Lecture Notes of the Unione Matematica Italiana

Edoardo Ballico
Alessandra Bernardi
Iacopo Carusotto
Sonia Mazzucchi
Valter Moretti *Editors*

Quantum Physics and Geometry

U
M
I
Unione
Matematica
Italiana

Springer

Lecture Notes of
the Unione Matematica Italiana 25

More information about this series at http://www.springer.com/series/7172

Editorial Board

The Editorial Policy can be found
at the back of the volume.

Edoardo Ballico • Alessandra Bernardi •
Iacopo Carusotto • Sonia Mazzucchi • Valter Moretti
Editors

Quantum Physics and Geometry

Springer

Unione
Matematica
Italiana

Editors

Edoardo Ballico
Dipartimento di Matematica
Università di Trento
Trento, Italy

Alessandra Bernardi
Dipartimento di Matematica
Università di Trento
Trento, Italy

Iacopo Carusotto
BEC Center
INO-CNR
Trento, Italy

Sonia Mazzucchi
Dipartimento di Matematica
Università di Trento
Trento, Italy

Valter Moretti
Dipartimento di Matematica
Università di Trento
Trento, Italy

ISSN 1862-9113 ISSN 1862-9121 (electronic)
Lecture Notes of the Unione Matematica Italiana
ISBN 978-3-030-06121-0 ISBN 978-3-030-06122-7 (eBook)
https://doi.org/10.1007/978-3-030-06122-7

Library of Congress Control Number: 2019932799

Mathematics Subject Classification (2010): Primary: 81-XX, Secondary: 14-XX

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Contributors

Edoardo Ballico Dipartimento di Matematica, Università di Trento, Trento, Italy

Alessandra Bernardi Dipartimento di Matematica, Università di Trento, Trento, Italy

Iacopo Carusotto BEC Center, INO-CNR, Trento, Italy

Luca Chiantini Dipartimento di Ingegneria dell’Informazione e Scienze Matematiche, Università di Siena, Siena, Italy

F. M. Ciaglia Sezione INFN di Napoli and Dipartimento di Fisica E. Pancini dell’Universitá Federico II di Napoli, Complesso Universitario di Monte S. Angelo, Naples, Italy

Frédéric Holweck Laboratoire Interdisciplinaire Carnot de Bourgogne, University Bourgogne Franche-Comté, Belfort, France

A. Ibort ICMAT, Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Depto. de Matemáticas, Univ. Carlos III de Madrid, Leganés, Madrid, Spain

Joseph M. Landsberg Department of Mathematics, Texas A&M University, College Station, TX, USA

G. Marmo Sezione INFN di Napoli and Dipartimento di Fisica E. Pancini dell’Universitá Federico II di Napoli, Complesso Universitario di Monte S. Angelo, Naples, Italy

Sonia Mazzucchi Dipartimento di Matematica, Università di Trento, Trento, Italy

Valter Moretti Dipartimento di Matematica, Università di Trento, Trento, Italy

Davide Pastorello Department of Mathematics, University of Trento, Trento Institute for Fundamental Physics and Applications (TIFPA), Povo, Trento, Italy

Bassano Vacchini Dipartimento di Fisica “Aldo Pontremoli”, Università degli Studi di Milano, Milan, Italy

INFN, Sezione di Milano, Milan, Italy

Chapter 1
Introduction

Edoardo Ballico, Alessandra Bernardi, Iacopo Carusotto, Sonia Mazzucchi, and Valter Moretti

The development of quantum mechanics has been one of the greatest scientific achievements of the early twentieth century. In spite of its remarkable success in explaining and predicting an amazing number of properties of our physical world, its interpretation has raised strong controversies among a wide community of scientists and philosophers. One of the hottest points of discussion is the meaning of the so-called quantum entanglement that, for systems of two or many particles, allows in particular the possibility for each particle of the system to be simultaneously located at different spatial positions. Entangled states display a special kind of correlations. Generally speaking, differently from the statistical correlations that are usually found in classical probability theory, quantum entanglement cannot be understood in terms of statistically distributed hidden variables and must involve the possibility for quantum systems of particles to be simultaneously in different single particle pure quantum states. Entangled states therefore present facets of the quantum worlds which are even more complicated than the famous example of a superposition of states in the so-called Schrödinger's cat which is simultaneously classically dead and alive. The peculiar phenomenology of quantum mechanics goes far beyond this paradoxical case: in contrast to the usual chain rules of classical conditional probability, the probability for a physical event to occur in a quantum framework

