Value indefiniteness, randomness and unpredictability in quantum foundations

Alastair Avery Abbott

Thèse de Doctorat

en cotutelle entre

l'École Normale Supérieure, France, et l'University of Auckland, Nouvelle-Zélande

En vue de l'obtention des grades de

Docteur de l'École Normale Supérieure et
Doctor of Philosophy, University of Auckland

École doctorale 540 : Transdisciplinaire Lettres/Sciences

Specialité : Informatique

Presentée et soutenue le 13 novembre 2015 par

Alastair Avery ABBOTT

De la Valeur Indéfinie aux Notions d'Aléatoire et d'Imprévisibilité Quantiques

Value Indefiniteness, Randomness and Unpredictability
in Quantum Foundations

Centre Cavaillès, USR 3608, CNRS, Collège de France et École Normale Supérieure
Department of Computer Science, University of Auckland

Thèse dirigée par	Cristian S. CALUDE	University of Auckland
	Giuseppe LONGO	CNRS & École Normale Supérieure
Membres du jury		
Présidente :	Misha KAVKA	University of Auckland
Rapporteur :	Gregg JAEGER	Boston University
Membre :	Michael J. DINNEEN	University of Auckland
Directeurs :	Cristian S. CALUDE	University of Auckland
	Giuseppe LONGO	CNRS & École Normale Supérieure

Numéro identifiant de la Thèse : 104900

Abstract

The outcomes of quantum measurements are generally considered to be random, but despite the fact that this randomness is an important element in quantum information theory, its nature is not well understood. In this thesis, we study several issues relating to the origin and certification of quantum randomness and unpredictability.

One of the key results in forming our understanding of quantum mechanics as an intrinsically indeterministic theory is the Kochen-Specker theorem, which shows the impossibility to consistently assign simultaneous noncontextual definite values to all quantum mechanical observables prior to measurement. However, the theorem, under the assumption that any definite values must be noncontextual, only strictly shows that some observables must be value indefinite. We strengthen this result, proving a stronger variant of the Kochen-Specker theorem showing that, under the same assumption, if a system is prepared in an arbitrary state $|\psi\rangle$, then every observable A is value indefinite unless $|\psi\rangle$ is an eigenstate of A.

The indeterministic nature of quantum measurements does little to explain how the quality of quantum randomness differs from classical randomness. We show that, subject to certain physical assumptions, a sequence of bits generated by the measurement of value indefinite observables is guaranteed, in the infinite limit, to be strongly incomputable. We further discuss how this can be used to build a quantum random number generator certified by value indefiniteness.

Next, we study the notion of unpredictability, which is central to the concept of (quantum) randomness. In doing so, we propose a formal model of prediction that can be used to asses the predictability of arbitrary physical experiments. We investigate how the quantum features of value indefiniteness and complementarity can be used to certify different levels of unpredictability, and show that the outcome of a single measurement of a value indefinite quantum observable is formally unpredictable. Finally, we study the relation between this notion of unpredictability and the computability-theoretic certification of quantum randomness.

Keywords: Quantum foundations, quantum randomness, quantum indeterminism, unpredictability, value indefiniteness, quantum measurement

Résumé

Les résultats de mesures quantiques sont généralement considérés comme aléatoires, mais leur nature aléatoire, malgré son importance dans la théorie de l'information quantique, est mal comprise. Dans cette thèse, nous étudions plusieurs problèmes liés à l'origine et la certification de l'aléatoire et l'imprévisibilité quantique.

L'un des résultats clés dans la formation de notre compréhension de la mécanique quantique comme théorie intrinsèquement indéterministe est le théorème de Kochen et Specker, qui démontre l'impossibilité d'attribuer simultanément, de façon cohérente, des valeurs définies et non-contextuelles à chaque observable avant la mesure. Cependant, si nous présumons qu'une observable à valeur définie doit être non-contextuelle, alors le théorème ne montre que le fait qu'il existe au moins une observable à valeur indéfinie. Nous renforçons ce résultat en démontrant une variante du théorème de Kochen et Specker qui montre que si un système est préparé dans un état quelconque $|\psi\rangle$, alors chaque observable A est à valeur indéfinie sauf si $|\psi\rangle$ est un état propre de A.

La nature indéterministe de la mesure quantique n'explique pas bien la différence de qualité entre l'aléatoire quantique et classique. Soumise à certaines hypothèses physiques, nous montrons qu'une suite de bits produite par la mesure des observables à valeurs indéfinies est garantie, dans la limite infinie, d'être fortement incalculable. De plus, nous discutons comment utiliser ces résultats afin de construire un générateur quantique de nombres aléatoires qui est certifié par des observables à valeurs indéfinies.

Dans la dernière partie de cette thèse, nous étudions la notion d'imprévisibilité, qui est au cœur du concept d'aléatoire (quantique). Ce faisant, nous proposons un modèle formel de (im)prévisibilité qui peut servir à évaluer la prévisibilité d'expériences physiques arbitraires. Ce modèle est appliqué aux mesures quantiques afin de comprendre comment la valeur indéfinie et la complémentarité quantique peuvent être utilisées pour certifier différents degrés d'imprévisibilité, et nous démontrons ainsi que le résultat d'une seule mesure d'une observable à valeur indéfinie est formellement imprévisible. Enfin, nous étudions la relation entre cette notion d'imprévisibilité et la certification de l'incalculabilité des suites aléatoires quantiques.

Mots-clés : Fondements de la mécanique quantique, aléatoire quantique, indéterminisme quantique, imprévisibilité, la valeur indéfinie, mesure quantique

For my father, Ken Abbott, with love

Acknowledgements

First and foremost I would like to thank my supervisors Cristian Calude and Giuseppe Longo for their support and enthusiasm. Their guidance and ongoing collaboration have been immensely important to me, and it had been a pleasure to work with them both over the last few years.

Secondly, I would like to thank Karl Svozil for his fruitful and continuing collaboration on many of the topics that have contributed to this thesis. I am grateful to the Technical University of Vienna for its hospitality during my visits to Vienna to work with Karl.

I would also like to thank Laurent Bienvenu, Thierry Paul and Gabriel Senno for many insightful discussions on quantum randomness.

I would like to thank Michael Reck for providing the Mathematica code to generate generalised beamsplitter setups from an arbitrary unitary transformations used to help generate the decomposition for Section 5.4.3.

I gratefully acknowledge the support of a University of Auckland Doctoral Scholarship for funding my doctoral studies, as well as the Marie Curie FP7-PEOPLE-2010-IRSES Grant RANPHYS for helping to fund the travel between my two cotutelle institutions.

I would like to thank Tania Roblot for proof-reading my thesis, and in particular the French portions of it, with a careful eye.

Last but not least, I would like to thank my mother, Marylin Avery, and my partner, Evgeniia Bychina, for their ongoing support, love and patience; without them, it would not have been possible to undertake such an endeavour. I am also eternally grateful to my father, Ken Abbott, who passed away shortly before I started my PhD and to whom this thesis is dedicated; I cannot understate his inspiration and support in encouraging me to pursue the things that I enjoy.

Contents

List of tables

List of figures

Résumé long en français

L'étude des fondements de la mécanique quantique joue un rôle important dans l'effort de comprendre la description quantique de la réalité physique, et de plus les différences entre cette description et celle offerte par la physique classique. Des développements dans ce domaine ont contribué à la poussée d'intérêt pour l'information quantique ces dernières décennies qui, à son tour, a conduit aux développements et même aux implémentations des systèmes cryptographiques quantiques et des générateurs quantiques de nombres aléatoires [56].

Au cœur de ces applications reste la nature aléatoire des mesures quantiques, et, en particulier, la croyance que ces mesures donnent des résultats intrinsèquement, même « vraiment », aléatoire d'une façon inatteignable en physique classique [8]. L'étude de ce caractère aléatoire implique non seulement l'usage des outils de la logique quantique et de l'informatique, mais également l'analyse philosophique pour le comprendre.

Cependant, le concept d'aléatoire est un concept assez subtil, et ni son origine, ni son degré n'est bien étudié ou compris. L'origine de l'aléatoire quantique est souvent réduite à l'indéterminisme des mesures quantiques, pour lequel les théorèmes de Bell [14] et de Kochen et Specker [80] offrent évidence, même s'ils ne parviennent pas à le garantir complètement. Pourtant, il ne faut pas confondre les concepts d'aléatoire et d'indéterminisme, car, bien qu'ils soient liés, ce sont néanmoins des concepts distincts. Pour obtenir une compréhension plus complète de l'aléatoire quantique, il faut donc mieux comprendre la relation entre l'indéterminisme, l'imprévisibilité, et l'aléatoire avec l'aide de modèles et d'outils formels.

Cette thèse peut être divisée en trois parties principales, dont chacune s'adresse, à son tour, à l'un de ces concepts. En entreprenant ce travail, nous utilisons pas seulement le cadre formel standard de la logique quantique et sa structure d'événements, qui nous permet de formaliser l'indéterminisme comme le concept de la valeur indéfinie, mais également les théories de calculabilité et d'information algorithmique. Ces théories nous fournissent des outils mathématiques qui sont essentiels afin de formaliser les notions d'aléatoire et d'imprévisibilité. En particulier, la théorie d'information algorithmique

donne une notion rigoureuse d'aléatoire comme l'absence de structure effective, alors que la calculabilité est indispensable pour formaliser la prévisibilité, vu que « prédire » signifie *dire*, de manière effective, *en avance*.

Dans la première partie (les Chapitres 3 et 4) nous nous intéressons à l'indéterminisme quantique, que nous formalisons dans le cadre formel de la logique quantique comme la notion de la valeur indéfinie. Alors que le théorème de Kochen et Specker ne montre que le fait qu'il existe au moins une observable à valeur indéfinie, nous renforçons ce résultat en démontrant une variante de ce théorème qui montre que si un système est préparé dans un état arbitraire $|\psi\rangle$, alors chaque observable A est à valeur indéfinie sauf si $|\psi\rangle$ est un état propre de A. Ainsi nous montrons que presque toute observable quantique est à valeur indéfinie.

Dans la deuxième partie (le Chapitre 5) nous nous tournons vers l'aléatoire quantique, ainsi que des concepts philosophiques d'aléatoire, y compris l'aléatoire algorithmique. Enfin, soumise à certaines hypothèses physiques, nous montrons qu'une suite de bits produite par la mesure des observables à valeurs indéfinies est garantie, dans la limite infinie, d'être fortement incalculable. De plus, nous proposons un générateur quantique de nombres aléatoire qui est certifié par la valeur indéfinie.

Dans la dernière partie (les Chapitres 6 et 7) nous considérons le concept d'imprévisibilité. Après avoir discuté des notions existantes d'imprévisibilité en physique classique et en théorie de l'information algorithmique, nous proposons un modèle formel général de (im)prévisibilité qui peut servir à évaluer la prévisibilité d'expériences physiques arbitraires. Ce modèle est appliqué aux mesures quantiques afin de comprendre comment la valeur indéfinie et la complémentarité quantique peuvent être utilisées pour certifier différents degrés d'imprévisibilité, et nous démontrons ainsi que le résultat d'une seule mesure d'une observable à valeur indéfinie est formellement imprévisible. Enfin, nous étudions la relation entre cette notion d'imprévisibilité et la certification de l'incalculabilité des suites aléatoire quantiques.

Dans ce long résumé, nous abordons ces trois parties à la suite. Nous résumons la motivation et le contexte de nos résultats dans ces trois parties, avant de présenter et discuter nos contributions liées à ces résultats.

Le travail de cette thèse a mené aux publications [3–7], dont deux sont publiées dans « Physical Review A », tandis que les autres sont actuellement sous considération dans d'autres revues.

Le théorème de Kochen et Specker et la valeur indéfinie

L'interprétation prédominante de la mécanique quantique est que le processus de mesure est intrinsèquement indéterministe [41]. De plus, cet indéterminisme semble être central à l'idée que les résultats des mesures quantiques, au contraire des systèmes classiques, sont « vraiment aléatoire » [8] et « intrinsèquement imprévisible » [139].

L'origine de ce point de vue se trouve à *la règle de Born*, qui donne la probabilité d'obtenir chaque résultat lors de la mesure d'une observable quantique. Alors que les éléments principaux de la mécanique quantique – les états, les dynamiques, les interactions, et même les propriétés observables – sont décrits dans le cadre formel d'un espace de Hilbert, la règle de Born associe, de plus, une distribution de probabilité à ce cadre. La probabilité peut être interprétée de plusieurs manières selon la situation physique ; il ne s'agit que d'un outil formel sans aucun sens physique intrinsèque [69, 117]. En particulier, elle peut représenter un manque épistémique d'information au lieu d'une propension objective.

Max Born fut le premier à prétendre, au contraire de la situation en physique classique, que la probabilité donnée par sa règle en mécanique quantique doit être comprise comme une probabilité objective [21]. Cependant, cette proposition de Born était largement une « inclination », alors pourquoi devrions-nous accepter un tel départ du déterminisme classique ? Einstein n'était bien pas convaincu, et, avec Podolsky et Rosen, en arguant que la mécanique quantique est incomplète, démontrèrent que la formalisme quantique implique le comportement non-local des états quantiques [51].

Alors que l'interprétation indéterministe devint généralement acceptée, ce ne fut pas jusqu'à l'apparition du théorème de Bell aux années soixante que nous avons eu un premier résultat formel sur la non-classicalité de la mesure quantique. En donnant ses célèbres inégalités sur les limites des corrélations disponibles dans les théories à variables cachées non-locales, mais qui sont violées par la mécanique quantique, Bell démontra l'incapacité d'expliquer les mesures quantiques avec une théorie déterministe non-locale [14]. Néanmoins, ceci n'assure pas définitivement que la mesure quantique soit indéterministe : il existe bien des interprétations de la mécanique quantique qui sont déterministes, mais non-locales [20]. Au mieux, le théorème de Bell nous permet de réduire l'indéterminisme quantique à la supposition que n'importe quel déterminisme physique soit local.

Le théorème de Kochen et Specker

Le théorème de Kochen et Specker fut démontré peu après celui de Bell, et, contrairement au théorème de Bell, s'exprime au niveau du cadre de la logique quantique. Il montre l'impossibilité d'associer une valeur définie et non-contextuelle (qui représente le résultat d'une mesure) à chaque observable quantique d'une façon cohérente [80]. Il s'agit, plus précisément, d'une contradiction entre les trois hypothèses suivantes :

(i) chaque observable a une valeur définie qui détermine, en avance, le résultat de sa mesure ;

(ii) la valeur définie associée à une observable devrait être non-contextuelle, c'est-à-dire indépendante des autres observables compatibles qui peuvent être mesurée simultanément avec celle-ci ;

(iii) les résultats d'une mesure (et donc aussi les valeurs définies) d'un ensemble d'observables compatibles doivent être cohérents avec les relations quantiques entre les observables dans cet ensemble.

La troisième condition est largement acceptée, puisqu'elle assure que les valeurs définies ne peuvent pas donner lieu aux observations qui ne sont pas en accord avec la mécanique quantique. Il faut donc abandonner soit la (i), soit la (ii), ou même les deux. Bien qu'ils existent des interprétations à valeurs définies contextuelles – les interprétations déterministes non-locales mentionnées ci-dessus se trouvent dans cette catégorie – qui donc choisissent d'abandonner la (ii), l'interprétation standard est qu'il faut rejeter la (i) et accepter le fait que la réalité quantique soit indéterministe.

Nous discuterons davantage la motivation pour rejeter la (i) au lieu de la (ii) dans la Section 4.4.3, mais permettons-nous d'explorer les conséquences d'insister sur la (i). Il existe, dans ce cas, un fossé entre l'interprétation habituelle du théorème et la conclusion formelle : la négation de la (i) est précisément qu'il existe au moins une observable à valeur indéfinie, alors qu'il est souvent pris d'impliquer l'absence complète des valeurs indéfinies. De plus, on ne peut pas dire quelles observables sont à valeurs indéfinies.

Dans le reste de cette partie de la thèse, nous entreprenons de fermer ce fossé et de démontrer que toute observable ne correspondant pas au « contexte de préparation du système » est à valeur indéfinie.

Un cadre formel de la valeur indéfinie

En visant à localiser la valeur indéfinie, nous concevons dans la Section 3.2 un cadre formel de la valeur (in)définie et de la contextualité. Comme dans les présentations normales du théorème de Kochen et Specker en logique quantique, la base de ce cadre

est celle des observables qui sont des projecteurs sur des états quantiques – qui, à leur tour, sont représentés comme vecteurs unitaires dans un espace de Hilbert. Dorénavant, quand nous parlons d'observables, il sera entendu que nous parlons implicitement de tels projecteurs.

Nous formalisons la notion d'une *fonction à attribution de valeurs*, qui attribue, à chaque observable dans un ensemble donné, une valeur qui peut aussi dépendre du contexte des observables (c'est-à-dire, le sous-ensemble d'observables compatibles). En permettant à cette fonction d'être partielle (c'est-à-dire non-définies sur certaines observables), contrairement aux autres cadres standards, nous pouvons formaliser des notions plus progressives de la contextualité et de la valeur indéfinie, ce qui est nécessaire afin de localiser la valeur indéfinie. Nous appelons *non-contextuelle* une telle fonction qui attribue une seule valeur à chaque observable définie dans chaque contexte qui la contient. Enfin, nous définissons la notion d'*admissibilité* d'une fonction à attribution de valeurs, qui signifie qu'elle satisfait, dans chaque contexte, aux relations quantiques entre les observables *qui sont à valeur définie* dans le contexte.

Avant d'aborder l'issue d'établir l'étendue de la valeur indéfinie dans les systèmes quantiques, il est utile de se demander si nous pouvons tout d'abord établir des limites sur le degré de la contradiction entre la valeur définie et la non-contextualité identifiée par le théorème de Kochen et Specker. Par exemple, est-il possible de montrer que la non-contextualité ou la valeur définie d'une seule observable mène à une contradiction ? Nous apportons une réponse négative dans la Section 3.4 en démontrant, dans le Théorème 30, que pour tout ensemble des observables il existe une fonction admissible à attribution de valeurs qui attribue à une observable une valeur définie et non-contextuelle.

Ce résultat met une limite importante sur l'étendue possible de la valeur indéfinie et la non-contextualité, et en conséquence nous ne pouvons pas espérer de démontrer que toute observable quantique est à valeur indéfinie et donc indéterministe. Cependant, ce ne devrait pas être surprenant voyant que, donné un système quantique préparé dans un état $|\psi\rangle$ arbitraire, la règle de Born stipule qu'une mesure de l'observable P_ψ qui projet sur cet état devrait donner le résultat '1' avec probabilité un, non-contextuellement. Ainsi, il n'est pas déraisonnable de postuler que, dans n'importe quel système il existe une telle observable qui est à valeur définie et non-contextuelle. De plus, cette *hypothèse d'état propre*, comme nous l'appelons, jouera un rôle important dans ce qui suit.

La localisation de la valeur indéfinie

Habituellement, les démonstrations du théorème de Kochen et Specker présentent un ensemble fini des observables et démontrent qu'il n'existe pas de fonction admissible à valeur définie et non-contextuelle sur cet ensemble. La démonstration de Kochen et

Specker donnèrent un tel ensemble de 117 observables [80], et bien que, depuis lors, beaucoup d'effort fût consacré à trouver des ensembles plus petits [27, 103], ces efforts ne changèrent pas le fait que le théorème ne montre que l'existence des observables à valeurs indéfinies, mais pas l'étendue de la valeur indéfinie.

En donnant une démonstration constructive du théorème du Gleason [62], Pitowsky [106] (et aussi avec Hrushovski [75]) montra un principe dit « le principe d'indétermination logique » qui montre l'impossibilité d'attribuer, d'une façon cohérente, la valeur 1, non-contextuellement à deux observables, un résultat bien plus fort que le théorème de Kochen et Specker. Cependant, en le montrant, ils supposent toujours que chaque observable soit à valeur définie, et donc, comme nous discutons en détail dans la Section 4.1, nous ne pouvons pas en tirer un résultat sur l'étendue de la valeur indéfinie.

Afin de progresser dans cette direction, il faut ainsi utiliser la notion plus nuancée d'une fonction partielle à attribution de valeurs que nous définissons. Ceci est tout à fait la voie que nous prenons : au lieu de supposer que chaque observable soit à valeur définie, nous déduisons qu'une observable est à valeur définie seulement quand elle l'est requise par l'admissibilité de la fonction et les valeurs des autres observables à valeurs définies qui sont compatibles avec celle-là.

Ayant conçu le cadre formel pour aborder la localisation de la valeur indéfinie, nous procédons, dans la Section 4.3, à présenter notre principale contribution à cette partie de la thèse. Dans le Théorème 34 nous démontrons le résultat suivant :

Soit $|\psi\rangle, |\phi\rangle$ deux états dans un espace de Hilbert de dimension supérieure ou égale à trois avec $0 < |\langle\psi|\phi\rangle| < 1$, et donc pour lesquels les projecteurs sur ces états, P_ψ et P_ϕ, sont incompatibles. Alors on peut trouver effectivement un ensemble des observables, dont P_ψ, P_ϕ, sur lequel il n'existe pas de fonction admissible à attribution de valeurs non-contextuelles qui attribue la valeur 1 à P_ψ et une valeur définie à P_ϕ.

Ce résultat montre qu'il n'est possible d'attribuer la valeur 1, non-contextuellement, qu'à une seule observable sur un système quantique. Nous démontrons ce théorème en trois étapes principales :

1. Tout d'abord nous le démontrons pour le cas spécial de $|\langle\psi|\phi\rangle| = \frac{1}{\sqrt{2}}$ dans le Lemme 35, ce qui implique donner un ensemble explicit avec les propriétés désirées.

2. Nous démontrons, dans le Lemme 36, une réduction entre le cas de $0 < |\langle\psi|\phi\rangle| < \frac{1}{\sqrt{2}}$ et le premier cas.

3. Enfin, dans ce qui est la partie la plus difficile de cette démonstration, nous donnons une réduction dans la direction opposée pour le dernier cas de $\frac{1}{\sqrt{2}} < |\langle\psi|\phi\rangle| < 1$. Afin de la démontrer, nous montrons deux Lemmes : le Lemme 39, qui diminue

le produit $|\langle\psi|\phi\rangle|$ par un petit montant, et le Lemme 40, qui applique par itération ce premier lemme jusqu'à ce que le résultat désiré soit obtenu.

Contrairement aux démonstrations du théorème de Kochen et Specker qui donnent un ensemble fini montrant la contradiction entre la valeur définie et la non-contextualité, le fait que les deux observables P_ψ et P_ϕ doivent être contenues dans l'ensemble construit nous force à donner pas un seul ensemble fini, mais une procédure effective pour obtenir un tel ensemble fini. En outre, le besoin de satisfaire la condition faible d'admissibilité de la fonction à attribution de valeurs requit que les observables dans l'ensemble soient soigneusement connectées, ce qui explique l'usage des réductions et des itérations compliquées dans les démonstrations des lemmes.

Interprétation physique

Le résultat du Théorème 34, tout comme le théorème de Kochen et Specker, est un résultat purement formel dans le cadre de la logique quantique. Bien qu'il mène à une interprétation physique naturelle en associant les valeurs définies d'observables avec les résultats de leurs mesures, il faut être prudent d'en tirer de telles conclusions sans considérer soigneusement les suppositions physiques qui sont implicites dans ce raisonnement. Nous nous occupons, dans la Section 4.4, de ce problème.

Premièrement, il y a une supposition liée au rôle des mesures qui est normalement gardée implicite lors d'une interprétation d'une théorie à variables cachées. Plus spécifiquement, il faut supposer qu'une mesure physique donne un résultat unique et significatif. Cela peut sembler évident, mais ce n'est pas le cas dans quelques interprétations de la mécanique quantique, comme la théorie des mondes multiples d'Everett [54], et il est donc important d'expliciter cette supposition.

Il faut également faire une connexion entre les valeurs définies par une fonction à attribution de valeurs et la réalisation d'un système quantique. On appelle fidèle (à une réalisation d'un système) toute fonction à attribution de valeurs qui attribue une valeur définie à une observable si et seulement si elle a un résultat physique prédéterminée sur le système.

Deuxièmement, nous considérons la question de « quand pouvons-nous attribuer une valeur définie à une observable ». Einstein, Podolsky et Rosen proposent que, si l'on peut prédire avec certitude le résultat d'une mesure, alors il doit exister une valeur définie avant la mesure [51], un principe que nous appelons le principe d'EPR.

Ce principe nous permet à formuler l'hypothèse d'état propre que nous avons mentionné plus haut, qui affirme qu'un système préparé dans un état $|\psi\rangle$ a une valeur définie pour chaque observable dont $|\psi\rangle$ est un état propre, et plus particulièrement que l'observable P_ψ a la valeur 1. Cette hypothèse est essentielle afin de donner une interprétation

physique au Théorème 34. Le principe d'EPR nous permet également à démontrer, dans le Théorème 44, qu'une fonction fidèle à attribution de valeurs doit être admissible.

Finalement, dans la Section 4.4.3 nous réitérons qu'il faut supposer que les valeurs définies soient non-contextuelles pour interpréter ces résultats comme montrant la valeur indéfinie de la mécanique quantique, et nous exposons quelques arguments à cette fin.

En utilisant ces suppositions, nous montrons dans la Proposition 45 l'interprétation principale du Théorème 34 : si un système quantique est préparé dans un état $|\psi\rangle$, alors chaque observable A dont $|\psi\rangle$ n'est pas un état propre doit être à valeur indéfinie sous n'importe quelle fonction fidèle à attribution de valeurs. Conséquemment, l'ensemble des observables à valeurs indéfinies a la mesure un (pour la mesure de Lebesgue), comme nous le montrons dans le Théorème 46.

Ces résultats, avec l'interprétation que nous venons d'énoncer, sont les principales contributions physiques de cette partie de la thèse. Ils nous permettent de savoir précisément quelles observables sont à valeurs indéfinies, et que presque toute observable est bien à valeur indéfinie, donc fermant le fossé entre le Théorème de Kochen et Specker et l'interprétation courante de la mécanique quantique.

L'aléatoire quantique et l'incalculabilité

Dans la deuxième partie de cette thèse nous nous tournons vers le concept d'aléatoire, et en particulier l'aléatoire quantique du point de vue de la valeur indéfinie que nous avons décrite et montrée dans la première partie. Tout d'abord, nous commençons par analyser des différents concepts philosophiques d'aléatoire dans la Section 5.1.

Des concepts d'aléatoire

Des notions d'aléatoire basées sur le hasard

Depuis longtemps, l'aléatoire a été associée avec les probabilités et l'uniformité, mais, comme nous en avons discuté plus haut, la probabilité n'est qu'un outil mathématique, et peut cacher un déterminisme sous-jacent ou même des structure très régulière qui ne sont pas intuitivement aléatoires. Il semble que cette association est plutôt limitée à la probabilité objective, pour laquelle une distribution de probabilité représente le hasard objectif, et non pas un manque épistémique d'information.

Nous avertissons, pourtant, qu'il ne faut pas confondre l'indéterminisme et le hasard avec l'aléatoire, ce qui s'appelle la « commonplace thesis » [50, 74], et qu'il faut garder ces concepts distincts. Malheureusement, cette identification semble être souvent prise dans la mécanique quantique en déclarant que les mesures quantiques sont aléatoires [8].

Au contraire, la valeur indéfinie ne sert pas, a priori, à garantir que l'on puisse considérer les résultat des mesures quantiques comme aléatoires.

Une approche plus prometteuse est de baser le concept d'aléatoire sur celui d'imprévisibilité. Ceci est exactement l'argumentation que Kofler et Zeilinger [81], et également Fitzsimons et al. [56], donnent pour l'aléatoire quantique, mais ils risquent tous de banaliser cette relation en considérant l'imprévisibilité comme conséquence évidente de l'indéterminisme. Il est plutôt nécessaire de développer une notion plus formelle de l'imprévisibilité pour la considérer comme base d'aléatoire, ce qu'ont fait, par exemple, Eagle [49] et Longo [30], en définissant l'aléatoire comme un type formel d'imprévisibilité. Nous revenons au problème de modélisation d'imprévisibilité dans la dernière partie de cette thèse.

Des notions algorithmiques d'aléatoire

Une notion d'aléatoire existe également dans une forme plus mathématisée dans la théorie de l'information algorithmique. Cette théorie formalise la notion d'aléatoire algorithmique – dite également aléatoire au sens de Martin-Löf – comme une suite de bits qui ne possède aucune structure calculable qui pourrait permettre de la compresser, et est une notion bien acceptée et étudiée.

Un résultat important mais peut-être surprenant est qu'il n'existe pas de suite absolument aléatoire dans le sens que chaque préfix d'une suite a une complexité maximale [47]. Les résultats de la théorie de Ramsey [65] renforcent ce résultat et, ensemble, ils montrent que la notion de l'aléatoire absolue n'a pas de sens mathématique : il n'existe que des degrés d'aléatoires. Alors, il faut se méfier des affirmations que l'aléatoire quantique est absolue et vraie.

L'aléatoire de processus et de produits

Les deux notions d'aléatoire discutées ci-dessus sont à la fois différentes mais complémentaires : la notion basée sur le hasard donne, par l'imprévisibilité, une notion d'aléatoire qui s'applique aux processus physiques, alors que la notion algorithmique s'applique aux résultats des suites d'événements physiques. Cependant, ces notions sont connectées, puisqu'un processus aléatoire (qui suit une probabilité uniforme) produit, avec probabilité un (mais sans certitude !), une suite aléatoire.

En effet, ces deux approches sont valides, et en pratique on voudrait garantir qu'un processus physique soit imprévisible et également qu'il produise une suite aléatoire. Nous proposons donc qu'il faille garder ces deux concepts séparés au lieu d'insister sur une notion d'aléatoire absolue, et évaluer un processus physique par rapport à ces deux formes d'aléatoires séparément.

La bi-immunité des suites quantiques aléatoires

Jusqu'ici, les tentatives d'expliquer l'aléatoire quantique ont généralement été limitées à une notion d'aléatoire de processus, par exemple en la réduisant à l'imprévisibilité. Alors que nous reviendrons à cette approche dans la prochaine partie, nous abordons d'abord, dans la Section 5.2, la possibilité de garantir une forme d'aléatoire algorithmique pour les suites des mesures quantiques.

À première vue, il peut sembler que cette tâche soit futile, puisque une suite de résultats des mesures prises d'une distribution uniforme est aléatoire au sens de Martin-Löf avec probabilité un. Cependant, la probabilité un n'est pas une certitude, et cela nous aiderait à comprendre la force de l'aléatoire quantique et les différences entre elle et l'aléatoire des systèmes classiques.

Bien que nous ne réussissions pas à montrer qu'une telle suite des résultats des mesures quantiques soit aléatoire au sens de Martin-Löf, pour des raisons que nous expliquons, nous démontrons qu'elle est fortement incalculable, plus spécifiquement, bi-immune, et nous montrons donc une différence concrète entre les suites aléatoires classiques et quantiques.

Afin de démontrer ce résultat, qui est notre principale contribution technique dans cette partie de la thèse, comme pour l'interprétation de la valeur indéfinie, nous clarifions et formulons soigneusement les hypothèses physiques dont nous avons besoin. En particulier, nous utilisons une fois de plus le principe d'EPR en formulant *l'hypothèse des éléments calculables de réalité*, qui spécifie une condition de plus sous laquelle nous pouvons déduire l'existence des valeurs définies.

En considérant une expérience où l'on prépare un système quantique, mesure une observable quantique à valeur indéfinie, note le résultat et répète, nous démontrons, dans le Théorème 47, que la suite générée dans la limite infinie par cette expérience est bi-immune. Ce résultat peut également être réduit aux mêmes suppositions que nous avons utilisé plus tôt pour dériver la valeur indéfinie.

Les générateurs quantiques de nombres aléatoires

L'une des applications principales de l'aléatoire quantique est la génération des nombre aléatoires. Plusieurs tels générateurs quantiques de nombres aléatoires ont été proposés [78, 105, 125, 126, 129] et créés [76], qui fonctionnent typiquement par mesurer un photon qui est préparé dans une superposition d'états de polarisation et donc produit un bit qui, avec un peu de chance, est distribué uniformément. Étant donné l'importance de nombres aléatoires dans les systèmes cryptographiques ainsi que, parmi d'autres, dans le modelage statistique, cette application de l'aléatoire quantique est cruciale.

En montrant qu'un tel générateur, s'il fonctionne en mesurant une observable à valeur indéfinie, produit une suite bi-immune dans la limite infinie, nous illustrons une différence conceptuelle concrète entre les générateurs de nombres aléatoires quantiques et classiques, même si cette limite n'est pas disponible en pratique, puisqu'un générateur classique ne peut produire qu'une suite calculable, même cyclique. Cependant, la plupart des propositions actuelles ne fonctionnent que dans un espace de Hilbert de dimension deux, et ne sont donc pas certifiées par la valeur indéfinie du Théorème 34.

Produire une suite certifiée par la valeur définie d'être bi-immune nécessite donc un générateur de nombres aléatoire qui fonctionne dans un espace de Hilbert de dimension supérieure ou égal à trois. Dans la Section 5.4 nous proposons un tel schéma pour un générateur qui fonctionne dans un espace de dimension trois par préparer un système quantique dans un état de spin 0 dans la direction x avant de mesurer l'observable de spin dans la direction z. Cette conception assure que l'on obtient une suite binaire et non pas ternaire, tandis qu'elle est robuste au malalignement, aidant à assurer l'uniformité de la distribution des bits.

Dans la dernière section de cette partie nous proposons une implémentation explicite utilisant des photons et un système généralisé des miroirs semi-réfléchissants (« generalised beamsplitters » en anglais), puisque l'usage des photons permet d'obtenir des débits binaires bien meilleurs qu'il n'est possible avec des atomes et des observables de spin. La suite générée par ce générateur quantique de nombres aléatoires est donc certifiée, toujours soumise aux hypothèses physiques que nous avons élaborées, d'être une suite fortement incalculable, quelque chose qui n'est point possible avec un générateur classique.

L'imprévisibilité des mesures quantiques

Dans la dernière partie de cette thèse, qui consiste des Chapitres 6 et 7, nous revenons à la notion d'imprévisibilité dans le but de créer un modèle formel d'imprévisibilité dans lequel nous pouvons étudier l'imprévisibilité des mesures des observables quantiques à valeurs indéfinies. Nous présentons d'abord certains concepts existants, quoique moins généraux, d'imprévisibilité en physique et mathématique afin de mettre en contexte et motiver notre modèle.

Des notions d'imprévisibilité

Depuis Poincaré, le concept d'imprévisibilité a pris une forme précise en physique classique sous le cadre de dynamiques chaotiques [107, 146], que nous discutons dans la Chapitre 6.

Cette imprévisibilité chaotique se présente, pas en conséquence d'indéterminisme, mais en conséquence de deux faits cruciaux :

1. Mesure : il n'est possible de mesurer qu'une approximation des conditions initiales de l'évolution d'un système ;

2. Sensibilité : les dynamiques chaotiques sont très sensibles aux petites fluctuations des conditions initiales sous le niveau de mesure.

Ces deux points s'interagissent d'une telle façon que l'évolution du système amplifie l'incertitude des conditions initiales au point que le système peut être n'importe où dans l'espace de phase, donc empêchant des prédictions. De plus, un tel système n'est point itérable : lors d'une répétition du système avec la même mesure des conditions initiales, la variation dans cette intervalle de mesure assure que les trajectoires divergent vites [12].

La théorie d'information algorithmique apporte aussi un concept d'imprévisibilité algorithmique qui s'applique aux suites de bits : la bi-immunité. Une suite bi-immune ne peut contenir qu'un nombre fini de bits qui sont calculables, c'est-à-dire prévisibles par un processus effectif. Cependant, comme nous le présentons dans la Section 6.2, une suite bi-immune peut toujours révéler des structures qui sont intuitivement prévisible. Nous considérons donc une notion plus forte, celle d'imprévisibilité au sens de Tadaki qui, comme nous le démontrons, résoudre ces défauts [134]. Bien qu'il soit possible de voir les suites aléatoires au sens de Martin-Löf comme imprévisibles, il nous semble que ceci est trop fort comme concept d'imprévisibilité et que la notion de Tadaki est plus raisonnable. Nous démontrons, dans le Théorème 55, qu'au contraire de la notion des suites aléatoires, la notion d'imprévisibilité au sens de Tadaki ne dépend pas de l'espace de mesure utilisé, et que cette notion représente donc une notion non-probabiliste d'imprévisibilité algorithmique.

Enfin, dans la Section 6.3, nous considérons le concept d'irréductibilité computationnelle, qui essaye de capturer la notion que les dynamiques de certains processus computationnels, et même physiques, ne peuvent pas être calculés plus vite qu'en suivant explicitement leurs dynamiques, et sont donc irréductibles [151, 166]. Nous considérons des diverses tentatives de formaliser ce concept et concluons que, bien que l'irréductibilité computationnelle contienne des éléments importants aux notions d'imprévisibilité, elle manque d'autres éléments essentiels d'imprévisibilité, et devrait être vue plutôt comme une notion d'optimalité de dynamiques.

Des modèles généralisés d'imprévisibilité

Ensuite, nous tournons notre attention aux modèles généraux d'imprévisibilité dans la Section 6.4, au contraire des notions plus spécifiques dont nous avons déjà présenté. Après avoir critiqué de plusieurs tels modèles, plus notablement ceux de Popper [108], Wolpert [153], et du cadre général d'Eagle [49], identifiant au fur et à mesure leurs éléments essentiels ainsi que leurs défauts, nous présentons notre cadre général d'imprévisibilité qui sert de base pour nos contributions dans cette partie.

En visant à formuler un modèle qui est applicable aux expériences physiques arbitraires, notre cadre consiste en les éléments suivants :

1. La spécification, qui doit être finie, d'une expérience dont on doit prédire le résultat.

2. Un agent de prédiction (dit un prédicteur), qui doit prédire le résultat de cette expérience. Nous modélisons cet agent comme une fonction calculable, puisqu'une prédiction doit être un processus *effectif*, un point que nous élaborons davantage.

3. Un extracteur, qui est un appareil physique que l'agent utilise pour extraire uniformément, par mesure, une quantité finie d'information du système qui peut être pertinente pour prédiction, mais qui est tout de même au-dehors de la spécification de l'expérience.

4. Une prédiction qui est faite par l'agent avec accès à un ensemble d'extracteurs.

Selon ce modèle, une expérience est imprévisible s'il existe un prédicteur qui ne fait aucune prédiction incorrecte dans n'importe quelle suite des répétitions infinie de l'expérience, en utilisant l'information extraite, à chaque prédiction, par un seul extracteur. En limitant l'ensemble d'extracteurs disponible au prédicteur, nous pouvons donner également une notion plus relativisée et donc épistémique d'imprévisibilité. Nous considérons plusieurs façons de classifier un tel ensemble d'extracteurs, ainsi qu'un exemple détaillé d'une expérience qui est prévisible en général, mais imprévisible pour un ensemble naturel d'extracteurs à précision de mesure limitée.

Alors que ce modèle a peut-être l'air d'être incompatible avec la notion algorithmique d'imprévisibilité que nous avons présentée, nous expliquons comment nous pouvons lier ces notions en montrant que, dans un cadre limité et relativisé, nous retrouvons la notion d'imprévisibilité au sens de Tadaki.

L'imprévisibilité quantique

Ayant formulé notre modèle d'imprévisibilité, nous l'appliquons aux mesures quantiques dans une tentative de formaliser les affirmations intuitives qu'elles soient intrinsèque-

ment imprévisibles. Ces affirmations prétendent, typiquement, que l'absence d'un résultat prédéterminé pour des mesures des observable à valeur indéfinie (qui sont donc indéterministes) implique tout simplement qu'un agent chargé de prédire le résultat de cette mesure ne peut pas faire mieux que de le deviner aveuglément [81].

Dans ce but, nous considérons une expérience générale, similaire à celle que nous avons considérée dans le contexte des suites bi-immunes et les générateurs quantiques de nombres aléatoires, où une observable à valeur indéfinie est mesurée à plusieurs reprises qui donne, dans la limite, une suite infinie de bits. En utilisant notre modèle, dans le Théorème 65, nous démontrons que cette expérience est bien imprévisible grâce à la valeur indéfinie d'observable mesurée, et qu'aucun bit de cette suite ne peut être prédit avec certitude.

Alors que ce résultat n'est pas tout à fait inattendu donné l'intuition exposée ci-dessus, en le démontrant dans un cadre formel nous précisons le concept et l'origine de l'imprévisibilité quantique qui, comme élaborée dans la deuxième partie de cette thèse, peut être vue comme une forme d'aléatoire de processus. Donc, ce résultat complémente le notre montrant la bi-immunité d'une telle suite et nous aide à comprendre l'aléatoire quantique en gros.

L'imprévisibilité et la complémentarité quantique

Bien que la valeur indéfinie puisse donc garantir l'imprévisibilité des mesures quantiques, les résultats qui nous assurent cette valeur indéfinie (e.g., le Théorème 34) tiennent seulement dans un espace de Hilbert de dimension supérieure ou égale à trois. Cependant, une grande partie des générateurs quantiques de nombres aléatoires fonctionnent dans un espace de Hilbert de dimension deux [125]. Il faut donc se demander s'il est possible d'utiliser d'autres propriétés quantiques afin de certifier l'imprévisibilité.

La complémentarité quantique exprime le fait que les observables non-compatibles ne puissent pas être mesurées simultanément parce qu'elles demandent des installations de mesure incompatibles. Outre le fait qu'il tienne dans tout système quantique, même de dimension deux, ce principe de complémentarité est souvent utilisé comme argument informel pour la valeur indéfinie. Pourtant, il est parfaitement compatible avec la valeur définie, comme le montre certains modèles déterministes de la complémentarité, tel que celui basé sur les automates de Mealy [131].

Dans la Section 7.3 nous précisons ce concept de complémentarité comme une restriction sur l'ensemble des extracteurs qu'un agent de prédiction peut accéder. En utilisant ce formalisme, nous démontrons dans le Théorème 69 qu'une expérience qui mesure à plusieurs reprises une observable complémentaire à celle de la préparation de l'état quantique est imprévisible pour un prédicteur avec accès à un tel ensemble restreint

d'extracteurs. Cela fournit une forme d'imprévisible qui est plus faible et plus épistémique que celle garantie par la valeur indéfinie, mais qui applique aux situations plus générales.

L'incalculabilité et l'imprévisibilité quantique

Vu que la valeur indéfinie implique la bi-immunité ainsi que l'imprévisibilité des mesures quantiques, et considérant aussi la relation entre l'imprévisibilité selon notre modèle formel et l'imprévisibilité au sens de Tadaki que nous avons clarifiée dans la Section 6.6, il est naturel de se demander si cette bi-immunité est une conséquence de l'imprévisibilité, ou si elle est un résultat indépendant de la valeur indéfinie. Dans cette toute dernière partie de la thèse, la Section 7.4, nous abordons cette question, clarifiant les relations entre ces concepts et celui d'aléatoire.

En considérant un exemple d'une expérience impliquant une dynamique chaotique que nous montrons étant imprévisible (toujours dans notre cadre formel), nous démontrons dans le Théorème 71 que cette expérience est capable de produire, dans la limite infinie, non seulement des suites incalculable (et même bi-immune ou aléatoire), mais également des suites calculables. Cela montre que l'imprévisibilité et la bi-immunité sont bien des conséquences indépendantes de la valeur indéfinie dans le cas quantique, et que l'assurance de la bi-immunité dans ce cas dépend de manière cruciale sur les hypothèses physiques qui sont faites. A fortiori, c'est vrai aussi pour les expériences imprévisibles relatives aux ensembles restreints d'extracteurs, puisqu'une expérience imprévisible dans le sens plus générale implique l'imprévisibilité relative à tout ensemble restreint d'une telle manière.

Ensuite, nous nous posons la question de si la complémentarité peut garantir une forme quelconque d'incalculabilité, de la même façon que la valeur indéfinie le fait. En donnant un exemple d'un système dont les observables agissent de façon complémentaire mais qui est complètement déterministe et à valeur définie, nous répondons au négatif : il existe des systèmes qui affichent de la complémentarité mais peuvent produire, dans la limite infinie, des suites calculables. La valeur indéfinie semble donc être une propriété plus forte sur le degré d'aléatoire et d'imprévisibilité qu'elle peut certifier.

Conclusions

En conclusion, nous utilisons la notion de la valeur indéfinie, que nous formalisons rigoureusement, pour formaliser et comprendre l'aléatoire quantique ainsi que l'imprévisibilité quantique. Au lieu de voir ces propriétés comme des conséquences triviales d'un indéterminisme supposé, cette approche formelle nous permet de formuler des résultats

mathématiques et aide à expliquer l'origine et la qualité de l'aléatoire quantique. Nous montrons que la valeur indéfinie peut garantir une notion d'aléatoire de produits – la bi-immunité des suites de bits générées par un générateur quantique de nombres aléatoires – ainsi qu'une notion d'aléatoire de processus, formalisée comme imprévisibilité dans un cadre formel.

Enfin, dans le dernier chapitre de la thèse nous présentons plusieurs questions ouvertes résultantes de notre travail.

Chapter 1

Introduction and outline

1.1 Background and motivation

The study of the foundations of quantum mechanics plays an important role in understanding how the quantum mechanical description of reality differs from the classical description of reality. Developments in quantum foundations have been crucial for the surge of interest in quantum information in the last decade, and have led to important developments in quantum cryptography and random number generation, even leading to the creation of practical devices and the implementation of protocols in the real world [56]. At the heart of quantum foundations is the study of the differences between quantum and classical measurement, and as a field it combines aspects of physics, theoretical computer science and cryptography, as well as philosophy, to understand and exploit quantum measurement.

1.1.1 Value indefiniteness

Bell's theorem [14] and the Kochen-Specker theorem [80] are perhaps two of the results which have been most influential in developing the modern understanding of quantum mechanics as an irreducibly nonclassical theory [91, 106]. Moreover, these two no-go theorems are seen as the strongest arguments for quantum mechanics being a fundamentally indeterministic theory, rather than one ruled by a deeper determinism below the level of the quantum mechanical description of reality.

However, these results do not guarantee quantum value indefiniteness, the notion that formalises indeterminism. Rather, further physical assumptions are required in order to rule out alternative deterministic, although necessarily nonclassical, descriptions of quantum mechanics. Furthermore, even under such assumptions they formally succeed

only in showing the existence of value indefiniteness, not the extent of it. These formal results thus fail to show that *all* nontrivial measurements result in a value that was not predetermined prior to measurement [4].

1.1.2 Quantum randomness

Closely related to the issue of quantum indeterminism, and key in many of the applications of quantum information theory, is the notion of quantum randomness. The outcomes of individual quantum measurements are often referred to as intrinsically or truly random [8, 105]. Such claims about quantum randomness stem largely from the understanding that such measurements are indeterministic, or value indefinite, since this indeterminism is absent in classical physical processes.

The notion of randomness, however, is more subtle than a simple equivalence with indeterminism [50], and a more careful analysis of quantum randomness is needed. Indeed, many different notions of randomness exist, both for physical processes and for sequences of events produced by such processes, and there is much evidence to show that the notion of true or absolute randomness is not mathematically robust [47, 65].

To understand the randomness produced by quantum random number generators or other devices, we thus need to study quantum randomness from a more rigorous perspective. In particular, questions such as the following ones need to be formally addressed:

- Does value indefiniteness guarantee any *formal* notion of unpredictability?
- Can the outputs of quantum random number generators be guaranteed to be stronger than what is obtainable from classical random number generators?
- How can value indefiniteness be used to certify (i.e., guarantee the production of) a formal notion of randomness?

1.1.3 Unpredictability

Key to understanding the properties of quantum randomness is the notion of unpredictability, which is closely related to randomness [49]. Unpredictability exists in many different forms: classical dynamical unpredictability, manifesting itself at the interaction between the inexactness of measurement and the chaotic dynamical behaviour of physical systems [12]; algorithmic notions of unpredictability for infinite sequences of bits [134]; and even computational definitions of unpredictability and irreducibility [166].

However, to understand randomness more broadly a more general formal model of unpredictability is needed, one which encompasses these various forms of unpredictabil-

ity. Only with such a model can we understand in a more unified fashion the different forms of unpredictability, and determine where quantum randomness fits into the picture.

1.2 Outline of the thesis

In this thesis we address several of the issues raised above, aiming to contribute to the understanding of quantum value indefiniteness, randomness and unpredictability.

In Chapter 2 we outline the basic concepts and definitions that will serve as a formal basis to this thesis. In particular, this includes the formal notions needed from quantum logic and algorithmic information theory.

