 = b$ and $\overline{b}^2 = \overline{b}$ hold true.

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

$$\begin{aligned} P_a(r) &= \rho\left(v_{a^{r_1}} v_{b^{r_2}} v_{a^{r_3}} \ldots\right) \\ P_b(r) &= \rho\left(v_{b^{r_1}} v_{a^{r_2}} v_{b^{r_3}} \ldots\right) \end{aligned} \tag{1.6.4}$$

So given any assignment of outcome probabilities P_a, P_b, one can regard the equations (1.6.4) 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 (1.6.3) hold by conservation of probability (1.3.1). This ends the proof. □

1.7 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 figure 1.1 on which the experimenter can conduct k different kinds of measurement. Suppose also that the jth measurement has $n_j \in \mathbb{N}$ possible 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 nth roots of unity.

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 maximal 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 maximal group C^*-algebra of the modular group.

1.8 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 1.4.1 in a finite truncation seem indeed appropriate. Among the obvious requirements for such an experiment are

- One needs a system with two dichotomic observables, which are very close to ideal von Neumann measurements.
- It has to be possible to measure these observables without destroying the observed system.

There is another important caveat: for sufficiently small systems with many symmetries, it can 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 with different orientations—are too small for a successful distinction of quantum theory vs. different general probabilistic theories along the lines proposed in this chapter. On the other hand, genuinely dichotomic measurements are hard to come by on bigger systems, as this requires a high level of degeneracy. The three-photon experiment or the quantum dot experiment described in section 1.2 might be good starting points for further investigation of all of these issues.

1.9 Conclusion

This chapter was concerned with the simplest non-trivial case of the representation 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 represents these probabilities? This question has been answered by theorem 1.4.1 to the extent that there are several infinite sequences of constraints, all of which come 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. On the other hand, theorem 1.6.3 shows that every point in the space of all probabilities can be represented by a general probabilistic model. In this sense, quantum-mechanical models are of a very specific kind. The present results yield no insight on the question why our world should be quantum-mechanical—to the contrary, the conditions in theorem (1.4.1) 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.

1.10 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. The variable of these matrix-valued functions is denoted by $t \in [0,1]$.

Theorem 1.10.1. *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*

$$\begin{aligned} M_1(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \mathbb{1}_2\right) \\ M_x(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \sigma_x\right) \\ M_z(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \sigma_z\right) \end{aligned} \tag{1.10.1}$$

if and only if the following conditions hold:

- *probability conservation:*

$$M_i(n,s) = M_i(n+1,s) + M_i(n+1,s+1) \quad \forall i \in \{1,x,z\} \tag{1.10.2}$$

- *non-negativity:*

$$M_1(n,s) \geq \sqrt{M_x(n,s)^2 + M_z(n,s)^2} \tag{1.10.3}$$

- *normalization:*

$$M_1(0,0) = 1 \tag{1.10.4}$$

Proof. This proof is an adaptation of the solution of the Hausdorff moment problem as it is outlined in [Wid41, III §2]. Given the state ρ, it follows that (1.10.2) holds by $1 = t + (1-t)$. For the non-negativity inequality, note that the 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

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

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 moments which satisfy the constraints (1.10.2), (1.10.3) and (1.10.4). First of all, (1.10.2) implies that

$$M_i(n,s) = \sum_{r=s}^{k-n+s} \binom{k-n}{r-s} M_i(k,r), \quad \forall k \geq n,\ i \in \{1,x,z\}, \tag{1.10.5}$$

which can be proven by induction on k. Since the binomial coefficient vanishes in that case, it is also possible to sum from $k=0$ up to $r=k$ without changing the left-hand side.

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 real linear subspace of $\mathcal{A}$.

Recall that the Bernstein polynomials [Lor86]

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

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,

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

The Bernstein polynomials can be used to construct a sequence of approximating states ρ_n on $\mathcal{P}$, $n \in \mathbb{N}$. The ρ_n 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,

$$\begin{aligned}
&|\rho_n(P_1(t)\mathbb{1}_2 + P_x(t)\sigma_x + P_z(t)\sigma_z)| \\
&\quad \leq \sum_{s=0}^{n} \binom{n}{s} \left[\left| P_1\left(\frac{s}{n}\right)\right| M_1(n,s) + \sqrt{P_x\left(\frac{s}{n}\right)^2 + P_z\left(\frac{s}{n}\right)^2} \cdot \right. \\
&\qquad \left. \cdot \left| \frac{P_x(\frac{s}{n})}{\sqrt{P_x\left(\frac{s}{n}\right)^2 + P_z\left(\frac{s}{n}\right)^2}} M_x(n,s) + \frac{P_z(\frac{s}{n})}{\sqrt{P_x\left(\frac{s}{n}\right)^2 + P_z\left(\frac{s}{n}\right)^2}} M_z(n,s) \right| \right] \\
&\quad \overset{(1.10.3)}{\leq} \sum_{s=0}^{n} \binom{n}{s} \left[\left| P_1\left(\frac{s}{n}\right)\right| M_1(n,s) + \sqrt{P_x\left(\frac{s}{n}\right)^2 + P_z\left(\frac{s}{n}\right)^2} \cdot M_1(n,s) \right] \qquad (1.10.6) \\
&\quad \overset{(1.10.5),\ (1.10.4)}{\leq} \max_{t\in[0,1]} \left[|P_1(t)| + \sqrt{P_x(t)^2 + P_z(t)^2} \right] \\
&\quad = \max_{t\in[0,1]} ||P_1(t)\mathbb{1}_2 + P_x(t)\sigma_x + P_z(t)\sigma_z||
\end{aligned}$$

where 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-valued polynomials

$$B_{n,s}\mathbb{1}_2,\ B_{n,s}\sigma_x,\ B_{n,s}\sigma_z; \quad s \in \{0,\ldots,n\}. \qquad (1.10.7)$$

Then the requirements (1.10.1) 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 (1.10.2), show that the diagram

$$\begin{tikzcd}
\mathcal{P}_k \arrow[rr] \arrow[dr] & & \mathcal{P}_{k+1} \arrow[dl] \\
& \mathbb{R} &
\end{tikzcd}$$

commutes for all k. Therefore, the $\widetilde{\rho}_k$ extend to a linear functional $\widetilde{\rho} : \mathcal{P} \to \mathbb{R}$, which is now defined on all of $\mathcal{P}$. The problem with $\widetilde{\rho}$ is that its boundedness is hard to check.

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 (1.10.6) 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 $||\widehat{\rho}\,|| = \widehat{\rho}(\mathbb{1}) = 1$ holds, and the construction of $\widehat{\rho}$ such that the equations (1.10.1) hold for this state.

In order to check this convergence, it is sufficient to consider the values of the states on the basis polynomials (1.10.7). 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.

$$\begin{aligned}
\widetilde{\rho}\,(B_{n,n-s}(t)\mathbb{1}_2) - &\rho_k\,(B_{n,n-s}(t)\mathbb{1}_2) \\
&= \binom{n}{s} M_1(n,s) - \binom{n}{s} \sum_{r=0}^{k} \binom{k}{r} \left(\frac{r}{k}\right)^{n-s} \left(1 - \frac{r}{k}\right)^{s} M_1(k,r) \\
&\overset{(1.10.5)}{=} \binom{n}{s} \sum_{r=0}^{k} \left[\binom{k-n}{r-s} - \binom{k}{r} \left(\frac{r}{k}\right)^{n-s} \left(1 - \frac{r}{k}\right)^{s} \right] M_1(k,r) \\
&= \binom{n}{s} \sum_{r=0}^{k} \left[\frac{\binom{k-n}{r-s}}{\binom{k}{r}} - \left(\frac{r}{k}\right)^{n-s} \left(1 - \frac{r}{k}\right)^{s} \right] \binom{k}{r} M_1(k,r)
\end{aligned}$$

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

$$|\widetilde{\rho}\,(B_{n,n-s}(t)\mathbb{1}_2) - \rho_k\,(B_{n,n-s}(t)\mathbb{1}_2)| \leq \binom{n}{s} \max_{r=0}^{k} \left| \frac{\binom{k-n}{r-s}}{\binom{k}{r}} - \left(\frac{r}{k}\right)^{n-s} \left(1 - \frac{r}{k}\right)^{s} \right| \tag{1.10.8}$$

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

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 (1.10.8) vanishes in the $k \to \infty$ limit. This finally ends the proof. □

Before studying the second 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 1.10.2. *$\mathcal{C}$ 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:*

$$\begin{gathered}
x_0 \leq x_1 \;\wedge\; y_0 \leq y_1 \\
(x_0 \leq \;\;1 \wedge y_0 \leq 0) \vee (x_0 \leq 0 \wedge y_0 \leq \;\;1) \vee \left(x_0^2 + y_0^2 \leq 1\right) \\
(x_1 \geq -1 \wedge y_0 \leq 0) \vee (x_1 \geq 0 \wedge y_0 \leq \;\;1) \vee \left(x_1^2 + y_0^2 \leq 1\right) \\
(x_1 \geq -1 \wedge y_1 \geq 0) \vee (x_1 \geq 0 \wedge y_1 \geq -1) \vee \left(x_1^2 + y_1^2 \leq 1\right) \\
(x_0 \leq \;\;1 \wedge y_1 \geq 0) \vee (x_0 \leq 0 \wedge y_1 \geq -1) \vee \left(x_0^2 + y_1^2 \leq 1\right)
\end{gathered}$$

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

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

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

$$\begin{gathered} -x + x_0 \le 0, \quad x - x_1 \le 0 \\ -y + y_0 \le 0, \quad y - y_1 \le 0 \\ x \cdot \cos\alpha + y \cdot \sin\alpha \le 1 \quad \forall \alpha \in [0, 2\pi] \end{gathered}$$

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 $x_0 \le x_1$ and $y_0 \le y_1$. On the other hand, if such a linear combination contains α-family inequalities for two or more 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 a unique way to replace 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:

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

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 $x_0 = 1$, $y_0 = 1$ and the circular arc in the first quadrant of the x_0-y_0-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. □

Theorem 1.10.3. *Given real numbers $M'_1(n,s)$, $M'_x(n,s)$ and $M'_z(n,s)$ for each $n \in \mathbb{N}_0$ and $s \in \{0, \dots, n\}$, there exists a state ρ on $\mathcal{A}$ that has the (integer and half-integer) moments*

$$\begin{aligned} M'_1(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \mathbb{1}_2\right) \\ M'_x(n,s) &= \rho\left(t^{n-s+1/2}(1-t)^s \cdot \sigma_x\right) \\ M'_z(n,s) &= \rho\left(t^{n-s}(1-t)^{s+1/2} \cdot \sigma_z\right) \end{aligned} \tag{1.10.9}$$

if and only if all of these numbers lie in $[-1, +1]$ and the following additional conditions hold:

- *probability conservation:*

$$M'_i(n,s) = M'_i(n+1,s) + M'_i(n+1,s+1) \quad \forall i \in \{1, x, z\} \tag{1.10.10}$$

- *non-negativity:*

$$M'_1(n,s) \ge 0 \tag{1.10.11}$$

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

$$\begin{aligned}&\left(\sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M'_x(n+k-1, s+k)\right)^2\\ &+\left(\sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M'_z(n+k-1, s-1)\right)^2 \leq M'_1(n,s)^2\end{aligned} \tag{1.10.12}$$

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

$$c_{n,k} = (-1)^k\binom{-1/2}{k} - (-1)^{k-n}\binom{-1/2}{k-n}$$

and the quantities

$$\begin{aligned}V_{x,\pm}(n) =& \sum_{k=0}^{\infty} c_{n,k}M'_x(k,k)\\ &\pm\sqrt{M'_1(n,n)^2 - \left(\sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M'_z(n+k-1, n-1)\right)^2}\\ V_{z,\pm}(n) =& \sum_{k=0}^{\infty} c_{n,k}M'_z(k,0)\\ &\pm\sqrt{M'_1(n,0)^2 - \left(\sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M'_x(n+k-1, k)\right)^2}\end{aligned}$$

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

$$\left(\sup_n V_{x,-}(n),\ \sup_n V_{z,-}(n),\ \inf_n V_{x,+}(n),\ \inf_n V_{z,+}(n)\right) \tag{1.10.13}$$

has to lie in the convex region $\mathcal{C}$ characterized in proposition (1.10.2).[4]

- *normalization:*
$$M'_1(0,0) = 1 \tag{1.10.14}$$

Proof. It will be shown first that these conditions are necessary. This is immediate for (1.10.10), (1.10.11) and (1.10.14). Furthermore, the (uniformly convergent) binomial expansions

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

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

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

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

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

$$\begin{aligned}\rho\left(t^{n-s}(1-t)^s\sigma_x\right) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}\rho\left(t^{n-s-1/2}(1-t)^{s+k}\sigma_x\right), \quad s\in\{0,\dots,n-1\}\\ \rho\left(t^{n-s}(1-t)^s\sigma_z\right) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}\rho\left(t^{n-s+k}(1-t)^{s-1/2}\sigma_z\right), \quad s\in\{1,\dots,n\}.\end{aligned} \tag{1.10.15}$$

In the present notation (1.10.1) and (1.10.9), this reads

$$\begin{aligned}M_x(n,s) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M_x'(n+k-1,s+k), \quad s\in\{0,\dots,n-1\}\\ M_z(n,s) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M_z'(n+k-1,s-1), \quad s\in\{1,\dots,n\}.\end{aligned} \tag{1.10.16}$$

Together with (1.10.3), these formulas imply the constraint (1.10.12) for all relevant values $s\in\{1,\dots,n-1\}$. Given in addition $M_x(0,0)=\rho(\sigma_x)$ and $M_z(0,0)=\rho(\sigma_z)$, the missing integer moments undetermined by (1.10.16) can be calculated as

$$\begin{aligned}M_x(n,n) &\overset{(1.10.2)}{=} M_x(0,0)-\sum_{k=1}^{n}M_x(k,k-1) \overset{(1.10.16)}{=} M_x(0,0)-\sum_{k=0}^{\infty}c_{n,k}M_x'(k,k),\\ M_z(n,0) &\overset{(1.10.2)}{=} M_z(0,0)-\sum_{k=1}^{n}M_z(k,1) \overset{(1.10.16)}{=} M_z(0,0)-\sum_{k=0}^{\infty}c_{n,k}M_z'(k,0).\end{aligned} \tag{1.10.17}$$

where the second steps also involve rearrangements of the sums. Since $M_x(n,n)$ is constrained by (1.10.3) 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 (1.10.17) shows that $M_x(0,0)$ has to lie in the interval

$$[V_{x,-}(n),V_{x,+}(n)] \tag{1.10.18}$$

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 (1.10.13) has to be in $\mathcal{C}$ by the additional constraint

$$M_x(0,0)^2+M_z(0,0)^2\leq M_1(0,0)^2=1. \tag{1.10.19}$$

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 hypotheses of theorem 1.10.1 such that the M'_x and M'_z can be recovered as

$$\begin{aligned} M'_x(n,s) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M_x(n+k,s+k) \\ M'_z(n,s) &= \sum_{k=0}^{\infty}(-1)^k\binom{1/2}{k}M_z(n+k,s), \end{aligned} \tag{1.10.20}$$

and such that the $M_1(n,s)$ coincide with the $M'_1(n,s)$. To begin, use (1.10.16) 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 (1.10.17). 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 (1.10.20) hold, independently of the chosen values for $M_x(0,0)$ and $M_z(0,0)$.

It remains to verify that, with these definitions of M_x and M_z, the requirements of theorem (1.10.1) can be satisfied for appropriate choices of $M_x(0,0)$ and $M_z(0,0)$. The equations (1.10.2) easily follow by direct calculation, using (1.10.10). Again by the binomial expansions, the second part of (1.10.3) is directly equivalent to (1.10.12) for $s \in \{1,\ldots,n-1\}$. In the case that $s=n>0$, it holds as long as $M_x(0,0)$ is chosen to lie in the interval (1.10.18); a similar statement holds for $s=0$ and $n>0$. For $s=n=0$, the constraint is equivalent to (1.10.19) 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 (1.10.13) 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. □

Chapter 2

Possibilistic physics

2.1 Introduction

Many aspects of the world are non-deterministic. The concepts and methods of probability theory and quantitative statistics have entered, for example, the realms of social sciences, biology, and finance. All of these areas are non-fundamental descriptions of some aspects of our world where the appearance of non-determinism and probability is an emergent phenomenon and originates from averaging over unknown parameters. However, since the advent of quantum theory in the early 20th century, even fundamental physics as the most basic description of nature has become probabilistic. In a fundamental theory of nature, the appearance of probabilistic features cannot be emergent, since by the very definition of fundamental physics there cannot exist any unknown and more fundamental parameters that need to be averaged over.

This raises the question whether physics actually obeys the laws of probability theory, on the most fundamental level. If yes, from which physical principle could the laws of probability—or its quantum counterparts—be derived? If no, what are possible alternatives to probability? It is this second question I am going to ponder here; since my personal belief is that no assumption is too elemenatary for careful scrutiny. I want to suggest that one can possibly completely despense of probabilities and replace them by the concept of *possibility*: a physical theory then would just state which events are possible, which are impossible, and nothing else.

Therefore, I do not have an answer to the question,

“What’s ultimately possible in physics?”

Instead, I want to argue that besides trying to find answers to this question within the framework of a given physical theory, one can also turn this procedure upside down and regard the answers to this question as *defining* a physical theory.

Specifying a physical theory by saying what is possible to occur and what is impossible to occur could be called *possibilistic physics*. In this chapter, I will describe a very general mathematical framework for possibilistic physics. As a start, I want to focus on the possibilistic analogue of general probabilistic theories, and in particular two-party Bell tests. Recall that a Bell test is a system which allows for detection of quantum non-locality, one of the most fascinating facets of quantum mechanics. Its possibilistic analogue will be described and characterized. Also, it is found that Spekkens’ toy theory of quantum mechanics [Spe07] is inconsistent in the usual probabilistic interpretation, but is a perfectly fine example of a possibilistic theory.

I am well aware that some of the philosophical arguments discussed in the last part of this chapter are not totally imperturbable. They should rather be regarded as a study of feasibility:

how much can one possibly to do with the concept of possibility and which arguments speak in favor of using it? In particular, how does this concept compare to probability? Further investigations of both the mathematical and the philosophical aspects are necessary.

Acknowledgements. I would like to thank the Max Planck Institute for providing an excellent research environment and for financial support within the IMPRS graduate program. I have profited from discussions with Adam-Christiaan van Roosmalen and Dirk Oliver Theis on finite configurations of orthogonal vectors and matroids with scalar product.

2.2 Recap of general probabilistic theories

Since possibilistic theories will be defined in analogy with general probabilistic theories, we should start by shortly recalling the latter before delving into the former. Note that my use of "prediction" and "theory" is non-standard terminology.

Quantum physics is, both in theory and in experiment, fundamentally non-deterministic. In an experiment, the outcome of a measurement cannot be predicted, even when the initial state of the system is known completely. Instead, what can be inferred from the theory is that the outcomes of many repetitions of the same experiment sould be independent random variables identically distributed according to a certain probability distribution. This implies that the relative asymptotic frequency of each outcome will converge to a certain value in the unit interval $[0, 1]$. It is this value that can be compared between theory and experiment.

Predictions and theories. A convenient framework for probabilistic theories like quantum mechanics is given by the concept of *general probabilistic theory.* To begin explaining this term, think of a physical system, which is to be observed, together with a finite number of measurements that can be performed on this system. Then a *prediction* is defined to be a specification of a probability distribution over the outcomes of each measurement. More precisely, for a set of n different measurements, where the ith measurement has the set $\mathcal{O}_i$ as its set of possible outcomes, a prediction is given by numerical values in terms of probability assignments

$$P_i : \mathcal{O}_i \longrightarrow [0, 1], \qquad \forall\, i = 1, \ldots, n\,,$$

such that for each measurement, some outcome occurs with certainty:

$$\sum_{x \in \mathcal{O}_i} P_i(x) = 1, \qquad \forall\, i = 1, \ldots, n\,. \tag{2.2.1}$$

In this chapter , the term "model" will often be used as a synonym for "prediction".

In quantum theory, and certainly in any other sensible theory of physics, the prediction depends on the initial state of the system and on the interaction dynamics between the system and the measuring apparatus. Therefore, no sensible theory would only allow for a single prediction. Instead, a general probabilistic theory is defined to be a convex subset of the set of all predictions: those that are allowed by the theory. Convexity is required since one can always take stochastic combinations of initial states to obtain the corresponding convex combination of predictions as the total prediction—e.g. flip a coin that decides which initial state to use in the experiment. We will later see that this is violated in the probabilistic interpretation of Spekkens' toy theory, turning it inconsistent.

This ends the definitions of prediction and (general) probabilistic theory. Note that a prediction makes no statement about what happens with the system after the measurement, and a probablistic theory makes no statement about how the prediction depends on the initial state. In this sense, the formalism only captures a tiny aspect of physics.

		a	
		$+$	$-$
b	$+$	0.20	0.31
	$-$	0.39	0.10

(a) When Alice measures a and Bob measures b.

		a		a'	
		$+$	$-$	$+$	$-$
b	$+$	0.20	0.31	0.27	0.03
	$-$	0.39	0.10	0.37	0.33
b'	$+$	0.57	0.20	0.39	0.00
	$-$	0.02	0.21	0.25	0.36

(b) For the full Bell test, where Alice and Bob each can choose among two measurements.

Figure 2.1: Example predictions in a general probabilistic theory.

The Bell test system. As an example system, let us analyze a Bell test experiment. This system consists of two observers, commonly called Alice and Bob, in spacelike separated regions. The simplest situation—not yet the Bell test—is that Alice measures a and Bob measures b, measurements that both have two possible outcomes, say, $+$ and $-$. In order to be able to talk about correlations between a and b, it is necessary to consider a and b together as a single measurement with four possible outcomes

$$\begin{aligned} \mathcal{O}_{a,b} = \big\{ &(+,+), \\ &(+,-), \\ &(-,+), \\ &(-,-) \big\} . \end{aligned} \tag{2.2.2}$$

A sample prediction for this measurement is shown in figure 2.1(a). A slightly more complicated system is the *Bell test*, where Alice can choose between the measurements a and a', whereas Bob can choose between the measurements b and b'. Again, the set of possible outcomes for each measurement is $\{+,-\}$. In total, this gives the four measurement combinations (a,b), (a,b'), (a',b), and (a',b'), which ought to be regarded as the elementary measurements. These measurements all have the same set of outcomes (2.2.2). A sample prediction is shown in figure 2.1(b); note that the probabilities sum to 1 in each of the four subsquares. Since the marginals for Alice do not depend on the choice of Bob's measurement, this sample prediction belongs to the theory "no signalling from Bob to Alice". And since the marginals of Bob do depend on the Alice's choice of measurement, this sample prediction does not belong to the theory "no signalling from Alice to Bob".

2.3 Spekkens' toy theory and general possibilistic theories

On Spekkens' toy theory. I will now show that Spekkens' toy theory of quantum mechanics [Spe07] does not fit into the framework of general probabilistic theories. This will give a motivation for the introduction of the framework of *general possibilistic theories*, of which Spekkens' toy qubits are an example.

Recall that the possible pure states of a Spekkens qubit are exactly the following:

■■□□, □□■■, ■□■□, □■□■, □■■□, ■□□■, ■■■■.

As noticed in [Spe07, III.A], these states are somewhat analogous to spin states of a spin 1/2 particle for which the spin is aligned along one of the coordinate axes. One incarnation of this correspondence is that the (reproducible) measurements [Spe07, III.D] that can be performed on a toy qubit are, up to relabelling the outcomes like + ↔ −, represented as in the table

	■■□□	□□■■	■□■□	□■□■	□■■□	■□□■	■■■■
$\boxed{+}\boxed{+}\boxed{-}\boxed{-}$	$+$	$-$	$\pm$	$\pm$	$\pm$	$\pm$	$\pm$
$\boxed{+}\boxed{-}\boxed{+}\boxed{-}$	$\pm$	$\pm$	$+$	$-$	$\pm$	$\pm$	$\pm$
$\boxed{+}\boxed{-}\boxed{-}\boxed{+}$	$\pm$	$\pm$	$\pm$	$\pm$	$-$	$+$	$\pm$

(2.3.1)

Each column of this table specifies the prediction in that state. The entries + and − denote definite outcomes where the measurement yields that outcome with certainty. Spekkens [Spe07, D] writes about the "±" entries standing for indefinite outcomes,

> [. . .] then the outcome is not determined. In a large ensemble of such experiments, one expects the two outcomes to occur with equal frequency.

Therefore, in the terminology of general probabilistic theories, the Spekkens qubits define a theory with exactly seven possible predictions. The problem now is that these seven predictions do not form a convex subset of the space of all probability assignments, turning outcomes of experiments ambiguous. For example, suppose we set up the following experiment: use a random initialization of the qubit such that it is initialized in the state ■■□□ with a probability of 2/3, and in the state □□■■ with a probability of 1/3. Then upon conducting the $\boxed{+}\boxed{+}\boxed{-}\boxed{-}$ measurement, the rules of probability dictate that + should occur with an asymptotic frequency of 2/3. On the other hand, the random initial state of the system should also be describable in terms of a mixed state; especially so since Spekkens' states are supposed to be states of subjective knowledge, not of objective existence. But the only (non-pure) mixed state in his theory is ■■■■, which yields, according to the rule quoted above, the outcome + with a probability of merely 1/2.