E. Ballico · A. Bernardi (✉)
Dipartimento di Matematica, Università di Trento, Trento, Italy
e-mail: edoardo.ballico@unitn.it; alessandra.bernardi@unitn.it

I. Carusotto
BEC Center, INO-CNR, Trento, Italy
e-mail: iacopo.carusotto@unitn.it

S. Mazzucchi · V. Moretti
Dipartimento di Matematica, Università di Trento, Trento, Italy
e-mail: sonia.mazzucchi@unitn.it; valter.moretti@unitn.it

E. Ballico et al. (eds.), *Quantum Physics and Geometry*,
Lecture Notes of the Unione Matematica Italiana 25,
https://doi.org/10.1007/978-3-030-06122-7_1

is computed by the interference of the complex-valued amplitudes corresponding to the different classical states. In dynamical processes, these classical positional states are described by paths that the system can follow during its evolution. This description of the physical world is commonly known as Feynman integral and implicitly requires that the system be simultaneously in different classical states at all intermediate times [1]. The mathematical counterpart of this picture is that quantum states of a composite system are described by a tensor product structure where each product entry represents a component of the system. In this picture, entanglement is encoded in quantum superpositions, that is linear combinations of completely decomposed tensors. In this sense, if the tensor product involves different states of a given component which are localized in far and causally separated spatial regions, a single component of the system may be simultaneously located in different places.

While the observable consequences of quantum mechanics have been experimentally explored all along the twentieth century, starting from the discrete energy levels of the hydrogen atom towards superconductivity and superfluidity in quantum condensed matter physics and precision measurements in quantum relativistic particle physics, the most basic and profound features of entanglement and its philosophical consequences have started being investigated only much more recently. A crucial step in this development was the formulation in 1935 of the so-called Einstein-Podolsky-Rosen (EPR) paradox raising doubts on the completeness of the quantum mechanical description of the physical world [2] in view of the existence of entangled states in the formalism of quantum theory and the Luders-von Neumann postulate on the instantaneous collapse of the wavefunction after a measurement procedure. The subsequent derivation in 1964 of the so-called Bell inequalities [3] was the milestone, which offered a quantitative criterion to test quantum mechanics against alternative hidden variable theories satisfying a local realism principle and essentially ruling out entangled states as proposed in the EPR paper. So far, the outcome of all experiments carried out along these lines starting from Aspect's 1982 one on cascaded photon emission [4] has been a strong confirmation of the predictions of quantum mechanics predicting violation of Bell's inequalities and ruling out the local realism principle. In the following years, the experiments have been gradually improved to better deal with various hidden assumptions or loopholes pointed out by various scientists. In 2015, for the first time, the violation of Bell's inequalities was corroborated by an experimental test of Bell's theorem by R. Hanson et al. certifying the absence of any additional assumptions or loophole [5].

In addition to a revolution in our philosophical understanding of the physical world around us, the success of quantum mechanics in describing these amazing features of the microscopic world has then given a dramatic boost into the exploration of their possible use in technological applications, e.g. to the quantum communication and quantum information processing, two new branches of science based on a dramatic change in perspective in logics and computation. As one can easily imagine, this paradigm shift is accompanied by the need of new mathematical and computer science tools for the description and the control of quantum mechanical systems and, more practically, for the full exploitation of the new possibilities opened by entanglement for communication and computation.

This special volume was prepared in the wake of the "International workshop on Quantum Physics and Geometry" organized during July 2017 in Levico Terme (Trento, Italy) (http://www.science.unitn.it/~carusott/QUANTUMGEO17/index.html) on these topics. This event, sponsored by CIRM with the precious support of INDAM, University of Trento, TIFPA-INFN and the INO-CNR BEC Center gathered world specialists in both physical sciences and in mathematics, with the aim of exploring possible interdisciplinary links between quantum information and geometry and contributing to the creation of a community of researchers trying to export advanced mathematical concepts to this new applicative field. The objective was to convey to a single event leading experts from the two fields, so to explore interdisciplinary connections and contribute establishing an active and long-lasting community. On the physics side, a conductive thread of the event has been the characterization of entanglement; on the mathematics one, different tools to describe it from different perspectives have been covered, including tensor decomposition, the classification of the orbit closures of some Lie groups, tensor network representations, and topological properties of the quantum states. The articles that follow give a hint of the rich developments that one may expect to result from this meeting of different worlds. While all contributions present exciting state-of-the-art results, they are also meant to offer a general, mathematics-oriented introduction to quantum science and technologies and to their latest developments.