In Chapter 3 we discuss quantum indeterminism, reviewing the key results, including the Kochen-Specker theorem, contributing to the development of the general consensus that quantum measurements are indeed indeterministic. We formalise precise notions of contextuality and value indefiniteness that are sufficiently general to allow us to consider varying degrees of these properties and examine the Kochen-Specker theorem more carefully. We show that the Kochen-Specker theorem, even under the appropriate physical assumptions, only guarantees the existence of *some* value indefiniteness, but does not show the *extent* of value indefiniteness.

In Chapter 4 we prove a variant of the Kochen-Specker theorem showing that, under the assumption that any value definite observables behave noncontextually, if a system is prepared in an arbitrary state $|\psi\rangle$, then *every* observable A is value indefinite unless $|\psi\rangle$ is an eigenstate of A. In contrast to standard proofs of the Kochen-Specker theorem, this stronger result requires a constructive method of reduction between Kochen-Specker sets – that is, the sets of observables used to derive Kochen-Specker type contradictions. As a consequence we show that: a) the set of value indefinite observables has measure one, that is, almost all observables are value indefinite; and b) value indefiniteness can be localised, that is, we can indicate precisely which observables are value indefinite.

In Chapter 5 we review and critically discuss various notions of randomness in order to assess claims about the nature of quantum randomness. We argue that most assertions of 'true' quantum randomness are based on a misplaced conflation of indeterminism and randomness, known as the commonplace thesis [50]. Instead, in order to understand quantum randomness, its unpredictability and algorithmic quality need to be studied more carefully.

We show that, under reasonable physical assumptions, infinite sequences of bits produced by the measurement of quantum value indefinite observables can be guaranteed to be bi-immune – a strong form of incomputability – something impossible for classical

random number generators.

We further propose a schema, as well as a possible implementation using generalised beamsplitters, for a quantum random number generator that is certified, via the Kochen-Specker theorem, by value indefiniteness and thus guaranteed to produce bi-immune sequences of bits.

In Chapter 6 we turn our attention to the understanding of unpredictability. We review various notions of unpredictability in classical physics, in algorithmic information theory, as well as a computational notion of unpredictability based on irreducibility. We review some proposed general frameworks for unpredictability, before motivating and formalising a new such framework. Our model of unpredictability is based on the prediction of physical events by a predicting agent, operating with effective means, and using finite information extracted (via measurement) from the environment. This model allows for a distinction and comparison of relativised and non-relativised notions of unpredictability.

Next, in Chapter 7, we apply this model of unpredictability to quantum randomness. We show that the outcome of a measurement of a value indefinite observable is formally unpredictable, while quantum complementarity can be used to give a weaker form of relativised unpredictability. This helps develop a clearer formal understanding of quantum randomness as a form of unpredictability.

Finally, we conclude the thesis in Chapter 8 with some open questions and future avenues of research in quantum foundations and randomness.

Chapter 2

Preliminaries

We assume a basic knowledge of computability theory and some understanding of quantum mechanics, but we will outline all the key notions and concepts needed from these fields in this thesis.

We use the notation $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ to denote the natural numbers (in which we include 0), the rational numbers, the real numbers and the complex numbers, respectively. We denote the positive integers by $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ and the non-negative reals by $\mathbb{R}^{\geq 0} = \{a \in \mathbb{R} \mid a \geq 0\}$. The cardinality of a finite set A will be denoted $|A|$, and the empty set by $\emptyset$.

The set of all finite bitstrings is denoted $\{0,1\}^* = \{\varepsilon, 0, 1, 00, 01, 000, \ldots\}$, where ε is the empty string. If $x \in \{0,1\}^*$ is a string, $|x|$ is the length of x, where $|\varepsilon| = 0$. The set of strings of length n is denoted $\{0,1\}^n = \{x \in \{0,1\}^* \mid |x| = n\}$.

The set of (right-)infinite binary sequences is denoted $\{0,1\}^\omega$. For any $\mathbf{x} \in \{0,1\}^\omega$, where $\mathbf{x} = x_1 x_2 x_3 \ldots$, we denote the prefix of length $n \in \mathbb{N}$ by $\mathbf{x} \upharpoonright n = x_1 x_2 \ldots x_n$ (for $n > 0$); $\mathbf{x} \upharpoonright 0 = \varepsilon$.

The *mth section* of a set $T \subset \{0,1\}^* \times \mathbb{N}^+$ is $T_m = \{x \in \{0,1\}^* \mid (x,m) \in T\}$. Given a set of prefixes $X \subset \{0,1\}^*$, the *cylinder* of X, $[X] \subset \{0,1\}^\omega$, is the set

$$[X] = \{\mathbf{x} \in \{0,1\}^\omega \mid \exists n \in \mathbb{N},\ \mathbf{x} \upharpoonright n \in X\}.$$

We write $[x]$ instead of $[\{x\}]$ for the cylinder generated by a singleton set – that is, an individual string. A set $X \subset \{0,1\}^*$ is *prefix-free* if, for any $x, y \in X$ with $x \neq y$, $[x] \cap [y] = \emptyset$.

Some familiarity with measure theory will be occasionally needed, in particular the Lebesgue (uniform) measure.

Definition 1. A *measure* on a space Ω is a countably additive function $\mu : \mathcal{F} \to \mathbb{R}^{\geq 0}$

satisfying $\mu(\emptyset) = 0$, where $\mathcal{F}$ is a σ-algebra on Ω. If $\mu(\Omega) = 1$ then μ is a *probability measure*.

A fundamental result in measure theory is that μ is uniquely determined by the values it takes on an algebra $\mathcal{A} \subset \mathcal{F}$ generating $\mathcal{F}$ [71].

If we consider measures on $\{0,1\}^\omega$, the cylinders $[x]$ for $x \in \{0,1\}^*$ generate the Borel σ-algebra $\mathcal{F}_B$ on $\{0,1\}^\omega$. The Lebesgue measure on $\{0,1\}^\omega$, $\mu_L : \mathcal{F}_B \to [0,1]$, is thus uniquely defined by its values on these cylinders: for all $x \in \{0,1\}^*$, $\mu_L([x]) = 2^{-|x|}$.

Similarly, the Lebesgue measure μ_L on $\mathbb{R}^n$ is characterised by its action on closed intervals: $\mu_L([a_1, b_1], [a_2, b_2], \ldots, [a_n, b_n]) = (b_1 - a_1)(b_2 - a_2) \cdots (b_n - a_n)$.

2.1 Quantum logic

Here we present the foundational aspects of quantum mechanics required for the thesis. To this end, we restrict ourselves to finite systems, and follow the Hilbert space presentation of quantum mechanics [70]. We cover the basic logical event structure of states, measurements, observables, etc., following the standard approach of quantum logic [130]. We refer the reader to [118] for a more thorough overview of quantum mechanics.

A quantum mechanical system is represented by an n-dimensional Hilbert space $\mathbb{C}^n$, which takes the standard inner product. An element of $\mathbb{C}^n$ is denoted by the ket (vector) $|\cdot\rangle$, and the inner product by $\langle\cdot|\cdot\rangle$, which satisfies $\langle x|y\rangle = \langle y|x\rangle^*$, where $\cdot^*$ denotes the complex conjugate.

Quantum mechanical states are represented by unit vectors in $\mathbb{C}^n$, and for the rest of the thesis a state $|x\rangle \in \mathbb{C}^n$ will always be assumed to be of unit length (i.e., $|\langle x|x\rangle| = 1$). Only the direction of a vector is important in defining a physical state, so two states $|x\rangle$ and $|y\rangle$ are considered equivalent if they differ only by a phase shift, that is, if $|\langle x|y\rangle| = 1$. Two states are orthogonal if $\langle x|y\rangle = 0$.

The Hilbert space structure means that the superposition principle applies to physical states. Thus, if $\{|x_1\rangle, \ldots, |x_n\rangle\}$ is an orthonormal basis for $\mathbb{C}^n$, any *superposition* of these basis states $|\psi\rangle = \sum_{i=1}^n \alpha_i |x_i\rangle$ with $\sum_{i=1}^n |\alpha_i|^2 = 1$ is also a valid physical state.

Of particular importance in quantum information are the states in $\mathbb{C}^2$, called *qubits*, which are usually expressed with respect to a computational basis $\{|0\rangle, |1\rangle\}$.

Measurable properties of quantum states are represented by operators called observables.

Definition 2. An *observable* is a Hermitian operator A in a Hilbert space $\mathbb{C}^n$. That is, for any states $|x\rangle, |y\rangle \in \mathbb{C}^n$ we have $\langle x|A|y\rangle = \langle y|A|x\rangle^*$.

The eigenvalues of an observable A are precisely the possible outcomes obtainable from a measurement of the observable A.

A class of observables of particular importance in quantum logic are the *projection observables*. Specifically, if $|\psi\rangle \in \mathbb{C}^n$ is a quantum state, then $P_\psi = \frac{|\psi\rangle\langle\psi|}{|\langle\psi|\psi\rangle|}$ is an observable projecting onto the linear subspace spanned by $|\psi\rangle$; that is, it is a rank-1 or one-dimensional projection observable. Projection observables represent yes-no propositions in quantum logic, and yield either the value 1 or 0 upon measurement, indicating the state 'has' the property represented by the eigenstate $|\psi\rangle$.

The dynamics and interactions of quantum systems are given by the action of a unitary operator on its state-vector. The act of measurement, however, is not described within the Hilbert space framework. Instead, when one measures an observable A with eigenvalues $\{a_1, \ldots, a_n\}$ and corresponding eigenstates[1] $\{|a_1\rangle, \ldots, |a_n\rangle\}$, one obtains one of the eigenvalues a_i probabilistically, and the system 'collapses' to the corresponding eigenstate $|a_i\rangle$ after measurement. This probability is given by the *Born rule* [21]: one obtains the eigenvalue a_i with probability $|\langle a_i|\psi\rangle|^2 = \langle\psi|P_{a_i}|\psi\rangle$.

An important theorem in quantum logic is Gleason's theorem [62], which shows that the Born rule is the only probability distribution on quantum states satisfying certain 'reasonable' criteria. In order to state it more precisely, let us first introduce the notion of a frame function.

Definition 3. Let $n \geq 2$. A *frame function* on a set $S \subset \mathbb{C}^n$ of (normalised) quantum states is a function $p : S \to [0, 1]$ such that:

1. if $\{|x_1\rangle, \ldots, |x_n\rangle\} \subset S$ is an orthonormal basis then $\sum_{i=1}^n p(|x_i\rangle) = 1$, and if $\{|x_1\rangle, \ldots, |x_k\rangle\} \subset S$ is orthonormal with $k < n$ then $\sum_{i=1}^k p(|x_i\rangle) \leq 1$;

2. for all complex $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ and all $|x\rangle \in S$, $p(|x\rangle) = p(\alpha\,|x\rangle)$ whenever $\alpha\,|x\rangle \in S$ also.

Theorem 4 (Gleason, [62])**.** *Let $n \geq 3$, and assume that p is a frame function on the set of unit vectors in $\mathbb{C}^n$ satisfying $p(|\psi\rangle) = 1$ for some (normalised) $|\psi\rangle \in \mathbb{C}^n$. Then, for all $|\phi\rangle \in \mathbb{C}^n$, $p(|\phi\rangle) = |\langle\psi|\phi\rangle|^2$.*

Finally, we introduce the notion of compatible observables.

Definition 5. Two observables A and B are *compatible* or *co-measurable* if they commute; that is, if $[A, B] = AB - BA = 0$.

[1] We assume that the spectrum of A is non-degenerate for simplicity, and label the eigenstates by their corresponding eigenvalue. It is simple to extend this to the degenerate case.

Compatible observables represent properties which can be simultaneously measured on a quantum system without disturbing it. As a result of the Born rule, incompatible observables cannot be simultaneously measured because the measurement of one causes the system to collapse into one of the eigenstates of the measured observables, thus altering the state.

2.2 Computability and algorithmic randomness

We define various notions of computability and randomness for infinite sequences of bits. These notions come from the field of algorithmic information theory, and we refer the reader to [29, 47] for further background on computability and randomness. The theory is based around the Turing model of computation and functions computable by Turing machines [122].

Definition 6. A function $f : \{0,1\}^* \to \{0,1\}^*$ is *computable* if there exists a deterministic Turing machine which, on every input $x \in \{0,1\}^*$, halts and outputs $f(x)$.

We denote the domain of a function f by $\operatorname{dom} f$. Recall that a partial function is a function that may be undefined on some elements in its domain.

Definition 7. A partial function $f : \{0,1\}^* \to \{0,1\}^*$ is *partially computable* if there exists a deterministic Turing machine which, for every input $x \in \{0,1\}^*$, halts and outputs $f(x)$ if $x \in \operatorname{dom} f$, and does not halt if $x \notin \operatorname{dom} f$.

Definition 8. A set $A \subseteq \{0,1\}^*$ is called *computably enumerable* (c.e.) if $A = \operatorname{dom} f$ for some partially computable function f.

Definition 9. A set $A \subseteq \{0,1\}^*$ is *computable* if both A and its complement $\bar{A}$ are computably enumerable. Otherwise, it is *incomputable*.

These definitions can be naturally extended to other countable sets such as $\mathbb{N}$ or $\mathbb{Q}$ via coding.

There is a natural bijection between infinite sequences in $\{0,1\}^\omega$ and sets of natural numbers. In particular, for any $\mathbf{x} \in \{0,1\}^\omega$, one can view this as the set $A_{\mathbf{x}} = \{i \in \mathbb{N} \mid x_i = 1\}$. Thus, we say that $\mathbf{x}$ is computable if and only if $A_{\mathbf{x}}$ is computable, etc.

A sequence $\mathbf{x}$ is bi-immune if it contains no infinite computable subsequence. More formally, we have the following definition.

Definition 10. A sequence $\mathbf{x} = x_1 x_2 \cdots \in \{0,1\}^\omega$ is *bi-immune* if there exists no infinite computable set $A \subset \mathbb{N}^+$ and computable function $f : A \to \{0,1\}$ such that, for all $n \in A$, $f(n) = x_n$.

We will briefly need the notion of computable and left-c.e. real numbers.

Definition 11. A real $\alpha \in \mathbb{R}$ is *computable* if the set $\{q \in \mathbb{Q} \mid q < \alpha\}$ is computable.

Definition 12. A real $\alpha \in \mathbb{R}$ is *left-computably enumerable*, or *lower semi-computable* if the set $\{q \in \mathbb{Q} \mid q < \alpha\}$ is computably enumerable.

Although not strictly a computability theoretic notion, the notion of Borel normality is important since it expresses the uniformity of a sequence of bits, and thus serves as a very primitive notion of randomness. Borel normal sequences are those in which every finite string appears with the expected frequency [29]. Let $N_i^m : \{0,1\}^* \to \mathbb{N}$ count the number of overlapping occurrences of the ith binary string (in lexicographical order) of length m in a given string.

Definition 13. A sequence $\mathbf{x} \in \{0,1\}^\omega$ is *Borel normal* if, for every $m \geq 1$ and every $1 \leq i \leq 2^m$, we have

$$\lim_{n\to\infty} \frac{N_i^m(\mathbf{x} \upharpoonright n)}{n} = 2^{-m}.$$

Finally, we proceed to the definition of algorithmic, or Martin-Löf, randomness, which formalises the notion that an infinite sequence is random or patternless.

In order to do so, we need the notion of a prefix-free Turing machine, which is a Turing machine whose domain is a prefix-free set. The algorithmic formulation of random sequences makes use of the prefix-free complexity of a string. Loosely speaking, the complexity of a string x with respect to a particular Turing machine T is the length of the shortest program for T which, when run, halts and outputs x.

Definition 14. The *prefix-free (Kolmogorov) complexity* of a string $x \in \{0,1\}^*$ induced by a prefix-free Turing machine W is $H_W(x) = \min\{|p| \mid W(p) = x\}$.

It is well known that there are universal Turing machines which can simulate any other Turing machine.

Theorem 15. *There exists a universal Turing machine U such that, for every prefix-free Turing machine W, there is a constant c (depending only on U and W) such that $H_U(x) \leq H_W(x) + c$ for all $x \in \{0,1\}^*$.*

The intuition behind the notion of algorithmic randomness is that a random sequence should not contain any computable patterns which allow it to be compressed, since such patterns would be a symptom of non-randomness.

Definition 16. A sequence $\mathbf{x} \in \{0,1\}^\omega$ is *algorithmically random* or *Martin-Löf random*, if there exists a constant c such that $H_U(\mathbf{x} \upharpoonright n) \geq n - c$ for all $n \geq 1$.

This definition is due to Chaitin [33]. However, this notion of randomness was first formulated by Martin-Löf [89] in a different way, which also allows one to consider whether sequences are random with respect to non-uniform measures. We give the definition of this formulation also, since we will need it in the proof of Theorem 55.

Let $\mu : \mathcal{F}_B \to \mathbb{R}^{\geq 0}$ be a probability measure (recall that $\mathcal{F}_B$ is the Borel σ-algebra on $\{0,1\}^\omega$).

Definition 17. A set $A \subset \{0,1\}^\omega$ is *μ-Martin-Löf null* if there exists a c.e. set $T \subset \{0,1\}^* \times \mathbb{N}^+$ such that, for all $n \in \mathbb{N}^+$, $A \subset [T_n]$ and $\mu([T_n]) \leq 2^{-n}$, where T_n is the nth section of T.

The c.e. sets $T \subset \{0,1\}^* \times \mathbb{N}^+$ in this definition are known as *Martin-Löf tests*.

Definition 18. A sequence $\mathbf{x} \in \{0,1\}^\omega$ is *μ-Martin-Löf random* if $\{\mathbf{x}\}$ is not a μ-Martin-Löf null set.

It is well known that this is equivalent to algorithmic randomness if one takes μ to be the Lebesgue measure, μ_L [47].

Theorem 19. *A sequence $\mathbf{x} \in \{0,1\}^\omega$ is algorithmically random if and only if it is μ_L-Martin-Löf random, where μ_L is the Lebesgue measure.*

Chapter 3

The Kochen-Specker theorem and quantum value indefiniteness

The predominant interpretation of quantum mechanics is that the quantum measurement process is intrinsically indeterministic [41]. This indeterminism appears, moreover, to be at the heart of claims that quantum measurement outcomes can provide 'true randomness' [8] that is 'intrinsically unpredictable' [139] in a way that no classical physical phenomena is capable of.

We will study the status of quantum randomness and unpredictability in more detail in the following chapters. First, however, it is important to understand the origin of this quantum indeterminism and the principles that it is based on; it is always possible to assume indeterminism in the absence of a deterministic explanation, but to understand quantum randomness properly, and especially to certify real devices using it [105], we need to carefully consider its basis.

In this chapter we review how Bell's theorem [14] and the Kochen-Specker theorem [80] show the impossibility of classically deterministic theories. While they don't completely discount other, nonclassical, deterministic explanations of the apparent indeterminism, the existence of indeterminism can thus be based on precise, fundamental, physical assumptions. These results, however, only show the existence of some indeterminism – a property we formalise as value indefiniteness – but not the extent of this value indefiniteness. In the next chapter we extend these results, proving a variant of the Kochen-Specker theorem showing that almost all observables are value indefinite, bringing the formal results closer to the intuition regarding quantum indeterminism.

The work of these two chapters covers, in a unified framework, many of the results published in [3, 4, 7].

3.1 Quantum indeterminism and value indefiniteness

The origin of the debate about quantum indeterminism resides in the probabilistic nature of the Born rule. While the principal elements of quantum mechanics are described within the Hilbert space framework – the states, the dynamical evolution and interactions, as well as the observable properties – the Born rule specifies a probability distribution for the outcomes of measurements on top of this framework. This fact, along with the irreversible (i.e., non-unitary) 'collapse' of the state upon measurement, has long been a source of philosophical debate, and continues to be so today [147].

The heart of the problem is that probability is, technically, a formal mathematical tool and has no inherent physical meaning. There are many different interpretations of probability, and rather than there being any question as to which is *the* correct interpretation, the reality is rather that different interpretations may be more appropriate than others in different situations [69, 117]. Thus, one has to consider the *physical* scenario being modelled in determining how a probability within the *mathematical* model of the scenario should be interpreted.

3.1.1 Interpreting probability distributions

Probabilities, for example, may be perfectly reasonable tools in modelling scenarios in which we have limited knowledge. For example, consider that Alice flips a coin, hides the result and asks her friend Bob to guess what the outcome of the flip was. Bob, having not seen the result, assigns a probability distribution to heads/tails. In such a case, a probability distribution naturally represents merely Bob's degree of knowledge, and should be interpreted as a subjective probability distribution [69, 138]. This probability is *epistemic*: it depends on the knowledge of the observer, and different observers could reasonably assign different subjective probability distributions to the same scenario. For example, Alice, having peeked, knows the result is heads, and thus assigns a different distribution than Bob.

This subjectivist interpretation of probability is, although more subtly so, the way probability is generally viewed in classical physics. In statistical mechanics, for example, the velocity of particles within a gas is given by a probability distribution. Each particle in the gas follows a deterministic, reversible trajectory, and hence its velocity is not objectively probabilistic at all. However, as an observer we can only measure the macrostate of the system, and hence are forced to describe the velocities of individual particles using the appropriate probability distribution. In fact, as a result of the ergodic theorem, we can go a step further: almost all initial conditions (in the measure theoretical sense) for a particle will result in a trajectory in which the proportion of time

it spends in a particular region of phase space is equal to the probability assigned by the distribution of finding it in this region. Thus, for a typical set of initial conditions, the probability distribution is validated by the average dynamics over time [123, 138]. Of course, this raises the further question of why real gases should be in such 'typical' states, and whether the choice of the Lebesgue measure is valid [9, 57].

This subjectivistic view of probabilities is common also in other classical systems that are often considered unpredictable, such as chaotic systems. We model certain properties of these systems with probabilities not because we believe they are indeterministic, but because we are unable to measure their state accurately enough to determine their behaviour with sufficient precision to make useful predictions [16, 146].

3.1.2 Probabilities in quantum mechanics

Born was the first to argue that the probabilities in quantum mechanics should not be interpreted in the subjective fashion that they are in classical mechanics, declaring that he was 'inclined to give up determinism in the world of atoms' [21]. He thus proposed, in essence, that quantum probabilities represent real objective propensities [110, 128] for measurements to take on various outcomes; that the probability distribution given by the Born rule represents objective indeterminism as opposed to an epistemic limit. This represented a bold departure from the established dogma of classical determinism, and it is unsurprising that there was much debate around whether such an assumption was indeed justified [147]. After all, this amounted largely to an act of faith based on Born's inclination: why should we believe that quantum mechanics departs so radically from the determinism of classical mechanics?

This is all the more true given that, during the early years of quantum mechanics, quantum theory was used almost exclusively to explain statistical phenomena, such as the spectra of atoms or scattering distributions. Such distributions are obtained from large numbers of particles, a long stretch from the (relative) ease with which we can manipulate and probe the quantum mechanical properties of individual particles these days. Thus, despite the absence of a deterministic explanation for quantum phenomena, it is natural to demand further explanation as to why a more classical, ensemble-based interpretation could not also be possible, in principle, in quantum mechanics [110]. That is, why should we discount the possibility that the probabilities represent distributions of particles in definite, but unknown, states?

This indeed was the opinion of Einstein, who famously disagreed, stating that 'He does not throw dice' [22, p. 204]. Along with Podolsky and Rosen, Einstein argued, in formulating what is now known as the *EPR paradox*, that the quantum formalism and collapse associated with measurement implies that quantum states can behave nonlo-

cally [51]. To them, this was proof that quantum mechanics was 'incomplete', and needed to be completed by a more fundamental, deterministic, theory that would explain the apparent indeterminism arising at measurement.

In spite of this, the view that quantum measurements are intrinsically indeterministic gradually became accepted as the quantum orthodoxy, and remains so today [162]. The debate regarding the nature of quantum measurement received a subdued level of attention for a long period of time as a more practical-minded approach to quantum mechanics became the norm. After all, the theory was exceptionally successful in making accurate predictions and describing quantum phenomena, and the success of these aspects of the theory do not depend on its metaphysical interpretation.

Von Neumann was the first to make an attempt to show that it is impossible to complete quantum mechanics with an underlying deterministic theory – a 'hidden variable theory' – in the way that Einstein had envisaged. However, his purported proof of this impossibility [97], within the framework of quantum logic that he helped develop [17], was criticised and subsequently shown to be flawed [14, 94].

3.1.3 Bell's theorem

Bell's theorem was the first major breakthrough in this direction, showing that no *local* hidden variable theory can successfully reproduce all of the statistical predictions of quantum mechanics [14]. In particular, he derived inequalities involving expectation values of joint measurements on pairs of particles that must be satisfied by any local hidden variable model, but which can be violated by certain entangled quantum states. Since then, many variations and simpler versions of such inequalities have been given, such as the well-known CHSH inequalities [37], but the fundamental concept is unchanged.

Bell's theorem rules out certain classes of classical hidden variable theories, but it is important to note that this does not necessarily imply quantum indeterminism. One can give deterministic, but nonlocal, interpretations of quantum mechanics reproducing all its statistical predictions but in which indeterminism is completely absent [20]; Bell himself interpreted his results in this light [14]. Nonetheless, Bell's theorem can be seen as offering evidence to Born's original inclination for indeterminism. At the very least, they allow indeterminism to be reduced to the physical assumption that any determinism must be local (although still a classical assumption by nature, given that the inequalities show that quantum mechanics is indeed nonlocal, indeterministic or not).

3.1.4 The Kochen-Specker theorem

The Kochen-Specker theorem [80] was proved very shortly after Bell's theorem. It shows that the Hilbert-space structure of quantum mechanics makes it impossible to assign, prior to any measurement, 'classical' definite values predicting measurement outcomes to all quantum observables in a consistent manner.

Like Bell's theorem, the Kochen-Specker theorem received very little attention at the time, largely as a result of a prevailing disinterest in the metaphysical issues of quantum mechanics that these theories sought to address. Compared to Bell's theorem, however, it would take even longer for interest in the Kochen-Specker theorem to grow.

This can, for the most part, be explained by the apparent inability to test experimentally the Kochen-Specker theorem. While Bell's theorem was initially ignored for the most part, the realisation that it was possible to experimentally test Bell inequalities eventually led to a sufficient degree of interest and effort to find simpler or alternative forms of the inequality more suitable to experimental tests [36]. This was followed by actual realisations of such tests [10], confirming quantum nonlocality and precipitating the growth of interest in the subject.

The Kochen-Specker theorem, on the other hand, is formulated within the framework of quantum logic. Whereas the Bell inequalities are themselves independent of quantum mechanics, the Kochen-Specker theorem is not, and identifies a contradiction within the quantum mechanical framework, involving elements that cannot be simultaneously measured. As such, it is counterfactual in nature and not directly testable experimentally; after all, as Rob Clifton asked [39], 'how can you measure a contradiction?'

It is only more recently in the 1990s, following the success of experimental tests of Bell's theorem, that the Kochen-Specker theorem began to gain interest. This has only grown further with the more recent boom of interest in quantum information and foundational principles, and has led to further development.

In showing the impossibility of a classical 'two-valued' measure (i.e., value assignment) the Kochen-Specker theorem leaves open several possible conclusions for quantum mechanics, and, as for Bell's theorem, does not necessarily guarantee quantum indeterminism [156]. The Kochen-Specker theorem, more specifically, finds a contradiction between the following three assumptions, which will be formalised more rigorously in the next section:

(i) all observables have a predefined measurement outcome (a definite value);

(ii) the definite value associated with an observable should be noncontextual, that is, independent of what other compatible observables are simultaneously measured;

(iii) the measurement outcomes (and hence definite values) for a set of compatible observables must be consistent with the theoretical quantum predictions for the relations between them.

Condition (iii) of the Kochen-Specker theorem is largely uncontroversial, since any set of compatible observables are simultaneously co-measurable, and since quantum mechanics requires that the measured values be eigenvalues of the corresponding observables, the values obtained should thus obey the same relations as the observables. Indeed, one of the principal problems with von Neumann's earlier attempt at proving the impossibility of hidden variables failed precisely because he assumed that such relations be obeyed for *all* observables, even when not compatible. Since such observables are not co-measurable, such a condition indeed appears too strong, and quantum theory would seem only to imply that the relations hold for the expectation values of such observables [73]. The effort to correct this shortcoming of von Neumann's argument was, in many ways, what led both to Bell's theorem, and, more directly, the Kochen-Specker theorem. Hence, one must generally conclude that either (or even both) (i) and (ii) must be given up.

3.1.4.1 Value indefiniteness

Several alternative interpretations of quantum mechanics are contextual, and hence discard (ii). We will outline some such approaches later in Sec. 4.5.1, once we have formalised the notion of contextuality further. Perhaps the more widespread interpretation of the contradiction identified by the Kochen-Specker theorem, however, is that one must abandon (i), the idea that measurement outcomes are determined in advance at all: that quantum mechanics represents a value indefinite reality. This interpretation has, at the very least, been at the heart of recent interest and advances in quantum information and cryptography, where the practical advantages are based on precisely this indeterminism.

Perhaps paradoxically, this interpretation is often referred to simply as 'quantum contextuality' in the literature. This loose notion of contextuality, however, does not necessarily refer to hidden variables and hence does not contradict the assumption of (ii). We will return to discuss this issue in more detail in Section 4.5.2; however, we reserve the term 'contextuality' strictly for the contextual behaviour of definite values.

3.1.5 Global vs local value indefiniteness

If we choose to follow the standard interpretation of the Kochen-Specker theorem, requiring (ii) to hold – at least for any definite values that *do* exist – then there remains

an oft-overlooked gap between the formal result of the Kochen-Specker theorem and the general interpretation of it. Indeed, the negation of (i) is that *not all* measurement outcomes are predetermined: it does not prove that all measurements must result in the *ex nihilo* creation of an outcome, nor does it allow one to know *which* observables are value indefinite. We can, of course, postulate that if there is some value indefiniteness, this should, by symmetry or uniformity considerations, be the case for all observables. However, it is key to realise that this is not in any sense a formal consequence of the Kochen-Specker theorem, and constitutes an additional assumption. If possible, it would therefore be desirable to eliminate this assumption, instead deducing this conclusion from simpler, existing hypotheses.

The same limitation is in fact true of Bell's theorem, since Bell-inequalities are derived under the assumption that all measurement outcomes be predetermined. Thus, the violation of Bell inequalities, even if one assumes that hidden variables behave locally, only allows us to conclude the existence of some indeterminism, but not that all such measurements behave in such a way. However, the issue is even more complicated with Bell's theorem, since the statistical nature of the inequalities adds another layer of uncertainty as a violation must be built up over several rounds of measurements, and deducing that the indeterminism was present in all of them requires yet further assumptions. Moreover, only certain states and observables allow the deduction of Bell-inequalities, meaning they cannot be used to satisfactorily show the extent of quantum indeterminism.

The ability to determine precisely which observables are value indefinite and thus produce indeterministic measurement outcomes is of importance not only for our understanding of quantum measurements at a foundational level, but is equally important in many practical applications. In particular, the superiority of quantum random number generators over classical devices is regularly justified by the assertion that they produce bits that are 'intrinsically random' [125], a claim not strictly supported by the Kochen-Specker theorem, nor by Bell's theorem.

In the following chapter we will address precisely this issue: by using a modified, weakened set of assumptions, we show that *no* observable A can have a predetermined measurement outcome except if the quantum system is in a state $|\psi\rangle$ that is an eigenstate of A. This result, like the Kochen-Specker theorem, is proven within a purely formal, abstract framework, but we will then carefully discuss the specific physical assumptions that need to be made to give this result a solid physical interpretation.

Throughout these two chapters we will, unless explicitly specified, assume (ii) to hold, as is common in interpretations of the Kochen-Specker theorem, and our strengthened results and interpretation of the Kochen-Specker theorem thus rely on this condition. Indeed, our goal is to strengthen the conclusions that can be drawn from the Kochen-

Specker theorem under this hypothesis.

3.2 Formalising value indefiniteness and contextuality

We begin by presenting the formal framework we will use to localise value indefiniteness, which is similar to, but more general than, standard approaches to the Kochen-Specker theorem [24]. This framework is deliberately very flexible and allows us to consider varying degrees of value indefiniteness and contextuality – as is necessary if one wishes to explore the extent of value indefiniteness – in a way not possible with the more rigid but standard approach of quantum logic using two-valued (dispersionless) measures [17, 97, 130].

We refer the reader to Section 2.1 for definitions relating the the quantum mechanical formalism, but we recall, in particular, that we denote by P_ψ the operator projecting onto the linear subspace spanned by $|\psi\rangle$; that is, $P_\psi = \frac{|\psi\rangle\langle\psi|}{|\langle\psi|\psi\rangle|}$.

We fix a positive integer $n \geq 2$. Let $\mathcal{O} \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a nonempty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

Definition 20. A set $C \subset \mathcal{O}$ is a *context* in $\mathcal{O}$ if C has n elements (i.e., $|C| = n$) and for all $P_\psi, P_\phi \in C$ with $P_\psi \neq P_\phi$, $\langle\psi|\phi\rangle = 0$.

We denote the set of all contexts in $\mathcal{O}$ by $\mathcal{C}_\mathcal{O}$. Since distinct one-dimensional projection observables commute if and only if they project onto mutually orthogonal linear subspaces, a context $C \in \mathcal{C}_\mathcal{O}$ is thus a maximal set of compatible one-dimensional projection observables.

Since there is a direct correspondence between unit vectors and one-dimensional projection observables, a context is uniquely defined by an orthonormal basis in $\mathbb{C}^n$. Thus, in slight abuse of terminology, we sometimes refer to two commuting observables P_1 and P_2 as orthogonal, and a context as an orthogonal set of observables.

Recall that a partial function is one which may be undefined for some values in its domain. If it is defined everywhere, then it is total.

Definition 21. A *value assignment function (on $\mathcal{O}$)* is a partial two-valued function $v : \mathcal{O} \times \mathcal{C}_\mathcal{O} \to \{0, 1\}$.

A value assignment function formalises the notion of a hidden variable theory, and assigns values to some (possibly all) observables in $\mathcal{O}$, possibly dependent on the context in which an observable is to be measured.

For two contexts $C, C' \in \mathcal{C}_{\mathcal{O}}$ and $P \in C, P' \in C'$, we say that $v(P, C) = v(P', C')$ if both $v(P, C)$ and $v(P', C')$ are defined and have equal values. If either $v(P, C)$ or $v(P', C')$ are undefined or they are both defined but have different values, then $v(P, C) \neq v(P', C')$.

Definition 22. An observable $P \in C$, $C \in \mathcal{C}_{\mathcal{O}}$, is *value definite (under v) in the context* C if $v(P, C)$ is defined; otherwise it is *value indefinite (under v) in* C. If P is value definite in all contexts $C \in \mathcal{C}_{\mathcal{O}}$ for which $P \in C$ then we simply say that P is value definite under v. Similarly, if P is value indefinite under all such contexts C then we simply say that P is value indefinite under v.

Definition 23. The set $\mathcal{O}$ of observables is *value definite (under v)* if every observable $P \in \mathcal{O}$ is value definite under v.

Definition 24. An observable $P \in \mathcal{O}$ is *noncontextual (under v)* if, for all contexts $C, C' \in \mathcal{C}_{\mathcal{O}}$ with $P \in C, C'$, we have $v(P, C) = v(P, C')$. Otherwise, v is *contextual*.

Note that an observable which is value indefinite in a context is always contextual, even if it is assigned the same value in every context in which it is value definite. On the other hand, if an observable is value definite in all contexts containing it, it can be either contextual or not, depending on v.

Definition 25. The set $\mathcal{O}$ of observables is *noncontextual (under v)* if every observable $P \in \mathcal{O}$ which is not value indefinite (i.e., value definite *in at least one* context) is noncontextual under v. Otherwise, $\mathcal{O}$ is *contextual (under v)*.

Definition 26. The set $\mathcal{O}$ of observables is *strongly contextual* under v if every observable $P \in \mathcal{O}$ is contextual under v.

The notion of contextuality is thus a subtle one with many slight variations possible, and it is for this reason that we place an emphasis on carefully formalising it. Noncontextuality represents the classical notion that the value obtained via measurement should be independent of other compatible measurements that one makes on the system.

Every strongly contextual set of observables under v is contextual under v, provided that v is not undefined everywhere. However, the converse implication is false, as we will show in Sec. 3.4.

If an observable P is noncontextual then it is value definite, but this is not true for sets of observables: $\mathcal{O}$ can be noncontextual but not value definite if it contains an observable which is value indefinite. Thus, our terminology differs slightly from that, often used informally, where both value indefiniteness and contextual value definiteness are referred to as showing quantum contextuality. Our decision, however, is justified by the

fact that we treat noncontextuality as a specific property of value definite observables, and this will help clarify further discussion.

This formalism of value assignment functions allows us to consider a wide range of hidden variable models with varying degrees of contextuality and value indefiniteness. However, it does not by itself impose any structure on the function v. In order to apply this framework to quantum mechanics, we need to give such a structure, and thus formalise condition (iii) of the Kochen-Specker theorem mentioned informally in Sec. 3.1.4.

This condition, specifically, requires that for any given context $C \in \mathcal{C}_{\mathcal{O}}$, any functional relation between the observables in C (thus specifying another compatible observable, although generally *not* a projection observable) also be satisfied by the corresponding definite values, which would be, in turn, obtained by their simultaneous measurement. In particular, if such observables are value definite, these relations should be satisfied by their definite values. For projection observables, since, for any context C, $\sum_{P\in C} P = I$, the identity operator, this means that only one observable $P \in C$ can have $v(P, C) = 1$.

If $\mathcal{O}$ is value definite and noncontextual under v, this would require that $\sum_{P\in C} v(P, C) = 1$ for all $C \in \mathcal{C}_{\mathcal{O}}$. Traditionally, in the field of quantum logic this has been formalised by the notion of a two-valued (dispersionless) measure [130] or a Boolean frame function with weight 1 [62]. However, in order to localise value indefiniteness we need to generalise this for partial value assignment functions v, that is, the case where some observables in $\mathcal{O}$ may be value indefinite and hence the sum $\sum_{P\in C} v(P, C)$ is not well defined for some contexts.

Definition 27 (Admissibility)**.** Let $\mathcal{O}$ be a set of observables on $\mathbb{C}^n$ and let $v : \mathcal{O}\times\mathcal{C}_{\mathcal{O}} \to \{0, 1\}$ be a value assignment function. Then v is *admissible* if the following two conditions hold for every context $C \in \mathcal{C}_{\mathcal{O}}$:

(a) if there exists a $P \in C$ with $v(P, C) = 1$, then $v(P', C) = 0$ for all $P' \in C \setminus \{P\}$;

(b) if there exists a $P \in C$ with $v(P', C) = 0$ for all $P' \in C \setminus \{P\}$, then $v(P, C) = 1$.

Admissibility requires that the quantum predictions of condition (iii) of the Kochen-Specker theorem (see Sec. 3.1.4) are never violated, while allowing value indefiniteness of an observable P if both outcomes (0 and 1) of a measurement of P would be compatible with the definite values of other observables sharing a context with P. For example, if $v(P, C) = 1$, then a measurement of all the observables in a context C containing P must yield the outcome 1 for P, and hence to avoid contradiction the outcome 0 for the other observables in the context. On the other hand, if $v(P, C) = 0$, even though measurement of P must yield the outcome 0, any of the other observables in C could

yield the value 1 or 0 (as long as only one yields 1), hence we should not conclude the value definiteness of these other observables. We will justify the physical interpretation and form of the admissibility requirement more carefully later, in Sec. 4.4.2.

If $\mathcal{O}$ is noncontextual under an assignment function v, then the values v assigns to observables are independent of the context. Since we will assume noncontextuality when localising the value indefiniteness, it will be useful to define the notion of a noncontextual value assignment function for notational simplicity.

Definition 28. A *noncontextual value assignment function (on $\mathcal{O}$)* is a partial two-valued function $v : \mathcal{O} \to \{0, 1\}$, assigning values to some (possibly all) observables in $\mathcal{O}$.

Thus, if $\mathcal{O}$ is value indefinite under v we can simply talk about the value $v(P)$ of an observable $P \in \mathcal{O}$, independent of the context.

A noncontextual value assignment function $v : \mathcal{O} \to \{0, 1\}$ induces naturally a value assignment function $u_v : \mathcal{O} \times \mathcal{C}_\mathcal{O} \to \{0, 1\}$ such that, for all $P \in \mathcal{O}$ and $C \in \mathcal{C}_\mathcal{O}$ with $P \in C$, $u_v(P, C) = v(P)$. Thus, the definitions of value (in)definiteness and admissibility generalise naturally to noncontextual value assignment functions: *v is admissible if u_v is admissible*, and *$P \in \mathcal{O}$ is value definite under v if it is value definite under u_v*.

3.3 The Kochen-Specker theorem

With this terminology laid out, we can state the Kochen-Specker theorem formally.

Theorem 29 (Kochen-Specker, [80])**.** *Let $n \geq 3$. Then there exists a (finite) set $\mathcal{O}$ of one-dimensional projection observables on $\mathbb{C}^n$ such that there is no value assignment function v satisfying the following three conditions:*

(i) $\mathcal{O}$ is value definite under v; that is, v is a total function.

(ii) $\mathcal{O}$ is noncontextual under v.

(iii) v is admissible; that is, for every context $C \in \mathcal{C}_\mathcal{O}$, $\sum_{P \in C} v(P, C) = 1$.

We presented the theorem in this form deliberately in order to draw the comparison to our informal description given earlier in Sec. 3.1.4, and thus to clarify the associated discussion. However, it can equivalently be stated in the more simple form: *there exists a finite set of projection observables $\mathcal{O}$ on $\mathbb{C}^n$ such that there is no admissible noncontextual value assignment function v on $\mathcal{O}$.*

As we mentioned earlier, the condition of admissibility is largely uncontroversial: one can simultaneously measure the observables in a context and quantum mechanics

predicts precisely that exactly one of these measurements should give the result '1'. Thus, if we assume (ii) to be true then the Kochen-Specker theorem requires us to conclude the negation of (i): that $\mathcal{O}$ cannot be value definite, and hence *at least one* observable must be value indefinite.

Note that, by defining a set of observables to be noncontextual only if all value definite observables within it are noncontextual, such a conclusion can be made clear. If, as is often considered informally, noncontextuality is taken to imply value definiteness, even for an entire set of observables, then one cannot conclude value indefiniteness, since it would violate the very assumptions used to deduce it. Thus, by removing the dependence of (ii) on (i) and decoupling the assumptions we allow a much more nuanced analysis of the Kochen-Specker theorem and value indefiniteness.

3.3.1 The Kochen-Specker theorem up to the present

The original proof of the Kochen-Specker theorem was notoriously difficult, and involved a rather heavy mathematical formalism and several rather subtle elements. The specific finite set of observables given contains 117 observables connected in a rather clever construction [80]. This formalism and difficulty probably helped contribute to the long period of time between when the theorem appeared and when it started to gather real interest and attention.

It was only really following the success of experimental tests of Bell's theorem, as well as the emergence of the GHZ theorem [66], that the Kochen-Specker theorem finally received some attention and efforts were made to try and simplify the original argument. This started with Mermin [91, 92], and was continued by Peres [103], Clifton [38] and Cabello [24], amongst others.

These results significantly reduced the complexity of the proof, bringing down the number of observables needed from 117 to 31 [103], introducing much more symmetric and understandable sets of observables. The advancements culminated in Cabello's proof requiring only 18 observables, albeit in four-dimensional Hilbert space [27]. This proof is notable in its simplicity, and it is possible to show that no noncontextual value assignment is possible by a simple parity argument, without even considering potential value assignments. More recently, computational techniques have been used to exhaustively search for possible proofs and show that these are indeed the smallest possible Kochen-Specker sets obtainable [90, 101].

With the advent of quantum information and quantum cryptography, which propose practical uses for Bell inequality violation in verifying nonclassicality and nonlocality, there has been further interest in the Kochen-Specker theorem. These results have centred around the ability to derive testable 'noncontextuality inequalities' from proofs

of the Kochen-Specker theorem [83, 157, 158] as well as their experimental verification [79, 163]. These inequalities gave further incentive to the search for small proofs of the Kochen-Specker theorem, since smaller proofs lead naturally to smaller and more readily testable inequalities.

One of the main conceptual debates that surfaced around the Kochen-Specker theorem relates to the precision of measurements needed for the theorem to hold. Meyer claimed, in a much debated paper, that finite-precision measurement 'nullifies' the Kochen-Specker theorem [93]. More specifically, he showed that it is possible to assign definite values to all possible observables that can be specified by *rational valued* unit vectors (which are dense in the n-dimensional unit sphere), and argued that, since we can only ever specify, experimentally, an observable up to a rational approximation, that this casts doubt over the validity of the theorem. It was later shown that such value assignments lead to statistical predictions in contradiction with quantum mechanics [25] and hence are unsupportable, but only after much debate.

However, this response appears to miss a further crucial conceptual issue with this supposed nullification of the Kochen-Specker theorem. While it is of little debate that we can only experimentally measure rational approximations or intervals, a fact acknowledged by Poincaré and crucial to the development of the concept of chaotic systems, Meyer's nullification goes a step further in asserting that physical reality consists solely of these rationals. It is, after all, not the results of the measurements of the quantum observables, but the specification of the observables themselves which he asserts must be rational valued. While we may not be able to measure, and hence know, the precise observables we measure to more than a rational approximation, this does not guarantee in any way the observable actually measured is itself rational valued. Indeed, unless one refutes the existence of the continuum and poses an absolute limit on measurement, one should rather view the observable measured as a generic one within the interval specified by our rational approximation. With probability one, such an observable is *irrational* valued. Thus, the Kochen-Specker theorem, which requires only the *existence* of arbitrary observables and not our practical ability to measure them, hardly appears to be nullified by such an argument.

Throughout these advances, however, the nature of the theorem and its assumptions have remained largely unchallenged. In particular, the results have not addressed the extent of nonclassicality shown by the theorem, and in all the variants it remains impossible to determine which observables in particular must be value indefinite. Given the use of the Bell and Kochen-Specker theorems to justify the indeterministic nature of quantum mechanics and its use in quantum mechanics, it seems especially important to address this issue and try and strengthen the specific form – as opposed to simply the proof – of the theorem in an attempt to locate value indefiniteness.

3.4 Strong contextuality cannot be guaranteed

Before we proceed to our main results localising value indefiniteness, it is interesting to ask whether there are any limits we can pose on how strong the contradiction, identified by the Kochen-Specker theorem, between noncontextuality and value definiteness is. Is it possible, for example, to show that any value definiteness or noncontextuality would lead to a contradiction, and thus guarantee the strong contextuality of the set of projection observables on $\mathbb{C}^n$ for $n \geq 3$? We provide a negative response to this question: the contradiction cannot be maximal in the sense that no set of observables can be guaranteed to be strongly contextual.

Theorem 30. *Let $n \geq 2$, and $\mathcal{O}$ be an arbitrary set of one-dimensional projection observables on $\mathbb{C}^n$. Then for every observable $P \in \mathcal{O}$ there exists an admissible assignment function v such that $v(P, C) = 1$ for every context $C \in \mathcal{C}_\mathcal{O}$ with $P \in C$, and $\mathcal{O}$ is value definite under v.*

Proof. Let us consider the set

$$S_P = \{C \mid C \in \mathcal{C}_\mathcal{O} \text{ and } P \in C\} \subseteq \mathcal{C}_\mathcal{O}$$

of contexts in which P appears. If we define the assignment function v_P such that for every $C \in S_P$

$$v_P(Q, C) = \begin{cases} 1 & \text{for } P = Q, \\ 0 & \text{for } P \neq Q, \end{cases}$$

it is clear this satisfies $\sum_{Q \in C} v_P(Q, C) = 1$ for all $C \in S_P$. For $C \in \mathcal{C}_\mathcal{O} \setminus S_P$ the function v_P can be defined in any arbitrary contextual way to satisfy admissibility. The function is then admissible and assigns a definite value (namely 1) to the observable P (which is arbitrary) in a noncontextual fashion (i.e., $v_P(P, C) = 1$ for all $C \in S_P$). □

Indeed this should not be surprising in light of the predictions of quantum mechanics. Specifically, for a physical system prepared in the state $|\psi\rangle$, the Born rule predicts that measurement of the observable P_ψ should give the value 1, noncontextually, with probability 1. Nevertheless, it is important to place a bound on the degree of nonclassicality that we can guarantee [52, 132]. In fact, it is possible to go further: v_P can be constructed so that every observable $P' \in \mathcal{O}$ for which there is a context $C \in S_P$ such that $P', P \in C$ is noncontextual under v_P (in addition to P) with $v(P', C) = 0$. This is a consequence of the fact that no two observables P_1, P_2, orthogonal to P but in different contexts C_1, C_2 with $P \in C_1, C_2$, can both be in some third context C_3 with $P \notin C_3$. This scenario is shown in the 'star' Greechie diagram in Fig. 3.1, where nodes represent observables and smooth line segments contexts. Strong contextuality cannot

be guaranteed because such star-shaped pockets of noncontextuality are always possible under an admissible value assignment function,

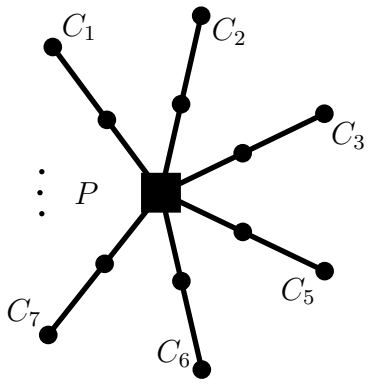


Figure 3.1: Greechie diagram showing an observable P with $v(P, C_i) = 1$ for $i \geq 1$ and the (infinite) set of compatible observables P' for which $v(P', C_i) = 0$. Observables are shown by nodes and contexts by smooth line segments. Circles represent the value 0 and squares the value 1.

