Probability

April 27, 2016

1 Classical Probability Spaces

A *probability space* [5, 7, 17] specifies the necessary conditions for reasoning coherently about collections of uncertain events. It consists of a *sample space* Ω, a space of *events* $\mathcal{E}$, and a *probability measure* μ. In this paper, we will only consider *finite* sets of events: we therefore define a sample space Ω as an arbitrary non-empty finite set and the space of events $\mathcal{E}$ as 2^Ω, the powerset of Ω. Given the set of events $\mathcal{E}$, a *probability measure* is a function $\mu : \mathcal{E} \to [0, 1]$ such that:

- $\mu(\Omega) = 1$, and
- for a collection E_i, of pairwise disjoint events, $\mu(\bigcup_i E_i) = \sum_i \mu(E_i)$.

Example 1 (Two-coin probability space)**.** Consider an experiment that tosses two coins. We have four possible outcomes that constitute the sample space $\Omega = \{HH, HT, TH, TT\}$. There are 16 total events including for example the event $\{HH, HT\}$ that the first coin is "heads," the event $\{HT, TH\}$ that the two coins land on opposite sides, and the event $\{HT, TH, TT\}$ that at least one coin is tails. Here is a possible probability measure for these events:

$$\begin{aligned}
\mu(\emptyset) &= 0 & \mu(\{HT, TH\}) &= 2/3 \\
\mu(\{HH\}) &= 1/3 & \mu(\{HT, TT\}) &= 0 \\
\mu(\{HT\}) &= 0 & \mu(\{TH, TT\}) &= 2/3 \\
\mu(\{TH\}) &= 2/3 & \mu(\{HH, HT, TH\}) &= 1 \\
\mu(\{TT\}) &= 0 & \mu(\{HH, HT, TT\}) &= 1/3 \\
\mu(\{HH, HT\}) &= 1/3 & \mu(\{HH, TH, TT\}) &= 1 \\
\mu(\{HH, TH\}) &= 1 & \mu(\{HT, TH, TT\}) &= 2/3 \\
\mu(\{HH, TT\}) &= 1/3 & \mu(\{HH, HT, TH, TT\}) &= 1
\end{aligned}$$

The assignment satisfies the two constraints for probability measures: the probability of the entire sample space is 1, and the probability of every collection of disjoint events (e.g., $\{HT, TH\} = \{HT\} \cup \{TH\}$) is the sum of the individual probabilities. The probability of collections of non-disjoint events (e.g., $\{HT, TH, TT\} = \{HT, TH\} \cup \{TH, TT\}$) may add to something different than the probabilities of the individual events. It is useful to think that this probability measure is completely induced by the two coins in question and their characteristics in the sense that each pair of coins induces a measure, and each measure must correspond to some pair of coins. In this example, the probability measure is induced by a weighted first coin and a double-headed second coin. □

In a strict computational or experimental setting, one may question the reliance of the definition of probability space on the uncountable and uncomputable real interval $[0, 1]$. This interval includes numbers like $0.h_1h_2h_3\ldots$ where h_i is 1 or 0 depending on whether Turing machine M_i halts or not. Such numbers cannot be computed. This interval also includes numbers like $\frac{\pi}{4}$ which can only be computed with increasingly large resources as the precision increases. Therefore, in a resource-aware setting, it is more appropriate to consider probability measures that map events to a finite set of elements computable with a fixed set of

$\vee$	*impossible*	*possible*	*unlikely*	*likely*	*overflow*
impossible	*impossible*	*possible*	*unlikely*	*likely*	*overflow*
possible	*possible*	*possible*	*possible*	*likely*	*overflow*
unlikely	*unlikely*	*possible*	*possible*	*likely*	*overflow*
likely	*likely*	*likely*	*likely*	*overflow*	*overflow*
overflow	*overflow*	*overflow*	*overflow*	*overflow*	*overflow*

Table 1: The operator $\vee$ on $\mathscr{L}_5 = \{\textit{impossible}, \textit{possible}, \textit{unlikely}, \textit{likely}, \textit{overflow}\}$

resources [2, 15]. The simplest such set, and the one we will consider exclusively in this paper, is the set $\mathscr{L}_2 = \{\textit{impossible}, \textit{possible}\}$ together with the operation $\vee$ where $x \vee y = \textit{impossible}$ if and only if $x = y = \textit{impossible}$. In relation to the first definition, one can interpret *impossible* as the closed interval $[0, 0]$, *possible* as the half-open interval $(0, 1]$, and $\vee$ as the addition of intervals. The definition of a probability measure in this case is modified as being a function $\mu : \mathcal{E} \to \mathscr{L}_2$ such that:

- $\mu(\Omega) = \textit{possible}$, and
- for a collection E_i, of pairwise disjoint events, $\mu(\bigcup_i E_i) = \bigvee_i \mu(E_i)$.

Example 2 (Two-coin probability space with finite set-valued probability measure)**.** Under the new set-valued requirement, the probability measure in the first example becomes:

$$\begin{aligned}
\mu(\emptyset) &= \textit{impossible} & \mu(\{HT, TH\}) &= \textit{possible}\\
\mu(\{HH\}) &= \textit{possible} & \mu(\{HT, TT\}) &= \textit{impossible}\\
\mu(\{HT\}) &= \textit{impossible} & \mu(\{TH, TT\}) &= \textit{possible}\\
\mu(\{TH\}) &= \textit{possible} & \mu(\{HH, HT, TH\}) &= \textit{possible}\\
\mu(\{TT\}) &= \textit{impossible} & \mu(\{HH, HT, TT\}) &= \textit{possible}\\
\mu(\{HH, HT\}) &= \textit{possible} & \mu(\{HH, TH, TT\}) &= \textit{possible}\\
\mu(\{HH, TH\}) &= \textit{possible} & \mu(\{HT, TH, TT\}) &= \textit{possible}\\
\mu(\{HH, TT\}) &= \textit{possible} & \mu(\{HH, HT, TH, TT\}) &= \textit{possible}
\end{aligned}$$

Compare to the first example, we can still get the information that the second coin is double-headed, although we loss the information that the first coin is weighted. □

If we consider set with more values, the probability measure may give us more information about the coins. For example, despite *impossible* and *possible*, we may also adopt three more values: *unlikely* as the interval $\left(0, \frac{1}{2}\right]$, *likely* as the interval $\left(\frac{1}{2}, 1\right]$, and *overflow* as the empty set $\emptyset$ which means the total probability may be excessed than one. In particular, $\textit{likely} \vee \textit{likely} = \textit{overflow}$ because the probability of two disjoint events should not both bigger than $\frac{1}{2}$. The complete rule for operator $\vee$ on $\mathscr{L}_5 = \{\textit{impossible}, \textit{possible}, \textit{unlikely}, \textit{likely}, \textit{overflow}\}$ is defined in table 1, or more abstractly, we define $(a, b] \vee (c, d] = (a + c, b + d] \cap [0, 1]$. The definition of a probability measure can be modified as a function $\mu : \mathcal{E} \to \mathscr{L}_5$ such that:

- $\mu(\Omega) \in \{\textit{possible}, \textit{likely}\}$ or equivalently $1 \in \mu(\Omega)$, and
- for a collection E_i, of pairwise disjoint events, $\mu(\bigcup_i E_i) = \bigvee_i \mu(E_i)$.

Example 3. [Two-coin probability space with $\mathscr{L}_5$-valued probability measure] Under the new $\mathscr{L}_5$-valued requirement, the probability measure in the first example becomes:

$$\begin{aligned}
\mu(\emptyset) &= \textit{impossible} & \mu(\{HT, TH\}) &= \textit{likely}\\
\mu(\{HH\}) &= \textit{unlikely} & \mu(\{HT, TT\}) &= \textit{impossible}\\
\mu(\{HT\}) &= \textit{impossible} & \mu(\{TH, TT\}) &= \textit{likely}\\
\mu(\{TH\}) &= \textit{likely} & \mu(\{HH, HT, TH\}) &= \textit{likely}\\
\mu(\{TT\}) &= \textit{impossible} & \mu(\{HH, HT, TT\}) &= \textit{unlikely}\\
\mu(\{HH, HT\}) &= \textit{unlikely} & \mu(\{HH, TH, TT\}) &= \textit{likely}\\
\mu(\{HH, TH\}) &= \textit{likely} & \mu(\{HT, TH, TT\}) &= \textit{likely}\\
\mu(\{HH, TT\}) &= \textit{unlikely} & \mu(\{HH, HT, TH, TT\}) &= \textit{likely}
\end{aligned}$$

In this example, we can get the information that the first coin is weighted and the second coin is double-headed. □

We will return to finite set-valued probability measures in Sec. **??**.

2 Quantum Probability Spaces

The mathematical framework above assumes that one has complete knowledge of the events and their relationships. However, in many practical situations, the structure of the event space is only partially known and the precise dependence of two events on each other cannot, a priori, be determined with certainty. In the quantum case, this partial knowledge is compounded by the fact that there exist non-commuting events which cannot happen simultaneously. To accommodate these more complex situations, we abandon the sample space Ω and reason directly about events. A quantum probability space therefore consists of just two components: a set of events $\mathcal{E}$ and a probability measure $\mu : \mathcal{E} \to [0, 1]$. We give an example before giving the formal definition.

Example 4 (One-qubit quantum probability space)**.** Consider a one-qubit Hilbert space with states $\alpha|0\rangle+\beta|1\rangle$ such that $|\alpha|^2+|\beta|^2 = 1$. The set of events associated with this Hilbert space consists of all projection operators. Each event is interpreted as a possible post-measurement state of a quantum system in current state $|\phi\rangle$. For example, the event $|0\rangle\langle 0|$ indicates that the post-measurement state will be $|0\rangle$; the event $|1\rangle\langle 1|$ indicates that the post-measurement state will be $|1\rangle$; the event $|+\rangle\langle +|$ where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ indicates that the post-measurement state will be $|+\rangle$; the event $\mathbb{1} = |0\rangle\langle 0| + |1\rangle\langle 1|$ indicates that the post-measurement state will be a linear combination of $|0\rangle$ and $|1\rangle$; and the empty event $\mathbb{0}$ states that the post-measurement state will be the empty state. As in the classical case, a probability measure is a function that maps events to $[0, 1]$: here is a partial specification of a possible probability measure:

$$\mu(\mathbb{0}) = 0, \quad \mu(\mathbb{1}) = 1, \quad \mu(|0\rangle\langle 0|) = 1, \quad \mu(|1\rangle\langle 1|) = 0, \quad \mu(|+\rangle\langle +|) = 1/2, \quad \ldots$$

Note that, similarly to the classical case, the probability of $\mathbb{1}$ is 1 and the probability of collections of orthogonal events (e.g., $|0\rangle\langle 0| + |1\rangle\langle 1|$) is the sum of the individual probabilities. In contrast, a collection of non-orthogonal events (e.g., $|0\rangle\langle 0|$ and $|+\rangle\langle +|$) is not itself an event. In the classical example, we argued that each probability measure is uniquely determined by two actual coins. A similar (but much more subtle) argument is valid also in the quantum case. By postulates of quantum mechanics and Gleason's theorem, it turns out that for large enough quantum systems, each probability measure is uniquely determined by an actual quantum state. □

To properly explain the previous example and generalize to arbitrary quantum systems, we formally discuss projection operators and then define a quantum probability space.

Definition 1 (Projection Operators; Orthogonality; Commutativity [12, 16, 14, 18])**.** Given a Hilbert space $\mathcal{H}$, a projection operator P is a linear transformation from $\mathcal{H}$ to itself such that $P^2 = P = P^\dagger$. Projection operators have the following properties:[1]

- Projection operators P_1 and P_2 are orthogonal if $P_1P_2 = P_2P_1 = \mathbb{0}$;
- Projection operators P_1 and P_2 commute if $P_1P_2 = P_2P_1$;
- If the projections P_1 and P_2 are orthogonal then $P_1 + P_2$ is also a projection;
- If the projections P_1 and P_2 commute then P_1P_2 is also a projection.

Definition 2 (Quantum Probability Space [3, 6, 16, 1, 11])**.** Given a Hilbert space $\mathcal{H}$, a *quantum probability space* consists of a set of events $\mathcal{E}$ and a probability measure $\mu : \mathcal{E} \to [0, 1]$ such that:[2]

[1] "Projection" is sometimes called "orthogonal projection" or "self-adjoint projection" to emphasize $P^\dagger = P$ [11].

[2] It is possible to define a more general space of events consisting of all operators $\mathcal{A}$ on $\mathcal{H}$ and consider $\mu : \mathcal{A} \to \mathbb{C}$ [11, 18]. When an operator $A \in \mathcal{A}$ is Hermitian, $\mu(A)$ is the expectation value of A. We does not take this approach because we want to focus only on probability.

- The set of events consists of all projections. This set includes the empty projection, projection operators $|\psi\rangle\langle\psi|$ for each state $|\psi\rangle$, sums of *orthogonal* projections, and products of *commuting* projections;
- $\mu(\mathbb{1}) = 1$, and
- for mutually orthogonal projections E_i, we have $\mu\left(\sum_i E_i\right) = \sum_i \mu\left(E_i\right)$.

□

2.1 Quantum Probability Measures

For a given set of events $\mathcal{E}$, there are many possible probability measures $\mu : \mathcal{E} \to [0, 1]$. The Born rule, a postulate of quantum mechanics, states that each quantum state $|\phi\rangle$ induces a probability measure μ_ϕ as follows:

$$\mu_\phi(E) = \langle\phi|E\phi\rangle$$

Conversely, Gleason's theorem states that given a probability measure μ, there exist a quantum state $|\phi\rangle$ that induces such a measure using the Born rule. The theorem is only valid in Hilbert spaces with dimension $d \geq 3$. It is instructive to study counterexamples in $d = 2$, i.e., the case of a one-qubit system. Consider five states $|\psi_0\rangle$ to $|\psi_4\rangle$ that form five orthogonal bases $\{|\psi_0\rangle, |\psi_1\rangle\}$, $\{|\psi_1\rangle, |\psi_2\rangle\}$, $\{|\psi_2\rangle, |\psi_3\rangle\}$, $\{|\psi_3\rangle, |\psi_4\rangle\}$, and $\{|\psi_4\rangle, |\psi_0\rangle\}$ and consider the probability measure defined as follows. For all $i \in \{0, 1, 2, 3, 4\}$, we have $\mu_X(|\psi_i\rangle\langle\psi_i|) = 1/2$. For each orthogonal basis, the probability is 1 as desired and yet it is impossible to find a single quantum state that realizes such a probability measure (see `http://tph.tuwien.ac.at/~svozil/publ/2006-gleason.pdf`)

Amr says: the rest needs cleaning up and perhaps does not even belong in this section

Although it seems that we need an infinite long table to specify the quantum probability measure μ, our μ is actually given by a simple formula $\langle 0|E|0\rangle$. In general, Born discovered each quantum state $|\psi\rangle \in \mathcal{H}\backslash\{0\}$ induces a probability measure $\tilde{\mu}_\psi : \mathcal{E} \to [0,1]$ on the space of events defined for any event $E \in \mathcal{E}$ as follows [4, 13]:

$$\tilde{\mu}_\psi(E) = \frac{\langle\psi|E|\psi\rangle}{\langle\psi|\psi\rangle} \tag{1}$$

The Born rule satisfies the following properties:

- It can be extend to mixed states. Given a mixed state represented by a density matrix $\rho = \sum_{j=1}^N q_j \frac{|\psi_j\rangle\langle\psi_j|}{\langle\psi_j|\psi_j\rangle}$, where $\sum_{j=1}^N q_j = 1$, i.e., $\mathrm{Tr}(\rho) = 1$, then the Born rule can be extended to ρ by

$$\tilde{\mu}_\rho(E) \quad = \quad \mathrm{Tr}(\rho E) = \sum_{j=1}^N q_j \tilde{\mu}_{\Psi_j}(E) \ . \tag{2}$$

  Notice that $\left(\{1,\ldots,N\}, 2^{\{1,\ldots,N\}}, \mu(J) = \sum_{j\in J} q_j\right)$ is a classical probability space. Therefore, when we discretize the Hilbert space later, we may need to discretize this probability space as well.

- $\tilde{\mu}_\rho$ is a probability measure for all mixed state ρ.
- $\langle\psi|\phi\rangle = 0 \Leftrightarrow \tilde{\mu}_\psi(|\phi\rangle\langle\phi|) = 0$.
- $\tilde{\mu}_\psi(E) = \tilde{\mu}_{\mathbf{U}|\psi\rangle}\left(\mathbf{U}E\mathbf{U}^\dagger\right)$,where $\mathbf{U}$ is any unitary map, i.e., $\mathbf{U}^\dagger\mathbf{U} = \mathbb{1}$.

Naturally, we may ask: is every probability measure induced from a state by the Born rule? The answer is yes by Gleason's theorem when the dimension ≥ 3 [6, 14, 16]. Furthermore, a simple corollary of Gleason's theorem can show the Born rule is the unique function satisfying conditions 1. to 3.

Corollary 1. The Born rule is the unique function satisfying conditions 1. to 3.

Proof. Assume there is another function $\tilde{\mu}'$ such that $\tilde{\mu}'_\rho$ is a quantum probability measure for all mixed state ρ. We are going to prove $\tilde{\mu}' = \tilde{\mu}$.

Fix a pure normalized state ϕ, $\tilde{\mu}'_\phi$ is a quantum probability measure by condition 2. By Gleason's theorem, there is a mixed state ρ', such that $\tilde{\mu}'_\phi(E) = \mathrm{Tr}(\rho' E) = \sum_{j=1}^N q_j \tilde{\mu}_{\psi_j}(E)$ for all event E.

Consider the event $E' = \mathbb{1} - |\phi\rangle\langle\phi|$, we have

$$\begin{aligned} 0 \overset{\text{Condition 3}}{=} & \quad \tilde{\mu}_\phi(E') \\ = & \quad \sum_{j=1}^N q_j \tilde{\mu}_{\psi_j}(E') \end{aligned}$$

Because $q_j > 0$, we have $\tilde{\mu}_{\psi_j}(E) = 0$, i.e., ψ_j is orthogonal to a co-dimension-1 subspace E'. However, the only subspace orthogonal to E' is span by $|\phi\rangle$. Hence, $\tilde{\mu}'_\phi = \tilde{\mu}_\phi$. □

Amr says: give example non-commuting events

Yu-Tsung says: Isn't $|0\rangle\langle 0|$ and $|+\rangle\langle +|$ an example in the example of One-qubit quantum probability space.

2.2 Plan

In the remainder of the paper, we consider variations of quantum probability spaces motivated by computation of numerical quantities in a world with limited resources:

- Instead of the Hilbert space $\mathcal{H}$ (constructed over the uncountable and uncomputable complex numbers $\mathbb{C}$), we will consider variants constructed over finite fields [10, 9, 8].
- Instead of real-valued probability measures producing results in the uncountable and uncomputable interval $[0, 1]$, we will consider finite set-valued probability measures [2, 15].

We will then ask if it is possible to construct variants of quantum probability spaces under these conditions. The main question is related to the definition of probability measures: is it possible to still define a probability measure as a function that depends on a single state? Specifically,

- given a state $|\psi\rangle$, is there a probability measure mapping events to probabilities that only depends on $|\psi\rangle$? In the conventional quantum probability space, the answer is yes by the Born rule [4, 13] and the map is given by: $E \mapsto \langle\psi|E\psi\rangle$.
- given a probability measure μ mapping each event E to a probability, is there a *unique* state ψ such that $\mu(E) = \langle\psi|E\psi\rangle$? In the conventional case, the answer is yes by Gleason's theorem [6, 14, 16].

3 All Continuous or All Discrete

Before we turn to the main part of the paper, we quickly dismiss the possibility of having one but not the other of the discrete variations. Specifically, it is impossible to maintain the Hilbert space and have a finite set-valued probability measure and it is also impossible to have a vector space constructed over a finite field with a real-valued probability measure.

3.1 Hilbert Space with Finite Set-Valued Probability Measure

However, there is a $\mathscr{L}_2$-valued probability measure

$$\hat{\mu}_1(E) = \begin{cases} \textit{impossible} & \text{, if } E = |+\rangle\langle+|; \\ \bar{\mu}(E) & \text{, otherwise.} \end{cases}$$

such that $\hat{\mu}_1 \neq \bar{\mu}_\psi$ for all mixed state $|\psi\rangle$.

3.2 Discrete Vector Space with Real-Valued Probability Measure

References

[1] Samson Abramsky. Big toy models: Representing physical systems as Chu spaces. *CoRR*, abs/0910.2393, 2009.

[2] Zvi Artstein. Set-valued measures. *Transactions of the American Mathematical Society*, 165:103–125, 1972.

[3] Garrett Birkhoff and John Von Neumann. The logic of quantum mechanics. *Annals of mathematics*, pages 823–843, 1936.

[4] Max Born. Zur quantenmechanik der stoßvorgänge (1926). In *Die Deutungen der Quantentheorie*, pages 48–52. Springer, 1984.

[5] William G. Faris. Appendix: Probability in quantum mechanics. In *The infamous boundary : seven decades of controversy in quantum physics*. Boston : Birkhauser, 1995.

[6] Andrew Gleason. Measures on the closed subspaces of a hilbert space. *Indiana Univ. Math. J.*, 6:885–893, 1957.

[7] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley, 1994.

[8] Andrew J Hanson, Gerardo Ortiz, Amr Sabry, and Yu-Tsung Tai. Geometry of discrete quantum computing. *Journal of Physics A: Mathematical and Theoretical*, 46(18):185301, 2013.

[9] Andrew J Hanson, Gerardo Ortiz, Amr Sabry, and Yu-Tsung Tai. Discrete quantum theories. *Journal of Physics A: Mathematical and Theoretical*, 47(11):115305, 2014.

[10] Andrew J Hanson, Gerardo Ortiz, Amr Sabry, and Yu-Tsung Tai. Corrigendum: Geometry of discrete quantum computing. *Journal of Physics A: Mathematical and Theoretical*, 49(3):039501, 2015.

[11] Hans Maassen. Quantum probability and quantum information theory. In *Quantum information, computation and cryptography*, pages 65–108. Springer, 2010.

[12] George W. Mackey. Quantum mechanics and hilbert space. *The American Mathematical Monthly*, 64(8):45–57, 1957.

[13] N. D. Mermin. *Quantum Computer Science*. Cambridge University Press, 2007.

[14] A. Peres. *Quantum Theory: Concepts and Methods*. Fundamental Theories of Physics. Springer, 1995.

[15] Madan L Puri and Dan A Ralescu. Strong law of large numbers with respect to a set-valued probability measure. *The Annals of Probability*, pages 1051–1054, 1983.

[16] Michael Redhead. *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics*. Oxford University Press, 1987.

[17] V.K. Rohatgi and A.K.M.E. Saleh. *An Introduction to Probability and Statistics*. Wiley Series in Probability and Statistics. Wiley, 2011.

[18] Jan Swart. Introduction to quantum probability. *Lecture Notes*, 2013.