The first contribution by J.M. Landsberg on "A very brief introduction to quantum computing and quantum information theory for mathematicians" summarizes the PhD course on "Quantum Information and Geometry" that he has given at Trento University with the support of INDAM during the months of June and July 2017 surrounding the Levico workshop. In combination with the recorded lectures that are available under request (https://drive.google.com/open?id=0B2Y1CpIKbFuSR1hVT3BfNmtTSFU), this long article aims at giving a complete coverage of the background material from both physics and computer science. The contribution by D. Pastorello on "Entanglement, CP-maps and quantum communications" reviews basic concepts of quantum mechanics and entanglement and then focuses on the potential of quantum entanglement as a resource in communication systems. The contribution by B. Vacchini on "Frontiers of open quantum system dynamics" presents important developments on the dynamics of quantum systems coupled to environments, which generalize to a wider context the quantum evolution in terms of the well-known Schrödinger equation. Mathematical results on the use of advanced geometrical concepts in quantum information theory are presented in the contribution by F. Holweck on "Geometric constructions over $\mathbb{C}$ and $\mathbb{F}^2$ for Quantum Information", with a special attention to the entanglement of pure multipartite systems and to contextuality issues [6]. In both problems, a central role is played by representation theory, which is respectively used to classify entanglement in terms of the closure diagram of the orbits in tensor spaces and for the description of commutation relations of the generalized N-qubit Pauli group. The contribution by L. Chiantini on "Hilbert functions and tensor analysis" illustrates the power of geometric methods for the decomposition of tensors and, in particular, offers a survey-style introduction to the important problem of the uniqueness of the decomposition (the so called "identifiability"), useful for signal processing and, possibly, for the representation of quantum states of many indistinguishable particles. As a final point, some extension to the famous Kruskal's criterion is proposed. Finally, the contribution by M. Ciaglia, A. Ibort and G. Marmo on "Differential Geometry of Quantum States, Observables and Evolution" summarizes an alternative geometric description of quantum mechanical systems in terms of the Kähler geometry of the space of pure states of a closed quantum system and discusses how the composition of systems and the resulting entanglement can be captured in this new setting.

We hope that this volume will trigger an active interest from the mathematical community towards the exciting challenges that quantum science and technology is raising to scientists of all disciplines.

References

1. R.P. Feynman, *QED: The Strange Theory of Light and Matter* (Princeton University Press, Princeton, 2006)
2. A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935)
3. J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987)
4. A. Aspect, P. Grangier, G. Roger, Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities. Phys. Rev. Lett. **49**, 91 (1982)
5. R. Hanson et al., Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers. Nature **526**, 682 (2015)
6. S. Kochen, E.P. Specker, The problem of hidden variables in quantum mechanics, in *The Logico-Algebraic Approach to Quantum Mechanics* (Springer, Dordrecht, 1975), pp. 293–328

Chapter 2
A Very Brief Introduction to Quantum Computing and Quantum Information Theory for Mathematicians

Joseph M. Landsberg

Abstract This is a very brief introduction to quantum computing and quantum information theory, primarily aimed at geometers. Beyond basic definitions and examples, I emphasize aspects of interest to geometers, especially connections with asymptotic representation theory. Proofs can be found in standard references such as Kitaev et al. (Classical and quantum computation, vol. 47. American Mathematical Society, Providence, 2002) and Nielson and Chuang (Quantum computation and quantum information. Cambridge University Press, Cambridge, 2000) as well as Landsberg (Quantum computation and information: Notes for fall 2017 TAMU class, 2017).