Chapter 4

Localising value indefiniteness

While the Kochen-Specker theorem certainly succeeds, as was the original intention, in showing that quantum mechanics must obey an entirely nonclassical event structure, it does not, as we have pointed out, show that all measurement outcomes must be indeterministic. As a consequence of the global nature of the hypothesis of the theorem – that *all* observables are value definite – one can only draw a global conclusion: that *not all* observables are value definite. That is, the theorem, even under the assumption of noncontextuality, cannot 'locate' value indefiniteness. This is an important point, not only for the foundational understanding of quantum mechanics, but also in practical applications: quantum random number generators and cryptographic schemes rely on the indeterminism of quantum mechanics providing 'irreducible randomness' [55]. To certify such claims, it is important to be able to localise value indefiniteness to ensure it applies to the observables measured in such applications.

4.1 The logical indeterminacy principle

Pitowsky [106] (also in the subsequent paper [75] with Hrushovski) gave a constructive proof of Gleason's theorem (Theorem 4 in Section 2.1) in terms of orthogonality graphs which motivated the study of probability distributions on finite sets of projection observables. In this context he proved a result called 'the logical indeterminacy principle' which has a striking similarity with the Kochen-Specker theorem and appears as if it could be used to locate value indefiniteness. Given that this principle is in fact stronger than the Kochen-Specker theorem, it is important to analyse this possible localisation of value indefiniteness more carefully.

Recall the definition of a frame function (Definition 3). For the sake of presenting

Pitowsky's logical indeterminacy principle, let us define further the following notion.

Definition 31. A *Boolean frame function* p on a set $S \subset \mathbb{C}^n$ of (normalised) quantum states is a frame function on S taking only the values 0 and 1; that is, for all $|x\rangle \in S$, $p(|x\rangle) \in \{0, 1\}$.

Since there is a direct equivalence between quantum states and one-dimensional projection observables, the notion of a frame function is a generalisation of a noncontextual, value definite, value assignment function to a more generalised probability measure assigning real numbers to observables [75]; the notions coincide and are essentially equivalent for Boolean frame functions.

Pitowsky's *logical indeterminacy principle* is the following:

Theorem 32 (Pitowsky, [106])**.** *For all states* $|a\rangle, |b\rangle \in \mathbb{C}^3$ *with* $0 < |\langle a|b\rangle| < 1$*, there exists a finite set of states* S *with* $|a\rangle, |b\rangle \in S$ *such that every frame function* p *on* S *satisfying* $p(|a\rangle), p(|b\rangle) \in \{0, 1\}$ *has* $p(|a\rangle) = p(|b\rangle) = 0$*.*

A consequence of this principle is that there is no Boolean frame function p on this set S such that $p(|a\rangle) = 1$ if $p(|b\rangle) \in \{0, 1\}$. From the *logical indeterminacy principle* we can readily deduce the Kochen-Specker theorem by identifying each state with the observable projecting onto the linear subspace spanned by it. As noted by Hrushovski and Pitowsky [75], however, the logical indeterminacy principle is stronger than the Kochen-Specker theorem because the result is true for arbitrary frame functions which can take any value in the unit interval $[0, 1]$, but which are restricted to Boolean values for $|a\rangle, |b\rangle$. The Kochen-Specker theorem, on the other hand, is proved under the assumption that *all* observables are assigned Boolean values, as is required for a Boolean frame function.

The form of the logical indeterminacy principle makes it tempting to conclude that it permits us to locate a value indefinite observable. Indeed, if we consider the entire set of unit vectors in $\mathbb{C}^3$, fix p, and choose $|a\rangle \in \mathbb{C}^3$ such that $p(|a\rangle) = 1$, then, by the logical indeterminacy principle, for every distinct non-orthogonal unit vector $|b\rangle \in \mathbb{C}^3$ it is impossible to have $p(|b\rangle) = 1$ or $p(|b\rangle) = 0$. It thus seems that we can conclude that the observable projecting onto the subspace spanned by $|b\rangle$ is value indefinite. However, such reasoning would be incorrect. It instead shows merely the non-existence of a p assigning 1 to $|a\rangle$ and a definite value to $|b\rangle$. However, as with the Kochen-Specker theorem, this does not rule out that the observable P_b could be value definite if *other states in the set* S have value indefinite projectors since the definition of a frame function requires that p be a total function.

This means that, using the logical indeterminacy principle, we get the same global information derived in the Kochen-Specker theorem, namely that some state in S has a

corresponding value indefinite projection observable, and no more. The reason for this limitation is the definition of a frame function, which must be defined everywhere: it can model local value definiteness, but not local value indefiniteness, which, as in the Kochen-Specker theorem, emerges only as a global phenomenon.

4.2 Localising the hypotheses

We now proceed to use our notion of admissibility to localise value indefiniteness. Once again, we remind the reader that, in doing so, we work under the assumption that the set of observables considered is noncontextual (i.e., any value definite observables are noncontextual), since we wish to strengthen the implications of the Kochen-Specker theorem under this particular assumption.

By using the fact that our definition of admissibility is carefully formulated to be compatible with the existence of value indefinite observables, we are able to take a conservative approach. Specifically, rather than assuming complete value definiteness of the entire set of observables considered, we require observables to be value definite only when their indefiniteness would allow the possibility of measurements[2] violating the quantum predictions specified in condition (iii) of the Kochen-Specker theorem (see the more detailed discussion and example below).

Theorem 30 implies that we can always have one observable value definite under an admissible assignment function. Thus, for this approach to work, we instead need, as a premise, a single value definite observable and then to show that the assumption that *any other* observable is value definite leads to a contradiction with the admissibility of the value assignment function.

Fortunately, there is a very reasonable physically motivated justification for this premise: as we discussed in the previous section, if a system is prepared in an arbitrary state $|\psi\rangle \in \mathbb{C}^n$, then measurement of the observable P_ψ should yield the outcome 1. Thus, it seems perfectly reasonable to require that, if $P_\psi \in \mathcal{O}$, $v(P_\psi) = 1$. We call this the *eigenstate assumption* [3] and will discuss this in more detail in Sec. 4.4.2 when we look carefully at the connection between our formal results and their physical interpretation. Furthermore, since the critical feature of a set $\mathcal{O}$ of observables is the orthogonality relations between these observables rather than the specific form of these observables, we can hence choose our basis at will. It is thus not unreasonable to consider that some observable in $\mathcal{O}$ has the value 1, and to fix the basis used to express $\mathcal{O}$ to that of the state $|\psi\rangle$ to make this observable coincide with P_ψ.

[2] If an observable is value indefinite, this must surely imply that both outcomes are *possibilities*.

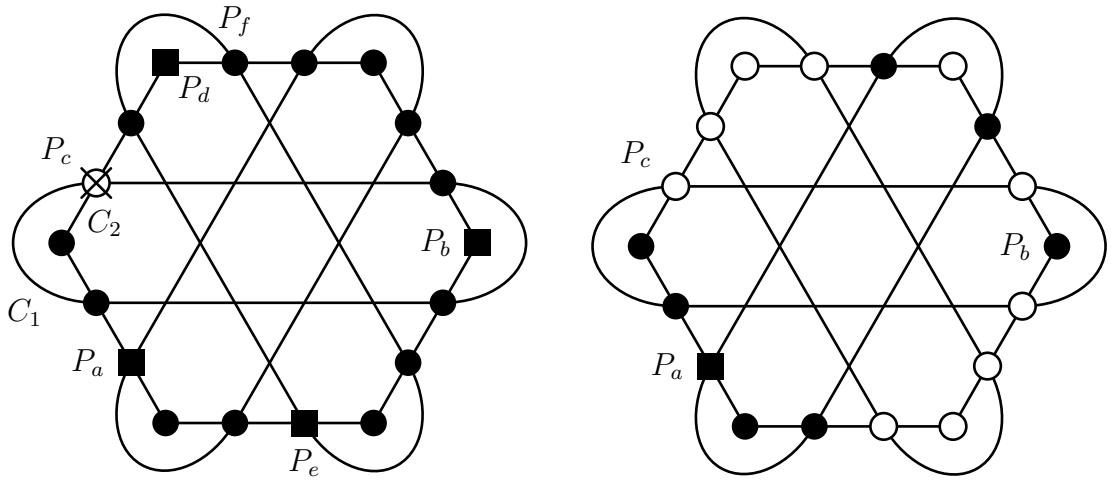


Figure 4.1: Greechie orthogonality diagram of a proof of the Kochen-Specker theorem [27]. The value of of v of each observable (node) P is represented as follows: $v(P) = 1$ – black square; $v(P) = 0$ – filled circle; $v(P)$ undefined (value indefinite) – hollow circle. (a) The contradiction arising when $v(P_a) = v(P_b) = 1$: v cannot be admissible, since this would require that $v(P_c) = 0$ and $v(P_c) = 1$ simultaneously, as shown by the cross in the diagram. (b) A possible admissible noncontextual value assignment when $v(P_a) = 1$ and $v(P_b) = 0$.

Example 33. Let us illustrate the difference between our weakened assumptions, and in particular admissibility, with the hypotheses of the Kochen-Specker theorem. This is important, as it serves to clarify the difference between our notion of admissibility and the properties of two-valued measures used in standard proofs of the Kochen-Specker theorem, as well as how the difference necessitates different reasoning in deducing a contradiction; the difference between these notions is subtle, since they coincide if complete value definiteness is assumed.

Consider the Greechie orthogonality diagram shown in Fig. 4.1, in which vertices depict observables and smooth lines or curves represent contexts. This well known diagram represents the 'orthogonality' relations between the observables used in a proof of the Kochen-Specker theorem due to Cabello et al. [27], containing only 18 observables on $\mathbb{C}^4$ and 9 contexts.

The Kochen-Specker theorem implies that there is no way to assign *every* observable in this diagram a value such that the admissibility requirements hold: that is, exactly one observable in each context should have the value 1.

Let us instead suppose not complete value definiteness, but only that $v(P_a) = v(P_b) = 1$ and that v is admissible and noncontextual, in order to try and derive a contradiction. Then, by working from P_a and P_b and applying the admissibility rule (a)

(recall Definition 27) one deduces that all observables in a context with P_a or P_b must take the value 0. One then notices that there are contexts containing 3 observables with the value 0, so we can deduce from (b) that the fourth must have the value 1. If we follow this line of reasoning, we can continue to assign values to observables in order to try and satisfy the admissibility requirements, as depicted in Fig. 4.1(a), where a black square represents the value 1, and a black circle the value 0. As we can see, by considering the contexts C_1 and C_2 we can infer that P_c must take both the values 1 and 0 respectively: both possibilities contradict the admissibility of v, as does the final possibility – that P_c is value indefinite. Thus, no admissible noncontextual v with the property that $v(P_a) = v(P_b) = 1$ exists on this set of observables. Note that, in Fig. 4.1(a), the contradiction obtained at P_c marked by the cross is a consequence of a specific succession of applications of the admissibility rules (a) and (b) in Definition 27. By applying these rules in a different order, one can obtain the contradiction also at P_d, P_e, or P_f; however, the location of the contradiction is irrelevant to the conclusion.

The most important aspect of this reasoning in this context is that it is deterministic: we proceed only by deducing the value definiteness of observables via conditions (a) and (b) in order to satisfy the admissibility of v.

Now let us assume that $v(P_a) = 1$ and $v(P_b) = 0$, as depicted in Fig. 4.1(b). We again apply condition (a) to observables commuting with P_a; however, we then see that neither (a) nor (b) can be used again to deduce the value of another observable. Normally, in proving that this diagram permits no consistent assignment of definite values, one would then proceed by assuming that one of the unfilled observables, such as P_c, must have either $v(P_c) = 1$ or $v(P_c) = 0$, and trying both possibilities. One can do this when proving the Kochen-Specker theorem since one assumes that every observable must have a definite value. However, in order to localise value indefiniteness we do not make this assumption. Hence, the value assignment in Fig. 4.1(b), with the observables represented by unfilled circles being value indefinite (e.g., $v(P_c)$ undefined) represents an admissible noncontextual value assignment.

Thus, under the assumption that $v(P_a) = 1$, the construction in Fig. 4.1 does not suffice to prove that $v(P_b)$ must be value indefinite, and hence cannot be used to localise value indefiniteness. It is not difficult to see that we reach the same conclusion irrespective of our choice of observables as P_a and P_b.

In proving the main result of this chapter, we give a set of observables for which this is the case. That is, there are observables P_a and P_b such that if $v(P_a) = 1$ then both $v(P_b) = 0$ and $v(P_b) = 1$ lead, via admissibility, to contradictions.

4.3 The localised variant of the Kochen-Specker theorem

In order to avoid arriving at the same inconclusive outcome regarding value indefiniteness as in Example 33, the contexts in the set of observables considered need to be much more carefully interconnected. Furthermore, we can only aim to prove the value indefiniteness of those observables in the specific set we consider. In order to prove a more general result, showing the value indefiniteness of a wide range of observables, we need either a set of orthogonality relationships that are realisable for many observables, or another novel approach. This second point in particular will require special attention in order to succeed in locating value indefiniteness.

The main result of this chapter, which succeeds in locating value indefiniteness, is the following theorem.

Theorem 34. *Let $n \geq 3$ and $|\psi\rangle, |\phi\rangle \in \mathbb{C}^n$ be unit vectors such that $0 < |\langle\psi|\phi\rangle| < 1$. We can effectively find a finite set of one-dimensional projection observables $\mathcal{O}$ containing P_ψ and P_ϕ for which there is no admissible noncontextual value assignment function on $\mathcal{O}$ such that $v(P_\psi) = 1$ and P_ϕ is value definite under v.*

Before we proceed to prove Theorem 34, let us first discuss some important relevant issues. We then present the proof in Section 4.3.2.

This theorem has a slightly different form from the standard Kochen-Specker theorem because of the requirement that a particular observable in the set $\mathcal{O}$ be assigned the value 1. However, since, as we will see, it is only the orthogonality relations between the observables in $\mathcal{O}$ which is important, a change of basis can always ensure that the required observable P_ψ be assigned the value 1.

In [3] we proved a restricted form of Theorem 34 which held only for $\sqrt{\frac{5}{14}} < |\langle\psi|\phi\rangle| < \frac{3}{\sqrt{14}}$, thus showing that a significant portion of, but not all, observables are value indefinite. Since we prove the extended version of this result in this chapter we will not reproduce the specific construction used for this restricted result, which is different from what we will use to prove Theorem 34; we instead refer the reader to [3] for details.

In particular, we proved the restricted result of [3] using an explicit set of orthogonality relations applicable to all observables within this restricted range. While it proved possible to produce constructions providing proofs of value indefiniteness for larger ranges of observables, new techniques were needed to extend this completely to the desired result, that is, for $0 < |\langle\psi|\phi\rangle| < 1$. In particular, as we will discuss in more detail later in Sec. 4.3.3, it seems unlikely that one can give a finite set of orthogonal relations with the desired properties, and instead constructive methods are essential in proving the more general result.

4.3.1 Insufficiency of existing Kochen-Specker diagrams

The first question to address is whether existing Kochen-Specker diagrams (i.e., Greechie diagrams specifying the orthogonality relations of $\mathcal{O}$) could be used to provide a set $\mathcal{O}$ of observables proving Theorem 34; it is not *a priori* obvious that such diagrams are unable to do so. In Example 33 we showed, as an example, that a particular simple and well-known Kochen-Specker diagram is not sufficient for this purpose. A careful search through existing diagrams [27, 80, 91, 102, 103, 135] showed that this is the case in general, and we were unable to find an existing Kochen-Specker diagram in which there are two observables P_a and P_b with the required property that if $v(P_a) = 1$, both $v(P_b) = 0$ and $v(P_b) = 1$ lead to a contradiction.

A second and deeper conceptual problem with the use of fixed Kochen-Specker diagrams as in existing proofs is the following. Since, in order to derive a contradiction, we need to assume that an observable P_ψ in the given set of observables has $v(P_\psi) = 1$, this limits the observables which can be shown to be value indefinite to, at best, the remaining ones in $\mathcal{O} \setminus \{P_\psi\}$. However, we wish to prove more: that *every* observable not commuting with P_ψ is value indefinite.

As a result, we need not only a set of observables with the required properties discussed above, but furthermore an approach to generalise this set of observables to arbitrary other observables. We overcome this apparent lack of generality via a method of reductions, which we present in the next section and will return to discuss later on.

4.3.2 Proof of Theorem 34

We prove Theorem 34 in three main steps:

1. We first prove it for the special case that $|\langle\psi|\phi\rangle| = \frac{1}{\sqrt{2}}$. We proved a similar result (for $|\langle\psi|\phi\rangle| = \frac{3}{\sqrt{14}}$) in [3], but this involved two separate diagrams applying to separate cases. Here we give a single diagram providing a much more compact, clear proof.

2. We prove a simple reduction for $0 < |\langle\psi|\phi\rangle| < \frac{1}{\sqrt{2}}$ to the first case.

3. The third and main part of the proof involves finding a reduction in the opposite sense, applying to the final case of $\frac{1}{\sqrt{2}} < |\langle\psi|\phi\rangle| < 1$. It is this final reduction allowing the complete proof that is the most involved technical aspect of the proof.

As is standard in Kochen-Specker proofs [24], we will work directly in the three-dimensional case of $\mathbb{C}^3$, since the case for $n > 3$ can be simply reduced to this situation.[3]

[3]In fact, only $\mathbb{R}^3$ is needed, since the orthogonality relationships we give can be expressed in $\mathbb{R}^3$.

Lemma 35. *Given any two unit vectors* $|a\rangle, |b\rangle \in \mathbb{C}^3$ *with* $|\langle a|b\rangle| = \frac{1}{\sqrt{2}}$ *there exists a finite set of observables* $\mathcal{O}$ *such that if* $v(P_a) = 1$ *then* P_b *is value indefinite under every admissible noncontextual assignment function* v *on* $\mathcal{O}$.

Proof. By choosing an appropriate basis we can assume, without loss of generality, that $|a\rangle = (1, 0, 0)$ and $|b\rangle = \frac{1}{2}(1, \sqrt{2}, 1)$. Let us consider the set $\mathcal{O} = \{P_a, P_b, P_i;\ i = 1, \ldots, 35\}$ of rank-1 projection observables where the vectors $|i\rangle$ for $i = 1, \ldots, 35$ are defined in Table 4.1 (with the normalisation factors emitted for simplicity). The orthogonality relations between these vectors gives the 26 contexts shown in Table 4.2. Note that these observables are quite 'tightly' connected: the context-observable ratio is relatively high. The Greechie diagram showing these orthogonality relations is shown in Fig. 4.2.

Table 4.1: The 37 vectors specifying the observables used in the proof of Lemma 35, with normalisation factors omitted.

$\|a\rangle = (1,0,0)$	$\|b\rangle = (\sqrt{2},1,1)$	$\|1\rangle = (0,1,1)$	$\|2\rangle = (0,1,-1)$
$\|3\rangle = (\sqrt{2},-1,-1)$	$\|4\rangle = (0,0,1)$	$\|5\rangle = (0,1,0)$	$\|6\rangle = (\sqrt{2},1,-3)$
$\|7\rangle = (1,-\sqrt{2},0)$	$\|8\rangle = (\sqrt{2},-3,1)$	$\|9\rangle = (1,0,-\sqrt{2})$	$\|10\rangle = (\sqrt{2},1,0)$
$\|11\rangle = (\sqrt{2},0,1)$	$\|12\rangle = (\sqrt{2},-2,-3)$	$\|13\rangle = (1,-\sqrt{2},\sqrt{2})$	$\|14\rangle = (\sqrt{2},-3,-2)$
$\|15\rangle = (1,\sqrt{2},-\sqrt{2})$	$\|16\rangle = (\sqrt{8},1,-1)$	$\|17\rangle = (\sqrt{8},-1,1)$	$\|18\rangle = (\sqrt{2},-7,-3)$
$\|19\rangle = (\sqrt{2},-1,3)$	$\|20\rangle = (\sqrt{2},-3,-7)$	$\|21\rangle = (\sqrt{2},3,-1)$	$\|22\rangle = (1,\sqrt{2},0)$
$\|23\rangle = (1,0,\sqrt{2})$	$\|24\rangle = (\sqrt{2},-1,-3)$	$\|25\rangle = (\sqrt{2},-1,1)$	$\|26\rangle = (\sqrt{2},-3,-1)$
$\|27\rangle = (\sqrt{2},1,-1)$	$\|28\rangle = (\sqrt{2},-1,0)$	$\|29\rangle = (\sqrt{2},0,-1)$	$\|30\rangle = (\sqrt{2},2,3)$
$\|31\rangle = (\sqrt{2},3,2)$	$\|32\rangle = (\sqrt{2},3,7)$	$\|33\rangle = (\sqrt{2},7,3)$	$\|34\rangle = (\sqrt{2},1,3)$
$\|35\rangle = (\sqrt{2},3,1)$			

Table 4.2: The 26 contexts used in the proof of Lemma 35.

$C_1 = \{P_a, P_1, P_2\}$	$C_2 = \{P_a, P_4, P_5\}$	$C_3 = \{P_b, P_2, P_3\}$	$C_4 = \{P_b, P_6, P_7\}$
$C_5 = \{P_b, P_8, P_9\}$	$C_6 = \{P_4, P_7, P_{10}\}$	$C_7 = \{P_5, P_9, P_{11}\}$	$C_8 = \{P_{10}, P_{12}, P_{13}\}$
$C_9 = \{P_{11}, P_{14}, P_{15}\}$	$C_{10} = \{P_1, P_{13}, P_{16}\}$	$C_{11} = \{P_1, P_{15}, P_{17}\}$	$C_{12} = \{P_{16}, P_{18}, P_{19}\}$
$C_{13} = \{P_{17}, P_{20}, P_{21}\}$	$C_{14} = \{P_3, P_{19}, P_{22}\}$	$C_{15} = \{P_3, P_{21}, P_{23}\}$	$C_{16} = \{P_{22}, P_{24}, P_{25}\}$
$C_{17} = \{P_{23}, P_{26}, P_{27}\}$	$C_{18} = \{P_4, P_{22}, P_{28}\}$	$C_{19} = \{P_5, P_{23}, P_{29}\}$	$C_{20} = \{P_{15}, P_{28}, P_{30}\}$
$C_{21} = \{P_{13}, P_{29}, P_{31}\}$	$C_{22} = \{P_8, P_{16}, P_{32}\}$	$C_{23} = \{P_6, P_{17}, P_{33}\}$	$C_{24} = \{P_7, P_{27}, P_{34}\}$
$C_{25} = \{P_9, P_{25}, P_{35}\}$	$C_{26} = \{P_1, P_{25}, P_{27}\}$		

Let us assume, for the sake of contradiction, that an admissible noncontextual v exists for $\mathcal{O}$, with $v(P_a) = 1$ and $v(P_b)$ defined (i.e., P_b value definite). Then there are two cases: $v(P_b) = 1$ or $v(P_b) = 0$.

Observables projecting onto complex linear subspaces can thus be handled by a simple change of basis to the set of observables defining the orthogonality relations.

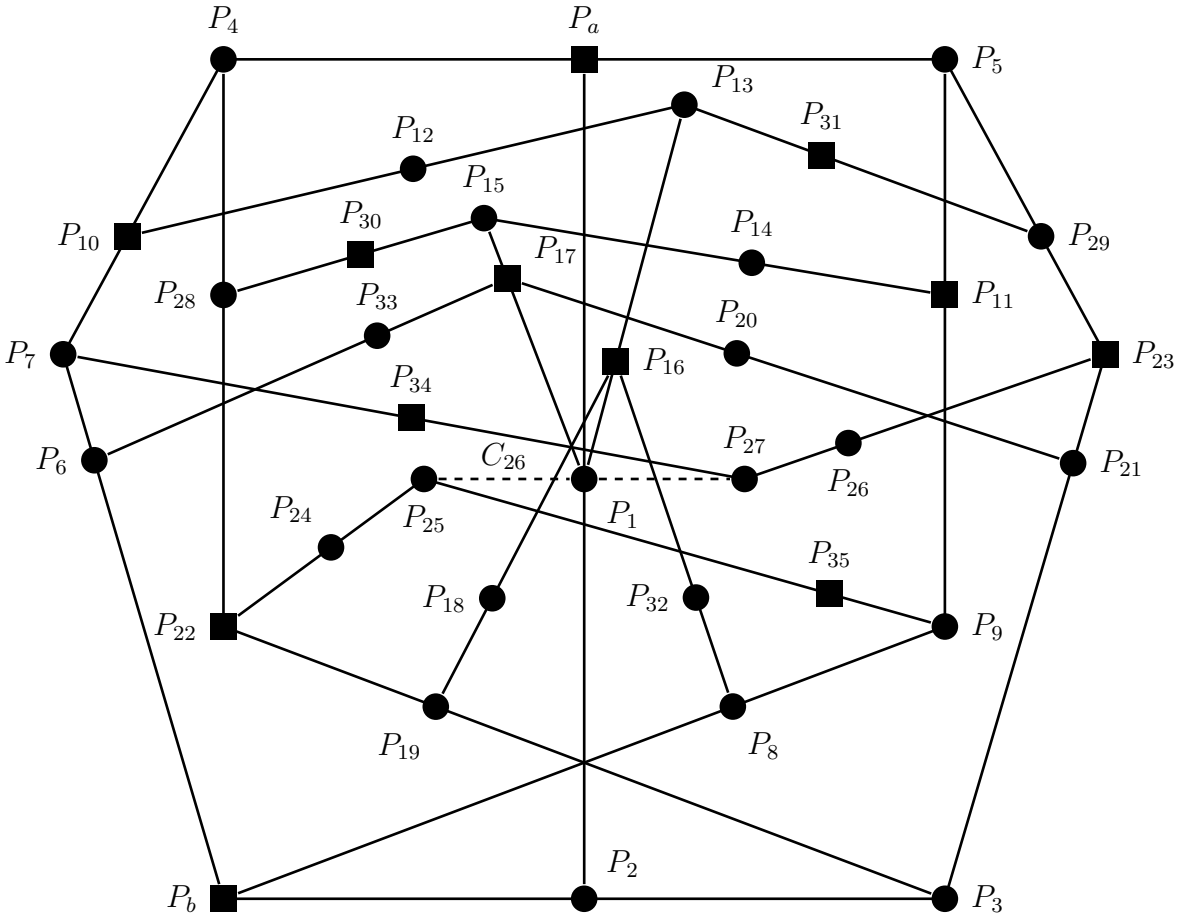


Figure 4.2: Greechie diagram showing the orthogonality relation between the observables in Table 4.1. We have shown the deduction of values for any admissible noncontextual v satisfying $v(P_a) = v(P_b) = 1$, where black squares represent the value 1, and circles the value 0. Observe that the context C_{26}, shown dotted, contains three observables with the value 0, and hence v is not admissible.

Case 1: $v(P_b) = 1$. Since $P_a \in C_1, C_2$ and $v(P_a) = 1$, admissibility requires that $v(P_1) = v(P_2) = v(P_4) = v(P_5) = 0$. Similarly, since $P_b \in C_3, C_4, C_5$ we have $v(P_3) = v(P_6) = v(P_7) = v(P_8) = v(P_9) = 0$. Since $v(P_4) = v(P_7) = 0$, admissibility in C_6 means that we must have $v(P_{10}) = 1$; similarly $v(P_{11}) = 1$ also. This chain of reasoning can be continued, applying the admissibility rules from Definition 27 one context at a time, as shown in Table 4.3. In this table, where the leftmost column indicates the value of v on the given observables, the values shown in bold in each column (context) are deduced from the admissibility rules based on the values of the other observables in the context which have already been deduced in the preceding columns. Note that, at each step, admissibility requires, deterministically, that certain observables take particular values; we never proceed by reasoning that $v(P_i)$ must be either 0 or 1 for some P_i as is common in proofs of the standard Kochen-Specker theorem (except for P_b, where

this is exactly the assumption that P_b is value definite), because this is not required by admissibility. Eventually, as we see, we deduce that $v(P_1) = v(P_{25}) = v(P_{27}) = 0$. But since $C_{26} = \{P_1, P_{25}, P_{27}\}$, this contradicts the admissibility of v.

Table 4.3: The values that must be taken for the shown observables under any admissible noncontextual assignment function v satisfying $v(P_a) = v(P_b) = 1$. The value (shown in the leftmost column) for observables in bold is deduced from the admissibility rules and observables appearing in columns to the left of that observable in the table, or from the assumption that $v(P_a) = v(P_b) = 1$.

v	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}
1	P_a	P_a	P_b	P_b	P_b	$\boldsymbol{P}_{10}$	$\boldsymbol{P}_{11}$	P_{10}	P_{11}	$\boldsymbol{P}_{16}$	$\boldsymbol{P}_{17}$	P_{16}	P_{17}	$\boldsymbol{P}_{22}$	$\boldsymbol{P}_{23}$	P_{22}	P_{23}
0	$\boldsymbol{P}_1$	$\boldsymbol{P}_4$	P_2	$\boldsymbol{P}_6$	$\boldsymbol{P}_8$	P_4	P_5	$\boldsymbol{P}_{12}$	$\boldsymbol{P}_{14}$	P_1	P_1	$\boldsymbol{P}_{18}$	$\boldsymbol{P}_{20}$	P_3	P_3	$\boldsymbol{P}_{24}$	$\boldsymbol{P}_{26}$
0	$\boldsymbol{P}_2$	$\boldsymbol{P}_5$	$\boldsymbol{P}_3$	$\boldsymbol{P}_7$	$\boldsymbol{P}_9$	P_7	P_9	$\boldsymbol{P}_{13}$	$\boldsymbol{P}_{15}$	P_{13}	P_{15}	$\boldsymbol{P}_{19}$	$\boldsymbol{P}_{21}$	P_{19}	P_{21}	$\boldsymbol{P}_{25}$	$\boldsymbol{P}_{27}$

Case 2: $v(P_b) = 0$. By following a similar line of reasoning, shown in Table 4.4, we once again deduce that $v(P_1) = v(P_{25}) = v(P_{27}) = 0$, a contradiction.

Table 4.4: The values that must be taken for the shown observables under any admissible noncontextual assignment function v satisfying $v(P_a) = 1$ and $v(P_b) = 0$.

v	C_1	C_2	C_3	C_{14}	C_{15}	C_{18}	C_{19}	C_{20}	C_{21}	C_{10}	C_{11}	C_{22}	C_{23}	C_4	C_5	C_{24}	C_{25}
1	P_a	P_a	$\boldsymbol{P}_3$	P_3	P_3	$\boldsymbol{P}_{28}$	$\boldsymbol{P}_{29}$	P_{28}	P_{29}	$\boldsymbol{P}_{16}$	$\boldsymbol{P}_{17}$	P_{16}	P_{17}	$\boldsymbol{P}_7$	$\boldsymbol{P}_9$	P_7	P_9
0	$\boldsymbol{P}_1$	$\boldsymbol{P}_4$	P_b	$\boldsymbol{P}_{19}$	$\boldsymbol{P}_{21}$	P_4	P_5	$\boldsymbol{P}_{15}$	$\boldsymbol{P}_{13}$	P_1	P_1	$\boldsymbol{P}_8$	$\boldsymbol{P}_6$	P_b	P_b	$\boldsymbol{P}_{27}$	$\boldsymbol{P}_{25}$
0	$\boldsymbol{P}_2$	$\boldsymbol{P}_5$	P_2	$\boldsymbol{P}_{22}$	$\boldsymbol{P}_{23}$	P_{22}	P_{23}	$\boldsymbol{P}_{30}$	$\boldsymbol{P}_{31}$	P_{13}	P_{15}	$\boldsymbol{P}_{32}$	$\boldsymbol{P}_{33}$	P_6	P_8	$\boldsymbol{P}_{34}$	$\boldsymbol{P}_{35}$

Hence, we must conclude that P_b cannot be value definite if v is admissible on $\mathcal{O}$ with $v(P_a) = 1$. □

We next show a 'contraction' lemma that constitutes a simple 'forcing' of value definiteness: given P_a and P_b with $v(P_a) = v(P_b) = 1$, there is a $|c\rangle$ which is 'closer' (i.e., at a smaller angle of our choosing; contracted) to both $|a\rangle$ and $|b\rangle$, for which $v(P_c) = 1$ as well if v is admissible. The form of the vectors $|c_\pm\rangle$ specified in the lemma will be used several times in the rest of the proof of Theorem 34.

Lemma 36. *Given any two unit vectors* $|a\rangle, |b\rangle \in \mathbb{C}^3$ *with* $0 < |\langle a|b\rangle| < 1$ *and* $z \in \mathbb{C}$ *such that* $|\langle a|b\rangle| < |z| < 1$, *we can effectively find a unit vector* $|c\rangle$ *with* $\langle a|c\rangle = z$, *and a finite set of observables* $\mathcal{O}$ *containing* P_a, P_b, P_c *such that if* $v(P_a) = v(P_b) = 1$, *then* $v(P_c) = 1$ *for every admissible noncontextual assignment function* v *on* $\mathcal{O}$.

Furthermore, if we choose our basis such that $|a\rangle = (0, 0, 1)$ *and* $|b\rangle = (\sqrt{1 - |p|^2}, 0, p)$, *where* $p = \langle a|b\rangle$, *then* $|c\rangle$ *can only be one of the following two vectors:* $|c_\pm\rangle = (x, \pm y, z)$, *where* $z = \langle a|c\rangle$, $x = p(1 - z^2)/(z\sqrt{1 - p^2})$ *and* $y = \sqrt{1 - x^2 - z^2}$.

Proof. Without loss of generality, we assume the $\langle a|b\rangle \in \mathbb{R}$ and choose a basis so that $|a\rangle = (0,0,1)$ and $|b\rangle = (q,0,p)$ where $p = \langle a|b\rangle$ and $q = \sqrt{1-p^2}$.

Note that, since $p < |z|$ and thus $p^2 < z^2$ we have

$$\frac{p^2(1-z^2)}{q^2z^2} = \frac{p^2 - p^2z^2}{q^2z^2} < \frac{z^2 - p^2z^2}{q^2z^2} = \frac{(1-p^2)z^2}{q^2z^2} = 1.$$

If we let $x = \frac{p(1-z^2)}{qz}$ we thus have

$$x^2 = \frac{p^2(1-z^2)}{q^2z^2}(1-z^2) < 1 - z^2.$$

We can then set $y = \sqrt{1-x^2-z^2} \in \mathbb{R}$, making $|c\rangle = (x,y,z)$ a unit vector such that $\langle a|c\rangle = z$.

Let $|\alpha\rangle = |a\rangle \times |c\rangle = (-y,x,0)$, $|\beta\rangle = |b\rangle \times |c\rangle = (-py, px - qz, qy)$ and note that $\langle \alpha|\beta\rangle = 0$ also. Thus, if we let $|\alpha'\rangle = |a\rangle \times |\alpha\rangle$ and $|\beta'\rangle = |b\rangle \times |\beta'\rangle$, then $\{|a\rangle, |\alpha\rangle, |\alpha'\rangle\}$, $\{|b\rangle, |\beta\rangle, |\beta'\rangle\}$ and $\{|\alpha\rangle, |\beta\rangle, |c\rangle\}$ are all orthonormal bases for $\mathbb{R}^3$ and thus $C_1 = \{P_\alpha, P_\beta, P_c\}$, $C_2 = \{P_a, P_\alpha, P_{\alpha'}\}$ and $C_3 = \{P_b, P_\beta, P_{\beta'}\}$ are all contexts in $\mathcal{O} = C_1 \cup C_2 \cup C_3$. This construction is illustrated in Fig. 4.3.

If v is an admissible noncontextual assignment function on $\mathcal{O}$ with $v(P_a) = v(P_b) = 1$ then we must have $v(P_\alpha) = v(P_\beta) = 0$ and hence $v(P_c) = 1$, as required. □

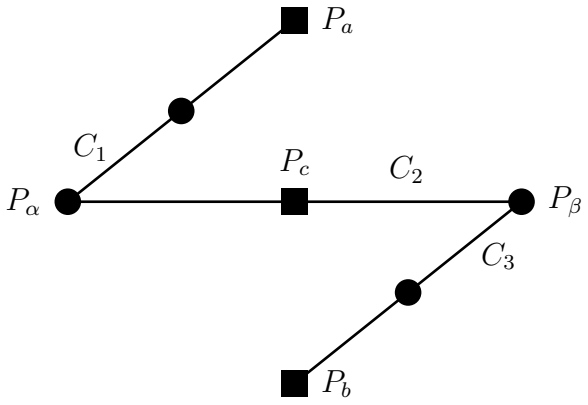


Figure 4.3: Greechie orthogonality diagram with an overlaid value assignment that illustrates the reduction in Lemma 36. Once again, the circles and squares represent observables that have the values 0 and 1 respectively.

The final part of the proof, finding from $|a\rangle, |b\rangle$ a vector $|c\rangle$ for which we must have $v(P_c) = 1$, and which is further apart from $|a\rangle$ than $|b\rangle$ is from $|a\rangle$, is the most challenging. Despite searching via many different methods, we were unable to find a single Greechie diagram specifying such a set of observables with the required constraints as we did in Lemma 36. Indeed, as we will discuss later, we conjecture that it is impossible

to do so. Rather, we use an iterated (constructive) approach to give the required set of observables for any particular $|c\rangle$.

We prove such a result in the following lemma, which was originally published in [4], with the help of computational analysis. We then prove a similar approach using a slightly different, but purely analytic approach. The computational proof, while perhaps less rigorous in the sense that it relies on the computational analysis of certain functions, is more illustrative and intuitive, thus helping to understand this crucial aspect of the proof of Theorem 34. The presentation of these two approaches follows the historical approach to the problem [4, 7].

4.3.2.1 Computational approach

The idea behind this approach comes from realising that, in the proof of Lemma 35, we start with $v(P_a) = v(P_b) = 1$ and derive $v(P_{v_{22}}) = 1$, where $\langle a|v_{22}\rangle = \frac{1}{\sqrt{3}} < \frac{1}{\sqrt{2}} = \langle a|b\rangle$. This thus constitutes an explicit case of an expansion (in angle) between observables that must be assigned the value 1, and if we extract the intermediary vectors required, we obtain the Greechie diagram shown in Fig. 4.4, where in the specific case discussed we have $|c\rangle = |v_{22}\rangle$.

In order to generalise this to arbitrary vectors $|b\rangle$ with $\langle a|b\rangle > \frac{1}{\sqrt{2}}$, we scale the *angles* between the vectors accordingly in a way in which we will soon make precise.

Note that Fig. 4.4 is constructed by 'gluing' together three copies of the reduction used in Lemma 36 and shown in Figure 4.3. It is thus realisable as long as $\langle a|b\rangle < \langle a|v_1\rangle$, $\langle a|v_1\rangle < \langle a|v_2\rangle$ and $\langle b|v_2\rangle < \langle b|c\rangle$, which is ensured to be true by the way we scale the vectors.

This reduction only allows us to find a $|c\rangle$ with $v(P_c) = 1$ which is only slightly further from $|a\rangle$ than $|b\rangle$ was. In order to expand the angle sufficiently, we thus have to iterate this procedure, applying it again with $|c\rangle$ as our new $|b\rangle$, until the angle is sufficiently large.

We break this into two lemmata: the first gives the general expansion, and then the second shows that we can iterate this expansion as required.

Lemma 37. *Given any two unit vectors $|a\rangle, |b\rangle \in \mathbb{C}^3$ with $\frac{1}{\sqrt{2}} < |\langle a|b\rangle| < 1$, we can effectively find a unit vector $|c\rangle$ with $0 < |\langle a|c\rangle| < |\langle a|b\rangle$ and a finite set of one-dimension projection observables $\mathcal{O}$ containing P_a, P_b, P_c such that if $v(P_a) = v(P_b) = 1$, then $v(P_c) = 1$, for every admissible noncontextual value assignment function v on $\mathcal{O}$.*

Proof. The constants which will be used for scaling, obtained from the reduction shown

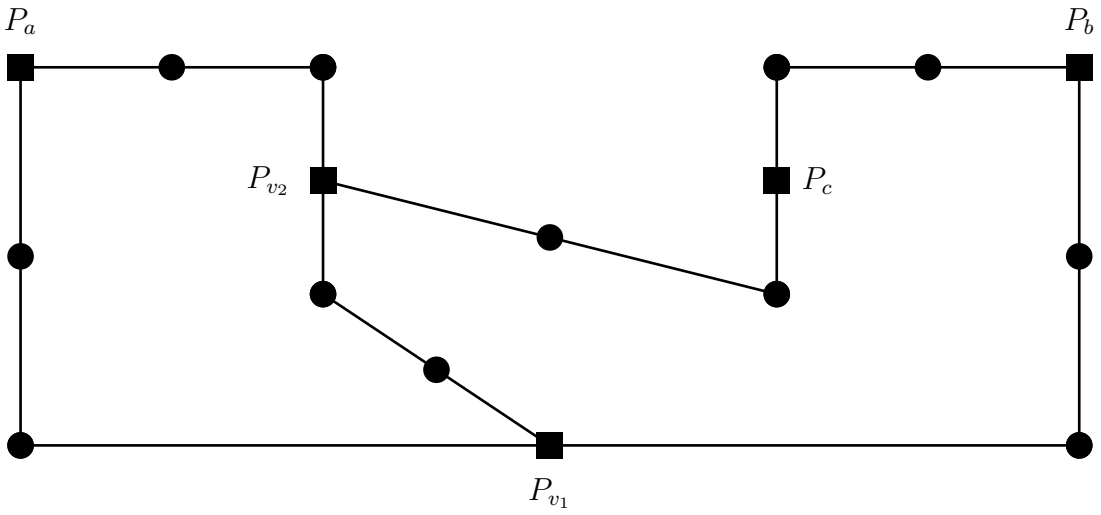


Figure 4.4: Greechie orthogonality diagram with an overlaid value assignment showing the reduction used in the computational proof of Lemma 37.

in Figure 4.4 and Table 4.1, are as follows:

$$\alpha_1 = \frac{\arccos\sqrt{\frac{2}{3}}}{\arccos\frac{1}{\sqrt{2}}}, \qquad \alpha_2 = \frac{\arccos\frac{2}{\sqrt{5}}}{\arccos\sqrt{\frac{2}{3}}}, \qquad \alpha_3 = \frac{\arccos\sqrt{\frac{2}{3}}}{\arccos\sqrt{\frac{2}{5}}}.$$

α_1, for example, is the ratio of the angle between $|a\rangle$ and $|b\rangle$ to the angle between $|a\rangle$ and $|c\rangle$; the others are found similarly. Given the initial vectors $|a\rangle$, $|b\rangle$ and the above constants, we thus make use of the following scaled angles between the relevant observables:

$$\theta_{a,b} = \arccos\langle a|b\rangle, \qquad \theta_{a,v_1} = \alpha_1\theta_{a,b}, \qquad \theta_{a,v_2} = \alpha_2\theta_{a,v_1}.$$

Once the form of $|v_2\rangle$ is determined via the procedure to follow, we take the following:

$$\theta_{b,v_2} = \arccos\langle b|v_2\rangle, \qquad \theta_{b,c} = \alpha_3\theta_{b,v_2}.$$

Without loss of generality, we assume $\langle a|b\rangle \in \mathbb{R}$ and fix our basis so that $|a\rangle = (1,0,0)$ and $|b\rangle = (p_1, q_1, 0)$ where $p_1 = \langle a|b\rangle$ and $q_1 = \sqrt{1-p_1^2}$. In order to show that $v(P_c) = 1$, we need find the form of the vectors $|v_1\rangle, |v_2\rangle, |c\rangle$ that satisfy the orthogonality relations shown in Fig. 4.4.

Following our scaling procedure, we want to choose $|v_1\rangle$ so that $\langle a|v_1\rangle = x_1 = \cos\theta_{a,v_1}$. From Lemma 36 we know this is possible since $x_1 > p_1$ (because $\alpha_1 < 1$), and we thus have $|v_1\rangle = (x_1, y_1, z_1)$, where $y_1 = p_1(1-x_1^2)/q_1x_1$ and $z_1 = \sqrt{1-x_1^2-y_1^2}$.

We now want to find the form of the vector $|v_2\rangle$, once again using Lemma 36 to guarantee the orthogonality constraints are satisfied, such that $\langle a|v_2\rangle = x_2 = \cos\theta_{a,v_2}$

(this is possible since $\alpha_2 < 1$). In order to use the same general form (specified in Lemma 36) as above, we perform a change of basis to bring $|v_1\rangle$ into the xy-plane, describe $|v_2\rangle$ in this basis using the above result, then perform the inverse change of basis. Our new basis vectors $|e_2\rangle, |f_2\rangle, |g_2\rangle$ are given by $|e_2\rangle = (1,0,0)$,

$$|f_2\rangle = (|v_1\rangle - x_1 |e_2\rangle)/q_2 = (0, y_1/q_2, z_1/q_2)$$

where $q_2 = \sqrt{1-x_1^2}$, and $|g_2\rangle = |e_2\rangle \times |f_2\rangle = (0, z_1/q_2, -y_1/q_2)$. We thus have the transformation matrix

$$T_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & y_1/q_2 & z_1/q_2 \\ 0 & z_1/q_2 & -y_1/q_2 \end{pmatrix}.$$

We can now put $y_2 = x_1(1-x_2^2)/q_2 x_2$ and $z_2 = \sqrt{1-x_2^2-y_2^2}$ so that in our original basis we have

$$|v_2\rangle = T_1(x_2, y_2, -z_2)^t = \left(x_2, \frac{y_1 y_2 - z_1 z_2}{q_2}, \frac{y_2 z_1 + y_1 z_2}{q_2}\right).$$

We note at this point that the constant θ_{b,v_2} is now determined, and we have

$$\langle b|v_2\rangle = p_1 x_2 + \frac{q_1}{q_2}(y_1 y_2 - z_1 z_2).$$

The final step is to apply Lemma 36 a third time to find the form of $|c\rangle$ such that $\langle b|c\rangle = x_3 = \cos\theta_{b,c}$ (again, such a $|c\rangle$ with the required orthogonality relations exists, since $\alpha_3 < 1$). Let $p_3 = \langle b|v_2\rangle$ and $q_3 = \sqrt{1-p_3^2}$. Again we perform a basis transformation, this time to the basis defined by $|e_3\rangle = |b\rangle = (p_1, q_1, 0)$,

$$\begin{aligned} |f_3\rangle &= (|v_2\rangle - p_3 |b\rangle)/k \\ &= \left(x_2 - p_3 p_1, \frac{(y_1 y_2 - z_1 z_2)}{q_2} - p_3 q_1, \frac{(y_2 z_1 + y_1 z_2)}{q_2}\right)/k, \end{aligned}$$

where k is a constant such that $|f_3\rangle$ is normalised, that is,

$$k = \sqrt{(x_2 - p_3 p_1)^2 + \left(\frac{(y_1 y_2 - z_1 z_2)}{q_2} - p_3 q_1\right)^2 + \left(\frac{y_2 z_1 + y_1 z_2}{q_2}\right)^2},$$

and

$$\begin{aligned} |g_3\rangle &= |e_3\rangle \times |f_3\rangle \\ &= \left(\frac{q_1}{q_2}(y_2 z_1 + y_1 z_2), \frac{-p_1}{q_2}(y_2 z_1 + y_1 z_2), \frac{p_1}{q_2}(y_1 y_2 - z_1 z_2) - q_1 x_2\right)/k. \end{aligned}$$

The transformation matrix is then given by

$$T_3 = \begin{pmatrix} p_1 & \frac{x_2 - p_3 p_1}{k} & \frac{q_1(y_2 z_1 + y_1 z_2)}{q_2 k} \\ q_1 & \frac{y_1 y_2 - z_1 z_2 - p_3 q_1 q_2}{q_2 k} & \frac{-p_1(y_2 z_1 + y_1 z_2)}{q_2 k} \\ 0 & \frac{y_2 z_1 + y_1 z_2}{q_2 k} & \frac{p_1(y_1 y_2 - z_1 z_2) - x_2 q_1 q_2}{q_2 k} \end{pmatrix}.$$

We now put $y_3 = p_3(1-x_3^2)/q_3x_3$ and $z_3 = \sqrt{1-x_3^2-y_3^2}$ so that in the original basis we have

$$\begin{aligned}|c\rangle =& T_3(x_3, y_3, -z_3)^t \\ =& \Bigg(x_3p_1 + \frac{y_3}{k}(x_2 - p_1p_3) - \frac{q_1z_3}{kq_2}(y_2z_1 + y_1z_2), \\ & x_3q_1 + \frac{y_3}{kq_2}(y_1y_2 - z_1z_2 - p_3q_1q_2) + \frac{z_3p_1}{kq_2}(y_2z_1 + y_1z_2), \\ & \frac{y_3}{kq_2}(y_2z_1 + y_1z_2) - \frac{z_3}{k}\left[\frac{p_1}{q_2}(y_1y_2 - z_1z_2) - q_1x_2\right]\Bigg). \end{aligned} \tag{1}$$

We thus need to prove that $\langle a|c\rangle < \langle a|b\rangle = p_1$, where

$$\langle a|c\rangle = x_3p_1 + \frac{y_3}{k}(x_2 - p_1p_3) - \frac{q_1z_3}{kq_2}(y_2z_1 + y_1z_2). \tag{2}$$

Note that only the first coordinate of the vector $|c\rangle$ in (1) is of importance for this. The product $\langle a|c\rangle$ is, with appropriate substitutions, a function of one variable, p_1; let us denote $f(p_1) = \langle a|c\rangle$. We thus need to determine if, for $p_1 \in \left(\frac{1}{\sqrt{2}}, 1\right)$, the inequality $f(p_1) < p_1$ holds. Unfortunately, once the appropriate substitutions are made, it takes several pages to write $f(p_1)$ in terms of p_1 only, involving several nested trigonometric and inverse-trigonometric functions, and a direct analytic analysis proved intractable, even with the aid of computer algebra systems.