More generally, such an argument makes it clear that—due to a violation of the convexity condition—no general probabilistic theory can have only a finite number of predictions. To avoid this problem, one could certainly take the convex hull of all predictions defined by the six pure states, and regard the resulting region as a modified Spekkens theory. The knowledge balance principle advocated in [Spe07] would still be satisfied. However, this would contravene the combinatorial flavor of the theory as having only a finite number of states.

The alternative is to leave the paradigm of general probabilistic theories. If one regards a "±" in (2.3.1) as merely stating that "both outcomes are possible", the problem about random mixtures disappears: in both ways of reasoning, one obtains nothing more but the statement "both outcomes are possible". Actually, it shouldn't really be much of a surprise that a theory of physics which is discrete and combinatorial in flavor can only make predictions of a nature that are themselves discrete, combinatorial, and therefore non-quantitative!

This is the approach that will be taken here. I will now start to outline a general framework for possibilistic theories of physics, which is analogous to the framework for general probabilistic theories outlined in the previous section. Spekkens' toy qubits serve as a perfectly generic example.

Possibilities and possibilistic predictions. In contrast to ordinary probability theory, where every event gets assigned a probability value lying in $[0, 1]$, we now merely assign to every event a possibility value. A possibility value is an element of the set $\{0, *\}$. The interpretation is that an event with possibility value 0 can be excluded and will certainly not occur, whereas an event with a possibility value of $*$ can occur, but it does not have to. Mathematically, this kind of possibility theory can be viewed as probability theory with coefficients in the semiring $\{0, *\}$, where the algebraic operations on this semiring are given by[1]

$$\begin{array}{ccc} 0+0=0, & 0+*=*, & *+*=* \\ 0\cdot 0=0, & 0\cdot *=0, & *\cdot *=*\,. \end{array} \tag{2.3.2}$$

In a physical setting, consider again n measurements where the set of outcomes of the ith measurement is $\mathcal{O}_i$. Now, a *possibilistic prediction* is specified in analogy with the probabilistc case by a possibility distribution, which is a function

$$\pi_i : \mathcal{O}_i \longrightarrow \{0, *\}, \qquad i = 1, \ldots, n$$

such that for each measurement, at least one outcome is possible. By virtue of the algebra (2.3.2), this condition is totally analogous to (2.2.1),

$$\sum_{x\in\mathcal{O}_i} \pi_i(x) = *, \qquad i = 1, \ldots, n \tag{2.3.3}$$

As a first example, consider a single binary measurement with $\{+, -\}$ as its set of possible outcomes. Then there are three possible predictions:

$$\begin{array}{lll} & \pi(+) = *, \quad \pi(-) = 0. & \text{Here, the outcome is } + \text{ with certainty.} \\ \text{or} & \pi(+) = 0, \quad \pi(-) = *. & \text{Here, the outcome is } - \text{ with certainty.} \\ \text{or} & \pi(+) = *, \quad \pi(-) = *. & \text{Here, both outcomes can occur.} \end{array}$$

For the third prediction, both outcomes are possible, and this is the only statement made by this prediction. Nothing at all is implied about how the two outcomes relate to each other.

Possibilistic theories. Just as in the probabilistic case, a *possibilistic theory* consists of a subset of all predictions. Like a general probabilistic theory needs to be closed under convex combinations corresponding to a probabilistic random choice of initial state, a possibilistic theory needs to be closed under sums (2.3.2), corresponding to a possibilistic choice of initial state. For suppose that we have two initial states available, corresponding to predictions π and π'. Now we let a coin flip[2] decide which initial state to use. In the combined experiment, an outcome will be possible if and only if it is possible in π or in π'. Therefore, the prediction for the combined experiment is $\pi + \pi'$.

The possibilistic Bell test. As a relevant example system, I now want to give sample predictions for a possibilistic Bell test. Figure 2.2 is a self-explaining analogue of figure 2.1. Note that each of the four subsquares contains at least one $*$, so that (2.3.3) holds. Now, the possibilistic marginals of Alice do not depend on the choice of Bob's measurement, and hence this sample prediction belongs to the possibilistic theory "no signalling from Bob to Alice", which are those satisfying the relation

$$\pi_{a,b}(x,+) + \pi_{a,b}(x,-) = \pi_{a,b'}(x,+) + \pi_{a,b'}(x,-)$$

together with its obvious variants. But when Bob chooses to measure b', he gets that the outcome $+$ is impossible when Alice measures a, whereas the outcome $+$ is possible when Alice measures a'. Hence, the prediction in figure 2.2(b) does not belong to the possibilistic theory "no signalling from Alice to Bob".

[1] Formally, this is isomorphic to the semiring of boolean truth values $(\top, \bot, \vee, \wedge)$.

[2] Here, it doesn't matter whether the coin flip itself is probabilistic or possibilistic.

		a	
		$+$	$-$
b	$+$	0	$*$
	$-$	0	$*$

(a) When Alice measures a and Bob measures b.

		a		a'	
		$+$	$-$	$+$	$-$
b	$+$	0	$*$	0	$*$
	$-$	0	$*$	$*$	0
b'	$+$	0	$*$	$*$	0
	$-$	0	0	$*$	$*$

(b) For the full Bell test, where Alice and Bob each can choose among two measurements.

Figure 2.2: Example predictions in a general possibilistic theory.

The search for possibilistic quantum mechanics. Quantum mechanical theories are a very special class of general probailistic theories. One of the original hopes of this work was that there might be a combinatorial framework for a possibilistic analogue of quantum mechanics encompassing the Spekkens model and also comprising other models that have interesting combinatorial properties. So far, this hope has remained unfulfilled. I will briefly digress to describe the ideas involved. The crucial structure of quantum theory is that of a Hilbert space, i.e. a vector space together with a positive definite bilinear form. The combinatorial analogue of a vector space is given by the mathematical structure of a *matroid* (see e.g. [Oxl92]). In the possibilistic framework, numerical values of the scalar product are irrelevant; the only information retained is whether a scalar product vanishes or not, i.e. the orthogonality relation. This led me to the study of matroids having a compatible orthogonality relation. With a good definition of compatibility, the linear subspaces of the matroid form an orthomodular lattice, hence this is closely connected to quantum logic. Then the whole structure of matroid plus orthogonality can also be encoded in a single function "orthogonal complement" going from subsets to subsets, such that the matroid linear hull of a subset can be recovered as the orthogonal bicomplement. But then since the orthogonality relation itself determines the orthogonal complement, the matroid structure is determined by the orthogonality relation alone. Such a relation is most conveniently represented as a graph, and therefore one can also speak of an *orthogonality graph*. Not every graph is an orthogonality graph in this sense; in fact, all the examples of orthogonality graphs that I could find can be decomposed as an orthogonal sum into one- and two-dimensional components, so that no interesting examples are known to me. In particular, the Spekkens two-qubit theory [Spe07, IV] does not fit into such a framework.

There are two further directions that should be explored along these lines: first, to see if categorical quantum mechanics [AC08] contains possibilistic theories. And second, to draw the comparison to modal logic and its "possible worlds".

2.4 Possibilistic Bell inequalities

The possibilistic Bell test scenario has been mentioned previously. In this section, I want to formulate the theory of possibilistic local hidden variables, mention the computation of possibilistic Bell inequalities, and show that possibilistic Popescu-Rohrlich boxes violate these inequalities.

The theory of possibilistic local hidden variables. To begin, a deterministic local hidden variable model is defined to be a prediction where each measurement has a definite outcome,

		a		a'	
		$+$	$-$	$+$	$-$
b	$+$	$*_{1,2}$	0	$*_1$	$*_2$
	$-$	0	$*_{3,4}$	$*_3$	$*_4$
b'	$+$	$*_1$	$*_3$	$*_{1,3}$	0
	$-$	$*_2$	$*_4$	0	$*_{2,4}$

(a) A possibilistic hidden variable model occuring in the Spekkens theory.

		a		a'	
		$+$	$-$	$+$	$-$
b	$+$	$*$	0	$*$	0
	$-$	0	$*$	0	$*$
b'	$+$	$*$	0	0	$*$
	$-$	0	$*$	$*$	0

(b) A possibilistic Popescu-Rohrlich box.

Figure 2.3: More example predictions for the possibilistic Bell test system.

and Alice's and Bob's measurements are independent in the sense that a composite outcome (x, y) is possible if and only if x is possible for Alice's measurement and y is possible for Bob's measurement.

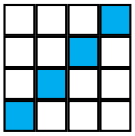
Then, a possibilistic local hidden variable model is defined to be a combination of deterministic local hidden variable models. This means that in can be written in the form

$$\pi_{a,b}(x,y) = \sum_{\lambda} \pi_a^{\lambda}(x) \cdot \pi_b^{\lambda}(y) \tag{2.4.1}$$

and analogously for $a \leftrightarrow a'$ and $b \leftrightarrow b'$. The parameter λ indexes the possibility distributions π_a^{λ}, $\pi_{a'}^{\lambda}$, π_b^{λ} and $\pi_{b'}^{\lambda}$ for Alice's and Bob's subsystems separately. The sum over λ allows for classical random-possibilistic correlations between the systems. Equation (2.4.1) corresponds to the representation of a probabilistic local hidden variable model as an integral over deterministic product models.

By checking all the possible combinations of measurements that can be done, one can show that the entangled states in the two-qubit Spekkens model are indeed always local hidden variable models. For the (inconsistent) probabilistic interpretation, this also has been observed by Spekkens [Spe07, VII]. Figure 2.3(a) shows the possibilistic prediction obtained by measuring $a = b = \boxed{+}\boxed{+}\boxed{-}\boxed{-}$, $a' = b' = \boxed{+}\boxed{-}\boxed{+}\boxed{-}$ in the state

$$(1 \cdot 1) \vee (2 \cdot 2) \vee (3 \cdot 3) \vee (4 \cdot 4) =$$



The indices on the $*$'s in figure 2.3(a) indicate a decomposition into deterministic local hidden variable models.

Popescu-Rohrlich boxes. Not all no-signalling predictions have local hidden variable models. In particular, the prediction shown in figure 2.3(b) does not; the pattern of 0's and $*$'s is reminiscient of a probabilistic Popescu-Rohrlich box, and therefore one might regard it as a possibilistic Popescu-Rohrlich box. By applying the permutations $+ \leftrightarrow -$, $a \leftrightarrow a'$ and $b \leftrightarrow b'$, one obtains eight different possibilistic Popescu-Rohrlich boxes.

Bell inequalities. How can one recognize a hidden variable model when one sees one? In the probabilistic case, there is a set of necessary and sufficient criteria: the CHSH inequalities. In the

		a		a'	
		$+$	$-$	$+$	$-$
b	$+$	L		R_1	
	$-$				
b'	$+$	R_2			
	$-$				R_3

Figure 2.4: Up to permutations, this represents the only possibilistic Bell inequality (2.4.2).

present framework, an analogous characterization turns out to be possible. Using an appropriate variant of Fourier-Motzkin elimination, it can be proven that any subset of predictions that is closed under the possibilistic sum (2.3.2) can be characterized by a collection of inequalities which are linear with respect to the operations (2.3.2). In fact, this method can also be used to *calculate* these inequalities. Besides the no-signalling equations and the requirement that each of the four subsquares needs to contain at least one $*$, one ends up with the non-trivial Bell inequality

$$\pi(L) \leq \pi(R_1) + \pi(R_2) + \pi(R_3) \qquad (2.4.2)$$

where the arguments represent measurement outcomes as depicted in figure 2.4, together with the obvious permutations $+ \leftrightarrow -$, $a \leftrightarrow a'$ and $b \leftrightarrow b'$ of these. Due to the form of the algebraic operations (2.3.2), such an inequality (2.4.2) is equivalent to the following implication:

$$\text{If } \pi(L) = *, \text{ then also } \pi(R_i) = * \text{ for at least one } i \in \{1, 2, 3\}. \qquad (2.4.3)$$

It is immediate to check that any deterministic hidden variable model satisfies the implication (2.4.3). But then by linearity, any hidden variable model satisfies this inequality. On the other hand, the Popescu-Rohrlich box from figure 2.3(b) violates several of the permutations of this inequality. It is guaranteed by the mathematics underlying the computation that any prediction that is not a hidden-variable model will violate at least one of (2.4.2)'s permutations $+ \leftrightarrow -$, $a \leftrightarrow a'$ and $b \leftrightarrow b'$.

Further details on the possibilistic Bell inequalities and the Fourier-Motzkin-type algorithm underlying their computation will appear elsewhere. A `C` implementation of this algorithm can be downloaded from [Fri09a], together with the input file used for the computation of figure 2.4.

2.5 Discussion of probabilistic vs. possibilistic

Obviously, every probabilistic prediction determines a corresponding possibilistic one, simply by taking an outcome to be impossible if it has probability 0, and taking it to be possible otherwise. From this naive point of view, probabilistic theories have a higher predictive power than their possibilistic counterparts, since an actual numerical value for a probability is certainly better than just the statement "the outcome can occur". This is a possible argument against possibilistic physics. In this section, I want to present some arguments in favor of it.

Hypothesis testing is possibilistic. How does one compare a probabilistic theory with experiment? In accordance with the scientific method, the goal of an experiment is to try and falsify the theory. In most cases—due to the non-deterministic nature of probability—this cannot be done in a single measurement alone. Instead, a series of measurements is required.

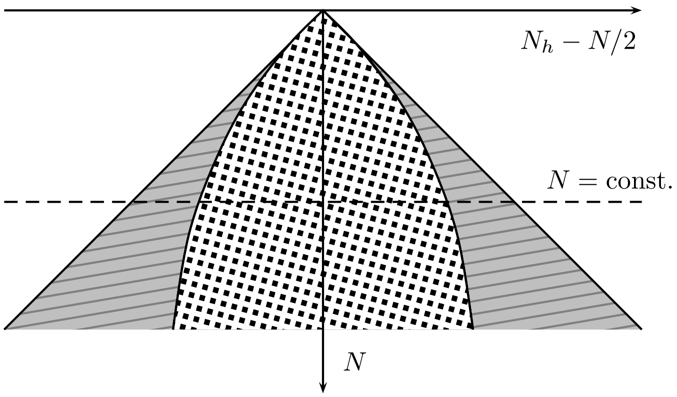


Figure 2.5: Regions of acceptance and rejection for a statistical significance test of the hypothesis "The coin is fair" (schematic).

For simplicity, I want to consider tests of a single hypothesis only and not comparison tests of two or more hypotheses, as they are usually done in statistics. So consider a coin flip as an experiment having the outcome h (heads) or t (tails). For example, the hypothesis may be that the coin is fair, i.e. that each outcome occurs with probability 1/2. Our experimentalist friend would run the experiment a certain number of times, say N times, and naively he would compare the number of heads N_h with the numbers of tails $N - N_h$. He would then run a statistical test on the pair (N_h, N) to determine how statistically significant the deviation from the expected value $(N/2, N)$ turns out to be. Based on an initially stipulated significance level, the hypothesis will be regarded either as confirmed or as falsified. See figure 2.5 for a schematic illustration: the fair coin hypothesis gets accepted in the square-filled region and rejected in the grey ruled region of (N_h, N)-space.

What this means is nothing but that the theory predicts the outcomes in the square-filled region to be possible, and the outcomes in the grey ruled region to be impossible. In this sense, hypothesis testing is possibilistic. Of course this is slightly misleading since the boundary between the acceptance region and the rejection region is not sharp. But then in fundamental physics, how do we know that this is the way it has to be? Upon regarding the hypothesis test as part of the physical theory itself, one can set up a possibilistic theory of measurement series and thereby obtain a precise sharp boundary between the acceptance region and the rejection region. Then given the theory, no debate over the statistical significance of experimental deviations from theoretical predictions would be possible. It is in this sense that a possibilistic theory—on the level of *series* of measurements—has a *higher predictive power* than a probabilistic one: the conditions for its falsification are absolutely clear-cut.

Probabilistic theories specify possible probabilities. There is another sense in which a probabilistic theory has a possibilistic aspect: any prediction is either allowed by the theory, or it is not. For example in the Bell test system, the boundary between the quantum region and the non-quantum region is absolutely sharp. The outcome probabilities within the quantum region can possibly occur in our quantum world, while the others cannot. So why is it that in this case, one uses probability on one level, but possibility on the other level?

What is the physics behind randomness? There is another important issue pertaining to series of measurements, which can also be illustrated using the fair coin example. Suppose that our experimentalist friend has conducted the experiment 40 times, and he has obtained the following series of outcomes,

`hhhhhhhhhhhhhhhhhhhhtttttttttttttttttttt.`

Then although the relative frequency of the two outcomes is exactly as expected, no sensible physicist would accept this series of outcomes as a confirmation of the fair coin hypothesis. Instead, he would possibly prefer an explanation like,

> “Some evil theorist has been tinkering with the apparatus while I was on coffee break.”

The same problem appears for the following conceivable series of outcomes,

`hthththththththththththththththththththt.`

The reason that both of the series of outcomes cannot be accepted as realistic is that a probabilistic theory actually predicts more than just the relative frequency of outcomes. It also predicts that the measurements ought to be statistically independent! However, actual criteria for when a series of outcomes is reasonably random are hard to come by; the mathematically soundest one is the concept of *Kolmogorov randomness*, which is based on concepts from computer science. However, Kolmogorov randomness as well as related measures of randomness are so intricate that a *direct* physical justification for the observation that realistic series of outcomes show statistical independence seems out of reach. Possibilistic physics would now come into the game if one can find a possibilistic theory of measurement series, where the possible outcomes all look suitably random, such that this theory can be derived from some basic physical principles.

Almost surely means certainly. In any probabilistic theory, an event that has probability 1 occurs with absolute certainty, while an event with probability 0 will certainly not occur. This assumption is necessary since otherwise tests of statistical significance would be meaningless. This excludes the possibility that some fixed measurement outcome occurs sometimes, but so infrequently that its occurence has an asymptotic relative frequency of 0. Why should this possibility be unrealistic? Finding an answer to this question is another problem that does not arise in possibilistic physics.

Flying saucers. Finally, let me give a possibilistic analysis of a situation described by Feynman in his *Messenger Lectures* [Fey]:

> I had a conversation about flying saucers some years ago with a layman—because I am scientific I know all about flying saucers. So I said, “I don’t think there are flying saucers”. So my antagonist said, “Is it impossible that there are flying saucers? Can you prove that it’s impossible?” “I don’t know, I can’t prove it’s impossible. It’s just very unlikely”. At that he said, “You are very unscientific. If you can’t prove it impossible, then how can you say that it’s unlikely?” But that is the way that is scientific. It is scientific only to say what’s more likely and [sic] less likely, and not to be proving all the time possible and impossible.

Let me try to circumvent the deep waters of the interpretation of subjective probability here and only mention the possibilistic alternative to Feynman’s point of view. One may consider the known answers to questions of the form

“Does this photograph show a real flying saucer?”
“Has this person been abducted by actual aliens?”

as a series of outcomes of a measurement taking values in the set $\{\text{yes}, \text{no}\}$. To the best of my knowledge, many of these questions have received a definite “no”, but so far none of them has seen a definite “yes”. Therefore, the prediction

$$\pi(\text{yes}) = *, \quad \pi(\text{no}) = 0$$

has already been falsified. The two remaining predictions

$$\begin{aligned} \text{Feynman:}\ \ & \pi(\text{yes}) = 0, \quad \pi(\text{no}) = * \\ \text{layman:}\ \ & \pi(\text{yes}) = *, \quad \pi'(\text{no}) = * \end{aligned}$$

are still valid hypotheses. However, since the first prediction π can be falsified while the second π' cannot, Feynman’s prediction that flying saucers do not exist is clearly superior over the layman’s hypothesis that both the existence and the non-existence of flying saucers is possible. More generally, suppose that the set of possible outcomes for prediction 1 is a proper subset of the set of possible outcomes for prediction 2. Then, as long as prediction 1 is consistent with observations, it should be preferred over prediction 2, due to its higher predictive power. This may be regarded as a manifestation of Occam’s razor, in the sense that the more parsimonious explanation is the better one.

Chapter 3

The quantum region for von Neumann measurements with postselection

3.1 Introduction

The following observation was made in chapter 1: upon subjecting any quantum system to the procedure,

(a) prepation of some initial state $|\psi\rangle$,

(b) application of a dichotomic von Neumann measurement q,

(c) postselection[1] with respect to some final state $|\phi\rangle$ such that $\langle\psi|\phi\rangle = 0$,

the usual rules of quantum mechanics imply that the two outcomes of q both necessarily occur with a conditional probability of 1/2. This is easiest to see on the level of amplitudes, where it follows from

$$0 = \langle\psi|\phi\rangle = \langle\psi|q|\phi\rangle + \langle\psi|(1-q)|\phi\rangle,$$

so that the two probabilities for measuring $q = 1$ or $q = 0$ are given by, respectively,

$$P(q=1) = \frac{|\langle\psi|q|\phi\rangle|^2}{|\langle\psi|q|\phi\rangle|^2 + |\langle\psi|(1-q)|\phi\rangle|^2} = \frac{1}{2}, \qquad P(q=0) = \frac{|\langle\psi|(1-q)|\phi\rangle|^2}{|\langle\psi|q|\phi\rangle|^2 + |\langle\psi|(1-q)|\phi\rangle|^2} = \frac{1}{2}.$$

Intuitively, this means that a dichotomic von Neumann measurement with postselection which is orthogonal to the inital state is guaranteed to be a perfectly unbiased random number generator.

So when $\langle\psi|\phi\rangle = 0$, there is only a single probability distribution over the outcomes which can arise for an intermediate dichotomic von Neumann measurement. Now the obvious question is, how does this generalize? What if the measurement has n outcomes instead of just 2? What if $|\phi\rangle$ is not orthogonal to $|\psi\rangle$? These are the kind of questions to be answered here.

Note that these questions are of interest in the foundations of quantum mechanics, since they are of the form "under which conditions is it possible to find a quantum-mechanical model for a given set of probabilities?".

[1] For an introduction to quantum mechanics with postselection and the counterintuitive effects it gives rise too, see e.g. [AV07].

Synopsis. Section 3.2 derives some elementary mathematical results about vectors in $\mathbb{C}^n$. The main result about probability distributions for von Neumann measurements with postselection follows in section 3.3. Then section 3.4 discusses some particular special cases of this result and determines to what extent transition probabilities between quantum states can be enhanced by a von Neumann measurement. Finally, section 3.5 briefly concludes.

Acknowledgements. I would like to thank Andreas Winter for an invitation to visit the Centre for Quantum Technologies, where this research has been conducted. I am indebted to Reinhard Werner for stimulating questions during a talk. Finally, this work would not have been possible without the excellent research conditions within the IMPRS graduate program at the Max Planck Institute and the invaluable advice provided by my supervisor Matilde Marcolli.

3.2 Mathematical Preliminaries

We will later need a solution to the following elementary mathematical problem:

> **Question:** Given n non-negative real numbers $x_1, \ldots, x_n$, is it possible to find complex numbers $z_1, \ldots, z_n$ such that $|z_k| = x_k$ and $\sum_k z_k = 0$?

We will see soon that this question can easily be reduced to the following proposition, where now the requirement $\sum_k z_k = 0$ has been replaced by the condition $\sum_k z_k = 1$.

Proposition 3.2.1. *For given $x_1, \ldots, x_n \in \mathbb{R}_{\geq 0}$, there exist $z_1, \ldots, z_n \in \mathbb{C}$ with*

$$|z_k| = x_k, \qquad \sum_{k=1}^{n} z_k = 1$$

if and only if the inequalities

$$x_k \leq 1 + \sum_{\substack{j=1 \\ j\neq k}}^{n} x_j, \qquad \sum_{j=1}^{n} x_j \geq 1 \tag{3.2.1}$$

hold.

Proof. The necessity of (3.2.1) is a direct consequence of the triangle inequality. The burden of the proof lies in showing that these inequalities are sufficient to guarantee the existence of a solution for the z_k. For this, it can be assumed without loss of generality that all the x_k are strictly positive.

Now we apply induction on n. In the case $n = 1$, the inequalities state that $x_1 \leq 1$, and $x_1 \geq 1$, so that $x_1 = 1$, which is what is required. For the induction step, given $x_1, \ldots, x_{n+1}$ which satisfy (3.2.1), it can be assumed that these numbers are ordered such that $x_1 \leq \ldots \leq x_{n+1}$. Then up to an irrelevant global phase, it is enough to find $z_1, \ldots, z_n \in \mathbb{C}$ such that $|z_k| = x_k$ and $\sum_{k=1}^{n} z_k = y$ for some freely chosen $y \in [|1 - x_{n+1}|, 1 + x_{n+1}]$, for these are the values of $|1-z_{n+1}|$ which can be attained by choosing the argument of z_{n+1} with $|z_{n+1}| = x_{n+1}$ appropriately. Using a rescaled version of the induction assumption, this can be done if and only if

$$x_k \leq y + \sum_{\substack{j=1 \\ j\neq k}}^{n} x_j, \qquad \sum_{j=1}^{n} x_j \geq y$$

By the assumed ordering of the x_k, the first inequality holds if and only if $y \geq x_n - \sum_{j=1}^{n-1} x_j$. Taking all conditions on y together, the number y has to lie in the interval $[|1-x_{n+1}|, 1+x_{n+1}]$, as well as in the interval $[x_n - \sum_{j=1}^{n-1} x_j, \sum_{j=1}^{n} x_j]$, and also y has to be positive. Therefore, the problem can be solved if and only if these two intervals have a non-empty intersection on the positive real axis. The intervals intersect if and only if the lower endpoint of any one interval is not above the upper endpoint of the other interval; in the present case,

$$|1-x_{n+1}| \leq \sum_{j=1}^{n} x_j, \qquad x_n - \sum_{j=1}^{n-1} x_j \leq 1 + x_{n+1}.$$

Now the first inequality holds by the assumption (3.2.1), while the validity of the second inequality already follows from the assumed ordering $x_n \leq x_{n+1}$. By $\sum_{j=1}^{n} x_j > 0$, the intervals even intersect on the positive real axis, so that a consistent choice for y is possible. This finishes the proof. □

Corollary 3.2.2. *Given non-negative real numbers $x_1, \ldots, x_n$, there exist complex numbers $z_1, \ldots, z_n$ with*

$$|z_k| = x_k, \qquad \sum_{k=1}^{n} z_k = 0$$

if and only if the inequalities

$$x_k \leq \sum_{\substack{j=1 \\ j\neq k}}^{n} x_j \tag{3.2.2}$$

hold.

Proof. If all x_k vanish, there is nothing to prove. If there is some k with $x_k > 0$, then it suffices to find z_j's for $j \neq k$ with

$$|z_j| = x_j, \;\; j \neq k, \qquad \sum_{\substack{j=1 \\ j\neq k}}^{n} z_j = x_k.$$

This is possible due to proposition 3.2.1 rescaled by a factor of x_k^{-1}. □

Lemma 3.2.3. *Given $z \in \mathbb{C}^n$, there exist $\psi, \phi \in \mathbb{C}^{n+2}$ with*

$$|\psi|^2 = 1 = |\phi|^2, \qquad \overline{\psi}_k \phi_k = \begin{cases} z_k & \text{for } k = 1, \ldots, n \\ 0 & \text{for } k = n+1, n+2 \end{cases}$$

if and only if the inequality

$$\sum_{k=1}^{n} |z_k| \leq 1 \tag{3.2.3}$$

holds.

Proof. The necessity of (3.2.3) follows from the Cauchy-Schwarz inequality evaluated on ψ and ϕ', where $\phi' \in \mathbb{C}^{n+2}$ is defined by the requirements that firstly, $|\phi'_k| = |\phi_k|$, and that secondly, the argument of ϕ'_k is such that $\overline{\psi}_k \phi'_k = |z_k| \in \mathbb{R}_{\geq 0}$. For the sufficiency of (3.2.3), choose any complex square root $\sqrt{z_k}$ for each z_k and consider the two vectors

$$\psi_k = \begin{cases} \overline{\sqrt{z_k}} & \text{for } k = 1, \ldots, n \\ \sqrt{1 - \sum_{j=1}^{n} |z_j|} & \text{for } k = n+1 \\ 0 & \text{for } k = n+2 \end{cases}, \qquad \phi_k = \begin{cases} \sqrt{z_k} & \text{for } k = 1, \ldots, n \\ 0 & \text{for } k = n+1 \\ \sqrt{1 - \sum_{j=1}^{n} |z_j|} & \text{for } k = n+2 \end{cases}.$$

□

3.3 Von Neumann measurements with postselection

Suppose now that we have our quantum system prepared in some initial state $|\psi\rangle$, apply a von Neumann measurement of some observable E having finite spectrum with distinct eigenvalues $\lambda_1, \ldots, \lambda_n$ and spectral projectors $E_1, \ldots, E_n$,

$$E = \sum_{k=1}^{n} \lambda_k E_k$$

and postselect with respect to some final state $|\phi\rangle$. Under these conditions, the probability—conditional with respect to successful postselection—of getting the outcome λ_k for the measurement of E is given by (see e.g. [AV07])

$$P(k) = \frac{|\langle\psi|E_k|\phi\rangle|^2}{\sum_{j=1}^{n} |\langle\psi|E_j|\phi\rangle|^2}, \tag{3.3.1}$$

where the normalization factor

$$S \equiv \sum_{j=1}^{n} |\langle\psi|E_j|\phi\rangle|^2$$

stands for the (unconditional) probability of successful postselection. Without loss of generality, we will label the outcomes by $1, \ldots, n$ instead of the eigenvalues $\lambda_1, \ldots, \lambda_n$ as the labels for measurement outcomes; this is entirely for notational convenience only.

Question 3.3.1. Given the transition amplitude $A = |\langle\psi|\phi\rangle|$, which probability distributions $P(\cdot)$ on $\{1, \ldots, n\}$ can occur in this way for which values of the success probability S?

Note that it is no loss of generality to ask this question only for pure states, since a mixed state can always be purified by adding an ancilla to the system with which it is entangled. Furthermore, just like the quantities $P(k)$ and S, the transition amplitude A also has an operational interpretation as the success probability of a kind of "postselection", namely postselection in the case when the intermediate measurement is not present. Therefore, one may think of all the quantities $P(k)$, S and A as given in terms of experimental data, and the question then is whether it is possible to find a quantum-mechanical model reproducing these particular values, without specifying the Hilbert space dimension or anything else in advance.

The case $A = 0$, $n = 2$ and $S \neq 0$ of this question has been treated in section 2 of [Fri10a], where it was found that, surprisingly, the only possibility is given by $P(1) = P(2) = 1/2$. Using the elementary mathematical results derived in the previous section, we are now ready to answer this question in complete generality.

Theorem 3.3.2. *A given $P(\cdot)$ with given A and S can occur in this way if and only if the following inequalities hold:*

$$\sqrt{P(k)} \leq \frac{A}{\sqrt{S}} + \sum_{j \neq k} \sqrt{P(j)}, \qquad \frac{A}{\sqrt{S}} \leq \sum_{k=1}^{n} \sqrt{P(k)} \leq \frac{1}{\sqrt{S}} \tag{3.3.2}$$

Proof. The main idea here is to use the completeness relation $\sum_k E_k = \mathbb{1}$ in order to obtain an identity for amplitudes

$$\langle\psi|\phi\rangle = \sum_{k=1}^{n} \langle\psi|E_k|\phi\rangle$$

and then translate this into conditions on the probabilities (3.3.1). To this end, we can apply 3.2.2 to

$$z_k = \langle\psi|E_k|\phi\rangle, \;\; k = 1, \ldots, n, \qquad z_{n+1} = -\langle\psi|\phi\rangle.$$

Then upon setting $x_k \equiv \sqrt{P(k)S} = |\langle\psi|E_k|\phi\rangle|$ for $k = 1, \ldots, n$, and defining $x_{n+1} = A$, it follows that the first inequalities of (3.3.2) are necessary, as well as the first inequality of the second formula. In the case that the E_k are rank-one projectors—so that they define an orthonormal basis of the Hilbert space—the remaining inequality is implied by lemma 3.2.3 applied to $z_1, \ldots, z_n$. In general, we can choose an orthonormal basis $\{|j\rangle\}_j$ in which all the E_k are diagonal, and apply an argument analogous to the proof of lemma 3.2.3 as follows:

$$\sum_{k=1}^{n} |z_k| = \sum_{k=1}^{n} |\langle\psi|E_k|\phi\rangle| \leq \sum_j |\langle\psi|j\rangle\langle j|\phi\rangle|.$$

Now let $|\phi'\rangle$ be the vector which has the components $\langle j|\phi'\rangle$ such that $\langle\psi|j\rangle\langle j|\phi'\rangle = |\langle\psi|j\rangle\langle j|\phi\rangle|$. It follows that

$$\sum_{k=1}^{n} |z_k| \leq \sum_j \langle\psi|j\rangle\langle j|\phi'\rangle = \langle\psi|\phi'\rangle \leq 1,$$

as was to be shown.

To see that the inequalities (3.3.2) taken together are also sufficient for the existence of a quantum-mechanical model, we again set x_k to be given by the square roots of the unnormalized probabilities as $x_k \equiv \sqrt{P(k)S}$ for $k = 1, \ldots, n$, and again define $x_{n+1} = A$. Then again by 3.2.2, some corresponding z_k's with $\sum_{k=1}^{n+1} z_k = 0$ can now assumed to be given, and they also satisfy $\sum_{k=1}^{n} |z_k| = \sum_{k=1}^{n} x_n \leq 1$ by the assumption (3.3.2). Now one can use lemma 3.2.3 to obtain the states on $\mathbb{C}^{n+2}$ which are given by

$$|\psi\rangle = \sum_{k=1}^{n+2} \psi_k |k\rangle, \qquad |\phi\rangle = \sum_{k=1}^{n+2} \phi_k |k\rangle$$

in conjunction with $E_k = |k\rangle\langle k|$ for $k = 1, \ldots, n$. The remaining two rank-one projections

$$|n+1\rangle\langle n+1|, \qquad |n+2\rangle\langle n+2|$$

can be added to any one or two of the E_k, so that one obtains a complete set of projectors. Then $\sqrt{P(k)S} = |\langle\psi|E_k|\phi\rangle|$ and $A = |\langle\psi|\phi\rangle|$ both hold by construction. The requirement $S = \sum_{k=1}^{n} |\langle\psi|E_k|\phi\rangle|^2$ is automatic by normalization of the probability distribution $P(\cdot)$. □

It is possible to rewrite the inequalities (3.3.2) in a slightly more convenient form. Since the first inequality holds for all k if and only if it holds for that k for which $P(k)$ is largest, it is enough to require

$$2\sqrt{\max_k P(k)} \leq \frac{A}{\sqrt{S}} + \sum_{k=1}^{n} \sqrt{P(k)}$$

Now using the definitions of “moments”

$$M_\infty \equiv \max_k P(k), \qquad M_{1/2} \equiv \sum_{k=1}^{n} \sqrt{P(k)} \tag{3.3.3}$$

we can see that the inequalities (3.3.2) are in fact equivalent to

$$\boxed{2\sqrt{M_\infty} - M_{1/2} \leq \frac{A}{\sqrt{S}} \leq M_{1/2} \leq \frac{1}{\sqrt{S}}} \tag{3.3.4}$$

so that the dependence on the distribution $P(\cdot)$ is only through the dependence on the quantities M_∞ and $M_{1/2}$.

Remark 3.3.3. (a) The proof of the theorem shows that it is sufficient to employ Hilbert spaces of dimension at most $n{+}2$. It is unclear whether the conditions (3.3.2) also guarantee the existence of a quantum-mechanical model using a Hilbert space of dimension n or $n{+}1$.

(b) One can also reformulate (3.3.2) in terms of the min-entropy and the Rényi 1/2-entropy

$$H_{1/2} = 2\log M_{1/2}, \qquad H_\infty = -\log M_\infty$$

where it means that

$$2\log\left(2e^{-H_\infty/2} - e^{H_{1/2}/2}\right) \leq \log\frac{A^2}{S} \leq H_{1/2} \leq \log\frac{1}{S}$$

Intuitively, the last inequality in this chain means that the more information one wants to obtain about the postselected ensemble, the lower the optimal probability for conducting a successful measurement with postselection is going to be. And by the second inequality in the chain, higher information gain for given success probability also implies lower transition amplitude from $|\psi\rangle$ to $|\phi\rangle$.

3.4 Discussion

Let us now look at some specific cases of this result.

Case $A = 0$, S arbitrary. This was studied for $n = 2$ in [Fri10a]. As long as we allow the success probability S to be arbitrarily small, all that remains are the inequalities

$$\sqrt{P(k)} \leq \sum_{j\neq k} \sqrt{P(j)} \tag{3.4.1}$$

For $n = 2$, this reads $\sqrt{P(1)} \leq \sqrt{P(2)}$ and $\sqrt{P(2)} \leq \sqrt{P(1)}$, implying that $P(1) = P(2) = 1/2$. Hence a dichotomic measurement with postselection which is orthogonal to the initial state is guaranteed to be a perfectly unbiased random number generator. Generally, the $\sqrt{P(k)}$ which satisfy (3.4.1) lie in the convex cone spanned by the rays of the form

$$\sqrt{P(k)} = \delta_{kl} + \delta_{km}$$

for some pair of indices $l \neq m$. The $n = 3$ case is illustrated in figure 3.1; one obtains a circular region in probability space, due to the fact that its boundary is then given by quadratic equations. Just as it should due to the result for the $n = 2$ case, this region intersects with any side of the triangle in exactly the middle of that side.

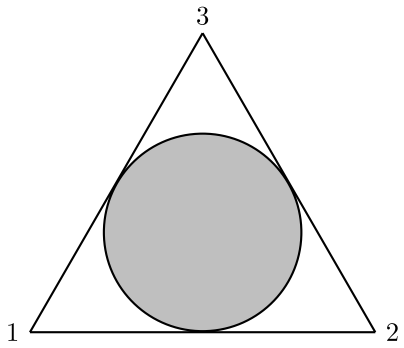


Figure 3.1: The quantum-mechanical region for $A = 0$ (orthogonal postselection), $n = 3$, and arbitrary success probability S (ternary plot).

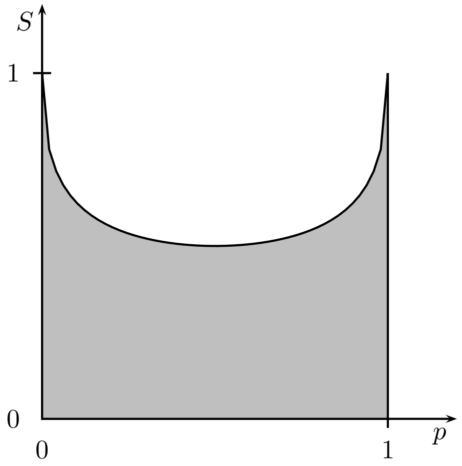


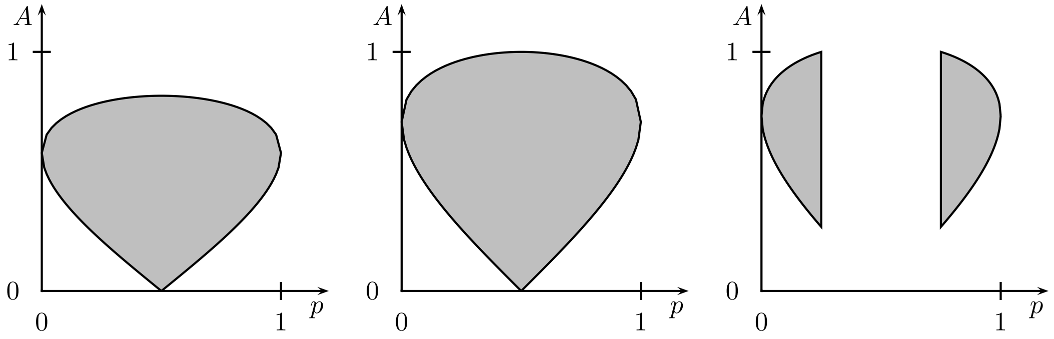
Figure 3.2: For $n = 2$, the possible quantum-mechanical success probabilities as a function of p.

Case $A \neq 0$, S arbitrary. Here, it is possible for any $P(\cdot)$ to find some appropriately small success probability S such that all inequalities in (3.3.4) hold, so no constraints abound. This is one reason why it is important to always consider S as an additional parameter.

Case $n = 2$, general. Here, the two probability values $P(1)$ and $P(2)$ determine each other uniquely, so let us write $P(1) = p$ and $P(2) = 1 - p$. Then the inequalities are

$$\left|\sqrt{p} - \sqrt{1-p}\right| \leq \frac{A}{\sqrt{S}} \leq \sqrt{p} + \sqrt{1-p} \leq \frac{1}{\sqrt{S}} \tag{3.4.2}$$

The projection of this into the p-S-plane, where only the last inequality is relevant, is shown in figure 3.2. For fixed S, some sections of the quantum region are graphed in figure 3.3. The first two inequalities of (3.4.2) define the upper and lower boundary curves in this case, while the third inequality ledas to vertical cuts whenever $S > 1/2$.



(a) $S = 1/3$.

(b) $S = 1/2$.

(c) $S = 2/(2+\sqrt{3}) \approx 0.536$.

Figure 3.3: Again $n = 2$. These plots show the quantum-mechanical region for (A, p) for some values of S. For bigger S than those shown, according to figure 3.2, the region rapidly shrinks down to the $p = 0$ and $p = 1$ lines.

The A-S-region. How does the transition amplitude relate in general to the probability of successful postselection? To study this, it is best to consider the inequalities in the form (3.3.4). Figure 3.4.3 shows an illustration of the following proposition.

Proposition 3.4.1. *For a given number of outcomes n, a pair of values (A, S) can appear in quantum theory if and only if*

$$\boxed{\frac{A^2}{n} \leq S \leq \frac{A^2+1}{2}} \tag{3.4.3}$$

Proof. Again it is first shown that these inequalities are necessary. Since $M_{1/2} \leq \sqrt{n}$, the second inequality in (3.3.4) implies that

$$A^2 \leq nS.$$

Now consider the expression

$$\frac{A^2}{S} + \frac{1}{S} \overset{(3.3.4)}{\geq} 4M_\infty + 2M_{1/2}^2 - 4\sqrt{M_\infty}M_{1/2} = 2\left[M_\infty + (M_{1/2} - \sqrt{M_\infty})^2\right]$$

and assume without loss of generality that $P(n) = \max_k P(k)$, so that

$$\frac{A^2}{S} + \frac{1}{S} \geq 2\left[P(n) + \left(\sum_{k=1}^{n-1}\sqrt{P(k)}\right)^2\right] \geq 2\left[P(n) + \sum_{k=1}^{n-1} P(k)\right] = 2,$$

as was to be shown.

For checking sufficiency of (3.4.3), consider first the case that $S \leq A^2$. Then since $2\sqrt{M_\infty} - M_{1/2}$ can at most be 1, it follows that the first inequality of (3.3.4) holds automatically. Now the possible values for $M_{1/2}$ are given by the closed interval $[1, \sqrt{n}]$, so that it is possible to find some value for $M_{1/2}$ in this interval which also satisfies (3.3.4) whenever $\frac{1}{\sqrt{S}} \geq 1$, which holds trivially, and $\frac{A}{\sqrt{S}} \leq \sqrt{n}$, which is true by assumption.

It remains to prove sufficiency when $A^2 \leq S \leq \frac{A^2+1}{2}$. Here, it is in fact enough to consider probability distributions $P(\cdot)$ supported on two elements, which brings us effectively down to the dichotomic case $n = 2$ from equation (3.4.2). By $\frac{A}{\sqrt{S}} \leq 1$, the middle inequality is automatic, so

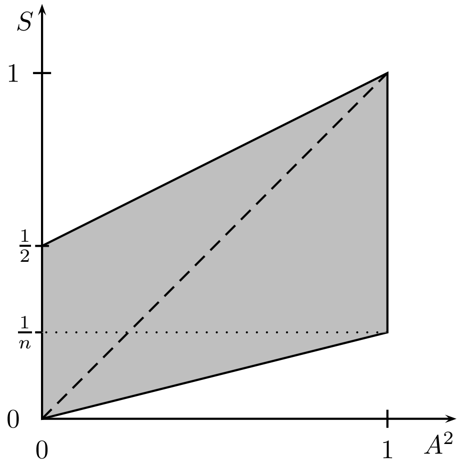


Figure 3.4: The quantum region of transition probabilities: A^2 is the transition probability without measurement, while S is the transition probability with n-ary von Neumann measurement. All points above the dashed line $S = A^2$ represent a measurement-enhanced transition probability.

one only needs to take care of the remaining two. A direct calculation finally shows that when solving the equation $\sqrt{p} + \sqrt{1-p} = \sqrt{S}$ for p, then the equation

$$\left|\sqrt{p} - \sqrt{1-p}\right| = \frac{A}{\sqrt{S}}$$

holds for the maximal allowed amplitude $A = \sqrt{2S-1}$. □

This result 3.4.1 states in particular that transition probabilities between quantum states can be enhanced by an appropriate intermediate von Neumann measurement, the outcome of which can be discarded. This constitutes a (rather weak) kind of measurement-based quantum control. (3.4.3) shows that when using such a procedure, the error probability—i.e. the probability that the desired transition does not happen—can be reduced by a factor of up to 2.

3.5 Conclusion

In this paper, we have determined when a probability distribution over a finite number of measurement outcomes can appear for some quantum-mechanical postselected ensemble, given that the transition amplitude between the initial and final states is known, as well as the success probability of the postselection. The ensuing conditions are inequalities which depend on the probability distribution only through its Rényi 1/2-entropy and its min-entropy.

Finally, it was found that a von Neumann measurement can enhance the transition probability between the initial and the final state. The maximal enhancement is independent of the number of outcomes and is such that the error probability decreases by a factor of 2.

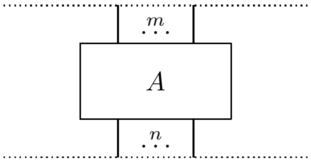
Chapter 4

A presentation of the category of stochastic matrices

4.1 The category of stochastic matrices

When turning to the actual definition of convex spaces in the next chapter, it will come in very handy to know something about stochastic matrices and the category they form. Recall that a **stochastic matrix** is a matrix with entries in $\mathbb{R}_{\geq 0}$ such that each column[1] sums to 1. The product of two stochastic matrices is again a stochastic matrix.

One way to think of a stochastic matrix A of size $n \times m$ is as a probabilistic map $[m] \to [n]$ meaning that it assigns to every $j \in [m]$ a probability distribution on $[n]$. It is useful to visualize this process as a "black box"



(4.1.1)

with m input strands and n output strands. In case of a deterministic map $[m] \to [n]$, each one of the m input strands would get mapped to a unique output strand. However now that we are dealing with probabilistic maps, an input strand may branch into several output strands, where each branch carries a certain fraction of the input strand.

These remarks should already suggest how to turn stochastic matrices into morphisms of a category:

Definition 4.1.1 (The finitary stochastic map category `FinStoMap`).

$$\mathrm{Obj}(\texttt{FinStoMap}) \equiv \mathbb{N}_0$$

$$\texttt{FinStoMap}(m,n) \equiv \textit{stochastic matrices of size } n \times m$$

Composition is defined by matrix multiplication.

[1] Hence, *stochastic matrix* here always means *column-stochastic matrix*, which is the less standard convention, but more consistent with interpreting matrix multiplication as composition of probabilistic maps (see the following paragraph).

It is clear that this satisfies the axioms of a category, as matrix multiplication is associative and the unit matrices act as identity morphisms. In the "black box" picture, composition is represented by vertical juxtaposition of the diagrams.

As an equivalent definition, one might take the morphisms in `FinStoMap` to be the conditional probability distributions on $[n]$ dependent on a distribution on $[m]$. Composition is then given by the Chapman-Kolmogorov equation. A third formulation could be as the category of communication channels on finite alphabets with concatenation of channels as composition of morphisms.

The goal of this chapter now is to find a different and purely algebraic description of `FinStoMap` in terms of generators and relations. This is related to but more elaborate than

- giving a presentation of a symmetric group S_n (see for example [CM57, 6.2])
- giving a presentation of the category of finite sets with deterministic maps (see [Mas97] for a precise statement and references)

Simpler variants of the statements and proofs given here would also apply to yield standard solutions to these two problems.

Lemma 4.1.2. `FinStoMap` *has all finite coproducts.*

Proof. $0 \in$ `FinStoMap` clearly is an initial object, thereby defining the empty coproduct. Now for binary coproducts of two objects $[n_1]$ and $[n_2]$. The inclusion morphisms are

$$\begin{pmatrix} \mathbb{1}_{n_1} \\ 0 \end{pmatrix} : [n_1] \to [n_1 + n_2], \qquad \begin{pmatrix} 0 \\ \mathbb{1}_{n_2} \end{pmatrix} : [n_2] \to [n_1 + n_2] \tag{4.1.2}$$

and satisfy the universal property

$$\begin{tikzcd}
{[n_1]} \arrow[dr, "\begin{pmatrix} \mathbb{1}_{n_1} \\ 0 \end{pmatrix}"'] \arrow[drr, bend left, "A_1"] & & \\
& {[n_1+n_2]} \arrow[r, dashed, "\exists!\, A"] & {[p]} \\
{[n_2]} \arrow[ur, "\begin{pmatrix} 0 \\ \mathbb{1}_{n_2} \end{pmatrix}"] \arrow[urr, bend right, "A_2"'] & &
\end{tikzcd}$$

since commutativity of this diagram is equivalent to $A = \begin{pmatrix} A_1 & A_2 \end{pmatrix}$, which clearly is a stochastic matrix provided that both A_1 and A_2 are. □

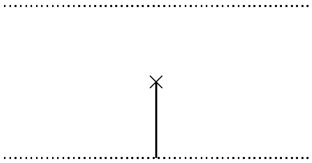
In the following, `FinStoMap` will be regarded as a strict monoidal category with respect to the coproduct. Then the tensor product of two stochastic matrices $A_1 : [m_1] \to [n_1]$ and $A_2 : [m_2] \to [n_2]$ is the block-diagonal matrix

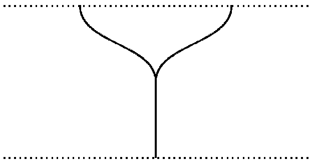
$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} : [m_1 + m_2] \to [n_1 + n_2]$$

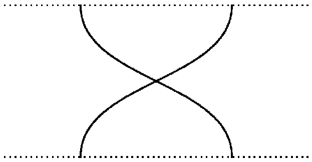
Note that this is quite different from the ordinary tensor product of matrices. In the "black box" picture, the tensor product is represented by horizontal juxtaposition of diagrams.

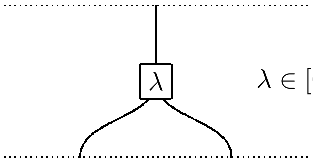
On the other hand, what follows now is the definition of a strict monoidal category `FinStoMap`$'$ in terms of generators and relations. Domain and codomain of each generator are indicated by the number of input strands and output strands, respectively, of each diagrammatic representation:

Definition 4.1.3. `FinStoMap`$'$ *is the strict monoidal category generated by one object* $[1]$ *with tensor powers* $[n] \equiv [1]^{\otimes n}$ *together with the family of morphisms*

$\partial =$ 

$e =$ 

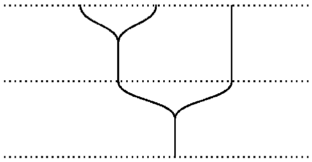
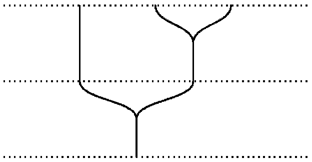
$s =$ 

$c_\lambda =$ 

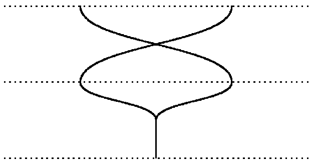
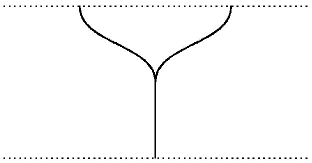
$\lambda \in [0,1]$

subject to the relations

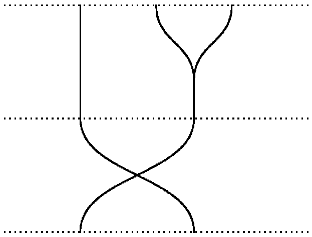
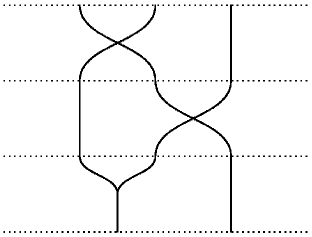
$e(e \otimes \mathrm{id}_{[1]}) \quad = \quad e(\mathrm{id}_{[1]} \otimes e)$:

 =  (4.1.3)

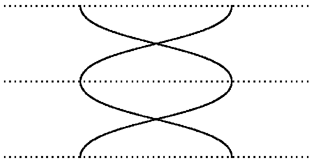
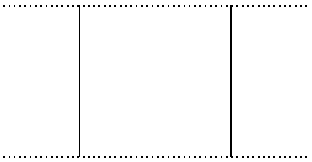
$es \quad = \quad e$:

 =  (4.1.4)

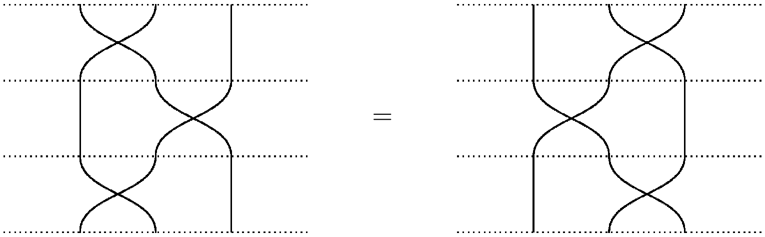
$s(\mathrm{id}_{[1]} \otimes e) \quad = \quad (e \otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]} \otimes s)(s \otimes \mathrm{id}_{[1]})$:

 =  (4.1.5)

$s^2 \quad = \quad \mathrm{id}_{[2]}$:

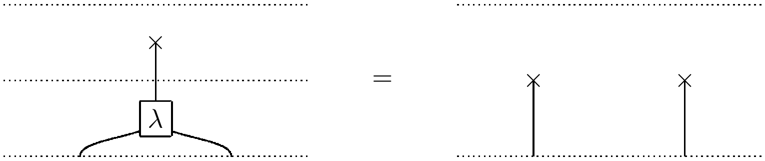
 =  (4.1.6)

$$(s\otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]}\otimes s)(s\otimes \mathrm{id}_{[1]}) \quad = \quad (\mathrm{id}_{[1]}\otimes s)(s\otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]}\otimes s)\ :$$



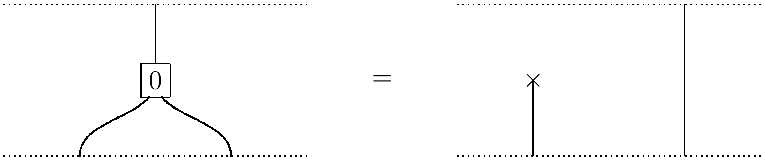
(4.1.7)

$$c_\lambda \partial \quad = \quad \partial \otimes \partial\ :$$



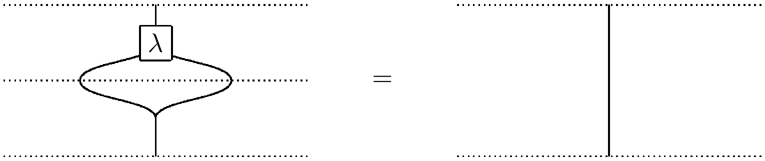
(4.1.8)

$$c_0 \quad = \quad \partial \otimes \mathrm{id}_{[1]}\ :$$



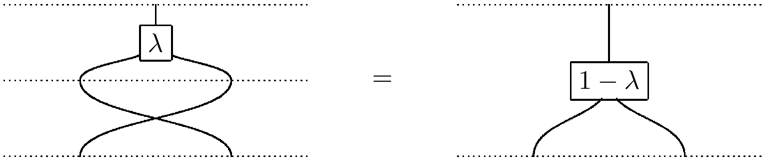
(4.1.9)

$$e\,c_\lambda \quad = \quad \mathrm{id}_{[1]}\ :$$



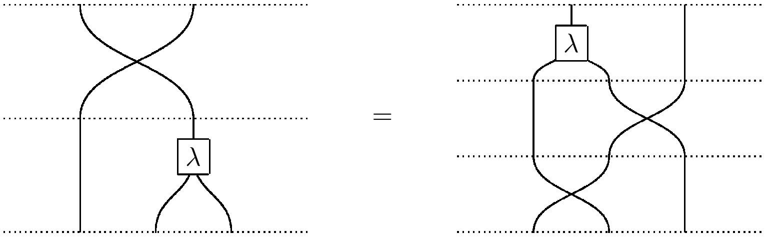
(4.1.10)

$$s\,c_\lambda \quad = \quad c_{1-\lambda}\ :$$



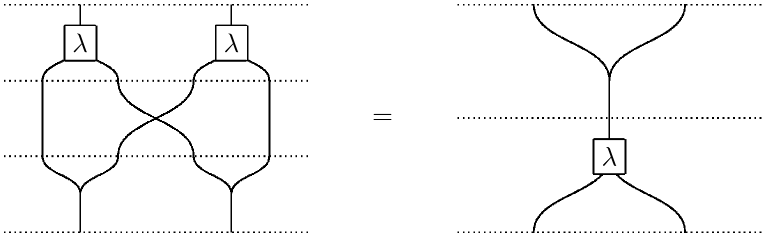
(4.1.11)

$$(\mathrm{id}_{[1]}\otimes c_\lambda)s \quad = \quad (s\otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]}\otimes s)(c_\lambda\otimes \mathrm{id}_{[1]})\ :$$



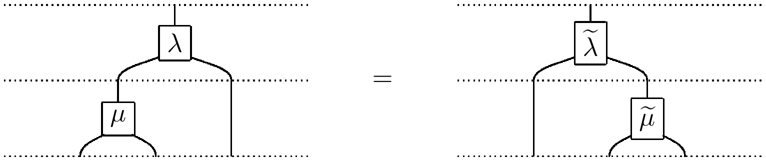
(4.1.12)

$$(e \otimes e)(\mathrm{id}_{[1]} \otimes s \otimes \mathrm{id}_{[1]})(c_\lambda \otimes c_\lambda) \quad = \quad c_\lambda e$$



(4.1.13)

$$(c_\mu \otimes \mathrm{id}_{[1]})c_\lambda \quad = \quad (\mathrm{id}_{[1]} \otimes c_{\widetilde{\mu}})c_{\widetilde{\lambda}} \ :$$



(4.1.14)

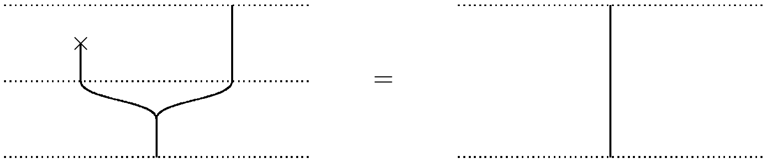
using the abbreviations

$$\widetilde{\lambda} = \lambda\mu, \qquad \widetilde{\mu} = \begin{cases} \lambda\frac{1-\mu}{1-\lambda\mu} & \textit{if } \lambda\mu \neq 1 \\ \textit{arbitrary} & \textit{if } \lambda = \mu = 1 \end{cases}$$

Hence, a morphism in $\mathtt{FinStoMap}'$ is described by a vertical juxtaposition of horizontal juxtapositions of generators and identity morphisms such that the strands match. Two such diagrams describe the same morphism if and only if there is a sequence of steps of the form (4.1.3)–(4.1.14) transforming the two diagrams into each other. The way to think of a diagrammatic representation of a morphism in $\mathtt{FinStoMap}'$ is as a probabilistic map $[m] \to [n]$, where the image of $j \in [m]$ can be obtained by following the jth input strand downwards, such that at an occurence of some c_λ one branches to the left with probability λ and branches to the right with probability $1-\lambda$. One can check easily that the defining relations of $\mathtt{FinStoMap}'$ are consistent with this interpretation.

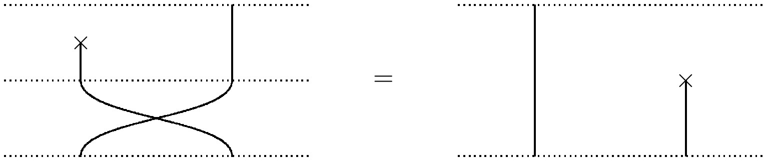
Remark 4.1.4. (a) By combining (4.1.9) with (4.1.10) and (4.1.11), we obtain two additional useful equations:

$$e(\partial \otimes \mathrm{id}_{[1]}) \quad = \quad \mathrm{id}_{[1]} \ :$$



(4.1.15)

$$s(\partial \otimes \mathrm{id}_{[1]}) \quad = \quad \mathrm{id}_{[1]} \otimes \partial \ :$$



(4.1.16)

As described in [Mas97], these relations are not implied by others if one determines an analogous presentation for the category of finite cardinals with deterministic maps, where the additional generators c_λ are not present.

(b) As already noted in [Mas97], the equations (4.1.5), (4.1.15) and (4.1.16) imply their mirror images by use of (4.1.6). The same holds true for (4.1.12).

(c) As can be seen from the relation (4.1.9), the generator ∂ is redundant for all morphisms $f : [m] \to [n]$ with $m \geq 1$. Hence its only function is to turn $[0]$ into an initial object in `FinStoMap`, as without ∂ there could be no morphism from $[0]$ to any other object.

Taking the strict monoidal functor $F : \mathtt{FinStoMap}' \to \mathtt{FinStoMap}$ to be the identity on objects, the assignments

$$\begin{aligned}
F(\partial) &\equiv () : [0] \longrightarrow [1] \\
F(e) &\equiv \begin{pmatrix} 1 & 1 \end{pmatrix} : [2] \longrightarrow [1] \\
F(s) &\equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : [2] \longrightarrow [2] \\
F(c_\lambda) &\equiv \begin{pmatrix} \lambda \\ 1-\lambda \end{pmatrix} : [1] \longrightarrow [2]
\end{aligned}$$

preverse the relations and hence uniquely define F. The motivation for these definitions is that they exactly match the interpretations of the generators of `FinStoMap`$'$ as the corresponding probabilistic maps. When a stochastic matrix A has a preimage $F^{-1}(A)$, this preimage then provides a possible way to turn the blank rectangle of the "black box" (4.1.1) into a concrete representation of strands branching, crossing, coalescing, and newly emerging.

The series of intermediate results following now will culminate in theorem 4.1.17 stating that the functor F is in fact an isomorphism of strict monoidal categories.

Lemma 4.1.5. *For $n \geq 1$, every morphism $f \in \mathtt{FinStoMap}'([1],[n])$ can be written in the form*

$$f = (\mathrm{id}_{[n-2]} \otimes c_{\lambda_{n-1}}) \cdots (\mathrm{id}_{[1]} \otimes c_{\lambda_2}) c_{\lambda_1} \tag{4.1.17}$$

with numbers $\lambda_j \in [0,1]$. The image $F(f)$ is a stochastic matrix

$$F(f) = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{n-1} \\ \eta_n \end{pmatrix}$$

with entries

$$\mu_j \equiv \lambda_j(1-\lambda_{j-1})\cdots(1-\lambda_1), \quad j = 1, \ldots n-1; \qquad \eta_n = (1-\lambda_{n-1})\cdots(1-\lambda_1) \tag{4.1.18}$$

Proof. First, note that any such f can be written without using the generators ∂, e, or s. For ∂, this is clear by the relation (4.1.9). Hence we may write f as a product of terms of the form $\mathrm{id}_{[k]} \otimes e \otimes \mathrm{id}_{[l]}$, $\mathrm{id}_{[k]} \otimes s \otimes \mathrm{id}_{[l]}$, and $\mathrm{id}_{[k]} \otimes c_\lambda \otimes \mathrm{id}_{[l]}$. Now consider the last term in this product which contains a generator e or s and hence has the form $\mathrm{id}_{[k]} \otimes e \otimes \mathrm{id}_{[l]}$ or $\mathrm{id}_{[k]} \otimes s \otimes \mathrm{id}_{[l]}$. Such a factor has $k + l + 2$ input strands. Since f itself only has a single input strand, there have to be $k+l+1$ factors afterwards each of which contains a generator c_λ. Hence by repeated application of deformed parametric associativity (4.1.14), we can write f in such a form that the factor immediately succeeding the $\mathrm{id}_{[k]} \otimes e \otimes \mathrm{id}_{[l]}$ or $\mathrm{id}_{[k]} \otimes s \otimes \mathrm{id}_{[l]}$ has the form $\mathrm{id}_{[k]} \otimes c_\lambda \otimes \mathrm{id}_{[l]}$. Then an application of the relation (4.1.10) or (4.1.11) removes the occurence of the unwanted generator e or s. This procedure now can be applied repeatedly until all occurences of e and s are removed. Comparing the number of input strands with output strands, it follows that there is a representation of f with exactly $n-1$ occurences of a generator c_λ, and no other generators. Again by repeated application of deformed parametric associativity, f then can be brought into the form whose existence was asserted.

For the second assertion, apply induction on n. For $n=1$, this is trivial, as then the product (4.1.17) is necessarily empty and hence implies $f = \mathrm{id}_{[1]}$. Taking the assertion for n as the induction assumption, we get for the case of $n+1$ that

$$F\left((\mathrm{id}_{[n-1]} \otimes c_{\lambda_n}) \cdots (\mathrm{id}_{[1]} \otimes c_{\lambda_2}) c_{\lambda_1}\right) = \begin{pmatrix} \mathbb{1}_{n-1} & 0 \\ 0 & \lambda_n \\ 0 & 1-\lambda_n \end{pmatrix} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{n-1} \\ \eta_n \end{pmatrix}$$

$$= \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{n-1} \\ \lambda_n \eta_n \\ (1-\lambda_n)\eta_n \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \\ \eta_{n+1} \end{pmatrix}$$

□

Proposition 4.1.6. *For every $n \in \mathbb{N}_0$, the map $F([1],[n]) : \mathtt{FinStoMap}([1],[n]) \to \mathtt{FinStoMap}'([1],[n])$ is bijective.*

Proof. This is clear for $n = 0$, as both $\mathtt{FinStoMap}([1],[0])$ and $\mathtt{FinStoMap}'([1],[0])$ are empty. For $n \geq 1$, suppose that we have a stochastic matrix

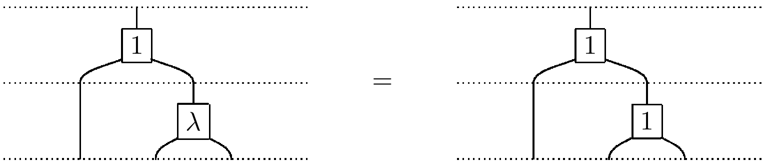
$$A_n = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{n-1} \\ \eta_n \end{pmatrix}$$

with entries $\mu_j \geq 0$, $\eta_n \geq 0$ satisfying $\eta_n = 1 - \sum_j \mu_j$. This matrix has a preimage under F of the form (4.1.17) if we can solve the system (4.1.18) for appropriate $\lambda_j \in [0,1]$. A solution is given by

$$\lambda_j = \frac{\mu_j}{1 - \sum_{k=1}^{j-1} \mu_k}$$

with the convention that $0/0$ may be an arbitrary value in $[0,1]$. Then it can be verified by direct calculation that this solves (4.1.18). As for uniqueness, note that the system of equations (4.1.18) can also be solved for the λ_j directly, and yields unique solutions as long as we never have $\lambda_j = 1$ for some j. In this exceptional case, we can take λ_k to be arbitrary for $k > j$. Hence the proof is complete if we can show that we get the same morphism in $\mathtt{FinStoMap}'$ no matter which choices of λ_k, $k > j$, we make. This follows from repeated application of the equation

$$(\mathrm{id}_{[1]} \otimes c_\lambda)c_1 \qquad = \qquad (\mathrm{id}_{[1]} \otimes c_1)c_1$$



which is a consequence of deformed parametric associativity (4.1.14). □

To extend this result to the general case, it is necessary to introduce several families of particular morphisms in `FinStoMap`′, which will then be used to reduce the general case to the previous proposition. The cyclic permutations $z_n : [n] \to [n]$ are defined recursively via

$$z_1 \equiv \mathrm{id}_{[1]}; \qquad z_{n+1} \equiv (\mathrm{id}_{[n-1]} \otimes s)(z_n \otimes \mathrm{id}_{[1]}), \quad n \geq 1 \tag{4.1.19}$$

The morphism z_n can be thought of as a permutation of the n strands which turns the leftmost strand into the rightmost strand while keeping the order of the other strands fixed. This interpretation is confirmed by the image of z_n in `FinStoMap`:

Lemma 4.1.7.

$$F(z_n) = \begin{pmatrix} 0 & \mathbb{1}_{n-1} \\ 1 & 0 \end{pmatrix} \tag{4.1.20}$$

Proof. Again induction on n. The case $n = 1$ is clear. Then,

$$F(z_{n+1}) = F(\mathrm{id}_{[n-1]} \otimes s)F(z_n \otimes \mathrm{id}_{[1]}) = \begin{pmatrix} \mathbb{1}_{n-1} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \mathbb{1}_{n-1} & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \mathbb{1}_{n-1} & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathbb{1}_n \\ 1 & 0 \end{pmatrix}$$

□

Lemma 4.1.8. *The cyclic permutation morphisms z_n are invertible and satisfy the following equations:*

(a) For any integer $n \geq 2$,

$$z_n = (\mathrm{id}_{[1]} \otimes z_{n-1})(s \otimes \mathrm{id}_{[n-2]}) \tag{4.1.21}$$

(b) For any integer $n \geq 1$,

$$z_n \otimes z_n = (\mathrm{id}_{[n-1]} \otimes z_{n+1})(z_{n+1} \otimes \mathrm{id}_{[n-1]})$$

(c) For any integer $n \geq 1$,

$$(z_n^{-1} \otimes \mathrm{id}_{[n]})(\mathrm{id}_{[n-1]} \otimes z_{n+1}) = (\mathrm{id}_{[n]} \otimes z_n)(z_{n+1}^{-1} \otimes \mathrm{id}_{[n-1]}) \tag{4.1.22}$$

(d) For any integer $n \geq 0$,

$$z_{n+1}(\partial \otimes \mathrm{id}_{[n]}) = \mathrm{id}_{[n]} \otimes \partial \tag{4.1.23}$$

Proof. Invertibility is clear as z_n is defined as a composition of invertible morphisms. All the following proofs use induction on n.

(a) Trivial for $n = 2$, while the induction step is

$$\begin{aligned} z_{n+1} &\overset{(4.1.19)}{=} (\mathrm{id}_{[n-1]} \otimes s)(z_n \otimes \mathrm{id}_{[1]}) \overset{\text{assumption}}{=} (\mathrm{id}_{[n-1]} \otimes s)(\mathrm{id}_{[1]} \otimes z_{n-1} \otimes \mathrm{id}_{[1]})(s \otimes \mathrm{id}_{[n-1]}) \\ &\overset{(4.1.19)}{=} (\mathrm{id}_{[1]} \otimes z_n)(s \otimes \mathrm{id}_{[n-1]}) \end{aligned}$$

(b) The case $n = 1$ states $\mathrm{id}_{[1]} \otimes \mathrm{id}_{[1]} = ss$, which is (4.1.6). The following calculation proves the assertion for $n + 1$ assuming its validity for n:

$$\begin{aligned} z_{n+1} \otimes z_{n+1} &= (\mathrm{id}_{[n+1]} \otimes z_{n+1})(z_{n+1} \otimes \mathrm{id}_{[n+1]}) \\ &\overset{(4.1.19),\ (4.1.21)}{=} (\mathrm{id}_{[2n]} \otimes s)(\mathrm{id}_{[n+1]} \otimes z_n \otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]} \otimes z_n \otimes \mathrm{id}_{[n+1]})(s \otimes \mathrm{id}_{[2n]}) \\ &\overset{\text{assumption}}{=} (\mathrm{id}_{[2n]} \otimes s)(\mathrm{id}_{[n]} \otimes z_{n+1} \otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]} \otimes z_{n+1} \otimes \mathrm{id}_{[n]})(s \otimes \mathrm{id}_{[2n]}) \\ &\overset{(4.1.19),\ (4.1.21)}{=} (\mathrm{id}_{[n]} \otimes z_{n+2})(z_{n+2} \otimes \mathrm{id}_{[n]}) \end{aligned}$$

(c) This is the previous equation in a different form.

(d) The statement is vacuous for $n = 0$. The induction step is

$$\begin{aligned} z_{n+2}(\partial \otimes \mathrm{id}_{[n+1]}) &\overset{(4.1.19)}{=} (\mathrm{id}_{[n]} \otimes s)(z_{n+1} \otimes \mathrm{id}_{[1]})(\partial \otimes \mathrm{id}_{[n+1]}) \\ &\overset{\text{assumption}}{=} (\mathrm{id}_{[n]} \otimes s)(\mathrm{id}_{[n]} \otimes \partial \otimes \mathrm{id}_{[1]}) \overset{(4.1.16)}{=} \mathrm{id}_{[n+1]} \otimes \partial \end{aligned}$$

□

Lemma 4.1.9. *For $f \in \texttt{FinStoMap}'([m],[n])$, we have*

$$z_{n+1}(\mathrm{id}_{[1]} \otimes f) = (f \otimes \mathrm{id}_{[1]}) z_{m+1} \tag{4.1.24}$$

Proof. This will be done in the following three steps:

(a) It holds for $f = \partial$, e, s and all c_λ.

(b) If it holds for f, then it also holds for any $\mathrm{id}_{[k]} \otimes f \otimes \mathrm{id}_{[l]}$.

(c) If it holds for $f_1 : [m] \to [n]$ and $f_2 : [n] \to [q]$, then it also holds for $f_2 f_1 : [m] \to [q]$.

This then covers all cases as every morphism is a composition of tensor products of generators and identity morphisms.

(a) For $f = \partial$, this is (4.1.16). For $f = e$, it is (4.1.5). For $f = s$ itself, this is the Yang-Baxter relation (4.1.7), while for c_λ it is (4.1.12).

(b) It is sufficient to prove this for the cases $k = 0$, $l = 1$ and $k = 1$, $l = 0$, as all other cases then follow by induction. For the first of these, this is the calculation

$$\begin{aligned} z_{n+2}(\mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]}) &= (\mathrm{id}_{[n]} \otimes s)(z_{n+1} \otimes \mathrm{id}_{[1]})(\mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]}) \\ = (\mathrm{id}_{[n]} \otimes s)(f \otimes \mathrm{id}_{[2]})(z_{m+1} \otimes \mathrm{id}_{[1]}) &= (f \otimes \mathrm{id}_{[2]})(\mathrm{id}_{[m]} \otimes s)(z_{m+1} \otimes \mathrm{id}_{[1]}) = (f \otimes \mathrm{id}_{[2]}) z_{m+2} \end{aligned}$$

while the second case works similarly using (4.1.21).

(c) Direct calculation:

$$\begin{aligned} z_{q+1}(\mathrm{id}_{[1]} \otimes f_2 f_1) &= z_{q+1}(\mathrm{id}_{[1]} \otimes f_2)(\mathrm{id}_{[1]} \otimes f_1) = (f_2 \otimes \mathrm{id}_{[1]}) z_{n+1}(\mathrm{id}_{[1]} \otimes f_1) \\ &= (f_2 \otimes \mathrm{id}_{[1]})(f_1 \otimes \mathrm{id}_{[1]}) z_{m+1} = (f_2 f_1 \otimes \mathrm{id}_{[1]}) z_{m+1} \end{aligned}$$

□

Two more classes of morphisms in `FinStoMap` need to be introduced. The single-strand inclusion

$$\iota^n_j \equiv \partial_{j-1} \otimes \mathrm{id}_{[1]} \otimes \partial_{n-j}$$

is a morphism $[1] \to [n]$ which maps a single input strand to the jth of n output strands. The projection morphisms $p^m_n : [mn] \to [n]$ coalesce m copies of a group of n strands into a single group of n strands and can be defined recursively by

$$p^2_0 \equiv \mathrm{id}_{[0]}; \qquad p^2_{n+1} \equiv (p^2_n \otimes e)(\mathrm{id}_{[n]} \otimes z_{n+2}), \quad n \geq 0; \qquad p^{m+1}_n \equiv p^2_n(p^m_n \otimes \mathrm{id}_{[n]}), \quad m \geq 2 \tag{4.1.25}$$

The interpretation of p^n_m as coalescing strands is confirmed by its image in `FinStoMap`:

Lemma 4.1.10. *For integers $m \geq 2$ and $n \geq 0$,*

$$F(p^m_n) = \underbrace{(\mathbb{1}_n \cdots \mathbb{1}_n)}_{m\ copies}$$

Proof. First, induction on n for $m = 2$:

$$F(p^2_{n+1}) = F(p^2_n \otimes e)F(\mathrm{id}_{[n]} \otimes z_{n+2}) = \begin{pmatrix} \mathbb{1}_n & \mathbb{1}_n & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} \mathbb{1}_n & 0 & 0 & 0 \\ 0 & 0 & \mathbb{1}_n & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \mathbb{1}_n & 0 & \mathbb{1}_n & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbb{1}_{n+1} & \mathbb{1}_{n+1} \end{pmatrix}$$

Then, induction on m for fixed n:

$$F(p^{m+1}_n) = F(p^2_n)F(p^m_n \otimes \mathrm{id}_{[n]}) = \begin{pmatrix} \mathbb{1}_n & \mathbb{1}_n \end{pmatrix} \begin{pmatrix} \mathbb{1}_n & \cdots & \mathbb{1}_n & 0 \\ 0 & \cdots & 0 & \mathbb{1}_n \end{pmatrix} = \begin{pmatrix} \mathbb{1}_n & \cdots & \mathbb{1}_n & \mathbb{1}_n \end{pmatrix}$$

□

Lemma 4.1.11. *For integer $n \geq 0$,*

$$p^2_{n+1} = (e \otimes p^2_n)(z^{-1}_{n+2} \otimes \mathrm{id}_{[n]}) \tag{4.1.26}$$

Proof. Induction on n. The statement is trivial for $n = 0$. The induction step is

$$p^2_{n+2} \overset{(4.1.25)}{=} (p^2_{n+1} \otimes e)(\mathrm{id}_{[n+1]} \otimes z_{n+3}) \overset{\text{assumption}}{=} (e \otimes p^2_n \otimes e)(z^{-1}_{n+2} \otimes \mathrm{id}_{[n+2]})(\mathrm{id}_{[n+1]} \otimes z_{n+3})$$
$$\overset{(4.1.22)}{=} (e \otimes p^2_n \otimes e)(\mathrm{id}_{[n+2]} \otimes z_{n+2})(z^{-1}_{n+3} \otimes \mathrm{id}_{[n+1]}) \overset{(4.1.25)}{=} (e \otimes p^2_{n+1})(z^{-1}_{n+3} \otimes \mathrm{id}_{[n]})$$

□

Lemma 4.1.12. *For any $f : [m] \to [n]$ and any integer $k \geq 2$, we have*

$$fp^k_m = p^k_n f^{\otimes k}$$

Proof. Consider the case $k = 2$ first. This then uses exactly the same steps as the previous lemma did.

(a) We have $p_1^2 = es = e$, and hence $p_2^2 = (e \otimes e)(\mathrm{id}_{[2]} \otimes s)(\mathrm{id}_{[1]} \otimes s \otimes \mathrm{id}_{[1]}) = (e \otimes e)(\mathrm{id}_{[1]} \otimes s \otimes \mathrm{id}_{[1]})$. For $f = \partial$, the assertion $\partial = e(\partial \otimes \partial)$ then directly follows from (4.1.15). For $f = e$, we need (4.1.4) together with several applications of (4.1.3). For $f = s$, the calculation uses (4.1.6) as well as several applications of (4.1.5) and its mirror image. Finally, for $f = c_\lambda$, this is (4.1.13).

(b) Straightforward calculation employing lemma 4.1.9:

$$\begin{aligned} p_{n+1}^2(f \otimes \mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]}) &= (p_n^2 \otimes e)(\mathrm{id}_{[n]} \otimes z_{n+2})(f \otimes \mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]}) \\ \overset{(4.1.24)}{=} (p_n^2 \otimes e)(f \otimes f \otimes \mathrm{id}_{[2]})(\mathrm{id}_{[m]} \otimes z_{m+2}) &\overset{\text{assumption}}{=} (f \otimes \mathrm{id}_{[1]})(p_m^2 \otimes e)(\mathrm{id}_{[m]} \otimes z_{m+2}) \\ &= (f \otimes \mathrm{id}_{[1]})p_{m+1}^2 \end{aligned}$$

as well as

$$\begin{aligned} p_{n+1}^2(\mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]} \otimes f) &\overset{(4.1.26)}{=} (e \otimes p_n^2)(z_{n+2}^{-1} \otimes \mathrm{id}_{[n]})(\mathrm{id}_{[1]} \otimes f \otimes \mathrm{id}_{[1]} \otimes f) \\ \overset{(4.1.24)}{=} (e \otimes p_n^2)(\mathrm{id}_{[2]} \otimes f \otimes f)(z_{m+2}^{-1} \otimes \mathrm{id}_{[m]}) &\overset{\text{assumption}}{=} (\mathrm{id}_{[1]} \otimes f)(e \otimes p_m^2)(z_{m+2}^{-1} \otimes \mathrm{id}_{[m]}) \\ &\overset{(4.1.26)}{=} (\mathrm{id}_{[1]} \otimes f)p_{m+1}^2 \end{aligned}$$

(c) Again the same simple calculation as in the previous proof (also using the same notation):

$$f_2 f_1 p_m^k = f_2 p_n^k f_1^{\otimes k} = p_q^k f_2^{\otimes k} f_1^{\otimes k} = p_q^k (f_2 f_1)^{\otimes k}$$

For general k, the statement is an easy consequence of the $k = 2$ case and the definition (4.1.25). Upon induction on k,

$$fp_m^{k+1} = fp_m^2(p_m^k \otimes \mathrm{id}_{[m]}) = p_n^2(fp_m^k \otimes f) = p_n^2(p_n^k f^{\otimes k} \otimes f) = p_n^2(p_n^k \otimes \mathrm{id}_{[n]})f^{\otimes(k+1)} = p_n^{k+1} f^{\otimes(k+1)}$$

□

Lemma 4.1.13. *For all integers $n \geq m \geq 0$,*

$$p_n^2(\mathrm{id}_{[m]} \otimes \partial^{\otimes n} \otimes \mathrm{id}_{[n-m]}) = \mathrm{id}_{[n]} \tag{4.1.27}$$

Proof. Induction on n. For $n = 0$, there is nothing to prove, hence proceed to the induction step and let us show that the equation holds for $n+1$ if it holds for n. Consider the case $m \leq n$ first. Then the assertion follows as in

$$\begin{aligned} p_{n+1}^2(\mathrm{id}_{[m]} \otimes \partial^{\otimes(n+1)} \otimes \mathrm{id}_{[n+1-m]}) &= (p_n^2 \otimes e)(\mathrm{id}_{[n]} \otimes z_{n+2})(\mathrm{id}_{[m]} \otimes \partial^{\otimes(n+1)} \otimes \mathrm{id}_{[n+1-m]}) \\ &= (p_n^2 \otimes e)\left[\mathrm{id}_{[m]} \otimes \partial^{\otimes(n-m)} \otimes z_{n+2}(\partial \otimes \mathrm{id}_{[n+1]})(\partial^{\otimes m} \otimes \mathrm{id}_{[n+1-m]})\right] \\ &\overset{(4.1.23)}{=} (p_n^2 \otimes e)\left[\mathrm{id}_{[m]} \otimes \partial^{\otimes(n-m)} \otimes (\mathrm{id}_{[n+1]} \otimes \partial)(\partial^{\otimes m} \otimes \mathrm{id}_{[n+1-m]})\right] \\ &= (p_n^2 \otimes e)(\mathrm{id}_{[m]} \otimes \partial^{\otimes n} \otimes \mathrm{id}_{[n+1-m]} \otimes \partial) \underset{(4.1.16)}{\overset{\text{assumption}}{=}} \mathrm{id}_{[n]} \otimes \mathrm{id}_{[1]} \end{aligned}$$

In the case that $m = n + 1$, we can use (4.1.26) to complete the induction step:

$$\begin{aligned} p_{n+1}^2(\mathrm{id}_{[n+1]} \otimes \partial^{\otimes(n+1)}) &= (e \otimes p_n^2)(z_{n+2}^{-1} \otimes \mathrm{id}_{[n]})(\mathrm{id}_{[n+1]} \otimes \partial^{\otimes(n+1)}) \\ &\overset{(4.1.23)}{=} (e \otimes p_n^2)(\partial \otimes \mathrm{id}_{[n+1]} \otimes \partial^{\otimes n}) \underset{(4.1.16)}{\overset{\text{assumption}}{=}} \mathrm{id}_{[1]} \otimes \mathrm{id}_{[n]} \end{aligned}$$

□

Lemma 4.1.14. *For all integers $n \geq m \geq 2$,*

$$p_n^m(\iota_1^n \otimes \cdots \otimes \iota_m^n) = \mathrm{id}_{[m]} \otimes \partial^{\otimes(n-m)}$$

Proof. For $m = 2$, apply induction on n. The case $n = 2$ is a direct calculation using $p_2^2 = (e \otimes e)(\mathrm{id}_{[1]} \otimes s \otimes \mathrm{id}_{[1]})$ together with the equations (4.1.15) and (4.1.16). The induction step is

$$\begin{aligned} p_{n+1}^2(\iota_1^{n+1} \otimes \iota_2^{n+1}) &= (p_n^2 \otimes e)(\mathrm{id}_{[n]} \otimes z_{n+2})(\iota_1^n \otimes \partial \otimes \iota_2^n \otimes \partial) \\ \overset{(4.1.23)}{=} (p_n^2 \otimes e)(\iota_1^n \otimes \iota_2^n \otimes \partial \otimes \partial) &\underset{(4.1.15)}{\overset{\text{assumption}}{=}} \mathrm{id}_{[2]} \otimes \partial^{\otimes(n-2)} \otimes \partial = \mathrm{id}_{[2]} \otimes \partial^{\otimes(n-1)} \end{aligned}$$

Finally, we use induction on m:

$$\begin{aligned} p_n^{m+1}(\iota_1^n \otimes \cdots \otimes \iota_m^n \otimes \iota_{m+1}^n) &= p_n^2(p_n^m \otimes \mathrm{id}_{[n]})(\iota_1^n \otimes \cdots \otimes \iota_m^n \otimes \iota_{m+1}^n) \\ \overset{\text{assumption}}{=} p_n^2(\mathrm{id}_{[m]} \otimes \partial^{\otimes(n-m)} \otimes \iota_{m+1}^n) &= p_n^2(\mathrm{id}_{[m]} \otimes \partial^{\otimes n} \otimes \mathrm{id}_{[1]} \otimes \partial^{\otimes(n-m-1)}) \\ = p_n^2(\mathrm{id}_{[m]} \otimes \partial^{\otimes n} \otimes \mathrm{id}_{[n-m]})(\mathrm{id}_{[m+1]} \otimes \partial^{\otimes(n-m-1)}) &\overset{(4.1.27)}{=} \mathrm{id}_{[m+1]} \otimes \partial^{\otimes(n-m-1)} \end{aligned}$$

□

In order for the following two propositions to make sense also in the cases $m = 0$ and $m = 1$, let us set $p_n^1 = \mathrm{id}_{[n]}$ and $p_n^0 = \partial^{\otimes n}$. Then lemma 4.1.10 immediately extends to these cases.

Proposition 4.1.15. *For any morphism $f : [m] \to [n]$ in* `FinStoMap′`*,*

$$f = p_n^m(f\iota_1^m \otimes \ldots \otimes f\iota_m^m)$$

Proof. For $m = 1$, the statement is trivial. For $m \geq 2$, this is an immediate consequence of the two lemmas 4.1.12 and 4.1.14. It remains to consider the degenerate case $m = 0$, where the equation asserts that $f = \partial^{\otimes n}$. But this in turn follows from repeated applications of (4.1.8), (4.1.15) and (4.1.16). □

We will also need the corresponding statement for stochastic matrices:

Proposition 4.1.16. *For any stochastic matrix $A : [m] \to [n]$, we have*

$$A = F(p_n^m)\,(AF(\iota_1^m) \otimes \ldots \otimes AF(\iota_m^m))$$

Proof. By definition, $F(\iota_j^m)$ is the single-column matrix with a 1 as the jth entry and zeros otherwise. Hence, $A_j \equiv AF(\iota_j^m)$ is simply the jth column of A. Consequently,

$$F(p_n^m)\,(AF(\iota_1^m) \otimes \ldots \otimes AF(\iota_m^m)) = \begin{pmatrix} \mathbb{1}_m & \cdots & \mathbb{1}_m \end{pmatrix} \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix} = \begin{pmatrix} A_1 & \cdots & A_m \end{pmatrix} = A$$

□

Theorem 4.1.17. *The functor F :* `FinStoMap′` *$\to$* `FinStoMap` *is an isomorphism of strict monoidal categories.*

Proof. The two previous propositions show that a morphism in $\texttt{FinStoMap}'([m],[n])$ or $\texttt{FinStoMap}([m],[n])$ is uniquely determined by an m-tuple of morphisms in $\texttt{FinStoMap}'([1],[n])$ or $\texttt{FinStoMap}([1],[n])$, respectively. This is expressed by the two horizontal bijections in the diagram

$$\begin{tikzcd}
\texttt{FinStoMap}'([m],[n]) \arrow[r, "4.1.15", "\sim"'] \arrow[d, "F([m],[n])"] & \texttt{FinStoMap}'([1],[n])^m \arrow[d, "4.1.6", "\sim"'] \\
\texttt{FinStoMap}([m],[n]) \arrow[r, "4.1.16", "\sim"'] & \texttt{FinStoMap}([1],[n])^m
\end{tikzcd}$$

which is commutative by construction of the two horizontal maps. By proposition 4.1.6, the right vertical arrow is a bijection. Hence the diagram shows that the left vertical arrow also has to be bijective. □

Chapter 5

Convex Spaces: Definition and Examples

5.1 Introduction

Looking at the history of mathematics, one easily finds an abundance of cases where abstract generalizations of concrete structures into abstract concepts spurred a variety of interesting developments or even opened up completely new fields. Some of the most obvious examples that spring to mind are:

- The concept of a *group*, which provides an abstract framework for the study of *symmetries*.
- *Riemannian manifolds*, were modelled after submanifolds of $\mathbb{R}^n$ with their *intrinsic geometry*.
- *Category theory*, originally conceived as an abstract framework for *cohomology theories*.
- *Operators on Hilbert space*, which generalize the *Fourier transform* and *integral equations*.

We now consider the notion of *convexity* as that property of a subset of a vector space that means that the set contains the line segment connecting every two points in that subset. An abstract framework for convexity has been developed in [Sto49] and has since been studied occasionally by various authors. This concept, which we prefer to call *convex space*, seems to be little known. Therefore, we try to promote the study of this concept and how it might be useful in all those areas of mathematics and its applications in which convexity plays a role.

More concretely, a convex space is a set together with a family of binary operations. These binary operations need to satisfy appropriate compatibility conditions which generate all those relations that one expects convex combinations to have. The most obvious examples are convex subsets of vector spaces. However, there is an entirely different class of convex spaces all of which are of a discrete nature, namely meet-semilattices, where all non-degenerate convex combination operations are given by the meet operation. Moreover, one can also construct examples of mixed type, where one has a semilattice as an underlying discrete structure, together with a convex subset of a vector space over each element of the semilattice. This is similar to how one can project a polytope onto its face lattice by mapping each point to the face it generates: then, the polytope becomes a "fiber bundle" over its face lattice with the face interiors as fibers. Using a slightly more elaborate variant of this construction, it can subsequently be shown that every convex space is of this form (unpublished).

Our main motivation for studying this subject comes from quantum mechanics, in particular the search for a very general framework for theories of physics. Without loss of generality, we can assume a theory of physics to be of epistemological nature; this means that what we describe is not the actual reality of the system itself, but merely the information an observer has about the system. Now information is usually incomplete, in which case the state that the observer believes the system to be in is given by a statistical ensemble. Therefore, it seems reasonable to assume that the set of the information states has the mathematical structure of convex combinations, which correspond to statistical superpositions of ensembles. This is the framework known as *general probabilistic theories* [Bar06], where the set of information states is taken to be a convex subset of a vector space. However since the underlying vector space lacks any physical motivation and solely serves the purpose of defining the convex combinations, we feel that convex spaces might form a natural framework for fundamental physics.

We now give an outline of the chapter. After settling notation in section 5.2, we start section 5.4 by proposing our definition of convex spaces in terms of a family of binary operations satisfying certain compatibility conditions. Using concepts from category theory, we then show that these compatibility conditions imply all the relations that we expect convex combinations to have. The main step relies on the results of chapter 4. As a first exercise in the theory of convex spaces, we then show in theorem 5.4.9 how a convex space structure on a set is uniquely determined by the collection of those maps that preserve convex combinations.

The remaining three sections are entirely dedicated to various classes of examples. Section 5.5 proceeds by giving a list of examples of "geometric type", which refers to those convex spaces that can be written as a convex subset of a vector space. Then in section 5.6, we study a discrete class of convex spaces. A discrete convex space in that sense turns out to be the same thing as a semilattice. None of these can be embedded into a vector space. Finally, section 5.7 describes constructions of convex spaces that have both a geometric and a combinatorial flavor. This concludes the chapter. We hope that the long list of examples explains why we deem convex spaces worthy of study.

5.2 Notation

The `typewriter font` denotes a category, for example `Set`. As in [Fri09d], we write $[n]$ as shorthand for the n-element set $\{1, \ldots, n\}$. The symbol $*$ stands for any one-element set and also for the unique convex space over that set. For a real number $\alpha \in [0,1]$, we set $\overline{\alpha} \equiv 1 - \alpha$. This notation increases readability in formulas involving binary convex combinations. The $\overline{\cdot}$ operation satisfies the important relations

$$\overline{\overline{\alpha}} = \alpha, \quad \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} - 1, \quad \overline{\alpha\beta} = \overline{\alpha} + \overline{\beta} - \overline{\alpha}\,\overline{\beta}.$$

Given a set $X \in \texttt{Set}$, we call

$$\Delta_X \equiv \left\{ f : X \to [0,1] \;\middle|\; f \text{ has finite support and } \sum_{x \in X} f(x) = 1 \right\}$$

the *simplex over* X. We also consider Δ_X as the set of all finite formal convex combinations $\sum_i \lambda_i \underline{x_i}$ with $x_i \in X$, where we use the underline notation $\underline{x_i}$ to emphasize that the sum is formal; this allows us to distinguish $x \in X$ from $\underline{x} \in \Delta_X$. Two formal convex combinations represent the same element of Δ_X if and only if they assign the same total weight to each element $x \in X$.

5.3 Some relevant literature

Let us quickly mention the relevant literature currently known to us. Convex spaces in conjunction with the additional structure of a suitable compatible total ordering were discussed by von Neumann and Morgenstern in their classic 1944 book [vNM07, 3.6] on game theory and microeconomics. Their motivation was that the utilities of economic goods or services should take values in a totally ordered set with the additional structure of compatible convex combinations. In this context, convex combinations arise from gambling with utilities and preferences: suppose that you prefer A over B, but you prefer B over C. Then which would you prefer, B or the convex combination $\frac{1}{2}A + \frac{1}{2}C$? Here, the convex combination stands for a coin toss with return A if the coin lands heads, and return C if the coin lands tails. Von Neumann and Morgenstern conclude that the set of utility values should be a convex space together with an additional order structure[1], and subsequently [vNM07, A.2] show that every such structure embeds into $\mathbb{R}$. According to their reasoning, this justifies measuring utilities by real numbers.

Another important milestone is Stone's

5.4 Defining convex spaces

We first define convex spaces and convex maps before turning to a formal justification of these definitions and proving a certain uniqueness property of a convex space structure.

Definition 5.4.1. *A* ***convex space*** *is given by a set $\mathcal{C}$ together with a family of binary convex combination operations*

$$cc_\lambda : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}, \quad \lambda \in [0,1]$$

that satisfies

- *The unit law:*
$$cc_0(x,y) = y \tag{5.4.1}$$
- *Idempotency:*
$$cc_\lambda(x,x) = x \tag{5.4.2}$$
- *Parametric commutativity:*
$$cc_\lambda(x,y) = cc_{1-\lambda}(y,x) \tag{5.4.3}$$
- *Deformed parametric associativity:*
$$cc_\lambda(cc_\mu(x,y),z) = cc_{\widetilde{\lambda}}(x, cc_{\widetilde{\mu}}(y,z)) \tag{5.4.4}$$

  with

$$\widetilde{\lambda} = \lambda\mu, \qquad \widetilde{\mu} = \begin{cases} \frac{\lambda\overline{\mu}}{\overline{\lambda\mu}} & \text{\textit{if} } \lambda\mu \neq 1 \\ \textit{arbitrary} & \text{\textit{if} } \lambda = \mu = 1. \end{cases}$$

The most obvious example for this kind of structure is a vector space, with convex combinations defined via the vector space structure as $cc_\lambda(x,y) \equiv \lambda x + \overline{\lambda} y$.

[1] Note that our idempotency axiom (5.4.2) is automatic in that framework.

Definition 5.4.1 is the picture of convex space that we shall work with. Usually, a convex space will be referred to simply by its underlying set $\mathcal{C}$, with the convex combination operations cc_λ being implicit. Also, instead of $cc_\lambda(x,y)$, we will usually use the more suggestive notation

$$\lambda x + \overline{\lambda} y \equiv cc_\lambda(x,y)$$

in which the laws (5.4.1)–5.4.4 now read

$$\begin{aligned} 0x + \overline{0}y &= y && (5.4.5) \\ \lambda x + \overline{\lambda} x &= x && (5.4.6) \\ \lambda x + \overline{\lambda} y &= \overline{\lambda} y + \overline{\overline{\lambda}} x && (5.4.7) \\ \lambda\left(\mu x + \overline{\mu} y\right) + \overline{\lambda} z &= \lambda\mu x + \overline{\lambda\mu}\left(\lambda \frac{\overline{\mu}}{\overline{\lambda\mu}} y + \frac{\overline{\lambda}}{\overline{\lambda\mu}} z\right) \quad (\lambda\mu \neq 1) && (5.4.8) \end{aligned}$$

Also, we will occassionally use convex combinations

$$\sum_{i=1}^{n} \lambda_i x_i, \qquad \lambda_i \geq 0, \quad \sum_{i=1} \lambda_i = 1$$

of more than two elements. This are to interpreted as iterated binary convex combinations. Appropriate normalizations have to be inserted, e.g. for $n = 3$,

$$\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = \overline{\lambda}_3 \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} x_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2} x_2 \right) + \lambda_3 x_3 .$$

(Note that $\overline{\lambda}_3 = \lambda_1 + \lambda_2$.) Deformed parametric associativity (5.4.4) then expresses the fact that this reduction to binary convex combinations does not depend on the order of bracketing.

Definition 5.4.2. *Given convex spaces $\mathcal{C}$ and $\mathcal{C}'$, a* ***convex map*** *from $\mathcal{C}$ to $\mathcal{C}'$ is a map $f : \mathcal{C} \to \mathcal{C}'$ that commutes with the convex combination operations:*

$$f(\lambda x + \overline{\lambda} y) = \lambda f(x) + \overline{\lambda} f(y).$$

Convex spaces together with convex maps form the ***category of convex spaces*** `ConvSpc`.

For example, a map between vector spaces is convex if and only if it is affine. Therefore in this context, the words “affine” and “convex” will be used synonymously.

We now turn to the technical task of justifying these definitions. The goal here is to justify these definitions: why are the compatibility conditions (5.4.1) to (5.4.4) sufficient to guarantee that the binary operations have all the properties we expect convex combinations to have? A less formally inclined reader may want to skip the remainder of this section.

So, what should a convex space formally be? Clearly, it has to be a set $\mathcal{C}$ together with some additional structure. This additional structure should make precise the intuition of an assignment

$$\mathfrak{m} : \Delta_{\mathcal{C}} \longrightarrow \mathcal{C}, \qquad \sum_{i=1}^{n} \lambda_i \underline{x}_i \mapsto \sum_{i=1}^{n} \lambda_i x_i, \tag{5.4.9}$$

mapping a *formal* convex combination $(\sum_{i=1}^{n} \lambda_i \underline{x}_i) \in \Delta_{\mathcal{C}}$ to an *actual* convex combination $(\sum_{i=1}^{n} \lambda_i x_i) \in \mathcal{C}$, in such a way that the properties

$$\mathfrak{m}(\underline{x}) = x, \qquad \mathfrak{m}\left(\sum_{i=1}^{n} \lambda_i \, \underline{\mathfrak{m}\left(\sum_{j=1}^{m_i} \mu_{ij} \underline{x}_{ij} \right)} \right) = \mathfrak{m}\left(\sum_{i=1}^{n} \sum_{j=1}^{m_i} \lambda_i \mu_{ij} \underline{x}_{ij} \right) \tag{5.4.10}$$

hold. This intuition is straightforward to make precise using the theory of monads and their algebras[2]. The following definition is a discrete version of the Giry monad studied in categorical probability theory [Gir82].

Definition 5.4.3 (the finitary Giry monad)**.** *We define the simplex functor* Δ *to be given by*

$$\Delta : \mathtt{Set} \to \mathtt{Set}, \quad \mathcal{C} \mapsto \Delta_{\mathcal{C}}, \quad \left(\mathcal{C} \xrightarrow{f} \mathcal{D}\right) \mapsto \left(\sum_i \lambda_i \underline{x}_i \mapsto \sum_i \lambda_i \underline{f(x_i)}\right).$$

Then the ***finitary Giry monad*** $\mathscr{G}_{\mathrm{fin}} = (\Delta, \eta, \mu)$ *is defined by the unit natural transformation*

$$\eta_{\mathcal{C}} : \mathcal{C} \to \Delta_{\mathcal{C}}, \quad x \mapsto \underline{x}$$

and the multiplication transformation

$$\mu_{\mathcal{C}} : \Delta_{\Delta_{\mathcal{C}}} \to \Delta_{\mathcal{C}}, \quad \sum_{i=1}^{n} \lambda_i \underline{\sum_{j=1}^{m_i} \mu_{ij} \underline{x}_{ij}} \mapsto \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{m_i} \mu_{ij} \underline{x}_{ij}$$

An algebra of $\mathscr{G}_{\mathrm{fin}}$ is given by a set $\mathcal{C}$ together with a structure map $\mathfrak{m} : \Delta_{\mathcal{C}} \to \mathcal{C}$, such that the diagrams

$$\begin{tikzcd} \mathcal{C} \arrow[rr, equal] \arrow[dr, "\eta_{\mathcal{C}}"'] & & \mathcal{C} \\ & \Delta_{\mathcal{C}} \arrow[ur, "\mathfrak{m}"'] & \end{tikzcd} \qquad \begin{tikzcd} \Delta_{\Delta_{\mathcal{C}}} \arrow[r, "\Delta_{\mathfrak{m}}"] \arrow[d, "\mu_{\mathcal{C}}"'] & \Delta_{\mathcal{C}} \arrow[d, "\mathfrak{m}"] \\ \Delta_{\mathcal{C}} \arrow[r, "\mathfrak{m}"] & \mathcal{C} \end{tikzcd} \tag{5.4.11}$$

commute. As can be seen directly from the definition of $\mathscr{G}_{\mathrm{fin}}$, these correspond exactly to the requirements (5.4.10). Hence, one definitively "correct" definition of convex space is given by

$$\text{convex space} = \mathscr{G}_{\mathrm{fin}}\text{-algebra}.$$

Remark 5.4.4. Since most of the applications we have in mind do not require convex combinations of infinitely many elements, it is sufficient to work with this finitary version of the Giry monad. The advantage of this is that it gives a purely algebraic description of convex spaces, thereby facilitating the reformulation 5.4.1. However for applications in which one needs a structure that allows to take convex combinations of infinitely many points, or more generally taking the barycenter of an arbitrary probability measure, one could define an *ultraconvex space* to be an algebra of the Giry monad $\mathscr{G}$ based on the functor $\mathcal{P} : \mathtt{Meas} \to \mathtt{Meas}$, where `Meas` is an appropriate category of measurable spaces. $\mathcal{P}$ maps each measurable space to the set of all its probability measures, together with an appropriate σ-algebra on that set. Algebras for the Giry monad over the category of polish spaces have been studied in [Dob06].

We now turn to the category of stochastic matrices `FinStoMap` that was introduced in [Fri09d]. We will see later that a structure (5.4.9) satisfying (5.4.10) also turns $\mathcal{C}$ uniquely into a model of the Lawvere theory $\mathtt{FinStoMap}^{\mathrm{op}}$, and vice versa. So, we now proceed to study what it means for a functor $L : \mathtt{FinStoMap}^{\mathrm{op}} \longrightarrow \mathtt{Set}$ to be product-preserving. For any $\mathcal{C} \in \mathtt{Set}$, consider the functor

$$\begin{array}{rcl} \prod_{\mathcal{C}} : \mathtt{FinMap}^{\mathrm{op}} & \longrightarrow & \mathtt{Set}, \qquad [n] \mapsto \mathcal{C}^{\times n} \\ \left([m] \xrightarrow{f} [n]\right)^{\mathrm{op}} & \mapsto & \left((x_1, \ldots, x_n) \mapsto (x_{f(1)}, \ldots, x_{f(m)})\right). \end{array}$$

[2] As pointed out by Leinster [Lei08], defining convex spaces in terms of an operad does not yield all properties that one desires; in particular, taking some convex combination of a point with itself would not necessarily give that point back. Therefore, defining them as algebras of a monad seems like the most canonical choice.

Using the notation of [Fri09d], the following well-known observation arises:

Proposition 5.4.5. *Consider a functor $L : \mathtt{FinStoMap}^{\mathrm{op}} \longrightarrow \mathtt{Set}$ with $L([n]) = \mathcal{C}^{\times n}$ for all $n \in \mathbb{N}_0$. Then the following conditions are equivalent:*

(a) L is product-preserving, i.e.

$$\begin{aligned} L\left(\begin{pmatrix} \mathbb{1}_{n_1} \\ 0 \end{pmatrix}\right) &= \left(\mathcal{C}^{\times n_1} \times \mathcal{C}^{\times n_2} \xrightarrow{p_1} \mathcal{C}^{\times n_1}\right) \\ L\left(\begin{pmatrix} 0 \\ \mathbb{1}_{n_2} \end{pmatrix}\right) &= \left(\mathcal{C}^{\times n_1} \times \mathcal{C}^{\times n_2} \xrightarrow{p_2} \mathcal{C}^{\times n_2}\right) \end{aligned} \tag{5.4.12}$$

for all $n_1, n_2 \in \mathbb{N}_0$, where p_1 and p_2 are the product projections in $\mathtt{Set}$*.*

(b) L maps $\otimes$ to $\times$.

(c) The diagram

$$\begin{tikzcd} \mathtt{FinMap}^{\mathrm{op}} \arrow[rr, hook] \arrow[dr, "\prod_{\mathcal{C}}"'] & & \mathtt{FinStoMap}^{\mathrm{op}} \arrow[dl, "L"] \\ & \mathtt{Set} & \end{tikzcd} \tag{5.4.13}$$

commutes.

Proof. (a)⇒(b): This follows from an application of L to the $\mathtt{FinStoMap}$-coproduct diagram

$$\begin{tikzcd} {[n_1]} \arrow[r, "f_1"] \arrow[d, hook] & {[m_1]} \arrow[d, hook] \\ {[n_1 + n_2]} \arrow[r, "f_1 \otimes f_2"] & {[m_1 + m_2]} \\ {[n_2]} \arrow[r, "f_2"] \arrow[u, hook] & {[m_2]} \arrow[u, hook] \end{tikzcd}$$

together with the product universal property in $\mathtt{Set}$.

(b)⇒(c): Since $L(\partial)$ is necessarily the unique map $\mathcal{C} \to *$, we know that the map

$$L(\partial^{\otimes k} \otimes \mathrm{id}_{[1]} \otimes \partial^{\otimes l}) : \mathcal{C}^{\times (k+1+l)} \longrightarrow \mathcal{C}$$

is the projection onto the $(k+1)$-th factor. Then for $f \in \mathtt{FinMap}([m],[n])$, the assertion follows from an application of L to the equation

$$f(\partial^{\otimes(k-1)} \otimes \mathrm{id}_{[1]} \otimes \partial^{\otimes(m-k)}) = \partial^{\otimes(f(k)-1)} \otimes \mathrm{id}_{[1]} \otimes \partial^{\otimes(n-f(k))}.$$

(c)⇒(a): The equations (5.4.12) are the special cases of the commutative diagram where one starts in $\mathtt{FinMap}$ with the coproduct inclusions. □

We now claim that the equation

$$L(A)(x_1, \ldots, x_n) = \left(\mathfrak{m}\left(\sum_{i=1}^{n} A_{i1}\underline{x}_i\right), \ldots, \mathfrak{m}\left(\sum_{i=1}^{n} A_{im}\underline{x}_i\right)\right) \tag{5.4.14}$$

uniquely determines a structure of $\texttt{FinStoMap}^{\mathrm{op}}$-model L on a set $\mathcal{C}$ from a $\mathscr{G}_{\mathrm{fin}}$-algebra structure $\mathfrak{m} : \Delta_{\mathcal{C}} \to \mathcal{C}$, and vice versa. Furthermore, we claim that this correspondence is such that morphisms of $\mathscr{G}_{\mathrm{fin}}$-algebras coincide with morphisms of $\texttt{FinStoMap}^{\mathrm{op}}$-models.

We first check that when $\mathfrak{m}$ is given, then L defined by (5.4.14) is a product-preserving functor. Functoriality is expressed by preservation of identities,

$$L(\mathbb{1}_n)(x_1, \dots, x_n) = (\mathfrak{m}(\underline{x}_1), \dots, \mathfrak{m}(\underline{x}_n)) \overset{(5.4.11)}{=} (x_1, \dots, x_n),$$

and contravariant preservation of matrix multiplication for $A : [m] \to [n]$ and $B : [n] \to [q]$. For the verification of the latter, we have to evaluate the expression

$$L\,(BA)\,(x_1, \dots, x_q) = \left(\mathfrak{m} \left(\sum_{i=1}^{q} (BA)_{i1} \underline{x}_i \right), \dots, \mathfrak{m} \left(\sum_{i=1}^{q} (BA)_{im} \underline{x}_i \right) \right).$$

We do this componentwise, where $k \in [m]$ is the component index,

$$\left[L\,(BA)\,(x_1, \dots, x_q)\right]_k = \mathfrak{m} \left(\sum_{i=1}^{q} (BA)_{ik} \underline{x}_i \right) = \mathfrak{m} \left(\sum_{i,j=1}^{q,n} B_{ij} A_{jk} \underline{x}_i \right)$$

$$\overset{(5.4.3)}{=} \mathfrak{m} \left(\mu_{\mathcal{C}} \left(\sum_{j=1}^{n} A_{jk} \underline{\sum_{i=1}^{q} B_{ij} \underline{x}_i} \right) \right) \overset{(5.4.11)}{=} \mathfrak{m} \left(\sum_{j=1}^{n} A_{jk} \, \underline{\mathfrak{m} \left(\sum_{i=1}^{q} B_{ij} \underline{x}_i \right)} \right)$$

$$\overset{(5.4.14)}{=} \mathfrak{m} \left(\sum_{j=1}^{n} A_{jk} \, \underline{\left[L(B)(x_1, \dots, x_q)\right]_j} \right)$$

$$\overset{(5.4.14)}{=} \left[L(A) \left(\left[L(B)(x_1, \dots, x_q)\right]_1, \dots, \left[L(B)(x_1, \dots, x_q)\right]_n \right)\right]_k$$

$$= \left[L(A)L(B)(x_1, \dots, x_q)\right]_k,$$

thereby showing that

$$L(BA)(x_1, \dots, x_q) = L(A)L(B)\,(x_1, \dots, x_q)\,,$$

which completes the verification of functoriality. Preservation of products is immediate, as the condition (5.4.13) holds by (5.4.14) and the first diagram of (5.4.11).

Now given two $\mathscr{G}_{\mathrm{fin}}$-algebras $\mathfrak{m} : \Delta_{\mathcal{C}} \to \mathcal{C}$ and $\mathfrak{m}' : \Delta_{\mathcal{C}'} \to \mathcal{C}'$, a morphism of algebras is a map $f : \mathcal{C} \to \mathcal{C}'$ such that the diagram

$$\begin{tikzcd} \Delta_{\mathcal{C}} \arrow[r, "\Delta_f"] \arrow[d, "\mathfrak{m}"'] & \Delta_{\mathcal{C}'} \arrow[d, "\mathfrak{m}'"] \\ \mathcal{C} \arrow[r, "f"] & \mathcal{C}' \end{tikzcd} \tag{5.4.15}$$

commutes. Then the induced functors L and L' behave with respect to f in the following way:

$$\left[L'(A)\,(f(x_1), \dots, f(x_n))\right]_k \overset{(5.4.14)}{=} \mathfrak{m}' \left(\sum_{i=1}^{n} A_{ik} \underline{f(x)_i} \right) = \mathfrak{m}' \left(\Delta_f \left(\sum_{i=1} A_{ik} \underline{x}_i \right) \right)$$

$$\overset{(5.4.15)}{=} f\left(\mathfrak{m}\left(\sum_{i=1}^{n} A_{ik}\underline{x}_i\right)\right) \overset{(5.4.14)}{=} f\left([L(A)(x_1,\dots,x_n)]\right)$$

thereby showing that $L'(A)f^{\times n} = f^{\times m}L(A)$, which means that f also is a morphism of $\mathtt{FinStoMap}^{\mathrm{op}}$-models.

Now for the other direction: given L, equation (5.4.14) requires that we define the structure map as

$$\mathfrak{m}\left(\sum_{i=1}^{n} \lambda_i \underline{x}_i\right) \equiv L\left(\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix}\right)(x_1,\dots,x_n) = L\big(\vec{\lambda}\big)(x_1,\dots,x_n). \tag{5.4.16}$$

We need to verify the desired properties (5.4.11). The unit condition is essentially trivial,

$$\mathfrak{m}\left(\underline{x}\right) = L\left(\mathbb{1}_1\right)(x) = x$$

while the associativity of the action requires more work:

$$\mathfrak{m}\left(\mu_{\mathcal{C}}\left(\sum_{i=1}^{n} \lambda_i \underline{\sum_{j=1}^{m} \mu_{ji}\underline{x}_j}\right)\right) \overset{(5.4.3)}{=} \mathfrak{m}\left(\sum_{i=1}^{n} \lambda_i \sum_{j=1}^{m} \mu_{ji}\underline{x}_j\right)$$

$$\overset{(5.4.16)}{=} L\left(\begin{pmatrix}\sum_{i=1}^{n} \lambda_i \mu_{1i}\\ \vdots\\ \sum_{i=1}^{n} \lambda_i \mu_{mi}\end{pmatrix}\right)(x_1,\dots,x_m)$$

$$= L\big(\underline{\mu}\vec{\lambda}\big)(x_1,\dots,x_m) = L\big(\vec{\lambda}\big)L\big(\underline{\mu}\big)(x_1,\dots,x_m)$$

where the matrix $\underline{\mu} = (\mu_{ji})_{j,i}$ has columns $\vec{\mu}_1,\dots,\vec{\mu}_n$, and after possibly adding dummy terms, we were able to assume that under the large underscore, neither the number of terms m nor the x_j depend on i. Since L maps coproducts to products, and the columns of the matrix $\underline{\mu}$ are exactly its coproduct components, we can continue the calculation with

$$= L\big(\vec{\lambda}\big)\left(L\big(\vec{\mu}_1\big)(x_1,\dots,x_m),\dots,L\big(\vec{\mu}_n\big)(x_1,\dots,x_m)\right)$$

$$\overset{(5.4.16)}{=} \mathfrak{m}\left(\sum_{i=1}^{n} \lambda_i \, \underline{L\big(\vec{\mu}_i\big)(x_1,\dots,x_m)}\right) \overset{(5.4.16)}{=} \mathfrak{m}\left(\sum_{i=1} \lambda_i \, \underline{\mathfrak{m}\left(\sum_{j=1}^{m} \mu_{ji}\underline{x}_j\right)}\right)$$

which shows that also the second diagram of (5.4.11) commutes.

What still remains to check is that morphisms of $\mathtt{FinStoMap}^{\mathrm{op}}$-models also are morphisms of the induced $\mathscr{G}_{\mathrm{fin}}$-algebras. This follows from essentially the same calculation as above:

$$\mathfrak{m}'\left(\Delta_f\left(\sum_{i=1} A_{ik}\underline{x}_i\right)\right) = \mathfrak{m}'\left(\sum_{i=1}^{n} A_{ik}\underline{f(x)_i}\right) = \left[L'(A)\left(f(x_1),\dots,f(x_n)\right)\right]_k$$

$$= f\left([L(A)(x_1,\dots,x_n)]\right) = f\left(\mathfrak{m}\left(\sum_{i=1}^{n} A_{ik}\underline{x}_i\right)\right).$$

Finally, as the observation concluding these considerations, it follows from the uniqueness statement of the correspondence $\mathfrak{m} \leftrightsquigarrow L$ that the construction of L from $\mathfrak{m}$ is inverse to the construction of $\mathfrak{m}$ from L.

Remark 5.4.6. This correspondence between algebras of a monad and models of a Lawvere theory is a particular instance of a well-known general correspondence between finitary monads and Lawvere theories [HP07]. (A monad is called *finitary* if the endofunctor preserves filtered colimits.)

Hence, we now have two definitively correct possible definitions of convex space: a $\mathcal{G}_{\mathrm{fin}}$-algebra, or a model of $\texttt{FinStoMap}^{\mathrm{op}}$. We can now apply theorem [Fri09d, 3.14] to show that the compatibility requirements of definition 5.4.1 do indeed give all the relations 5.4.10 that we expect convex combinations to have.

Proposition 5.4.7. *Given a set $\mathcal{C}$ together with a structure of $\texttt{FinStoMap}^{\mathrm{op}}$-model in terms of a product-preserving functor $L : \texttt{FinStoMap}^{\mathrm{op}} \longrightarrow \texttt{Set}$, the operations*

$$cc_\lambda \equiv L(c_\lambda) \tag{5.4.17}$$

define the structure of a convex space on $\mathcal{C}$. Conversely given cc_λ, there is a unique L such that (5.4.17) holds.

Proof. This is the main application of theorem [Fri09d, 3.14]. First note that due to proposition 5.4.5, any product-preserving L satisfies

$$\begin{array}{rcl} L(\partial): & \mathcal{C} \to *, & x \mapsto * \\ L(e): & \mathcal{C} \to \mathcal{C} \times \mathcal{C}, & x \mapsto (x,x) \\ L(s): & \mathcal{C} \times \mathcal{C} \to \mathcal{C} \times \mathcal{C}, & (x,y) \mapsto (y,x) \end{array}$$

Hence, L is automatically compatible with the relations [Fri09d, (2)-(7), (11), (12)].

However, L also needs to preserve the other relations of $\texttt{FinStoMap}'$. In exactly this order, preservation of each of the relations [Fri09d, (8), (9), (10) and (13)] is equivalent to one of the requirements (5.4.1) to (5.4.4). □

We now turn to proving that the category $\texttt{ConvSpc}$ enjoys a certain rigidity property expressed by theorem 5.4.9.

For the following lemma, consider the family of maps on the unit interval $[0,1]$ that is given by

$$f_{y_0,y_1} : [0,1] \longrightarrow [0,1], \qquad x \mapsto \overline{x} y_0 + x y_1, \quad y_0, y_1 \in [0,1].$$

Lemma 5.4.8. *(a) The unit interval $[0,1]$ has a unique structure of convex space in which all of the f_{y_0,y_1} are convex maps.*

(b) For every convex space $\mathcal{C}$ and every pair of points $x, y \in \mathcal{C}$, there is a unique convex map $g_{x,y} : [0,1] \to \mathcal{C}$ with $g(0) = x$ and $g(1) = y$.

Proof. (a) In order to distinguish elements of the convex space $[0,1]$ from coefficients in $[0,1]$, we distinguish the fomer by means of the underline notation $\underline{\cdot}$.

We first show that the convex combination $\frac{1}{2}\underline{0} + \frac{1}{2}\underline{1}$ is necessarily equal to $\underline{1/2}$. To this end, consider the flip map $f_{1,0}$:

$$f_{1,0}\left(\frac{1}{2}\underline{0} + \frac{1}{2}\underline{1}\right) = \frac{1}{2} f_{1,0}\left(\underline{0}\right) + \frac{1}{2} f_{1,0}\left(\underline{1}\right) = \frac{1}{2}\underline{1} + \frac{1}{2}\underline{0} = \frac{1}{2}\underline{0} + \frac{1}{2}\underline{1}$$

Hence, the assertion follows from the fact that $\underline{1/2}$ is the unique fixed point of $f_{1,0}$.

But then also for any pair $x, y \in [0,1]$, we have that

$$\frac{1}{2}\underline{x} + \frac{1}{2}\underline{y} = \frac{1}{2} f_{x,y}\left(\underline{0}\right) + \frac{1}{2} f_{x,y}\left(\underline{1}\right) = f_{x,y}\left(\frac{1}{2}\underline{0} + \frac{1}{2}\underline{1}\right) = f_{x,y}\left(\underline{\frac{1}{2}}\right) = \underline{\frac{1}{2}x + \frac{1}{2}y}$$

Next, we claim that when $x < y$, $p, q \in \mathbb{N}_0$ and $\lambda \in (0,1)$ with $q2^{-p} \le \lambda \le (q+1)2^{-p}$, then

$$\left(\overline{\lambda}\underline{x} + \lambda\underline{y}\right) \in \left[\overline{q2^{-p}}x + q2^{-p}y,\ \overline{(q+1)2^{-p}}x + (q+1)2^{-p}y\right] \tag{5.4.18}$$

We prove this by induction on p. For $p = 0$, this is given by

$$\overline{\lambda}\underline{x} + \lambda\underline{y} = f_{x,y}\left(\overline{\lambda}\underline{0} + \lambda\underline{1}\right) \in \operatorname{im}\left(f_{x,y}\right) = [x, y].$$

For $p \ge 1$, consider the case $\lambda \ge 1/2$ first, which is equivalent to $q \ge 2^{p-1}$. Then

$$\left(q - 2^{p-1}\right)2^{-(p-1)} \le 2\lambda - 1 \le \left(q + 1 - 2^{p-1}\right)2^{-(p-1)}$$

so that

$$\overline{\lambda}\underline{x} + \lambda\underline{y} = 2\overline{\lambda}\left(\frac{1}{2}\underline{x} + \frac{1}{2}\underline{y}\right) + (2\lambda - 1)\underline{y} = 2\overline{\lambda}\,\underline{\left(\frac{1}{2}x + \frac{1}{2}y\right)} + (2\lambda - 1)\underline{y}$$

which, by the induction assumption, is bigger than or equal to

$$\overline{(q - 2^{p-1})2^{-(p-1)}}\left(\frac{1}{2}x + \frac{1}{2}y\right) + (q - 2^{p-1})2^{-(p-1)}y = \overline{q2^{-p}}x + q2^{-p}y,$$

as was to be shown. The upper bound works in exactly the same way. The case $\lambda \le 1/2$ can either be treated in a similar way, or can be reduced to the case $\lambda \ge 1/2$ by an application of the flip map $f_{1,0}$.

But then by the principle of nested intervals, equation (5.4.18) shows that $\overline{\lambda}\underline{x} + \lambda\underline{y} = \underline{\overline{\lambda}x + \lambda y}$, which concludes the proof.

(b) For $\lambda \in [0,1]$, the requirements imply that we need to set

$$g(\lambda) \equiv \overline{\lambda}x + \lambda y.$$

We now verify that this is indeed a convex map. With $\mu, \lambda_1, \lambda_2 \in [0,1]$, we have

$$g\left(\mu\lambda_1 + \overline{\mu}\lambda_2\right) = \overline{\left(\mu\lambda_1 + \overline{\mu}\lambda_2\right)}\,x + \left(\mu\lambda_1 + \overline{\mu}\lambda_2\right)y. \tag{5.4.19}$$

We proceed by evaluating the first coefficient further,

$$\overline{(\mu\lambda_1 + \overline{\mu}\lambda_2)} = \overline{\mu\lambda_1} + \overline{\overline{\mu}\lambda_2} - 1$$

$$= \overline{\mu} + \overline{\lambda}_1 - \overline{\mu}\overline{\lambda}_1 + \mu + \overline{\lambda}_2 - \mu\overline{\lambda}_2 - 1 = \mu\overline{\lambda}_1 + \overline{\mu}\overline{\lambda}_2$$

proving that (5.4.19) yields

$$g\left(\mu\lambda_1 + \overline{\mu}\lambda_2\right) = \mu\left(\overline{\lambda}_1 x + \lambda_1 y\right) + \overline{\mu}\left(\overline{\lambda}_2 x + \lambda_2 y\right) = \mu g(\lambda_1) + \overline{\mu}g(\lambda_2),$$

as was to be shown. □

Theorem 5.4.9. *The identity functor is the only endofunctor of* $\texttt{ConvSpc}$ *that makes the diagram*

$$\begin{tikzcd}
\texttt{ConvSpc} \arrow[rr] \arrow[dr] & & \texttt{ConvSpc} \arrow[dl] \\
& \texttt{Set} &
\end{tikzcd}$$

commute.

Proof. Let $E : \texttt{ConvSpc} \to \texttt{ConvSpc}$ be such an endofunctor. Commutativity of the diagram means that for any $\mathcal{C}, \mathcal{C}' \in \texttt{ConvSpc}$, $E(\mathcal{C})$ and $E(\mathcal{C}')$ are convex spaces with the same underlying sets as $\mathcal{C}$ and $\mathcal{C}'$, respectively, such that

$$\texttt{ConvSpc}\,(\mathcal{C}, \mathcal{C}') \subseteq \texttt{ConvSpc}\,(E(\mathcal{C}), E(\mathcal{C}'))\,. \qquad (5.4.20)$$

Now consider $\mathcal{C} = \mathcal{C}' = [0,1]$. Then it follows from lemma 5.4.8(a) that $E([0,1]) = [0,1]$ with the standard structure of convex space.

Now consider $\mathcal{C} = [0,1]$ and $\mathcal{C}'$ arbitrary. Then by lemma 5.4.8(b), we know that for any $x, y \in \mathcal{C}'$,

$$\overline{\lambda}x + \lambda y = g_{x,y}(\lambda).$$

Therefore, the structure of convex space on $E(\mathcal{C}')$ is uniquely determined by (5.4.20), showing that $E(\mathcal{C}') = \mathcal{C}'$. □

Remark 5.4.10. Theorem 5.4.9 displays a rigidity of $\texttt{ConvSpc}$ that is far from valid for other categories of algebraic structures. For example for the category of groups $\texttt{Grp}$, there is a non-trivial automorphism $\cdot^{\mathrm{op}} : \texttt{Grp} \longrightarrow \texttt{Grp}$, given by mapping each group to its opposite group, such that the diagram

$$\begin{tikzcd}
\texttt{Grp} \arrow[rr, "\cdot^{\mathrm{op}}"] \arrow[dr] & & \texttt{Grp} \arrow[dl] \\
& \texttt{Set} &
\end{tikzcd}$$

commutes. Hence, the direct analogue of theorem 5.4.9 for groups is false.

5.5 Convex spaces of geometric type

The first main class of examples of convex spaces are the convex subsets of vector spaces, which will be discussed now. We will refer to those convex spaces that can be embedded into a vector space as **convex spaces of geometric type**. These are the convex spaces studied in convex geometry. We are aware that many relevant properties of a convex set do depend on an explicit embedding into a vector space: for example, the volume or the number of points with integer coordinates are properties that are not invariant under affine transformations and therefore are not invariants of the convex space structure alone. Nevertheless, we hope that the theory of convex spaces might be able to shed new light on some aspects of convex geometry in general and some of the following examples in particular.

We will see in the upcoming two sections that there are also interesting examples of convex spaces that are not of geometric type.

Theorem 5.5.1 (convex spaces of geometric type)**.** *Given a real vector space V and a convex subset $\mathcal{C} \subseteq V$, the vector space structure of V turns $\mathcal{C}$ into a convex space.*

Proof. This is clear by defining the convex combination operations cc_λ via the vector space structure in the obvious way as

$$cc_\lambda(x,y) \equiv \lambda x + \overline{\lambda} y$$

since then the equations (5.4.1)–(5.4.4) follow easily from the vector space axioms. □

The map which turns every such convex set into a convex space is functorial in the following sense: consider the category of convex sets, where objects are pairs $(V, \mathcal{C})$ with V a real vector space and $\mathcal{C} \subseteq V$ a convex subset, and the morphisms $(V, \mathcal{C}) \to (V', \mathcal{C}')$ are the affine maps $f : V \to V'$ with $f(\mathcal{C}) \subseteq \mathcal{C}'$. Then each morphism f restricts to a convex map between convex spaces $f_{|\mathcal{C}} : \mathcal{C} \to \mathcal{C}'$. This construction is clearly functorial.

All examples following now are convex spaces of geometric type. In each case, we also describe how the convex space arises as a convex subset of a vector space.

Example 5.5.2 (free convex spaces)**.** Given a set X, the simplex Δ_X is a convex subset of the vector space $\mathbb{R}^X$. Alternatively, we can regard Δ_X as the set of formal convex combinations of elements of X. In this interpretation, Δ_X is the "free" convex space generated by X in the sense of a functor $\mathtt{Set} \to \mathtt{ConvSpc}$ left adjoint to the forgetful functor $\mathtt{ConvSpc} \to \mathtt{Set}$. This property is clear from the monadic definition of convex spaces, where $\Delta_\cdot$ figures as the underlying functor of the monad $\mathscr{G}_{\text{fin}}$. As a third point of view, Δ_X can also be regarded as the set of finitely supported probability measures on X.

Example 5.5.3 (probability measures)**.** As a variant of the previous example, we may consider a set X together with any σ-algebra $\Omega \subseteq 2^X$, turning (X, Ω) into a measurable space. Then the set of probability measures on (X, Ω) is a convex subset of the vector space $\mathbb{R}^\Omega$. We denote this convex space by $\Delta_{(X,\Omega)}$.

Example 5.5.4 (invariant measures)**.** Let (X, Ω) be a measurable space together with an action of a group G or monoid G given by a homomorphism $G \to \mathrm{End}(X)$. For example when $G = (\mathbb{R}, +)$, this action turns X into a dynamical system. Then the set of *invariant measures*, which are those probability measures that are preserved by the action of G, form a convex subspace of $\Delta_{(X,\Omega)}$. Of particular importance are the *ergodic measures* as those that cannot be written as a non-trivial convex combination of other invariant measures.

Example 5.5.5 (conditional probability distributions / classical communication channels)**.** Given measurable spaces (X, Ω_X) and (Y, Ω_Y), a *conditional probability distribution* on Y dependent on X is defined to be a convex map $\Delta_{(X,\Omega_X)} \to \Delta_{(Y,\Omega_Y)}$. Such a map describes a classical communication channel, where an input $x \in X$ is represented by the Dirac measure on x and gets mapped to a probability distribution of noise-affected possible outputs $y \in Y$. The set of all such maps is a convex space under pointwise convex combinations.

Example 5.5.6 (states on C^*-algebras)**.** Given a C^*-algebra A, a *state on A* is a positive linear functional $\phi : A \to \mathbb{C}$ of unit norm. The states on A form a convex subset of the vector space $\mathbb{C}^A$. In the case $A = \mathcal{B}(\mathcal{H})$, this convex space is isomorphic to the convex set of unit trace positive trace-class operators on $\mathcal{H}$, the so-called **density matrices**. Upon setting $\mathcal{H}_n \equiv \mathbb{C}^n$ for $n \in \mathbb{N}$ and $H_n \equiv \ell^2(\mathbb{N})$ for $n = \infty$, the set of density matrices is given by

$$\mathcal{Q}_n \equiv \{\rho \in \mathcal{B}(\mathcal{H}_n) \mid \rho \geq 0,\ \mathrm{tr}(\rho) = 1\}.$$

This family of convex spaces is widely studied in quantum information theory. As a first example of how much information the convex space structure on $\mathcal{Q}_n$ contains, we show that one can use

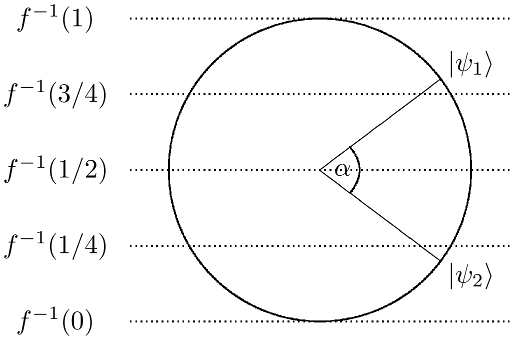


Figure 5.1: A two-dimensional section of the Bloch ball containing the states $|\psi_1\rangle$ and $|\psi_2\rangle$. The level sets of the optimal functional f are shown with pointed lines.

it to recover the scalar product of $\mathcal{H}_n$, at least up to a phase factor. This is achieved by the formula, depending on unit vectors $|\psi_1\rangle$ and $|\psi_2\rangle$,

$$\sqrt{1-|\langle\psi_1|\psi_2\rangle|^2} = \max_{f:\mathcal{Q}_n\to[0,1]\text{ convex}} \Big| f\left(|\psi_1\rangle\langle\psi_1|\right) - f\left(|\psi_2\rangle\langle\psi_2|\right)\Big|. \tag{5.5.1}$$

In order to prove the correctness of this equation, we consider the case $n=2$ first. Then $|\psi_1\rangle$ and $\psi_2\rangle$ can be identified with points on the Bloch sphere. The angle between these points, as seen from the center of the sphere, is given by

$$\cos\alpha = |\langle\psi_1|\psi_2\rangle|^2, \quad \alpha\in[0,\pi]$$

since the map $\rho\mapsto \mathrm{tr}(\rho|\psi_1\rangle\langle\psi_1|)$ is convex and can therefore be identified with a cartesian coordinate for the sphere. This situation is illustrated in figure 5.1.

Now when f is a $[0,1]$-valued convex functional on the Bloch ball, the value $|f\left(|\psi_1\rangle\langle\psi_1|\right) - f\left(|\psi_2\rangle\langle\psi_2|\right)|$ is maximal at most when f attains both 0 and 1. Then we call $f^{-1}(1)$ the "north pole" and $f^{-1}(0)$ the "south pole"; these points are clearly unique and diametrically opposite. Also it is clear that an optimal f will be such that $|\psi_1\rangle$ and $|\psi_2\rangle$ are aligned symmetrically with respect to the equator. Then,

$$f(|\psi_1\rangle\langle\psi_1|) = \frac{1}{2}+\frac{1}{2}\sin\left(\frac{\alpha}{2}\right), \quad f(|\psi_2\rangle\langle\psi_2|) = \frac{1}{2}-\frac{1}{2}\sin\left(\frac{\alpha}{2}\right)$$

so that

$$|f\left(|\psi_1\rangle\langle\psi_1|\right) - f\left(|\psi_2\rangle\langle\psi_2|\right)| = \sin\left(\frac{\alpha}{2}\right) = \sqrt{1-|\langle\psi_1|\psi_2\rangle|^2}\,,$$

as was to be shown.

For general n, consider the Hilbert space spanned by $|\psi_1\rangle$ and $|\psi_2\rangle$. When $|\psi_1\rangle$ and $|\psi_2\rangle$ are linearly dependent, (5.5.1) holds trivially, hence we may assume the span to be two-dimensional. This yields an embedding $\mathcal{Q}_2 \hookrightarrow \mathcal{Q}_n$. In this way, every convex functional $\mathcal{Q}_n\to[0,1]$ can be restricted to $\mathcal{Q}_2\to[0,1]$, and then the "$\geq$" part of (5.5.1) follows from the previous considerations. On the other hand, the f constructed in the two-dimensional case is of the form $\rho\mapsto\langle\psi|\rho|\psi\rangle$, where $|\psi\rangle$ is an appropriate linear combination of $|\psi_1\rangle$ and $|\psi_2\rangle$. Therefore, this optimal f can actually be extended to all of $\mathcal{Q}_n$, so that this "$\geq$" bound is in fact tight.

Example 5.5.7 (KMS states)**.** A KMS state is a certain kind of state on a C^*-algebra relevant for equilibrium thermodynamics.

In statistical physics, thermal equilibrium of a system with its environment is described by an equilibrium state depending on the temperature. This state is usually given by the canonical ensemble's density matrix $\rho = \mathcal{Z}(\beta)^{-1}e^{-\beta H}$, where $\beta = 1/kT$ is the inverse temperature of the system, H stands for its Hamiltonian, and $\mathcal{Z}(\beta) = \mathrm{tr}(e^{-\beta H})$ denotes the partition function. However in some cases, the trace in the definition of $\mathcal{Z}(\beta)$ need not converge, such that the canonical ensemble does not exist. For example in the context of spontaneous symmetry breaking, there is clearly no unique equilibrium state. In these situations, equilibrium thermodynamics has to be phrased in terms of KMS states.

We now describe the notion of KMS state in detail. On the quantum level, a system is described by its C^*-algebra of observables A and a one-parameter group of automorphisms $\alpha_t : A \to A$; typically, this group is given by the Heisenberg picture time evolution $\alpha_t(a) = e^{iHt}ae^{-iHt}$. Then by definition, a state $\varphi : A \to \mathbb{C}$ is a *Kubo-Martin-Schwinger (KMS) state* [KM08a, p. 178] for inverse temperature β if and only if for all $a, b \in A$, there is a continuous function $F_{a,b}(z)$ defined on the strip $0 \leq \mathrm{Im}(z) \leq \beta$, and holomorphic on the interior of the strip, such that

$$F_{a,b}(t) = \varphi(a\alpha_t(b)), \qquad F_{a,b}(t + i\beta) = \varphi(\alpha_t(b)a). \tag{5.5.2}$$

It is then clear that the KMS states for fixed β form a convex subset of the convex space of all states on A. As a plausibility check, one may observe that the canonical ensemble $\varphi(a) = \mathcal{Z}(\beta)^{-1}\mathrm{tr}(e^{-\beta H}a)$ is a KMS state whenever the partition function $\mathcal{Z}(\beta) = \mathrm{tr}(e^{-\beta H})$ converges.

Example 5.5.8 (unit balls)**.** Let $(E, ||\cdot||)$ be a normed space. Then the unit ball

$$B_1 \equiv \{x \in E \mid ||x|| \leq 1\}$$

is a convex space in E. Conversely, the convex space B_1 determines the norm via

$$||x|| = \frac{1}{\sup\{r \in \mathbb{R}_{>0} \mid rx \in B_1\}}.$$

The same applies to seminorms.

Example 5.5.9 (torus actions on symplectic manifolds)**.** This is material taken from the book [Aud04].

Let (M, ω) be a compact connected symplectic manifold together with a collection of Hamiltonian functions $H_1, \ldots, H_n$ such that the H_i pairwise Poisson commute and generate (almost) periodic flows. Then the image of the map

$$f : M \to \mathbb{R}^n, \quad x \mapsto (H_1(x), \ldots, H_n(x))$$

is convex.

The proof of this result follows from proposition 5.5.10 together with the statement that all the level sets $f^{-1}(t)$, $t \in \mathbb{R}^n$, are empty or connected. The latter is a deep theorem the proof of which heavily relies on Morse theory.

Proposition 5.5.10. *Let X be a topological space and $\mathcal{F}$ a collection of functions $f : X \to \mathbb{R}^{n_f}$ such that*

- *$\mathcal{F}$ is closed under composition with linear projection maps $\mathbb{R}^{n_1} \twoheadrightarrow \mathbb{R}^{n_2}$,*
- *all level sets $f^{-1}(t)$, $f \in \mathcal{F}$, $t \in \mathbb{R}^{n_f}$, are empty or connected.*

Then $\mathrm{im}(f) \subseteq \mathbb{R}^{n_f}$ is convex for every $f \in \mathcal{F}$.

Proof. (see also [Aud04, p. 114].) We need to show that the intersection of $\mathrm{im}(f)$ with every affine line in $\mathbb{R}^{n_f}$ is connected. To this end, choose such an affine line and some linear projection $\pi : \mathbb{R}^{n_f} \twoheadrightarrow \mathbb{R}^{n_f-1}$ that maps this affine line to a point. The inverse image of this point under π is just the given affine line. Then by assumption, the preimage of this affine line in X has to be connected, therefore showing that the intersection of $\mathrm{im}(f)$ with this affine line also is connected. □

The statement of the next example can be proven by applying a certain refinement of example 5.5.9. We refer to [Aud04, IV.4.11] for more details.

Example 5.5.11 (the Schur-Horn theorem)**.** Consider an n-tuple of not necessarily distinct numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Then there is a hermitian $n \times n$-matrix A with $\mathrm{diag}(A) = (a_1, \ldots, a_n) \in \mathbb{R}^n$ and eigenvalues $\lambda_1, \ldots, \lambda_n$ if and only if

$$(a_1, \ldots, a_n) \in \mathrm{conv}\left(\left\{\, (\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}),\ \sigma \in S_n \right\}\right)$$

where $\mathrm{conv}(\cdot)$ stands for the convex hull in $\mathbb{R}^n$ of its argument and S_n is the group of permutations of $[n]$.

Example 5.5.12 (metrics)**.** These are actually two related examples. For the first, let X be a set. A metric on X is a function $d : X \times X \longrightarrow \mathbb{R}_{\geq 0}$ satisfying definiteness, symmetry, and the triangle inequality. A convex combination of two metrics is again a metric. Therefore, the set of metrics is a convex space of geometric type lying in the vector space $\mathbb{R}^{X \times X}$.

For the second example, consider a manifold M and the set of Riemannian metrics on M. A Riemannian metric is a positive definite symmetric tensor of rank $(0, 2)$ on M. Therefore, the set of Riemannian metrics is a convex space of geometric type lying the vector space $\mathcal{T}^0_2(M)$ of all rank $(0, 2)$ tensors on M.

Example 5.5.13 (non-example: points on a Riemannian manifold)**.** Take $\mathcal{C}$ to be a subset of a Riemannian manifold, such that each pair of points $x, y \in \mathcal{C}$ can be joined by a unique geodesic $[x, y] \subseteq \mathcal{C}$. Upon fixing the affine parameter λ of the geodesic $[a, b]$ such that $\lambda = 0$ at y and $\lambda = 1$ at x, one might be tempted to define the convex combination $\lambda x + \overline{\lambda} y$ as the point on $[a, b]$ corresponding to the affine parameter λ. Then this satisfies the unit law, idempotency and parametric commutativity. Now assume that deformed parametric associativity also holds, thereby turning $\mathcal{C}$ into a convex space. Then any triple of points $x, y, z \in \mathcal{C}$ defines a convex map $\Delta_3 \to \mathcal{C}$ that maps straight lines to geodesics. But then by virtue of the geodesic deviation equation, the manifold is flat along the triangle spanned by x, y and z. Since this triple was arbitrary, the manifold is flat on all of $\mathcal{C}$. Conversely if the manifold is flat on $\mathcal{C}$, we are exactly in the situation of theorem 5.5.1.

Example 5.5.14 (color perception and chromaticity)**.** The physical color of light is given by its spectral density $I(\lambda)$, where $I(\lambda)d\lambda$ is the intensity of light in the wavelength interval $[\lambda, \lambda + d\lambda]$. Hence a priori, there are infinitely many physical degrees of freedom in the spectrum. However since the human eye only has three different kinds of receptors, our perception projects this two a three-dimensional space, which we perceive as three different kinds of visual colors.

More formally, a physical color is defined by a finite measure $d\mu$ on the space of wavelengths $[0, \infty)$. The corresponding visual color is obtained by integrating $d\mu$ with respect to three non-

[4] Both images were copied from `http://en.wikipedia.org/wiki/CIE_1931_color_space` using the GNU FDL.

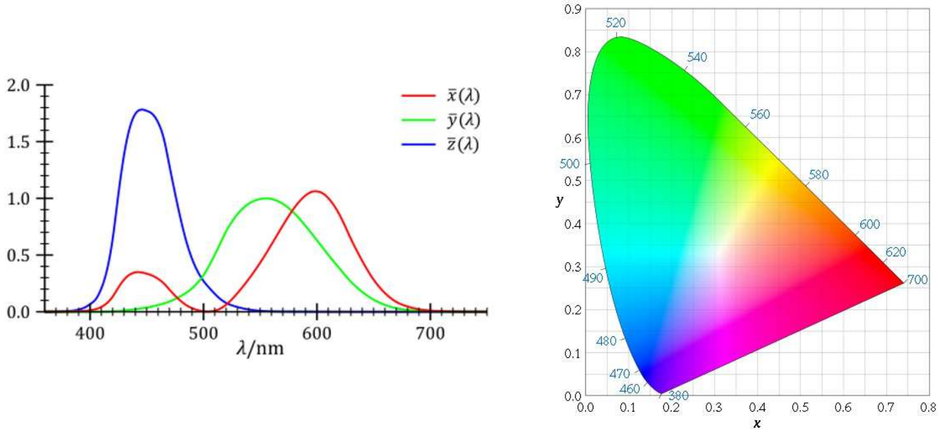


Figure 5.2: The CIE 1931 color matching functions and the resulting chromaticity diagram[4]. The curved part of the boundary is formed by the monochromatic colors of the specified wavelengths.

negative *color matching functions*[5] $\overline{x}(\lambda)$, $\overline{y}(\lambda)$, $\overline{z}(\lambda)$:

$$\begin{aligned} X &= \textstyle\int \overline{x}(\lambda) d\mu \\ Y &= \textstyle\int \overline{y}(\lambda) d\mu \\ Z &= \textstyle\int \overline{z}(\lambda) d\mu. \end{aligned}$$

Hence we get a convex map from the convex space of all finite measures on $[0, \infty)$ to the convex space $\mathbb{R}^3_{\geq 0}$, such that scaling the measure by a non-negative constant also scales all (X, Y, Z) by that constant. The chromaticity diagram in figure 5.2 depicts the image of this convex map in a two-dimensional cross-section which corresponds to restricting to colors of specified brightness. Since the image of any convex map is convex, so is the color region of the chromaticity diagram. Morally speaking, we can think of any physical color $d\mu$ as a free convex combination of monochromatic colors, i.e. Dirac measures on $[0, \infty)$. Then every visual color in the chromaticity diagram is a convex combination of monochromatic colors.

Convex sets also feature prominently in many kinds of optimization problems. We start with a particular example of a linear programming problem.

Example 5.5.15 (static friction for rigid bodies)**.** Consider a long and thin rod with quadratic cross-section lying on a flat surface. Then upon application of a small force along the side of the rod, the static friction between the rod and the surface keeps the rod from sliding. The question is: under the assumption that the force applies on the side of the rod towards its end, how big can that force be without the rod starting to slide? The situation is illustrated in figure 5.3.

We assume all physical parameters (mass and length of the rod, coefficient of friction, ...) to be known and set them to unity without loss of generality. Then as shown in the figure, the friction forces along the rod are described in terms of a linear density $f(x)$ with the constraint that there is a maxmial amount of friction for each length element, so that $|f(x)| \leq 1$. Now upon application of a small enough force $\vec{F}$, the friction will adjust in such a way that the force

[5] Note that for technical reasons, these do actually not coincide with the response functions of the eye's receptors.

is balanced, i.e. $\vec{F} + \vec{e}_y \int_0^1 f(x)dx = 0$, and torque is balanced, i.e. $\int_0^1 xf(x)dx = 0$. Hence the maximal force that can be applied is given by the solution of the linear program

$$\begin{gathered} -1 \leq f(x) \leq +1 \\ \int_0^1 xf(x)dx = 0 \\ \max\left(\int_0^1 f(x)dx\right) \end{gathered}$$

As always in linear programming, the set of admissible solutions $f(x)$ is determined by a set of linear equalities and inequalities, and therefore is convex. We can solve this problem by introducing a Lagrange multiplier μ for the equality constraint, and solving the optimization problem

$$\begin{gathered} -1 \leq f(x) \leq +1 \\ \max\left(\int_0^1 f(x)dx + \mu \int_0^1 xf(x)dx\right) = \max\left(\int_0^1 (\mu x + 1)\, f(x)dx\right) \end{gathered}$$

It is clear this problem has a unique optimal solution given by

$$f^*_\lambda(x) = \begin{cases} +1 & \text{for } \mu x + 1 > 0 \\ -1 & \text{for } \mu x - 1 < 0 \end{cases} .$$

Then the torque constraint $\int_0^1 xf(x)dx = 0$ holds if and only if $\mu = -\sqrt{2}$, so that the optimal configuration is given by

$$f^*(x) = \begin{cases} +1 & \text{for } x < 1/\sqrt{2} \\ -1 & \text{for } x > 1\sqrt{2} \end{cases} .$$

With this result, we determine the absolute value of the maximal force to be

$$F = \int_0^1 f^*(x)dx = \sqrt{2} - 1.$$

We expect that these considerations can be generalized to arbitrary rigid bodies in $\mathbb{R}^n$. To this end, f will have to be replaced by a vector-valued function $\vec{f}(x)$ restricted such as $|\vec{f}(x)| \leq \rho(x)$, where ρ is the rigid body's density distribution, while there will be one linear constraint for each component of the total torque. Then the set of admissible $\vec{f}(x)$ is a convex space that comes with a convex map to the vector space of all potential forces acting on a certain point of the rigid body. The forces that can be applied at that point without the body starting to slide are exactly given by the image of this convex map.

Introducing a Lagrange multiplier as above is a special case of duality theory for linear programs. Hence the following question arises: when formulating convex programming in the context of convex spaces, is there a nice notion of duality that generalizes the classical Karush-Kuhn-Tucker theory? What are appropriate constraint qualifications guaranteeing strong duality?

Since linear programming is a relatively easy optimization problem, one tries to reduce other optimization problems to the linear case. This is done for combinatorial optimization problems in particular, and hence convex spaces might also be of relevance for those.

Example 5.5.16 (combinatorial optimization)**.** For us, a combinatorial optimization problem is given by a finite set $X = \{x_1, \ldots, x_n\}$ (the search space) and a linear subspace

$$\mathcal{OF} \subseteq \mathbb{R}^X$$

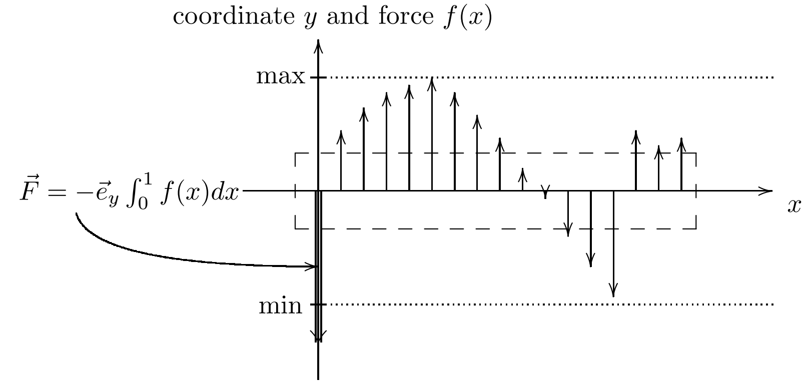

coordinate y and force $f(x)$
max
$\vec{F} = -\vec{e}_y \int_0^1 f(x)dx$
x
min

Figure 5.3: Candidate distribution of static friction along a thin rod upon application of the force $\vec{F}$. The dashed lines indicate the contour of the rod as seen from above.

that is the class of all possible *objective functions*. A particular *instance* of the problem is then given by specifying some $f \in \mathcal{OF}$, and the task is to find the optimal value

$$\max_{i=1,\ldots,n} f(x_i) = ?\,.$$

Typically, n is so large that brute-force enumeration of the search space is practically impossible, and therefore one needs to exploit the structure of $\mathcal{OF}$ as the way it lies inside $\mathbb{R}^X$.

For example, let X be the set of all Hamiltonian cycles in a finite graph G, and $\mathcal{OF}$ the set of all functions on X which one obtains by assigning a weight to each edge of G and mapping a Hamiltonian cycle to the sum of its edge weights. In this way, one obtains the famous *travelling salesman problem* on G.

Since all that matters is how a candidate point x_i behaves under objective functions, we can identify x_i with the evaluation map

$$x_i : \mathcal{OF} \to \mathbb{R}, \quad f \mapsto f(x_i).$$

In this way, X becomes identified with a finite subset of $\mathbb{R}^{\mathcal{OF}}$. Now consider the polytope

$$\mathcal{P} \equiv \operatorname{conv}\left(\{x_1, \ldots, x_n\}\right) \subseteq \mathbb{R}^{\mathcal{OF}}.$$

Then each $f \in \mathcal{OF}$ turns into a convex map $f : \mathcal{P} \to \mathbb{R}$. In practice, one tries to describe $\mathcal{P}$ in terms of linear inequalities, which reduces the combinatorial optimization problem to a linear optimization problem. For example in case of the travelling salesman problem, $\mathcal{P}$ is the *travelling salesman polytope* over G.

Example 5.5.17 (Dempster-Shafer theory)**.** Dempster-Shafer theory is a mathematical framework dealing with quantitative reasoning with evidence and belief. It finds applications for example in artificial intelligence and machine learning [PH98]. A *probability mass function* on a (finite) set X is defined to be a map $m : 2^X \to [0,1]$ such that

$$m(\emptyset) = 0, \qquad \sum_{A \subseteq X} m(A) = 1.$$

Morally, $m(A)$ measures an agent's confidence that a specific element of X lies in A, but the agent is completely ignorant about which element of A it might be. Probability measures may be identified with those probability mass functions that are supported on the singleton subsets. Abstractly, the convex space of probability mass functions on X coincides with the simplex $\Delta_{2^X\setminus\{\emptyset\}}$.

Example 5.5.18 (quantum measures)**.** According to Sorkin et al. [CDH$^+$07], a *quantum measure* on a (finite) set X is a map $\mu : 2^X \to [0,1]$ that satisfies the condition

$$\mu(A \cup B \cup C) - \mu(A \cup B) - \mu(A \cup C) - \mu(B \cup C) + \mu(A) + \mu(B) + \mu(C) = 0$$

whenever $A, B, C \subseteq X$ are disjoint events. In general, the convex space of quantum measures is not a simplex.

Example 5.5.19 (decision theory)**.** In the mathematical theory of decision (single-

It is clear that no list of relevant examples of convex sets could ever be complete. Therefore we simply end this list here by mentioning some particularly severe omissions:

- Polytopes in general [Zie95] as a certain kind of finitely generated convex spaces.
- In particular, lattice polytopes and their relation to toric varieties [Ful93].
- The geometry of numbers [Sie89] studying integer points (potentially over number fields) in convex subsets of $\mathbb{R}^n$.
- The Bernstein-Kushnirenko theorem expressing the generic number of non-trivial solutions to a system of polynomial equations in terms of a geometric invariant of a collection of polytopes [Stu98].
- The set of Bayesian networks on a fixed directed acyclic graph [KM08b].

5.6 Convex spaces of combinatorial type

Now we turn to convex spaces that cannot be embedded as convex subsets of vector spaces. The smallest of these is a convex space structure on a two-element set.

Example 5.6.1 (two-point convex space)**.** Let $\mathcal{FC} = \{i, f\}$ be a two-element set, and define convex combinations of the two elements as

$$\lambda i + \overline{\lambda} f \equiv \begin{cases} f & \text{if } \lambda = 0 \\ i & \text{if } \lambda \neq 0 \end{cases}$$

This satisfies all the axioms for a convex space.

Naively, one would deem the previous example pathological. Earlier on in the study of convex spaces, we were also trying to exclude such cases by changing the definition of convex space by requiring $\mathcal{C}$ to be a topological space and the convex combination operations to be continuous. However, we soon found out that example 5.6.1 is just a special case of a very natural class of convex spaces of combinatorial type, which should not be considered pathological at all. One reason is that $\mathcal{FC}$ from the previous example turns out to be the $\mathcal{F}$ace $\mathcal{C}$lassifier for convex spaces, with f representing a $f$ace and i the $i$nterior complement. Another reason is remark 5.6.4.

Definition 5.6.2. *A convex space $\mathcal{C}$ is said to be of **combinatorial type** if each function*

$$(0,1) \longrightarrow \mathcal{C}, \quad \lambda \mapsto \lambda x + \overline{\lambda} y$$

is constant.

Then when combining this definition with the axioms (5.4.1)–5.4.4, we see that a convex space of combinatorial type is nothing but a set $\mathcal{C}$ together with a binary operation

$$cc_{\frac{1}{2}} : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$$

which is idempotent, commutative and associative. It is well-known that such an algebraic structure is exactly the same thing as a meet-semilattice, which is a poset $(\mathcal{C}, \leq)$ such that each pair of elements has a **meet**, i.e. a greatest lower bound. In the following, the term **semilattice** always stands for **meet-semilattice**.

We digress briefly to describe the monad and the Lawvere theory underlying semilattices. The monad is a version of the **powerset monad** (or **Manes monad**) and is defined over the functor that maps every set to the set of its finite nonempty subsets.

Definition 5.6.3 (the finitary Manes monad)**.** *The finitary Manes monad $\mathscr{M}_{\text{fin}} \equiv (\mathcal{P}_{\text{fin}}, \varepsilon, \omega)$ is given by the functor*

$$\mathcal{P} : \texttt{Set} \to \texttt{Set}, \quad A \mapsto \mathcal{P}(A) \equiv \{B \subseteq A \mid B \neq \emptyset \textit{ is finite}\}$$

with the obvious action on morphims, the unit natural transformation

$$\varepsilon_A : A \to \mathcal{P}A, \quad x \mapsto \{x\}$$

and the multiplication transformation

$$\omega_A : \mathcal{P}\mathcal{P}A \to \mathcal{P}A, \quad C \mapsto \bigcup_{B \in C} B.$$

The Lawvere theory of semilattices is the category `FinMultiMap` of finite cardinals together with multivalued functions.

We can now see how both the monad and the Lawvere theory underlying convex spaces of combinatorial type are related to $\mathscr{G}_{\text{fin}}$ and `FinStoMap`. To this end, consider the semiring $\mathcal{S}_2 \equiv \{0, 1\}$ with $1 + 1 \equiv 1$. Then the monad $\mathscr{M}_{\text{fin}}$ originates from $\mathscr{G}_{\text{fin}}$ by replacing the $\mathbb{R}_{\geq 0}$-coefficients of $\mathscr{G}_{\text{fin}}$ by $\mathcal{S}_2$-coefficients. In the same way, `FinMultiMap` originates from `FinStoMap` by making the same change of coefficients: a multivalued function $[m] \to [n]$ is the same thing as a matrix $M_{n \times m}(\mathcal{S}_2)$ that is "stochastic" in the sense that all coefficients sum to 1.

More formally, changing coefficients along the semiring homomorphism

$$\mathbb{R}_{\geq 0} \to \mathcal{S}_2, \quad \lambda \mapsto \operatorname{sgn}(\lambda)$$

yields a morphism of Lawvere theories $\texttt{FinStoMap}^{\text{op}} \to \texttt{FinMultiMap}^{\text{op}}$ and a morphism of monads $\mathscr{G}_{\text{fin}} \to \mathscr{M}_{\text{fin}}$ given by

$$\Delta_X \longrightarrow \mathcal{P}(X), \quad \sum_{i \text{ with } \lambda_i > 0} \lambda_i x_i \mapsto \{x_1, \ldots, x_n\}$$

These morphisms imply that a semilattice naturally carries a convex space structure.

Remark 5.6.4. What does this change of coefficients mean in the information-theoretic interpretation of convex spaces? The answer is that $\mathcal{S}_2$ coefficients only care about qualitative *possibilities*, while $\mathbb{R}_{\geq 0}$ coefficients contain information about quantitative *probabilities*.

We now give a few examples of semilattices.

Example 5.6.5 (free semilattices)**.** Given a set X, the free semilattice over X is given by $\mathcal{C} \equiv \mathcal{P}(X)$ together with the partial order

$$A, B \in \mathcal{P}(X): \quad A \leq B \iff A \supseteq B.$$

Then the meet of two finite non-empty subsets of X is given by their union.

Example 5.6.6 (possibility measures)**.** Given a measurable space (X, Ω), a **possibility measure** on (X, Ω) is a map $\mu : \Omega \longrightarrow [0,1]$ such that $\mu(\emptyset) = 0$, $\mu(X) = 1$ and

$$\mu\left(\bigcup_{i\in\mathbb{N}} X_i\right) = \sup_{i\in\mathbb{N}} \mu\left(X_i\right)$$

for every countable family of subsets $X_i \in \Omega$.

Intuitively, μ measures the plausibility an observer assigns to an event. A possibility of 0 means that the event is impossible. On the other hand, a possibility of 1 means that the event is totally unsurprising, although it need not occur with absolute certainty.

The set of possibility measures on (X, Ω) is a semilattice with respect to the ordering

$$\mu \leq \mu' \iff \mu(Y) \leq \mu'(Y) \;\; \forall Y \in \Omega.$$

The meet operation is given by

$$(\mu_1 \wedge \mu_2)(Y) = \min\left\{\mu_1(Y), \mu_2(Y)\right\}.$$

Example 5.6.7. Consider $\mathcal{C} = \mathbb{N}$ as a partially ordered set with respect to divisibility:

$$x \leq y \iff x|y$$

Then the meet of two natural numbers is given by their greatest common divisor. Hence, $(\mathbb{N}, |)$ is a semilattice which encodes some number-theoretic information.

On the other hand, the decomposition of an integer into its prime factors yields an isomorphism of partially ordered sets $(\mathbb{N}, |) \cong \mathbb{N}^{\times\mathbb{P}}$, where $\mathbb{P}$ denotes the set of prime numbers, and $\mathbb{N}^{\times\mathbb{P}}$ carries the product order. This means that there is nothing to gain from studying the semilattice $(\mathbb{N}, |)$ by itself without any additional structure.

5.7 Convex spaces of mixed type

The above two types of convex spaces should be considered to be extreme cases. In general, a convex space will have a flavor of both the geometrical type and the combinatorial type. For example when starting with a convex space of geometrical type, the following construction will add a combinatorial flavor:

Example 5.7.1 (adjoining a point at infinity)**.** Let $\mathcal{C}$ be any convex space. Then we define a new convex space as $\mathcal{C}_\infty \equiv \mathcal{C} \cup \{\infty\}$, where the convex combinations are inherited from $\mathcal{C}$ together with, for all points $x \in \mathcal{C}$,

$$\lambda\infty + \overline{\lambda}x \equiv \begin{cases} x & \text{for } \lambda = 0 \\ \infty & \text{for } \lambda \neq 0 \end{cases}$$

There is much more general construction lying behind this example: starting with a semilattice $\mathcal{S}$, we choose a convex space $\mathcal{C}_s$ for each $s \in \mathcal{S}$. The $\mathcal{C}_s$ may be of geometric type, but this is not required. Now we consider the disjoint union

$$\mathcal{C} \equiv \bigcup_{s \in \mathcal{S}} \mathcal{C}_s.$$

Hence, $\mathcal{C}$ is a set over $\mathcal{S}$ with fibers $\mathcal{C}_s$. Furthermore, for every relation $s \leq s'$, we choose a convex map $f_{s,s'} : \mathcal{C}_{s'} \longrightarrow \mathcal{C}_s$, such that this data amounts to a functor

$$f_{\cdot,\cdot} : \mathcal{S}^{\mathrm{op}} \longrightarrow \mathtt{ConvSpc}, \quad s \mapsto \mathcal{C}_s, \quad (s \leq s') \mapsto f_{s,s'}$$

where the poset $\mathcal{S}$ is considered as a category in the usual way. Now we can define convex combinations on $\mathcal{C}$ as

$$\lambda \in (0,1),\, x \in \mathcal{C}_s,\, y \in \mathcal{C}_t : \quad \lambda x + \overline{\lambda} y \equiv \lambda f_{s\wedge t,s}(x) + \overline{\lambda} f_{s\wedge t,t}(y) \ \in \mathcal{C}_{s\wedge t}.$$

Intuitively speaking: for taking a non-trivial convex combination of some point in $\mathcal{C}_s$ and some point in $\mathcal{C}_t$, we have to transport both of them to $\mathcal{C}_{s\wedge t}$ first and then can take the convex combination there. We denote the resulting convex space by $\mathcal{C} = \mathcal{S}_f \ltimes \mathcal{C}_\cdot$.

Example 5.7.1 is subsumed by this construction upon setting $\mathcal{S} \equiv \mathcal{FC}$ (from example 5.6.1), $\mathcal{C}_f \equiv \mathcal{C}$ and $\mathcal{C}_i \equiv \{\infty\}$. The map $f_{f,i} : \mathcal{C} \to \{\infty\}$ is trivially unique.

Example 5.7.2 (a lottery)**.** Suppose we buy a ticket for a lottery. Also suppose that we do not really care about what the prizes are, as long as we win *something*; hence before the results are drawn, we only care about our subjective probability of winning $p \in [0,1]$. But then as soon as we know that we have a winning ticket (i.e. $p = 1$), of course we also become interested in what the prize actually is – the possibilities being, say, an apple a or a banana b. Hence in this stage of the process, our subjective state of information is given by an element of $\Delta_{\{a,b\}}$. In total, our possible states of subjective information are given by the convex space

$$[0,1) \cup \Delta_{\{a,b\}}$$

where convex combinations within $[0,1)$ or within $\Delta_{\{a,b\}}$ are the ordinary ones, while in addition, for a coefficient $\lambda \in (0,1)$ and a point $p \in [0,1)$,

$$\lambda p + \overline{\lambda} \left(\mu a + \overline{\mu} b\right) \equiv \lambda p + \overline{\lambda}.$$

Intuitively speaking, $\Delta_{\{a,b\}}$ acts on $[0,1)$ by convex combinations with 1. As illustrated in figure 5.4, one can view this convex space as the quotient of $\Delta_{\{p=0,a,b\}}$ where all formal convex combinations with fixed positive coefficient of $p = 0$ are identified.

Since $1 \notin [0,1)$, this convex space is not of the form $\mathcal{S}_f \ltimes \mathcal{C}_\cdot$ for any $\mathcal{S}$ and $\mathcal{C}_\cdot$.

Example 5.7.3 (convex space of convex sets)**.** Let V be a real vector space, and take $\mathcal{C}$ to be the set of all convex subsets of V:

$$\mathcal{C} \equiv \{C \subseteq V \mid C \text{ is convex}\}$$

Then convex combinations of two convex subsets C_1 and C_2 can be defined by

$$\lambda C_1 + \overline{\lambda} C_2 \equiv \left\{\lambda c_1 + \overline{\lambda} c_2,\, c_i \in C_i\right\}.$$

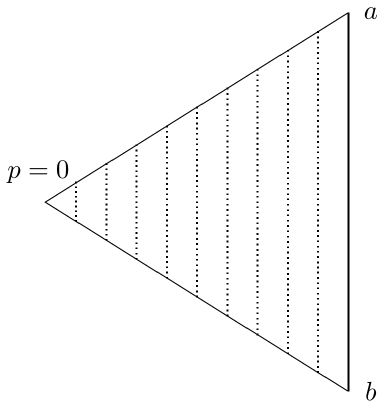


Figure 5.4: The convex space from example 5.7.2. All points on a dotted line are identified, while the points on the line connecting a to b stay distinct.

Except in the degenerate case $V = 0$, this convex space is neither of geometric type nor of combinatorial type. For example when $V = \mathbb{R}$, we can use open and closed intervals to get relations of the form

$$\frac{1}{2}(0,1) + \frac{1}{2}[0,1] = (0,1),$$

which cannot possibly hold in a convex space of geometric type. Similar examples abound in higher dimensions.

When considering only those subsets $C \subseteq V$ that are the convex hulls of finitely many points, we obtain the *convex space of polytopes in V*. This is a convex space of geometric type[6]

[6] Sketch of proof: suppose that $\lambda P + (1-\lambda)Q = \lambda P' + (1-\lambda)Q$. This implies $n\lambda P + (1-\lambda)Q = n\lambda P' + (1-\lambda)Q$ for any $n \in \mathbb{N}$. Then $P = P'$ follows by choosing n large enough.

Bibliography

[AC08] Samson Abramsky and Bob Coecke. Categorical quantum mechanics. Technical Report arXiv:0808.1023, Aug 2008. Comments: 63 pages with 22 pictures; Chapter in the Handbook of Quantum Logic and Quantum Structures vol II, Elsevier, 2008.

[AS01] Erik M. Alfsen and Frederic W. Shultz. *State spaces of operator algebras*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 2001. Basic theory, orientations, and C^*-products.

[Aud04] Michèle Audin. *Torus actions on symplectic manifolds*, volume 93 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, revised edition, 2004.

[AV07] Yakir Aharonov and Lev Vaidman. The two-state vector formalism: An updated review. In Iacute. L. Egusquiza J. G. Muga, R. S. Mayato, editor, *Lecture Notes in Physics, Berlin Springer Verlag*, volume 734 of *Lecture Notes in Physics, Berlin Springer Verlag*, pages 399–+, 2007.

[Bar06] Jonathan Barrett. Information processing in generalized probabilistic theories. 2006, arXiv:quant-ph/0508211v3. preprint.

[CDH$^+$07] David Craig, Fay Dowker, Joe Henson, Seth Major, David Rideout, and Rafael D. Sorkin. A Bell inequality analog in quantum measure theory. *J. Phys. A*, 40(3):501–523, 2007.

[CM57] H. S. M. Coxeter and W. O. J. Moser. *Generators and relations for discrete groups*. Springer-Verlag, Berlin, 1957.

[Dob06] Ernst-Erich Doberkat. Eilenberg-Moore algebras for stochastic relations. *Inform. and Comput.*, 204(12):1756–1781, 2006.

[Fey] Richard P. Feynman. The character of physical law: seeking new laws. Messenger Lectures. `http://cdsweb.cern.ch/record/1048168`.

[Fri09a] Tobias Fritz, 2009. `http://guests.mpim-bonn.mpg.de/fritz/2009/semilattice_fourier_motzkin.tar.gz`.

[Fri09b] Tobias Fritz. Convex spaces I: Definition and examples. 2009. `http://arxiv.org/abs/0903.5522`.

[Fri09c] Tobias Fritz. Possibilistic physics. 2009. `http://www.fqxi.org/community/forum/topic/569`.

[Fri09d] Tobias Fritz. A presentation of the category of stochastic matrices. 2009. `http://arxiv.org/abs/0902.2554`.

[Fri10a] Tobias Fritz. On the existence of quantum representations for two dichotomic measurements. *J. Math. Phys.*, 2010. to appear, `http://arxiv.org/abs/0908.2559`.

[Fri10b] Tobias Fritz. The quantum region for von neumann measurements with postselection. 2010, `http://arXiv.org/abs/1003.4437`. submitted.

[Ful93] William Fulton. *Introduction to toric varieties*, volume 131 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1993. The William H. Roever Lectures in Geometry.

[Gir82] Michèle Giry. A categorical approach to probability theory. In *Categorical aspects of topology and analysis (Ottawa, Ont., 1980)*, volume 915 of *Lecture Notes in Math.*, pages 68–85. Springer, Berlin, 1982.

[HP07] Martin Hyland and John Power. The category theoretic understanding of universal algebra: Lawvere theories and monads. In *Computation, meaning, and logic: articles dedicated to Gordon Plotkin*, volume 172 of *Electron. Notes Theor. Comput. Sci.*, pages 437–458. Elsevier, Amsterdam, 2007.

[Khr09] Andrei Khrennikov. *Contextual Approach to Quantum Formalism.* Fundamental ories of Physics, 160. Springer, Dordrecht, 2009.

[KJR04] Aephraim M. Steinberg Kevin J. Resch, Jeff S. Lundeen. Experimental realization of the quantum 3-box problem. *Physics Letters A*, 324:125–131, 2004.

[KM08a] Masoud Khalkhali and Matilde Marcolli, editors. *An invitation to noncommutative geometry.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008. Lectures from the International Workshop on Noncommutative Geometry held in Tehran, 2005.

[KM08b] Uffe B. Kjærulff and Anders L. Madsen. *Bayesian networks and influence diagrams.* Information Science and Statistics. Springer, New York, 2008. A guide to construction and analysis.

[Lei08] Tom Leinster. Comment on the n-Category Café, `http://golem.ph.utexas.edu/category/2008/10/entropy_diversity_and_cardinal.html`, 2008.

[Lor86] George G. Lorentz. *Bernstein polynomials.* Chelsea Publishing Co., New York, second edition, 1986.

[Mas97] A. Massol. Minimality of the system of seven equations for the category of finite sets. *Theoret. Comput. Sci.*, 176(1-2):347–353, 1997.

[Oxl92] James G. Oxley. *Matroid theory.* Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1992.

[PH98] Simon Parsons and Anthony Hunter. A review of uncertainty handling formalisms. In *Applications of Uncertainty Formalisms*, pages 8–37, London, UK, 1998. Springer-Verlag.

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

[Sie89] Carl Ludwig Siegel. *Lectures on the geometry of numbers.* Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[Spe07] Robert W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Phys. Rev. A*, 75(3):032110, Mar 2007.

[Sto49] M. H. Stone. Postulates for the barycentric calculus. *Ann. Mat. Pura Appl. (4)*, 29:25–30, 1949.

[Stu98] Bernd Sturmfels. Polynomial equations and convex polytopes. *Amer. Math. Monthly*, 105(10):907–922, 1998.

[Świ75] Tadeusz Świrszcz. Monadic functors and categories of convex sets. *Proc. Inst. Math. Pol. Acad. Sci., Warsaw*, 1975. Preprint No. 70.

[vNM07] John von Neumann and Oskar Morgenstern. *Theory of games and economic behavior.* Princeton University Press, Princeton, NJ, anniversary edition, 2007. With an introduction by Harold W. Kuhn and an afterword by Ariel Rubinstein.

[Wid41] D. V. Widder. *The Laplace Transform.* PUP, 1941.

[Zie95] Günter M. Ziegler. *Lectures on polytopes*, volume 152 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

Abstracts of chapters

Chapter 1: On the existence of quantum representations for two dichotomic measurements. Under which conditions do outcome probabilities of measurements possess a quantum-mechanical model? This kind of problem is solved here for the case of two dichotomic von Neumann measurements which can be applied repeatedly to a quantum system with trivial dynamics. The solution uses methods from the theory of operator algebras and the theory of moment problems. The ensuing conditions reveal surprisingly simple relations between certain quantum-mechanical probabilities. It also shown that generally, none of these relations holds in general probabilistic models. This result might facilitate further experimental discrimination between quantum mechanics and other general probabilistic theories.

This chapter has also been published as [Fri10a].

Chapter 2: Possibilistic Physics. I try to outline a framework for fundamental physics where the concept of probability gets replaced by the concept of possibility. Whereas a probabilistic theory assigns a state-dependent probability value to each outcome of each measurement, a possibilistic theory merely assigns one of the state-dependent labels "possible to occur" or "impossible to occur" to each outcome of each measurement. It is argued that Spekkens' combinatorial toy theory of quantum mechanics is inconsistent in a probabilistic framework, but can be regarded as possibilistic. Then, I introduce the concept of possibilistic local hidden variable models and derive a class of possibilistic Bell inequalities which are violated for the possibilistic Popescu-Rohrlich boxes. The chapter ends with a philosophical discussion on possibilistic vs. probabilistic. It can be argued that, due to better falsifiability properties, a possibilistic theory has higher predictive power than a probabilistic one.

This chapter was an entry [Fri09c] for the essay contest "What's ultimately possible in physics?" by the Foundational Questions Institute FQXi.

Chapter 3: The quantum region for von Neumann measurements with postselection. It is determined under which conditions a probability distribution on a finite set can occur as the outcome distribution of a quantum-mechanical von Neumann measurement with postselection, given that the scalar product between the initial and the final state is known as well as the success probability of the postselection. An intermediate von Neumann measurement can enhance transition probabilities between states such that the error probability shrinks by a factor of up to 2.

This chapter has been submitted for publication and is also available as a preprint [Fri10b].

Chapter 4: A presentation of the category of stochastic matrices. This chapter gives generators and relations for the strict monoidal category of probabilistic maps on finite cardinals (i.e., stochastic matrices).

This chapter has also been published in a slightly different form as a preprint [Fri09d].

Chapter 5: Convex Spaces: Definition and Examples. We try to promote convex spaces as an abstract concept of convexity which was introduced by Stone [Sto49] as "barycentric calculus". A convex space is a set where one can take convex combinations in a consistent way. By identifying the corresponding Lawvere theory as the category from chapter 4 and using the results obtained there, we give a different proof of a result of Świrszcz [Świ75] which shows that convex spaces can be identified with algebras of a finitary version of the Giry monad. After giving an extensive list of examples of convex sets as they appear throughout mathematics and theoretical physics, we note that there also exist convex spaces that cannot be embedded into a vector space: semilattices are a class of examples of purely combinatorial type. In an information-theoretic interpretation, convex subsets of vector spaces are probabilistic, while semilattices are possibilistic. Convex spaces unify these two concepts.

This chapter has also been published in a previous form as a preprint [Fri09b].