2.1 Overview

I begin, in Sect. 2.2, by presenting the postulates of quantum mechanics as a natural generalization of probability theory. In Sect. 2.3 I describe basic entanglement phenomena of "super dense coding", "teleportation", and Bell's confirmation of the "paradox" proposed by Einstein-Podolsky-Rosen. In Sect. 2.4 I outline aspects of the basic quantum algorithms, emphasizing the geometry involved. Section 2.5 is a detour into classical information theory, which is the basis of its quantum cousin briefly discussed in Sect. 2.7. Before that, in Sect. 2.6, I reformulate quantum theory in terms of density operators, which facilitates the discussion of quantum information theory. Critical to quantum information theory is *von Neumann entropy* and in Sect. 2.8 I elaborate on some of its properties. A generalization of "teleportation" is discussed in Sect. 2.9. Regarding practical computation, the exponential growth in size of $(\mathbb{C}^2)^{\otimes n}$ with n that appears in quantum information theory leads to the notion of "feasible" states discussed in Sect. 2.10, which has interesting algebraic geometry associated to it. I conclude with a discussion of representation-theoretic

J. M. Landsberg (✉)
Department of Mathematics, Texas A&M University, College Station, TX, USA
e-mail: jml@math.tamu.edu

E. Ballico et al. (eds.), *Quantum Physics and Geometry*,
Lecture Notes of the Unione Matematica Italiana 25,
https://doi.org/10.1007/978-3-030-06122-7_2

aspects of quantum information theory, including a discussion of the quantum marginal problem in Sect. 2.11. I do not discuss topological quantum computing, which utilizes the representation theory of the braid group. For those interested in more details from this perspective, see [18].

2.2 Quantum Computation as Generalized Probabilistic Computation

In this section I take the point of view advocated in [1] and other places that quantum computing should be viewed as a natural generalization of probabilistic computing, and more generally that the laws of quantum mechanics as generalizations of the laws of probability.

2.2.1 Classical and Probabilistic Computing via Linear Algebra

This section is inspired by Arora and Barak [2, Exercise 10.4].

Classical communication deals with *bits*, elements of $\{0, 1\}$, which will be convenient to think of as elements of $\mathbb{F}_2$, the field with two elements. Let $f_n : \mathbb{F}_2^n \to \mathbb{F}_2$ be a sequence of functions. Give $\mathbb{R}^2$ basis $\{|0\rangle, |1\rangle\}$ (such notation is standard in quantum mechanics) and give $(\mathbb{R}^2)^{\otimes m} = \mathbb{R}^{2^m}$ basis $\{|I\rangle \mid I \in \{0, 1\}^m\}$. In this way, we may identify $\mathbb{F}_2^m$ with the set of basis vectors of $\mathbb{R}^{2^m}$. A computation of f_n (via an arithmetic or Boolean circuit) may be phrased as a sequence of linear maps on a vector space containing $\mathbb{R}^{2^n}$, where each linear map comes from a pre-fixed set agreed upon in advance. In anticipation of what will come in quantum computation, the pre-fixed set of maps (called *gates* in the literature) will be taken from maps having the following properties:

1. Each linear map must take probability distributions to probability distributions. This implies the matrices are *stochastic*: the entries are non-negative and each column sums to 1.
2. Each linear map only alters a small number of entries. For simplicity assume it alters at most three entries, i.e., it acts on at most $\mathbb{R}^{2^3}$ and is the identity on all other factors in the tensor product.

In quantum computation, the first property will be replaced by requiring the linear maps to be completely positive and trace preserving (see Sect. 2.7). The second is the same and justified because “universal” quantum computing is possible with such maps, even requiring the three factors to be adjacent, which is essentially due to the classical Cartan-Dieudonné theorem.

To facilitate comparison with quantum computation, first restrict to reversible classical computation. The complexity class of a sequence of functions in classical reversible computation is the same as in arbitrary classical computation.

For example, if we want to effect $(x, y) \mapsto x * y$, consider the map

$$|x, y, z\rangle \mapsto |x, y, z \oplus (x * y)\rangle = |x, y, z \oplus (x \wedge y)\rangle \tag{2.1}$$

(where the second expression is for those preferring Boolean notation) and act as the identity on all other basis vectors (sometimes called *registers*). Here z will represent "workspace bits": x, y will come from the input and z will always be set to 0 in the input. In the basis $|000\rangle, |001\rangle, |010\rangle, |100\rangle, |011\rangle, |101\rangle, |110\rangle, |111\rangle$, of $\mathbb{R}^8$, the matrix is

$$\begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix}. \tag{2.2}$$

This gate is sometimes called the *Toffoli gate* and the matrix the *Toffoli matrix*.