Using symbolic calculation in Mathematica (see Appendix A for the code and full details) for a Taylor series expansion around $p_1 = 1$, we find that for small $|p_1 - 1|$,

$$f(p_1) = 1 - m(1-p_1) + \mathcal{O}\left((p_1-1)^2\right),$$

where $m \approx 1.27$ is a constant. Hence $\lim_{p_1\to 1^-} f(p_1) = 1$ as claimed and for some $\varepsilon > 0$ we have $f(p_1) < p_1$ for $p_1 \in (1-\varepsilon, 1)$. Further, the continuity of f on this domain can be readily guaranteed by verifying the continuity of each individual term as a function of p_1 on its respective domain (see Appendix A for details). From Figure 4.5 and the above results it follows that to prove the inequality $f(p_1) < p_1$ for all $p_1 \in \left(\frac{1}{\sqrt{2}}, 1\right)$ we need to show that for no $p_1 \to 1$ (which implies $f(p_1) \to p_1$) we have $f(p_1) > p_1$.

Since we know from the Taylor series expansion that $f(p_1) < p_1$ in the neighbourhood of $p_1 = 1$, if for some $p_1' \in \left(\frac{1}{\sqrt{2}}, 1\right)$ we were to have $f(p_1') > p_1'$, then for some p_1'' we must have $\frac{\mathrm{d}}{\mathrm{d}p_1} f(p_1'') < 1$, which can be seen to be false from Fig. 4.6, as required.

Thus, there exists a set of observables $\mathcal{O}$, with $\{P_a, P_b, P_{v_1}, P_{v_2}, P_c\} \subset \mathcal{O}$ such that, under any admissible noncontextual value assignment function on $\mathcal{O}$ with $v(P_a) = v(P_b) = 1$, we must have $v(P_c) = 1$ also, and $\langle a|c\rangle < \langle a|b\rangle$ as required. □

We now prove that we can iterate Lemma 37 in order to find a vector $|c\rangle$ sufficiently far from $|a\rangle$.

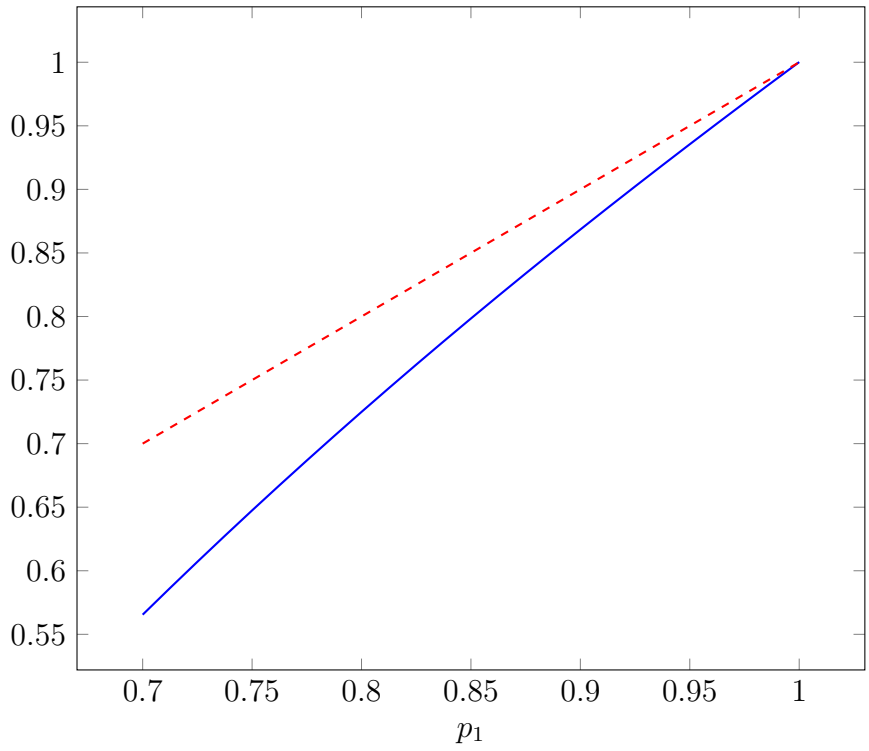


Figure 4.5: Plot of p_1 (dashed red line) and $f(p_1)$ (solid blue line) for $p_1 \in (0.7, 1) \supset \left(\frac{1}{\sqrt{2}}, 1\right)$.

Lemma 38. *Given any two unit vectors $|a\rangle, |b\rangle \in \mathbb{C}^3$ with $\frac{1}{\sqrt{2}} < |\langle a|b\rangle| < 1$, we can effectively find a unit vector $|c\rangle$ with $0 < |\langle a|c\rangle| \leq \frac{1}{\sqrt{2}}$ and a finite set of one-dimensional projection observables $\mathcal{O}$ containing P_a, P_b, P_c such that if $v(P_a) = v(P_b) = 1$, then $v(P_c) = 1$, for every admissible, noncontextual assignment function v on $\mathcal{O}$.*

Proof. We prove by iterating Lemma 37, and use the notation $|c_0\rangle \equiv |b\rangle$ to indicate the 0th iteration. We start with $|c_0\rangle$ and for each $i \geq 0$, as long as $\langle a|c_i\rangle > \frac{1}{\sqrt{2}}$, apply the construction used in the proof of Lemma 37 to generate $|c_{i+1}\rangle$ for the next iteration.

Let $r_i = \langle a|c_i\rangle$. Then, as in Lemma 37, taking the function $f(p_1)$ as defined in (2) (recall that $\langle a|c\rangle$ was a function of p_1 only and hence $\langle a|c_{i+1}\rangle$ depends only on r_i), we have $f(r_i) < r_i$ for $i \geq 1$. Furthermore, as a result of iteration, $\langle a|c_i\rangle = f^i(r_0)$ for $i \geq 1$.

It remains to show that this iteration in fact terminates with the desired condition. That is, that for some finite $n > 0$ we have $f^n(r_0) \leq \frac{1}{\sqrt{2}}$.

However, from Figure 4.5 along with the fact that the derivative $\frac{\mathrm{d}f}{\mathrm{d}p_1}$ is positive, as seen in Fig. 4.6, the difference $p_1 - f(p_1)$ is strictly decreasing with p_1 on $\left(\frac{1}{\sqrt{2}}, 1\right) \subset (0.7, 1)$. Finally, since we can also see that $f(\frac{1}{\sqrt{2}}) > 0$, it follows that for a finite n we indeed have $f^n(r_0) \in \left(0, \frac{1}{\sqrt{2}}\right]$ as required.

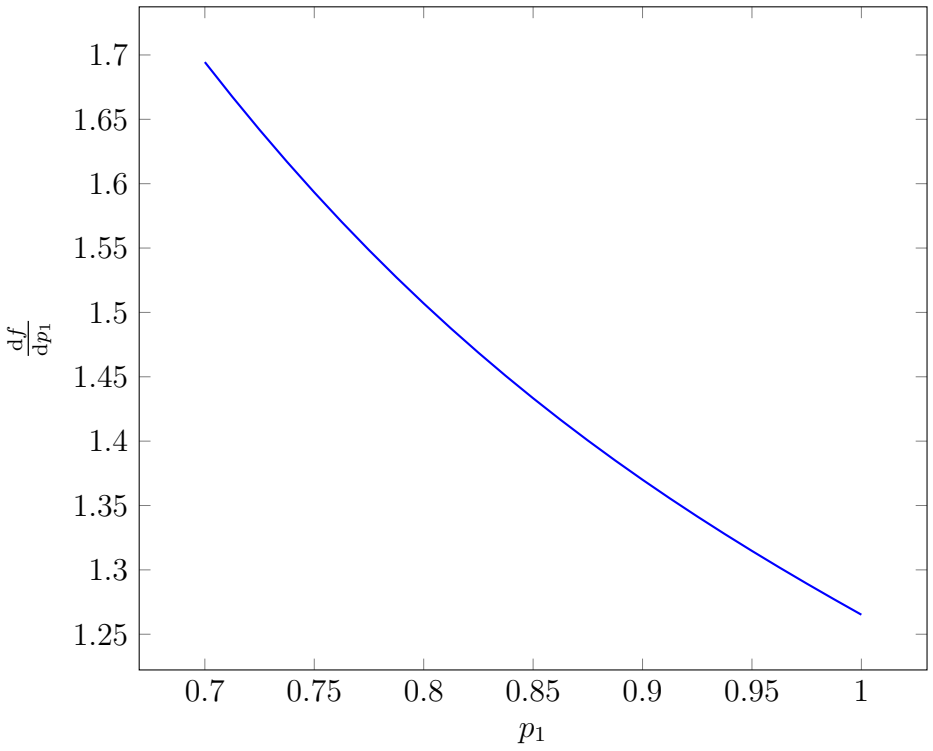


Figure 4.6: Plot of $\frac{df}{dp_1}$ for $p_1 \in (0.7, 1) \supset \left(\frac{1}{\sqrt{2}}, 1\right)$.

By Lemma 37, for each $i = 0, \ldots, n-1$ there exists a set $\mathcal{O}_i$ of projection observables such that $v(P_{c_i+1}) = 1$ under any admissible noncontextual v on $\mathcal{O}_i$ satisfying $v(P_a) = v(P_{c_i}) = 1$. Hence, if we take the set $\mathcal{O} = \cup_{i=0}^{n-1}\mathcal{O}_i$ we must have $v(P_{c_n}) = 1$ under any admissible noncontextual v on $\mathcal{O}$ satisfying $v(P_a) = v(P_b) = 1$, and $\langle a|c_n\rangle \leq \frac{1}{\sqrt{2}}$ as required. □

4.3.2.2 Analytic approach

We now present a second approach to the reduction in the opposite direction. Rather than searching for a single vector $|c\rangle$ which is closer to $|a\rangle$ than $|b\rangle$ is, we instead find (from $|a\rangle, |b\rangle$) two vectors $|c\rangle, |d\rangle$ specifying observables P_c, P_d for which $v(P_c) = v(P_d) = 1$, and which are further apart from each other than $|a\rangle$ is from $|b\rangle$. This allows for a much more symmetrical situation and simpler Greechie diagram, thus producing vectors for which there are much simpler expressions, and hence simplifying the analysis. Like Lemma 38, this approach relies on the iteration of a particular expansion.

As with the previous approach, we break this process into two steps. We first prove a lemma specifying a single iteration of the reduction, and gives an explicit formula for the amount of expansion provided. We then show a further lemma proving that this expansion can be iterated to meet the required conditions.

Lemma 39. *Given any two unit vectors* $|a\rangle, |b\rangle \in \mathbb{C}^3$ *with* $\frac{1}{3} < |\langle a|b\rangle| < 1$, *we can effectively find unit vectors* $|c\rangle, |d\rangle$ *with* $0 < |\langle c|d\rangle| < |\langle a|b\rangle|$ *and a finite set of one-dimensional projection observables* $\mathcal{O}$ *containing* P_a, P_b, P_c, P_d *such that if* $v(P_a) = v(P_b) = 1$, *then* $v(P_c) = v(P_d) = 1$, *for every admissible noncontextual assignment function* v *on* $\mathcal{O}$.

Proof. Let $\langle a|b\rangle = \alpha$. Without loss of generality, we will consider only the positive, real case of $\frac{1}{3} < \alpha < 1$. We fix an orthonormal basis such that, written in this basis, $|a\rangle$ and $|b\rangle$ lie in the xz-plane bisected by the z-axis. In this basis we thus have

$$|a\rangle = \left(\sqrt{1-\beta^2}, 0, \beta\right), \ |b\rangle = \left(-\sqrt{1-\beta^2}, 0, \beta\right),$$

where

$$\beta = \sqrt{\frac{\alpha+1}{2}}. \tag{3}$$

It is readily confirmed that

$$\langle a|b\rangle = \beta^2 - (1-\beta^2) = 2\beta^2 - 1 = \alpha$$

as desired. Note that we thus have

$$\sqrt{\frac{2}{3}} < \beta < 1. \tag{4}$$

Figure 4.7 shows the curve representing all the possible vectors specifying observables which can be forced to take the value 1 from the construction in Lemma 36. We use two applications of Lemma 36 applied to $|a\rangle, |b\rangle$ to give two such vectors $|c\rangle, |d\rangle$ lying in the yz-plane.

We can also see, at least for the chosen vectors $|a\rangle, |b\rangle$ that are shown in Fig. 4.7, that $\langle a|b\rangle > \langle c|d\rangle$. Indeed it appears that the vectors $|c\rangle$, $|d\rangle$ shown in the yz-plane provide the maximum separation possible, and the symmetry under exchange of $|a\rangle$ and $|b\rangle$ of Lemma 36 seems to support this. However, it is not necessary to prove this is the case. Rather, we will show directly that the vectors $|c\rangle, |d\rangle$ provide the required expansion. To do so, we derive a simple explicit form for $|c\rangle, |d\rangle$ and thus $\langle c|d\rangle$. We focus first on finding $|c\rangle$; the form of $|d\rangle$ follows immediately.

Rather than use basis transformations to attempt to apply Lemma 36 to find the form of $|c\rangle$ and $|d\rangle$ in this specific case, we will re-derive the result explicitly making use of our symmetrised basis choice.

The vectors $|a\rangle, |b\rangle, |c\rangle$ need to follow the orthogonality relations shown in Fig. 4.3 in order to conclude that $v(P_c) = 1$. That is, we need vectors $|e\rangle, |f\rangle$ such that $\{|e\rangle, |f\rangle, |c\rangle\}$ is an orthonormal set, and further that $\langle a|e\rangle = \langle b|f\rangle = 0$.

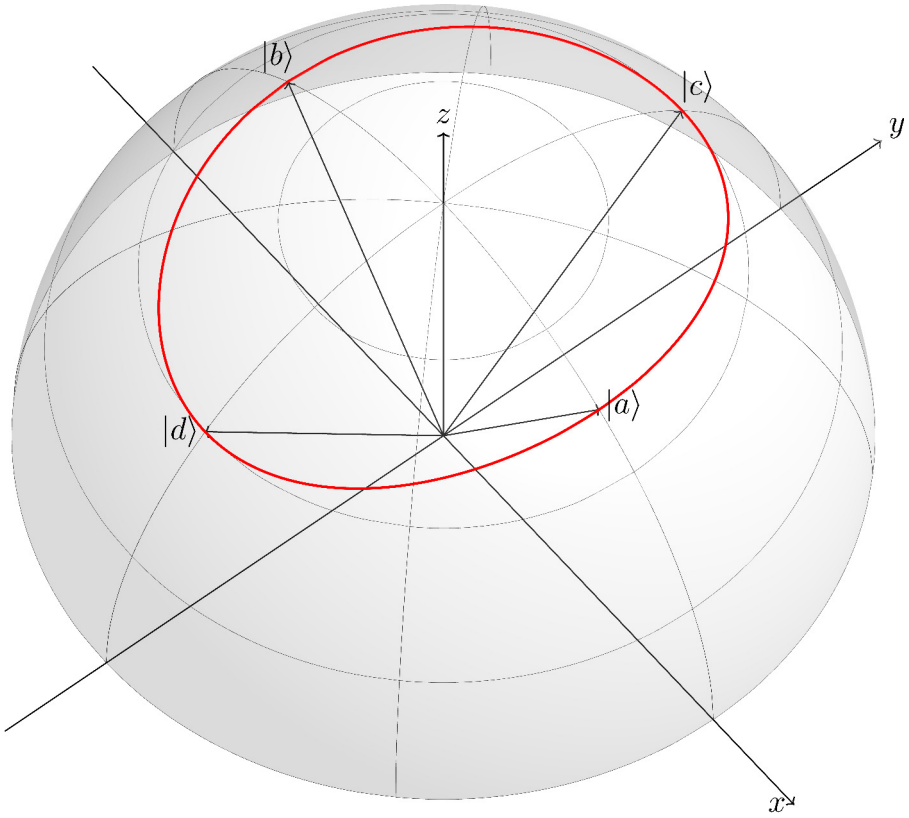


Figure 4.7: A plot of the possible vectors $|c\rangle$ that Lemma 36 can force to take the value 1. The bold (red) curve represents the position on the unit sphere of such vectors for given $|a\rangle, |b\rangle$. Note that $|c\rangle$ and $|d\rangle$ are further apart from each other than $|a\rangle$ and $|b\rangle$, as is evident from the contour lines on the hemisphere.

Since we choose $|c\rangle$ to be in the yz-plane, we can write it in the parameterised form $|c\rangle = (0, \sqrt{1-\gamma^2}, \gamma)$, where $\gamma > 0$ remains to be found. Since $|e\rangle$ should be orthogonal to both $|a\rangle$ and $|c\rangle$, we have

$$|e\rangle = |a\rangle \times |c\rangle = \left(-\beta\sqrt{1-\gamma^2}, -\gamma\sqrt{1-\beta^2}, \sqrt{(1-\beta^2)(1-\gamma^2)}\right).$$

Similarly, we have

$$|f\rangle = |b\rangle \times |c\rangle = \left(-\beta\sqrt{1-\gamma^2}, \gamma\sqrt{1-\beta^2}, -\sqrt{(1-\beta^2)(1-\gamma^2)}\right).$$

Further, the orthogonality of $|e\rangle$ and $|f\rangle$ gives us

$$\begin{aligned}
\langle e|f\rangle &= \beta^2(1-\gamma^2) - \gamma^2(1-\beta^2) - (1-\beta^2)(1-\gamma^2) \\
&= \beta^2 - \beta^2\gamma^2 - \gamma^2 + \beta^2\gamma^2 - 1 + \gamma^2 + \beta^2 - \beta^2\gamma^2 \\
&= 2\beta^2 - \beta^2\gamma^2 - 1 \\
&= 0
\end{aligned}$$

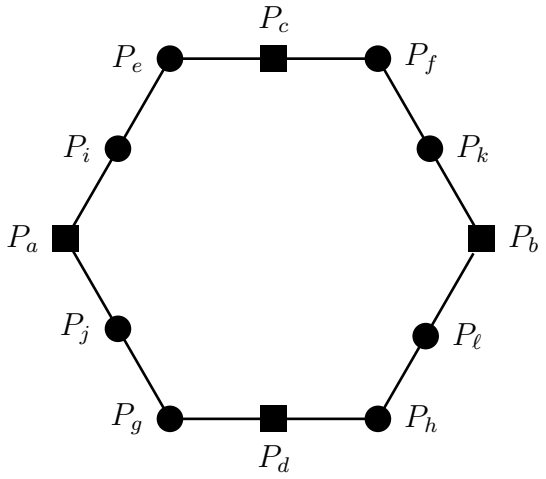


Figure 4.8: Greechie orthogonality diagram with an overlaid value assignment that illustrates the reduction in Lemma 39. Once again, the circles and squares represent observables that have the values 0 and 1 respectively.

and hence $\beta^2(2-\gamma^2)=1$. Thus,

$$\gamma = \sqrt{2-\frac{1}{\beta^2}}\,. \tag{5}$$

Further, it is readily verified that $\frac{1}{\sqrt{2}} < \gamma < 1$ for $\sqrt{\frac{2}{3}} < \beta < 1$, and hence for all $\frac{1}{3} < \alpha < 1$ (recall Eqn. 4).

Similarly, we find $|d\rangle = (0, -\sqrt{1-\gamma^2}, \gamma)$ using a further two auxiliary vectors $|g\rangle, |h\rangle$ forming the orthonormal set $\{|d\rangle, |g\rangle, |h\rangle\}$ where $\langle a|g\rangle = \langle b|h\rangle = 0$.

This construction and the associated orthogonality relations are shown in Fig. 4.8.

Thus, if we let $|i\rangle = |a\rangle \times |e\rangle$, $|j\rangle = |a\rangle \times |g\rangle$, $|k\rangle = |b\rangle \times |f\rangle$ and $|\ell\rangle = |b\rangle \times |h\rangle$ to complete the contexts, and let $\mathcal{O} = \{P_a, P_b, P_c, P_d, P_e, P_f, P_g, P_h, P_i, P_j, P_k, P_\ell\}$, as a consequence of the resulting orthogonality relations, shown in Fig. 4.8, then $v(P_c) = v(P_d) = 1$ for any admissible noncontextual v on $\mathcal{O}$ with $v(P_a) = v(P_b) = 1$.

It remains then just to show that

$$\langle c|d\rangle = 2\gamma^2 - 1 < \langle a|b\rangle = \alpha = 2\beta^2 - 1. \tag{6}$$

We note that $\langle c|d\rangle > 0$ for $\gamma > \frac{1}{\sqrt{2}}$.

We finish the proof by showing proving (6), that is, that $\langle c|d\rangle < \alpha$, or, equivalently, $\gamma^2 < \beta^2$. But since we can write

$$\left(\beta - \frac{1}{\beta}\right)^2 = \beta^2 - \frac{1}{\beta^2} - 2$$

we have from (5)

$$\gamma^2 = 2 - \frac{1}{\beta^2} = \beta^2 - \left(\beta - \frac{1}{\beta}\right)^2 < \beta^2,$$

concluding the proof.

We note for completeness that we can write $\langle c|d\rangle$ directly in terms of α from Eqns. 3, 5 and 6 as

$$\langle c|d\rangle = 3 - \frac{4}{\alpha + 1} \cdot \tag{7}$$

□

We now prove that by iterating this procedure we can find a pair of vectors arbitrarily far apart from each other.

Lemma 40. *Given any two unit vectors $|a\rangle, |b\rangle \in \mathbb{C}^3$ with $\frac{1}{3} < |\langle a|b\rangle| < 1$, we can effectively find unit vectors $|c\rangle, |d\rangle$ with $0 < |\langle c|d\rangle| \leq \frac{1}{3}$ and a finite set of observables $\mathcal{O}$ containing P_a, P_b, P_c, P_d such that if $v(P_a) = v(P_b) = 1$, then $v(P_c) = v(P_d) = 1$, for every admissible noncontextual assignment function v on $\mathcal{O}$.*

Proof. We prove by iterating Lemma 39, and use the notation $|c_0\rangle \equiv |a\rangle$ and $|d_0\rangle \equiv |b\rangle$, indicating the 0th iteration. We start with $|c_0\rangle, |d_0\rangle$ and for each $i \geq 0$, as long as $|c_i\rangle, |d_i\rangle$ satisfy $\langle c_i|d_i\rangle > \frac{1}{3}$, apply the construction used in the proof of Lemma 39 to generate $|c_{i+1}\rangle, |d_{i+1}\rangle$ for the next iteration. In particular, $|c_{i+1}\rangle, |d_{i+1}\rangle$ satisfy the equality (7) for $\alpha_i = \langle c_i|d_i\rangle$ (and hence $\alpha_0 = \langle c_0|d_0\rangle = \langle a|b\rangle$).

By Lemma 39, we know that $\langle c_i|d_i\rangle > \langle c_{i+1}|d_{i+1}\rangle$ for each iteration i. We now prove that the process cannot produce an infinite sequence $|c_0\rangle, |d_0\rangle; |c_1\rangle, |d_1\rangle; \cdots$, with $\langle c_i|d_i\rangle > \frac{1}{3}$ for all i, that is, for some i we have $\langle c_i|d_i\rangle \leq \frac{1}{3}$. (The sequence must stop here, since Lemma 39 cannot be applied for $\langle c_i|d_i\rangle \leq \frac{1}{3}$.)

From (7) we define the function $s : \left(\frac{1}{3}, 1\right) \to (0, 1)$ such that

$$s(u) = 3 - \frac{4}{u + 1},$$

giving the inner product of the next pair in the iteration. We thus have $s(\alpha_0) = \alpha_1$ and, more generally, $\alpha_i = s^i(\alpha_0)$. We can thus rephrase the problem: *does there exist a k such that $s^k(\alpha_0) \leq \frac{1}{3}$?*

Let us, for the sake of contradiction, assume the contrary. Then $(\alpha_i)_i = (s^i(\alpha_0))_i$ is an infinite strictly decreasing sequence of reals with $\alpha_i > \frac{1}{3}$ for all i. For any finite i we thus have

$$\begin{aligned} s^i(\alpha_0) = \alpha_i &= \alpha_0 - |\alpha_1 - \alpha_0| - \cdots - |\alpha_i - \alpha_{i-1}| \\ &= \alpha_0 - (\alpha_0 - \alpha_1) - \cdots - (\alpha_{i-1} - \alpha_i) \\ &= \alpha_0 - \sum_{k=0}^{i-1} (\alpha_k - \alpha_{k+1}). \end{aligned}$$

Let us define the function $D : \left(\frac{1}{3}, 1\right) \to \left(0, \frac{1}{3}\right)$ such that

$$D(u) = u - s(u) = u - \left(3 - \frac{4}{u+1}\right)$$

so that

$$\alpha_i = \alpha_0 - \sum_{k=0}^{i-1} D(\alpha_k).$$

We can show that $\frac{\mathrm{d}D}{\mathrm{d}u} < 0$ for $u \in \left(\frac{1}{3}, 1\right)$: calculating the derivative we have

$$\frac{\mathrm{d}D}{\mathrm{d}u} = 1 - \frac{4}{(u+1)^2} < 1 - \frac{4}{(1+1)^2} = 0.$$

Since D is thus a strictly decreasing function on $\left(\frac{1}{3}, 1\right)$ and $\alpha_k < \alpha_0$ for all $k > 0$, we have $D(\alpha_0) < D(\alpha_k)$ for all $k > 0$. Hence we set

$$\alpha_i = \alpha_0 - \sum_{k=0}^{i-1} D(\alpha_k) < \alpha_0 - iD(\alpha_0).$$

Since $D(\alpha_0) = \alpha_0 - \alpha_1 > 0$ is a positive constant, it is not possible that $s^i(\alpha_0) = \alpha_i > \frac{1}{3}$, for all $i > 0$, because in this case we would have $\frac{1}{3} < \alpha_0 - iD(\alpha_0)$, for all $i > 0$, a contradiction.

In fact, if k is the smallest positive integer greater than $\frac{\alpha_0 - \frac{1}{3}}{D(\alpha_0)}$, then $\alpha_k \leq \frac{1}{3}$, as required. We note that $s^{k+1}(\alpha_0)$ is not defined.

By Lemma 39, for each $i = 0, \ldots, k-1$ there exists a set $\mathcal{O}_i$ of observables such that $v(P_{c_{i+1}}) = v(P_{d_{i+1}}) = 1$ under any v admissible on $\mathcal{O}_i$ satisfying $v(P_{c_i}) = v(P_{d_i}) = 1$. Hence, if we take the set $\mathcal{O} = \cup_{i=0}^{k-1} \mathcal{O}_i$ we must have $v(P_{c_k}) = v(P_{d_k}) = 1$ under any admissible noncontextual v on $\mathcal{O}$ satisfying $v(P_a) = v(P_b) = 1$, and $\langle c_k | d_k \rangle \leq \frac{1}{3}$, as required. □

Lemmata 35, 36 and 40 together[4] show that, if $v(P_\psi) = 1$, then we cannot have $v(P_\phi) = 1$ if v is admissible. We are now in a position to put these results together to show that we also cannot have $v(P_\phi) = 0$ and thus prove Theorem 34.

Proof of Theorem 34. If we have $|\langle \psi | \phi \rangle| = \frac{1}{\sqrt{2}}$ then, by Lemma 35, there exists a finite set $\mathcal{O}$ for which there is no admissible noncontextual v on $\mathcal{O}$ satisfying the requirements, so we are done.

Otherwise, we proceed directly to prove that there exists a set of observables $\mathcal{O}$ containing P_ψ, P_ϕ for which there is no admissible noncontextual assignment function v on $\mathcal{O}$ with $v(P_\psi) = 1$ and P_ϕ value definite. We show this in two cases: first that

[4]Note that we could equally use the computational result of Lemma 38 instead of Lemma 40 for this.

$v(P_\phi) \neq 1$ and then that $v(P_\phi) \neq 0$. Let us first show that there is a set $\mathcal{O}_1$ for which $v(P_\phi) \neq 1$ if v is admissible on $\mathcal{O}_1$.

There are two cases: either $0 < |\langle\psi|\phi\rangle| < \frac{1}{\sqrt{2}}$ or $1 > |\langle\psi|\phi\rangle| > \frac{1}{\sqrt{2}}$.

If $0 < |\langle\psi|\phi\rangle| < \frac{1}{\sqrt{2}}$, then by Lemma 36 there exists a vector $|\phi'\rangle$ such that $\langle\psi|\phi'\rangle = \frac{1}{\sqrt{2}}$ and a set $\mathcal{O}_2$ of observables containing $P_\psi, P_\phi, P_{\phi'}$ such that if v is admissible on $\mathcal{O}_2$, $v(P_{\phi'}) = 1$ also. But, by Lemma 35, there exists a set $\mathcal{O}_3$ of observables containing $P_\psi, P_{\phi'}$ such that if v is admissible on $\mathcal{O}_3$ and $v(P_\psi) = 1$, $P_{\phi'}$ must be value indefinite. Thus, if we take $\mathcal{O}_1 = \mathcal{O}_2 \cup \mathcal{O}_3$ we cannot have $v(P_\phi) = 1$ as required.

If $1 > |\langle\psi|\phi\rangle| > \frac{1}{\sqrt{2}}$, then by Lemma 40 there exist two vectors $|\psi'\rangle, |\phi'\rangle$ such that $0 < |\langle\psi'|\phi'\rangle| \leq \frac{1}{3}$ and a set $\mathcal{O}_4$ of observables containing $P_\psi, P_\phi, P_{\psi'}, P_{\phi'}$ such that if v is admissible on $\mathcal{O}_4$ then $v(P_{\psi'}) = v(P_{\phi'}) = 1$ also. But, by Lemma 36, there exists a vector $|\phi''\rangle$ such that $\langle\psi'|\phi''\rangle = \frac{1}{\sqrt{2}}$ and a set $\mathcal{O}_5$ of observables containing $P_{\psi'}, P_{\phi''}, P_{\phi'}$ such that if v is admissible, $v(P_{\phi''}) = 1$ also. Finally, once more by Lemma 35, there exists a set $\mathcal{O}_6$ for which v there is no admissible v on $\mathcal{O}_5$ satisfying $v(P_{\psi'}) = v(P_{\phi''}) = 1$. Hence, there is no admissible v on the set $\mathcal{O}_1 = \mathcal{O}_4 \cup \mathcal{O}_5 \cup \mathcal{O}_6$ such that $v(P_\phi) = 1$ as required.

This shows that there exists a set $\mathcal{O}_1$ of observables containing P_ψ, P_ϕ such that we cannot have $v(P_\phi) = v(P_\psi) = 1$ if v is admissible on $\mathcal{O}_1$. It remains to show that there exists a set $\mathcal{O}_0$ such that we cannot have $v(P_\phi) = 0$ if v is admissible on $\mathcal{O}_0$.

Let us assume, without loss of generality, that $|\psi\rangle = (1, 0, 0)$ and $|\phi\rangle = (p, \sqrt{1-p^2}, 0)$ where $p = |\langle\psi|\phi\rangle|$. Then let $|\alpha\rangle = (0, 1, 0)$, $|\beta\rangle = (0, 0, 1)$ and $|\phi'\rangle = (\sqrt{1-p^2}, p, 0)$. Then $\{|\psi\rangle, |\alpha\rangle, |\beta\rangle\}$ and $\{|\phi\rangle, |\phi'\rangle, |\beta\rangle\}$ are orthonormal bases for $\mathbb{C}^3$ and hence $C_1 = \{P_\psi, P_\alpha, P_\beta\}$ and $C_2 = \{P_\phi, P_{\phi'}, P_\beta\}$ are contexts in $\mathcal{O}_7 = C_1 \cup C_2$. But if v is admissible on $\mathcal{O}_7$ and $v(P_\psi) = 1$, $v(P_\phi) = 0$, admissibility implies that $v(P_\phi) = 1$.

As we have shown just before, there exists a set $\mathcal{O}_8$ of observables containing $P_\psi, P_{\phi'}$ such that there is no admissible noncontextual assignment function v on $\mathcal{O}_8$ with $v(P_\psi) = v(P_{\phi'}) = 1$, and hence there is no admissible noncontextual v on $\mathcal{O}_0 = \mathcal{O}_7 \cup \mathcal{O}_8$ such that $v(P_\psi) = 1$ and $v(P_\phi) = 0$.

Having covered all cases, we are forced to conclude that there is a set $\mathcal{O} = \mathcal{O}_0 \cup \mathcal{O}_1$ of containing P_ψ and P_ϕ such that if $v(P_\psi) = 1$, P_ϕ cannot be value definite if v is admissible on $\mathcal{O}$. □

The important difference between Theorem 34 and the Kochen-Specker theorem lies in what physical conclusions can be drawn from the theorems which, of course, are purely mathematical results. However, before we proceed to discuss this interpretation and the associated physical assumptions that are required, let us first discuss some final issues relating to Theorem 34 and its proof.

4.3.3 Proof size

Since the first appearance of the Kochen-Specker theorem [80], much attention has been given to reducing the number of observables and contexts needed to obtain a contradiction and prove the theorem.

Conceptually, however, the key point is probably that the theorem can be proved using a *finite* set of observables; if a contradiction only arose when an infinity of observables were considered, this would potentially raise questions about the physicality of the theorem and its use of counterfactuals, and its interpretation would be more questionable [106].

Due to its ability to locate value indefinite observables, the form of Theorem 34 immediately means that a single finite set $\mathcal{O}$ of observables will never suffice to prove the value indefiniteness of all observables P_ϕ not commuting with P_ψ for a given state $|\psi\rangle$. There are infinitely many such observables, and one must, by definition, include P_ϕ in $\mathcal{O}$ to localise value indefiniteness to P_ϕ. Rather, the nature of Theorem 34 means we must look for constructive methods to obtain a set $\mathcal{O}_\phi$ for a given P_ϕ, which is precisely what we have done in our proof of the result.

Of course, a given set of orthogonality relations (i.e., a Greechie diagram) may be realisable non-trivially (i.e., not simply by a basis transformation equivalent to a unitary transformation on the set) for an infinity of different sets $\mathcal{O}$ containing P_ψ, as is the case with the diagram depicted in Fig. 4.3. Thus, it would be preferable to find a given set of orthogonality relations for which a set $\mathcal{O}_\phi$ of observables realising these relations and containing both P_ψ and P_ϕ for any P_ϕ. Since we were unable to give such a set of relations, we had to iterate reductions in both proofs given (i.e., in Lemma 40 and Lemma 38) a number of times depending on P_ψ, with no upper bound (but only ever finitely many times).

Furthermore, it seems that it is difficult, if not impossible, to succeed in giving a fixed set of orthogonality relations that works in all cases. In order to show an observable P_a has $v(P_a) = 1$ using the admissibility requirements, one must give a context $\{P_a, P_b, P_c\} \subset \mathcal{O}$ for which it is already known that $v(P_b) = v(P_c) = 0$. This implies two observable P_d and P_e such that $v(P_d) = v(P_e) = 1$ and $\langle b|d\rangle = \langle c|e\rangle = 0$. But this is precisely the case described in Lemma 36. However, in Lemma 39 we showed the limitations of this process in 'widening the angle' between vectors whose projectors both take the value 1 – hence the necessity of iterating Lemma 39.

As a result, we formulate the following conjecture.

Conjecture 41. *There exists no $n \in \mathbb{N}$ such that, for all $|\psi\rangle, |\phi\rangle$ with $0 < |\langle\psi|\phi\rangle < 1$, there exists a set of one-dimensional projection observables $\mathcal{O}_{\psi,\phi}$ containing P_ψ and P_ϕ*

with $|\mathcal{O}_{\psi,\phi}| \leq n$ *such that, under any noncontextual admissible value assignment* v *on* $\mathcal{O}_{\psi,\phi}$ *with* $v(P_\psi) = 1$, P_ϕ *is value indefinite.*

Thus, in contrast to the Kochen-Specker theorem, it seems that arbitrarily large sets of observables are needed to show that a given observable P_ϕ is value indefinite. Nonetheless, the critical point is once again that for *any given* P_ϕ, we can show that P_ϕ is value indefinite with a *finite* set of observables, and hence that the counterfactual reasoning used is no more problematic than in the Kochen-Specker theorem.

4.4 A physical interpretation of localised value indefiniteness

Theorem 34 shows that, under certain mathematical conditions, particular systems must contain a formal kind of value indefiniteness. Although this lends naturally to a particular physical interpretation, as we have briefly discussed, one should be particularly careful in drawing such physical conclusions without looking at what extra physical assumptions are hidden in this process. One must carefully identify these physical assumptions needed to interpret these formal results, as well as scrutinising the justification for certain elements of the model.

Here we will do precisely that. We will discuss the various assumptions that need to be taken into account and how these justify the model, and in particular admissibility. Finally, we will discuss some further issues relating to the possible interpretations following from the Kochen-Specker theorem as well as our results.

4.4.1 The role of measurement

An inherent assumption in any attempt to attribute physical meaning to the Kochen-Specker theorem and the related results is that measurement constitutes a physically meaningful process. In particular, one must assume the

Measurement assumption: Measurement is fundamental and yields a physically meaningful and unique result.

This may seem rather self-evident, but it is not true of interpretations of quantum mechanics such as the many-worlds interpretation, where measurement is just a process by which the apparatus or experimenter becomes entangled with the state being 'measured' [54]. In such an interpretation it does not make sense to talk about the unique 'result' of a measurement, let alone any definite values which one may assign to them in advance. Rather, both outcomes are seen to actually occur, and the notion of a measurement result loses its ontological status.

Furthermore, it is worth making explicit the fact that, whenever we talk about the measurement outcomes of a particular *physical* system in a state $|\psi\rangle$ by reference to a value assignment function v, we (normally implicitly) assume that v is a faithful representation of this particular realisation of the physical system. Let us be more explicit.

Definition 42. A *(physical) realisation r_ψ of a state $|\psi\rangle$* is a physical system prepared in the quantum state $|\psi\rangle$.

Of course, the standard interpretation is that $|\psi\rangle$ is the maximal description possible of any realisation r_ψ of it, but we need to consider that this may not be the case in order to consider the implications of no-go theorems properly.

Definition 43. A value assignment function v is a *faithful representation* of a realisation r_ψ of a state $|\psi\rangle$ if an observable P in a context C is value definite under v with value $v(P, C)$ if and only if its outcome is physically predetermined to be precisely the value $v(P, C)$.

The Kochen-Specker theorem, as well as our results, talk only about value assignment functions – faithful or not. Usually, it is implicitly assumed that a value assignment function is faithful – if it is not then it has no real relation to the physical system that it is meant to model and is of little interest. Nonetheless, we feel it is important to make all the relevant assumptions explicit, and to make any interpretation we need, specifically, to consider the features of any faithful v for any realisation r_ψ of $|\psi\rangle$. Thus, when we wish to discuss the actual indefiniteness or indeterminism of physical measurements, we will always consider value assignment functions that are faithful representations of the system considered.

4.4.2 Assignment of definite values

A further issue that is important not only in justifying the requirement of admissibility in our model, but also critical in giving it a physical meaning, is the question of when we can conclude that definite values should be assigned to an observable, and determining the nature of any faithful value assignment function. This is intimately related to the issue of the faithfulness of a value assignment function, as an assignment function faithfully representing a system in state $|\psi\rangle$ must have definite values whenever a measurement outcome on the state is predetermined. So when can we determine that a measurement outcome is predetermined? The question is perhaps more subtle than it first appears.

Einstein, Podolsky and Rosen (EPR), in their seminal paper on the EPR paradox said [51, p. 777]:

> If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality[5] corresponding to this physical quantity.

From the physicist's point of view, the ability to predict the value of an observable with certainty seems sufficient to posit the existence of a definite value associated with that observable. However, the identification that EPR make between certainty and probability one is less sound. Mathematically, the statement is simply not true: for infinite measure spaces, probability zero events not only can, but must occur – for example, every point on the real line has probability 0 under the Lebesgue measure. One can only say an event is certain if its complement is the empty set.

Nonetheless, modulo these small difficulties, the principle outlined by EPR seems to outline a sound condition for value definiteness; indeed, without some such principle we would be left unable to ever reasonably conclude the presence of value definiteness. Thus, reformulating this slightly, we will take take the following as a guiding principle:

EPR principle: If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists a definite value prior to observation corresponding to this physical quantity.

With the formalism of quantum mechanics entirely based on probability spaces, what then can we say about the existence of any definite values associated with any measurement in the quantum mechanical description of physical reality? A deterministic theory is based on a description of a state which is complete in that it specifies definite values for all observables. The state in quantum theory, however, is given as a wave function, which in turn is determined by the operators of which the system is an eigenstate. This is further backed up by more recent results showing the impossibility to view the wave-function as simply an epistemic 'catalogue' of results, and that it is rather an ontological description [111]. Quantum theory is thus based on the notion that a physical state is 'completely characterised by the wave function', which is an eigenstate of some operator and is determined for any context containing the said operator; as EPR note, the 'physical quantity' corresponding to that operator has 'with certainty' the corresponding eigenvalue [51, p. 778]. The theory then presents a probabilistic framework to express the behaviour of other observables and their measurement.

While the Kochen-Specker theorem and related results explore the possibility to explain these probabilistic outcomes via an underlying determinism, one would expect these approaches to coincide on measurements confirming the known property of the sys-

[5] An element of physical reality corresponds to the notion of a definite value, possibly contextual, as outlined in this paper.

tem corresponding to its preparation state. It is thus reasonable to assume, as discussed more briefly earlier, the

Eigenstate assumption: Let $|\psi\rangle$ be a quantum state and v be a faithful assignment function of a realisation r_ψ of $|\psi\rangle$. Then $v(P_\psi, C) = 1$ for any context $C \in \mathcal{C}_\mathcal{O}$ with $P_\psi \in C$.

It is worth noting that this assumption is similar to the 'eigenstate-eigenvalue link' discussed in [128], although the eigenstate-eigenvalue link is stronger in the crucial fact that it considers that the relation is bi-directional, whereas we do not assume that a system must be in an eigenstate of an observable if the observable is value definite.

We can finally justify the requirement that a faithful assignment function v should be admissible by again using the EPR principle relating to the assignment of definite values.

Theorem 44. *Let v be a faithful value assignment function of a system realising the state $|\psi\rangle$. Then v must be admissible.*

Proof. Let $\mathcal{O}$ be the set of one-dimensional projection observables on $\mathbb{C}^n$ for $n \geq 2$, $C = \{P_1, \ldots, P_n\} \in \mathcal{C}_\mathcal{O}$ a context of $\mathcal{O}$, and v a faithful assignment function on $\mathcal{O}$ with $v(P_1, C) = 1$.

Since P_1 and P_i (for $i \neq 1$) are compatible (physically co-measurable), if we measure them both, the system will collapse into the eigenstate of P_1 corresponding to the eigenvalue 1. Since this final state would also be an eigenstate of P_i, it follows from the fact that $\sum_{j=1}^{n} P_j = I$ that this state corresponds to the eigenvalue 0 of P_i and hence, by the eigenstate assumption, $v(P_i, C) = 0$. Thus we conclude that $v(P_i, C) = 0$ for all $2 \leq i \leq n$.

By a similar argument, we see that if instead $v(P_i, C) = 0$ for $2 \leq i \leq n$ we must have $v(P_1, C) = 1$. □

This justifies that a faithful assignment function v must be admissible, hence justifying the final element of our model.

4.4.3 Noncontextuality

Similar to the manner in which the Kochen-Specker theorem finds a contradiction between complete noncontextuality and value definiteness, Theorem 34 finds a contradiction between noncontextuality and the value definiteness of any observable not corresponding to the preparation observable of the system. Our notion of noncontextuality is weaker than that used in the Kochen-Specker theorem, since we define it, and require it to hold, only for those observables that are value definite, rather than the complete set under consideration. Nonetheless, a negation of either assumption (or even both) is a

valid mathematical conclusion of the theorem. A specific interpretation of the theorem thus inevitably relies on physical and philosophical assumptions.

Both options lead to rather different interpretations, and if we accept the possibility of a contextual reality, then Theorem 34 leads to the same interpretational conclusion as the Kochen-Specker theorem. In this thesis, and in particular in the following chapters when we consider more carefully the certification of quantum randomness, we opt to assume the noncontextuality of measurement outcomes for measurements of observables whose outcome is predetermined, and thus give up the historic notion of complete determinism and classical omniscience.

This assumption might be in contradiction to that of some physicists who, in the tradition of the realist Bell (see the oft-quoted text, [14]), tend to opt for contextuality. The option for contextuality saves realistic omniscience and 'contextual value definiteness' at the price of introducing a more general dependence of at least some potential observables on the measurement context.

Nonetheless, we feel this assumption is quite reasonable. Our assumption of noncontextuality requires only that value definite observables – that is, those which are classically deterministic – behave in the classical, noncontextual manner. Refusing any value indefiniteness, on the other hand, appears a somewhat stronger assumption, and forces this classical property on *all* observables.

At the very least, the fields of quantum information theory and cryptography are intimately connected to the indeterministic view of quantum mechanics, and such an assumption allows our results to contribute to these fields, as well as for us to investigate, in the forthcoming chapters, their practical implications.

Thus we make the

Noncontextuality assumption: The outcome of measurements on a quantum system can be faithfully represented by a noncontextual value assignment function.

4.4.4 A physical interpretation

With these physical assumptions made clear, we can express more carefully our interpretation, how it follows from Theorem 34, and the physical assumptions we make. This allows us to show the extent of indeterminism in quantum mechanics resulting from our formal result.