The swap (negation) gate $\neg$ is realized by the matrix

$$\sigma_x = \begin{pmatrix} 0&1\\ 1&0 \end{pmatrix}. \tag{2.3}$$

The swap and Toffoli matrices can perform any computation that is accomplished via a sequence of matrices drawn from some finite set of Boolean operations, each acting on a fixed number of basis vectors with at worst a polynomial in n size increase in the number of matrices needed. For those familiar with Boolean circuits, any sequence of Boolean circuits (one for each n) may be replaced by a sequence with just Toffoli and negation gates with at worst a polynomial (in n) blow up in size.

A probability distribution on $\{0, 1\}^m$ may be encoded as a vector in $\mathbb{R}^{2^m}$: If the probability distribution assigns probability p_I to $I \in \{0, 1\}^m$, assign to the distribution the vector $v = \sum_I p_I |I\rangle \in \mathbb{R}^{2^m}$.

The matrices (2.2), (2.3) realize classical computation. To add randomness to enable probabilistic computation, introduce the matrix

$$\begin{pmatrix} \frac{1}{2}&\frac{1}{2}\\ \frac{1}{2}&\frac{1}{2} \end{pmatrix}$$

which acts on a single $\mathbb{R}^2$ corresponding to a fair coin flip. Note that the coin flip matrix is not invertible, which will be one motivation for quantum computation in Sect. 2.2.2. Work in $\mathbb{R}^{2^{n+s+r}}$ where r is the number of times one needs to access a random choice and s is the number of matrices (arithmetic operations) in addition to the coin tosses needed to compute f.

A probabilistic computation, viewed this way, starts with $|x0^{r+s}\rangle$, where $x \in \mathbb{F}_2^n$ is the input. One then applies a sequence of admissible stochastic linear maps to it, and ends with a vector that encodes a probability distribution on $\{0,1\}^{n+s+r}$. One then restricts this to $\{0,1\}^{p(n)}$, that is, one takes the vector and throws away all but the first $p(n)$ entries. This vector encodes a probability sub-distribution, i.e., all coefficients are non-negative and they sum to a number between zero and one. One then renormalizes (dividing each entry by the sum of the entries) to obtain a vector encoding a probability distribution on $\{0,1\}^{p(n)}$ and then outputs the answer according to this distribution. Note that even if our calculation is feasible (i.e., polynomial in size), to write out the original output vector that one truncates would be exponential in cost. A stronger variant of this phenomenon will occur with quantum computing, where the result will be obtained with a polynomial size calculation, but one does not have access to the vector created, even using an exponential amount of computation.

To further prepare for the analogy with quantum computation, define a probabilistic bit (a *pbit*) to be an element of

$$\{p_0|0\rangle + p_1|1\rangle \mid p_j \in [0,1] \text{ and } p_0 + p_1 = 1\} \subset \mathbb{R}^2.$$

Note that the set of pbits (possible states) is a convex set, and the basis vectors are the extremal points of this convex set.

2.2.2 A Wish List

Here is a wish list for how one might want to improve upon the above set-up:

1. Allow more general kinds of linear maps to get more computing power, while keeping the maps easy to compute.
2. Have reversible computation: we saw that classical computation can be made reversible, but the coin flip was not. This property is motivated by physics, where many physical theories require time reversibility.
3. Again motivated by physics, one would like to have a continuous evolution of the probability vector, more precisely, one would like the probability vector to depend on a continuous parameter t such that if $|\psi_{t_1}\rangle = X|\psi_{t_0}\rangle$, then there exist admissible matrices Y, Z such that $|\psi_{t_0+\frac{1}{2}t_1}\rangle = Y|\psi_{t_0}\rangle$ and $|\psi_{t_1}\rangle = Z|\psi_{t_0+\frac{1}{2}t_1}\rangle$ and $X = ZY$. In particular, one wants operators to have square roots. (Physicists sometimes state this as "time evolution being described by a semi-group".)

One way to make the coin flip reversible is, instead of making the probability distribution be determined by the sum of the coefficients, one could take the sum of the squares. If one does this, there is no harm in allowing the entries of the output vectors to become negative, and one could use

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.4}$$

for the coin flip. The matrix H is called the *Hadamard matrix* or *Hadamard gate* in the quantum computing literature. If we make this change, we obtain our second wish, and moreover have many operations be "continuous", because the set of matrices preserving the norm-squared of a real-valued vector is the *orthogonal group* $O(n) = \{A \in Mat_{n\times n} \mid AA^T = \mathrm{Id}\}$. So for example, any rotation has a square root.

However our third property will not be completely satisfied, as the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

which represents a reflection, does not have a square root in $O(2)$.

To have the third wish satisfied, allow vectors with *complex* entries. From now on let $i = \sqrt{-1}$. For a complex number $z = x + iy$ let $\overline{z} = x - iy$ denote its complex conjugate and $|z|^2 = z\overline{z}$ the square of its norm.

So we go from pbits, $\{p|0\rangle + q|1\rangle \mid \ p, q \geq 0 \text{ and } p + q = 1\}$ to *qubits*, the set of which is

$$\{\alpha|0\rangle + \beta|1\rangle \mid \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1\}. \tag{2.5}$$

The set of qubits, considered in terms of real parameters, looks at first like the 3-sphere S^3 in $\mathbb{R}^4 \simeq \mathbb{C}^2$. However, the probability distributions induced by $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are the same so it is really S^3/S^1 (the Hopf fibration), i.e., the two-sphere S^2. In the quantum literature this is referred to as the *Bloch sphere*. Geometrically, it would be more natural (especially since we have already seen the need to re-normalize in probabilistic computation) to work with projective space $\mathbb{CP}^1 \simeq S^2$ as our space of qubits, instead of a subset of $\mathbb{C}^2$. So the set of qubits is better seen as (2.5) modulo the equivalence $|\psi\rangle \sim e^{i\theta}|\psi\rangle$.

For $v = (v_1, \dots, v_n) \in \mathbb{C}^n$, write $|v|^2 = |v_1|^2 + \cdots + |v_n|^2$. The set of stochastic matrices is now replaced by the unitary group

$$\mathbf{U}(n) := \{A \in Mat_{n\times n}(\mathbb{C}) \mid \ |Av| = |v| \ \forall |v\rangle \in \mathbb{C}^n\}.$$

The unitary group satisfies the third wish on the list: For all $A \in \mathbf{U}(n)$, there exists a matrix $B \in \mathbf{U}(n)$ satisfying $B^2 = A$.

Consider wish 1: it is an open question! However at least our generalized probabilistic computation includes our old probabilistic computation because the matrices (2.2), (2.3), (2.4) are unitary.

An indication that generalized probability may be related to quantum mechanics is that the interference patterns observed in the famous two slit experiments is manifested in generalized probability: one obtains a "random bit" by applying H to $|0\rangle$: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. However, if one applies a second quantum coin flip, one loses the randomness as $H^2 = \mathrm{Id}$ so $H^2|0\rangle = |0\rangle$, which, as pointed out in [1], could be interpreted as a manifestation of interference.

2.2.3 Postulates of Quantum Mechanics and Relevant Linear Algebra

Here are the standard postulates of quantum mechanics and relevant definitions from linear algebra.

P1 Associated to any isolated physical system is a Hilbert space $\mathcal{H}$, called the *state space*. The system is completely described at a given moment by a unit vector $|\psi\rangle \in \mathcal{H}$, called its *state vector*, which is well defined up to a phase $e^{i\theta}$ with $\theta \in \mathbb{R}$. Alternatively one may work in projective space $\mathbb{P}\mathcal{H}$.

Explanations A *Hilbert space* $\mathcal{H}$ is a (complete) complex vector space endowed with a non-degenerate Hermitian inner-product, $h : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$, where by definition h is linear in the first factor and conjugate linear in the second, $h(|v\rangle, |w\rangle) = \overline{h(|w\rangle, |v\rangle)}$ for all v, w, and $h(|v\rangle, |v\rangle) > 0$ for all $|v\rangle \neq 0$.

The Hermitian inner-product h allows an identification of $\mathcal{H}$ with $\mathcal{H}^*$ by $|w\rangle \mapsto \langle w| := h(\cdot, |w\rangle)$. This identification will be used repeatedly. Write $h(|v\rangle, |w\rangle) = \langle w|v\rangle$ and $|v| = \sqrt{\langle v|v\rangle}$ for the *length* of $|v\rangle$.

If $\mathcal{H} = \mathbb{C}^n$ with its standard basis, where $|v\rangle = (v_1, \dots, v_n)$, the *standard Hermitian inner-product* on $\mathbb{C}^n$ is $\langle w|v\rangle = \sum_{j=1}^n \overline{w}_j v_j$. I will always assume $\mathbb{C}^n$ is equipped with its standard Hermitian inner-product.