Proposition 45. *If a quantum system is prepared in an arbitrary state* $|\psi\rangle \in \mathbb{C}^n$ *for* $n \geq 3$*, then, assuming the measurement, noncontextuality and eigenstate assumptions, no observable* P_ϕ *for* $0 < |\langle\psi|\phi\rangle| < 1$ *can be value definite under any faithful noncontextual value assignment function.*

Although Theorem 34 and its interpretation in Proposition 45 formally apply only to one-dimensional projection observables, we note that it is not difficult to generalise them to more general classes of observables. Since an observable A with a non-degenerate spectrum, eigenvalues $a_1, \ldots, a_n$, and eigenstates $|a_1\rangle, \ldots, |a_n\rangle$ can be expressed in terms of projection observables via its spectral decomposition $A = \sum_{i=1}^{n} a_i P_{a_i}$, it makes sense to consider it to be value definite if and only if all the projectors P_{a_i}, $i = 1, \ldots, n$, are value definite.[6]

Thus we can conclude more generally that any observable A such that $|\psi\rangle$ is not an eigenstate of A must be value indefinite, and the measurement of A then produces an outcome that is not-predetermined in advance. That is, the measurement of A yields a value indeterministically, and the outcome is created *ex nihilo* by measurement. This represents a complete departure from classical realism, and formalises the quantum indeterminism that is often assumed *a priori*, basing it on more fundamental, explicit, physical assumptions.

This is in stark contrast to the Kochen-Specker theorem, which supports, under the same assumptions, a significantly weaker interpretation: that *some* observables must be value indefinite. This eliminates the need to assume that the nonclassicality that the Kochen-Specker theorem implies should apply uniformly to all observables, instead deriving this result. Since the Kochen-Specker theorem cannot locate value indefiniteness, the physical conclusions drawn from it have much less practical value. For example, since one can never be sure that they are measuring a value definite observable (one can imagine, for example, a demon ensuring that the value indefiniteness always occurs at some other observable), this creates a loophole in the generation of random numbers via quantum mechanics that is supposed to be certified by quantum indeterminism.

Conceptually, this means that Theorem 34 goes significantly further than the Kochen-Specker theorem in showing the *extent* of nonclassicality that the quantum logic event-structure implies.

We can formalise this even further from a measure theoretic point of view.

Theorem 46. *Let $|\psi\rangle$ be an arbitrary state in $\mathbb{C}^n$ for $n \geq 3$. Then the set of one-dimensional projection observables that are value definite for this state under any noncontextual value assignment function on $\mathbb{C}^n$ has Lebesgue measure zero.*

Proof. Let v be a noncontextual value assignment function on $\mathbb{C}^n$. Since the system is in the state $|\psi\rangle$, we have $v(P_\psi) = 1$ by the eigenstate assumption.

Then, by Theorem 34, every observable P_ϕ is value indefinite under v if $0 < |\langle\psi|\phi\rangle| < 1$. That is, the set of value definite observables is precisely $D = \{P_\psi\} \cup \{P_\phi \mid \langle\psi|\phi\rangle = 0\}$.

[6] Intuitively, if one such P_{a_i} has the predetermined value 1 then one must obtain a_i upon measurement of A; admissibility then requires that all P_{a_j} have the predetermined value 0 for $j \neq i$.

However, the set $\{P_\phi \mid \langle\psi|\phi\rangle = 0\}$ is isomorphic to $\mathbb{C}^{n-1}$, which has Lebesgue measure zero in $\mathbb{C}^n$ since any subspace of dimension smaller than n has Lebesgue measure zero in $\mathbb{C}^n$. □

For the simplest case of $n = 3$, if we let $|\psi\rangle = (1, 0, 0)$ then the set D in the above proof corresponds to the set $\{(1, 0, 0)\} \cup \{(0, x, y) \mid |x|^2 + |y|^2 = 1\}$ on the three-dimensional (complex) unit sphere, consisting of (i) a single point of dimension zero, and (ii) a great circle of dimension one. Again this set has Lebesgue measure zero on the unit sphere, and hence the set of value indefinite observables has measure one.

4.4.5 State-independence and testability

One of the strengths of the Kochen-Specker theorem that has been repeatedly emphasised is the fact that the contradiction between its hypotheses is derived independently of the state a quantum system is prepared in; this is commonly referred to as state-independence. This is in contrast to violation of Bell-type inequalities (which occur only for particular entangled states) and shows that the nonclassicality results from the structure of quantum mechanics itself, rather than features of particular states, such as entanglement [79, 163]. Consequently, various experimental inequalities based on the Kochen-Specker theorem that, although often simpler, are state-dependent have been criticised, and much effort has been expended to find simple, state-independent inequalities to test [26].

In contrast to the Kochen-Specker theorem, the form of Theorem 34 and, in particular, the interpretation that *for a given state* $|\psi\rangle$, any observable P_ϕ not commuting with P_ψ is value indefinite, may suggest that Theorem 34 does not share this state-independence. As a result, this issue deserves a little discussion.

The state-independence of the Kochen-Specker theorem ensures that no quantum state in $n \geq 3$ dimensional Hilbert space admits a classical assignment of definite values to all observables within certain finite sets. This is true also with Theorem 34: for any quantum state $|\psi\rangle$, all observables not contained within the 'star' of observables commuting with P_ψ (see Fig. 4.9) are value indefinite. Of course, this set of observables that are guaranteed to be value indefinite will differ for different states $|\psi\rangle$, but never on a set of non-zero measure.

Rather, it is not Theorem 34 that is state-dependent, but the proof we have given: to show that a given observable P_ϕ is value indefinite, we need a set $\mathcal{O} = \mathcal{O}_\phi$ particular to this $|\phi\rangle$. However, as we discussed in the preceding section, this is perfectly reasonable given the form of the theorem.

One can emphasise further the state-independence of Theorem 34 by restating the theorem in the following form: '*Only a single one-dimensional projection observable*

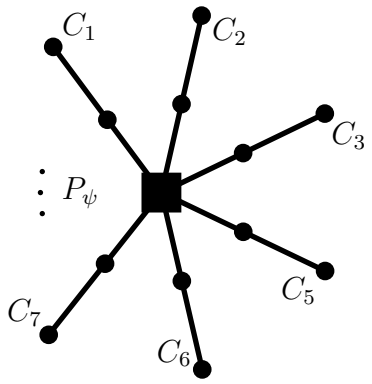


Figure 4.9: Greechie diagram showing an observable P_ψ with $v(P_\psi) = 1$ and the (infinite) set of compatible observables P_ϕ for which $v(P_\phi) = 0$. This is the maximal extent of value definiteness for a system in state $|\psi\rangle$ – no other one-dimensional projection observables in $\mathbb{C}^3$ can be value definite.

on the Hilbert space $\mathbb{C}^n$ for $n \geq 3$ can be assigned the value 1 by an admissible non-contextual value assignment function'. In this form the state-independence is clear; the illusion of state-dependence enters because of the connection, via the eigenstate assumption, between the 'one observable assigned the value 1' and the particular state $|\psi\rangle$ (and corresponding observable P_ψ with $v(P_\psi) = 1$) which is necessary for the physical interpretation of the theorem.

The importance of the state-independence of the Kochen-Specker theorem arises, in part, in the use of Kochen-Specker sets of observables in testable inequalities. It is important to note that, even though these inequalities are sometimes referred to as 'Kochen-Specker inequalities' [83], they are better seen simply as noncontextuality inequalities. These inequalities are derived under the assumption only of noncontextuality, ignoring the admissibility requirements, and bounds on quantities are calculated over all possible noncontextual value assignments. A key result shows that one can derive such an inequality from any Kochen-Specker set [158]. It is clear that these value assignments cannot obey the admissibility requirements, since the Kochen-Specker theorem shows precisely that no classical value assignment can do so.

The strength of Theorem 34, on the other hand, relies precisely on the use of the admissibility requirements to determine when definite values should be assigned. Hence, while one can use the methods of [158] to derive inequalities from the constructions in the proof of Theorem 34, these bounds would be calculated over all noncontextual value assignments (subject to $v(P_\psi) = 1$), without paying heed to admissibility, and hence would offer no conceptual advantage over existing inequalities. Furthermore, since our construction in Lemma 35, for example, contains 37 observables, these would pose no experimental benefit to existing, simpler, inequalities either [79].

Nonetheless, the state-independence of the result shows that the value indefiniteness of almost all observables in quantum mechanics is indeed a deep feature of the theory – of the logical structure of Hilbert space – rather than a property of particular states.

4.5 The limits of value indefiniteness

Before we proceed to discussing some of the consequences of the strengthened variant of the Kochen-Specker theorem, let us discuss some further issues relating to notions of noncontextuality and contextuality, as well as their relation to value indefiniteness and use in the contemporary literature.

4.5.1 Contextuality

While in this thesis we focus on exploring the consequences of value indefiniteness under the assumption of noncontextuality, it is important to keep in mind that it seems unlikely that one can definitively rule out a contextual value definite model of reality [121]. It is thus instructive to consider briefly some contextual alternatives.

In such a model, physical reality is maintained, but the outcome of measurement of an observable would depend explicitly on any other compatible observables also measured. That is, we would need an explicitly contextual value assignment function to model this physical reality. The successful experimental verification of Bell inequalities [145] means that such a reality would necessarily have to be nonlocal: the outcome of a measurement could depend on the choice of compatible observable measured, even if it is done so (and even chosen) at a space-like separated point in space-time. Furthermore, one can envisage systems for which the measurement of an observable A is followed by measurement of a compatible observable B or C – the outcome of the first measurement would depend on the choice of observable to be made in the future, a highly unintuitive reality.

While all such classical models must have this general structure, there are many different approaches to creating a cohesive picture or interpretation of quantum mechanics explaining such value definite contextuality. The most explicit and well known such approach is the de Broglie-Bohm pilot wave theory [20], also known as Bohmian mechanics. While this approach was not explicitly created with contextuality or nonlocality in mind, it can be readily seen to exhibit these phenomena.

Bell, in response to his own theorem, was somewhat more circumspect, instead choosing to highlight the influence of the macroscopic arrangement of the apparatus, and insisted that the 'result of an observation may reasonably depend not only on the state of the system [...] but also on the complete disposition of the apparatus' [14, Sec. 5]. In

this way he explains the possible context dependence as a result of the fact that measuring contexts involves, as a consequence of complementarity, incompatible measurement arrangements.

In this viewpoint, even when the macroscopic measurement apparatuses are still idealised as being perfect, their many degrees of freedom (which may far exceed the order of Avogadro's number) contribute to any measurement of a single quantum. Most of these degrees of freedom might be totally uncontrollable by the experimenter, and would hence result in an epistemic uncertainty which is dominated by the combined complexities of interactions between the single quantum measured and the (macroscopic) measurement device producing the outcome, and thus giving the illusion of indeterminism.

In such a measurement, the pure single quantum and the measurement apparatus would become entangled. In the absence of one-to-one uniqueness between the macroscopic states of the measurement apparatus and the quantum, any measurement would amount to a partial trace resulting in a mixed state of the apparatus, and consequently to an uncertainty and unpredictability of the measurement outcome obtained. Thus, realism may be maintained, but, in Bell's terms, the outcome may be irreversible 'for all practical purposes' [15].

4.5.2 The Kochen-Specker theorem and quantum contextuality

There is a final, further, issue that needs to be clarified regarding the relationship between the Kochen-Specker theorem (and consequently the variant we have proven) and contextuality. In particular, there is a growing trend of viewing the Kochen-Specker theorem as 'proving quantum contextuality' [18, 124, 139, 157, 163]. This interpretation could easily be thought to be incompatible with ours, which relies on our 'noncontextuality assumption', but the issue is rather one of terminology than an actual contradiction.

Such statements are generally made without any explicit formal definition of contextuality. Our noncontextuality assumption requires only that value definite observables behave noncontextually, not all quantum observables. Indeed, as we discussed in Sec. 3.2, under our definition of contextuality, any value indefinite observable is contextual. Thus, it is indeed true that the Kochen-Specker theorem implies contextuality, but it says nothing about whether this contextuality is value definite or indefinite.

We nonetheless choose to avoid referring to Kochen-Specker as implying contextuality in order to avoid any such confusion, given the importance of the limited form of noncontextuality required by the noncontextuality assumption. Furthermore, as we showed in Theorem 30, we can never guarantee that all observables are contextual (i.e., strong contextuality) and indeed it is reasonable to assume that some observables are noncontextual.

Beyond avoiding any confusion, we also wish to emphasise in particular the value indefiniteness guaranteed by Theorem 34 under our assumptions, something which is not implied by contextuality alone. This is important in order to avoid creating the perception of any link between contextuality and quantum indeterminism or randomness.

4.6 Conclusion

While quantum value indefiniteness gives a formal basis to the belief that quantum measurement outcomes are intrinsically indeterministic, we must be careful before jumping to conclusions about the implications of this for quantum randomness and unpredictability.

Quantum value indefiniteness itself represents simply an absence of predetermined measurements outcomes, that is, of determinism. Most of the rest of this thesis will be devoted to exploring precisely these issues of quantum randomness and unpredictability in more detail.

Finally, it is important to keep in mind that no derivation or claim of quantum value indefiniteness is absolute. Rather, it can only ever be guaranteed relative to the physical assumptions that one employs, as we highlighted in the previous sections.

Chapter 5

Quantum randomness and incomputability

Accompanying the standard interpretation that quantum measurements are intrinsically indeterministic – that is, the measured observables are value indefinite and the outcomes not predetermined – is the view that the outcomes of such measurement are therefore intrinsically, or irreducibly, random [161]. This randomness plays an essential role in the active field of quantum information and cryptography [8, 40], and serves as the basis for the quality of quantum random number generators (QRNGs) which promise to produce 'true randomness' [78, 105, 125].

Randomness is a subtle concept, and many different definitions of randomness exist. Indeed, there is much philosophical disagreement as to what exactly the notion of randomness is, and how it relates to indeterminism, chance and unpredictability [50]. Hence, although there is an intuitive connection between quantum indeterminism and randomness, we should be cautious in claiming that quantum value indefiniteness immediately guarantees the randomness of quantum measurements. It is instead important to study precisely what form of randomness (if any) manifests itself in quantum measurements, and to understand exactly what can be guaranteed of devices such as QRNGs.

In this chapter we look more closely at various notions of randomness and the extent to which they are present in quantum measurements. We show how, in addition to providing physical access to an objective probability distribution, quantum value indefiniteness can certify that infinite sequences of quantum measurement results are strongly incomputable. This goes beyond what is certified by the objective probability distribution alone, showing a stronger, algorithmic form of unpredictability. We finally propose a QRNG that, via the Kochen-Specker theorem, is certified to produce such

incomputable sequences in the infinite limit.

5.1 The concept of randomness

5.1.1 Chance-based notions of randomness

The notion of randomness has long been associated with probability. In cryptographic settings, for example, randomness usually refers to uniformly distributed random variables: random bits are those which are generated independently and identically, with equal probabilities of 0 and 1 [140]. As a notion of randomness this is problematic for the same reason that, as we discussed in Sec. 3.1, probability alone does not guarantee any form of indeterminism. Probability distributions are only a mathematical tool and may hide an underlying determinism or patterns, instead expressing an epistemic (even uniform) uncertainty regarding the bits produced. There are, for example, computable Borel normal sequences such as Champernowne's constant, $0100011011000\ldots$, created by appending the binary representation of every integer $0, 1, 2, \ldots$ [34]. A deterministic device outputting such a sequence would appear, in the limit, to be producing statistically uniform bits, and an unknowing observer could well model this as a uniform distribution, despite the clear absence of randomness. Thus, the fact we represent a system probabilistically certainly falls short of providing a sufficient condition for, let alone a definition of, randomness. Nonetheless, there is at least an intuitive connection between randomness and probability, and a good definition of randomness should at least explain the relation between these two concepts [50].

Randomness, rather than being necessarily associated with probabilities, seems rather to be related to *objective* probability distributions; that is, scenarios where the probability distribution represents objective chance, rather than an epistemic lack of information. Indeed, randomness has historically been intimately connected to the notions of chance and indeterminism, and these concepts have often been conflated in the literature. Hellman, for example, has argued that physical randomness and indeterminism are essentially the same concept [74]. This identification of indeterminism and randomness appears to be one of the principal reasons behind the belief that quantum measurements are intrinsically random [8], although often this link is implicit rather explicit. Eagle argues strongly against this 'commonplace thesis' that chance and randomness are not merely related, but one and the same concept [50]. He argues that not only does this trivialise the argument for randomness, but this thesis ignores other important aspects of randomness such as unpredictability, and avoids scientifically fruitful notions of product randomness and the existence of examples that appear to show scenarios that are 'chancy' but intuitively not random.

While quantum value indefiniteness, either via blind assumption or, more plausibly, deduced via the Bell and Kochen-Specker theorems, shows that quantum mechanics indeed contains such indeterministic, 'chance' events, this alone does not show that quantum measurements are indeed random.

5.1.1.1 Randomness as unpredictability

Rather than attributing quantum randomness directly to value indefiniteness, some authors have taken the subtly different approach of identifying the unpredictability provided by value indefiniteness as the feature providing randomness. Kofler and Zeilinger, for example, attribute 'objective randomness' in quantum mechanics to the fact that we can do no better than make probabilistic guesses in predicting measurement results [81]. Fitzsimons et al. go a step further, and define 'intrinsic randomness' as unpredictability with unlimited computational power [56], although they fail to define precisely this notion of unpredictability. As with Kofler and Zeilinger, they see indeterminism (i.e., value indefiniteness) as providing an assurance that this unpredictability is ensured.

The use of unpredictability in these arguments, however, appears to play a rather shallow role, and rather than providing a formal model of unpredictability they seem rather to equate unpredictability with indeterminism. This point of view seems to originate with Laplace's infamous demon, an argument that he laid out in *A Philosophical Essay on Probabilities* [82]:

> We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.

Laplace's demon is often (mis)interpreted as showing that determinism leads to a notion of absolute predictability, and the subsequent equivalence between indeterminism and unpredictability. This analysis ignores the fact that many classical systems may contain intrinsic, if epistemic, unpredictability as a result of sensitivity to initial conditions and chaotic mixing [12, 85]. One can hardly criticise Laplace for this oversight, since his essay predates Poincaré's seminal work on the instability of the three-body problem by some 90 years [107], but such deterministic unpredictability is well understood today [146]. Laplace's demon should instead be understood as a formulation of determinism [50],

and indeed the predicting demon he proposes is not physical: the inexact nature of measurement is fundamental, so we can never obtain the complete state exactly. Further, the analysis the demon would have to undergo in order to predict the future of every body in the universe would require, at the very least, infinite memory and computational power just to write and process the exact phase space coordinates of all such bodies.

Thus, although the attempt to argue for quantum randomness from unpredictability may indeed be a reasonable approach, one should not assume *a priori* that such unpredictability follows directly from indeterminism. Instead, the notion of unpredictability needs to be worked through much more carefully.

Several of the more promising philosophical efforts towards providing a more satisfactory definition of randomness have indeed taken this approach and singled out the unpredictability of random events as the characteristic property of randomness. Eagle, for example, developed a particular notion of unpredictability and defines randomness as maximal unpredictability [49]. Longo has argued for a more relativised notion of randomness, considering it to be unpredictability within a given formal system, where unpredictability is essentially relative to the physical measure, such as the approximation of initial conditions [30]. A key aspect of unpredictability is that, rather then being a consequence of objective indeterminism, it arises at the interface of measurements of a physical system and the formal description of the system, and must be formulated carefully in such terms [85]. If randomness is defined in terms of unpredictability in such a way it thus takes on a subjective element. Given the problems associated with equating randomness with objective indeterminism, this should not necessarily be seen as problematic, nor need it detract from the status of quantum randomness which nevertheless appears to be based on the intrinsic value indefiniteness within the theory [50].

Thus, while quantum measurements are routinely claimed to be intrinsically random, this largely results from a conflation of the concepts of randomness, indeterminism and unpredictability, which we have argued are in fact distinct concepts. In any case, there is more to the issue than a trivial implication from value indefiniteness to randomness, and value indefiniteness certainly does not 'confirm the existence of a new form of randomness' [8].

It is nonetheless clear that there is a relation between these concepts, and, intuitively, value indefiniteness provides a form of unpredictability. Unpredictability is a good candidate as *a* form of randomness, but in order to draw any conclusions about quantum randomness from this, one needs to consider it within a reasonable, general, formal framework. We will return to the issue of modelling unpredictability and develop such a framework, as well as applying it to quantum randomness, in Chapters 6 and 7.

5.1.2 Algorithmic notions of randomness

In addition to unpredictability, a further intuitive property of randomness is the absence of patterns. Indeed, if an infinite sequence of events exhibits pattern or order, this would seem to indicate that the sequence is not random. The absence of patterns is a particularly important feature of randomness in cryptographic settings, since cryptography relies on the use of random bits not containing any pattern that an adversary can exploit [50]. This is of course related to the issue of unpredictability discussed in the previous section, since patterns, intuitively, would give an adversary a method of prediction which could potentially be used to break a cryptographic scheme.

The notion of randomness as the absence of patterns has been rigorously formalised and studied in the field of algorithmic information theory (AIT) [29, 47]. Thus, in contrast to the lack of consensus over notions of randomness based on unpredictability and indeterminism, the notion of algorithmic randomness is well defined and its properties are, mathematically, well understood.

In AIT, the randomness of finite bitstrings is expressed as their inability to be compressed by a universal Turing machine; that is, random strings have Kolmogorov complexity at least equal to their length in bits. This incompressibility expresses the inability for a Turing machine to exploit any patterns within the string to compress it; such strings are, in a sense, maximally random.

This approach to the randomness of finite strings is, on the other hand, problematic as an absolute notion of randomness, since the complexity of any string is only fixed up to a constant depending on the universal Turing machine used. Thus, in order to develop a more rigorous notion of algorithmic randomness it is necessary to consider the limit case of infinite sequences of bits.

A particularly surprising and fundamental result in AIT is that no infinite sequence $\mathbf{x} \in \{0,1\}^\omega$ has every prefix, that is, $\mathbf{x} \upharpoonright n$ for $n \geq 1$, incompressible, even by a fixed finite number of bits [29]. Thus, in a rigorous sense, there are no maximally random sequences. This surprising conclusion can be emphasised even more explicitly by a result that, in fact, predates the development of algorithmic information theory, coming instead from Ramsey theory. This result shows that there are certain types of patterns present in *every* infinite sequence [65, 133]. As a result, there are no 'truly' or 'absolutely' random sequences; for infinite sequences these are mathematically vacuous notions.

In order to develop a consistent notion of algorithmic randomness, one must instead use the more subtle notion of prefix-free Kolmogorov complexity. Maximally random finite strings of length n have, under this complexity measure, complexity of order $n + \log n$, rather than of order n. As before, there are no infinite sequences $\mathbf{x}$ with all prefixes $\mathbf{x} \upharpoonright n$ being maximally random, but there are sequences for which all such pre-

fixes are incompressible, that is, having prefix-free complexity of order n. It is precisely these sequences which are algorithmically random, and are sometimes called Martin-Löf random.

The algorithmically random sequences contain no patterns allowing them to be compressed by a prefix-free Turing machine, and as such form a rigorous definition for a sequence of random objects. While there are other variations and degrees of algorithmic randomness [47], it is certainly the most accepted as an intuitively reasonable, yet rigorous, definition of randomness [50]. Furthermore, irrespective of how much one strengthens the notion of randomness, one can never achieve the vacuous notion of absolute algorithmic randomness; there is instead an infinite hierarchy of notions of randomness [47].

The notion of algorithmic, or Martin-Löf, randomness succeeds in capturing an important intuition about random events. The notion of randomness as an objective notion of (uniform) probability fails to completely capture this absence of patterns that algorithmic randomness addresses: it provides a probabilistic guarantee of this, since almost all sequences (in the measure-theoretic sense) are Martin-Löf random, but is unable to guarantee the absence of computable patterns completely. Furthermore, the non-existence of maximally random sequences shows that we should resist any urge to refer to quantum (or any other form of) randomness as being 'absolute' or 'true' randomness.

5.1.3 Process and product randomness

The two approaches to defining a notion of randomness that we have outlined – the first drawing on the notions of chance and unpredictability, the second on an algorithmic notion of incompressibility – represent fundamentally different conceptual approaches. The first seeks to formalise a notion of randomness for processes and events, while the second defines a notion of randomness for the output (in the infinite limit) of such processes, and is sometimes referred to as *product randomness* [50].

There is nonetheless a connection between these process and product notions of randomness, since an objective probability distribution of the type present in quantum mechanics will, with probability one, produce an algorithmically random sequence in the infinite limit. Conversely, all algorithmically random sequences are Borel normal, and hence fulfil the statistical predictions of a uniform distribution.[7] Indeed, the Martin-Löf formulation of algorithmic randomness shows that random sequences are precisely those which are typical, in a formal sense, with respect to the measure in question.

[7]Both the notions of Martin-Löf randomness and Borel normality can be generalised to other probability measures [2, 29], although their connection to patternlessness becomes murkier, especially with more complicated probability measures [50].

Both these approaches are valid, and in practice one generally wants not only an unpredictable process generating bits, but also a patternless sequence. In cryptography, for example, it is essential to be able to generate bits unpredictable to an adversary, and ideally ones that are not predetermined in any way. But on the flip-side, when using such bits, for example, as a one-time pad, one ideally wants them to be patternless. To illustrate this point, note that even if the string of n 0s, $000\ldots0$, has the same probability of being produced by an objective uniform probability source as any other string of length n, namely 2^{-n}, few people would be happy to use this string as a one-time pad.

Thus, while unpredictability may appear the most sensible route to formalising process randomness – and indeed it is essential if one wishes to formalise a notion of randomness for *individual* events –, it appears that the algorithmic notion of randomness is equally invaluable. Instead of attempting to define a unified notion of randomness, it is perhaps more sensible to keep these two notions of randomness separate, although there is, as discussed, a deep link between the two. Hence, one should be ever more wary of claims of absolute randomness, and instead focus on clearly identifying *which* forms of randomness are present in particular physical phenomena.

In quantum mechanics, the claims of quantum randomness focus almost uniquely around the process notion of randomness. Since quantum value indefiniteness provides certification of the ontological nature of the distribution specified by the Born rule, it seems plausible that one can formalise the unpredictability this provides and hence clarify the nature of such randomness. Nonetheless, in order to conclude that value indefiniteness indeed certifies a form of randomness, this process of formalisation is essential. We will return to this issue in Chapter 7, and show that, with respect to a specific generalised model, value indefiniteness indeed leads to unpredictability. However, we reiterate that we should not view this randomness as 'true' or 'absolute', since it does not address the product of quantum measurements, and in the formal sense we have discussed, true randomness is mathematically impossible.

Recently there has been a new generation of QRNGs that claim to produce randomness certified in a device-independent manner by the violation of Bell inequalities [105, 139]. These QRNGs rely on the violation of these inequalities to show the impossibility that the generated bits were predetermined classically. As such, they certify a form of value indefiniteness, rather than randomness. Moreover, as we discussed in the previous chapter, the violation of such inequalities only allows one to conclude value indefiniteness under additional, although perhaps reasonable, physical assumptions. Thus, not only is this certification necessarily relative to these physical assumptions, it can only be seen as a form of randomness if the connection between value indefiniteness and randomness, which we have argued is nontrivial, is better understood.

In summary, while value indefiniteness intuitively suggests unpredictability, and hence a form – although not an absolute notion – of randomness, such a connection requires further clarification within a formal framework. Moreover, such certification from value indefiniteness provides no certification of any algorithmic form of randomness. Thus, in order to better understand the quality of quantum randomness, we need to look more closely at whether value indefiniteness has any connection to such algorithmic product notions of randomness.

5.2 Incomputability of quantum random sequences

While value indefiniteness, via the Kochen-Specker theorem, gives a formal basis to the notion of quantum indeterminism and the objective nature of the quantum probability distribution, is it possible to use value indefiniteness to guarantee any algorithmic, product notions of random, even to partial extent? Initially, it might seem like such a question is futile, since, if one considers a scenario of 'maximal misalignment' between preparation and measurement contexts, the Born rule specifies that quantum measurement outcomes are uniformly distributed, and hence the sequence formed by concatenating the outputs of such measurements is, in the infinite limit, algorithmically random with probability one. However, simply because the set of non-random sequences has measure zero does not mean that it is *impossible* to obtain such sequences.

The issue of probability zero events is a particularly subtle one [159], and it is problematic to view such events as impossible, especially in infinite measure spaces. Indeed, every individual sequence has probability zero, and yet *some* sequence not only can, but must be obtained. Furthermore, under a frequentist interpretation of probability, such an identification is problematic even for finite strings, since an event can still (even infinitely often) occur so long as its limit frequency is zero.

It may seem like the desire to guarantee algorithmic properties of quantum randomness is a moot point, since the probability zero difference between guaranteeing their presence and the probability one assurance of their presence would seem to have little practical benefit. However, such a result would be conceptually important in understanding the nature of quantum randomness, and would show an explicit difference between quantum randomness and classical forms of randomness.

While we are unable to show from value indefiniteness alone that quantum random sequences are algorithmically random – for reasons which we will discuss – we show that they are bi-immune, a strong form of incomputability and a weaker notion of product randomness, still beyond the reach of any classical source of randomness.

5.2.1 Physical assumptions

As was the case with value indefiniteness, there is no absolute way to be sure that sequences of bits generated by quantum measurements must be random, or even incomputable. Of course, just as for value indefiniteness, one can simply assume this to be the case, but without further evidence this would be completely unjustified. Instead, we must once again make some reasonable assumptions in order to proceed.

In giving a physical interpretation to the results of Theorem 34 locating quantum value indefiniteness we made use of the EPR principle regarding the existence of definite values relating to observable properties. By using the EPR principle to motive a further physical assumption, formalising and generalising the ideas from [31], we show that sequences produced by quantum measurements are bi-immune, a strong form of incomputability [3].

Let us consider a system which we prepare in a quantum state $|\psi\rangle$, measure the observable P_ϕ where $0 < |\langle\psi|\phi\rangle| < 1$ producing a single bit, rinse and repeat in an algorithmic fashion *ad infinitum*. Let $\mathbf{x} = x_1 x_2 \cdots \in \{0,1\}^\omega$ denote the infinite sequence produced by concatenating the outputs of these measurements. Let r_i denote the physical realisation of the ith preparation of the state $|\psi\rangle$, and v_i the faithful value assignment function for r_i.

If there exists a computable function $f : \mathbb{N} \to \{0,1\}$ such that, for every i, $f(i) = x_i$, then this function f gives an effective procedure to compute *in advance* the result of each measurement. It is crucial that f be computable: there exists such a function for any sequence of outcomes, but if it is not computable it does not give us any method to predict its values. Furthermore, it is essential that this condition only be applied to infinite sequences, since computability is only a meaningful concept at this infinite limit; it is clear that any technique which allows prediction of every measurement with certainty must also do so when the measurements are continued *ad infinitum*.

Thus, using the EPR assumption, we formulate the

Computable elements of reality assumption: If there exists a computable function $f : \mathbb{N} \to \{0,1\}$ such that for every i, $f(i) = x_i$, then there is a definite value associated with the observable P_ϕ measured at each step. That is, the ith realisation of $|\psi\rangle$, r_i, has $v_i(P_\phi) = f(i)$ and thus P_ϕ is value definite for r_i.

We note that the assumption above does not postulate the existence of an effective way to find or to compute the computable function f: *such a function simply exists*. Furthermore, we follow EPR in noting that this is certainly only a sufficient condition for definite values to be present; it is by no means a necessary condition, and there may be other perfectly reasonable conditions under which value definiteness can be deduced.

5.2.2 Bi-immunity of x

Let us once more consider the infinite sequence $\mathbf{x}$ produced in the manner described above by a hypothetical experiment run *ad infinitum*. We show that, as long as the observable P_ϕ measured is value indefinite, the infinite sequence $\mathbf{x}$ must be bi-immune: it can contain no infinite computable subsequence.

This result relies not only on the computable elements of reality assumption, but also the measurement assumption, since we must assume that $\mathbf{x}$ is actually produced (not that, for example, all infinite sequences are generated in different universes).

Theorem 47. *Let $\mathbf{x} \in \{0,1\}^\omega$ be an infinite sequence produced by repeated preparation of a state $|\psi\rangle$ followed by measurement of a value indefinite observable P_ϕ in an algorithmic fashion as described above. Then, assuming the measurement and computable elements of reality assumptions, the sequence $\mathbf{x}$ is bi-immune*

Proof. For the sake of contradiction let us assume that $\mathbf{x}$ as described above is computable. Then, by definition, there must exist a Turing machine T (and thus a computable function) that can be associated with $\mathbf{x}$ allowing us to predict with certainty every value x_i. From the computable elements of reality assumption, it follows that for each realisation r_i of $|\psi\rangle$, the observable P_ϕ is value definite under any faithful assignment function v_i, and that $v_i(P_\phi) = x_i$. However, this contradicts directly the value indefiniteness of P_ϕ, and hence $\mathbf{x}$ cannot be computable.

We can generalise this to show that it cannot be bi-immune either. Let us assume, for the sake of contradiction, that $\mathbf{x}$ is not bi-immune, and hence contains a computable subsequence. This means that there exists an infinite computable set A and a computable function $T : A \to \{0,1\}$ such that, for all $n \in A$, $T(n) = x_n$. Since A is computable, one can perform the sub-experiment that consists of discarding each repetition i if $i \notin A$; since A is computable this is also an algorithmically performed experiment. This sub-experiment produces precisely the computable subsequence of $\mathbf{x}$ as output. But as we showed above, this is in contradiction with the value indefiniteness of the observables measured for every repetition, and once again we arrive at a contradiction, and hence $\mathbf{x}$ is bi-immune. □

More importantly, using our physical interpretation of Theorem 34 stated in Proposition 45, this allows us to show that, under the same physical assumptions leading to value indefiniteness, one obtains also bi-immunity.

Corollary 48. *Let $\mathbf{x} \in \{0,1\}^\omega$ be an infinite sequence produced by repeated preparation of a state $|\psi\rangle$ in dimension $n \geq 3$ Hilbert space, followed by measurement of an observable P_ϕ for $|\phi\rangle \in \mathbb{C}^n$, $0 < |\langle\psi|\phi\rangle| < 1$, in an algorithmic fashion as described above. Then,*

assuming the eigenstate, noncontextuality, measurement and computable elements of reality assumptions, the sequence **x** *is bi-immune*

We note briefly that these results are more general than those proved in [31], since they make use of the ability to locate value indefiniteness and do not require any assumption about the uniformity of the bits produced. We also note once more the importance of the physical hypotheses made. As for the interpretation and conclusion of value indefiniteness from the Kochen-Specker theorem, the bi-immunity of quantum randomness is necessarily relative to the physical assumptions made, and it is impossible to give an absolute certification of such a notion of randomness.

The bi-immunity of quantum randomness we have proven is certainly a weaker notion of product randomness than the ideal of algorithmic randomness. Bi-immunity, as a strong form of incomputability, is independent of the physical measure, and does not rely on the uniformity of bits generated, whereas Martin-Löf randomness does, even though it can be formulated for different measures. Value indefiniteness, in representing the absence of physical reality corresponding to the outcomes of measurements, is also independent of the measure used. Indeed, if a system is prepared in a state $|\psi\rangle$, then any observable P_ϕ is value indefinite as long as $0 < |\langle\psi|\phi\rangle| < 1$, and hence has no requirement that the probability of measuring a 1 be 0.5.

Thus, in order to guarantee Martin-Löf randomness, one needs something more than value indefiniteness, a way to combine the distribution predicted by the Born rule with the bi-immunity provided by value indefiniteness. It remains an open question to find a way to combine these aspects of quantum mechanics in such a way as to do so.

5.3 Quantum random number generators

A lot of effort has been devoted to attempting to exploit quantum randomness in order to generate random numbers. The classical approach to random number generation is to use pseudo random number generators (RNGs). These are mathematical formula or, more generally, algorithms which, starting with a small 'random' seed, usually extracted from some physical or user generated data, compute a sequence of bits which appears statistically random [140]. By their very nature, such methods are entirely deterministic: once the initial seed is chosen the entire pseudorandom sequence is uniquely determined. In the infinite limit, such a sequence is thus guaranteed to be computable, whereas one would expect, with probability one, a sequence sampled from a true uniform distribution to be algorithmically random. Furthermore, in most real cases, pseudorandom sequences are eventually cyclic. Instead, effort is generally made to make such sequences computationally difficult to distinguish from those generated by a uniform distribution [140],

as this provides a level of cryptographic security. Nonetheless, it is clear that although pseudorandom sequences are designed to look random, they are not. Indeed, issues with pseudo RNGs have led to many real-world cryptographic problems, and are increasingly important in real-world security. While there have been some efforts to use physical phenomena, such as chaotic behaviour, to produce random numbers, these have suffered from various issues [127] and have not seen much practical success. Given the prevailing interpretation of quantum mechanics as a fundamentally indeterministic theory, it is thus natural to try and use quantum phenomena to address these issues; in particular to try and build practical quantum random number generators (QRNGs).

Some early such approaches made use of the timing of radioactive decay [119], while others have looked to make use of quantum mechanical noise in electrical circuits [120]. The majority of research, however, has focused on cleaner quantum systems, usually photonic systems, which have simple theoretical descriptions and can be easily modelled, allowing better control over the probability distribution produced, as well as being capable of producing the high bitrates required in many practical applications [78].

The simplest, and perhaps most popular, approach uses beamsplitters to produce photons in a 50-50 superposition of polarisation states, before measuring this polarisation using, for example, polarising beamsplitters [113, 129]. This technique has been applied, amongst other uses, to show violation of Bell inequalities under strict locality conditions [78] and as a one-time pad to encrypt sequences [143]. Many variations have been presented, including techniques that use entangled photon pairs in order to increase the bitrate [68] or decrease bias [55].

A particularly noteworthy example is that of Stefanov et al. [125]. Their approach, although very simple, has led to the most successful commercial QRNG to date, Quantis [76], produced by ID Quantique in Geneva. As a result, it is possible to buy and test such devices; a detailed analysis showed some detectable correlation to be present, apparently the consequence of poor normalisation techniques [1], although this does not impact the quantum nature of the outcomes.

More recently there have been several devices proposed that, instead of using polarisation or related beamsplitter techniques to generate bits, make use of photon arrival times [59, 126, 142, 144]. For example, by dividing time into blocks of an equal, sufficiently short, period, one can assign a photon detection a 0 or 1 depending on whether it was detected in an even or odd numbered block [48]. This method has also seen several commercial devices [104, 112], although not (yet) with the same popular success as Quantis.

This approach has the advantage that it allows much higher bitrates to be readily achieved, but it sacrifices much of the theoretical clarity of the beamsplitter-based approaches. With beamsplitter-based QRNGs, one can describe simply the superposition

of quantum states and the observable giving rise to the bits obtained upon measurement. In timing-based approached, on the other hand, this is not the case: the time being measured does not correspond to any quantum observable nor, by extension, value indefiniteness, and instead analysis of photon statistics is generally used. As such, it is much more difficult to identify precisely the quantum origin of the random bits, and hence any clear theoretical certification is somewhat more difficult.

A final approach, that has a slightly different conceptual stance, is the use of Bell or noncontextuality inequality violation in order to certify random number generation. This was first proposed by Pironio et al. [105], and since then many further variations have been considered [139, 141]. This approach uses pairs of particles (ideally photons, but due to constraints in closing the detection loophole in Bell's theorem existing implementations have sometimes used atoms in traps) and tests violation of the inequalities. As a byproduct of the measurements made in testing the inequalities, this produces bits much as in other QRNGs, but with the added advantage that, by ensuring the equalities are violated, it is possible to certify that the generated bits cannot have been produced classically.

Such an approach, although not providing a better source of quantum random bits, allows one to verify the quantum nature of the device, which has particular relevance in device-independent quantum cryptography, where one needs random numbers but cannot necessarily trust the devices they have access to [105]. Technically, such results require some initial randomness, and hence act as randomness expanders rather than generators [40]. The violation of Bell or noncontextuality inequalities allows one to certify the nonclassicality of the RNG, but, in order to guarantee that the numbers are truly generated indeterministically, they require the assumption that this nonclassicality allows us to conclude that the devices are indeed quantum mechanical, and further that quantum measurements are indeed indeterministic, as is the case with the other QRNGs discussed. The Bell inequality violation is indeed an important resource for cryptography, but one must keep in mind that, as for the Kochen-Specker theorem, this need not *a priori* imply the intrinsic indeterminism of the associated measurement outcomes.

5.4 A proposed QRNG certified by value indefiniteness

As we have shown in the previous chapter, under simple physical assumptions, it is possible to show that almost all quantum observables are value indefinite in $n \geq 3$ dimensional Hilbert space. Thus, this value indefiniteness can be used to more care-

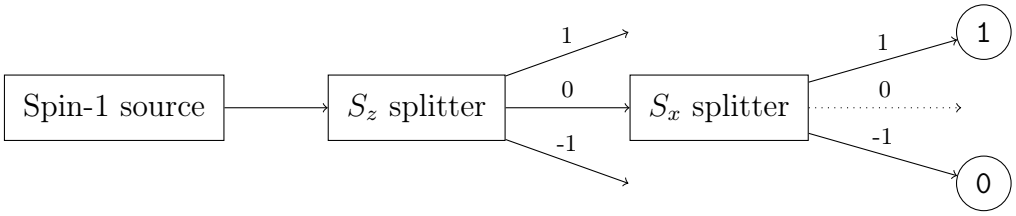


Figure 5.1: Experimental schema for a configuration of a quantum random number generator producing bits certified by quantum value indefiniteness.

fully justify, or certify, the randomness produced by QRNGs. Such a certification is not device-independent, but instead a form of certification that allows us to explain more precisely the advantage of QRNGs, and why they indeed are not bound to produce computable, pseudorandom sequences like classical devices. This complements, not contradicts, device-independent certification.

Unfortunately, most of the QRNGs proposed thus far operate in two-dimensional Hilbert space, where Theorem 34 does not apply. Furthermore, the timing-based schemes do not allow one to easily attribute the bits to value indefinite observables.

Here we propose a schema for a simple, optical QRNG, operating in three-dimensional Hilbert space and hence certified by value indefiniteness.

5.4.1 Experimental schema

Figure 5.1 shows the conceptual schema for the proposed QRNG. Spin-1 particles are prepared in the $S_z = 0$ state, and then the incompatible S_x observable is measured. Since $\langle S_z = 0 | S_x = 0 \rangle = 0$ and $\langle S_z = 0 | S_x = \pm 1 \rangle = \frac{1}{\sqrt{2}}$, measurement of the S_x observable will yield the values ± 1 with probability 0.5 each, and 0 with probability zero. By the eigenstate assumption, since the $|S_z = 0\rangle$ state is an eigenstate of the S_x observable, the $P_{S_x=0}$ observable is value indefinite and hence we *cannot* obtain the outcome 0 in the ideal case, a stronger statement than this merely being true with probability zero.

Since the proposed setup uses spin-1 particle, it operates in a three-dimensional Hilbert space. Despite this, the construction ensures that the measured value is nonetheless a binary, rather than tertiary value, as is usually desired in RNGs. As a result of this dimensionality, the system is guaranteed to contain value indefiniteness as a result of Proposition 45, and in particular, since $\langle S_z = 0 | S_x = \pm 1 \rangle = \frac{1}{\sqrt{2}}$, the projection observables $P_{S_z=\pm 1}$ are value indefinite under any faithful value assignment function. Since S_x can, by the Spectral Decomposition theorem [130], be decomposed as $S_x = \sum_{a \in \{-1,0,+1\}} P_{S_x=a}$, S_x is similarly value indefinite, and hence the measurement produces a result of ± 1 which cannot have been determined prior to measurement, that

is, indeterministically.

Thus, rather than assuming the measured observables are value indefinite, as is the case with most existing systems operating in a two-dimensional Hilbert space, for our proposed schema this can be based on the eigenstate and noncontextuality assumptions used to interpret Theorem 34. As a result, the bits produced by this QRNG design are certified by quantum value indefiniteness in a way not possible with existing proposals.

5.4.2 Robustness to misalignment

Before we proceed to describe a possible explicit realisation of the QRNG outlined above, we wish to briefly make a couple of points on the robustness of this certification by value indefiniteness to experimental imperfections.

We can describe the measurement context more generally by the spin observable $S(\theta, \varphi)$, where θ and φ are the polar and azimuthal angles respectively, and we thus have $S_x = S(\pi/2, 0)$ and $S_z = S(0, 0)$. Explicitly, using the standard orthonormal S_z basis with $|S_z = +1\rangle = (1, 0, 0)$, $|S_z = 0\rangle = (0, 1, 0)$, and $|S_z = -1\rangle = (0, 0, 1)$, this operator is represented in matrix form as

$$S(\theta, \varphi) = \begin{pmatrix} \cos(\theta) & \frac{e^{-i\varphi}\sin(\theta)}{\sqrt{2}} & 0 \\ \frac{e^{i\varphi}\sin(\theta)}{\sqrt{2}} & 0 & \frac{e^{-i\varphi}\sin(\theta)}{\sqrt{2}} \\ 0 & \frac{e^{i\varphi}\sin(\theta)}{\sqrt{2}} & -\cos(\theta) \end{pmatrix}. \tag{8}$$

Misalignment and imperfection in an experimental setup will, in general, lead to angles θ and φ differing slightly from $\pi/2$ and 0 respectively. While a change in φ only induces a phase shift and does not alter the probability of measuring any particular eigenvalue, a change in θ will alter the probabilities of detection.

A detailed calculation (e.g., by diagonalising $S(\theta, \varphi)$ to find its eigenvalues) finds that in general we have

$$|S(\theta, \varphi) = +1\rangle = \left(e^{-2i\varphi}\cos^2\frac{\theta}{2}, \frac{e^{-i\varphi}\sin\theta}{\sqrt{2}}, \sin^2\frac{\theta}{2} \right),$$
$$|S(\theta, \varphi) = -1\rangle = \left(e^{-2i\varphi}\sin^2\frac{\theta}{2}, \frac{e^{-i\varphi}\sin\theta}{\sqrt{2}}, \cos^2\frac{\theta}{2} \right),$$

and hence

$$|\langle S_z = 0 | S(\theta, \varphi) = \pm 1\rangle| = \sin\theta/\sqrt{2},$$

meaning that the probability of obtaining a $+1$ or -1 when measuring the S_x observable remains equal even when θ is not exactly $\pi/2$. Thus, if we discard any outcomes of 0 and identify $+1$ and -1 with 0 and 1 respectively, the sequence generated should obey a uniform distribution even when this misalignment is present.

Although there are bound to be other experimental imperfections which will lead to bias in any actual experimental implementation, this eliminates one major source of bias, in effect converting the misalignment into a loss of efficiency (since we discard the measurements yielding 0, which should theoretically never occur) instead of bias. This is in distinct contrast to setups based on single beamsplitters, in which misalignment introduces bias into the distribution of bits [1, 28]. Furthermore, this misalignment does not affect in any way the certification by value definiteness: unless the misalignment is maximal (in which case no bits will be produced anyway), the conditions of Theorem 34 will be satisfied.

5.4.3 Proposed realisation using generalised beamsplitters

Since it is not particularly feasible to directly use spin-1 particles in a QRNG with an acceptably high bitrate, we present an outline of a possible realisation using photons that is expressed in terms of generalised beamsplitters [114, 164]. Generalised beamsplitters are based on the possibility to decompose an arbitrary unitary transformation U_n on n-dimensional Hilbert space into two-dimensional transformations U_2 of two-dimensional subspaces thereof, a possibility that can be used to parametrise $U(n)$ [95]. In more physical terms, they amount to serial stacks of phase shifters and beamsplitters in the form of an interferometer with n input and output ports such that the beamsplitters act on only two (sub-)paths each, which, together with the phase shifters (affecting single paths at any one time), realise the associated transformations in $U(2)$. These components can be conveniently arranged into 'triangle form' with n in- and out-bound beam paths.

In order to realise an arbitrary spin observable $S(\theta, \varphi)$, the eigenvectors of the corresponding matrix given in (8) form the rows of a unitary matrix which is decomposed into $U(2)$ matrices and can be implemented with beamsplitters and phase shifts [114]. In particular, let us consider the S_x observable, that is, the specific case of $\theta = \frac{\pi}{2}$ and $\varphi = 0$. We then have

$$S_x = S\left(\pi/2, 0\right) = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

with the associated normalised eigenvectors

$$\begin{aligned} |S_x = +1\rangle &= \tfrac{1}{2}\left(1, \sqrt{2}, 1\right), \\ |S_x = 0\rangle &= \tfrac{1}{\sqrt{2}}\left(1, 0, -1\right), \\ |S_x = -1\rangle &= \tfrac{1}{2}\left(1, -\sqrt{2}, 1\right). \end{aligned}$$

These are used to form the rows of the unitary matrix U_x given by the matrix

$$U_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}.$$

While many variations on unitary matrix representations for beamsplitters exist [32, 67, 114, 160], without loss of generality we can represent an arbitrary $U(2)$ matrix realised by a beamsplitter and external phase shift as

$$\begin{pmatrix} \sqrt{T} & ie^{i\phi}\sqrt{R} \\ i\sqrt{R} & e^{i\phi}\sqrt{T} \end{pmatrix},$$

where ϕ represents the phase of an external phase shifter on the second input port, and $T, R \in [0, 1]$ are the transmittance and reflectance of the beamsplitter respectively (with $R + T = 1$). The beamsplitter arrangement to realise U_x can be found by transforming U_x into the identity matrix I_3 by successive right-multiplication by adjoints of $U(2)$ matrices of the above form – each one making an individual off-diagonal element equal to zero – followed by a final set of phase shifters [114].

In our specific case, we have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & -i \end{pmatrix} \cdot \begin{pmatrix} \sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} & 0 \\ i\sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \sqrt{\frac{3}{4}} & 0 & -i\sqrt{\frac{1}{3}} \\ 0 & 1 & 0 \\ i\sqrt{\frac{1}{4}} & 0 & -\sqrt{\frac{3}{4}} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \\ 0 & i\sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} \end{pmatrix} = U_x.$$

This corresponds to three beamsplitters with transmittances $T_{3,2} = T_{2,1} = \frac{1}{3}$, $T_{3,1} = \frac{3}{4}$, and phases $\phi_{3,2} = \phi_{2,1} = -\pi/2$, $\phi_{3,1} = \pi$, where $T_{i,j}$ and $\phi_{i,j}$ are the parameters for the beamsplitter operating on beams i and j (beams 1,2,3 correspond to $S_z = +1, 0, -1$ respectively). Two final phase shifts of $-\pi/2$ are needed on beams 2 and 3. The physical realisation of U_x is depicted in Fig. 5.2.

This setup is equivalent to the spin-1 schema certified by value indefiniteness that is illustrated in Fig. 5.1. This possible realisation with beamsplitters shows that, although needing a three-dimensional system such as a spin-1 particle in order for Kochen-Specker type theorems to apply and thus provide certification via value indefiniteness, these systems can be implemented with readily available optical methods, rather than careful control of spin-1 particles or atoms, greatly improving the bitrate of such devices [35]. Such a beamsplitter implementation, however, unfortunately means that the robustness to bias discussed in the previous section will not hold exactly, since bias at individual beamsplitters may lead to an observable not of the form $S(\theta, \varphi)$ being implemented exactly. However, there exist many unbiasing techniques which can be used to remove bias in such generated streams of bits [1, 2].

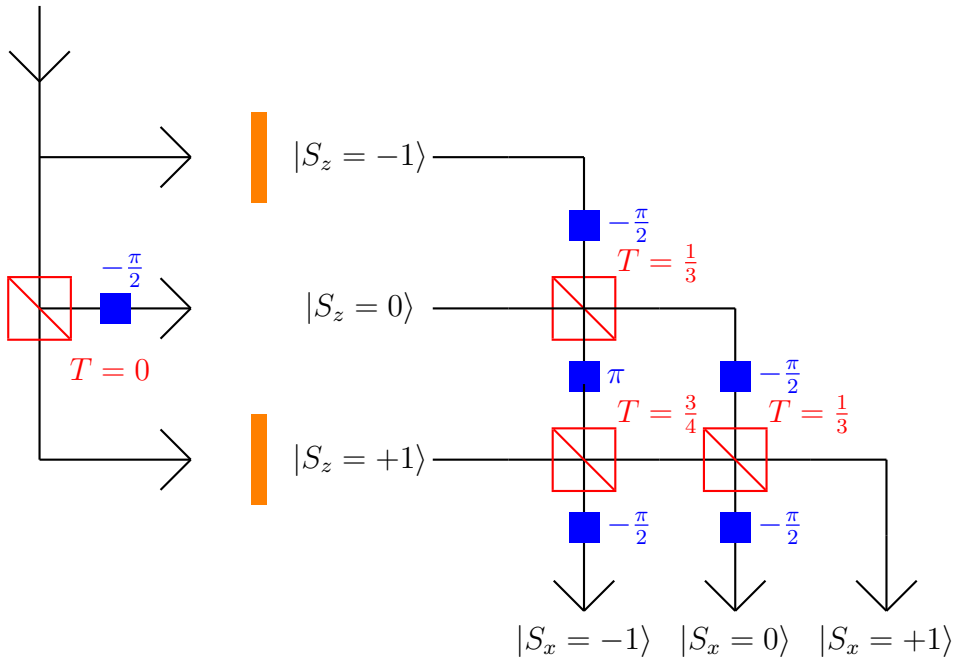


Figure 5.2: Configuration of a QRNG with a preparation and a measurement stage, including filters blocking $|S_z = +1\rangle$ and $|S_z = -1\rangle$. (For ideal beam splitters, these filters would not be required.) The measurement stage (right array) realises a unitary quantum gate U_x, corresponding to the projectors onto the S_x state observables for spin state measurements along the x-axis, in terms of generalised beamsplitters.

Not only is this proposed QRNG certified by value indefiniteness, and thus the bits generated do not correspond to any property existing prior to their generation, as a result of Theorem 47, in the infinite limit, such a device can be guaranteed to produce a bi-immune sequence. Although this is only a limit property, and hence offers perhaps little practical benefit, it highlights the difference between such a device certified by value indefiniteness and pseudo RNGs, which are guaranteed to produce *computable* sequences in the infinite limit.

Chapter 6

Concepts and models of unpredictability

In this chapter, we work towards formalising a framework of (un)predictability which can be used to assess the (un)predictability of arbitrary physical experiments. We first review various notions of unpredictability across several domains: physical and dynamical unpredictability, algorithmic notions of unpredictability, and finally a computational notion based on irreducibility. We then review previous work on generalised models of unpredictability, before motivating and formalising a new model based around the ability for a predicting agent to effectively predict the outcome of experiments using finite information extracted from the system and its environment.

6.1 Physical unpredictability

When we think of unpredictable events in classical physics, perhaps the first such events that come to mind are the archetypical 'random' events: the toss of a die or the flip of a coin. Why are these events considered to be unpredictable? After all, the trajectory of a coin is governed by Newtonian mechanics and is hence uniquely determined the instant it is released by the precise initial conditions. The unpredictability arises not because of any indeterminism, but as a result of two critical facts.

1. Measurement: we can only ever measure an approximation of the precise initial conditions;

2. Sensitivity: the dynamics are sufficiently sensitive to the initial conditions that the approximation garnered by measurement is not good enough for us to predict

the outcome from.

The dependence on the accuracy of measurement of such events was exemplified by a clever experiment by Diaconis et al. [46] who, by carefully controlling the initial conditions, produced perfectly predictable coin flips.

These examples may not be the best examples of classical unpredictability from a technical point of view, but they serve to outline the main contributing factors, which we will now discuss in more detail.

6.1.1 Intervals of measurement

In classical mechanics the state of a dynamical system is represented by a point in the pertinent phase space, which can be mathematically represented as a point in $\mathbb{R}^n$, where n is the number of degrees of freedom of the system. While such a point determines, via the dynamical equations, the trajectory of the system in phase space, it is impossible to know precisely what the state of the system actually is. This follows from the realisation that any physical measurement can only ever yield a rational number, or, equivalently, an interval specifying a continuous range of possible values. This corresponds to determining a *region* of phase space of non-zero measure containing the point representing the state of the system.

This limitation of measurement is somewhat self evident and had been long understood. However, its implication for unpredictability was not recognised until Poincaré, in his famous work on the three-body problem, realised that [107]

> it may happen that slight differences in the initial conditions produce very great differences in the final phenomena; a slight error in the former would make an enormous error in the latter.

Hence, the uncertainty introduced by the unavoidable imprecision of measurement can lead to much greater uncertainty and, ultimately, unpredictability – a phenomenon that Poincaré saw as randomness.

It is important that this role of measurement imprecision not be seen merely as a practical limitation. Although such unpredictability results from an epistemic lack of information, it should nonetheless be seen as a fundamental feature of the theory due to this unavoidable physical role of measurement [85]. Rather, this emphasises that predictability is 'means-relative' in the sense that the degree or scale of unpredictability depends on the abilities of the predicting agent [96].

6.1.2 Dynamical chaos

A particularly important example is that of systems that exhibit dynamic chaos, which include the three-body problem. Indeed, Poincaré was the first to demonstrate that some systems may be not admit analytic solutions and instead exhibit exponential sensitivity to initial conditions [85], and as a result the fundamental interval of measurement around the initial conditions blows up to impair prediction. However, this was followed up by many others including Turing, who described how the 'displacement of a single electron by a billionth of centimetre at one moment might make the difference between a man being killed by an avalanche a year later, or escaping' [137, p. 440], and later Lorenz, with the better known 'butterfly effect' [86], eventually leading to the notion of chaos being more rigorously formalised. Indeed, in some cases it is not only that the solutions to the dynamical equations diverge exponentially fast, but that such analytic solutions do not exist at all [84].

6.1.2.1 Defining Chaos

The notion of chaos tries to capture two main intuitive concepts [146]:

1. Sensitive dependence on initial conditions;

2. Irregular behaviour that 'mixes' trajectories.

The first point is natural based on our previous discussion. The second point, on the other hand, while more subtle is necessary to intuitively capture chaos: the doubling of a real number, for example, exhibits sensitive dependence on initial conditions, since the difference between two close numbers will grow exponentially fast, but this lacks the complexity and unpredictability intuitively necessary for chaos.

Several different approaches to formalising these notions have been proposed [88], but perhaps the most accepted definition is due to Devaney [45].[8]

Definition 49. A dynamical system is chaotic (in the sense of Devaney [45]) if:

1. It exhibits sensitive dependence on initial conditions: arbitrarily close points eventually diverge as the system evolves;

2. The system is topologically transitive: any approximation of a point in phase space contains points whose trajectories will enter every other region of phase space;

3. The set of periodic points is dense in the phase space.

[8] We refer the reader to [45] for formal definitions. We outline only roughly these notions, since we will not need them in any technical detail.

The third condition enforces a certain degree of stability in the system, and has little relevance to unpredictability. Indeed, some definitions of chaos leave out this condition [88].

The condition of topological transitivity, sometimes called topological mixing, is, however, crucial. It shows that, given an approximation of the initial conditions, after a long enough period of time, the system could be anywhere in the phase space. That is, the approximation is useless for prediction too far into the future.

A final property often related to chaos is that of (weak) mixing, which differs slightly from topological mixing. Mixing requires that the set of possible initial conditions contained within a specific interval or region of phase space spread out evenly across the phase space (in a specific measure theoretical sense) as time tends to infinity. Although mixing turns out not to be a sufficient nor a necessary condition for chaos as defined above, some authors have argued that is constitutes an appropriate definition of chaos by itself [146].

6.1.2.2 Properties of chaotic systems

One important feature of these notions of chaos is that they are all limit properties [98]. That is, it is only in the limit of infinite time that their chaoticity is fully expressed. Nonetheless, for any approximation of the initial conditions, this means that after long enough times the properties of chaos will be expressed more and more fully, and thus lead to finite limits on prediction.

It would perhaps seem *prima facie* that chaos has little or no non-trivial relation to algorithmic notions of randomness – indeed, one can have completely computable chaotic systems [148]. Surprisingly, however, there are some nontrivial connections of interest. If one considers suitably effectivised dynamical systems[9] that exhibit weak mixing then the typical points for the dynamics are precisely the Schnorr random points (a form of algorithmic randomness weaker than, but closely related to, Martin-Löf randomness) [60]. In this context, typical points are those which obey a kind of ergodic property, and thus are precisely those expressing the 'mixing' within the system.

In these systems, the Schnorr randomness of this measure-one set of points within the phase space plays an essential role in the mixing behaviour of the system, a property often associated with unpredictability.

6.1.3 Dynamical unpredictability

Unpredictability in classical systems arises not as a result of either the approximation of initial conditions or of chaotic dynamics, but rather because of the interaction between

[9]Specifically, the dynamics should be computable and and take place in a computable metric space.

these two things [85, 146]. That is, the fact that any measurement necessarily results in an interval approximating the state of the system, and this uncertainty in the initial conditions is then blown up in a way that prohibits prediction. Furthermore, this fundamental approximation means that if we repeat the experiment we can do no better than to ensure the initial conditions are the same *up to our limit of approximation*. As a result, if we repeat the experiment with the same approximated initial conditions, the outcome of the experiment will in general be different, since the precise initial conditions would differ.

There is one further, related, element contributing to unpredictability, which is the fact that no real system is ever perfectly isolated. Thus, in addition to the uncertainty inherent in any measurement of the initial conditions of a system, there is a further uncertainty affecting the dynamics resulting from external effects that are not accounted for within the formal model of the system. For example, the gravitational effect of an electron far outside the solar system, although minuscule, is large enough to alter the dynamics of molecules (or even billiard balls) bouncing chaotically on earth in a way that, as a result of the extreme sensitivity of chaos, produces noticeable effects after a short period of time [117].

One normally ignores such effects since they are much harder to formally model than sensitivity to initial conditions, and the interaction alone between chaos and approximate measurement is generally sufficient, if not the dominant effect, to explain the unpredictability in real systems. However, in more complicated systems, such as biological ones, this effect is perhaps as, if not more, important in explaining the manifest unpredictability.

6.2 Algorithmic notions of unpredictability

The physical notions of unpredictability discussed in the previous section present a process-based approach to analysing the unpredictability of particular physical systems. In other words, this approach is centred around the *dynamics* of particular systems.

In contrast, computability theory concerns the properties of finite or infinite sequences of bits, and allows us to ask, for example, whether particular infinite sequences are computable or not – a fixed, non-dynamical, property of a particular sequence [29]. Nonetheless, such properties can be viewed in the context of (algorithmic) unpredictability, since a Turing machine is perhaps the most general notion of an *effectively* predictable process. Thus, the very fact that there are incomputable sequences indicates, perhaps, the existence of absolutely (as opposed to within a particular theory describing a system) unpredictable phenomena. The field of algorithmic information theory allows

for further, more careful analysis, as it formalises various levels of unpredictability and notions of algorithmic randomness [47].

In this section, we will look more closely at several algorithmic notions of unpredictability and the relation between them, and discuss the extent to which they really capture the notion of unpredictability.

6.2.1 Incomputability, bi-immunity and Martin-Löf randomness

The computability of an infinite sequence clearly represents a form of predictability, since it implies the existence of a deterministic Turing machine capable of methodically computing, or predicting, every bit that will appear in the sequence. Incomputability, however, falls short of guaranteeing any real unpredictability, since an incomputable sequence can contain extremely regular behaviour. For example, one can have every even-positioned bit a 0, a simple, infinite, computable pattern within a possibly incomputable sequence. Thus, it seems we need substantially more to consider an infinite sequence unpredictable.

Bi-immunity is a much stronger form of incomputability (indeed it represents a form of maximal incomputability, although not maximal information content or randomness), and appears a more promising candidate for unpredictability. Recall that an infinite bit-sequence is bi-immune if it contains no infinite computable subsequence. Note that the definition requires not only that there is such an infinite subsequence, but that one can compute also its location within the sequence. If this were not the case, any sequence with infinitely many 0s (and thus all incomputable sequences) would contain the computable subsequence $000\ldots$; instead we must be able, for example, to compute the positions of these 0s.

Bi-immunity addresses most of the issues with viewing incomputability alone as unpredictability, since we can only compute or know in advance finitely many bits within the sequence. However, some intuitively predictable sequences are nonetheless bi-immune, such as the sequence produced by doubling each bit in a bi-immune sequence.

Proposition 50. *Let* $\mathbf{x} = x_1x_2\cdots \in \{0,1\}^\omega$ *be a bi-immune sequence. Then the sequence* $\mathbf{y} = x_1x_1x_2x_2\ldots$ *is also bi-immune.*

Proof. Let us assume, for the sake of contradiction, that $\mathbf{y} = x_1x_1x_2x_2\ldots = y_1y_2y_3y_4\ldots$ is not bi-immune. Then, from the definition of bi-immunity, there exists an infinite computable set $K \subset \mathbb{N}^+$ and a computable function $f : K \to \{0,1\}$ such that for all $k \in K$, $f(k) = y_k$.

Since K is infinite, either $K_0 = K \cap \{n \in \mathbb{N} \mid n \mod 2 = 0\}$ or $K_1 = K \cap \{n \in \mathbb{N} \mid n \mod 2 = 1\}$ is infinite, since $K = K_0 \cup K_1$; further both K_0 and K_1 are clearly computable.

If K_0 is infinite then, for all $k \in K_0$, $f(k) = y_k = x_{k/2}$ by the construction of $\mathbf{y}$. Thus, if we choose $K_0' = \{k/2 \mid k \in K_0\}$, and let $f_0 : K_0' \to \{0,1\}$ be defined as $f_0(k) = f(2k) = y_{2k} = x_k$ we see that K_0' and f_0 define an infinite computable subsequence in $\mathbf{x}$, contradicting the bi-immunity of $\mathbf{x}$.

Similarly, if K_0 is finite and hence K_1 is infinite, we proceed as follows. Note that, for all $k \in K_1$, $f(k) = y_k = x_{(k+1)/2}$ by construction of $\mathbf{y}$. Thus, if we choose $K_1' = \{(k+1)/2 \mid \in K_1\}$, and let $f_1 : K_1' \to \{0,1\}$ be defined as $f_1(k) = f(2k-1)y_{2k-1} = x_k$ we see that K_1' and f_1 define an infinite computable subsequence in $\mathbf{x}$, again contradicting the bi-immunity of $\mathbf{x}$.

Note that we do not need to be able to determine which of K_0 and K_1 is infinite, it suffices to know that one of them is. □

Bi-immune sequences can, as we also mentioned in the previous chapter, still contain statistical bias – for example, more 0s than 1s, or in the case of the sequence above, no 01s or 10s – as these need not introduce incomputability in a sequence. However, this is not necessarily a barrier for unpredictability, especially in any objective sense, since such a bias does not allow us to 'say in advance' with any certainty the values of particular bits. Nonetheless, the issue shown in Proposition 50 does need to be addressed, and means bi-immunity also falls short of being a satisfactory notion of unpredictability for sequences.

One possible, extreme, approach is to consider Martin-Löf randomness. Recall that a sequence $\mathbf{x}$ is Martin-Löf random if all prefixes $\mathbf{x}\restriction n$ for $n \geq 1$ cannot be compressed by more than a fixed constant by a universal prefix-free Turing machine. Martin-Löf random sequences thus contain no 'algorithmic' patterns that can be used to compress them. Such patterns could be seen as a form of predictability, so in this sense such random sequences are indeed intuitively unpredictable. However, this notion might be too strong, since it considers even very weak statistical patterns as a form of predictability, even when they do not allow any bit to be known in advance. It does, however, address the types of issues illustrated in Proposition 50.

6.2.2 Tadaki unpredictability

In this section, we present a further notion that represents a good compromise between bi-immunity and Martin-Löf randomness as a candidate for a form of algorithmic predictability with certainty, due to Tadaki [134].

Definition 51. An infinite sequence of bits $\mathbf{x} = x_1 x_2 \cdots \in \{0,1\}^\omega$ is *Tadaki predictable* (or total strongly predictable, in Tadaki's terminology) if there exists a Turing machine $F : \{0,1\}^* \to \{0,1,W\}$ that halts on every input, and satisfies the following two conditions:

(i) for every n, either $F(\mathbf{x}\upharpoonright n) = x_{n+1}$ or $F(\mathbf{x}\upharpoonright n) = W$;

(ii) the set $\{n \in \mathbb{N}^+ \mid F(\mathbf{x}\upharpoonright n) \neq W\}$ is infinite.

F is called a *Tadaki predictor* for $\mathbf{x}$.

If a sequence $\mathbf{x}$ is not Tadaki predictable, we say it is *Tadaki unpredictable*.

As with incomputability, by varying the strength of effectivity endowed upon the predictor, one can strengthen or weaken the notion of unpredictability. While the notion presented is perhaps the most natural, this can be put into practice more generally. For example, one could consider the predictive power of finite state transducers [134], or at the other extreme, of predictors with access to incomputable oracles [47]. However, the Church-Turing thesis [42] privileges the computational model of Turing machines (and all other equivalent models), and thus the notion of Tadaki predictability is perhaps the most reasonable if one wishes to form a realistic, absolute notion of algorithmic unpredictability.

Tadaki predictability can be related to the various other algorithmic notions of unpredictability we have discussed. Perhaps most importantly are the following two results.

Theorem 52 (Tadaki, [134, Theorem 4])**.** *If $\mathbf{x} \in \{0,1\}^\omega$ is a Martin-Löf random sequence, then $\mathbf{x}$ is Tadaki unpredictable*

Theorem 53. *If $\mathbf{x} \in \{0,1\}^\omega$ is not bi-immune, then $\mathbf{x}$ is Tadaki predictable.*

Proof. Assume, for the sake of contradiction, that $\mathbf{x}$ is not bi-immune. Then there is an infinite computable set $K \subset \mathbb{N}^+$ and a computable function $f : K \to \{0,1\}$ such that for all $k \in K$, $f(k) = x_k$. Hence, for a string $y \in \{0,1\}^*$ the function

$$F(y) = \begin{cases} f(|y|+1) = x_{|y|+1}, & \text{if } |y|+1 \in K, \\ W, & \text{otherwise,} \end{cases}$$

is a Tadaki predictor for $\mathbf{x}$. □

Furthermore, the notion of Tadaki unpredictability is strictly stronger than bi-immunity, since there exist bi-immune, Tadaki predictable sequences.

Fact 54. *There exists a sequence $\mathbf{x} \in \{0,1\}^\omega$ such that $\mathbf{x}$ is bi-immune and Tadaki predictable.*

Proof. Let $\mathbf{x} = x_1x_2\ldots$ be a bi-immune sequence. As we showed in Proposition 50, the sequence $\mathbf{y} = y_1y_2\cdots = x_1x_1x_2x_2\ldots$ created by doubling the bits of $\mathbf{x}$ is also bi-immune. However, $\mathbf{y}$ has a Tadaki predictor F defined for all $z = z_1\ldots z_n \in \{0,1\}^n$ as

$$F(z_1\ldots z_n) = \begin{cases} z_n, & \text{if } n \text{ is odd,} \\ W, & \text{if } n \text{ is even,} \end{cases}$$

since this correctly predicts the value of every bit at an even position in $\mathbf{y}$. □

This final result shows that Tadaki predictability addresses the issue we raised in Proposition 50, and such intuitively predictable but strongly incomputable sequences are indeed predictable with respect to this notion.

While classical notions of randomness such as Martin-Löf randomness are measure dependent (i.e., in general if a sequence $\mathbf{x} \in \{0,1\}^\omega$ is random with respect to a measure μ, it will not be random with respect to a different measure μ'), this is, as we saw also for bi-immunity, not the case for Tadaki unpredictability.

Before we prove this, let us recall that a Bernoulli measure μ_p with heads probability p is the function $\mu_p : \mathcal{F}_B \to [0,1]$ (where $\mathcal{F}_B$ is the Borel algebra on $\{0,1\}^\omega$) defined for $x \in \{0,1\}^*$ as $\mu_p([x]) = p^{\#_0(x)}(1-p)^{n-\#_0(x)}$, where $\#_0(x)$ is the number of 0s in x. We will also make use of the Martin-Löf-test formulation of randomness from Definition 18.

Theorem 55. *Let p be a computable real with $0 < p < 1$, and let μ_p be the Bernoulli measure with heads probability p. If $\mathbf{x} \in \{0,1\}^\omega$ is μ_p-Martin-Löf random then $\mathbf{x}$ is Tadaki unpredictable.*

Proof. Without lack of generality we assume $p > 0.5$. (The case of equality is covered by Theorem 52.)

Let us assume for the sake of contradiction that $\mathbf{x} = x_1x_2\ldots$ has a predictor F. Let $m \in \mathbb{N}$ be large enough that $m \geq \frac{-1}{\lg p}$.

Let us define the function $g : \{0,1\}^* \to \mathbb{N}$ for $y = y_1\ldots y_n \in \{0,1\}^*$ as

$$g(y_1\ldots y_n) = \left|\{i < n \mid F(y_1\ldots y_i) = y_{i+1}\}\right|,$$

which counts the number of bits in y that F correctly predicts.

Next, for each $k \in \mathbb{N}^+$ let $V_k \subset \{0,1\}^*$ be the set

$$V_k = \left\{y \in \{0,1\}^* \mid g(y) = mk,\ F(y_1\ldots y_{|y|-1}) = y_{|y|}\right\}.$$

For every string $y \in V_k$, F predicts exactly mk bits of y, including the last bit. Note that V_k is a prefix-free set: if there exist strings $y, z \in V_k$ with $|y| > |z|$ and $[y] \subset [z]$ then we must have $g(z) > g(y)$, a contradiction with the definition of V_k.

We introduce the notation $i_j^y = \min\{\ell \mid g(y_1 \dots y_\ell) = j\}$ for $y \in V_k$, so i_j^y is the index of the jth digit in y predicted by F.

Finally, we let

$$U_k = \left\{ y_1 \dots y_{i_1^y - 1} z_1 y_{i_1^y + 1} \dots y_{i_{mk}^y - 1} z_{mk} \mid y = y_1 \dots y_{u_{mk}^y} \in V_k,\ z \in \{0,1\}^{mk} \right\},$$

formed by replacing the predicted bits $y_{i_1^y} \dots y_{i_{mk}^y}$ by all strings $z \in \{0,1\}^{mk}$. Note that $V_k \subset U_k$ and that U_k is also a prefix-free set since for any two strings $u_1, u_2 \in U_k$ with $u_1 \neq u_2$ either u_1 and u_2 are both formed from the same string $y \in V_k$, in which case $|u_1| = |u_2|$ and it is clear that $[u_1] \cap [u_2] = \emptyset$, or they are formed from different strings $y_1, y_2 \in V_k$, in which case it follows from the prefix-freeness of V_k that $[u_1] \cap [u_2] = \emptyset$.

We will show that $\mu_p([V_k]) \leq 2^{-k}$ for all $k \geq 1$ and hence the V_k form the sections of a μ_p-Martin-Löf test V. We have

$$\begin{aligned}
\mu_p([V_k]) &= \sum_{y \in V_k} \mu_p([y]) \\
&= \sum_{y \in V_k} \mu_p([y_1 \dots y_{i_1^y} \dots y_{i_{mk}^y}]) \\
&= \sum_{y \in V_k} \mu_p([y_1 \dots y_{i_1^y - 1} y_{i_1^y + 1} \dots y_{i_2^y - 1} y_{i_2^y + 1} \dots y_{i_{mk}^y - 1}]) \mu_p([y_{i_1^y} \dots y_{i_{mk}^y}]) \\
&= \sum_{y \in V_k} \sum_{z \in \{0,1\}^{mk}} \mu_p([y_1 \dots y_{i_1^y - 1} z_1 y_{i_1^y + 1} \dots y_{i_{mk}^y - 1} z_{mk}]) \mu_p([y_{i_1^y} \dots y_{i_{mk}^y}]),
\end{aligned}$$

where the first step follows from the prefix-freeness of V_k and the additivity of μ_p over disjoint subsets. Note that for all $y \in \{0,1\}^*$, $\mu_p([y]) \leq p^{|y|}$ since we assumed $p > 0.5$ (for $p < 0.5$ we simply interchange heads and tails probabilities). Hence, we have

$$\begin{aligned}
\mu_p([V_k]) &\leq p^{mk} \sum_{y \in V_k} \sum_{z \in \{0,1\}^{mk}} \mu_p([y_1 \dots y_{i_1^y - 1} z_1 y_{i_1^y + 1} \dots y_{i_2^y - 1} z_2 y_{i_2^y + 1} \dots y_{i_{mk}^y - 1} z_{mk}]) \\
&= p^{mk} \mu_p([U_k]) \\
&\leq p^{mk},
\end{aligned}$$

where the final two steps follow from the prefix-freeness of U_k and the facts that $[U_k] \subset \{0,1\}^\omega$ and $\mu_p(\{0,1\}^\omega) = 1$.

Since we chose m such that $m \geq \frac{-1}{\lg p}$ we thus have

$$\begin{aligned}
\mu_p([V_k]) &\leq p^{mk} \\
&\leq p^{\frac{-k}{\lg p}} \\
&\leq p^{\log_p(2^{-k})} \\
&\leq 2^{-k}.
\end{aligned}$$

It is clear that the sets V_k are computable since F is computable, and hence they form the sections of a μ_p-Martin-Löf test $V = \{(y, k) \mid y \in V_k\}$. Finally, it is easy to see that $\mathbf{x} \in [V_k]$ for all k since there are infinitely many n such that $F(\mathbf{x} \upharpoonright n) = x_{n+1}$ by the assumption of Tadaki predictability.

But this shows precisely that $\{\mathbf{x}\}$ is μ_P-Martin-Löf null and hence that $\mathbf{x}$ is not μ_p-Martin-Löf random, a contradiction. Thus, we must conclude that $\mathbf{x}$ is not Tadaki predictable. □

This result clearly shows that the unpredictability is independent of the measure used, and does not guarantee any statistical uniformity, as was also the case for bi-immunity. This is not unreasonable, since predictability relates to whether or not we can predict a particular bit, not necessarily how *well* we can guess it. For example, even though a biased sequence resulting from a loaded coin (say, containing in the limit 1/3 heads) is an atypical sequence to be produced by a biased coin, it is still not predictable in that we still have no way of knowing *for sure* the outcome of any individual flip of the coin.

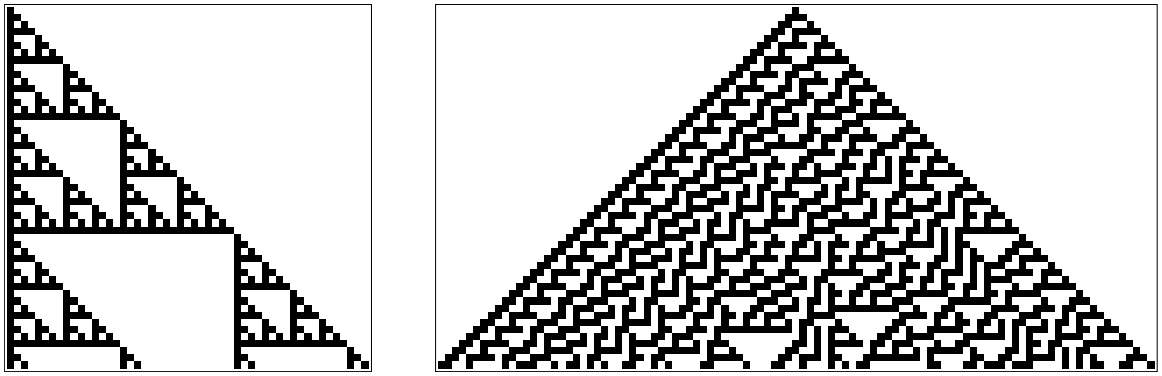
6.3 Computational irreducibility

The concept of computational irreducibility (CIR) was proposed by Wolfram and elaborated in detail in *A New Kind of Science* [151, Sec. 6]. Combining both computational and dynamical approaches, it takes a rather different approach to understanding unpredictability, proposing that it results from the inability to describe certain dynamics simply. Such an approach is interesting and sufficiently different from the physical and algorithmic approaches to unpredictability we have discussed in the preceding sections to warrant further investigation.

In this section we will briefly overview the notion of computational irreducibility, before discussing some different approaches to providing a more formal basis to the generally informal concept. We will then discuss whether CIR indeed presents a reasonable explanation for unpredictability, ultimately concluding that, although containing some interesting features, it fails to account for several important aspects of unpredictability. Nonetheless, by examining it in some detail we can gain a better understanding of what elements are essential for a generalised model of unpredictability.

6.3.1 An overview of computational irreducibility

Computational irreducibility is a property of the dynamics of a particular computational system – its *computational dynamics* – and attempts to capture the idea that a compu-



(a) (b)

Figure 6.1: Two elementary cellular automata, corresponding to rules 60 and 30, respectively, with a single black cell initial state. The first shows reducible behaviour, while the second is presumed to be computationally irreducible: there seems no easy way to determine the nth state other than computing the ECA dynamics shown.

tation may be irreducible in the sense that there is no way to 'shortcut' it: in order to determine the nth state of the system we have to simulate its dynamics, computing the intermediate states in doing so. To quote Wolfram, 'the behaviour of such systems may in general be determined in detail essentially only by explicit simulation of their time evolution' [149, p. 31]. Thus, CIR views unpredictability as arising from the fact that, in order to predict the behaviour of certain systems, we can do no better than simply letting them evolve, and hence cannot predict their behaviour in advance.

Computational irreducibility is perhaps most clearly illustrated in the domain of cellular automata in which it was originally introduced, and we will mostly restrict our discussion to this context. One-dimensional cellular automata consist of a one-dimensional array of cells, each of which can be in finitely many states, and at each time-step the cells are updated based on fixed rules that depend only on a finite set of neighbouring cells. A particularly important class of cellular automata is the two-state 'elementary' cellular automata (ECA), for which the state of each cell is updated based on its own state and the states of its two neighbours. In Figure 6.1 we show two such ECA. In Figure 6.1(a) the dynamics are relatively simple, and it is possible to compute the nth state with a very simple algorithm (by taking the parity of the numbers in the nth row of Pascal's triangle) meaning its evolution is readily predictable. In contrast, the dynamics of the ECA in Figure 6.1(b) are much more complicated, and it does not seem possible to give any such formula in this case. Furthermore, there seems to be no way to even compute the nth state without 'following the dynamics' and computing the $n-1$ preceding states, and its dynamics thus seem somewhat unpredictable.

This notion can, of course, be extended to the dynamics of other forms of com-

putation, but the interest in CIR goes beyond cellular automata and Turing machine computations. Wolfram, and more generally the digital physics community, see all real processes, be they physical, biological, etc., as computational, and CIR is seen as particularly relevant under this viewpoint. This is especially the case given one of Wolfram's other key conjectures: the principle of computational equivalence, which states that almost all computational processes are universal, and thus of equivalent computational power [151]. Thus, he claims, CIR is not merely an interesting concept, but a ubiquitous one with deep consequences. In particular, if CIR is a common feature of phenomena in the natural sciences, he claims that this could have profound effects on our ability to understand and predict scientific phenomena, since science traditionally searches for exactly the kind of simple descriptions that CIR denies [151] in order to describe and predict the behaviour of systems.

6.3.2 Formalising computational irreducibility

Despite these bold claims regarding CIR there is a lack of formal work on CIR, and in particular the concept lacks a rigorous definition, with Wolfram and others [13, 77] switching between related, but not quite consistent, informal definitions of CIR. Even if CIR is to be investigated via the experimental approach to mathematics that Wolfram advocates, a rigorous definition is undoubtedly needed. It is only with such a definition that the consequences of CIR can be more carefully understood and investigated, whether formally or experimentally.

We can group the various informal uses of CIR in the literature into the following three informal definitions of varying strength.

1. A computational system is CIR if there is no closed-form formula describing the nth state of the system as a function of its initial state.

2. A computational system is CIR if it is impossible to compute the nth state of the system more efficiently than by computing the dynamics of the system.

3. A computational system is CIR if it is impossible to compute the nth state of the system without following the same computational path as the dynamics of the system.

It is relatively clear that these notions are not equivalent, although they certainly are related to some extent.

If the concept is to be more formally studied it is necessary to decide which of these informal concepts should be formalised. Such a decision depends not only on the

intuitive concept that one wishes to capture, but equally on the need to ensure that the concept is mathematically robust.

6.3.3 CIR, closed-form solutions and unpredictability

By definition, computational systems such as ECA are completely deterministic: just as for classical (physical) dynamical systems, the dynamics are uniquely determined by the initial conditions. As we saw in our discussion of chaotic systems, however, this does not necessarily preclude unpredictability.

The notion of a closed-form solution, however, is not so well defined for discrete computational systems. Whereas the differential equations of some classical systems have no closed-form solution, the computability of computational systems means there is always a computable function giving the nth state of the system. This approach to CIR thus appears problematic to formulate well. One may require that there exist no functions computing the nth state in a time scaling as a (polynomial) function of $\log n$ – that is, the number of digits in n – as opposed to n, but immediately this restricts the notion of CIR somewhat.

Since we are interested specifically in unpredictability, it is important to look at the extent to which this formulation of CIR implies unpredictability, particularly given that this is one of the key claims of the proponents of CIR. The non-existence of closed-form solutions is often associated with dynamical chaos and unpredictability, although it is not a requirement of chaos. Indeed there exist chaotic systems that do permit closed form solutions [64]. For example, the logistic map for $\mu = 4$ given by $x_{n+1} = \mu x_n(1-x_n)$ with a seed $x_0 \in (0,1)$ is chaotic but has the closed form solution

$$x_n = \frac{1}{2}\Big(1 - \cos\left[2^n \cos^{-1}(1-2x_0)\right]\Big).$$

With this particular example, as for other chaotic systems, unpredictability is still present as a result of the sensitivity to the initial conditions, which renders the uncertainty yielded from the closed-form solution too large to give meaningful predictions. With computational systems, however, the discreteness plays a critical role [12], eliminating this sensitivity to the initial conditions. Thus, computational systems that are CIR are perfectly iterable: when they are reinitialised with the same initial conditions their dynamics are exactly the same. This is not the case in classical chaotic systems, since one can only ever initialise the initial conditions *up to a given accuracy*, and this intrinsic uncertainty in measurement renders exact iterability impossible.

One can try and simulate this uncertainty by proposing a coarse-graining scheme. Taking ECA as an example one can group cells into blocks of n, where several combinations of the states of these cells correspond to a single coarse-grained state. This is

the approach taken by Israeli and Goldenfield [77], who showed that some ECA which are intuitively CIR become reducible when coarse-grained and hence show globally predictable behaviour. While such a coarse-graining can be used to simulate a form of non-iterability by considering iterability with respect to the coarse-graining, this fails to guarantee any unpredictability. Since, unlike in the continuum, only a finite number of state configurations correspond to a single coarse-grained configuration, one can simply compute the dynamics for all such possibilities and, after a finite amount of time, distinguish them – something impossible in chaotic systems where a finite interval of phase space contains continuously many points.

Thus, although the non-existence of closed-form solutions is related to unpredictability, it appears rather to be a byproduct, rather than a necessary condition of it. In ignoring the role of the observer and measurement, such a definition of CIR fails to capture the elements that lead to physical unpredictability and instead seems to suggest a much weaker, complexity theoretic notion of unpredictability. The non-iterability of classical dynamics resulting from these limits on measurement is an essential aspect of unpredictability in classical systems, and this aspect is lost in the discrete computational dynamics to which CIR applies.

6.3.4 Following computational paths

The notion of CIR as the inability to compute the nth state of a computational system without following the path of the computational dynamics seems more closely related to computational *irreducibility* as the notion of there being no other way to find the nth state of a system than by following or running it [150], although its intuitive relation to unpredictability is perhaps less clear.

This was the notion that Zwirn and Delahaye attempted to formalise in what appears to be the only attempt to carefully define CIR [165, 166]. They considered the ability to compute with a Turing machine the nth state of an ECA (given a fixed encoding $\langle\cdot\rangle$ for ECA states) without computing any approximations of intermediate states in the process. Unfortunately, the formalism given in [165, 166] contains many technical issues, such as confounding the configurations and tape contents of Turing machines, as well as a notion of approximation that is not sufficiently general. However, these issues all appear fixable, and one can define such a notion of an 'approximate computation' of an ECA A by a Turing machine T by requiring there to be points in time $t_1, \ldots, t_n$ such that, at time t_i the configuration of T can be *efficiently reduced* to the encoding $\langle a_i \rangle$ of the ith state in the computation of A.

Since such systems are computable, the efficiency of the reduction mapping the simulation to the dynamics is essential, because the computations are trivially *compu-*

tationally reducible to each other. As a result, however, one loses the objectivity of the notion of CIR, and instead it becomes relative to the strength or form of reduction.

A more important issue is the robustness of such a definition, since it is not clear that there exist any two algorithms computing $\langle a_n \rangle$ with the same time complexity that are not reducible to each other. The existence of such an example is essential for such a formulation of CIR, as otherwise the notion reduces to a purely complexity theoretic one. It is perhaps questionable whether this is in fact possible, since it has been argued that there is no robust way to form equivalence classes of machines computing the 'same algorithm as opposed to just computing the same function' [19], a problem that has obvious links to the one at hand.

While formalising the notion of 'following similar computational paths' may be interesting in its own right, with applications to the computation of digits of constants such as π [11], it is not clear that this is essential for the notion of CIR. In particular, it is not clear why an algorithm computing the nth state of a system that does not approximate the system's dynamics, but which is nonetheless no more efficient, should count as a reduction. Furthermore, this concept seems even less relevant for unpredictability, since there seems to be little reason to privilege, as a method of prediction, computations following a different computational path to the natural dynamics. In cases where an alternative computation seems to provide a more direct prediction, this seems rather to be due to its efficiency than the specific computational path.

6.3.5 Complexity theoretic approach to CIR

The final approach to defining CIR is to take a more complexity theoretic approach, defining a CIR system as one whose dynamics cannot be computed asymptotically faster. For an ECA A, for example, this would mean that there is no algorithm T which, on input n, computes $\langle a_n \rangle$ with more than a logarithmic[10] improvement in time over A. Indeed, this seems in many ways closest to the conception Wolfram had in mind in proposing CIR [149, 150], and its simplicity makes it attractive as a notion of CIR. Furthermore, it does not seem to have the conceptual limitations of the other two potential definitions in relation to irreducibility: a CIR system under this definition is irreducible in the clear sense that its dynamics are *computationally optimal*.

The connection between this formulation of CIR and unpredictability is nonetheless still limited, since the inability to compute asymptotically faster does not rule out the computation being used to 'say in advance' (*prædicere*); indeed, computation has no inherent time scale, per se. The computability and perfect iterability of discrete com-

[10]The logarithmic factor is necessary to avoid speed-up theorems [53] and issues related to machine representations.

putational systems means, as we discussed above, that they are in some sense perfectly predictable.

This notion of CIR, however, when viewed in conjunction with Wolfram's principle of computation equivalence [151] on the ubiquitousness of universality, does have some connection to a different form of unpredictability. The existence of efficient universal Turing machines [87, 122] gives an immediate example of CIR systems under this complexity theoretic formulation of CIR, since such systems cannot be more efficiently simulated, themselves already being efficient simulators. The efficiency of the universality is essential, since systems that behave universally, but not optimally so, can be reduced to other more efficient universal machines. This is an important caveat, since, for example, although the rule 110 ECA is known to be universal, it is very inefficiently so – it simulates a computation of T time steps in time $O(T^4 \log^2 T)$ [154] – and claims of its CIR thus appear dubious [61, 77].

The fact that such universal systems are limited by the halting problem [122] means that there are certain properties about the long term behaviour of such systems which cannot be computationally resolved, thus representing an explicit form of (computational) unpredictability. For such questions there is no way to compute in advance the behaviour of the system, one must simply run them and wait. However, to fully justify the claims that CIR is so important in the natural sciences [151] and can help explain the unpredictability of physical systems, one must justify that such systems are not just capable of universality, but actually implement optimally universal behaviour, a bold claim needing more careful mathematical treatment.

6.3.6 Conclusions on CIR and unpredictability

We have discussed in some detail three possible approaches to formalising the concept of CIR, as well as how these notions serving as possible definitions relate to the concept of unpredictability. While CIR appears to be most robustly formalisable as a complexity theoretic notion, its relation to unpredictability appears rather weak. The perfect iterability and computability of computational systems such as cellular automata mean that the unpredictability found in classical systems arising, via measurement, at the interface between the system and observer is nonexistent. Rather, CIR represents a property of *optimality* of certain computational systems.

Nonetheless, CIR does highlight the need to include a computational element in a model of unpredictability: predictability necessitates the ability to compute in advance the behaviour of certain systems. The challenge, and what we will undertake in the following section, is to combine this notion of predicting via computational means and the essential role of measurement to provide a more suitable, general model of unpre-

dictability.

6.4 Generalised models of unpredictability

While the algorithmic notions of unpredictability discussed in Sec. 6.2 allow for a somewhat more objective notion of unpredictability than that usually discussed in the context of physical theories, they are too abstract to be applied directly in more practical contexts. Moreover, they are 'product' rather than 'process' notions of unpredictability, which limits their applicability in many physical scenarios.

In the rest of this chapter we take a different approach, and consider more general frameworks in which unpredictability can be analysed. We first study and critique various models of unpredictability that have been presented and used in the literature. We then proceed to develop a new model of unpredictability which is sufficiently general to be applied to relatively arbitrary physical processes, makes use of relevant physical information in order to asses the predictability of such processes, but retains certain aspects of effectivity from computability theory which allow it to be sufficiently general and powerful [5, 6].

6.4.1 Review of models of unpredictability

To predict – in Latin *prædicere*, 'to say beforehand' – means to forecast what will occur under specific conditions before the phenomenon happens. We will discuss some various definitions of predictability proposed by different authors, in particular with regards to their suitability for capturing the notion of predictability of individual physical events or sequences thereof in the most general sense.

As is the case with the notion of randomness, which is often considered to be synonymous with probabilities in physics, probabilities are often taken to imply unpredictability within physical systems. However, for very much the same reason that they are not suitable as a notion of randomness, they fall short of providing a solid generalised or objective notion of unpredictability. In particular, there is no guarantee that an epistemic probability is not hiding perfectly predictable, deterministic behaviour.

In cryptographic applications probability is perhaps a slightly more suitable notion of unpredictability precisely because it is epistemic, rather than objective, unpredictability that is normally required [48]. That is, one generally wants a secret key that is unpredictable for any adversary: if the adversary behaves rationally, they can do no better than assigning an (ideally almost uniform) probability distribution for the secret key. One would expect, of course, this to be also true if the key were unpredictable with respect to a more objective form of indeterminism.

In order to pursue a more suitable notion of unpredictability which avoids any issues related to the use of particular representations within theories, it seems a more robust path is to formulate prediction in terms of a 'predicting agent' of some form. This is indeed the approach taken by some definitions, and that we also will follow.

In Section 6.1 we discussed the notion of unpredictability within dynamical systems. In these systems, unpredictability has long been linked to chaos and the inability to calculate with sufficient precision the future state of a system given a particular observable initial condition [146]. Note that, while chaos is formally linked to measure theory, this notion of unpredictability relies on more than simple probabilistic formalism – indeed, it is formalised within deterministic dynamical systems. Although not a general model of unpredictability, this notion emphasises a critical aspect: the role of observation, since although a system may presumably have a well-defined initial state (a point in phase space), any observation yields an interval of positive measure (a region of phase space). This certainly seems the correct path to follow in formalising predictability, but more generality and formalism is needed to provide a definition for arbitrary physical processes.

Popper defines prediction in terms of 'physical predicting machines', although he takes the fairly unconventional viewpoint that unpredictability *is* indeterminism [108]. He considers these as real machines that can take measurements of the world around them, compute via physical means, and output (via some display or tape, for example) predictions of the future state of the system. He then studies experiments which must be predicted with a certain accuracy and considers these to be predictable if it is *physically* possible to construct a predictor for them. Via a form of diagonalisation argument, Popper shows that this is not possible for all such experiments. This definition of prediction is unfortunately rather abstract, and it is not particularly clear how to work with this in all but trivial specific cases, since the notion of a physical predicting machine is difficult to consider practically. It is sufficient for the type of abstract argument Popper wishes to use, but not overly suitable to serve as a base for a generalised framework for unpredictability.

Wolpert formalised this notion much further in developing a general abstract model of physical inference [153]. Like Popper, Wolpert was interested in investigating the limits of inference, including prediction, arising from the simple fact that any inference device must itself be a physical device, hence an object whose behaviour we can try to predict. While Wolpert's aim was not so focused on the predictability arising from the nature of specific physical theories, he identified and formalised the need for an experimenter to develop prediction techniques and initialise them by interacting with the environment via measurements. However, Wolpert, like Popper, was interested mainly in the limits inherent in the notion of such inference devices, and arrives at such limits

by considering inference devices forced to make self-referential predictions.

Popper's and Wolpert's notions of predictability perhaps lack generality by requiring the predictor to be embedded, that is, physically present, in its environment [136], and their abstract natures means that they are not so suited to investigating the predictability of particular physical processes, but rather of the physical world as a whole.

A more modern and technical definition of unpredictability was given by Eagle [49] in defining randomness as maximal unpredictability. While we have already discussed the relation between randomness and unpredictability at some length, Eagle's definition of unpredictability deserves further attention. He defined prediction relative to a particular theory and for a particular predicting agent, an approach thus with some similarity to that of Wolpert. Specifically, a prediction function is defined as a function mapping the state of the system described by the theory and specified epistemically (and thus finitely) by the agent to a probability distribution of states at some time. This definition formalises more clearly prediction as the output of a function operating on information extracted about the physical system by an agent. This framework, however, renders predictability relative to a particular physical theory, rather than producing a more objective notion as we want.

In particular, in order to relate the intrinsic indeterminism of a system to unpredictability, it would be more appropriate to have a definition of events as unpredictable *in principle*. Thus, the predictor's ignorance of a better theory might change their associated epistemic ability to know if an event is predictable or not, but would not change the fact that an event may or may not be, in principle, predictable.

Last but not least, it is important to restrict the class of prediction functions by imposing some effectivity (i.e., computability) constraints. Indeed, we suggest that 'to predict' is to say in advance in some effective/constructive/computable way what physical event or outcome will happen. Thus, motivated by the Church-Turing thesis, we choose here Turing computability as this seems to provide the most uniform and general model of effectivity which corresponds to the power available to any predicting agent. Any predicting agent operating with incomputable means – incomputable or infinite inputs, or procedures, that can go beyond the power of algorithms (for example, by executing infinitely many operations in a finite amount of time) – seems to be physically highly speculative if not impossible [44]. Technically, 'controlled incomputability' could be easily incorporated in the model, if necessary. One must be careful, however, not to remove all such constraints of effectivity from the model, otherwise one runs the risk of viewing any deterministic process as predictable, since one can associate a (generally incomputable) function to any deterministic infinite sequence.

Taking these points into account, we propose in the next section a definition, similar in some aspects to Wolpert's and Eagle's definitions, based on the ability of some com-

putably operating agent to correctly predict using finite information extracted from the system of the specified experiment. Unlike Eagle [49], we consider only prediction with certainty, rather than with probability. While it is not difficult nor perhaps unreasonable to extend our definition to the more general scenario, we wish to focus on a more absolute notion of unpredictability; this is sufficient, and perhaps even advantageous, for our main application of interest: quantum unpredictability. Moreover, in doing so we avoid any potential pitfalls related to probability one or zero events [159].

Our main aim is to define the (correct) prediction of individual events [49], which can be easily extended to an infinite sequence of events. An individual event can be correctly predicted simply by chance, and a robust definition of predictability clearly has to avoid this possibility. Popper succinctly summarises this predicament in [108, pp. 117–118]:

> If we assert of an observable event that it is unpredictable we do not mean, of course, that it is logically or physically impossible for anybody to give a correct description of the event in question before it has occurred; for it is clearly not impossible that somebody may hit upon such a description accidentally. What is asserted is that certain rational methods of prediction break down in certain cases—the methods of prediction which are practised in physical science.

One possible approach is then to demand a proof that the prediction is correct, thus formalising the 'rational methods of prediction' that Popper refers to. However, this is notoriously difficult and must be made relative to the physical theory considered, which generally is not well axiomatised and may change over time as our understanding evolves. Instead we demand that such predictions be *repeatable*, and not merely one-off events. This point of view is consistent with Popper's own framework of empirical falsification [109]: an empirical theory (in our case, the prediction) can never be proven correct, but it can be falsified through decisive experiments pointing to incorrect predictions. Specifically, we require that the *predictions remain correct in any arbitrarily long (but finite) sequence of repetitions of the experiment.*

6.5 Proposed formal model of (un)predictability

Let us lay out the formalism for this model, which formulates a notion of predictability for individual events by considering the ability for a predicting agent, acting via uniform, effective means, to predict correctly and reproducibly the outcome of an experiment using some finite information the agent extracts from the 'system' and its 'environment'

as input. We further consider the possibility that the extracting power of the agent may be limited, thus allowing us to consider also a relativised notion of unpredictability.

More precisely, the model consists of several elements:

1. The specification of an experiment E for which the outcome must be predicted.

2. A predicting agent or 'predictor', which must predict the outcome of the experiment. We model this as an effectively computable function, a choice which we will justify further.

3. An extractor ξ, which is a physical device the agent uses to (uniformly) extract information pertinent to prediction that may be outside the scope of the experimental specification E. This could be, for example, the time, the measurement of some parameter, the iteration of the experiment, etc.

4. A prediction made by the agent with access to a set Ξ of extractors.

6.5.1 The formal model

We will next elaborate on, and formalise the individual aspects of the model.

Experimental specification. An experimental specification is a finite specification of an experiment for which the outcome is to be predicted. We restrict ourselves to the case where the result of the experiment, that is, the value to be predicted, is a single bit: 0 or 1. However, this can readily be generalised to the case of finite or countably many output values; that is, when the outcome can be finitely specified. On the other hand, it does not make sense to predict an outcome requiring an infinite description, such as a real number, since this can never be measured exactly. In such a case the outcome would be an approximation of the real – a rational number, and thus finitely specifiable.

The experimental specification, being finite, can not normally specify exactly the required setup of the experiment, as a precise description of experimental conditions generally involves real-valued parameters. Rather, it is expressed with finite precision and with respect to the symmetries pertinent to the experimenter and their limited capacities. A particular trial of E is associated with the parameter λ which fully describes the 'state of the universe' in which the trial is run. As an example, one could consider E to specify the flipping of a certain coin, or it could go further and specify, up to a certain accuracy, the initial dynamical conditions of the coin flip. In both cases, λ contains further details – such as the exact initial conditions of a particular flip – which could be used by an agent in trying to predict the result of E.

The parameter λ will generally[11] be 'an infinite quantity' – for example, an infinite sequence or a real number – structured in an unknown manner (i.e., we do not force any specific encoding on λ). Forcing a specific encoding upon λ, such as a real number, may impose an inadequate structure (e.g., metric, topological) which is not needed for what follows. While λ is generally not in its entirety an obtainable quantity, it contains any information that may be pertinent to prediction – such as the time at which the experiment takes place, the precise initial state, any hidden parameters, etc. – and any predictor can have practical access to a finite amount of this information. We can view λ as a resource from which one can extract finite information in order to try and predict the outcome of the experiment E.

Predicting agent. The predicting agent (or 'predictor') is, as one might expect, the agent trying to predict the outcome of a particular experiment, using potentially some data obtained from the system (i.e., from λ) to help in the process. Since such an agent should be able to produce a prediction in a finite amount of time via some uniform procedure, we need the prediction to be *effective* in the computational sense of the term.

Formally, we describe a predicting agent as a computable function P_E (i.e., an algorithm) which halts on every input and outputs either 0,1, or 'prediction withheld'. Thus, the agent may refrain from making a prediction in some cases if it is not certain of the outcome. This allows us to consider more carefully the ability of a predicting agent in the infinite limit when it may only be able to correctly predict with certainty almost all trials of an experiment. P_E will generally be dependent on E, but its definition as an abstract algorithm means *it must be able to operate without interacting with the subsystem whose behaviour it predicts*. This is necessary to avoid the possibility that the predictor affects the very outcome it is trying to predict.

We note finally that, as mentioned in Sec. 6.2.2 in the context of Tadaki predictability, the choice of computability as the level of effectivity required can be strengthened or weakened, as long as some effectivity is kept. Our alternative choice here is motived by the Church-Turing thesis, a rather robust assumption [42] (see also the discussions in Sec. 6.2.2 and Sec. 6.4).

Extractor. An extractor is a physically realisable device which a predicting agent can use to extract (a finite amount of) useful data that may not be a part of the description of E from λ to use for prediction – that is, as input to P_E. In many cases this can be viewed as a measurement instrument, whether it be a ruler, a clock, or a

[11] If one insists on a discrete or computational universe – whether it be as a 'toy' universe, in reality or in virtual reality – then λ could be conceived as a finite quantity. This is, however, the exception, and in the standard view of real physical experiments λ would be infinite, even if the prediction itself is discrete or finite. We will not consider this possibility further here.

more complicated device.

Formally, an extractor is a function $\lambda \mapsto \xi(\lambda) \in \{0,1\}^*$, where $\xi(\lambda)$ is a finite string of bits, which can be physically realised without altering the system, that is, passively. We require that $\xi(\lambda)$ be a finite string since, in order to be used by P_E for prediction, $\xi(\lambda)$ should be finite and effectively codable.

Prediction. We define now the notion of a correct prediction for a predicting agent having access to a fixed (finite or infinite) set Ξ of extractors.

Definition 56. Given a particular extractor ξ, we say the prediction of a run of E with parameter λ is *correct for* ξ if the output $P_E(\xi(\lambda))$ is the same as the outcome of the experiment.

That is, the predictor P_E correctly predicts E when using information extracted from λ by ξ as input.

However, this is not enough to give us a robust definition of predictability, since for any given run it could be that we predict correctly by chance. To overcome this possibility, we need to consider the behaviour of repeated runs of predictions.

Definition 57. A *repetition procedure for* E is an algorithmic procedure for resetting and repeating the experiment E.

Generally this will be of the form 'E is prepared, performed, and reset in a specific fashion'. The specific procedure is of little importance, but the requirement is needed to ensure that the way the experiment is repeated cannot give a predicting agent power that should be beyond their capabilities or introduce mathematical loopholes by 'encoding' the answer in the repetitions or particular initial conditions, for example; both the prediction and repetition should be performed algorithmically.

Definition 58. We say the predictor P_E is *k-correct for* ξ if for any repetition procedure for E (giving parameters $\lambda_1, \lambda_2, \ldots$ when E is repeated) there exists an $n \geq k$ such that after n repetitions of E producing the outputs $x_1, \ldots, x_n$, the sequence of predictions $P_E(\xi(\lambda_1)), \ldots, P_E(\xi(\lambda_n))$:

1. contains k correct predictions,

2. contains no incorrect prediction; that is, the remaining $n-k$ predictions are withheld.

If P_E is k-correct for ξ we can bound the probability that P_E is in fact operating by chance and may not continue to give correct predictions, and thus give a measure of our confidence in the predictions of P_E. Specifically, the sequence of n predictions made by P_E can be represented as a string of length n over the alphabet $\{T, F, W\}$,

where T represents a correct prediction, F an incorrect prediction, and W a withheld prediction. Then, for a predictor that is k-correct for ξ there exists an $n \geq k$ such that the sequence of predictions contains k T's and $(n-k)$ W's. There are $\binom{n}{k}$ such possible prediction sequences out of 3^n possible strings of length n. Thus, the probability that such a correct sequence would be produced by chance tends to zero as expected when k goes to infinity because

$$\frac{\binom{n}{k}}{3^n} < \frac{2^n}{3^n} \leq \left(\frac{2}{3}\right)^k.$$

Clearly the confidence we have in a k-correct predictor increases as k tends to infinity. We thus formalise the notion of predictability with respect to this limit scenario to avoid the possibility that, as Popper described, one may produce correct predictions accidentally.

Definition 59. We say the predictor P_E is *correct for* ξ if it is k-correct for ξ for all $k \geq 1$.

It is important to note that the infinity used in going to this limit case is only *potential*, not actual: its role is to guarantee arbitrarily many correct predictions. If P_E is correct for ξ, then P_E never makes an incorrect prediction and the number of correct predictions can be made arbitrarily large by repeating E enough times.

From this notion of correctness we can define predictability both relative to a set of extractors, and in a stronger, non-means-relative form.

Definition 60. Let Ξ be a set of extractors. An experiment E is *predictable for* Ξ if there exists a predictor P_E and an extractor $\xi \in \Xi$ such that P_E is correct for ξ. Otherwise, it is *unpredictable for* Ξ.

This means that P_E has access to an extractor $\xi \in \Xi$ which, when using this extractor to provide input to P_E, can be made to give arbitrarily many correct predictions by repeating E enough (but finitely many) times, without ever giving an incorrect prediction.

We can extend this to a more objective notion of predictability by considering the set of all possible extractors [6].

Definition 61. An experiment is *(simply) predictable* if there exists a predictor P_E and an extractor ξ such that P_E is correct for ξ. Otherwise, it is *(simply) unpredictable*.

We will only insist on referring to events as simply (un)predictable when we wish to avoid ambiguity with informal notions of (un)predictability or in direct contrast to predictability relative to a set of extractors. If there is no ambiguity, we will just refer to such events as (un)predictable.

Finally, we can use this notion of a predictable experiment to define a notion of predictability of individual events.

Definition 62. The outcome x of an *single trial* of the experiment E is *predictable (for* Ξ*)* if E is predictable (for Ξ). Otherwise, it is unpredictable (for Ξ).

We emphasise here that the predictability of the result of a single trial is predictability *with certainty*, as opposed to simply with probability one.

6.5.2 Some remarks on relativisation

The notion of simple predictability defined above is clearly the stronger notion, and it is this that we will pursue initially in relation to quantum unpredictability. However, we wish to briefly discuss some issues in relating to the relativised unpredictability we have defined, in order to clarify this notion further.

Beyond indeterminism, which offers the most obvious physical case for unpredictability and which we will discuss explicitly in the context of quantum mechanics, it does not seem simple to find physical properties which can guarantee unpredictability. This is a result of the stringent requirements the definition imposes: we must prove that no predictor-extractor pair exists satisfying the requirements of prediction. The inability to do so does not mean such phenomena are necessarily unpredictable, but only that we cannot prove either way.

In some physical situations, particularly in classical physics, our inability to predict would seem to be linked to our epistemic lack of information – often due to measurement. Put differently, it is a result of only having access to a set Ξ of extractors of limited power. Our relativised model of prediction attempts to capture this, defining predictability relative to a given set of extractors Ξ. Thus, relativised unpredictability is generally epistemic in nature, since it is due to the inability for a predicting agent to have access to an extractor extracting the information required for prediction. Simple unpredictability, on the other hand, is an objective notion, as it does not depend on the limited powers of any such agent.

6.5.2.1 Choosing the set of extractors Ξ

In defining this notion, we deliberately avoided saying anything about how Ξ should be specified. Here we outline two possible ways this can be done.

The simplest but most restrictive way would be to explicitly specify the set of extractors. As an example, let us consider the experiment of firing a cannonball from a cannon and the task of predicting where it will land (assume for now that the muzzle velocity is known and independent of firing angle). Clearly the position will depend on

the angle the cannonball is fired at. Then if we are limited to measuring this with a ruler, we can consider, for example, the set of extractors

$$\Xi = \{\xi \mid \xi(\lambda) = (x, y) \text{ where } x \text{ and } y \text{ are the muzzle position to an accuracy of 1cm}\}$$

and then consider predictability with respect to this set Ξ (e.g., by using trigonometry to calculate the angle of firing, and then where the cannonball will land).

Often it is unrealistic to characterise completely the set of extractors available to an agent in this way – think about a standard laboratory full of measuring devices that can be used in various ways. Furthermore, such devices might be able to measure properties indirectly, so we might not be able to characterise the set Ξ so naively. Nonetheless, this can allow simple consideration and analysis of predictability in various situations, such as under-sensitivity to initial conditions.

A more general approach, although requiring further assumptions, is to limit the 'information content' of extractors. This avoids the difficulty of having to explicitly specify Ξ. Continuing with the same example as before, we could require that no extractor $\xi \in \Xi$ can allow us to know the firing angle better than 1°. This circumvents any problems raised by the possibility of indirect measurement, but of course requires us to have faith in the assumption that this is indeed the case; it could be possible that we *can* extract the angle better than this, but we simply do not know how to do it with our equipment. (This would not be a first in science!) Nonetheless, this approach captures well the epistemic position of the predicting agent.

Let us formalise this more rigorously. We hypothesise that we cannot do any better than a hypothetical extractor ξ' extracting the desired physical quantity. Then we characterise Ξ by asserting: for all $\xi \in \Xi$ there is no computable function f such that for every parameter λ, $f(\xi(\lambda))$ is more accurate than ξ'. Obviously, the evaluation of 'more accurate' requires a (computable) metric on the physical quantity extracted, something not unreasonable physically, given that observables tend to be measured as rational approximations of reals [85].

This general approach would need to be applied and carefully justified on a case by case basis, given assumptions about the capabilities available to the predicting agent.

One can view this in the context of the epistemic unpredictability within dynamical systems discussed in Sec. 6.1. Such a restriction on the set of extractors corresponds naturally to positing an explicit limit on our accuracy of observation. This goes beyond the statement that a particular measuring instrument cannot measure beyond this accuracy, but states that we do not have access to any instrument that can be used to deduce accuracy beyond this limit. This may be due to purely practical constraints, or deeper limits, for example limiting measurements of positions based on thermal fluctuations, etc. [12].

Either of these approaches, and perhaps others, can be used with our relativised model of prediction. In any such case of relativisation, one would need to argue that the set Ξ for which unpredictability is proven is relevant physically. This is unavoidable for any epistemic model of prediction.

Let us illustrate the use of relativised unpredictability with a more interesting example of a hypothetical experiment which is predictable, but its intuitive unpredictability is well captured by the notion of relativised unpredictability. In particular, let us consider a simple chaotic dynamical system. As we discussed in Section 6.1.3, chaos is often associated with unpredictability within a system. However, chaos is, formally, an asymptotic property [98], and we will see that, as a result, the unpredictability of chaotic systems is not so simple as might be initially suspected.

Example 63. For simplicity, we will take the example of the dyadic map, that is, the operation $d : \{0,1\}^\omega \to \{0,1\}^\omega$ defined by $d(x_1x_2x_3\dots) = x_2x_3\dots$, as in [6]. We work with this archetypal example since it is mathematically clear and simple, and is known to be chaotic and equivalent (more precisely, topologically conjugate) to many others, such as the logistic map $a_{n+1} = \mu a_n(1-a_n)$ (where $a_n \in (0,1)$ for $n \geq 0$) with $\mu = 4$ [45]. However, the analysis could equally apply to more familiar (continuous) chaotic physical dynamics, such as that of a double pendulum.

Let us consider the hypothetical experiment E_k (for fixed $k \geq 1$) which involves iterating the dyadic map k times (i.e., d^k) on an arbitrary 'seed' $\mathbf{x} = x_1x_2\dots$. The outcome of the experiment is then taken to be the first bit of the resulting sequence $d^k(\mathbf{x}) = x_{k+1}x_{k+2}\dots$, that is, x_{k+1}. This corresponds to letting the system evolve for some fixed time k before measuring the result.

While the shift d (and hence d^k) is chaotic [45] and generally considered to be unpredictable, it is clearly (simply) predictable if we have an extractor that can 'see' (or measure) more than k bits of the seed. That is, take the extractor $\xi_k(\lambda_\mathbf{x}) = x_{k+1}$ which clearly extracts only finite information, and the identity Turing machine T_I as P_{E_k} so that, for any trial of E_k with parameter $\lambda_\mathbf{x}$ we have $P_{E_k}(\xi_k(\lambda_\mathbf{x})) = T_I(x_{k+1}) = x_{k+1}$, which is precisely the result of the experiment.

On the other hand, if we consider that there is some limit ℓ on the 'precision' of measurement of $\mathbf{x}$ that we can perform, the experiment is unpredictable relative to this limited set of extractors Ξ_ℓ defined such that for every sequence $\mathbf{x}$, every computable function f there exists λ such that for all $j > \ell$, $f(\xi(\lambda)) \neq x_j$. It is clear that for $\ell = k$, given the assumption that this is the limit of our precision, the experiment E_k is unpredictable for Ξ_k. Indeed, if this were not the case, the pair (ξ, P_{E_k}) allowing prediction would make arbitrarily many correct predictions, thus contradicting the assumption of limited precision of measurements.

This example may appear somewhat artificial, but this is not necessarily so. If one considers the more physical example of a double pendulum, as mentioned earlier, one can let it evolve for a fixed time t and attempt to predict its final position (e.g., above or below the horizontal plane) given a set limit ℓ on the precision of any measurement of the initial position in phase space. If the time t is very short, we may well succeed, but for long t this becomes unpredictable.

This re-emphasises that chaos is an asymptotic property, occurring only strictly at infinite time. While, in the limit, it indeed seems to correspond well to unpredictability, in finite time the unpredictability of chaotic systems is relative: a result of our limits on measurement. Of course, in physical situations such limits may be rather fundamental: thermal fluctuations and quantum uncertainty seem to pose very real limits on measurement precision [85], although in most situations the limits actually obtained are of a far more practical origin.

6.6 Relation to algorithmic notions of unpredictability

We can study the relation between our model of unpredictability, which is applicable to arbitrary physical systems, and the algorithmic notions of unpredictability that we discussed in Sec. 6.2, by considering a toy model in the following way, giving them a physical interpretation. Consider a black box $B(\mathbf{x})$ with a button that, when pressed, gives the next digit of $\mathbf{x}$ (starting from some arbitrary position k); by repeating this operation one can slowly learn, in order, the bits of $\mathbf{x}$ (modulo a finite prefix of length $k-1$). A sequence is Tadaki predictable if there is a uniform way to compute infinitely often x_{n+1} having learnt the initial segment $x_1 \dots x_n$, with the proviso that we must know *in advance* when – that is, the times at which – we will be able to do so.

When viewed from the physical point of view described above, there is a clear relation to our notion of predictability. In particular, we can consider a deterministic experiment $E_{\mathbf{x}}$ that consists of generating a bit from the black box $B(\mathbf{x})$, and asking if $E_{\mathbf{x}}$ is predictable for the 'prefix' extractor $\xi_p(\lambda_i) = x_1 \dots x_{i-1}$ for the trial of $E_{\mathbf{x}}$ producing x_i – that is, using just the results of the previous repetitions of $E_{\mathbf{x}}$. (We assume, for simplicity and without loss of generality, that $k = 1$.) Although $B(\mathbf{x})$ is not (generally) finitely specifiably (since $\mathbf{x}$ is infinite), we assume that one has *physical* access to such a black box and can thus finitely prepare the experiment $E_{\mathbf{x}}$. It is not too difficult to see that there is an equivalence between predictability and Tadaki total predictability in this scenario.

Fact 64. *$E_{\mathbf{x}}$ is predictable (for ξ_p) if and only if $\mathbf{x}$ is Tadaki totally predictable.*

Proof. It suffices to simply equate the function F from the Definition of Tadaki predictability and the predictor P_E, as well as the outputs 'W' and 'withheld'. □

While the physicality of such a black box is clearly debatable, this hypothetical scenario allows us to see the relation between the purely mathematical algorithmic notion of Tadaki unpredictability and our generalised model. In general, algorithmic information theoretical properties of sequences could be explored using this model via such an approach. However, the relation between these notions exists only when one considers particular, abstract, extractors such as ξ_p. The generality of our model originates in the importance it affords to physical properties of systems, *via* extractors, which are essential for prediction in real systems. Depending on the physical scenario investigated, physical devices might permit us to extract information allowing to predict an experiment, regardless of the algorithmic content of this information, as long as finite information suffices for a single prediction.

Chapter 7

Unpredictability of quantum measurements

In this chapter, we aim to put into practice the framework of unpredictability formalised in the previous chapter. In particular, we apply it to the analysis of quantum measurements, which are often claimed, at least informally, to be unpredictable [8, 139].

By working with a clear, formalised notion of unpredictability, we are able to look much more closely at which principles give rise to this unpredictability, as well as the physical assumptions under which this is valid.

We first look at the relation between quantum value indefiniteness, of the kind which can be identified by Theorem 34 in Chapter 3 and show that this formalised notion of indeterminism indeed guarantees unpredictability. We then turn our attention to quantum complementarity, and show that this provides a weaker, relativised notion of unpredictability, and requires stronger physical assumptions to be used to certify any more objective unpredictability. Finally, we discuss the relationship between these forms of quantum unpredictability and incomputability, and in particular the results of Chapter 5 on the incomputability of quantum randomness.

7.1 Quantum unpredictability from value indefiniteness

The justification for the claims that quantum measurement results are unpredictable seems to be based on the understanding that quantum mechanics is a fundamentally indeterministic theory. Intuitively, quantum indeterminism is seen as the absence of physical reality before the act of measurement; if no unique element of physical real-

ity [51] corresponding to a particular physical quantity exists, this is reflected by the said quantity being indeterminate. That is, for such an observable none of the of the possible exclusive measurement outcomes are certain to occur prior to measurement, and therefore, it is argued, we should conclude that any kind of prediction with certainty is impossible [81]. For example, an agent trying to predict the outcome of a measurement of a projection observable in a basis unbiased with respect to the preparation basis (i.e., if there is a 'maximal mismatch' between preparation and measurement) could do no better than blindly guess the outcome of the measurement.

This argument is too informal to be taken as a direct argument for unpredictability, since the notions of unpredictability and indeterminism need to be carefully formalised and considered to give the statement any formal meaning. However, with the formalisms we have presented at hand, it serves as a good starting point.

In order to properly analyse how this may lead to unpredictability, we need to work from this formal notion of value indefiniteness and make use of the more rigorous definition of unpredictability that we have formulated. This notion will allow us to clarify the possible origins of unpredictability in quantum mechanics more clearly.

7.1.1 Unpredictability of individual quantum measurements

Throughout this section we will consider a general quantum experiment E_Q, which is closely related to the hypothetical infinite experiment analysed in the context of incomputability in Chapter 5.

More specifically, let E_Q be an experiment in which a quantum system is prepared in an arbitrary (but fixed) state $|\psi\rangle$ in dimension $n \geq 3$ Hilbert space and a value indefinite projection observable P_ϕ (i.e., with $0 < |\langle\psi|\phi\rangle| < 1$) is measured producing a single bit x. We similarly assume (as in Section 4.4.4) the measurement, noncontextuality and eigenstate assumptions, which hence guarantees that P_ϕ is value indefinite, since we indeed have a mismatch between the preparation and measurement contexts. We note that we could simply assume that P_ϕ is value indefinite under any faithful value assignment function, but, since we wish to explore more carefully the physical origin of unpredictability, it seems more reasonable, and certainly more consistent with our prior results, to work from the same set of basic physical assumptions.

The nature of the physical system in which this state is prepared and the experiment performed is not important, whether it be photons passing through generalised beamsplitters [114], or ions in an atomic trap. However, we require that the system must be at least three-dimensional, since the results used to derive value indefiniteness, such as Theorem 34, require this as an assumption. Of course, if we were to blindly take value-indefiniteness as an assumption for all systems this would not be necessary.

We first show that experiments utilising quantum value indefinite observables cannot have a predictor which is correct for some ξ, and hence E_Q is unpredictable.

Theorem 65. *The experiment E_Q producing a bit from the measurement of a value indefinite observable is unpredictable.*

Proof. Let us assume for the sake of contradiction that there exists an extractor ξ and a predictor P_{E_Q} for E_Q which is correct for ξ. This means that there is a repetition scenario in which E_Q is repeated, algorithmically, *ad infinitum*, and for which P_{E_Q} never makes an incorrect prediction for any infinite sequence $\mathbf{x} = x_1 x_2 \ldots$ of bits produced via this repetition procedure.

Since P_E *never* makes an incorrect prediction, each of its predictions is correct with certainty. Then, according to the EPR principle we must conclude that each such correct prediction corresponds to a value definite property of the system measured in E_Q. However, we chose E_Q such that this *is not* the case: each x_i is the result of the measurement of an observable P_ϕ which is value indefinite under any faithful value assignment function. Thus we obtain a contradiction: P_ϕ must be both value definite and indefinite under any faithful value assignment function, and hence we must conclude that no such predictor P_{E_Q} can exist. □

Moreover, since there does not exist a predictor P_{E_Q} which is correct for some ξ, for such a quantum experiment E_Q, no single outcome is predictable with certainty.

Corollary 66. *In an infinite repetition of E_Q generating the infinite sequence $\mathbf{x} = x_1 x_2 \ldots$ as described above, no single bit x_i, $i \geq 1$, can be predicted with certainty.*

These results are not unexpected, since they largely confirm the intuition that quantum measurement are indeed unpredictable (unless one measures a known property, corresponding to the system being in an eigenstate of the measurement observable) and that this arises from quantum indeterminism. However, there is nonetheless merit in formalising and deriving such a result within this framework. Rather than simply assuming quantum indeterminism, unpredictability, etc., as quantum folklore, this formalises the relationship between the concepts and clarifies the physical assumptions needed to arrive at such conclusions. In this way, we show that quantum unpredictability follows from the same assumptions giving rise to value indefiniteness in Kochen-Specker type results.

7.2 Complementarity

While these results show that value indefiniteness leads to unpredictability, this is not to say that this is the only origin of quantum unpredictability. The quantum phenomena

of complementarity has also been linked to unpredictability and, contrary to the value indefiniteness pinpointed by the Kochen-Specker theorem and Theorem 34, is present in all quantum systems, including two-dimensional systems. By itself complementarity is not *a priori* incompatible with value definiteness: it is possible, for example, to give toy models based on automata or generalised urn models that feature complementarity but not value indefiniteness [131, 155]. Although these models can not completely reproduce quantum mechanics – the Kochen-Specker theorem, for example, forbids this for nontrivial systems, and nonlocality is a further issue – they nonetheless show that complementarity itself constitutes a weaker hypothesis than value indefiniteness, even though it is sometimes taken as 'evidence' when arguing that value indefiniteness is present in all quantum systems.

It is therefore of interest to see if complementarity alone can guarantee some degree of unpredictability. This interest is not only theoretical, but also practical as some current quantum random generators, such as Quantis [76], operate in two-dimensional Hilbert space where the Kochen-Specker theorem cannot be used to certify value indefiniteness, and would hence seem to (implicitly) rely on complementarity for certification.

7.2.1 Quantum complementarity

Since complementarity can be taken to mean a range of different concepts [58], it is important that we first discuss briefly the notion of quantum complementarity and the particular form we will use before we proceed to an analysis of its predictability.

The principle of complementarity was originally formulated and promoted by Pauli [99]. As originally intended it is more of a general principle than a formal statement about quantum mechanics, and states that it is impossible to simultaneously (i.e., jointly) measure formally non-commuting observables; for this reason commutativity is nowadays often synonymous with co-measurability. It is often discussed in the context of the position and momentum observables, but it is equally applicable to any other non-commuting observables such as spin operators corresponding to different directions, such as S_x and S_y, which operate in two-dimensional Hilbert space.

Given a pair of such 'complementary' observables and a spin-$\frac{1}{2}$ particle, measuring one observable alters the state of the particle so that the measurement of the other observable can no longer be performed on the original state. Such complementarity is closely related to Heisenberg's original uncertainty principle [72], which postulated that any measurement arrangement for an observable necessarily introduces uncertainty into the value of any complementary observable. For example, an apparatus used to measure the position of a particle, would necessarily introduce uncertainty in the knowledge of the momentum of said particle. This principle and supposed proofs of it have been the

subject of longstanding (and ongoing) debate [23, 43, 116].

More precise are the formal uncertainty relations due to Robertson [115] – confusingly also often referred to as Heisenberg's uncertainty principle – which state that the standard deviations of the position and momentum observables satisfy $\sigma_x\sigma_p \geq \hbar/2$, and give a more general form for any non-commuting observables A and B. However, this mathematically only places constraints on the variances of repeated measurements of such observables, and does not formally imply that such observables cannot be co-measured, let alone have co-existing definite values, as is often claimed [110, Ch. 3].

In contrast to such uncertainty relations, complementarity is usually taken to mean the stronger statement that it is impossible to simultaneously measure pairs of non-commuting observables, and that a measurement of one will result in an irreversible loss of information relating to the other, non-measured, observable. Although one may define simultaneous (or joint) measurability in several ways, such as the existence of a joint distribution or the nonexistence of uncertainty relations [58], we take this to mean the possibility to measure two observables A and B such that subsequent measurements of either A or B yield the same results (i.e., the state is not altered). We will take the negation of this as our basis in formalising complementarity, but we do not claim that such a loss of information need be more than epistemic; to deduce more from the uncertainty relations one has to assume quantum indeterminism – that is, value indefiniteness. This assumption is indeed often made implicitly, as the indeterminism of measurements is part of the standard quantum mechanical canon, but we do not make this assumption as we wish to see to what extent complementarity alone guarantees unpredictability.

7.2.2 Complementarity and value definiteness: a toy configuration

In order to illustrate that complementarity is not incompatible with value definiteness we briefly consider an example of a toy-model of a system that is value definite but exhibits complementarity. This model was outlined in [131] and concerns a system modelled as an automaton; a different, but equivalent, generalised urn-type model is described in [155].

More specifically, the system is modelled as a Mealy automaton.

Definition 67. A *Mealy automaton* is a 5-tuple $M = (Q, \Sigma, \Theta, \delta, \omega)$ where Q is the set of states, Σ and Θ the input and output alphabets, respectively, $\delta : Q \times \Sigma \to Q$ the transition function and $\omega : Q \times \Sigma \to \Theta$ the output function.

If one is uncomfortable thinking of a system as an automaton, one can consider the system as a black box, whose internal workings as an automaton are hidden. The

state of the system thus corresponds to the state q of the automaton, and each input character $a \in \Sigma$ corresponds to a measurement, the output of which is $\omega(q, a)$ and the state of the automaton changes to $q' = \delta(q, a)$. To give a stronger correspondence to the quantum situation, we demand that repeated measurements of the same character $a \in \Sigma$ (i.e., observable) gives the same output: for all $q \in Q$, $\omega(q, a) = \omega(\delta(q, a), a)$. The system is clearly value definite, since the output of a measurement is defined prior to any measurement being made.

However, if we have two 'measurements' $a, b \in \Sigma$ such that $\omega(q, a) \neq \omega(\delta(q, b), a)$ then the system exhibits complementarity: measuring b changes the state of the system from q to $q' = \delta(q, b)$, and, as a consequence, we lose the ability to know $\omega(q, a)$.

While this example is not necessarily intended to realistically model a quantum system, it represents well many aspects of quantum logic, and serves to show that complementarity itself is not incompatible with value definiteness.

7.2.3 Complementarity as an argument for value indefiniteness

While complementarity is not incompatible with value definiteness, it is worth briefly discussing whether it nonetheless provides good evidence of quantum value indefiniteness.

On its own, complementarity only tells us that we cannot obtain via measurement a pre-existing value for certain observables. The choice of whether to interpret this as being due to the actual non-existence of these parameters or not could be seen as a choice of faith between determinism and indeterminism. Einstein famously preferred to stick to a deterministic explanation, while his contemporaries were more willing to take the bold move of attributing the seemingly unpredictable results of quantum measurements to indeterminism.

The prevailing preference to give up determinism means that, these days, one usually prefers to attribute this to indeterminism, and hence associate complementarity with this indeterminism. However, this view is heavily influenced by the Bell and Kochen-Specker theorems, and the indeterminism deduced from them (formally, via value indefiniteness).

This argument suffers from a degree of circular reasoning: complementarity is taken as evidence for value indefiniteness because value indefiniteness is already believed, thanks to independent results with additional hypotheses. Complementarity itself is, thus, compatible with value definiteness, and we should be cautious of using it as an argument for value indefiniteness, since the latter cannot be derived from the former. Hence, any unpredictability resulting from complementarity alone can be interpreted as being relative to the limits imposed by the principle of complementarity, rather that due to an absence of physical reality.

7.3 Complementarity and unpredictability

In order to consider the unpredictability of measurements of complementary observables, we will make use of the relativised notion of unpredictability we introduced in the previous chapter. This is relatively natural, since complementarity places clear restrictions on the information that any extractor can measure, simultaneously, in a systems.

Complementarity tends to be more of a general principle than a formal statement, hence in order to investigate mathematically the degree of unpredictability that complementarity entails we need to give complementarity a solid formalism. While several approaches are perhaps possible, following our previous discussion we choose a fairly strong form of complementarity and consider it not as an absolute impossibility to simultaneously know the values of non-commuting observables, but rather as a restriction on our current set of extractors – that is, using standard quantum measurements and other techniques we currently have access to.

Definition 68. Let E be an experiment involving a quantum system, and let Λ_A be the set of parameters λ corresponding to the situation in which the value $v(A)$ of an observable A is known.[12] We say that a set of extractors Ξ is *restricted by complementarity* if, for any two incompatible quantum observables A, B (i.e., $[A, B] \neq 0$), there does not exist an extractor $\xi \in \Xi$ and partially computable function f such that, whenever the value $v(A)$ of the observable A is known, the following holds for an infinite set $\Lambda \subset \Lambda_A$: for all $\lambda \in \Lambda$, $f(\xi(\lambda)) = v(B)$, and $f(\xi(\lambda))$ is undefined for all $\lambda \in \Lambda_A \setminus \Lambda$.

It would be tempting to require that $v(B)$ cannot be "extracted" for any single trial $\lambda \in \Lambda_A$ without altering the system, but, as in the definition of predictability, we need to ensure that one cannot correctly obtain $v(B)$ simply by chance. Thus, this definition requires that the value $v(B)$ cannot be reliably extracted an infinite number of times. We stress that this does not imply that A and B cannot simultaneously have definite values, simply that we cannot *know* both at once.

As for our analysis of value indefinite observables, let us consider an experiment E_C that prepares a system in an arbitrary pure state $|\psi\rangle$, thus giving $v(P_\psi) = 1$ for the

[12] We assume for simplicity that the observables A and B have discrete spectra (as for bounded systems), that is, the eigenvalues are isolated points, and hence the values $v(A)$ and $v(B)$ can be uniquely determined by measurement. Furthermore, since the choice of units is arbitrary (e.g., we can choose $\hbar = 1$) one can generally assume that $v(A)$ and $v(B)$ are rational-valued, and hence can be known 'exactly'. Even if this were not the case, a finite approximation of $v(A)$ is sufficient to uniquely identify it, and thus is enough here.

For continuous observables it is obviously impossible to identify precisely $v(A)$ or $v(B)$. Such systems are generally idealisations, but one can still handle this case by considering observables A' and B' that measure A and B to some fixed accuracy. Protection by complementarity may depend on this accuracy. For example, for position and momentum, one expects complementarity to apply only when the product of accuracies in position and momentum is less than $\hbar/2$ according to the uncertainty relations.

projection observable $P_\psi = |\psi\rangle\langle\psi|$, before performing a projective measurement onto a state $|\phi\rangle$ with $0 < |\langle\psi|\phi\rangle| < 1$ (thus $[P_\psi, P_\phi] \neq 0$) and outputting the resulting bit.

It is not difficult to see that if this experiment is unpredictable relative to an agent whose predicting power is restricted by complementarity. More formally, we have the following theorem.

Theorem 69. *Let Ξ be restricted by complementarity. Then the experiment E_C described above is unpredictable for Ξ.*

Proof. If this were not the case, there would exist an extractor $\xi \in \Xi$ and a computable predictor P_{E_C} such that, under any repetition procedure giving parameters $\lambda_1, \lambda_2, \ldots$, we have $P_{E_C}(\xi(\lambda_i)) = x_i$ for infinitely many i and $P_{E_C}(\xi(\lambda_i))$ witheld otherwise, where x_i is the outcome of the ith iteration/trial. But if we define f such that $f = P_{E_C}$ when prediction is not witheld, and undefined otherwise, then the pair (ξ, f) contradicts the restriction by complementarity, and hence E_C is unpredictable for Ξ. □

It is important to note that this result holds regardless of whether the observables measured are value definite or not, although the value definite case is of more interest. Indeed, if the observables are value indefinite then we are guaranteed unpredictability without assuming restriction by complementarity, and hence we gain little extra by considering this situation.

As a concrete example, consider the preparation of a spin-$\frac{1}{2}$ particle, for instance an electron, prepared by in a $S_z = +\hbar/2$ state before measuring the complementary observable $2S_x/\hbar$ producing an outcome in $\{-1, +1\}$. This could, for example, be implemented by a pair of orthogonally aligned Stern-Gerlach devices. Next let us assume that the system is indeed value definite. The preparation step means that, prior to the trial of the experiment being performed, $v(S_z)$ is known, and by assumption $v(S_x)$ exists (i.e., is value definite) and is thus 'contained' in the parameter λ. The assumption that Ξ is restricted by complementarity means that there is no extractor $\xi \in \Xi$ able to be used by a predictor P_E giving $P_E(\xi(\lambda_i)) = 2v(S_x)/\hbar = x_i$, thus giving unpredictability for Ξ.

As we noted at the start of the section, this is a fairly strong notion of complementarity (although not the strongest possible). A weaker option would be to consider only that we cannot directly extract the definite values: that there is no $\xi \in \Xi$ such that $\xi(\lambda) = v(S_x)$ for all λ. However, this does not rule out the possibility that there are other extractors allowing us to indirectly measure the definite values (unless we take the strong step of assuming Ξ is closed under composition with computable functions, for example). This weaker notion of complementarity would thus seem insufficient to derive unpredictability for Ξ, although it would not show predictability either. We would thus,

at least for the moment, be left unsure about the unpredictability of measurements limited by this weak notion of complementarity.

7.3.1 Means-relative versus absolute complementarity

In expressing the notion of complementarity as a restriction on the set of extractors Ξ available to any predicting agent, we made a deliberate choice to consider the most general notion of complementarity possible. This means that complementarity, in this form, is to some extent a 'means-relative' condition, as opposed to an absolute limit on possible extractors. As a result, we deduced that complementarity is only able to guarantee an epistemic, relativised form of unpredictability. The examples we have given that show the possibility to conceive toy models that are not unpredictable, but still certified by a form of complementarity, show that this is indeed a good general approach to complementarity.

However, one could choose to argue that, especially in the case of quantum complementarity, the concept of complementarity should be formulated as the stronger hypothesis that no such extractor $\xi \in \Xi$ extracting complementary values can physically exist *for any set* Ξ *of extractors*. However, this constitutes an additional, relatively strong and certainly unproven, physical assumption, especially in the case of interest of a value definite reality subject to the principle of complementarity. It would, in this case, mean the existence of definite values that are *in principle* unknowable – a strongly metaphysical assumption that is by its very nature untestable.

If one were to make such an assumption, complementarity would guarantee (simple) unpredictability (i.e., not just a relativised form of unpredictability), since the definition of an extractor requires that it be physically implementable in principle.

7.4 Incomputability, unpredictability, and quantum randomness

As we discussed at length in Chapter 5, the notion of randomness is a subtle one, and we should be careful not to claim that the unpredictability of quantum measurements implies that quantum randomness is 'truly random' in any sense. We showed then that, under the appropriate physical assumptions, one can use value indefiniteness to guarantee that the output of the kind of infinite experiment we have been discussing can be guaranteed to be bi-immune, although this is of course well short even of Martin-Löf randomness. Furthermore, as discussed in Chapter 5, maximal randomness in the sense

that no correlations exist between successive measurement results is mathematically impossible [29, 65]: there exist only degrees of randomness with no upper limit.

Nonetheless, the unpredictability of quantum measurement outcomes certainly appears to add a stronger formal basis to the intuitions generally expressed regarding quantum randomness, and can help to explain its origin. As mentioned earlier, Eagle has argued that a physical process is random if it is 'maximally unpredictable' [49]. In this light it may be reasonable to consider quantum measurements as random events, giving a more formal meaning to the notion of 'quantum randomness'. However, given the intricacies of randomness, it should be clear that this refers to the measurement *process*, and does not entail that quantum measurement outcomes are maximally random. As a result, any claims regarding the quality of quantum randomness need to be analysed carefully.

Given the relation between unpredictability and Tadaki total unpredictability (which implies bi-immunity) discussed in Sec. 6.6, it is natural to ask whether the bi-immunity of sequences generated by measuring repeatedly a value indefinite observable is a general consequence of its unpredictability, or if it is an independent consequence of value indefiniteness.

7.4.1 Unpredictability and incomputability

The links between unpredictability and Tadaki total unpredictability we explored in Sec. 6.6 are relative to the use of specific extractors – such as the 'prefix' extractor ξ_p – which limit the predicting agent to an algorithmic framework, and need not hold when other more physically relevant extractors are considered. Furthermore, for the unpredictability of an experiment E to guarantee that *any* outcome of an infinite repetition of E be incomputable – a much weaker statement than bi-immunity – it would have to be the case that (taking the contrapositive) if even a single infinite repetition $\lambda_1, \lambda_2, \ldots$ of E could generate a computable sequence this would imply that E is predictable. However, the definition of a predictor P_E for E requires that P_E gives correct predictions for *all* repetitions. Hence, we will elaborate a simple example of an unpredictable experiment E that can produce *both* computable and incomputable sequences, showing that unpredictability does not imply incomputability (let alone bi-immunity).

Example 70. Recall that the dyadic map $d : \{0,1\}^\omega \to \{0,1\}^\omega$ is chaotic and is defined by $d(x_1x_2x_3\ldots) = x_2x_3\ldots$ (see Example 63). Let us consider an experiment E_d which involves iterating the dyadic map $k \geq 2$ times on a 'seed' $\mathbf{x} = 0x_2x_3\ldots$ until $x_{k+1} = 0$. In other words, given $\mathbf{x}$ we look for the smallest integer $k \geq 2$ such that $x_{k+1} = 0$, hence $d^k(\mathbf{x}) = 0x_{k+2}x_{k+3}\ldots$. *If such a k exists, then the outcome of the experiment is $x_{k+2} \in \{0,1\}$.* Note that this experiment differs from the experiment E_k

used in Example 63 in that the number of iterations, k, may vary depending on the seed, whereas in E_k it is constant.

We assume that such an E_d (ideally) is physically implementable. We have chosen this example for simplicity; a more 'physically natural' example might be the evolution of a chaotic double pendulum from some set of initial condition (i.e., up to finite accuracy) for which the outcome is read off once the pendulum returns sufficiently close to its initial conditions. *Let us assume further that any sequence $\mathbf{x} = x_1x_2\ldots$ such that $x_1 = 0$ is a valid physical seed.* For the case of a double pendulum this is akin to assuming that the position of a pendulum can take any value in the continuum rather than be restricted to a countable, discrete set of states – not an unreasonable, if nonetheless important, assumption.

Theorem 71. *The experiment E_d can, when repeated ad infinitum, produce both computable and incomputable sequences.*

Proof. The experiment can, of course, be repeated in many different ways – that is, under many different repetition scenarios – to generate an infinite sequence, but it suffices to consider the simplest case where the transformed seed $\mathbf{x}^{(1)} = d^k(\mathbf{x})$ after one iteration is taken as the seed for the next step; note that this, by design, satisfies the requirement that the first bit of $\mathbf{x}^{(1)}$ is 0 (i.e., $x_1^{(1)} = 0$), provided k exists.

Let $\mathbf{y} = y_1y_2\ldots$ be an arbitrary infinite sequence, and consider the sequence $\mathbf{x} = 010y_10y_20y_3\ldots$. For any such sequence $\mathbf{x}$ of this form, $d^2(\mathbf{x}) = 0y_10y_2\ldots$, so the outcome of E_d with seed $\mathbf{x}$ is precisely y_1, and the new seed $\mathbf{x}^{(1)} = d^2(\mathbf{x}) = 0y_10y_2\ldots$. Similarly, for all i, starting with the seed $\mathbf{x}^{(0)} = \mathbf{x}$, the outcome of the ith repetition is precisely y_i, since a minimum number of $k = 2$ applications of d suffices for the first bit of $d^2(\mathbf{x}^{(i-1)})$ to be 0, and the seed after this repetition is precisely $\mathbf{x}^{(i)} = 0y_i0y_{i+1}\ldots$. If the repetition is started with the seed $\mathbf{x}$ one obtains the infinite sequence $\mathbf{y}$ by repeating E_d to infinity. In particular, since $\mathbf{y}$ can be any sequence at all, one can obtain both computable and incomputable sequences by repeating E_d. Note that, since $\mathbf{y}$ (and $\mathbf{x}$) is an infinitely specified quantity we cannot 'choose' the seed $\mathbf{x}$ for the repetition; the important point is simply that any such $\mathbf{x}$ is a *possibility.* □

Let us show also that E_d is unpredictable.

Theorem 72. *The experiment E_d is (simply) unpredictable.*

Proof. Let us assume, for the sake of contradiction, that there exists a predictor P_{E_d} and extractor ξ_d such that P_{E_d} is correct for ξ_d. Then P_{E_d} must give infinitely many correct predictions using ξ_d for any two runs $\lambda_1\lambda_2\ldots$ and $\lambda'_1\lambda'_2\ldots$ which differ only in their seeds $\mathbf{x}$ and $\mathbf{x}'$. In particular, this is true if $\mathbf{x}, \mathbf{x}'$ are sequences of the form $0a_1a_2\ldots$

where $a_i \in \{1^t00, 1^t01\}$ for all i, and $t \geq 1$ is fixed, since these are possible seeds for E_d. For such seeds $\mathbf{x}, \mathbf{x}'$ the minimum $k \geq 2$ such that the first bit of $d^k(\mathbf{x})$ is 0 is precisely $k = t + 1$. Furthermore, if we let $\mathbf{x}^{(0)} = \mathbf{x}$ and $\mathbf{x}^{(i)} = d^{k_i}\left(\mathbf{x}^{(i-1)}\right)$ be the seed for the ith repetition of E_d, then $k_i = t + 1$ for all i; that is, each iteration of E_d shifts the seed precisely $t + 1$ bits. Thus, to make infinitely many correct predictions for E_d starting with seeds $\mathbf{x}$ and $\mathbf{x}'$ correctly, P_E must have access, via ξ_d, to more than $t + 3$ bits of the current seed, since the first $t+2$ bits of $\mathbf{x}^{(i)}$ and $\mathbf{x}'^{(i)}$ are the same for all i. However, since t is arbitrary, and the same extractor ξ_d must be used for all repetitions regardless of the seed, this implies that ξ_d is *infinitely accurate*, which is, again, *not physically possible* for an extractor. Consequently, E_d must be unpredictable. □

The construction of E_d may be slightly artificial and its unpredictability relies, of course, on certain physical assumptions about the possibility of certain extractors. However, this concrete example shows that there is no mathematical obstacle to an unpredictable experiment producing both computable and incomputable outcomes when repeated, and is, at the very least, physically conceivable.

Any link between the unpredictability of an experiment and computability theoretic properties of its output thus relies critically on physical properties – and assumptions – of the particular experiment. Indeed, this careful dependance on the particular physical description of E is one of the strengths of this general model. This gives the model more physical relevance as a notion of (un)predictability than purely algorithmic proposals.

The bi-immunity of quantum randomness is a crucial illustration of this fact. Although bi-immunity does not guarantee the unpredictability of an experiment (see Example 63), it can also be derived, via the relevant physical assumptions, from value indefiniteness. For this particular quantum experiment bi-immunity complements, but is independent of, unpredictability.

7.4.2 Relativised unpredictability and incomputability

Given the relationship between complementarity and relativised unpredictability, and hence its relevance for quantum unpredictability, it is important to also look at the relation between experiments that are unpredictable with respect to restricted sets of extractors, but not simply unpredictable, and the computability of sequences that these experiments produce.

Example 70 shows that a simply unpredictable experiment can produce both computable and incomputable, even algorithmically random, sequences. It thus follows, *a fortiori*, that the same is true for relativised unpredictability, since a simply unpredictable experiment is also unpredictable for any subset of extractors: there exist exper-

iments that are unpredictable for a restricted sets of extractors, and which are capable of producing, in the limit, computable outcomes.

7.4.3 Incomputability and complementarity

Even though the (relativised) unpredictability associated with complementary quantum observables cannot guarantee incomputability, one may ask whether this complementarity may, with reasonable physical assumptions, lead directly to incomputability, much as value indefiniteness does.

We will show that complementarity, unlike value indefiniteness, cannot guarantee any kind of incomputability. Specifically, we will show how an, admittedly toy, (value definite) system exhibiting complementarity (and thus unpredictable relative for extractors limited by the complementarity principle) can produce computable sequences when repeated.

Example 73. Consider an experiment E_M involving the prediction of the outcome of measurements on an (unknown but fixed) Mealy automaton $M = (Q, \Sigma, \Theta, \delta, \omega)$, which we can idealise as a black box, with $\{x, z\} \in \Sigma$ characters in the input alphabet, output alphabet $\Theta = \{0, 1\}$ and satisfying the conditions that a) for all $q \in Q$ and $a \in \Sigma$, $\omega(q, a) = \omega(\delta(q, a), a)$, and b) x and z are complementary: that is, for all $q \in Q$ we have $\omega(q, z) \neq \omega(\delta(q, x), z)$ and $\omega(q, x) \neq \omega(\delta(q, z), x)$. Note that the specification of E_M does not require M to be in any particular initial state, which in general is unknown. This automaton is deliberately specified to resemble measurements on a qubit, and can be viewed as a toy model of a two-dimensional value definite quantum system, where the outcomes of measurements are determined by some unknown, hidden Mealy automaton. Since the Kochen-Specker theorem does not apply to two-dimensional systems, this value definite toy model poses no direct contradiction with quantum mechanics [80], even if it is not intended to be particularly realistic. We complete the specification of E_M by considering a trial of E_M to be the output on the string xz, that is, if the automaton is initially in the state q, the output is $\omega(\delta(q, x), z)$, and the final state is $\delta(\delta(q, x), z)$. This is a clear analogy to the preparation and measurement of a qubit using complementary observables, of the type discussed earlier.

We wish to show that E_M is unpredictable for a set Ξ_C of extractors that expresses the restriction by complementarity present in Mealy automata. In particular, let us consider the set Ξ_C that, in analogy to the restriction by complementarity of two quantum observables defined earlier, is restricted by an analogue of complementarity for the inputs $x, z \in \Sigma$.

Definition 74. Let Λ_x be the set of parameters λ corresponding to M being in a state

q in the set $\{q \in Q \mid \delta(q', x) = q \text{ for some } q' \in Q\}$.[13] A set Ξ of extractors is *restricted by M-complementarity* if there is no extractor $\xi \in \Xi$ and partially computable function f such that, if M is in a state q with $\lambda \in \Lambda_x$, the following holds for an infinite set $\Lambda \subset \Lambda_x$: for all $\lambda \in \Lambda$, $f(\xi(\lambda)) = \omega(q, x))$, and $f(\xi(\lambda))$ is undefined for all $\lambda_{\in}\Lambda_x \setminus \Lambda$.

That means that, if M is in an 'eigenstate' of x, we cannot extract the output of the input z (and similarly for z and x interchanged).

Theorem 75. *The experiment E_M is unpredictable for Ξ_C if Ξ_C is restricted by M-complementarity.*

Proof. Let us assume for the sake of contradiction that E_M is predictable for Ξ_C: that is, there is a predictor P_{E_M} and an extractor $\xi \in \Xi_C$ such that E_M is predictable for ξ. Thus, from the definition of predictability, when E_M is is repeated under any repetition procedure, P_{E_M} must provide infinitely correct predictions and no incorrect ones. This must thus be true if E_M is repeated by inputting x to prepare the ith trial so that each λ_i is in Λ_x. For such a repetition procedure, the output of the ith trial of E_M is precisely $\omega(\delta(q_i, x), z) = \omega(q_i, z)$, and for each trial we have either $P_{E_M}(\xi(\lambda_i)) = \omega(q_i, z)$ or prediction witheld. But if we define f such that $f = P_{E_M}$ when prediction is not witheld, and undefined otherwise, then the pair (ξ, f) contradicts the restriction by M-complementarity, and hence we conclude that E_M is unpredictable for Ξ_C. □

It is important to understand that the unpredictability of E_M for any Ξ_C restricted by M-complementarity expresses the inability to give a single predictor/extractor pair that gives correct predictions for *any* valid repetition procedure, rather than just for a single repetition procedure. Indeed, if we consider perhaps the simplest repetition procedure, where the final state of the system after the ith trial is the initial state for the $(i+1)$th trial, then the sequence produced by the infinite repetition of trials is necessarily computable – even cyclic – since it simply represents the run of the automaton. This computability, however, fails to provide a predictor for E_M since it would fail to provide correct predictions for other repetition procedures, where, for example, a new copy of the system in a new initial state is used for each trial. This same observation means that the fact that any Mealy automaton is learnable in the infinite limit [63] equally fails to provide a general method of prediction for E_M.

This example does show, however, that the experiment E_M, although unpredictable for Ξ_C, is capable of producing computable sequences, even if it need not do so under all repetition procedures, and hence computability is not excluded by complementarity.

[13] Note that such a state q satisfies $\omega(q', x) = \omega(\delta(q', x), x) = \omega(q, x)$, and hence q is an 'eigenstate' of x.

We note that one could easily consider slightly more complicated scenarios where the outcomes are controlled not by a Mealy automaton, but an arbitrary computable – or even, in principle, incomputable – function; complementarity is agnostic with respect to the computability of the output of such an experiment. If indeed we were to consider a toy system modelled as a Turing machine, one loses the simplicity of the finite-state model, as well as a certain degree of finiteness, since Turing machines must in general have access to arbitrary large, although only ever finite, memory [122].

Let us nonetheless entertain such an example, and consider such a system and a corresponding experiment E_T which, by analogy to E_M, performs a finite computation on the working tape of the Turing machine, before outputting a single bit. If such an E_T were iterated, as we considered for E_M, keeping the contents of the working tape between iterations (i.e., its internal state – always finite), this iteration could produce, in the infinite limit, any computable sequence. Such a sequence may be 'obviously' computable – such as the sequence $000\ldots$ – but it could equally be something far less obvious, such as the digits in the binary expansion of $\pi = \pi_1\pi_2\ldots$ at prime indices, that is, $\pi_p = \pi_2\pi_3\pi_5\pi_7\pi_{11}\ldots$. Hence, this scenario cannot be easily ruled out empirically, regardless of the computability and subsequent predictability of the resulting sequences. Further emphasising this, we note that computable sequences can also be Borel normal, as for Champernowne's constant or (as conjectured) π (and, perhaps, even π_p), and thus satisfy many statistical properties one would expect of random sequences.

Our point was not to propose this as a realistic physical model (although it perhaps cannot be dismissed so easily; if quantum mechanics is value definite, but contextually so, such a model is not so implausible conceptually) but to illustrate a conceptual possibility. Value indefiniteness rules this computability out, but complementarity fails to do the same in spite of its intuitive interpretation as a form of quantum uncertainty. At best it can be seen as an epistemic uncertainty, as it at least poses a physical barrier to the knowledge of any definite values. The fact that complementarity cannot guarantee incomputability is in agreement with the fact that value definite, contextual models of quantum mechanics are perfectly possible (see Sec. 4.5.1); such models need not contradict any principle of complementarity, and can be computable or incomputable.

7.5 Summary

The unpredictability of single bits generated by the measurement of a value indefinite quantum observable formalises and confirms the intuition regarding the unpredictability of such measurements. As we discussed in Section 5.1, unpredictability is a key notion of randomness for physical processes, and by formalising such a general notion of unpre-

dictability we allow the randomness of physical events to be more carefully evaluated.

As our formalism makes clear, unpredictability can come in several different strengths, from a relativised epistemic form, to the simple unpredictability that we prove for quantum value indefinite measurements. The non-relativised form of a unpredictability provides a more suitable candidate for a general definition of process randomness, since one generally conceives such randomness to be an objective, rather than epistemic notion. However, as our formulation makes clear, this should not be taken as evidence for a form of absolute randomness, since one can vary the strength of unpredictability by varying the level of effectivity of the predictor. Thus, as for algorithmic forms of randomness, several strengths of process randomness are possible, with no absolute or maximal form of randomness possible. However, as for Martin-Löf randomness, the notion of predictability based on Turing computability is perhaps the most natural.

Value indefiniteness can thus be used to certify not only the strong incomputability of sequences of bits generated by quantum measurements, but also the unpredictability and subsequent randomness of individual quantum measurements. This gives a formal notion to help clarify the precise strength and degree of quantum randomness.

Chapter 8

Conclusions and open questions

In this thesis we have discussed several issues at the core of the notion of quantum randomness.

In one of the main theoretical results of the thesis we extended the Kochen-Specker theorem, proving a stronger variant (Theorem 34) that formally shows the extent of quantum value indefiniteness. This adds a much stronger basis to the intuition that all non-trivial quantum measurements are indeterministic, a critical prerequisite to quantum randomness.

We proved that infinite sequences of bits generated by measurements of value indefinite observables are bi-immune, thus showing a formal algorithmic difference in strength between classical and quantum sources of randomness. This scenario is precisely that which quantum random number generators attempt to reproduce, and we propose such a design that is certified by value indefiniteness.

Finally, we presented a general framework for unpredictability and showed, in support of the standard intuition, that individual quantum measurements of value indefinite observables are unpredictable with respect to our model.

These results help provide a more nuanced and complete understanding of the nature of quantum randomness, beyond the much flaunted claims of true quantum randomness that reduce it simply to indeterminism.

8.1 Open questions and future research

We conclude this thesis with some open questions raised by our research.

8.1.1 Value indefiniteness of two-dimensional spaces

Theorem 34, in extending the Kochen-Specker theorem to localise value indefiniteness, allows quantum indeterminism to be deduced from more fundamental physical principles. However, the formal result, like the Kochen-Specker theorem, only holds in dimension three or higher Hilbert spaces. While value indefiniteness can be postulated to be present also in two-dimensional Hilbert spaces, this is less satisfying than deriving it from formal results. Although it is well known that there are counterexamples to the Kochen-Specker theorem in two-dimensional Hilbert spaces [80], it would be interesting to see if there are any stronger, but still reasonable, physical assumptions that can be used to prove value indefiniteness even in the two-dimensional case.

8.1.2 Orthogonality relations for proving Theorem 34

Much attention has been given to the orthogonality relations (Greechie diagrams) used to prove the Kochen-Specker theorem. The proof of Theorem 34, unlike the Kochen-Specker theorem, requires arbitrarily large (but always finite) sets of observables to deduce the value indefiniteness of certain observables. In Section 4.3.3 we posed Conjecture 41, hypothesising that this is unavoidable, and that it is impossible to give a fixed orthogonality diagram which can be used to prove the value indefiniteness of any observable. It would be interesting and valuable to our understanding of quantum foundations to confirm this conjecture.

8.1.3 Beyond quantum bi-immunity

While we showed in Theorem 47 that an infinite sequence produced by measuring value indefinite quantum observables is guaranteed to be bi-immune, we failed to show that such a sequence is Martin-Löf random, a much more desirable notion of randomness. As we discussed in Section 5.2.2, this is primarily due to the measure-independence of this result. Thus, it would be interesting to look at how one can combine the distribution predicted by the Born rule with this guarantee of bi-immunity to see if a stronger, measure-dependent, notion of algorithmic randomness can be guaranteed in the same way bi-immunity is.

8.1.4 Alternative principles certifying quantum randomness

Although we have approached the issue of quantum randomness from the view of quantum value indefiniteness, using this to certify both the bi-immunity and unpredictability

of quantum randomness, it would be of interest to see if there are other quantum properties that can be used to certify forms of randomness.

8.1.5 Computational irreducibility

In Section 6.3 we discussed several possible routes to formalising the notion of computational irreducibility (CIR) introduced by Wolfram [151]. The concept of CIR is generally dealt with informally, and it would be valuable to study certain properties of CIR more formally. We identified one particular route, based on the complexity theoretic optimality of certain computational dynamics, that appears to be the most robust and reasonable option.

We did not pursue this avenue because we determined its relation to unpredictability was not strong enough to warrant pursuing further in that direction, but the concept of CIR is nonetheless interesting. However, it remains to be rigorously defined and certain factors such as the leeway in efficiency given to simulations need careful consideration. It would be interesting to do so and apply the notion to certain computational systems (automata, Turing machines, etc.) as well as to formally study the computational irreducibility of universality.

Appendix A

Further details and code

A.1 Further details for the proof of Lemma 37

The computational proof of Lemma 40 in Sec. 4.3.2.1 relies critically on the analysis of the function $f(p_1) = \langle a|c\rangle$ for $p_1 \in \left(\frac{1}{\sqrt{2}}, 1\right)$, where $p_1 = |\langle a|b\rangle|$. Here we give further details of this analysis, which was carried out using Wolfram Mathematica 9.0.1.0 [152].

Specifically, we have

$$f(p_1) = \langle a|c\rangle = x_3 p_1 + \frac{y_3}{k}(x_2 - p_1 p_3) - \frac{q_1 z_3}{k q_2}(y_2 z_1 + y_1 z_2),$$

where the constants are defined in terms of p_1 as follows:

$$\alpha_1 = \frac{\arccos\sqrt{\frac{2}{3}}}{\arccos\frac{1}{\sqrt{2}}}, \qquad \alpha_2 = \frac{\arccos\frac{2}{\sqrt{5}}}{\arccos\sqrt{\frac{2}{3}}}, \qquad \alpha_3 = \frac{\arccos\sqrt{\frac{2}{3}}}{\arccos\sqrt{\frac{2}{5}}},$$

$$\theta_{a,b} = \arccos p_1, \qquad \theta_{a,v_1} = \alpha_1 \theta_{a,b}, \qquad \theta_{a,v_2} = \alpha_2 \theta_{a,v_1},$$

$$q_1 = \sqrt{1 - p_1^2}, \qquad x_1 = \cos\theta_{a,v_1}, \qquad y_1 = \frac{p_1(1 - x_1^2)}{q_1 x_1}, \qquad z_1 = \sqrt{1 - x_1^2 - y_1^2},$$

$$q_2 = \sqrt{1 - x_1^2}, \qquad x_2 = \cos\theta_{a,v_2}, \qquad y_2 = \frac{x_1(1 - x_2^2)}{q_2 x_2}, \qquad z_2 = \sqrt{1 - x_2^2 - y_2^2},$$

$$p_3 = p_1 x_2 + q_1 \frac{y_1 y_2 - z_1 z_2}{q_2}, \qquad \theta_{b,v_2} = \arccos p_3, \qquad \theta_{b,c} = \alpha_3 \theta_{b,v_2},$$

$$q_3 = \sqrt{1 - p_3^2}, \qquad x_3 = \cos\theta_{b,c}, \qquad y_3 = p_3 \frac{(1 - x_3^2)}{q_3 x_3}, \qquad z_3 = \sqrt{1 - x_3^2 - y_3^2},$$

$$k = \sqrt{(x_2 - p_3 p_1)^2 + \left(\frac{(y_1 y_2 - z_1 z_2)}{q_2} - p_3 q_1\right)^2 + \left(\frac{y_2 z_1 + y_1 z_2}{q_2}\right)^2}.$$

A.1.1 Continuity of f

The continuity of f on the domain $\left(\frac{1}{\sqrt{2}}, 1\right)$ can be shown by looking at the continuity of each term above.

We can easily see that $\theta_{a,b}$ is continuous on this domain since $p_1 < 1$, and furthermore that $\theta_{a,b} \in \left(0, \frac{\pi}{4}\right)$. Thus, θ_{a,v_1} and θ_{a,v_2} are also continuous and non-zero. It is clear that q_1 is continuous and $q_1 \in (0, 1)$, and the continuity of x_1 follows from the continuity of θ_{a,v_1}, and $x_1 > 0$. Thus, since $q_1 x_1 \neq 0$ we deduce the continuity of y_1 and z_1. From an analogous argument we get the continuity of q_2, x_2, y_2, z_2, p_3, as well as that $p_3 \in (0, 1)$. Thus, this shows further the continuity of θ_{b,v_2}. The remaining terms, including k can readily be shown to be continuous (as a function of p_1) in a similar fashion, with $k \neq 0$.

Thus, since f is composed of terms that are continuous on $\left(\frac{1}{\sqrt{2}}, 1\right)$ with non-zero denominators, it follows that f is continuous on this domain.

A.1.2 Limit behaviour of f

The Mathematica code below uses these constants and the form of $f(p_1)$ to give the following Taylor expansion of f at $p_1 = 1$, showing the behaviour of $f(p_1)$ as $p_1 \to 1$ from below. It also calculates the derivative $\frac{\mathrm{d}f}{\mathrm{d}p_1}$ which is used to generate Fig. 4.6.

$$
\begin{aligned}
f(p_1) =& 1 + \frac{(p_1 - 1)}{\pi^2 \arccos^2 \sqrt{\frac{2}{5}}} \left(\pi^2 \left(\arccos^2 \sqrt{\frac{2}{5}} + \operatorname{arcosh}^2 \sqrt{\frac{2}{3}} \right) \right. \\
& + 8 \arccos \frac{2}{\sqrt{5}} \left(\arccos \frac{2}{\sqrt{5}} \left(2 \arccos^2 \sqrt{\frac{2}{3}} \right. \right. \\
& + \sqrt{\left(\pi^2 + 16 \operatorname{arcosh}^2 \sqrt{\frac{2}{3}} \right) \left(\arccos^2 \sqrt{\frac{2}{5}} + \operatorname{arcosh}^2 \sqrt{\frac{2}{3}} \right)} \Bigg) + 4 \arccos \sqrt{\frac{2}{3}} \\
& \left. \left. \times \sqrt{\left(\arccos^2 \sqrt{\frac{2}{5}} + \operatorname{arcosh}^2 \sqrt{\frac{2}{3}} \right) \left(\arccos^2 \sqrt{\frac{2}{3}} + \operatorname{arcosh}^2 \frac{2}{\sqrt{5}} \right)} \right) \right) \\
& + \mathcal{O}((p_1 - 1)^2),
\end{aligned}
$$

which numerically simplifies to

$$
f(p_1) = 1 - 1.2658(1 - p_1) + \mathcal{O}((p_1 - 1)^2).
$$

A.1.3 Mathematica code

```
$Assumptions = 0 < p1 < 1;
f[p1_] :=
 Module[{a, \[Alpha]1, \[Alpha]2, \[Alpha]3, q1,
   b, \[Theta]ab, \[Theta]av1, x1, y1, z1, v1, \[Theta]av2, p2, q2,
   x2, y2, z2, v2, \[Theta]bv2, \[Theta]bc, p3, q3, k, x3, y3,
   z3}, \[Alpha]1 = ArcCos[Sqrt[2/3]]/ArcCos[1/Sqrt[2]];
  \[Alpha]2 = ArcCos[Sqrt[4/5]]/ArcCos[Sqrt[2/3]];
  \[Alpha]3 = ArcCos[Sqrt[2/3]]/ArcCos[Sqrt[2/5]];
  a = {1, 0, 0};
  q1 = Sqrt[1 - p1^2];
  b = {p1, q1, 0};
  \[Theta]ab = ArcCos[a.b];
  \[Theta]av1 = \[Alpha]1 \[Theta]ab;
  x1 = Cos[\[Theta]av1];
  y1 = p1 (1 - x1^2)/(q1 x1);
  z1 = Sqrt[1 - x1^2 - y1^2];
  v1 = {x1, y1, z1};
  \[Theta]av2 = \[Alpha]2 \[Theta]av1;
  p2 = x1; q2 = Sqrt[1 - x1^2] ;
  x2 = Cos[\[Theta]av2] ;
  y2 = p2 (1 - x2^2)/(q2 x2);
  z2 = Sqrt[1 - x2^2 - y2^2];
  v2 = {x2, (y1 y2 - z1 z2)/q2, (y2 z1 + y1 z2)/q2};
  \[Theta]bv2 = ArcCos[b.v2];
  \[Theta]bc = \[Alpha]3 \[Theta]bv2;
  p3 = b.v2;
  q3 = Sqrt[1 - p3^2];
  norm[x_] := Sqrt[x.x]; k = norm[v2 - p3 b];
  x3 = Cos[\[Theta]bc];
  y3 = p3 (1 - x3^2)/(q3 x3) ;
  z3 = Sqrt[1 - x3^2 - y3^2];
  Return[x3 p1 + y3/k (x2 - p1 p3) - (z3 q1)/(k q2) (y2 z1 + y1 z2)]]
Series[f[p1], {p1, 1, 1}]
D[f, p1]
```

Bibliography

[1] A. A. Abbott, L. Bienvenu, and G. Senno. Non-uniformity in the Quantis random number generator. *CDMTCS Research Report Series 472*, 2014.

[2] A. A. Abbott and C. S. Calude. Von Neumann normalisation of a quantum random number generator. *Computability*, 1:59–83, 2012.

[3] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness. *Physical Review A*, 86:062109, 2012.

[4] A. A. Abbott, C. S. Calude, and K. Svozil. Value-indefinite observables are almost everywhere. *Physical Review A*, 89:032109, 2013.

[5] A. A. Abbott, C. S. Calude, and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6(4):773–789, 2015.

[6] A. A. Abbott, C. S. Calude, and K. Svozil. On the unpredictability of individual quantum measurement outcomes. In L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, and W. Schulte, editors, *Fields of Logic and Computation II – Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday*, volume 9300 of *Lecture Notes in Computer Science*, pages 69–86. Springer International, Switzerland, 2015.

[7] A. A. Abbott, C. S. Calude, and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness. *Journal of Mathematical Physics*, 56:102201, 2015.

[8] A. Acín. True quantum randomness. In A. Suarez and P. Adams, editors, *Is Science Compatible with Free Will?: Exploring Free Will and Consciousness in the Light of Quantum Physics and Neuroscience*, chapter 2, pages 7–22. Springer-Verlag, New York, 2013.

[9] D. Albert. Physics and chance. In Y. Ben-Menahem and M. Hemmo, editors, *Probability in Physics*. Springer-Verlag, Berlin Heidelberg, 2012.

[10] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A new violation of Bell's inequalities. *Physical Review Letters*, 49(2):91–94, 1982.

[11] D. H. Bailey, P. B. Borwein, and S. Plouffe. On the rapid computation of various polylogarithmic constants. *Mathematics of Computation*, 66(218):903–913, 1997.

[12] F. Bailly and G. Longo. Randomness and determinism in the interplay between the continuum and the discrete. *Mathematical Structures in Comptuer Science*, 17(2):289–305, 2007.

[13] B. Beckage, S. Kauffman, L. J. Gross, A. Zia, and C. Koliba. More complex complexity: Exploring the nature of computation irreducibility across physical, biological, and human social systems. In H. Zenil, editor, *Irreducibility and Computation Equivalence*, pages 79–88. Springer-Verlag, Berlin Heidelberg, 2013.

[14] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447–452, 1966.

[15] J. S. Bell. Against 'measurement'. *Physics World*, 3:33–41, 1990.

[16] L. M. Berliner. Statistics, probability and chaos. *Statistical Science*, 7(1):69–90, 1992.

[17] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37(4):823–843, 1936.

[18] P. Blasiak. Classical systems can be contextual too: Analogue of the Mermin-Peres square. *Annals of Physics*, 353:326–339, 2015.

[19] A. Blass, N. Dershowitz, and Y. Gurevich. When are two algorithms the same? *Bulletin of Symbolic Logic*, 15(2):145–168, 2009.

[20] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I, II. *Physical Review*, 85(2):166–193, 1952.

[21] M. Born. Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik*, 38:803–837, 1926. English translation by J. A. Wheeler and W. H. Zurek, in [147, Chap. I.2].

[22] M. Born. *Physics in my generation*. Springer, New York, second edition, 1969.

[23] P. Busch, P. Lahti, and R. F. Werner. Measurement uncertainty relations. *Journal of Mathematical Physics*, 55:042111, 2014.

[24] A. Cabello. A simple proof of the Kochen-Specker Theorem. *European Journal of Physics*, 15:179–183, 1994.

[25] A. Cabello. Finite-precision measurement does not nullify the Kochen-Specker theorem. *Physical Review A*, 65:52101, 2002.

[26] A. Cabello. Experimentally testable state-independent quantum contextuality. *Physical Review Letters*, 101:210401, 2008.

[27] A. Cabello, J. M. Estebaranz, and G. García-Alcaine. Bell-Kochen-Specker Theorem: A proof with 18 vectors. *Physics Letters A*, 212:183–187, 1996.

[28] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil. Experimental evidence of quantum randomness incomputability. *Physical Review A*, 82:022102, 2010.

[29] C. S. Calude. *Information and Randomness: An Algorithmic Perspective.* Springer-Verlag, Berlin, second edition, 2002.

[30] C. S. Calude and G. Longo. Classical, quantum and biological randomness as relative incomputability. *Natural Computing*, to appear, 2015.

[31] C. S. Calude and K. Svozil. Quantum randomness and value indefiniteness. *Advanced Science Letters*, 1(2):165–168, 2008.

[32] R. A. Campos, B. E. A. Saleh, and M. C. Teich. Quantum-mechanical lossless beam splitter: $SU(2)$ symmetry and photon statistics. *Physical Review A*, 40(3):1371, 1989.

[33] G. J. Chaitin. Algorithmic information theory. *IBM Journal of Research and Development*, 21(4):350–359, 1977.

[34] D. G. Champernowne. The construction of decimals normal in the scale of ten. *Journal of the London Mathematical Society*, 8:254–260, 1933.

[35] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Reviw Letters*, 111:130406, 2013.

[36] J. F. Clauser and A. Shimony. Bell's Theorem: Experimental tests and implications. *Reports on Progress in Physics*, 41:1881–1926, 1978.

[37] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880, 1969.

[38] R. K. Clifton. Getting contextual and nonlocal elements-of-reality the easy way. *American Journal of Physics*, 61(5):443–447, 1993.

[39] R. K. Clifton. Private communication to Karl Svozil, 1995.

[40] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and General*, 44:095305, 2011.

[41] R. Colbeck and R. Renner. No extension of quantum theory can have improved predictive power. *Nature Communications*, 2(411), 2011.

[42] B. J. Copeland. The Church-Turing thesis. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Fall 2008 edition, 2008.

[43] R. Cowen. Proof mooted for quantum uncertainty. *Nature News*, 498(7455):419–420, 27 June 2013.

[44] M. Davis. Why there is no such discipline as hypercomputation. *Applied Mathematics and Computation*, 178:4–7, 2006.

[45] R. L. Devaney. *An Introduction to Chaotic Dynamical Systems*. Benjamin/Cummings Publishing Company, Inc., Menlo Park, 1986.

[46] P. Diaconis, S. Holmes, and R. Montgomery. Dynamical bias in the coin toss. *SIAM Review*, 49(2):211–235, 2007.

[47] R. G. Downey and D. R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Theory and Applications of Computability. Springer, New York Dordrecht Heidelberg London, 2010.

[48] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields. A high speed, post-processing free, quantum random number generator. *Applied Physics Letters*, 93:031109, 2008.

[49] A. Eagle. Randomness is unpredictability. *The British Journal for the Philosophy of Science*, 56(4):749–790, 2005.

[50] A. Eagle. Chance versus randomness. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Spring 2014 edition, 2014.

[51] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[52] A. C. Elitzur, S. Popescu, and D. Rohrlich. Quantum nonlocality for each pair in an ensemble. *Physics Letters A*, 162(1):25–28, 1992.

[53] P. van Embde Boas. Ten years of speedup. In J. Becvár, editor, *Proceedings of MFCS*, volume 32 of *Lecture Notes in Computer Science*, pages 13–29. Springer-Verlag, Berlin Heidelberg, 1975.

[54] H. D. Everett, III. "Relative state" formulation of quantum mechanics. *Reviews of Modern Physics*, 29(3):454–462, 1957.

[55] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro. Secure self-calibrating quantum random-bit generator. *Physical Review A*, 75:032334, 2007.

[56] J. F. Fitzsimons, E. G. Rieffel, and V. Scarani. Quantum frontier. In J. Zander and P. J. Mosterman, editors, *Computation for Humanity: Information Technology to Advance Society*. CRC Press, Boca Raton, FL, 2013.

[57] R. Frigg. Why typicality does not explain the approach to equilibrium. In M. Suárez, editor, *Probabilities, Causes and Propensities in Physics*. Springer, 2011.

[58] T. Fritz. Nonlocality with less complementarity. *Physical Review A*, 85:022102, 2012.

[59] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter. High speed optical quantum random number generation. *Optics Express*, 18(12):13029–13037, 2010.

[60] P. Gács, M. Hoyrup, and C. Rojas. Randomness on computable probability spaces—a dynamical point of view. *Theory of Computing Systems*, 48:465–485, 2011.

[61] V. García-Morales. Universal map for cellular automata. *Physics Letters A*, 376:2645–2657, 2012.

[62] A. M. Gleason. Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)*, 6(6):885–893, 1957.

[63] E. M. Gold. Limiting recursion. *The Journal of Symbolic Logic*, 30(1):28–48, 1965.

[64] J. A. González, L. I. Reyes, and L. E. Guerrero. Exact solutions to chaotic and stochastic systems. *Chaos*, 11(1):1–15, 2001.

[65] R. Graham and J. H. Spencer. Ramsey theory. *Scientific American*, 262:112–117, Sept. 1990.

[66] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem with inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990.

[67] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Multiparticle interferometry and the superposition principle. *Physics Today*, 46(8):22, 1993.

[68] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An. A random number generator based on quantum entangled photon pairs. *Chinese Physics Letters*, 21(10):1961–1964, 2004.

[69] A. Hájek. Interpretations of probability. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Winter 2012 edition, 2014.

[70] P. R. Halmos. *Finite-dimensional Vector Spaces*. Springer, New York Heidelberg Berlin, 1974.

[71] P. R. Halmos. *Measure Theory*. Springer-Verlag, New York, 1974.

[72] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, 43(3):172–198, 1927. English translation in Ref. [147, pp. 62–84].

[73] C. Held. The Kochen-Specker Theorem. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Winter 2014 edition, 2014.

[74] G. Hellman. Randomness and reality. In P. D. Asquith and I. Hacking, editors, *Philosophy of Science Association Proceedings*, volume 2, pages 79–97. East Lansing, MI, 1978.

[75] E. Hrushovski and I. Pitowsky. Generalizations of Kochen and Specker's theorem and the effectiveness of Gleason's theorem. *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, 35(2):177–194, 2004.

[76] ID Quantique. Random number generation using quantum physics, Version 3.0. *ID Quantique White Paper*, April 2010. `http://www.idquantique.com/wordpress/wp-content/uploads/Quantum-RNG-White-Paper.pdf`.

[77] N. Israeli and N. Goldenfeld. Computational irreducibility and the predictability of complex physical systems. *Physical Review Letters*, 92(074105), 2004.

[78] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71:1675–1680, 2000.

[79] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos. State-independent experimental test of quantum contextuality. *Nature*, 460(7254):494–497, July 2009.

[80] S. B. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)*, 17(1):59–87, 1967.

[81] J. Kofler and A. Zeilinger. Quantum information and randomness. *European Review*, 18(4):469–480, 2010.

[82] P. S. Laplace. *A Philosophical Essay on Probabilities*. John Wiley & Sons, New York, 1902.

[83] J.-A. Larsson. A Kochen-Specker inequality. *Europhysics Letters*, 58(6):799, 2002.

[84] G. Longo and M. Montévil. Models vs. simulations: a comparison by their theoretical symmetries. In L. Magnani and T. Berlotti, editors, *Springer Handbook of Model-Based Science*. Springer, Dordrecht, 2016.

[85] G. Longo and T. Paul. The mathematics of computing between logic and physics. In S. B. Cooper and A. Sorbi, editors, *Computability in Context: Computation and Logic in the Real World*, chapter 7, pages 243–274. Imperial College Press/World Scientific, London, 2008.

[86] E. N. Lorenz. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20(2):130–141, 1963.

[87] M. Margenstern, editor. *Algorithmic Randomness, Quantum Physics and Incompleteness*. Springer, Berlin, 2005.

[88] M. Martelli, M. Dang, and T. Seph. Defining chaos. *Mathematics Magazine*, 71(2):112–122, 1998.

[89] P. Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, 1966.

[90] B. D. McKay, N. D. Megill, and M. Pavičić. Algorithms for Greechie diagrams. *International Journal of Theoretical Physics*, 39(10):2381–2406, 2000.

[91] D. N. Mermin. Hidden variables and the two theorems of John Bell. *Reviews of Modern Physics*, 65:803–815, 1993.

[92] N. D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(72):3373–3376, 1990.

[93] D. A. Meyer. Finite precision measurement nullifies the Kochen-Specker Theorem. *Physical Review Letters*, 83(19):3751, 1999.

[94] M. Mugur-Schächter. *Etude du caractère complet de la mécanique quantique*. Gauthier-Villars, Paris, 1964.

[95] F. D. Murnaghan. *The Unitary and Rotation Groups*. Spartan Books, Washington, D.C., 1962.

[96] W. C. Myrvold. Statistical mechanics and thermodynamics: A Maxwellian view. *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, 42(4):237–243, 2011.

[97] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ, 1955.

[98] T. Paul. Semiclassical analysis and sensitivity to initial conditions. *Information and Computation*, 207(5):660–669, 2009.

[99] W. Pauli. Die allgemeinen Prinzipien der Wellenmechanik. In H. Geiger and K. Scheel, editors, *Handbuch der Physik*, volume 24, page 126, Springer, Berlin, 1933. English translation in [100, pp. 771–938].

[100] W. Pauli. *Collected Scientific Papers*, volume I. Interscience, New York, 1964.

[101] M. Pavičić, J.-P. Merlet, and N. D. Megill. Exhaustive enumeration of Kochen-Specker vector systems. *INRIA Rapport de recherche, No. 5388*, 2004.

[102] M. Pavičić, J.-P. Merlet, B. McKay, and N. D. Megill. Kochen-Specker vectors. *Journal of Physics A: Mathematical and General*, 38:1577–1592, 2005.

[103] A. Peres. Two simple proofs of the Kochen-Specker Theorem. *Journal of Physics A: Mathematical and General*, 24:L175–L178, 1991.

[104] PicoQuant. Quantum random number generator 'PQRNG 150'. `http://www.picoquant.com/products/pqrng150/pqrng150.htm`.

[105] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmchenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's Theorem. *Nature*, 464(09008), 2010.

[106] I. Pitowsky. Infinite and finite Gleason's theorems and the logic of indeterminacy. *Journal of Mathematical Physics*, 39(1):218–228, 1998.

[107] H. Poincaré. *Science et Méthode*. Flammarion, Paris, 1908.

[108] K. R. Popper. Indeterminism in quantum physics and in classical physics. Part I. *The British Journal for the Philosophy of Science*, 1(2):117–133, 1950.

[109] K. R. Popper. *The Logic of Scientific Discovery*. Basic Books, New York, 1959.

[110] K. R. Popper. *Quantum Theory and the Schism in Physics*, volume III of *Postscript to The Logic of Scientific Discovery*. Routledge, London and New York, 1992.

[111] M. F. Pusey, J. Barrett, and T. Rudolph. On the reality of the quantum state. *Nature Physics*, 8:475–478, 2012.

[112] qutools. quRNG – Quantum Random Number Generator. `http://www.qutools.com/products/quRNG/index.php`.

[113] J. G. Rarity, M. P. C. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41:2435–2444, 1994.

[114] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58–61, 1994.

[115] H. P. Robertson. The uncertainty principle. *Physical Review*, 34:163–164, 1929.

[116] L. A. Rozema, A. Darabi, D. H. Mahler, A. Hayat, Y. Soudagar, and A. M. Steinberg. Violation of Heisenberg's measurement-disturbance relationship by weak measurements. *Physical Review Letters*, 109:100404, 2012.

[117] D. Ruelle. *Hasard et Chaos*. Editions Odile Jacob, Paris, 1991.

[118] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, Reading, MA, revised edition, 1994.

[119] H. Schmidt. Quantum-mechanical random-number generator. *Journal of Applied Physics*, 41(2):462–468, 1970.

[120] Y. Shen, L. Tian, and H. Zou. Practical quantum random nubmer generator based on measuring the shot noise of vacuum states. *Physical Review A*, 81(063814), 2010.

[121] A. Shimony. Contextual hidden variables theories and Bell's inequalities. *The British Journal for the Philosophy of Science*, 35(1):25–45, 1984.

[122] M. Sipser. *Introduction to the Theory of Computation*. Cengage Learning, Boston, 2nd edition, 2005.

[123] L. Sklar. *Physics and Chance*. Cambridge University Press, Cambridge, 1993.

[124] R. W. Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Physical Review A*, 71:052108, 2005.

[125] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[126] M. Stipčević and B. M. Rogina. Quantum random number generator based on photonic emission in semiconductors. *Review of Scientific Instruments*, 78(4):045104, 2007.

[127] T. Stojanovski and L. Kocarev. Chaos-based random number generators—Part I: Analysis. *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, 48(3):281–288, 2001.

[128] M. Suárez. Quantum selections, propensities and the problem of measurement. *The British Journal for the Philosophy of Science*, 55(2):219–255, 2004.

[129] K. Svozil. The quantum coin toss — testing microphysical undecidability. *Physics Letters A*, 143(9):433–437, 1990.

[130] K. Svozil. *Quantum Logic*. Springer, Singapore, 1998.

[131] K. Svozil. Logical equivalence between generalized urn models and finite automata. *International Journal of Theoretical Physics*, 44:745–754, 2005.

[132] K. Svozil. How much contextuality? *Natural Computing*, 11(2):261–265, 2012.

[133] E. Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arithmetica*, 27:199–245, 1975.

[134] K. Tadaki. Phase transition and strong predictability. In O. H. Ibarra, L. Kari, and S. Kopecki, editors, *Unconventional Computation and Natural Computation*, volume 8553 of *Lecture Notes in Computer Science*, pages 340–352. Springer, 2014.

[135] J. Tkadlec. Diagrams of Kochen-Specker type constructions. *International Journal of Theoretical Physics*, 39(3):921–926, 2000.

[136] T. Toffoli. The role of the observer in uniform systems. In G. J. Klir, editor, *Applied General Systems Research, Recent Developments and Trends*, pages 395–400. Plenum Press, New York, London, 1978.

[137] A. M. Turing. Computing machinery and intelligence. *Mind*, 59(236):433–460, 1950.

[138] J. Uffink. Subjective probability and statistical physics. In C. Beisbart and S. Hartmann, editors, *Probabilities in Physics*, 2011.

[139] M. Um, X. Zhang, J. Zhang, Y. Wang, S. Yangchao, D.-L. Deng, L.-M. Duan, and K. Kim. Experimental certification of random numbers via quantum contextuality. *Scientific Reports*, 3:1627, 2013.

[140] S. P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7(1–3):1–336, 2011.

[141] V. C. Vivoli, P. Sekatski, J.-D. Bancal, C. C. W. Lim, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard. Comparing different approaches for generating random numbers device-independently using a photon pair source. *New Journal of Physics*, 17:023023, 2015.

[142] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 98(171105), 2011.

[143] P. X. Wang, G. L. Long, and Y. S. Li. Scheme for a quantum random number generator. *Journal of Applied Physics*, 100(5):056107, 2006.

[144] M. A. Wayne, E. R. Jeffrey, G. M. Aksolrod, and P. G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.

[145] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, 81(23):5039–5043, 1998.

[146] C. Werndl. What are the new implications of chaos for unpredictability? *British Journal for the Philosophy of Science*, 60(1):195–220, 2009.

[147] J. A. Wheeler and W. H. Zurek, editors. *Quantum Theory and Measurement*. Princeton University Press, Princeton, NJ, 1983.

[148] J. A. Winnie. Computable chaos. *Philosophy of Science*, 59(2):263–275, 1992.

[149] S. Wolfram. Universality and complexity in cellular automata. *Physica D*, 10:1–35, 1984.

[150] S. Wolfram. Undecidability and intractability in theoretical physics. *Physical Review Letters*, 54(8):735–738, 1985.

[151] S. Wolfram. *A New Kind of Science*. Wolfram Media, Inc., Champaign, IL, 2002.

[152] Wolfram Research, Inc. *Mathematica 9.0.1.0*. Wolfram Research, Inc., Champaign, IL, 2012.

[153] D. H. Wolpert. Physical limits of inference. *Physica D*, 237:1257–1281, 2008.

[154] D. Woods and T. Neary. The complexity of small universal Turing machine: A survey. *Theoretical Computer Science*, 410(4–5):443–450, 2009.

[155] R. Wright. Generalized urn models. *Foundations of Physics*, 20(7):881–903, 1990.

[156] C. Wuthrich. Can the world be shown to be indeterministic after all? In C. Beisbart and S. Hartmann, editors, *Probabilities in Physics*. Oxford University Press, Oxford, 2011.

[157] S. Yu and C. H. Oh. State-independent proof of Kochen-Specker theorem with 13 rays. *Physical Review Letters*, 108:030402, 2012.

[158] X.-D. Yu and D. M. Tong. Coexistence of Kochen-Specker inequalities and non-contextuality inequalities. *Physical Review A*, 89:010101, 2014.

[159] A. Zaman. On the impossibility of events of zero probability. *Theory and Decision*, 23:157–159, 1987.

[160] A. Zeilinger. General properties of lossless beam splitters in interferometry. *American Journal of Physics*, 49(9):882–883, 1981.

[161] A. Zeilinger. A foundational principle for quantum mechanics. *Foundations of Physics*, 29(4):631–643, 1999.

[162] A. Zeilinger. The message of the quantum. *Nature*, 438:743, 2005.

[163] C. Zu, Y. X. Wang, D. L. Deng, X. Y. Chang, K. Liu, P. Y. Hou, H. X. Yang, and L. M. Duan. State-independent experimental test of quantum contextuality in an indivisible system. *Physical Review Letters*, 109:150401, 2012.

[164] M. Zukowski, A. Zeilinger, and M. A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Physical Review A*, 55:2564–2579, 1997.

[165] H. Zwirn. Computational irreducibility and computational analogy. *arXiv:1304.5247v3*, 2013.

[166] H. Zwirn and J.-P. Delahaye. Unpredictability and computational irreducibility. In H. Zenil, editor, *Irreducibility and Computation Equivalence*. Springer, Berlin Heidelberg, 2013.

Abstract

The outcomes of quantum measurements are generally considered to be random, but despite the fact that this randomness is an important element in quantum information theory, its nature is not well understood. In this thesis, we study several issues relating to the origin and certification of quantum randomness and unpredictability.

One of the key results in forming our understanding of quantum mechanics as an intrinsically indeterministic theory is the Kochen-Specker theorem, which shows the impossibility to consistently assign simultaneous noncontextual definite values to all quantum mechanical observables prior to measurement. However, the theorem, under the assumption that any definite values must be noncontextual, only strictly shows that some observables must be value indefinite. We strengthen this result, proving a stronger variant of the Kochen-Specker theorem showing that, under the same assumption, if a system is prepared in an arbitrary state $|\psi\rangle$, then every observable A is value indefinite unless $|\psi\rangle$ is an eigenstate of A.

The indeterministic nature of quantum measurements does little to explain how the quality of quantum randomness differs from classical randomness. We show that, subject to certain physical assumptions, a sequence of bits generated by the measurement of value indefinite observables is guaranteed, in the infinite limit, to be strongly incomputable. We further discuss how this can be used to build a quantum random number generator certified by value indefiniteness.

Next, we study the notion of unpredictability, which is central to the concept of (quantum) randomness. In doing so, we propose a formal model of prediction that can be used to asses the predictability of arbitrary physical experiments. We investigate how the quantum features of value indefiniteness and complementarity can be used to certify different levels of unpredictability, and show that the outcome of a single measurement of a value indefinite quantum observable is formally unpredictable. Finally, we study the relation between this notion of unpredictability and the computability-theoretic certification of quantum randomness.

Keywords: Quantum foundations, quantum randomness, quantum indeterminism, unpredictability, value indefiniteness, quantum measurement

Résumé

Les résultats de mesures quantiques sont généralement considérés comme aléatoires, mais leur nature aléatoire, malgré son importance dans la théorie de l'information quantique, est mal comprise. Dans cette thèse, nous étudions plusieurs problèmes liés à l'origine et la certification de l'aléatoire et l'imprévisibilité quantique.

L'un des résultats clés dans la formation de notre compréhension de la mécanique quantique comme théorie intrinsèquement indéterministe est le théorème de Kochen et Specker, qui démontre l'impossibilité d'attribuer simultanément, de façon cohérente, des valeurs définies et non-contextuelles à chaque observable avant la mesure. Cependant, si nous présumons qu'une observable à valeur définie doit être non-contextuelle, alors le théorème ne montre que le fait qu'il existe au moins une observable à valeur indéfinie. Nous renforçons ce résultat en démontrant une variante du théorème de Kochen et Specker qui montre que si un système est préparé dans un état quelconque $|\psi\rangle$, alors chaque observable A est à valeur indéfinie sauf si $|\psi\rangle$ est un état propre de A.

La nature indéterministe de la mesure quantique n'explique pas bien la différence de qualité entre l'aléatoire quantique et classique. Soumise à certaines hypothèses physiques, nous montrons qu'une suite de bits produite par la mesure des observables à valeurs indéfinies est garantie, dans la limite infinie, d'être fortement incalculable. De plus, nous discutons comment utiliser ces résultats afin de construire un générateur quantique de nombres aléatoires qui est certifié par des observables à valeurs indéfinies.

Dans la dernière partie de cette thèse, nous étudions la notion d'imprévisibilité, qui est au cœur du concept d'aléatoire (quantique). Ce faisant, nous proposons un modèle formel de (im)prévisibilité qui peut servir à évaluer la prévisibilité d'expériences physiques arbitraires. Ce modèle est appliqué aux mesures quantiques afin de comprendre comment la valeur indéfinie et la complémentarité quantique peuvent être utilisées pour certifier différents degrés d'imprévisibilité, et nous démontrons ainsi que le résultat d'une seule mesure d'une observable à valeur indéfinie est formellement imprévisible. Enfin, nous étudions la relation entre cette notion d'imprévisibilité et la certification de l'incalculabilité des suites aléatoires quantiques.

Mots-clés : Fondements de la mécanique quantique, aléatoire quantique, indéterminisme quantique, imprévisibilité, la valeur indéfinie, mesure quantique