Remark 2.2.1 When studying quantum mechanics in general, one needs to allow infinite dimensional Hilbert spaces, but in the case of quantum computing, one restricts to finite dimensional Hilbert spaces, usually $(\mathbb{C}^2)^{\otimes N}$.

P2 The state of an isolated system evolves with time according to the *Schrödinger equation*

$$i\hbar \frac{d|\psi\rangle}{dt} = X|\psi\rangle$$

where $\hbar$ is a constant (*Planck's constant*) and X is a fixed *Hermitian operator*, called the *Hamiltonian* of the system. (Physicists, enamored of the letter H, often also use it to denote the Hamiltonian.) Here, recall that the *adjoint* of an operator $X \in \mathrm{End}(\mathcal{H})$, is the operator $X^\dagger \in \mathrm{End}(\mathcal{H})$ such that $\langle X^\dagger v|w\rangle = \langle v|Xw\rangle$ for all $v, w \in \mathcal{H}$ and X is *Hermitian* if $X = X^\dagger$. For a general Hilbert space, the Unitary group is $\mathbf{U}(\mathcal{H}) := \{U \in \mathrm{End}(\mathcal{H}) \mid |Uv| = |v| \ \forall |v\rangle \in \mathcal{H}\}$.

How is generalized probability related to Schrödinger's equation? Let $U(t) \subset \mathbf{U}(\mathcal{H})$ be a smooth curve with $U(0) = \mathrm{Id}$. Write $U'(0) = \frac{d}{dt}|_{t=0}U(t)$. Consider

$$\begin{aligned} 0 &= \frac{d}{dt}|_{t=0}\langle v|w\rangle \\ &= \frac{d}{dt}|_{t=0}\langle U(t)v|U(t)w\rangle \\ &= \langle U'(0)v|w\rangle + \langle v|U'(0)w\rangle. \end{aligned}$$

Thus $iU'(0)$ is Hermitian. We are almost at Schrödinger's equation. Let $\mathfrak{u}(\mathcal{H}) = T_{\mathrm{Id}}\mathbf{U}(\mathcal{H})$ denote the Lie algebra of $\mathbf{U}(\mathcal{H})$ so $i\mathfrak{u}(\mathcal{H})$ is the space of Hermitian endomorphisms. For $X \in \mathrm{End}(\mathcal{H})$, write $X^k \in \mathrm{End}(\mathcal{H})$ for $X \cdots X$ applied k times. Write $e^X := \sum_{k=0}^{\infty} \frac{1}{k!}X^k$. If X is Hermitian, then $e^{iX} \in \mathbf{U}(\mathcal{H})$. Postulate 2 implies the system will evolve unitarily, by (assuming one starts at $t = 0$), $|\psi_t\rangle = U(t)|\psi_0\rangle$, where

$$U(t) = e^{\frac{-itX}{\hbar}}.$$

Measurements Our first two postulates dealt with isolated systems. In reality, no system is isolated and the whole universe is modeled by one enormous Hilbert space. In practice, parts of the system are sufficiently isolated that they can be treated as isolated systems. However, they are occasionally acted upon by the outside world, and one needs a way to describe this outside interference. For our purposes, the isolated systems will be the Hilbert space attached to the input in a quantum algorithm and the outside interference will be the measurement at the end. That is, after a sequence of unitary operations one obtains a vector $|\psi\rangle = \sum z_j|j\rangle$ (here implicitly assuming the Hilbert space is of countable dimension), and as in generalized probability:

P3 The probability of obtaining outcome j under a measurement is $|z_j|^2$.

In Sect. 2.6, motivated again by probability, **P1, P3** will be generalized to new postulates that give rise to the same theory, but are more convenient to work with in information theory.

A typical situation in quantum mechanics and quantum computing is that there are two or more isolated systems, say $\mathcal{H}_A, \mathcal{H}_B$ that are brought together (i.e., allowed to interact with each other) to form a larger isolated system $\mathcal{H}_{AB}$. The larger system is called the *composite system*. In classical probability, the composite space is $\{0, 1\}^{N_A} \times \{0, 1\}^{N_B}$. In our generalized probability, the composite space is $(\mathbb{C}^2)^{\otimes N_A} \otimes (\mathbb{C}^2)^{\otimes N_B} = (\mathbb{C}^2)^{\otimes(N_A+N_B)}$: