Categorical Quantum Dynamics

Stefano Gogioso

Trinity College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2016

Per Aspera Ad Astra

Contents

Chapter 1

Introduction

1.1 Summary of this work

Since their original introduction, strongly complementary observables have been a fundamental ingredient of the ZX calculus, one of the most successful fragments of Categorical Quantum Mechanics (CQM). In this thesis, we show that strong complementarity plays a vastly greater role in quantum theory.

Firstly, we use strong complementarity to introduce dynamics and symmetries within the framework of CQM, which we also extend to infinite-dimensional separable Hilbert spaces: these were long-missing features, which open the way to a wealth of new applications. The coherent treatment presented in this work also provides a variety of novel insights into the dynamics and symmetries of quantum systems: examples include the extremely simple characterisation of symmetry-observable duality, the connection of strong complementarity with the Weyl Canonical Commutation Relations, the generalisations of Feynman's clock construction, the existence of time observables and the emergence of quantum clocks.

Secondly, we show that strong complementarity is a key resource for quantum algorithms and protocols. We provide the first fully diagrammatic, theory-independent proof of correctness for the quantum algorithm solving the Hidden Subgroup Problem, and show that strong complementarity is the feature providing the quantum advantage. In quantum foundations, we use strong complementarity to derive the exact conditions relating non-locality to the structure of phase groups, within the context of Mermin-type non-locality arguments. Our non-locality results find further application to quantum cryptography, where we use them to define a quantum-classical secret sharing scheme with provable device-independent security guarantees.

All in all, we argue that strong complementarity is a truly powerful and versatile building block for quantum theory and its applications, and one that should draw a lot more attention in the future.

1.2 Background literature

1.2.1 Categorical Quantum Mechanics

This work takes its roots in the framework of **categorical quantum mechanics** (CQM) [AC09, CK15], which its extends and refines in a number of aspects. The general motivation behind the application of category-theoretic tools lies in the intuition that the features distinguishing quantum theory from classical physics can be understood in terms of the way quantum processes compose, sequentially and in parallel (we refer to this as an **operational**, or **process-theoretic**, description of quantum theory). The framework of symmetric monoidal categories is particularly suited for operational descriptions, and comes with a natural diagrammatic formalism [JS91, BS10, CK15, Kis12, Sel07, CH12], combining the rigour of the category theory with the versatility of graphical manipulation. The diagrammatic formalism has quickly become a major selling point of CQM, and receives plenty of interest on its own [CD11, Bac14, Had15, Kis12, KZ15].

The operational and process-theoretic description of quantum theory given by CQM [AH12b, CK15] is in a certain sense antipodal to the traditional Hilbert space formulation, which heavily relies on explicit complex-linear structure. Several intermediate approaches exist, such as quantum circuits and generalised probabilistic theories [Har01, Bar07], and have been applied to a diversity of topics in quantum information and foundations. The framework of **operational probabilistic theories** (OPTs) is perhaps the closest, in spirit, to CQM: it was developed in [CDP10, CDP11, CS15] with the aim of obtaining an informational derivation of quantum theory, it comes with a graphical calculus and it has a strong operational and process-theoretic flavour to it; work to connect OPTs to CQM is currently being undertaken [Tul16, GS16]. Despite the diagrammatic and operational similarities, the approach to quantum theory of OPTs is quite different from that of CQM: the former relies on explicit probabilistic structure, and is mainly axiomatic in nature, while the latter focuses on categorical structures (with no explicit summations or probabilities), and is mostly constructive. The processes which OPTs are concerned with are physical processes[1], or processes appearing in their convex decompositions[2]. On the contrary, CQM is concerned with the study of arbitrary processes with interesting categorical properties, which are used as building blocks of physical processes. In a nutshell, OPTs take physical processes and impose axioms on the way they can be probabilistically decomposed, while CQM

[1] Such as quantum channels, aka completely positive trace-preserving maps.

[2] Such as sub-normalised pure states, appearing in the convex decomposition of density matrices.

studies how certain building blocks compose and interact to form larger processes of physical interest.

1.2.2 Dagger compact structure

The categorical environment of choice for pure-state quantum theory in CQM is that of dagger compact symmetric monoidal categories: the dagger structure is the categorical abstraction of operator adjunction[3] in the Hilbert space formalism, while the compact structure corresponds to operator-state duality. Within this environment, the most common building blocks used by CQM are certainly †-Frobenius algebras, which provide the coherent/pure versions of the classical operations of copy, delete and match, and are a key component in the treatment of classicality [CP07, CPP10]. Special commutative †-Frobenius algebras correspond to orthonormal bases [CPV13], or equivalently to non-degenerate observables in the Hilbert space formalism.

The †-compact structure can furthermore be used to provide a categorical environment for the operational treatment of mixed-state quantum theory: the CPM construction [Sel07, CP10] represents quantum channels as a diagrammatic version of their Kraus decomposition in the Hilbert space formalism[4], and a partial trace naturally arises. In the CPM formalism, †-Frobenius algebras can be used to define decoherence maps for all orthonormal bases, and the ensuing mixed quantum-classical formalism can be given categorical dignity via the CP* construction [CHK14, CH15], which connects the operational picture to the study of C*-algebras and algebraic quantum theory.

1.2.3 Some application of CQM

Throughout the years, the categorical and diagrammatic formalisms have yielded many novel characterisations of quantum structures, with applications to quantum foundations, information and computation. In quantum foundations, the CQM framework has been applied to study features of causality [CPV13, CK15, Coe16] and non-locality [CDKW12, Gog15a], both operationally and in connection with the sheaf-theoretic framework for contextuality of [AB14, AMB12, ABK$^+$15] (which is also applicable to OPTs [CY16]). In quantum information and computation, the framework has been applied to the study of quantum algorithms and protocols

[3] And of bra/ket duality as a special case.

[4] A similarity which becomes even more apparent in the more general CP construction [CH12].

[CD11, Vic12b, ZV14, Vic12a, VV16, CK17, Zam12], measurement-based and cluster-state quantum computing [Dun15, Hor11], complementarity [MV15, DD16, ZV14], and the information theoretic characterisation of quantum theory [HK16]. Relational models for non-deterministic classical computation have also been explored using tools from CQM, both as toy models for quantum theory [Pav09, Abr13, Gog15c, Mar, Coe16, CE12, BD15] and in their own right as models of computation [Pav09, BV14].

1.2.4 The ZX calculus

One of the most successful and intriguing fragments of CQM is the **ZX calculus**. First introduced in [CD11], the ZX calculus is a diagrammatic graphical calculus for multi-qubit systems, designed to reason formally about quantum algorithms and protocols, as well as to derive rigorous results on quantum foundations and information. Its simple but rigorous presentation makes the ZX calculus ideal for diagrammatic reasoning and automated proof-checking [Kis12, KZ15]. The ZX calculus has been shown to be *universal* and *sound* for pure qubit quantum mechanics [CD11], as well as *complete* for pure qubit *stabiliser* quantum mechanics [Bac14, BD15]. However, the ZX calculus is known to be incomplete for pure qubit quantum mechanics [dWZ14].

Since its introduction, the ZX calculus has found plenty of applications in quantum information: it was used to describe the fundamental gates of quantum circuits [CD11, Dun15], to formalise a number of quantum protocols [CD11, Zam12, CK17], to describe the logical structure of information flow in topological cluster-state quantum computing [Hor11], and to provide a categorical model of Spekkens's toy theory [CE12, BD15].

1.2.5 Applications of strong complementarity

In several applications of the ZX calculus, key steps are performed by a specific set of rules relating the Z and X observables, namely the **bialgebra law** and **coherence laws**. It is possible to show that classical structures satisfying these rules also satisfy the Hopf law [DD16, Kis12], and that the associated observables are **complementary** (or **mutually unbiased**): as a consequence, the property defined by the the bialgebra and coherence laws is often referred to as **strong complementarity**.

Complementarity plays an important role in the correctness and security of certain quantum protocols, but its classification in arbitrary dimensions has proven to be remarkably tricky; strongly complementary pairs of non-degenerate observables on finite-dimensional Hilbert spaces, on the other hand, are completely classified by finite abelian groups [Kis12], and hence much easier to work with.

A number of applications of CQM rely on strong complementarity as their active ingredient: most relevant are its appearance as an abstract version of the quantum Fourier transform in group-theoretic quantum algorithms [Vic12b, ZV14, Zen15, GZ15a], and the role it plays in connecting Mermin-type non-locality scenarios to the structure of phase groups in abstract process theories [CDKW12, CES10, GZ15b].

1.3 Brief synopsis of this work

1.3.1 A primer of CQM

In Chapter 2, we provide a primer of the framework of Categorical Quantum Mechanics. We begin by introducing symmetric monoidal categories as a general model for process theories, and we characterise dagger compact structure in relation to inner products and operator-state duality, thus capturing what we believe to be the essential operational and structural features of pure-state quantum theory.

In order to model mixed-state behaviour, we proceed to present environment structure and the CPM construction. We introduce †-Frobenius algebras in relation to observables, classicality and the coherent manipulation of data[5], and we use them to construct measurements, preparations and decoherence maps in the context of the CP* construction. Finally, we provide a recap of the sheaf-theoretic framework for non-locality and contextuality, and connect it to our portrayal of process theories.

1.3.2 Coherent dynamics and symmetries

In Chapter 3 we use strong complementarity to introduce symmetries and dynamics within the framework of CQM. Our approach relies on a coherent treatment of group theory and representation theory, similar in spirit to the way in which †-Frobenius algebras provide a coherent treatment of classical data manipulation.

We define a new notion of "coherent group", based on strongly complementary pairs of quasi-special †-Frobenius algebras and modelling an abstract coherent counterpart of classical groups. By analogy with the relatable case of finite periodic lattices, we prove general results about symmetry-observable duality, the Weyl canonical commutation relations and a weak form of the uncertainty principle, and we establish that coherent groups show the same fundamental structural and operational features that would be expected of position/momentum pairs.

We consider representations of coherent groups as a model of coherent symmetric systems, in analogy with the traditional identification of classical symmetric systems with classical group representations, and we characterise them as the Eilenberg-Moore

[5] When talking about "coherent data", or the "coherent encoding/manipulation" of classical data, we will be talking about classical data which has been encoded into quantum systems via orthonormal bases, and is manipulated using $\mathbb{C}$-linear extensions of classical deterministic functions. We will argue in Chapter 2 that coherent data plays a huge role in quantum computing and in the foundations of quantum theory: it is used to construct oracles, entangled states, as well as many other building blocks used in the design of quantum protocols. Coherent data enjoys all those features of $\mathbb{C}$-linearity which coalesce to provide quantum advantage and non-classical behaviour, while at the same time allowing for a good deal of classical intuition to play a positive role in designing quantum algorithms.

algebras of a certain monad, with equivariant maps arising as the Eilenberg-Moore morphisms between them.

We present a new framework for the treatment of infinite-dimensional separable Hilbert spaces in CQM, and explicitly construct a coherent group corresponding to the position/momentum pair for the textbook case of wavefunctions on a 1-dimensional continuous space with periodic boundary conditions (i.e. with translation group isomorphic to the circle group S^1).

Finally, we apply all the techniques developed in the remainder of the Chapter to the study of quantum dynamics, with an explicit treatment of continuous periodic, discrete and discrete periodic dynamics of finite-dimensional and separable quantum systems. We talk about quantum dynamics, Hamiltonians and Schrödinger's Equation. We use the symmetry/observable duality properties of our coherent framework to provide simple diagrammatic proofs of Stone's Theorem on 1-parameter unitary groups and von Neumann's Mean Ergodic Theorem, and we give an abstract proof of correctness for the the Feynman clock construction. We conclude the Section by turning our attention to the description of synchronised dynamical systems, the existence of time observables, and the emergence of quantum clocks.

1.3.3 Strong complementarity in quantum algorithms

In Chapter 4 we move away from quantum foundations, and we present two applications of strong complementarity to quantum algorithms.

Firstly, we put to work the connection between strong complementarity and the quantum Fourier transform in a fully diagrammatic, theory-independent proof of correctness for the quantum subroutine of the algorithm solving the Hidden Subgroup Problem (HSP). In doing so, we definitively prove that strong complementarity is the structural feature providing the quantum advantage in the HSP. As an immediate application of our theory-independent approach, we conclude that Simon's problem can be efficiently solved in real quantum theory.

Secondly, we investigate the relationship between strong complementarity and phase groups, and we formulate a broad generalisation of Mermin's non-locality argument for GHZ states. Our results provide an exact characterisation of the relationship between phase groups and non-locality, bringing the research programme of [CDKW12, CES10] to a close. We relate our findings to the framework of All-vs-Nothing arguments, and we put them to work in the definition of a device-independent quantum-classical secret sharing scheme, extending the classical scheme of Hillery, Bužek and Berthiaume [HBB99].

Chapter 2

Categorical Quantum Mechanics

2.1 Symmetric monoidal categories

2.1.1 Objects as physical systems

Categorical quantum mechanics is first and foremost a theory of systems and processes, composing sequentially and in parallel. **Symmetric monoidal categories** (henceforth SMCs) provide a very general framework to model such systems and processes, and come with a natural graphical/diagrammatic language [JS91, JSV96]; because of this, they are often referred to as **process theories** in the literature.

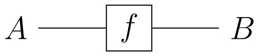
The objects of the SMC are taken to correspond to physical systems, and are diagrammatically denoted by wires:

$$A \;\text{———}\; A \tag{2.1}$$

The identity id_A on an object/system A is associated to the process of "doing nothing" to the system, and is also denoted by the same undecorated wire which represents the system in Diagram 2.1. This free confusion between objects and identity morphisms is fairly common in category theory, and has an interesting physical interpretation: possession of a static system is the same thing as the process of continuing to do nothing with it.

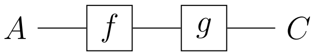
2.1.2 Sequential composition of processes

The morphisms of the SMC are taken to correspond to processes connecting physical systems: a morphism $A \to B$ embodies a process taking a state in system A as its input and returning a state in system B as its output. The **sequential composition** of processes (with compatible intermediate systems) is embodied by composition of morphisms in the category, and assumed to be associative. Diagrammatically, a morphism/process $f : A \to B$ is denoted by a labelled box:



(2.2)

Composition $g \circ f : A \to C$ of two morphisms $f : A \to B$ and $g : B \to C$ is denoted by composition of boxes along the intermediate wire:

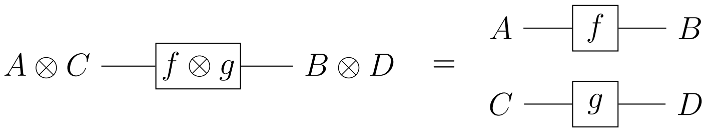


(2.3)

Composition of multiple processes is obtained by repeated pairwise composition. Also, the labels for systems (input, output or intermediate) might be omitted when clear from context and/or when not relevant.

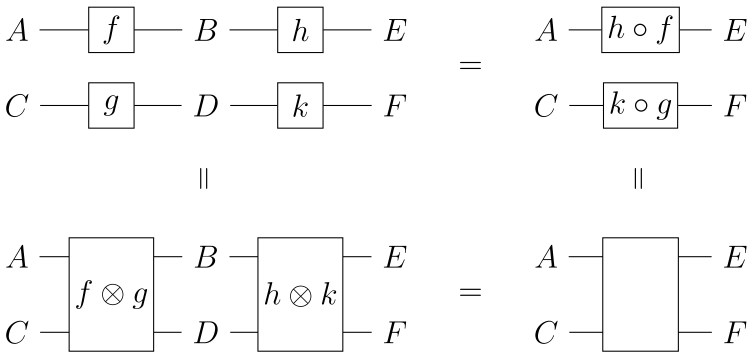
2.1.3 Parallel composition of processes

The description of parallel composition of processes also requires the description of parallel composition of systems: given two processes $f : A \to B$ and $g : C \to D$, their **parallel composition**, denoted $f \otimes g$, transforms the joint system formed by A and C, denoted $A \otimes C$, into the joint system formed by B and D, denoted $B \otimes D$. A minimal notion of parallel composition and joint systems is captured by *monoidal categories*, and $\otimes$ is called the **tensor product**. Diagrammatically, a joint system $A \otimes C$ is denoted by parallel wires for A and C, and parallel composition of processes is denoted by parallel boxes:



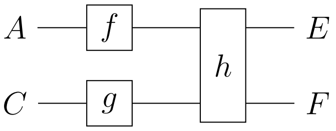
(2.4)

For a monoidal category $\mathcal{C}$, the tensor product is a functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, and hence parallel composition and sequential composition distribute over each other:



(2.5)

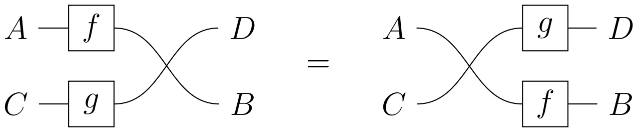
While the diagrammatic formalism for categories was 1-dimensional, with processes represented by a line of wires and boxes, the diagrammatic formalism for monoidal categories is 2-dimensional, with processes represented by parallel wires and boxes on them. Boxes need not be confined to single wires, but can connect multiple wires together: there could be processes $h : B \otimes D \to E \otimes F$ which cannot be obtained as parallel composition of processes $B \to D$ and $E \to F$, and which need to be represented by boxes spanning multiple wires.



(2.6)

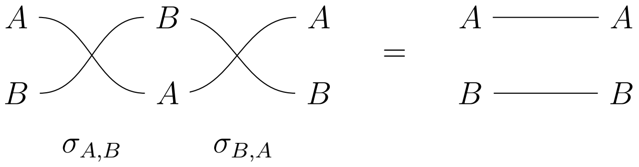
Morphisms which arise from parallel composition are said to be **separable**, and may (but need not) be represented by parallel boxes on parallel wires, as done in Equation 2.4. Conversely, processes represented by parallel boxes on parallel wires are necessarily separable.

Adequately capturing the notion of joint system turns out to be slightly problematic: the axioms of monoidal categories do not guarantee that $A \otimes B$ and $B \otimes A$ will be the same system, or even isomorphic: the linear order which systems are parallely composed in is relevant. To obviate this problem, one might introduce a natural isomorphism $\sigma_{A,B}$, called the **symmetry isomorphism**, which swaps A and B, so that $A \otimes B$ and $B \otimes A$ are effectively the same system, and the linear order becomes irrelevant; this leads to the definition of *symmetric monoidal categories*. In the graphical presentation, the symmetry isomorphism $\sigma_{A,B}$ is represented as a crossing of the wires and the naturality condition guarantees that processes can be made to "slide" through the wire crossing:



(2.7)

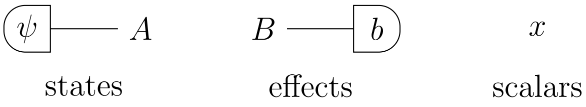
The symmetry isomorphism comes with the additional requirement that $\sigma_{B,A} = \sigma_{A,B}^{-1}$:



(2.8)

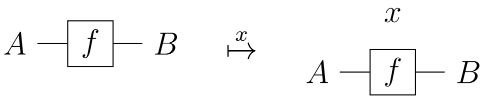
2.1.4 States, effects and scalars

The tensor product is associative, and comes with a **tensor unit** I: categorically, this means that there are natural isomorphisms $\alpha_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ (the **associator**), $\rho_A : A \otimes I \to A$ (the **right unitor**), and $\lambda_A : I \otimes A \to A$ (the **left unitor**). The tensor unit models the trivial system, and processes from/to the tensor unit have a special status. Processes $I \to A$ are called the **states** of A and processes $A \to I$ are called the **effects** of A. Processes $I \to I$ are called the **scalars** of the SMC, and they form a commutative monoid under composition[1], with the identity id_I as its unit. Diagrammatically, the wire for the tensor unit is almost always omitted[2]. Hence, states are processes with no input wires, effects are processes with no output wires, and scalars are processes with no wires attached at all:



(2.9)

For any systems A and B, the processes $A \to B$ come with a canonical monoid action of the scalars on them, given by the tensor product:



(2.10)

Diagrammatically, the scalar 1 (our alternative notation for id_I from now on) is a special case: being the identity of the trivial system and acting as the identity on processes, it is usually not represented at all, or equivalently it is represented by an empty diagram.

States, effects and scalars provide a point of connection between SMCs and set-theoretic formulations. A process $f : A \to B$ in a SMC can be seen in three different ways as a set function: (i) mapping states $\psi : I \to A$ of A to states $f \circ \psi : I \to B$ of B; (ii) mapping effects $b : B \to I$ of B to effects $b \circ f : A \to I$ of A; (iii) mapping pairs (ψ, b) of a state on A and an effect on B to scalars $b \circ f \circ \psi$. We say that a SMC has **enough states** if any two processes $f, g : A \to B$ are equal whenever they are equal as functions on the states of A . Dually, we say that a SMC has **enough effects** if any two processes $f, g : A \to B$ are equal whenever they are equal as functions on the effects of B. We say that a SMC has **enough states and effects** if any two

[1] Both sequential and parallel: for scalars $x, y : I \to I$, sequential composition $(y \circ x)$ coincides with parallel composition followed by a unitor ($\lambda_I(x \otimes y)$ and/or $\rho_I(x \otimes y)$).

[2] One can always use unitors and their inverses to insert/remove tensor units as needed to correctly match input/output systems for processes in the diagrams. In this work, unitors and associators are always omitted, as their application is obvious from context.

processes $f, g : A \to B$ are equal whenever they are equal as functions mapping pairs of a state A and an effect of B to scalars.

2.1.5 Examples of symmetric monoidal categories

The category of sets. The category Set having sets as objects and functions as morphisms is symmetric monoidal, with function composition as sequential composition of processes. The tensor product on objects is given by the Cartesian product $A \times B$ of sets, with the singleton set $\mathbb{1}$ as tensor unit, while the parallel composition of morphisms is given by product of functions $f \times g := \big(a, b\big) \mapsto \big(f(a), g(b)\big)$. States of an object A in Set are exactly the elements of set A. Because $\mathbb{1}$ is terminal, there is a unique effect $A \to \mathbb{1}$ for each A, and hence a unique scalar $id_{\mathbb{1}}$; hence Set has enough states, but not enough effects. Every category with finite products and terminal object similarly forms a symmetric monoidal category (but need not have enough states, e.g. the category of groups).

The category of Hilbert spaces. The category Hilb having Hilbert spaces as objects and bounded linear maps as morphisms is symmetric monoidal, with function composition as sequential composition of processes. The tensor product on objects is that of Hilbert spaces $\ell^2[A] \otimes \ell^2[B] \cong \ell^2[A \times B]$, with $\mathbb{C}$ as tensor unit. The tensor product on morphisms is the Kronecker product. The states of a Hilbert space $\ell^2[A]$ are exactly the vectors in $\ell^2[A]$, where vector $|\psi\rangle$ is seen as the map $\mathbb{C} \to \ell^2[A]$ sending $\xi \mapsto \xi|\psi\rangle$; the effects of a Hilbert space $\ell^2[A]$ are exactly the continuous linear functionals on it; the scalars are the complex numbers $\mathbb{C}$, with $\otimes$ as multiplication. The category Hilb has enough states and effects.

Categories of matrices over semirings. The category of finite-dimensional Hilbert spaces fHilb (a full subcategory of Hilb) presents no issues of continuity, and its construction can be straightforwardly extended from $\mathbb{C}$ to an arbitrary commutative semiring R. The category R-Mat of free, finite-dimensional semimodules over R has objects in the form R^X, where X is a finite set, and morphisms $R^X \to R^Y$ are the $Y \times X$ matrices with values in R. Sequential composition is matrix composition[3], and parallel composition is Kronecker product of matrices. The states of R^X are X-indexed, R-valued vectors; the effects of R^X are R-linear functionals $R^X \to R$; the scalars form the semiring R, with both $\circ$ and $\otimes$ coinciding with the semiring

[3] A semiring has the minimal requirements for matrix composition, namely an addition and a multiplication with appropriate distributivity.

multiplication. The category R-Mat always has enough states and effects. This is a large family of categories, which includes a number of examples of interest for CQM and related disciplines.

(i) The category fHilb of finite-dimensional Hilbert spaces[4], for $R = \mathbb{C}$. This is the traditional arena of pure-state quantum theory.

(ii) The category $\mathbb{R}$-Vect of finite-dimensional real vector spaces, for $R = \mathbb{R}$. This is the arena of pure-state real quantum theory.

(iii) The category fRel of finite sets and relations between them, for $R = \mathbb{B}$, the booleans. This is the arena of non-deterministic computation, and provides a toy model for pure-state quantum theory.

(iv) The category of finite-dimensional convex cones over simplices, for $R = \mathbb{R}^+$. This is the arena of classical probabilistic systems.

(v) The category of multi-sets and "multi-relations", for $R = \mathbb{N}$.

In computer science, semirings are often used to model resources in computation.

(vi) The *boolean semiring* $(\mathbb{B}, \vee, \wedge)$ is used to model non-deterministic computation (related to the complexity class NP).

(vii) The *probability semiring* $(\mathbb{R}^+, +, \times)$ is used to model probabilistic computation (related to the complexity classes BPP and PP).

(viii) The *natural numbers* $(\mathbb{N}, +, \times)$ is used to model counting problems (related to the complexity class #P).

(ix) The *tropical semirings* $(M, \min, +)$—where $(M, +, 0)$ is a totally ordered monoid with an absorbing maximal element ∞—is used in the Floyd-Warshall algorithm [Flo62] for shortest-path finding in directed graphs (and a number of other optimisation problems solvable within the framework of *tropical geometry* [Sim88, Pin98, Mik04, SS07]).

(x) The *Viterbi semiring* $([0,1], \max, \times)$ is used by the Viterbi algorithm [Vit62] to find the most likely sequence of hidden states in a Hidden Markov Model.

[4] The same as the category $\mathbb{C}$-Vect of finite-dimensional complex vector spaces.

(xi) Locales (related to intuitionistic logic) and commutative unital quantales (related to linear logic [Yet90] and generalised metrics for topological spaces [Kop88]) both find a number of applications in programming semantics and other areas of computer science [Abr87, AV93, FK97].

Because of these examples, the category R-Mat can be interpreted as modelling classical computation with resources encoded by a semiring R. However, the $R = \mathbb{R}^+, \mathbb{B}, \mathbb{R}$ cases also suggest an interpretation of R-Mat as modelling classical non-deterministic systems, with the semiring R encoding a notion of non-determinism: when using this interpretation, we will refer to R-Mat as the category of **classical R-probabilistic systems**. It should be noted that both the category fPFun of finite sets and partial functions (modelling partial deterministic classical computation) and the category fSet of sets and total functions (modelling deterministic classical computation) are subcategories of R-Mat for all choices of semiring R.

2.2 Dagger-compact categories

2.2.1 Dagger, isometries and unitaries

Some of the most iconic features of quantum theory, such as unitaries and the bra-ket notation, depend on a notion of inner product on states. Because composition of states and effects already produces scalars, a categorical way to introduce an inner product in a SMC is to guarantee state-effect duality, in a way compatible with parallel and sequential composition of processes. This approach leads to **dagger symmetric monoidal categories** (henceforth †-SMC) [Sel07], symmetric monoidal categories $\mathcal{C}$ equipped with an involutive functor $\dagger : \mathcal{C} \to \mathcal{C}^{\text{op}}$ of SMCs, the **dagger**, which is furthermore the identity on objects. Concretely, to each process $f : A \to B$ in a †-SMC $\mathcal{C}$ is associated a process $f^\dagger : B \to A$ in $\mathcal{C}$, called the **adjoint** of f, in a way such that $(f^\dagger)^\dagger = f$. Being a functor of SMCs further implies that $id_A^\dagger = id_A$, that $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$, and that $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$. There is a further requirement that $\sigma_{A,B}^\dagger = \sigma_{A,B}^{-1}$. For an operational characterisation of the Hermitian adjoint in quantum theory, see [SC16].

Although there is no mention of linearity, a †-SMC comes with an **inner product**, where two states ϕ and ψ are sent to the the scalar $\phi^\dagger \circ \psi$. We will say that a process $f : A \to B$ is an **isometry** if $f^\dagger f = id_A$, and that it is a **unitary** if it is furthermore invertible (equivalently, if $f^\dagger$ is also an isometry, i.e. $f f^\dagger = id_B$). Isometries preserve the inner product of states:

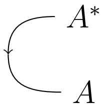
$$\left(\phi^\dagger f^\dagger\right)\left(f\psi\right) = \phi^\dagger\left(f^\dagger f\right)\psi = \phi^\dagger id_A\psi = \phi^\dagger\psi \tag{2.11}$$

The category Hilb is a †-SMC, with dagger given by the Hermitian adjoints. More generally, any choice of involutive semiring isomorphism $^\dagger : R \to R$ endows the category R-Mat with the structure of a †-SMC.

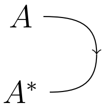
2.2.2 Dagger compact structure

The dagger abstractly captures state-effect duality, but says nothing about operator-state duality, the other important correspondence in quantum theory. The latter requires *compact closed* structure [DR89, KL80, BD95], and is a much more restrictive property. Dagger structure taken together with compact closed structure leads to the definition of dagger compact categories [AB04, AB05]. Here, we will (loosely) follow the presentation of compact closed categories given by [Sel10, Sel09].

We say that a SMC is **compact closed** if every object A comes with a **dual object** A^*, a **cup** $\eta_A : I \to A^* \otimes A$ and a **cap** $\varepsilon_A : A \otimes A^* \to I$



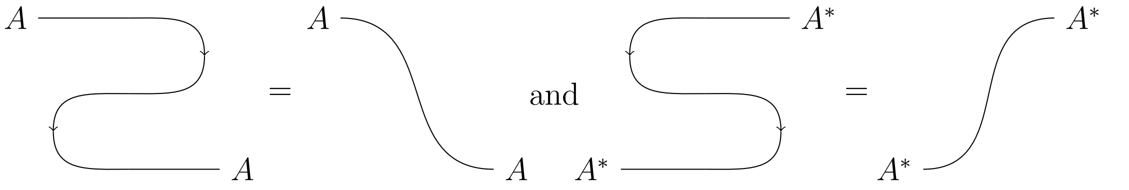
cup η_A



cap ε_A

(2.12)

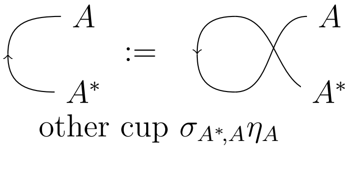
which satisfy the following **yanking equations** (where the right hand sides are just the identity morphisms id_A and id_{A^*}):



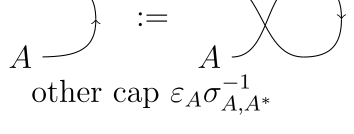
(2.13)

Duals are required to distribute (contravariantly) over the tensor product $(A \otimes B)^* = A^* \otimes B^*$, and to respect the tensor unit $I^* = I$ (technically, they are canonically isomorphic rather than equal, but the distinction can be safely ignored here).

These definitions actually hold in a generic monoidal category. In a SMC, the symmetry isomorphism gives one more cup and one more cap, themselves satisfying yanking equations:



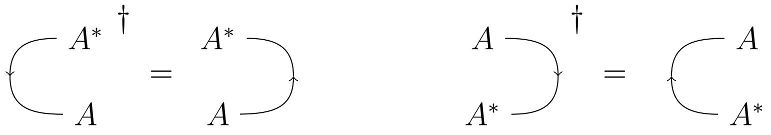
other cup $\sigma_{A^*,A}\eta_A$



other cap $\varepsilon_A\sigma^{-1}_{A,A^*}$

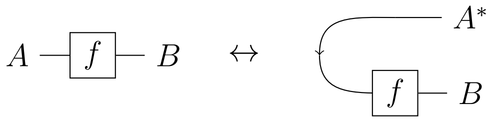
(2.14)

In a †-SMC, one more cup should arise in principle as $\varepsilon_A^\dagger$, and one more cap as $\eta_A^\dagger$: however, one imposes additional coherence conditions ensuring that these new cup and cap coincide with those of Equation 2.14, i.e. that $\varepsilon_A^\dagger = \sigma_{A^*,A}\eta_A$ and $\eta_A^\dagger = \varepsilon_A\sigma_{A,A^*}^\dagger$. A compact closed †-SMC satisfying these two additional requirements is called a **dagger compact category** [AB04, AB05]. Note that the little arrow markings flip upside-down when taking the adjoint:



(2.15)

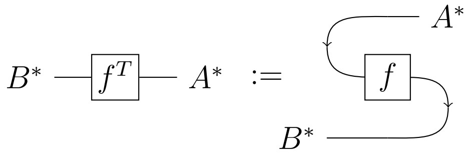
Because of the yanking equations, compact closed structure provides a form of **operator-state duality**, a bijection[5] between processes $A \to B$ and states $I \to A^* \otimes B$ given as follows:



(2.16)

In a dagger compact category, the adjoint induces an inner product on operators via operator-state duality, which we will refer to as the **Hilbert-Schmidt inner product** (because that is what it is called in fHilb).

The dagger structure induces an involutive symmetry on processes, sending a process $f : A \to B$ to its adjoint $B \to A$. Similarly, the compact closed structure induces another involutive symmetry, sending $f : A \to B$ to its **transpose** $f^T : B^* \to A^*$ defined as follows, and vice versa:



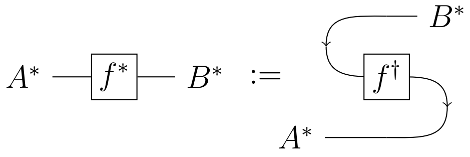
(2.17)

Correspondence 2.16 in particular bijects the states of the dual object A^* with the effects of A: as a consequence, the transpose f^T can be seen as a process acting on effects rather than states, sending an effect $b : B \to I$ on B to the effect $b \circ f : A \to I$ on A obtained by pre-composition with $f : A \to B$.

The adjoint and transpose symmetries commute, and together they generate a symmetry group on processes isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, with the following **conjugate**

[5] When the SMC is enriched, this always is an isomorphism in the appropriate category.

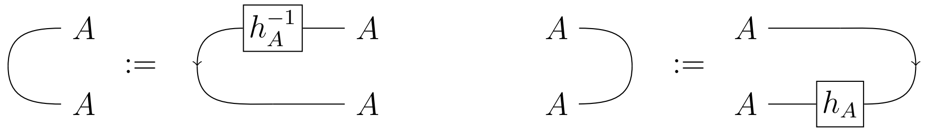
symmetry $f \mapsto f^* := (f^\dagger)^T = (f^T)^\dagger$ as the fourth group element:



(2.18)

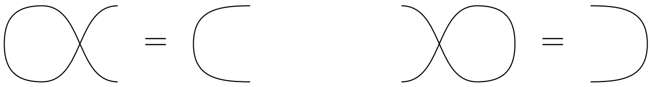
Like the transpose, the conjugate can also be seen as a process acting on effects.

A **self-duality structure** on a compact closed SMC is a family of isomorphisms $h_A : A \to A^*$ satisfying four coherence conditions laid out in [Sel10]. With these, we can define a new pair of **symmetric cup** and **symmetric cap**:



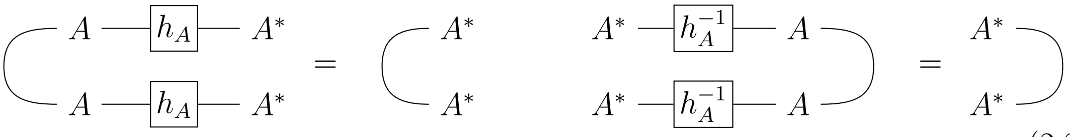
(2.19)

The first two conditions on h_A concern the relationship of duals with the tensor product: $h_I = id_I$ and $h_{A\otimes B} = \sigma_{A^*,B^*}\big(h_A \otimes h_B\big)$, where the symmetry isomorphism is required since $h_{A\otimes B} : A \otimes B \to B^* \otimes A^*$. The third coherence condition is symmetry:



(2.20)

The last condition relates the symmetric cup/cap on an object A to the symmetric cup/cap on the dual object A^*:



(2.21)

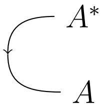
In a dagger compact category, Equation 2.15 can be seen to state that the two caps are the adjoints of the two cups; for a self-duality structure in a compact closed category, on the other hand, Equation 2.20 states that there is only one symmetric cup and one symmetric cap. It is then natural to require that self-duality structures in a dagger compact category lead to a symmetric cap which is adjoint to the symmetric cup[6]: this is equivalent to unitarity of the h_A isomorphisms, which is imposed as an additional coherence condition on self-duality structures in dagger compact categories.

2.2.3 Examples of dagger compact categories

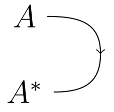
Finite-dimensional Hilbert spaces. The category fHilb of finite-dimensional Hilbert spaces is dagger compact, but the larger category Hilb of Hilbert spaces is not

[6] Which also validates the graphical notation we've chosen.

(it has dual objects, and state-effect duality, but it cannot have a cup or cap). For a finite-dimensional Hilbert space A, the dual object is defined to be its dual space A^*, the Hilbert space of linear functionals $A \to \mathbb{C}$. The cap ε_A is obtained from the inner product, as the linear map $A \otimes A^*$ which sends a state $|\psi\rangle$ of A and an effect $\langle a|$ of A (i.e. a state of A^*) to the complex number $\langle a|\psi\rangle$; the other cap is obtained by first applying a symmetry isomorphism σ^{-1}_{A,A^*}, and the two cups are obtained by taking adjoints. In terms of an orthonormal basis $|e_j\rangle_{j=1}^{\dim A}$ (any basis), the cup and cap can be written as follows, where states of A^* are represented by effects of A, and effects of A^* by states of A:

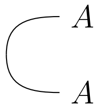


$$= \sum_{j=1}^{\dim A} |(e_j^{(A)})^\dagger\rangle \otimes |e_j^{(A)}\rangle \qquad \sum_{j=1}^{\dim A} \langle e_j^{(A)}| \otimes \langle (e_j^{(A)})^\dagger| =$$

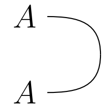


(2.22)

Choice of basis $|e_j^{(a)}\rangle_j$ induces a self-duality structure h_A, and the symmetric cup and cap given by Equation 2.19 for this self-duality structure take the following form:



$$= \sum_{j=1}^{\dim A} |e_j^{(A)}\rangle \otimes |e_j^{(A)}\rangle \qquad \sum_{j=1}^{\dim A} \langle e_j^{(A)}| \otimes \langle e_j^{(A)}| \quad =$$



(2.23)

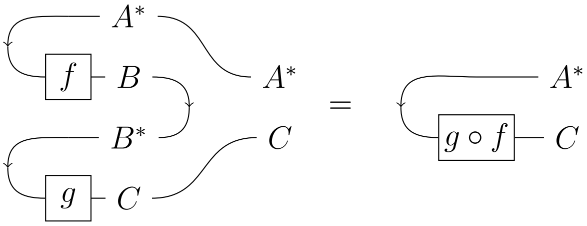
Because they satisfy the yanking equations, substituting the symmetric cup and cap in Equations 2.17 and 2.18 induce another transpose symmetry and another conjugate symmetry on processes (this time sending $f : A \to B$ to $f^{T_h} : B \to A$ and $f^{*_h} : A \to B$). Contrary to the transpose and conjugate symmetries induced by the dagger compact structure, these symmetries are basis-dependent. Similarly, the symmetric cup and cap of Equation 2.19 (and related transpose and conjugate) are basis-dependent, while the cup and cap of Equation 2.12 (and related transpose and conjugate) are basis-independent.

Categories of matrices over semirings. Now consider the †-SMC R-Mat, where R is a commutative semiring with involution. Because the objects are (essentially) in the form R^n for all natural numbers n, one can choose the canonical orthonormal basis $|e_j^{(n)}\rangle := 1 \mapsto (\delta_{ij})_{i=1}^n$, and Equation 2.23 readily give a family of symmetric cups and caps (they only involve the scalars 0 and 1, which behave the same way in any semiring). The dual space to the free R-semimodule R^n is the free R-semimodule of R-linear maps $R^n \to R$, itself isomorphic to R^n. Self-duality structures and symmetric cups/caps can be defined from choices of basis exactly like in the complex case. It should be noted that the existence of a dagger compact structure is related to the inner product, but has nothing to do with its non-degeneracy: the latter depends on the specific choice of involution, while the former exists for all choices of involution.

2.2.4 The matrix algebra

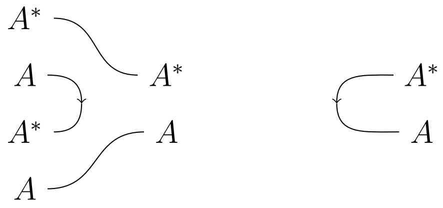
We have seen in Equation 2.16 that compact closed structure implements operator-state duality: it is natural to ask whether composition of operators can always be internalised by a process acting on the corresponding states, and this question leads to the definition of the *matrix algebra*.

If $f : A \to B$ is a process in a compact closed category, we will denote the corresponding state by $\lfloor f \rfloor : I \to A^* \otimes B$. The state $\lfloor g \circ f \rfloor : I \to A^* \otimes C$ corresponding to the composition of two processes $f : A \to B$ and $g : B \to C$ can be obtained as follows in terms of the corresponding states $\lfloor f \rfloor$ and $\lfloor g \rfloor$:



(2.24)

For processes $A \to A$, composition is a monoid operation, with the identity id_A as its unit. There is an internal monoid on object $A^* \otimes A$ corresponding to composition:



multiplication left/right unit

(2.25)

Similarly we can use the other cup and cap to construct a comultiplication and counit. The multiplication, unit, comultiplication and counit in a SMC form a Frobenius algebra (more on Frobenius algebras later), known as the **matrix algebra**. In a †-SMC, they form a symmetric †-Frobenius algebra (which in fHilb corresponds to the C*-algebra B $[A]$ of bounded operators on Hilbert space A).

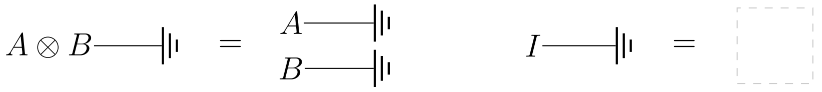
2.3 Environments, causality and purification

2.3.1 Environment structures

Dagger compact categories capture a number of structures typical of pure-state quantum theory, such as inner product, state-effect duality and operator-state duality.

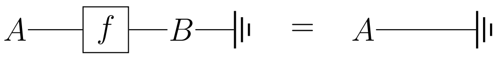
However, one additional component is necessary to make the leap from pure-state to mixed-state, and that component is the *environment structure*.

An **environment structure** for a SMC consists of a family of processes $\bar{\top}_A : A \to I$ for all objects, the **discarding maps**, such that:



(2.26)

The empty diagram on the RHS of the right equation is the scalar 1. Given an environment structure, a process $f : A \to B$ is said to be **normalised** if performing the process and then discarding the output is the same as discarding the input:



(2.27)

Discarding maps are also called **traces** by those of the Hilbert-space persuasion, in which case normalised processes should be referred to as **trace-preserving**. In the effectus community, the discarding map $\bar{\top}_X$ is also known as the *truth* (or *ground*) on X, and normalised processes are known as *total*.

Thanks to Equation 2.26, normalised processes in a SMC $\mathcal{C}$ with environment structure $\bar{\top}$ are guaranteed to form a sub-SMC $\mathcal{C}_{\bar{\top}}$, the **normalised subcategory**. In the normalised subcategory, the tensor unit I is terminal: there is a unique effect, namely $\bar{\top}_X$, on any system X, and there is a unique scalar id_I. This means that the discarding maps truly lose all information about the system, and thus define a sensible notion of discarding.[7]

2.3.2 Discarding maps in categories of matrices

The simplest example of environment structures is given by the category Set of sets and total functions, where the tensor unit (the singleton set $\mathbb{1}$) is already terminal: the discarding map $\bar{\top}_X$ on a set X is the unique total function $X \to \mathbb{1}$, and Set $=$ Set$_{\bar{\top}}$. The category fSet of finite sets and total functions is a subcategory of R-Mat for any semiring R, and endows the latter with its environment structure. If $|\psi\rangle : \mathbb{1} \to R^X$ is a state in R-Mat, then $\bar{\top}_X|\psi\rangle$ is the sum $\sum_{x \in X} \langle x|\psi\rangle$ of all entries of column vector $|\psi\rangle$, and normalised states are exactly those with entries summing to the multiplicative unit 1 of semiring R. Similarly, the normalised processes $R^X \to R^Y$ are those with $Y \times X$ matrix having normalised vectors as columns. The following examples are of interest in the applications we will consider here:

[7] This statement can be given categorical dignity by saying that $\bar{\top}$ is a monoidal natural transformation from the identity functor to the terminal endofunctor (of SMCs), the one sending all objects to I and all processes to the scalar id_I.

(i) in $\mathbb{R}^+$-Mat, the normalised subcategory is the category fStoch of finite sets and stochastic maps between them (with probability distributions as states);

(iia) in $\mathbb{B}$-Mat, the normalised states of $\mathbb{B}^X$ are the non-empty subsets of X, and the normalised processes $\mathbb{B}^X \to \mathbb{B}^Y$ are the relations $f \subseteq X \times Y$ which are total, i.e. such that $\operatorname{dom} f = X$;

(iib) in the subcategory fPFun $\leq$ $\mathbb{B}$-Mat of finite sets and partial functions, the normalised processes are the total functions, yielding $\text{fPFun}_{\bar{\top}} = \text{fSet}$;

(iii) in $\mathbb{N}$-Mat, the normalised subcategory is the category fSet of finite sets and functions.

2.3.3 The CPM construction

We have seen that the discarding maps inherited from fSet give the desired notion of normalised states and processes in the case of $\mathbb{R}^+$-Mat, the category modelling classical probabilistic systems. In the case of quantum theory, on the other hand, discarding is done by inner products and traces, and we need a different construction.

In the traditional formulation of quantum mechanics, the transition from pure-state to mixed-state sees the Hilbert space formalism replaced by the operator formalism: the states on a Hilbert space A are taken to be the positive self-adjoint operators $\rho : A \to A$, forming the $\mathbb{R}^+$-semimodule (aka convex cone) $\mathcal{L}[A]$, and more general processes $\Phi : \mathcal{L}[A] \to \mathcal{L}[B]$ are taken to be *completely positive (CP) maps*, sending positive self-adjoint operators $\rho : A \to A$ to positive self-adjoint operators $\Phi(\rho) : B \to B$. By **Kraus' Theorem**, the **CP maps** $\mathcal{L}[A] \to \mathcal{L}[B]$ are exactly those in the following form, known as **Kraus decomposition**:

$$\Phi(\rho) = \sum_{i=1}^{\dim A} \sum_{j=1}^{\dim B} B_{ij}\, \rho\, B_{ij}^\dagger \tag{2.28}$$

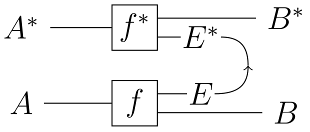
where the linear maps $B_{ij} : A \to B$ are known as the **Kraus operators**[8]. As a special case of Kraus' Theorem, one recovers a decomposition of positive self-adjoint operators in terms of pure states (not necessarily normalised):

$$\rho = \sum_{j=1}^{\dim B} |\psi_j\rangle\langle\psi_j| \tag{2.29}$$

[8] Note that the Kraus decomposition is only unique up to unitary transformations of the Kraus operators $B_{ij} \mapsto B'_{kl} := \sum_i \sum_j u_{klij} B_{ij}$.

In the operator formalism, the discarding map on system $\mathcal{L}[A]$ is given by the *trace*, sending state $\rho \in \mathcal{L}[A]$ to $\mathrm{Tr}\ \rho \in \mathbb{R}^+$. *Normalised states* are exactly those in the form of Equation 2.29 with $\sum_j \langle \psi_j | \psi_j \rangle = 1$; traditionally, the pure states $|\psi_j\rangle$ are chosen to be orthogonal (appealing to the spectral theorem) and then renormalised to yield a convex mixture of orthonormal states $\rho = \sum_j p_j \, |\phi_j\rangle\langle\phi_j|$, where $p_j \in \mathbb{R}^+$ sum to 1 and are interpreted as probabilities. Normalised CP maps are called *trace-preserving*, and by Kraus' Theorem they are exactly those satisfying $\sum_i \sum_j B_{ij}^\dagger B_{ij} = id_A$.

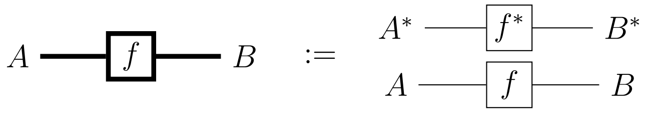
Categories of completely positive maps, also known as **CPM categories** [Sel07, CP10], can be constructed for all dagger compact categories, in a process which mimics the way in which the operator model of mixed-state quantum mechanics (corresponding to the CPM category CPM[fHilb]) is constructed from the Hilbert space model of pure-state quantum mechanics (corresponding to the dagger compact category fHilb). Given a dagger compact category $\mathcal{C}$, the corresponding CPM category CPM[$\mathcal{C}$] is defined as the subcategory of $\mathcal{C}$ having objects in the form $A^* \otimes A$ and morphisms in the following form:



(2.30)

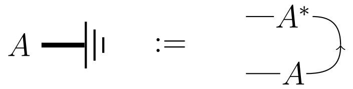
where $f : A \to E \otimes B$ is a morphism of $\mathcal{C}$, and $f^* : A^* \to B^* \otimes E^*$ is its conjugate (obtained via the dagger compact structure). In CPM[$\mathcal{C}$], the object $A^* \otimes A$ is simply written A, so that the process depicted in Diagram 2.30 is considered a process $A \to B$ in CPM[$\mathcal{C}$]. Processes in the CPM category are called **completely positive (CP) maps**. The system E in Diagram 2.30 is often interpreted as an **environment** which is operationally inaccessible, and hence must be "discarded" after the process has taken place. In the case of CPM[fHilb], i.e. in the operator model of mixed-state quantum mechanics, Diagram 2.30 can be seen as an alternative formulation of Kraus decomposition.

Diagrammatic reasoning about categories of completely positive maps often involves two distinct SMCs: the original category $\mathcal{C}$ and the CPM category CPM[$\mathcal{C}$]. As a consequence, a stylistic convention is adopted where systems and processes of the CPM category CPM[$\mathcal{C}$] are denoted by thicker wires, boxes and decorations. For example, the "doubled" version $f^* \otimes f$ of a process $f : A \to B \otimes E$ will be denoted as f with thicker wires and box:



(2.31)

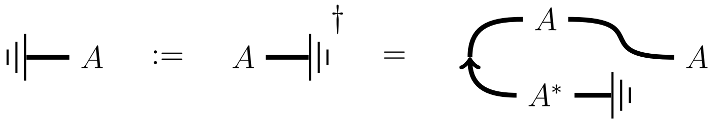
The caps from compact closed structure play a particularly important role in the definition of the CPM category, and are given their own decoration:



(2.32)

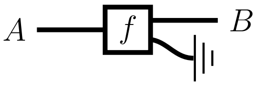
The CP map **double** $[f]$ defined by Equation 2.31 is called the **double** of process f, while the CP map ⏚$_A$ defined by Equation 2.32 is called the **discarding map** on system A. The discarding maps ⏚$_A$ form a canonical environment structure for CPM$[\mathcal{C}]$. In mixed-state quantum mechanics, the double of a linear map f is the CP map **double** $[f] := \rho \mapsto f \circ \rho \circ f^\dagger$, while the discarding map ⏚$_A$ sends a positive state $\rho \in \mathcal{L}[A]$ to its trace Tr $\rho \in \mathcal{L}[\mathbb{C}] \cong \mathbb{R}^+$.

CPM categories CPM$[\mathcal{C}]$ are dagger compact, and the rules of diagrammatic reasoning for dagger compact categories apply to them. The compact structure for CPM$[\mathcal{C}]$ is given by the doubles of the cups and caps of $\mathcal{C}$, while the adjoint of a process in the form of Diagram 2.30 is given by first taking the adjoint in $\mathcal{C}$, and then using the following equation for the adjoint of the discarding map:



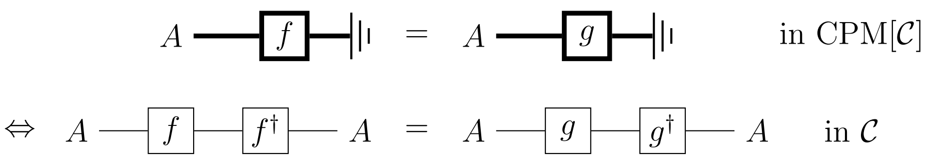
(2.33)

Because the doubled processes **double** $[f]$ and the discarding maps ⏚$_A$ are well-defined CP maps, it is legitimate to rephrase the very definition of the CPM category by saying that its processes are exactly those in the following form:



(2.34)

This means that doubled processes and discarding maps are enough to *express* all CP maps. However, in order to *prove results about* CP maps, we need a graphical axiom relating a generic CPM category CPM$[\mathcal{C}]$ to the corresponding original category $\mathcal{C}$. The required relationship is encoded by the following **CPM axiom**, which characterises the action of discarding maps in CPM$[\mathcal{C}]$ in terms of the dagger structure of $\mathcal{C}$:



(2.35)

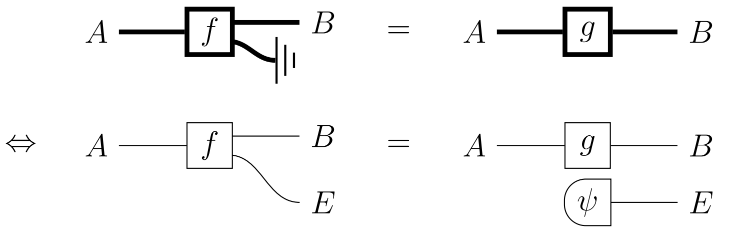
It is possible to state an exact correspondence between CPM categories and dagger compact categories satisfying the CPM axiom above.

Theorem 2.1 (**CPM Categories** [Coe08, CP10, CH12])**.**
Let $\mathcal{C}$ be a dagger compact category with an environment structure $(\overset{=}{\top}_A)_{a \in \mathrm{obj}\,\mathcal{C}}$ satisfying Equation 2.33. Let $\mathcal{D}$ be another dagger compact category, together with a functor $\Phi : \mathcal{D} \to \mathcal{C}$ of dagger compact categories which is a bijection on objects (so that the compact closed structure of $\mathcal{C}$ is exactly the image under Φ of the compact closed structure of $\mathcal{D}$). Assume that all morphisms in $\mathcal{C}$ take the form of Equation 2.34 for some morphism f in the image of Φ, and that the CPM Axiom is satisfied. Then there is a (necessarily unique) isomorphism of dagger compact categories $F : \mathcal{C} \to \mathrm{CPM}[\mathcal{D}]$ such that $F\big(\Phi(f)\big) = \textbf{\textit{double}}\,[f]$ for all morphisms f of $\mathcal{D}$ and $F(\overset{=}{\top}_{\Phi(A)}) = \overset{=}{\top}_A$ for all objects A of $\mathcal{D}$.

2.3.4 Purification

Observe that CP maps in CPM[$\mathcal{C}$] arising as doubles of morphisms in $\mathcal{C}$ form a dagger compact subcategory Double [$\mathcal{C}$]: they are closed under parallel and sequential composition and dagger, and the cups and caps of CPM[$\mathcal{C}$] arise themselves as doubled processes. In the case of mixed-state quantum mechanics, the **doubled category** Double [fHilb] corresponds to linear maps of Hilbert spaces *up to global phase*: it is in fact this category, rather than fHilb, that models pure-state quantum mechanics. More generally, we want to see Double [$\mathcal{C}$] as a sub-category of pure processes within a larger category CPM[$\mathcal{C}$] of mixed processes: for this to be meaningful, we need the doubled category to satisfy some core operational characteristics of purity in mixed-state quantum theory.

Purity is a feature arising at the interface between quantum theory and thermodynamics [CDP10, CS15]: pure processes can broadly be interpreted as not involving any probabilistic mixing due to non-trivial interactions with a discarded environment. Former work on purity has taken the following approach: purity is defined as a property, and the *purification axiom* is formulated as the requirement that all processes be expressible as a combination of pure processes and discarding maps. Because CPM categories already come with the guarantee that all processes are expressible as combinations of doubled processes and discarding maps, we will turn things the other way around. We will say that a CPM category satisfies the **Purification axiom** if doubled processes (which we want to interpret as pure) satisfy the following abstract version of purity:



(2.36)

with the additional requirement that $\bar{\bar{\top}}_E \circ \textbf{double}\,[\psi] = 1$ (i.e. ψ is a normalised state), or equivalently that $\langle\psi|\psi\rangle = 1$ (by the CPM axiom). Operationally, the Purification axiom can be given the following interpretation: the only way a process $(id_B \otimes \bar{\bar{\top}}_E) \circ \textbf{double}\,[f]$ involving the discarding of an environment E can result in a pure process g is if the environment being discarded is disconnected altogether from the pure process (i.e. the interaction with the environment is **trivial**). In a category which satisfies the purification axiom, we will also refer to the doubled processes as **pure processes**, and to the doubled subcategory as **pure subcategory**.

The Purification axiom is a non-trivial requirement for CPM categories, and there are many inequivalent examples of CPM categories violating it.

Theorem 2.2 (CPM categories violating the Purification axiom). *Let R be a commutative semiring with involution in which the multiplicative unit 1 is additively idempotent*[9]*. Then* CPM[R-Mat] *violates the Purification Axiom.*

Proof. Let X be any finite set with at least two elements, and let $\mathcal{P}^+(X)$ be the set of non-empty subsets of X. To obtain a counterexample to the Purification axiom 2.36, we construct an $f : R^X \to R^X \otimes R^{\mathcal{P}^+(X)}$ such that $(id_{R^X} \otimes \bar{\bar{\top}}_{R^{\mathcal{P}^+(X)}}) \circ \textbf{double}\,[f] = \textbf{double}\,[id_{R^X}]$ but f does not decompose as $id_{R^X} \otimes \psi$ for any state $\psi : R \to R^{\mathcal{P}^+(X)}$. Indeed, consider the map f defined as follows:

$$f := \sum_{U \in \mathcal{P}^+(X)} \sum_{x \in U} |x\rangle \otimes |U\rangle \otimes \langle x| \tag{2.37}$$

Note that this map cannot decompose as $id_{R^X} \otimes \psi$ for any state ψ:

$$f|x\rangle = |x\rangle \otimes \Big(\sum_{U \in \mathcal{P}^+(X)} \delta_{x \in U} |U\rangle \Big) \tag{2.38}$$

Now consider its doubled version $\textbf{double}\,[f]$, and discard the system $R^{\mathcal{P}^+(X)}$ to obtain the following morphism $R^X \to R^X$ of CPM[R-Mat], which we write down

[9] Examples include all locales (e.g. the booleans $\mathbb{B}$), all tropical semirings (e.g. the tropical semiring $(\mathbb{R}, \min, +)$ or the Viterbi semiring $([0,1], \max, \times) \cong (\mathbb{R}^+, \min, +)$) and all commutative unital quantales.

explicitly as a morphism $R^X \otimes R^X \to R^X \otimes R^X$ of R-Mat by using the expression ⏚$_{R^{\mathcal{P}^+(X)}} = \sum_{U \in \mathcal{P}^+(X)}$ **double** $[\langle U|]$ for the discarding map on $R^{\mathcal{P}^+(X)}$:

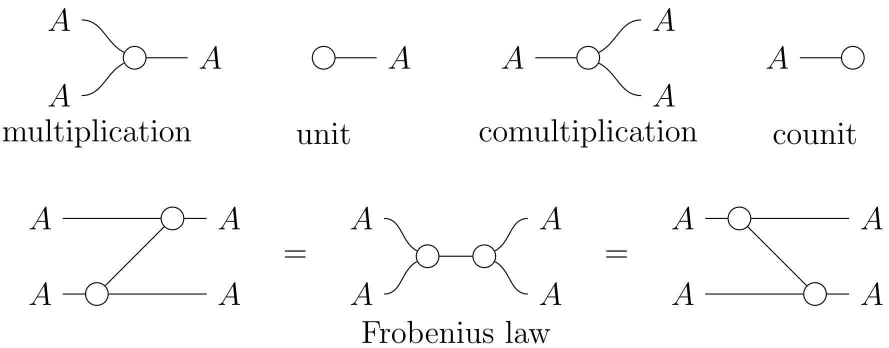
$$
\begin{aligned}
&\sum_{x,y \in X} \sum_{U \in \mathcal{P}^+(X)} \delta_{x,y \in U} \big(|x\rangle \otimes |y\rangle\big) \otimes \big(\langle x| \otimes \langle y|\big) \\
&= \sum_{x,y \in X} \Big(\sum_{U \in \mathcal{P}^+(X)} \delta_{x,y \in U}\Big) \big(|x\rangle \otimes |y\rangle\big) \otimes \big(\langle x| \otimes \langle y|\big) \\
&= \sum_{x,y \in X} \big(|x\rangle \otimes |y\rangle\big) \otimes \big(\langle x| \otimes \langle y|\big) = \textbf{double}\,[id_{R^X}]
\end{aligned}
\tag{2.39}
$$

where the second equality follows from the fact that $\sum_{U \in \mathcal{P}^+(X)} \delta_{x,y \in U} = 1$, since 1 is additively idempotent and there is at least one U such that $x, y \in U$ (furthermore, we have used the fact that $0^\dagger 0 = 0$ and $1^\dagger 1 = 1$, so that $\delta^\dagger_{x,y \in U} \delta_{x,y \in U} = \delta_{x,y \in U}$). This concludes our proof. □

2.4 Coherent data manipulation

2.4.1 Dagger Frobenius algebras

Frobenius algebras are a fundamental ingredient of quantum theory, where they are intimately related to the notion of observable. Consider a monoid (A, ⟩○– , ○–) on an object A of a †-SMC $\mathcal{C}$: a binary operation ⟩○– : $A \otimes A \to A$ (the **multiplication**) which is associative and has the state ○– : $I \to A$ (the **unit**) as its bilateral unit. We will refer to this fact by saying that ⟩○– and ○– satisfy **associativity**, or the **associative law**, and the **left/right unit laws**. Then the adjoints –○⟨ := (⟩○–)† : $A \to A \otimes A$ (the **comultiplication**) and –○ := (○–)† : $A \to I$ (the **counit**) automatically form a comonoid on A in $\mathcal{C}$ (i.e. they satisfy **coassociativity** and the **left/right counit laws**). A **†-Frobenius algebra** on an object A in $\mathcal{C}$ is one such pair of monoid and comonoid on A, which are furthermore related by the following **Frobenius law**:

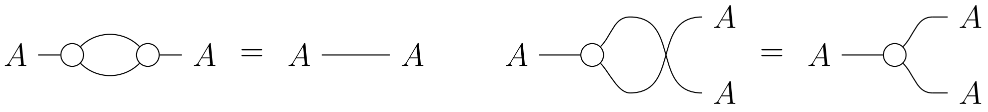


multiplication unit comultiplication counit

(2.40)

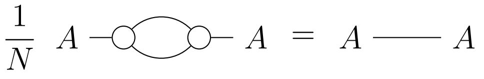
Frobenius law

A †-Frobenius algebra is said to be **special** if the comultiplication -○< is an isometry, and **commutative** if the monoid and comonoid are commutative:



speciality commutativity (2.41)

More generally, a **quasi-special** †-Frobenius algebra is one with comultiplication -○< which is an isometry up to a **normalisation factor** N, where N is in the form $n^\dagger n$ for some invertible scalar n:



(2.42)

quasi-speciality

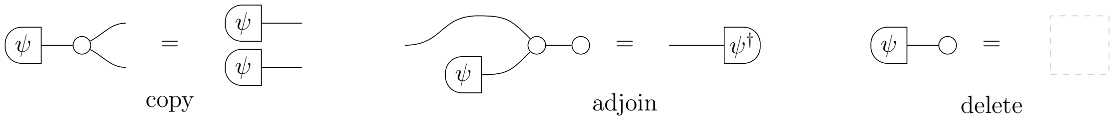
Speciality corresponds to the particular case of quasi-speciality in which $N = 1$. By normalisation, any quasi-special Frobenius algebra corresponds to a unique special Frobenius algebra: as such, quasi-speciality can be used in place of speciality to simplify some definitions and results, without causing any issue of interpretation.

Because several combinations of these properties will play a role in this work, we introduce a number of short-hands for †-Frobenius algebras:

†-Frobenius algebras	commutative	arbitrary
special	†-SCFA	†-SFA
quasi-special	†-qSCFA	†-qSFA
arbitrary	†-CFA	†-FA

2.4.2 Quantum observables

The importance of †-SCFAs in the foundations of quantum mechanics comes from the fact that they correspond to orthonormal bases, i.e. non-degenerate quantum observables. Key to this correspondence is the notion of **classical states** for a †-FA ○, those states ψ which are copied/adjoined/deleted by ○ in the following sense:



copy adjoin delete

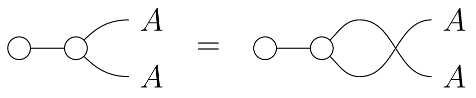
(2.43)

Note that the RHS of the delete condition is the scalar 1.

Theorem 2.3 ([CPV13])**.** *In* fHilb*, the classical states for a †-SCFA ○ always form an orthonormal basis*[10]*. Furthermore, any orthonormal basis arises this way for a unique †-SCFA. More generally, if ○ is a †-qSCFA, with normalisation factor N, then the classical states for ○ form an orthogonal basis, each state having norm $\sqrt{N}$. Furthermore, any orthogonal basis where all states have the same norm $\sqrt{N}$ arises this way for a unique †-qSCFA.*

The concept of classical states forming a basis is generalised to arbitrary †-SMC by the notion of enough classical states. A †-FA ○ on an object A is said to have **enough classical states** if its classical states separate morphisms from A (i.e. any two morphisms $f, g : A \to B$ are equal whenever $f \circ \psi = g \circ \psi$ for all classical states ψ of ○). Because of the copy condition, a †-FA with enough classical states is always necessarily commutative[11].

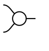
This algebraic characterisation of quantum observables is not limited to the non-degenerate case of orthonormal bases, but can be extended to the more general case of complete families of orthogonal projectors (i.e. to possibly degenerate quantum observables). To do so, one considers **symmetric** †-Frobenius algebras[12], i.e. those satisfying the following equation:

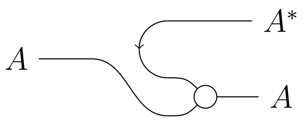


(2.44)

Independently of their relevance to Theorem 2.4 below, symmetric †-Frobenius algebras have the desirable feature that the inner product structure (the cup and cap) that they define is symmetric. As a consequence, the adjoin condition holds both in the formulation of Equation 2.43 and in the "conjugate" formulation, the one having the state on the other side of the symmetric cap.

Theorem 2.4 ([Vic11])**.** *In* fHilb*, symmetric †-SFAs are in bijective correspondence with C*-algebras, and hence with complete families of orthogonal projectors.*

The core observation in the proof of Theorem 2.4 is that the following map $A \to A^* \otimes A$ is in fact a monoid homomorphism from the algebra (A,  ,) to the matrix algebra on $A^* \otimes A$:



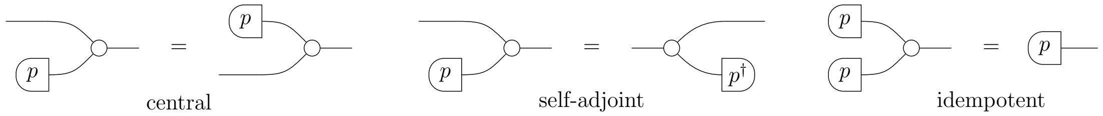
(2.45)

[10] It should also be noted that the copy and delete conditions are sufficient to characterise classical states in the case of fHilb.

[11] To see this, just compose both sides of the commutativity equation with an arbitrary classical state and copy the state through, obtaining the same result on both sides.

[12] Commutative †-FAs are a special case of symmetric †-FAs.

Elements of the algebra (A, ⟩○– , ○–) are sent to operators $p : A \to A$ (or, to be precise, to the corresponding states $\lfloor p \rfloor : I \to A^* \otimes A$ under compact closure): in fact, as Theorem 2.4 shows, they are sent to a C*-algebra of operators $A \to A$. Elements which are central for the algebra get sent to operators which commute with all other operators in the image, elements which are self-adjoint get sent to self-adjoint operators, and elements which are idempotent get sent to idempotent operators:



central self-adjoint idempotent

(2.46)

In particular, the central self-adjoint idempotents of the algebra (A, ⟩○– , ○–) are mapped to the central projectors of the image C*-algebra. The non-zero minimal[13] central self-adjoint idempotents are mapped to the unique complete family of orthogonal projectors $(p_j)_j$ corresponding to the C*-algebra (i.e. the one given by the *Artin–Wedderburn theorem for finite-dimensional C*-algebras*).

2.4.3 A brief digression on observables

In the traditional presentation of pure-state quantum mechanics, observables are identified with self-adjoint operators. This is mainly because the latter have two extremely useful features: (i) the eigenspaces of a self-adjoint operator form a complete family of orthogonal subspaces; (ii) the eingenvalues of a self-adjoint operator are real, and automatically possess the linear structure necessary to treat them as the values of a random variable. As a consequence of these features, it is always possible to see a self-adjoint operator as defining a unique measurement with real-valued outcomes, with each eigenspace corresponding to a definite outcome for the measurement.

This identification is slick and full of useful consequences[14], but at the end of the day it is no more than a trick, or a fortuitous coincidence. To explain why one should not take the identification of observables and self-adjoint operators too seriously, we lay down the following issues.

- Self-adjoint operators in quantum mechanics correspond to measurements with real-valued outcomes. While many examples of naturally real-valued observables exist in the physical literature[15], this is in no way general: to fit other

[13] Under the partial order defined by letting $p \preceq q$ if and only if $p = q + s$ for some s which is mapped to a positive self-adjoint operator.

[14] For example, it leads to the identification of $\langle\psi|H|\psi\rangle$ as the expected value of the measurement corresponding to H on a pure state $|\psi\rangle$.

[15] For example, position/momentum of unbounded particles, energy, number, etc.

measurements within this framework, a potentially unnatural identification of measurement outcomes with real values will be needed.

- Even vector-valued measurements cannot be accommodated directly by self-adjoint operators: instead, another slick trick is needed, where families of self-adjoint operators are considered, each operator associated to an individual vector coordinate.

- While measurement of states in probabilistic theories always result in probability distributions over the classical outcomes, they need not yield a real-valued random variable, and a notion of expectation might not be well defined for them. On the other hand, self-adjoint operators always yield a notion of expected value on the real values associated to the measurement outcomes, which might be spurious at best and misleading at worst.

- The identification is not a defining property of self-adjoint operators, instead relying on the Spectral Theorem (a heavyweight result in linear algebra) for its entire justification. The identification of observables as the self-adjoint generators of unitary symmetries requires Stone's Theorem (another heavyweight result).

As an example of a situation in which self-adjoint operators are unsuitable, we consider the position observable for a periodic lattice, which we can think of as valued in the translation group $G = \prod_{d=1}^{D} \mathbb{Z}_{n_d}$ (just like the usual position observable for a 1-dim wavefunction is valued in the translation group $\mathbb{R}$). Because there is no group homomorphism $\prod_{d=1}^{D} \mathbb{Z}_{n_d} \rightarrow \mathbb{R}^D$, there is no natural way to identify the position observable with a family $(x_d)_{d=1}^{D}$ of self-adjoint operators.

We could try to extract one such identification by considering the family of self-adjoint operators $(\mathbf{x}_d)_{d=1}^{D}$ which exponentiates to the unitary representation $(V_{\chi_p})_{p\in G}$ of the boost symmetry in the following way:

$$\left(V_{\chi_p}\right)_d = e^{2\pi i \frac{p_d \mathbf{x}_d}{n_d}} \tag{2.47}$$

This attempt, which in the traditional case shows that the position observable generates the boost symmetry, cannot work here: there are infinitely many equivalent families $(\mathbf{x}_d)_{d=1}^{D}$ which satisfy the equation above, corresponding to the infinitely many possible choices of representatives in $\mathbb{Z}$ (which is a subset of the reals) for the congruence classes modulo n_d. Furthermore, the periodic nature of positions means that there is no well-defined notion of expected value, and the one arising from any given choice of representatives in $\mathbb{R}$ is misleading.

The objections above will turn out to be extremely pertinent to our work, and we will therefore reject the identification of observables and self-adjoint operators. When talking about observables, we will be referring to the CQM notion of observables as (special) †-Frobenius algebras.

2.4.4 Coherent data manipulation

Further to their correspondence with quantum observables, †-Frobenius algebras find concrete use as fundamental building blocks of quantum algorithms and protocols [Vic12b, BH12, CK17, GK17]. When designing quantum protocols, classical data is often encoded into quantum systems using orthonormal bases. In this context, the four processes forming a special †-SCFA can be seen as the abstract, "coherent" versions of some basic data manipulation primitives:

(a) the comultiplication -< $= |\psi_x\rangle \mapsto |\psi_x\rangle \otimes |\psi_x\rangle$ acts as coherent copy;

(b) the counit -○ $= |\psi_x\rangle \mapsto 1$ acts as coherent deletion;

(c) the multiplication >- $= |\psi_x\rangle \otimes |\psi_y\rangle \mapsto \delta_{xy}|\psi_x\rangle$ acts as a coherent matching;

(d) the unit ○- $= \sum_x |\psi_x\rangle$ acts as coherent superposition (up to normalisation).

These "coherent" operations seldom appear alone, but are instead composed amongst themselves and with other primitives to form unitaries and CP maps appearing in quantum algorithms and protocols (as shown in the next Chapters).

When talking about **coherent data**, we will be thinking of classical data, valued in some finite set X, which has been **coherently encoded** into an orthonormal basis $|x\rangle_{x\in X}$ of some finite-dimensional Hilbert space $\mathcal{H}$. Having fixed coherent encodings of its input and output data into orthonormal bases $|x\rangle_{x\in X}$ and $|y\rangle_{y\in Y}$ of Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, when talking about the **coherent** encoding of a classical function $F : X \to Y$ we will be thinking of its $\mathbb{C}$-linear map extension to $\mathcal{H} \to \mathcal{K}$:

$$f := \sum_{x\in X}\sum_{y\in Y} |F(x)\rangle\langle x| \tag{2.48}$$

The term **coherent** is chosen as the opposite of **decohered**, a term which we will use to denote classical data and processes (which we see as arising from quantum operations by appropriate decoherence). This choice of nomenclature is self-consistent: the original classical function F (the decohered version) is obtained back by decohering the $\mathbb{C}$-linear map f from Equation 2.48 (the coherent version) in the orthonormal bases that were used to encode the classical input and output data.

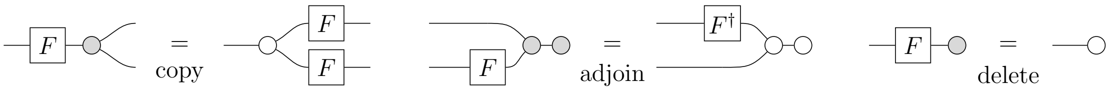
Coherent encodings of classical functions play a huge role in quantum computing and in the foundations of quantum theory: they are used to construct oracles (e.g. in the Deutsch-Josza algorithm, in Grover's algorithm and in the algorithm solving the abelian HSP), Frobenius algebras (see above), groups algebras (see below), entangled states (e.g. unnormalised Bell states, GHZ states and W states), and many other building blocks used to design quantum protocols. This is because coherent data enjoys all those features of $\mathbb{C}$-linearity (such as superposition, interference and non-commutative observables) which coalesce to provide quantum advantage and non-classical behaviour, while at the same time allowing for a good deal of classical intuition to play a positive role in designing quantum algorithms. A significant part of the development of CQM has been devoted to capturing the defining algebraic and diagrammatic properties of coherent manipulation of classical data, with the aim of designing quantum protocols and reasoning about them without explicit reference to the $\mathbb{C}$-linear structure itself.

The defining properties of †-SCFAs—one of the most fundamental structures in CQM—can indeed be seen as characterising the topological flow of classical information. As such, †-SCFAs in arbitrary †-SMCs are often interpreted as modelling coherent copy/deletion/matching operations on data which has been coherently encoded using their classical states, and are known as **classical structures** in the literature (a characterisation which becomes exact when the †-SCFA has enough classical states). Because non-degenerate observables in quantum mechanics correspond exactly to all the possible ways that classical data can be coherently encoded into a quantum system, †-qSCFAs are chosen in CQM to be the generalisation of non-degenerate observables and commutative C*-algebras from finite-dimensional quantum systems to arbitrary †-SMCs. As a natural consequence, symmetric †-qSFAs are chosen to be the generalisation of generic observables and C*-algebras.[16]

If classical states for a symmetric †-qSFA are interpreted as coherently encoding classical data in an object of a †-SMC, it becomes interesting to understand which processes can be interpreted as coherently encoding classical functions on that data. Classical states are defined by three conditions: they are coherently copied, adjoined and deleted. Similarly, we should expect the coherent versions of classical functions to respect the same coherent copy, adjoin and delete operations that define the states, so that they will end up mapping classical states to classical states. As a consequence,

[16] The generalisation further extends to quasi-special †-Frobenius algebras, which are are interpreted as the unnormalised versions of observables.

we will say that a process $f : A \to B$ is **○-to-● classical**, where ○ and ● are symmetric †-qSFAs on A and B respectively, if it satisfies the following three conditions:

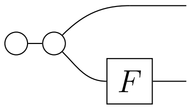


(2.49)

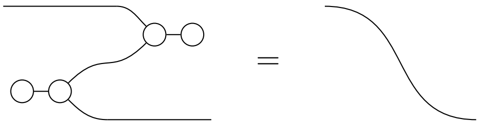
A ○-to-● classical process always sends classical states of ○ to classical states of ●. In fHilb, the ○-to-● classical process between †-qSCFAs are exactly those taking the form of Equation 2.48, where $|x\rangle_{x\in X}$ and $|y\rangle_{y\in Y}$ are the orthonormal bases associated with ○ and ● respectively.

2.4.5 Bell states and effects

The adjoin condition for classical processes involves a setup which is strongly reminiscent of the operator-state duality induced by the compact closed structure:

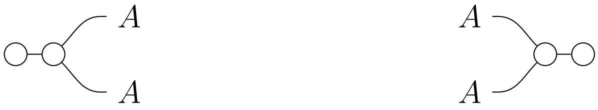


where



(2.50)

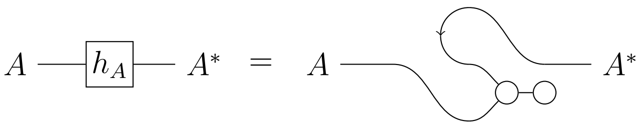
This is not a coincidence. Indeed, any symmetric †-FA on a system A in a †-SMC induces a **symmetric cup** (also known as a **Bell state**) and a **symmetric cap** (also known as a **Bell effect**) on A:



symmetric cup / Bell state   symmetric cap / Bell effect

(2.51)

Just like the symmetric cup and cap for a self-duality structure, the ones above satisfy the yanking equations (because of Frobenius law and unit laws), and Equations 2.20 (because of symmetry). When the category is dagger compact, the symmetric cup and cap defined by a †-FA on a system A also satisfy Equations 2.19 for the **self-duality isomorphism** $h_A : A \to A^*$ defined as follows:



(2.52)

2.4.6 Observables in classical physics

From the discussion above, it might sound like †-FAs are restricted to modelling quantum observables, and are unsuitable to model classical observables: luckily, this couldn't be further from the truth.

An observable on a classical system X can be though to be a partition $X = \sqcup_{i\in I} X_i$ of its set of **microstates** X into non-empty disjoint subsets $(X_i)_{i\in I}$, the **macrostates**, indexed by some classical outcome set I. However, a complete picture should also take into account the fact that different microstates $x \in X_i$ within the same macrostate X_i are connected by certain internal symmetries, which can be modelled by a connected groupoid [BV14]. Overall, we can think of an observable on a classical system X as a groupoid[17] $\oplus_{i\in I} G_i$, where G_i are connected groupoids and the macrostates are taken to be the underlying sets $X_i := |G_i|$ (i.e. are obtained by forgetting the internal symmetries). As it turns out, this picture of classical observables coincides with that of (symmetric) †-SFAs in the dagger compact category Rel of sets and relations.

Theorem 2.5 (Observables for classical systems [Pav09, CHK14]).
The †-SFAs $\circ$ on an object X of Rel *are the groupoids $G := \oplus_{i\in I} G_i$ on the set X:*

(a) the algebra multiplication $\succ\!\!-$ is a partial function $X \times X \rightharpoonup X$, corresponding to the groupoid multiplication:

$$\succ\!\!- \circ (|x\rangle \otimes |y\rangle) = \begin{cases} x \cdot y \text{ in } G_i & \text{if both } x, y \in G_i \text{ for some } i, \\ 0 & \text{otherwise}; \end{cases} \tag{2.53}$$

(b) the algebra unit is the union $\circ\!- = \bigcup_{i\in I} \sum_{u \text{ unit of } G_i} |u\rangle$ of all the units[18] for all the connected groupoids $(G_i)_{i\in I}$.

The $\circ$-classical states take the form $|X_i\rangle := \bigcup_{x\in G_i} |x\rangle$. Also, $\circ$ is necessarily symmetric.

Proof. The correspondence between †-SFAs and groupoids is a result of [Pav09, CHK14]. In particular, $\circ$ is necessarily symmetric: $x \cdot y = u$ for some unit u implies that $x, y, u \in G_i$ for some $i \in I$, and hence that $y \cdot x = v$ for some other unit $v \in G_i$. Now consider a $\circ$-classical state $|\psi\rangle$, with $\psi \subseteq X$. The copy condition is the requirement that $x, y \in \psi$ if and only if $x \cdot y$ is defined and $x \cdot y \in \psi$; the delete condition is the requirement that $u \in \psi$ for at least one unit u; the adjoin condition is the requirement that $x \in \psi$ if and only if $x^{-1} \in \psi$. Hence the classical states are exactly those in the form $|X_i\rangle$ for $X_i := |G_i|$. □

[17] In this subsection, and only in this subsection, the symbol $\oplus$ is used to denote the disjoint union of groupoids, which is the co-product in the category of groupoids. Every groupoid is expressible in a unique way as the co-product of its connected components.

[18] Recall that elements in a groupoid can have distinct left and right units, so that even connected groupoids can have more than one unit.

2.4.7 Canonical Frobenius algebras

Finally, a brief remark about the relationship between †-Frobenius algebras and the CPM construction. In this Section, we have characterised †-Frobenius algebras in fHilb as quantum observables, while in the previous Section we have noted that the real category modelling pure-state quantum theory is the pure subcategory of CPM[fHilb], rather than fHilb. So a question arises: how does our characterisation of †-Frobenius algebras in fHilb affect the pure subcategory of CPM[fHilb]? The answer turns out to be rather simple.

Because of their diagrammatic definition, the †-FAs (A, >○– , ○–, –○< , –○) from a dagger compact $\mathcal{C}$ give rise to †-FAs in the doubled subcategory of CPM[$\mathcal{C}$]:

$$\big(A, \textbf{double}\,[\;{>}{\circ}{-}\;]\,, \textbf{double}\,[{\circ}{-}]\,, \textbf{double}\,[\;{-}{\circ}{<}\;]\,, \textbf{double}\,[{-}{\circ}]\big) \tag{2.54}$$

The †-FAs in CPM[$\mathcal{C}$] that arise this way are said to be **canonical**. In this work, we will only consider canonical †-FAs when working with CPM categories.

2.5 Measurements, decoherence and classicality

2.5.1 Probabilistic theories

We have seen before that a generalised notion of finite classical systems, where probabilities are replaced by a generic involutive[19] semiring R, can be modelled by the dagger compact category R-Mat. We will refer to these as **classical R-probabilistic systems**, or simply **classical probabilistic systems** in the case $R = \mathbb{R}^+$.

The category fSet of finite sets and functions, modelling finite deterministic classical systems, is always a sub-SMC of R-Mat, which it endows with the following environment structure:

$$⏚_{R^X} := \Big(\sum_{x \in X} p_x |x\rangle\Big) \mapsto \sum_{x \in X} p_x \tag{2.55}$$

The normalised states in R-Mat are the **R-distributions**, the states $\sum_{x \in X} p_x |x\rangle$ such that $\sum_{x \in X} p_x = 1$, and the normalised processes are the **R-stochastic maps**, the linear maps $R^X \to R^Y$ which send R-distributions on X to R-distributions on Y. In the case of classical probabilistic systems, normalised states are probability distributions on finite sets, and normalised processes are stochastic maps.

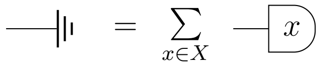
[19] The involution can simply be the identity $id_R : R \to R$. When talking about the probabilistic case $R = \mathbb{R}^+$, we will always implicitly assume that the involution is the identity.

The category R-Mat is enriched in the category of commutative monoids (or CMon-enriched), by which we mean that the processes $R^X \to R^Y$ between fixed systems R^X and R^Y form a commutative monoid, and that composition, tensor product and dagger all respect the commutative monoid structure. Specifically, the addition $f + g : R^X \to R^Y$ between morphism $f, g : R^X \to R^Y$ in R-Mat is given by addition of matrices, and the zero element $0 : R^X \to R^Y$ is given by the zero matrix. Furthermore, the tensor product is linear, i.e. it distributes over the addition and respects the zero element:

$$\begin{cases} f \otimes (g+h) & = f \otimes g + f \otimes h \\ (g+h) \otimes f & = g \otimes f + h \otimes f \end{cases} \qquad \begin{cases} f \otimes 0 & = 0 \\ 0 \otimes f & = 0 \end{cases} \tag{2.56}$$

We will use **distributively** CMon-**enriched** to refer to a SMC which is CMon-enriched with linear tensor product. When talking about distributively CMon-enriched †-SMCs, we will furthermore require that the dagger be linear.

It is important to note that the scalars of a distributively CMon-enriched SMC always form a commutative semiring, which in a distributively CMon-enriched †-SMC further comes with an involution given by the dagger. Using enrichment, the discarding maps ⏚$_{R^X}$ can be expressed as follows:



(2.57)

When working in the foundations of quantum theory, the existence and behaviour of classical systems are often entirely taken for granted, and manifest themselves in a variety of ways across the different frameworks and formalisms. In a purely process-oriented framework, such as the one underlying this work, classical systems and processes should be explicitly modelled by the physical theory under investigation, together with their interface with other systems. On these lines, we distil four requirements that any such theory should respect when modelled by a SMC $\mathcal{C}$:

1. the SMC $\mathcal{C}$ has R-Mat (or a category equivalent to it) as a full sub-SMC, where R is the semiring encoding the desired notion of non-determinism (we will refer to this as the **classical subcategory**, and to its objects as the **classical systems**);

2. the SMC $\mathcal{C}$ is distributively CMon-enriched, with scalars forming the semiring R, and the enrichment of $\mathcal{C}$ extends the enrichment defined above for R-Mat;

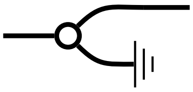
3. the SMC $\mathcal{C}$ comes with a choice of environment structure, extending the environment structure defined above for R-Mat.

We will refer to a SMC satisfying the requirements above as a **R-probabilistic theory**, or simply as a **probabilistic theory** in the case $R = \mathbb{R}^+$. R-probabilistic theories automatically come with a number of handy features built in, amongst which: marginalisation, conditioning, classical control, and convex combination. In this work, we will restrict ourselves to the special case of R-probabilistic CP* categories, but a full discussion of R-probabilistic theories — in connection to the framework of Operational Probabilistic Theories [CDP10, CDP11] — has appeared in [GS16].

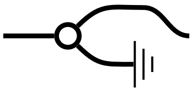
2.6 The CP* construction

2.6.1 The CP* construction and quantum theory

We now wish to construct a R-probabilistic theory from scratch, using Frobenius algebras to define decoherence maps. Let CPM[$\mathcal{C}$] be a CPM category, and let $\circ$ be a canonical symmetric †-SFA (i.e. a symmetric †-SFA in $\mathcal{C}$) on some system A. The **decoherence map** $\mathrm{dec}_{\circ}$ associated to $\circ$ is the process $A \to A$ in CPM[$\mathcal{C}$] defined as follows:

$\mathrm{dec}_{\circ} \quad :=$  (2.58)

Decoherence maps associated to symmetric †-SFAs are always normalised (because of speciality), idempotent (because of associativity and speciality), and self-adjoint (because of Frobenius law, unit laws and symmetry). In the quantum case of CPM[fHilb], decoherence maps take the following form, in terms of the complete family of orthogonal projectors $(p_x)_{x \in X}$ associated to $\circ$:

 $\quad = \quad \rho \mapsto \sum_{x \in X} p_x \, \rho \, p_x$ (2.59)

That is, the decoherence maps defined by symmetric canonical †-SFAs in CPM[fHilb] are exactly the decoherence maps that are traditionally associated with quantum observables (seen as complete families of orthogonal projectors).

The **Karoubi envelope**[20] of a SMC $\mathcal{D}$, which we denote by Split [$\mathcal{D}$], is the SMC defined as follows:

(i) the objects of Split [$\mathcal{D}$] are the pairs (A, e) of an object A of $\mathcal{D}$ and an idempotent morphism $e : A \to A$;

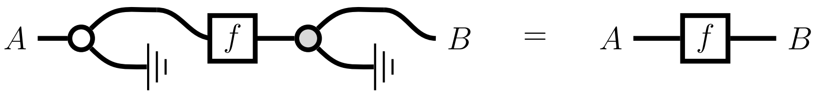
[20] Also known as *idempotent completion*, or *Cauchy completion.*

(ii) the morphisms $(A, e) \to (B, e')$ in Split $[\mathcal{D}]$ are the morphisms $f : A \to B$ in $\mathcal{D}$ which satisfy $e' \circ f \circ e = f$, i.e. which are invariant under pre-composition with e and under post-composition with e';

(iii) composition is inherited from $\mathcal{D}$, while the identity on object (A, e) is the morphism $e : (A, e) \to (A, e)$.

Because $\mathcal{D}$ is a SMC, the Karoubi envelope Split $[\mathcal{D}]$ is also a SMC, and contains $\mathcal{D}$ as the full sub-SMC spanned by the objects in the form (A, id_A).

We now consider the Karoubi envelope Split $[\mathrm{CPM}[\mathcal{C}]]$ and restrict our attention the the full sub-SMC[21] having objects in the form $(A, \mathrm{dec}_{\bigcirc})$, where $\bigcirc$ is a canonical symmetric †-SFA $\bigcirc$ on A. The processes $(A, \mathrm{dec}_{\bigcirc}) \to (B, \mathrm{dec}_{\circledcirc})$ are exactly those satisfying the following condition:



(2.60)

The full sub-SMC of Split $[\mathrm{CPM}[\mathcal{C}]]$ defined above is known in the literature as a **CP* category** [CHK14, CH15], and denoted by $\mathrm{CP}^*[\mathcal{C}]$. Traditionally, CP* categories are constructed as a generalisation of the category of finite-dimensional C*-algebras, using the correspondence with symmetric †-SFAs on fHilb proven by [Vic11]: this is known as the *CP* construction*, and the resulting category is exactly the same as the one we constructed above using decoherence maps and the Karoubi envelope. In the quantum case, these two equivalent ways of constructing $\mathrm{CP}^*[\mathrm{fHilb}]$ reflect different perspectives on the quantum-classical interface:

(a) the decoherence construction we presented gives an operational perspective, showing that $\mathrm{CP}^*[\mathrm{fHilb}]$ is the category of super-selected finite-dimensional quantum systems[22];

(b) the CP* construction gives an algebraic/logical perspective, showing that $\mathrm{CP}^*[\mathrm{fHilb}]$ is the category of finite-dimensional C*-algebras.

Amongst the many objects of the CP* category $\mathrm{CP}^*[\mathrm{fHilb}]$, two particular groups stand out: (a) the objects associated with †-SCFAs (or commutative C*-algebras),

[21] Because decoherence maps obtained from symmetric †-SFAs are self-adjoint, the subcategory is in fact a †-SMC.

[22] This can be seen from Equation 2.59, which expresses the decoherence in terms of the complete family of projectors associated with a quantum observable. The projectors determine the super-selection sectors associated with the observable, and the morphisms between different super-selected quantum systems are exactly the CP maps that respect the super-selection sectors.

corresponding to quantum system with 1-dimensional super-selection sectors; (b) the objects associated with the matrix algebras, corresponding to quantum systems with a single super-selection sector (i.e. which are trivially super-selected). The objects associated with the matrix algebras span a full sub-SMC which is equivalent to CPM[fHilb], and as a consequence CP*[fHilb] is interpreted as an extension of mixed-state quantum theory. The objects associated with †-SCFAs, on the other hand, span a full sub-SMC which is equivalent to $\mathbb{R}^+$-Mat: indeed, if we denote by $K(\circ)$ the set of classical states of a †-SCFA $\circ$, then in CPM[fHilb] the decoherence map $\mathrm{dec}_{\bigcirc}$ takes the following form:

$$\mathrm{dec}_{\bigcirc} = \rho \mapsto \sum_{x \in K(\bigcirc)} |x\rangle\langle x|\, \rho\, |x\rangle\langle x| \tag{2.61}$$

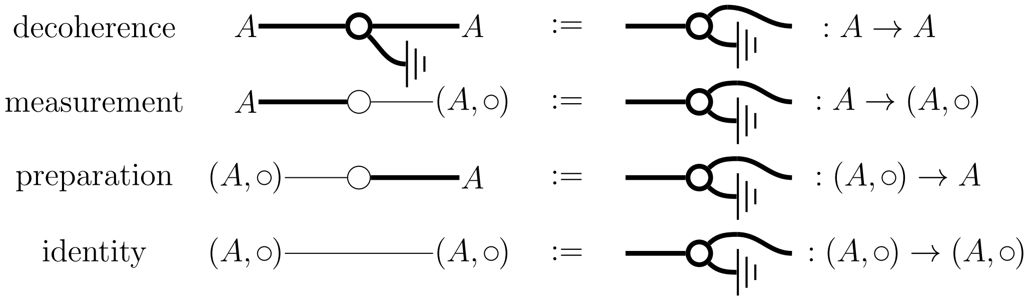
Furthermore, the CPM category CPM[fHilb] is distributively CMon-enriched, and both the enrichment and the discarding maps transfer to CP*[fHilb]: as a consequence, CP*[fHilb] is a probabilistic theory, with classical systems given by objects associated with †-SCFAs.

2.6.2 The CP* construction and R-probabilistic theories

We now go back to Split [CPM[$\mathcal{C}$]] for a generic dagger compact category $\mathcal{C}$. First of all, we tackle a technical issue with the CP* construction: in the quantum case, the CP* category includes the CPM category as the full subcategory given by the quantum systems with trivial super-selection (those associated with the matrix algebras). In general, however, there is no guarantee that the objects associated with the matrix algebras will span a full subcategory of CP*[$\mathcal{C}$] isomorphic to CPM[$\mathcal{C}$]. Here is where our construction and the CP* construction diverge: the latter aims to study a generalisation of the category of finite-dimensional C*-algebras, while our aim is to construct an R-probabilistic theory which **extends** a given physical theory modelled by CPM[$\mathcal{C}$]. As a consequence, we modify the definition of the CP* category.

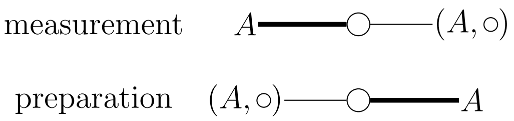
From now on, we redefine CP*[$\mathcal{C}$] to be the full sub-category of Split [CPM[$\mathcal{C}$]] spanned by objects in the form (A, id_A) and objects in the form $(A, \circ)$, with $\circ$ a canonical symmetric †-SFA on A. We refer to objects in the form (A, id_A) as the **CPM systems**, and to objects in the form $(A, \mathrm{dec}_{\bigcirc})$ as the **decohered systems**. Following established conventions, we denote CPM systems (A, id_A) as A, and decohered systems $(A, \mathrm{dec}_{\bigcirc})$ as $(A, \circ)$. The CPM systems always span a full subcategory isomorphic to CPM[$\mathcal{C}$], and we use the doubled notation from CPM categories to denote them and the morphisms between them. Again following established conventions, we use single wires for decohered systems, and single borders for morphisms solely involving decohered systems, while we retain doubled notation for morphisms involving both decohered systems and CPM systems.

If $\circ$ is a canonical symmetric †-SFA on an object A, the decoherence map $\text{dec}_{\bigcirc}$ is always a process $\text{dec}_{\bigcirc} : A \to A$ in $\text{CP}^*[\mathcal{C}]$. Because of idempotence, however, it is also a process $A \to (A, \circ)$ and a process $(A, \circ) \to A$: we will refer to the former as the **measurement** in $\circ$, and the latter as the **preparation** in $\circ$. The single and doubled notation distinguish between the different cases:



(2.62)

Because of idempotence, the measurement and preparation for $\circ$ satisfy the abstract properties defining measurement-preparation pairs in R-probabilistic theories [GS16], save for the fact that we don't yet have an R-probabilistic theory in our hands (and, even if we did, $(A, \circ)$ need not always be a classical system). However, we have already seen that $\text{CP}^*[\text{fHilb}]$ is a probabilistic theory, and we can begin by checking that measurements and preparations as defined above yield the usual notions in the case of quantum theory, when $(A, \circ)$ is a classical system:



$$= \quad \rho \mapsto \Big(\langle x|\rho|x\rangle\Big)_{x\in K(\bigcirc)}$$

$$= \quad x \mapsto |x\rangle\langle x| \tag{2.63}$$

When saying that $\text{CP}^*[\mathcal{C}]$ is an ***R*-probabilistic CP* category**, we will mean that it satisfies the following requirements:

(i) the category $\text{CP}^*[\mathcal{C}]$ is distributively CMon-enriched, with R as its involutive semiring of scalars[23].

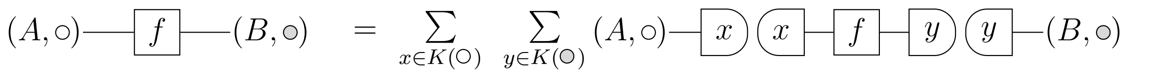
(ii) the **classical systems** are defined to be those decohered systems $(A, \circ)$ where $\circ$ is a †-SCFA with enough classical states, and such that the $\circ$-classical states are orthonormal and form a finite set;

[23] Equivalently, we can ask for $\text{CPM}[\mathcal{C}]$ to be enriched, as the two categories mutually inherit enrichment and discarding maps.

(iii) for each $n \in \mathbb{N}$, there is some classical system $(A, \circ)$ such that the †-SCFA $\circ$ has exactly n classical states.

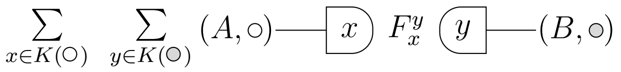
Indeed, processes $(A, \circ) \to (B, \circledcirc)$ between two classical systems in the CP* category form an R-module which is isomorphic to the R-module of processes $R^{K(\circledcirc)} \to R^{K(\circ)}$ in the category R-Mat of classical R-probabilistic systems:

(i) firstly, every process $f : (A, \circ) \to (B, \circledcirc)$ is determined by the R-valued matrix $\big(\langle y|f|x\rangle\big)^{y \in K(\circledcirc)}_{x \in K(\circ)}$ obtained by testing against classical states of the two †-SCFAs:



(2.64)

(ii) secondly, for every matrix $\big(F^y_x\big)^{y \in K(\circledcirc)}_{x \in K(\circ)}$ there is a unique process $(A, \circ) \to (B, \circledcirc)$ corresponding to it:



(2.65)

Hence the full sub-SMC of an R-probabilistic CP* category spanned by the classical systems is equivalent to R-Mat, and our definition of classical systems for a CP* category is consistent with the nomenclature used in R-probabilistic theories.

2.7 Non-locality and contextuality

While generally of interest to understand the background of this work, this section is only directly relevant to the proof of non-locality for generalised Mermin-type arguments, and to the proof of device-independent security for the related quantum-classical secret sharing protocols.

2.7.1 The sheaf-theoretic framework

In the context of this work, **contextuality** and **non-locality** will be used interchangeably, and will be understood in the sense of the sheaf-theoretic framework of [AB14]. Consider the abstract setup of a Bell test:

(i) N parties are given devices $B_1, ..., B_N$ which might share some global state ρ;

(ii) each device B_j takes an input, the **measurement choice**, freely chosen by party j from some finite set M_j;

(iii) upon receiving input $m_j \in M_j$, the device B_j produces some output o_j, the **measurement outcome**, in some finite set O_j;

(iv) no signalling is possible between the devices from before the first input is given to after the last outputs has been produced.

The sheaf-theoretic framework characterises the distribution on joint outputs conditional on joint inputs from the point of view of sheaf theory, showing that non-locality and contextuality are related to the (non-) existence of global sections for a particular presheaf. The framework doesn't rely on any concrete description of the state ρ or the devices $B_1, ..., B_N$, focusing instead on the distributional properties of joint measurement outcomes $\underline{o} := (o_1, ..., o_N)$ conditional to the joint measurement choice $\underline{m} := (m_1, ..., m_N)$.

The framework begins by identifying a finite set $\mathcal{X}$ of inputs, which in the Bell test setup above (the one used in this work) would be $\mathcal{X} = \sqcup_{j=1}^{N} M_j$. The disjoint union preserves information about which party each measurement is associated to, so we will adopt the notation m_j for generic elements of $\mathcal{X}$, where m is the measurement and j is the party. For each subset $U \subseteq \mathcal{X}$, the family of all potential[24] **joint outcomes** takes the following form:

$$\mathcal{E}[U] := \prod_{m_j \in U} O_j \tag{2.66}$$

The powerset $\mathcal{P}(\mathcal{X})$ is a poset (hence a poset category) under inclusion $V \subseteq U$ of subsets. We can define a functor $\mathcal{E} : \mathcal{P}(\mathcal{X})^{\text{op}} \to \text{Set}$, i.e. a **presheaf**, by setting:

(i) if $U \in \mathcal{P}(\mathcal{X})$, then we define $\mathcal{E}[U] := \prod_{m_j \in U} O_j$ as above;

(ii) if $V \subseteq U$, then we define $\mathcal{E}[V \subseteq U] := \text{res}^U_V$ to be the following **restriction map** $U \xrightarrow{\text{Set}} V$:

$$\text{res}^U_V = s \mapsto s|_V \tag{2.67}$$

A **section** s **over** U (or U**-section**) is one in the following form:

$$s = \{(m_j, s(m_j)) \mid m_j \in U\} \in \prod_{m_j \in U} O_j \tag{2.68}$$

The restriction map sends a section s over U to its restriction $s|_V$ over V:

$$s|_V = \{(m_j, s(m_j)) \mid m_j \in V\} \in \prod_{m_j \in V} O_j \tag{2.69}$$

[24] Not all subsets of measurements need be compatible in each concrete scenario: see below for the definition of measurement contexts.

The definition of the set of possible joint inputs requires further consideration: it is a fundamental feature of quantum mechanics that not all measurements on a system are compatible, and we shouldn't expect different measurement choices in each M_j to have a consistent assignment of outcomes. Instead, the framework requires us to specify a set $\mathcal{M}$ of **measurement contexts**, subsets $C \subseteq \mathcal{X}$ of measurements which are mutually compatible (and therefore have a well-defined notion of joint outcome). Even though more general setups are allowed, we will assume that our measurement contexts all take the form $C = \{m_1, ..., m_N\}$ for $m_j \in M_j$, which we will denote by $\underline{m}$: each party chooses exactly one input for their device, but we allow the possibility that not all combinations of inputs might be allowed/interesting. The only requirement is that $\cup_{C \in \mathcal{M}} C = \mathcal{X}$, i.e. that $\mathcal{M}$ be a **global cover** of $\mathcal{X}$ (each measurement choice for each player appears in at least one measurement context), where we consider $\mathcal{X}$ to be endowed with the discrete topology. One can also define the **local covers** for any $U \subseteq \mathcal{X}$ as the families $(U_i)_{i \in I}$ such that $\cup_{i \in I} U_i = U$.

The choice of the discrete topology on $\mathcal{X}$ makes $\mathcal{P}(\mathcal{X})$ its locale of open subsets, and one can define a notion of **sheaf** on it. Because it is defined in terms of sections[25], the presheaf $\mathcal{E}$ is in fact a sheaf on the locale $\mathcal{P}(\mathcal{X})$, and we shall refer to it as the **sheaf of events**. The sheaf of events $\mathcal{E}$ and the measurement cover $\mathcal{M}$ are the two ingredients required to define a **measurement scenario** $(\mathcal{E}, \mathcal{M})$: the former gives the joint measurement outcomes conditional on all possible measurement choices, while the latter specifies the compatible joint measurement choices.

The next step in the framework sees the introduction of generalised notions of probabilities and distributions. In quantum mechanics, probabilities can be seen as taking values in the commutative semiring $\mathbb{R}^+ := (\mathbb{R}^+, +, 0, \cdot, 1)$ of non-negative reals (in fact they fall within the interval $[0, 1]$, a consequence in the semiring $\mathbb{R}^+$ of the normalisation condition requiring that probabilities add up to 1). In other circumstances, one may be interested in the **possibilities** associated with events, living in the commutative semiring $\mathbb{B} = (\{0, 1\}, \vee, 0, \wedge, 1)$ of the booleans. In the sheaf-theoretic treatment of contextuality, one works with an arbitrary commutative semiring $R = (|R|, +, 0, \cdot, 1)$.

Given a set X, an R**-distribution** on X is a function $d : X \to R$ which has finite **support** $\operatorname{supp} d := \{s \in X \mid d(s) \neq 0\}$ and such that:

$$\sum_{s \in \operatorname{supp} d} d(s) = 1 \tag{2.70}$$

[25] Compatibility of local sections amounts to compatibility over the intersection of the domains, and hence compatible local sections can always be glued together.

One can then define a functor $\mathcal{D}_R : \mathrm{Set} \to \mathrm{Set}$ as follows:

(i) for any set X, define $\mathcal{D}_R[X]$ to be the set of R-distributions over X;

(ii) for any function $f : X \to Y$, define $\mathcal{D}_R[f] : \mathcal{D}_R[X] \to \mathcal{D}_R[Y]$ to be the following function:

$$\mathcal{D}_R[f] = d \mapsto \left[t \mapsto \sum_{f(s)=t} d(s) \right] \tag{2.71}$$

Composing this functor with the sheaf of events yields the **presheaf of distributions** $\mathcal{D}_R\mathcal{E} : \mathcal{P}(\mathcal{X})^{\mathrm{op}} \to \mathrm{Set}$, which captures the structure of R-distributions on joint measurement outcomes under marginalisation. The presheaf sends each set U of measurements (the objects of the presheaf category $\mathcal{P}(\mathcal{X})$) to the set $\mathcal{D}_R\mathcal{E}[U]$ of **R-distributions on U-sections**, and sends any inclusion $V \subseteq U$ (the morphisms of the presheaf category $\mathcal{P}(\mathcal{X})$) to the corresponding marginalisation of distributions:

$$\mathcal{D}_R\mathcal{E}[V \subseteq U] = d \mapsto d|_V := \left[t \mapsto \sum_{s|_V=t} d(s) \right] \tag{2.72}$$

We will refer to $d|_V$ as the **marginal** of d. Indeed, $d|_V$ can be manipulated into taking the following, familiar form:

$$t \in \mathcal{E}[V] \implies d|_V(t) := \sum_{s \in \mathcal{E}[V] \text{ s.t. } s|_V=t} d(s) \tag{2.73}$$

In quantum mechanics, if C is a set of compatible measurements on some state ρ, then there is a probability distribution $d \in \mathcal{D}_{\mathbb{R}^+}\mathcal{E}[C]$ on the joint outcomes of the measurements, and the typical contextuality argument involves showing that the probability distributions on different contexts cannot be obtained, in a no-signalling scenario, as marginals of some non-contextual hidden variable. In the sheaf-theoretic framework, a **(no-signalling) empirical model** is defined to be a compatible family of distributions $(\zeta_C)_{C \in \mathcal{M}}$ for the global cover $\mathcal{M}$ of measurement contexts[26]; the usual no-signalling property is shown in [AB14] to be a special case of the compatibility condition. In other literature (usually treating probabilistic models), empirical models for Bell tests are usually given explicitly as conditional (probability) distributions, in a format akin to the following:

$$\zeta_{\underline{m}}(\underline{o}) := \mathbb{P}[\, \underline{o} \,|\, \underline{m} \,] \tag{2.74}$$

[26] A compatible family of distributions $(a_C)_{C \in \mathcal{M}}$ is one such that $a_C|_{C \cap C'} = a_{C'}|_{C \cap C'}$ for all possible pairs of measurement contexts $C, C' \in \mathcal{M}$.

where $\underline{m} = (m_1, ..., m_N) \in \mathcal{M}$ are the measurement contexts used by the scenario and $\underline{o} \in \prod_j O_j$ are the joint outcomes. This is the format we will use in the last section of this work. In the probabilistic case, empirical models for a fixed scenario form a polytope. However, this need not be the same as the no-signalling polytope which is traditionally studied in quantum information theory, because the set of measurement contexts need not include all possible combinations of all possible measurements for each party (i.e. it need not always be the case that $\mathcal{M} = \prod_j M_j$, although it is necessarily the case that $\mathcal{M} \subseteq \prod_j M_j$).

A **global section** for an empirical model[27] $(\zeta_C)_{C\in\mathcal{M}}$ is a distribution $d \in \mathcal{D}_R\mathcal{E}[\mathcal{X}]$ over the joint outcomes of all measurements which marginalises to the distributions specified by the empirical model:

$$d|_C = \zeta_C \text{ for all } C \in \mathcal{M} \tag{2.75}$$

The fundamental observation behind the sheaf-theoretic framework is that the existence of a global section for an empirical model is equivalent to the existence of a **non-contextual hidden variable model** (also known as a **local hidden variable model**). Concretely, the existence of a global section d means that there is a finite set Λ, an R-distribution $q(\lambda) : \Lambda \to R$ and a family of functions $f_j^\lambda : M_j \to O_j$ such that:

$$\zeta_{\underline{m}}(\underline{o}) = \sum_{\lambda\in\Lambda} q(\lambda) \prod_j \delta_{f_j^\lambda(m_j)=o_j} \tag{2.76}$$

We will say that an empirical model $(\zeta_C)_{C\in\mathcal{M}}$ is **contextual** (or **non-local**) if it does not admit a global section.

Contextuality of probabilistic models is interesting in itself, but more refined notions can be obtained by relating $\mathbb{R}^+$ to two other semirings: the reals, modelling signed probabilities, and the booleans, modelling possibilities. Observe that the construction $\mathcal{D}_R$ is functorial in R, so that for any morphism of semirings $r : R \to R'$ we can define the following:

$$\mathcal{D}_r[U] := (d : U \to R) \mapsto (r \circ d : U \to R') \tag{2.77}$$

In particular, there is an injective morphism of semirings $i^+ : \mathbb{R}^+ \hookrightarrow R$ sending $x \in \mathbb{R}^+$ to $x \in \mathbb{R}$, and a surjective morphism of semirings $p : \mathbb{R}^+ \to \mathbb{B}$ sending $0 \mapsto 0$ and $x \mapsto 1$ for all $x > 0$ (the latter mapping is well defined for all positive semirings).

If $(\zeta_C)_{C\in\mathcal{M}}$ is a probabilistic empirical model, i.e. one in the semiring $\mathbb{R}^+$, then $(\zeta_C)_{C\in\mathcal{M}}$ can be seen as an empirical model $(i^+ \circ \zeta_C)_{C\in\mathcal{M}}$ in the semiring $\mathbb{R}$: regardless

[27] From now on, no-signalling is implicitly assumed.

of whether $(\zeta_C)_{C \in \mathcal{M}}$ was contextual or not over $\mathbb{R}^+$, it can be shown [AB14] that over the reals $\mathbb{R}$ it always admits a global section. On the other hand, any probabilistic empirical model $(\zeta_C)_{C \in \mathcal{M}}$ can be assigned a corresponding possibilistic empirical model $(p \circ \zeta_C)_{C \in \mathcal{M}}$ in the semiring $\mathbb{B}$ of the booleans (and each boolean function $p \circ \zeta_C$ can equivalently be seen as the characteristic function of the subset $\operatorname{supp} \zeta_C \subseteq \mathcal{E}[C]$).

Note that contextuality is a contravariant property with respect to change of semiring: if $(\zeta_C)_{C \in \mathcal{M}}$ is an empirical model in a semiring R and $r : R \to R'$ is a morphism of semirings, then contextuality of $(r \circ \zeta_C)_{C \in \mathcal{M}}$ implies contextuality of $(\zeta_C)_{C \in \mathcal{M}}$ (because a global section d of the latter is mapped to a global section $r \circ d$ of the former). We will say that a probabilistic empirical model $(\zeta_C)_{C \in \mathcal{M}}$ is **possibilistically contextual** if the corresponding possibilistic model $(p \circ \zeta_C)_{C \in \mathcal{M}}$ is contextual (as opposed to **probabilistically contextual**, which we use to say that $(\zeta_C)_{C \in \mathcal{M}}$ is contextual over $\mathbb{R}^+$). Because of contravariance, possibilistic contextuality implies probabilistic contextuality, but the opposite is not true: the Bell model given in [AB14] is probabilistically contextual but not possibilistically contextual.

Seeing distributions $d \in \mathcal{D}_{\mathbb{B}}\mathcal{E}[U]$ as indicator functions of the subsets $\operatorname{supp} d \subseteq \mathcal{E}[U]$ endows them with a partial order:

$$d' \preceq d \text{ if and only if } \operatorname{supp} d' \subseteq \operatorname{supp} d \tag{2.78}$$

The existence of a global section $d \in \mathcal{D}_{\mathbb{B}}\mathcal{E}[U]$ for a possibilistic empirical model $(\zeta_C)_{C \in \mathcal{M}}$ implies that:

$$d|_C \preceq \zeta_C \text{ for all } C \in \mathcal{M} \tag{2.79}$$

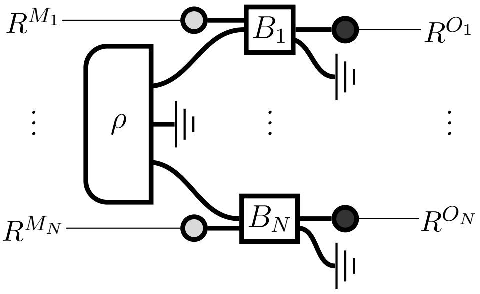
We say that a possibilistic empirical model $(\zeta_C)_{C \in \mathcal{M}}$ is **strongly contextual** if there is no distribution $d \in \mathcal{D}_{\mathbb{B}}\mathcal{E}[\mathcal{X}]$ such that Equation 2.79 holds. In particular, the GHZ model given in [AB14], corresponding to Mermin's original non-locality argument, is strongly contextual. Because of Equation 2.78, strong contextuality implies contextuality, but the opposite is not true: the possibilistic Hardy model give in [AB14] is possibilistically contextual, but not strongly contextual. We will say that a probabilistic empirical model is strongly contextual if the associated possibilistic empirical model is strongly contextual, yielding the following hierarchy of notions of contextuality for probabilistic empirical models:

$$\text{probabilistically contextual} \Leftarrow \text{possibilistically contextual} \Leftarrow \text{strongly contextual} \tag{2.80}$$

2.7.2 Contextuality in R-probabilistic theories

The relevance of the sheaf-theoretic framework to this work stems from the following result: in any R-probabilistic theory, Bell tests give rise to no-signalling empirical models (with R-distributions) in the sheaf-theoretic framework, which can be used to prove contextuality/non-locality of the tests independently of the specific theory. As mentioned before, we will be interested in the CP* case, but the definitions below straightforwardly extend to arbitrary R-probabilistic theories.

Definition 2.6. *A **Bell test** in an R-probabilistic CP* category is a process in the following form, for some normalised state ρ and some normalised processes $B_1, ..., B_N$:*

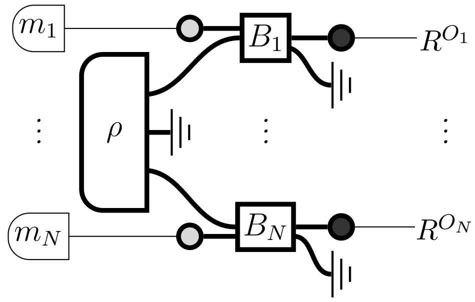


(2.81)

We have denoted by M_j the set of classical states for each classical input system $(\mathcal{H}_j, \circ_j)$, and by O_j the set of classical states for each classical output system $(\mathcal{K}_j, \bullet_j)$.

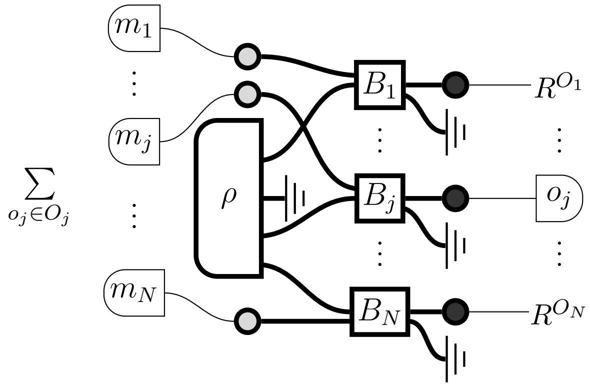
Theorem 2.7 (Bell tests and sheaf-theoretic non-locality [GS16]). *Bell tests in R-probabilistic CP* categories give rise to R-valued no-signalling empirical models $(\zeta_{\underline{m}})_{\underline{m} \in \mathcal{M}}$ as follows, for any measurement cover $\mathcal{M}$:*

$\zeta_{\underline{m}} \quad :=$



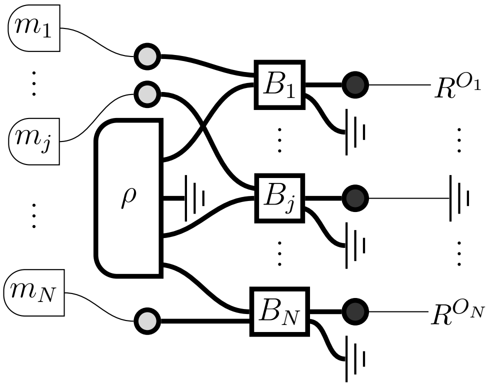
$\in \quad \mathcal{D}_R\mathcal{E}[\underline{m}]$ (2.82)

Proof. All we need to show is that the states in Equation 2.82 (indexed by the measurement contexts $\underline{m} \in \mathcal{M}$) satisfy no-signalling and are normalised. Marginalising over party j yields the following state, which we want to prove independent of m_j:



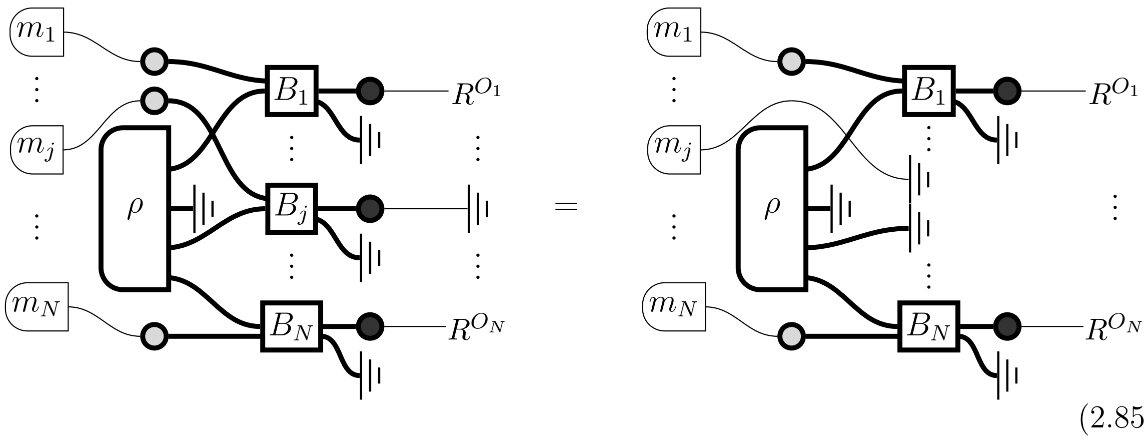
(2.83)

The discarding map on the classical output systems $(\mathcal{K}, \bullet_j)$ can be written as $\overline{\top}_{(\mathcal{K}_j,\bullet_j)} = \sum_{o_j}\langle o_j|$ in terms of the classical states $(|o_j\rangle)_{o_j\in O_j}$ of $\bullet_j$. Hence the marginalised state in Diagram 2.83 can be rewritten as follows:



(2.84)

Because the $\bullet_j$ measurement, the process B_j and the $\circ_j$ preparation are all normalised, we conclude that the state of Diagram 2.83 is independent of m_j:



(2.85)

Marginalising over all outputs leaves us with $\overline{\top} \circ \rho$, which equals 1 (independently of the measurement context $\underline{m}$) since ρ is normalised. Hence the state of Diagram 2.84 is also an R-distribution, completing our proof that Bell tests always give rise to no-signalling empirical models. □

Theorem 2.8 (**Locality of R-probabilistic theories over fields**). *If R is a field, then all R-probabilistic CP* categories are local.*

Proof. Theorem 5.4 from Ref. [AB14] states that all no-signalling empirical models over the signed-probability field $\mathbb{R}$ admit a local hidden variable model in terms of signed probabilities. Although the original result was proven for $\mathbb{R}$, close inspection reveals that it holds for no-signalling empirical models over any field R: as a consequence, Bell-type measurement scenarios in R-probabilistic theories where R is a field give rise to no-signalling empirical models admitting local hidden variable models. Finally, R-probabilistic theories have a sub-SMC of finite R-probabilistic classical systems, with all R-distributions as normalised states and all R-stochastic maps as normalised processes: as a consequence, all local hidden variable models valued in R can be realised in any and all of them. □

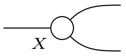
2.8 Some toy models of quantum theory

In this Section, we present a number of toy models of quantum theory constructed using the framework for R-probabilistic CP* categories presented above. These examples are taken from the very recent [Gog17].

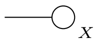
2.8.1 Theories of wavefunctions over semirings

Note that two different linear structures intervene in the definition of quantum theory: the $\mathbb{C}$-linear structure of wavefunctions, modelling superposition, interference and phases, and the $\mathbb{R}^+$-linear structure of probability distributions over classical systems. We have already seen that the framework of R-probabilistic theories replaces the probability semiring $\mathbb{R}^+$ with a more general commutative semiring R as a model of classical non-determinism. In this Section, we construct a large class of toy models of quantum theory by considering theories of wavefunctions with amplitudes valued in some commutative semiring with involution S, generalising the field with involution $\mathbb{C}$ traditionally used in quantum mechanics. To do so, we consider the dagger compact category S-Mat (dagger and compact closed structure will be defined using the involution), and we require classical non-determinism to arise via the Born rule, as embodied by the CP* construction. The corresponding quantum-classical theory will therefore be modelled by CP*[S-Mat], and the main result of this Section (Theorem 2.10) will show that this is an R-probabilistic theory (where R the sub-semiring of positive elements of S, see Definition 2.9 below).

The category S-Mat for a commutative semiring with involution S is defined as in the previous Section, but it comes with additional structure. Indeed, we can define dagger and compact closed structures on S-Mat exactly as done in fHilb (which is $\mathbb{C}$-Mat), with conjugation taken using the involution * of S in place of complex conjugation. Each object S^X in S-Mat comes with at least one orthonormal basis $|x\rangle_{x \in X}$, as well as an associated special commutative †-Frobenius algebra $\circ_X$:

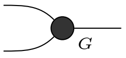


$$= \sum_{x \in X} |x\rangle \otimes |x\rangle \otimes \langle x|$$

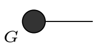


$$= \sum_{x \in X} \langle x| \qquad (2.86)$$

For any group structure $G = (X, \cdot, 1)$ on any finite set X, one also obtains an associated †-Frobenius algebra $\bullet_G$ on S^X by linearly extending the group multiplication and unit:

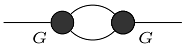


$$= \sum_{x,y \in X} |x \cdot y\rangle \otimes \langle x| \otimes \langle y|$$

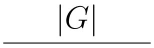


$$= \quad |1\rangle \qquad (2.87)$$

The †-Frobenius algebra is commutative if and only if the group is, and it always satisfies the following:



$$=$$



$$(2.88)$$

Unfortunately, $\bullet_G$ is not quasi-special (a.k.a. normalisable) unless the scalar $|G|$ takes the form $z_G^* z_G$ for some $z_G \in S$ which is multiplicatively invertible: when this is the case, however, we have a legitimate strongly complementary pair $(\circ_X, \bullet_G)$ in S-Mat corresponding to the finite group G (see next Chapter). When G is abelian these strongly complementary pairs can be used (under additional conditions) to implement quantum protocols such as the algorithm to solve the abelian Hidden Subgroup Problem [Vic12b, GK17] or generalised Mermin-type arguments [GZ15b, GZ17] (see Chapter 4). This also means that certain objects in S-Mat support fragments of the ZX calculus[28] [CD11, Bac14], opening the way to the application of well-established diagrammatic techniques to reason in these categories.

In quantum theory, the probabilistic semiring $\mathbb{R}^+$ arises as a sub-semiring of $\mathbb{C}$ fixed by complex conjugation, namely the sub-semiring of those elements $z \in \mathbb{C}$ taking the form $z = x^* x$: this is, essentially, a hallmark of the Born rule. In general commutative semirings with involution, elements in the form $x^* x$ need not be closed under addition, but it is true their closure under addition always form a semiring.

[28] To be precise, they always support the spider rules (but cups/caps for the two algebras are generally distinct), the bialgebra rules, the Hopf laws (with non-trivial antipode), the copy rules, and a generalised version of the π-copy rules (see [Bac14]). A Hadamard unitary can be defined if and only if the S-valued unitary multiplicative characters for G form an orthonormal basis for S^X, and in this case the colour-change rules are also supported (taking care, where relevant, to consider the adjoint of the Hadamard in place of the Hadamard itself).

Definition 2.9. *Let S be a commutative semiring with involution. Then we define its* ***sub-semiring*** *R* ***of positive elements*** *in S to be the closure under addition in S of the subset $\{x^* x \mid x \in S\}$.*

When classical non-determinism is introduced via the Born rule, quantum theory naturally gives rise to a probabilistic theory. Similarly, it is possible to prove that any theory of wavefunctions valued in a commutative semirings with involution S gives rise to an R-probabilistic theory, where R is the corresponding sub-semiring of positive elements.

Theorem 2.10. *Let S be a commutative semiring with involution, and let R be its sub-semiring of positive elements. Then* $\mathrm{CP}^*[S\text{-Mat}]$ *is R-probabilistic under the* CMon*-enrichment inherited from* S-Mat.

Proof. In order for $\mathrm{CP}^*[S\text{-Mat}]$ to be R-probabilistic under the CMon-enrichment of S-Mat, we need to show that it satisfies the following three conditions:

(i) there is a full sub-SMC $\mathrm{CP}^*[S\text{-Mat}]_K$ which is equivalent to R-Mat;

(ii) the CMon-enrichment of S-Mat must restrict to a well-defined enrichment for $\mathrm{CP}^*[S\text{-Mat}]$, coinciding on $\mathrm{CP}^*[S\text{-Mat}]_K$ with the enrichment of R-Mat;

(iii) the SMC $\mathrm{CP}^*[S\text{-Mat}]$ comes with an environment structure which restricts to the the canonical one from R-Mat on the full subcategory $\mathrm{CP}^*[S\text{-Mat}]_K$.

Firstly, we show that the CMon-enrichment of S-Mat restricts to a well-defined CMon-enrichment for $\mathrm{CP}^*[S\text{-Mat}]$. Because S-Mat is a category of matrices, this is in turn true if and only if the scalars of $\mathrm{CP}^*[S\text{-Mat}]$ are closed under addition in S-Mat, i.e. if and only if they form a sub-semiring of S (they are always necessarily closed under multiplication). To see that this is true, it suffices to show that the scalars of $\mathrm{CP}^*[S\text{-Mat}]$ form exactly the sub-semiring R of positive elements of S (we have to show it anyway, if we want our theory to be R-probabilistic!). Indeed, the generic scalar of $\mathrm{CP}^*[S\text{-Mat}]$ takes the form $\overset{-}{\top}_{S^D} \circ \mathbf{double}\,[|\psi\rangle] = \sum_{d=1}^{D} p_d^* p_d$ for a generic state $|\psi\rangle := \sum_{d=1}^{D} p_d |d\rangle$ of S-Mat.

For condition (i), consider the full-subcategory $\mathrm{CP}^*[S\text{-Mat}]_K$ of $\mathrm{CP}^*[S\text{-Mat}]$ spanned by those objects in the form $(S^X, \mathrm{dec}_{\bigcirc_X})$, where X is a finite set, $\bigcirc_X$ is the special commutative †-Frobenius algebra on S^X associated with the orthonormal basis $|x\rangle_{x \in X}$, and $\mathrm{dec}_{\bigcirc_X} : S^X \to S^X$ is the decoherence map for $\bigcirc_X$, which is a self-adjoint idempotent normalised CP map. Morphisms $(S^X, \mathrm{dec}_{\bigcirc_X}) \to (S^Y, \mathrm{dec}_{\bigcirc_Y})$ are exactly those in the following form, where $(f_{xy})_{x \in X, y \in Y}$ is an arbitrary matrix of scalars (i.e. elements of R):

$$\sum_{y \in Y} \sum_{x \in X} \mathbf{double}\left[|y\rangle\right]\ f_{xy}\ \mathbf{double}\left[\langle x|\right] \tag{2.89}$$

As a consequence, $\mathrm{CP}^*[S\text{-Mat}]_K$ is equivalent to R-Mat. Condition (ii) is satisfied as well. For condition (iii), it suffices to consider the canonical environment structure given by the CP^* construction. Because decoherence maps are normalised, this environment structure restricts to the canonical one on $\mathrm{CP}^*[S\text{-Mat}]_K$. □

Note that the scalars of $\mathrm{CP}^*[S\text{-Mat}]$ are the elements of R, and that the pure scalars are those in the form $\xi^*\xi$ for some $\xi \in S$: as a consequence, not all scalars of $\mathrm{CP}^*[S\text{-Mat}]$ need be pure (in contrast to what happens with ordinary quantum theory). In what follows, we will try as much as possible to construct theories where all scalars are pure, but there are examples (such as the case of p-adic quantum theory) where this cannot be achieved. When all scalars are pure, the requirement that $|G| = z_G^* z_G$ is always automatically satisfied for all finite groups G, and we only need to care about $|G|$ being invertible as a scalar in S (a fact which always holds true whenever S is a semi-field/field and $|G|$ is non-zero in S). We will now proceed to construct a number of toy models within this framework.

2.8.2 Real quantum theory

The simplest non-conventional example is given by the ring $\mathbb{R}$ of signed reals (with the trivial involution), which yields the **probability semiring** $\mathbb{R}^+$ as its sub-semiring of positive elements; in particular, all positive elements are pure scalars. The corresponding probabilistic theory $\mathrm{CP}^*[\mathbb{R}\text{-Mat}]$ is known as **real quantum theory** [JNW34, Bae12, BDP13, Wil16]: it is arguably the most well-studied of the quantum-like theories, and the closest to ordinary quantum theory. Thus said, real quantum theory can be distinguished from ordinary quantum theory because it fails to be *locally tomographic* [Ara80, Wot90, CDP10], i.e. bipartite (mixed) states in real quantum theory cannot in general be distinguished by product measurements alone. Equivalently, one can check that the CP maps $\mathbf{double}\left[\sigma_x\right] + \mathbf{double}\left[\sigma_z\right] - \mathbf{double}\left[id_{\mathbb{R}^2}\right]$ and $\mathbf{double}\left[\sigma_y\right]$ on $\mathbb{R}^2$ in $\mathrm{CPM}[\mathbb{R}\text{-Mat}]$ cannot be distinguished by applications to mixed states of $\mathbb{R}^2$ alone, because the latter are described by density matrices which are always real symmetric[29].

[29] By σ_x, σ_y and σ_z we have denoted the complex qubit Pauli matrices, which give rise to real CP maps on $\mathbb{R}^2$ when doubled.

The group of phases in $\mathbb{R}$ is $\{\pm 1\} \cong \mathbb{Z}_2$, and non-trivial interference is possible in real quantum theory. For example, each of the Pauli X eigenstates $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ of the qubit $\mathbb{R}[\mathbb{Z}_2]$ in real quantum theory yields the uniform distribution when measured in the Pauli Z basis $|0\rangle, |1\rangle$, but their superposition $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ yields the outcome corresponding to $|0\rangle$ with certainty.

Finally, Bell's theorem goes through in real quantum theory (as it only involves states and measurements on the ZX greater circle of the Bloch sphere), and the latter is a non-local probabilistic theory (because the states and processes of real quantum theory are a subset of those of quantum theory).

2.8.3 Relational quantum theory

Examples of an entirely different nature are given by considering distributive lattices Ω (with the trivial involution), which yield themselves back as their sub-semirings of positive elements (because of multiplicative idempotence); in particular, all positive elements are pure scalars. Distributive lattices seem to be almost as far as one can go from the probabilistic semiring $\mathbb{R}^+$, but the category Ω-Mat has been studied extensively as a toy model of quantum theory (especially in the boolean case $\Omega = \mathbb{B}$) [Pav09, AH12b, EDLP09, Zen15, CE12], and the corresponding CPM category has also received some attention on its own [Mar, Gog15c]. We refer to the corresponding Ω-probabilistic (or **possibilistic**) theory as **relational quantum theory**.

The group of phases in Ω is the singleton $\{1\}$, and no interference is possible in relational quantum theory. Relational quantum theories also feature very few quantum-to-classical transitions: there is a unique basis on each system, namely the one given by the elements of the underlying set. They are local tomographic on pure states, but they fail to be tomographic altogether on mixed states: for example, the pure state $|\psi\rangle\langle\psi|$ for $|\psi\rangle := |0\rangle + |1\rangle$ and the mixed state $|0\rangle\langle 0| + |1\rangle\langle 1|$ are distinct, but cannot be distinguished by measurement. In fact, a characteristic trait of relational quantum theories is exactly that superposition and mixing are essentially indistinguishable (because of idempotence) [AH12b, Mar, Gog15c], and this can be used to show that relational quantum theories are entirely local [AH12b, Gog15c].

2.8.4 Hyperbolic quantum theory

Turning our attention back to real algebras, we can consider the commutative ring of **split complex numbers** $\mathbb{C}[\sqrt{1}] := \mathbb{R}[X]/(X^2 - 1)$, a two-dimensional real algebra. Split complex numbers take the form $(x + jy)$, where $x, y \in \mathbb{R}$ and $j^2 = 1$; in particular, they have non-trivial zero-divisors in the form $a(1\pm j)$, because $(1+j)(1-j) = 1-j^2 = 0$. They come with the involution $(x+jy)^* := x-jy$, which yields the **signed-probability ring** $\mathbb{R}$ as sub-semiring of positive elements; in particular, all positive elements are pure scalars. We refer to the corresponding $\mathbb{R}$-probabilistic (or **quasi-probabilistic**) theory $\mathrm{CP}^*[\mathbb{C}[\sqrt{1}]\text{-Mat}]$ as **hyperbolic quantum theory**[30] [Khr03, Khr10, Nym11]. Because scalars form a field, Theorem 2.8 (and the original Theorem 5.4 from [AB14]) implies that hyperbolic quantum theory is a local theory.

The group of phases in $\mathbb{C}[\sqrt{1}]$ consists of the elements with square norm 1, i.e. the elements in the form $x + jy$ which lie on the following unit hyperbola of the real plane:

$$1 = (x + jy)^*(x + jy) = x^2 - y^2 \tag{2.90}$$

In fact, the natural geometry for the split complex numbers is that of the real plane endowed with the Lorentzian metric $-dy^2 + dx^2$, i.e. that of the Minkowski plane. Just like multiplication by phases in $\mathbb{C}$ forms the circle group $U(1)$ of rotations around the origin for the Euclidean plane, multiplication by phases in $\mathbb{C}[\sqrt{1}]$ forms the group $SO(1,1)$ of orthochronous homogeneous Lorentz transformations for the Minkowski plane, and we have the isomorphism of Lie groups $\mathbb{Z}_2 \times \mathbb{R} \cong SO(1,1)$ given by $(s,\theta) \mapsto s(\cosh(\theta) + j\sinh(\theta))$.

hyperbolic quantum theory is a local theory, in the sense that every empirical model arising in hyperbolic quantum theory admits a local hidden variable model in terms of signed probabilities (the notion of classical non-determinism for hyperbolic quantum theory) [AB14]. While signed probabilities might at first sound unphysical, an operational interpretation exists in terms of unsigned probabilities on signed events [AB14][31].

2.8.5 Parity quantum theory

A simple variation on relational quantum theory (over the booleans) is given by using symmetric difference of sets, instead of union, as the superposition operation. This leads us to consider the finite field with two elements $\mathbb{Z}_2 := (\{0,1\}, +, 0, \times, 1)$, with trivial involution, in place of the booleans $\mathbb{B} := (\{0,1\}, \vee, 0, \times, 1)$, also with trivial involution. The multiplication is the same, but addition is now non-idempotent, and superposition is no longer the same as mixing. The **parity semiring** $\mathbb{Z}_2$ yields itself

[30] Clifford referred to functions of split complex numbers as "functions of a motor variable" [Cli71], so we could say that hyperbolic quantum theory is the theory of **wavefunctions of a motor variable** (how does **motor quantum theory** sound?).

[31] Where the sign of the events themselves cannot be observed, yielding an epistemic restriction which is not too far removed from the one which originally motivated Spekkens's toy model [Spe07, CB17]

back as its sub-semiring of positive elements (in particular, all positive elements are pure scalars), and we refer to the corresponding $\mathbb{Z}_2$-probabilistic theory $\mathrm{CP}^*[\mathbb{Z}_2\text{-Mat}]$ as **parity quantum theory**.

Remark 2.11. *Because the involution is trivial, parity quantum theory as defined here pretty much coincides with the $\mathbb{Z}_2$ case of modal quantum theory [Shu12, Shu16], but it should be noted that the philosophical interpretation of $\mathbb{Z}_2$-valued probabilities is significantly different. In modal quantum theory, the interest is in generating possibilistic tables by using finite fields, subsequently interpreting all zero values as the boolean* 0 *and all non-zero values as the boolean* 1*. In parity quantum theory, the non-determinism itself is interpreted to be natively $\mathbb{Z}_2$-valued, and no attempt is made to translate the resulting empirical models into possibilistic ones. Indeed, such an interpretation would not be natural within our semiring-oriented framework, as no semiring homomorphism can exists from any finite field into the booleans.*

The group of phases in $\mathbb{Z}_2$ is the singleton $\{1\}$, but interference is still possible in parity quantum theory: this somewhat counter-intuitive situation is made possible by the fact that 1 is its own additive inverse in $\mathbb{Z}_2$, so that triviality of the group of phases is slightly deceptive. Indeed, consider the four two-qubit states below, which form an orthonormal basis for $\mathbb{Z}_2^2$:

$$\begin{aligned} |\psi_{012}\rangle &:= |00\rangle + |01\rangle + |10\rangle \qquad & |\psi_{123}\rangle &:= |01\rangle + |10\rangle + |11\rangle \\ |\psi_{230}\rangle &:= |10\rangle + |11\rangle + |00\rangle \qquad & |\psi_{301}\rangle &:= |11\rangle + |00\rangle + |01\rangle \end{aligned} \tag{2.91}$$

For example, we have $|10\rangle = |\psi_{012}\rangle + |\psi_{123}\rangle + |\psi_{230}\rangle$. When measured in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, the normalised states $|01\rangle$, $|10\rangle$ and $|\psi_{012}\rangle$ all have non-zero $\mathbb{Z}_2$-probability of yielding an outcome in the set $\{01, 10\}$, but their superposition $|01\rangle + |10\rangle + |\psi_{012}\rangle = |00\rangle$ (also a normalised state) has zero $\mathbb{Z}_2$-probability of yielding an outcome in that set.

R-probabilistic theories can be similarly constructed for modal quantum theory over any other finite field $\mathbb{F}_{p^n}$ [Shu12, Shu16], by taking $S := \mathbb{F}_{p^n}$ with the trivial involution. However, these theories have a lot of non-pure scalars—namely the $(p^n - 1)/2$ non-squares in $\mathbb{F}_{p^n}$—and their phases are close to trivial—namely they are $\{\pm 1\}$ if $p > 2$ and $\{1\}$ if $p = 2$. Instead, we will consider a more sophisticated construction based on quadratic extensions of finite fields, which we call "finite-field quantum theory".

What will make finite-field quantum theory extremely attractive for CQM is the fact that it is a local theory (by Theorem 2.8), in which it is nonetheless possible to formulate non-trivial quantum algorithms (such as the one solving the abelian

Hidden Subgroup Problem), as well as non-trivial “non-locality” arguments (such as generalised Mermin-type arguments). This is in stark contrast with the more traditional toy models based on relational quantum theory, in which the quantum Fourier transform cannot be performed for non-trivial groups [GZ15a],precluding the implementation of algorithms based on it, and in which all Mermin-type arguments are necessarily trivial [CDKW12, GZ15b] (see Chapter 4).

2.8.6 Finite-field quantum theory

Consider a finite field $\mathbb{F}_{p^n}$ (with p odd), and let ϵ be a generator for the cyclic group $\mathbb{F}_{p^n}^\times$ of invertible (aka non-zero) elements in $\mathbb{F}_{p^n}$ (i.e. a primitive element for $\mathbb{F}_{p^n}$). We consider the ring $\mathbb{F}_{p^n}[\sqrt{\epsilon}] := \mathbb{F}_{p^n}[X^2 - \epsilon]$, equipped with the involution $(x + y\sqrt{\epsilon})^* := (x - y\sqrt{\epsilon})$: because ϵ is a primitive element, $\mathbb{F}_{p^n}(\sqrt{\epsilon}) \cong \mathbb{F}_{p^{2n}}$ is a field. We are in fact working with the quadratic extension of fields $\mathbb{F}_{p^n}(\sqrt{\epsilon})/\mathbb{F}_{p^n}$, equipped with the usual involution and (squared) norm:

$$\left|x + y\sqrt{\epsilon}\right|^2 = (x - y\sqrt{\epsilon})(x + y\sqrt{\epsilon}) = x^2 - \epsilon y^2 \tag{2.92}$$

The sub-field $\mathbb{F}_{p^n}$ (given by the elements in the form $x + 0\sqrt{\epsilon}$) is the sub-semiring of positive elements (and we will shortly see that all positive elements are pure scalars).

The phases in $\mathbb{F}_{p^n}(\sqrt{\epsilon})$ are the points (x, y) of the $\mathbb{F}_{p^n}^2$ plane lying on the unit hyperbola $x^2 - \epsilon y^2 = 1$, which does not factor as a product of two lines because ϵ is a primitive element. The following iconic result of Galois theory due to Hilbert can be used to characterise them (see e.g. [Hil98] for a proof).

Theorem 2.12 (Hilbert’s Theorem 90).
Let L/K be a finite cyclic field extension, and let $\sigma : L \to L$ be a generator for its cyclic Galois group. Then the multiplicative group of elements $\xi \in L$ of unit relative norm $N_{L/K}(\xi) = 1$ is isomorphic to the quotient group $L^\times/K^\times$.

Corollary 2.13. *The phases in $\mathbb{F}_{p^n}(\sqrt{\epsilon})$ form the cyclic group $\mathbb{F}_{p^{2n}}^\times/\mathbb{F}_{p^n}^\times \cong \mathbb{Z}_{p^n+1}$.*

Proof. We have a quadratic extension $\mathbb{F}_{p^n}(\sqrt{\epsilon})/\mathbb{F}_{p^n}$, with 2-element Galois group generated by the involution $\sigma := \xi \mapsto \xi^*$, and corresponding field norm $N_{\mathbb{F}_{p^n}(\sqrt{\epsilon})/\mathbb{F}_{p^n}}(\xi) := \xi^*\xi$. By Hilbert’s Theorem 90, the multiplicative group of those $\xi \in \mathbb{F}_{p^{2n}}$ such that $\xi^*\xi = 1$ is isomorphic to the quotient group $\mathbb{F}_{p^n}(\sqrt{\epsilon})^\times/\mathbb{F}_{p^n}^\times$. But $\mathbb{F}_{p^n}(\sqrt{\epsilon})^\times \cong \mathbb{F}_{p^{2n}}^\times$ is cyclic with $p^{2n} - 1$ elements, and $\mathbb{F}_{p^n}^\times$ has $p^n - 1$ elements: hence the quotient is cyclic with $(p^{2n} - 1)/(p^n - 1) = p^n + 1$ elements, i.e. it is $\mathbb{Z}_{p^n+1}$. □

Another interesting consequence of Hilbert's Theorem 90 is the fact that the positive elements in finite-field quantum theory are all pure scalars.

Lemma 2.14. *All scalars in* $\mathrm{CP}^*[\mathbb{F}_{p^n}(\sqrt{\epsilon})\text{-Mat}]$ *are pure.*

Proof. Because $\mathbb{F}_{p^n}(\sqrt{\epsilon})$ is a field, we have that $a^*a = b^*b$ if and only if $a = \xi b$ for some ξ such that $\xi^*\xi = 1$, i.e. for some phase ξ. Equality up to phase is an equivalence relation on elements of $\mathbb{F}_{p^n}(\sqrt{\epsilon})$ (because phases form a group under multiplication), and there are exactly $p^n + 1$ phases by Corollary 2.13: as a consequence, there are exactly $(p^{2n} - 1)/(p^n + 1) = p^n - 1$ non-zero pure scalars in $\mathrm{CP}^*[\mathbb{F}_{p^n}(\sqrt{\epsilon})\text{-Mat}]$, i.e. all the scalars are in fact pure (since the zero scalar always is). □

While finite-field quantum theory and parity quantum theory might not have as direct a physical interpretation as hyperbolic quantum theory and relational quantum theory, they have the major advantage of dealing with wavefunction valued over a field, so that objects are finite-dimensional vector spaces (equipped with a non-standard inner product, in the case of finite-field quantum theory). This opens the door for a systematic study of quantum systems in these theories using standard tools from finite geometry. Further investigation in this direction is left to future work.

2.8.7 p-adic quantum theory

We now look at the construction of ***p*-adic quantum mechanics** [VV89, RTVW89, Khr91, Khr93, Pal16a, Pal16b], where $R := Q_p$ is the field of p-adic numbers, and S is some quadratic extension. In this Section, we will use the notation Q_p to denote the p-adic numbers, and Z_p to denote the p-adic integers, to distinguish them from the finite field $\mathbb{Z}_p$ of integers modulo p; note that this convention is different from the one used in many texts on p-adic arithmetic, where $\mathbb{Z}_p$ is used for the p-adic integers (and $\mathbb{Q}_p$ for the p-adic numbers).

When $p > 2$, the p-adic numbers $x := p^{\operatorname{ord} x} \sum_{i=0}^{+\infty} x_i p^i$ fall within four distinct quadratic classes—jointly labelled by the parity of the order $\operatorname{ord} x \in \mathbb{Z}$ and by the quadratic class of the first non-zero digit $x_0 \in \mathbb{Z}_p^\times$—and there are three corresponding inequivalent quadratic extensions. This means that there is no way to obtain all positive elements as pure scalars by a single quadratic extension. This would seem to indicate that mixed states play a necessary role in the emergence of p-adic probabilities, which cannot all be obtained from pure states alone: the potential physical significance of this observation might become the topic of future work.

We consider the quadratic extension $S := Q_p(\sqrt{\epsilon})$, where $p \geq 3$ and ϵ is a primitive element in the field $\mathbb{Z}_p$ of integers modulo p, and we follow the presentation of [RTVW89]. A generic element of $Q_p(\sqrt{\epsilon})$ takes the form $c + s\sqrt{\epsilon}$, for $c, s \in Q_p$, and its square norm is $|c+s\sqrt{\epsilon}|^2 = (c-s\sqrt{\epsilon})(c+s\sqrt{\epsilon}) = c^2 - \epsilon s^2$. Whether an element $x \in Q_p$ can be written in this form, i.e. whether it is a pure scalar in $\mathrm{CP}^*[Q_p(\sqrt{\epsilon})\text{-Mat}]$, is determined by the *sign function* $\mathrm{sgn}_\epsilon\, x$, which takes the value $+1$ if $x = c^2 - \epsilon s^2$ for some $c, s \in Q_p$, and the value -1 otherwise. An explicit form for the sign function (in the $p \neq 2$ case) is given by Equation (2.34) of [RTVW89], which specialised to our case ($\tau = \epsilon$ and $\mathrm{ord}\,\tau = 0$) reads $\mathrm{sgn}_\epsilon\, x = (-1)^{\mathrm{ord}\, x}$. Hence the pure scalars in $\mathrm{CP}^*[Q_p(\sqrt{\epsilon})\text{-Mat}]$ are exactly the p-adic numbers x with even order $\mathrm{ord}\, x$; closure of this set under addition yields $R := Q_p$ as sub-semiring (field, in fact) of positive elements in $S := Q_p(\sqrt{\epsilon})$.

The phases in p-adic quantum theory are those $\xi := (c + s\sqrt{\epsilon}) \in Q_p(\sqrt{\epsilon})$ such that $\xi^*\xi = c^2 - \epsilon s^2 = 1$. In [RTVW89] (Equation (4.35) of Section IV.C, and Equation (C12b) of Appendix C.3) it is shown that phases form a multiplicative group C_ϵ isomorphic to the additive group $\mathbb{Z}_{p+1} \times pZ_p$—here $(\mathbb{Z}_{p+1}, +, 0)$ are the integers modulo $p+1$, while $(pZ_p, +, 0)$ is the additive subgroup of Z_p formed by those p-adic integers which are divisible by p. In particular, C_ϵ is an infinite group with the cardinality of the continuum, and each "sheet" pZ_p is a profinite[32] torsion-free group, which is best understood by looking at the descending normal series $pZ_p \triangleright p^2 Z_p \triangleright ... \triangleright p^m Z_p \triangleright ...$ and considering the finite cyclic quotients $p^n Z_p / p^m Z_p \cong \mathbb{Z}_{p^{m-n}}$.

Remark 2.15. *Similar considerations apply to the the construction of p-adic quantum theory for the other two quadratic extensions $Q_p(\sqrt{p})$ and $Q_p(\sqrt{p\epsilon})$ available in the case of $p \geq 3$ (although the cases $p = 3$ and $p \geq 5$ have to be treated separately), as well as the seven quadratic extensions available in the case of $p = 2$. The phase groups take a similar (but not identical) form to the one presented here, and the full details can be found in [RTVW89] (Section IV.C and Appendices C.3, C.4).*

2.8.8 Tropical quantum theory

Relational quantum theory involves semirings which are both additively and multiplicatively idempotent, parity quantum theory involves a semiring which is only multiplicatively idempotent, and ordinary quantum theory involves a semiring which is neither additively nor multiplicatively idempotent. We now give examples of theories with wave-

[32] And hence both compact and totally disconnected.

functions based in semirings which are additively idempotent but not multiplicatively idempotent, namely the tropical semirings [Sim88, Mas87, Sim94, Pin98, Mik04, SS07].

Definition 2.16. *A* ***tropical semiring*** *is the commutative semiring* $(M, \min, \infty, +, 0)$ *obtained from a totally ordered commutative monoid* $(M, +, 0, \leq)$ *having an absorbing element* ∞ *which is larger than all elements in the monoid. In the tropical semiring,* $\min$ *is the addition,* ∞ *is the additive unit,* $+$ *is the multiplication and* 0 *is the multiplicative unit. The nomenclature is extended to semirings isomorphic to the explicitly min-plus semirings used above (e.g. max-plus formulations, or the Viterbi semiring).*

Examples of tropical semirings appearing in the literature include the tropical reals $(\mathbb{R} \sqcup \{\infty\}, \min, \infty, +, 0)$, the tropical integers $(\mathbb{Z} \sqcup \{\infty\}, \min, \infty, +, 0)$, the tropical naturals $(\mathbb{N} \sqcup \{\infty\}, \min, \infty, +, 0)$, and the Viterbi semiring $([0, 1], \max, 0, \cdot, 1)$ (which is a tropical semiring because it is isomorphic to the explicitly min-plus semiring $(\mathbb{R}^+ \sqcup \{\infty\}, \min, \infty, +, 0)$ via the semiring homomorphism $x \mapsto -\log x$). In fact, there is an easy characterisation of which commutative semirings arise as tropical semirings (the proof is omitted as it is a straightforward check).

Lemma 2.17. *A commutative semiring* $(S, +, 0, \cdot, 1)$ *is a tropical semiring if and only if for all* $a, b \in S$ *we have* $a = a + b$ *or* $b = a + b$ *(in which case we can set* $\min(a, b) = a + b$*).*

From now on, we will revert back to usual semiring notation, and we will rely on the result above to connect with the min-plus notation typical of tropical geometry [SS07]. We will, however, remember that tropical semirings come with a total order respected by the multiplication, and we will occasionally use min, max and $\leq$.

Lemma 2.18. *The only involution possible on a tropical semiring* $(S, +, 0, \cdot, 1)$ *is the trivial one, with sub-semiring of positive elements* $(\{x^2 \mid x \in S\}, +, 0, \cdot, 1)$.

Proof. Let * be an involution for the tropical semiring S: $x \leq y$ implies that $x = x + y$, so that $x^* = x^* + y^*$ and $x^* \leq y^*$. But then $x \leq x^*$ implies $x^* \leq (x^*)^* = x$ (and similarly for $x^* \leq x$), so that $x^* = x$ is the trivial involution. Now consider the tropical semiring with trivial involution, so that the positive elements are exactly those in the form x^2 for some $x \in S$. But in a tropical semiring we have that $x^2 + y^2 = (x + y)^2$ (as Speyer and Sturmfels put it, "the Freshman's dream holds in tropical arithmetic." [SS07]): hence the squares are closed under addition $+$, and form a sub-semiring. □

If S is a tropical semiring and $R := (\{x^2 \,|\, x \in S\}, +, 0, \cdot 1)$ is its sub-semiring of positive elements, we refer to the R-probabilistic theory $\mathrm{CP}^*[S\text{-Mat}]$ as **tropical quantum theory**.

Just as in the case of relational quantum theory, the group of phases in a tropical semiring S is always trivial (because $x^2 = 1$ implies $x = 1$ in any totally ordered monoid $(S, \cdot, 1, \leq)$), and there is no interference. Similarly, there is a unique orthonormal basis on each system, the only unitaries/invertible maps are permutations, and superposition cannot be distinguished from mixing by measurements alone. Tropical quantum theory does not admit any implementation of the algorithm for the abelian Hidden Subgroup Problem, nor does it admit any generalised Mermin-type non-locality arguments.

The parallelisms with relational quantum theory become less surprising when one realises that tropical quantum theory is another generalisation of quantum theory over the booleans, which form a totally ordered distributive lattice, and hence are a particular case of tropical semiring. (Proof of the following result is omitted, as it is a straightforward check.)

Lemma 2.19. *Any totally ordered distributive lattice* $(\Omega, \vee, \bot, \wedge, \top)$ *is a tropical semiring* $(\Omega, \wedge, \top, \vee, \bot)$*; conversely, every tropical semiring* $(S, +, 0, \cdot, 1)$ *which has* 1 *as least element and such that* $x^2 = x$ *for all* $x \in S$ *is a totally ordered distributive lattice* $(S, \cdot, 1, +, 0)$*.*

In the light of the result above, we expect tropical quantum theory to be local, exactly like relational quantum theory, but further investigation of this question is left to future work.

Chapter 3

Categorical Quantum Dynamics

3.1 Introduction

3.1.1 A coherent approach to quantum symmetries

We have seen in the previous Chapter that the importance of Frobenius algebras to quantum foundations and quantum algorithms stems from their connection to the coherent manipulation of classical data: in quantum foundations, coherent operations precede classical operations, as the latter can be obtained from the former by decoherence; in quantum algorithms, coherence is one of the resources involved in providing quantum advantage (e.g. see the next Chapter).

We claim that quantum symmetries and dynamics should similarly be understood by studying the coherent versions of primitive notions from classical symmetries and dynamics. We will see how strong complementarity, an algebraic notion born to capture the special relation between a vector basis and its corresponding Fourier basis, embodies the coherent counterpart of finite-dimensional group theory. Thanks to our coherent approach, we are able to obtain clear and intuitive proofs for a number of known results, as well as a wealth of new insights. The simple and accessible case of periodic lattice symmetry (i.e. finite abelian group symmetry) will be used in the first half of the chapter to showcase some of the salient features of our approach, but the results proven will always be as general as possible.

From the point of view of a mathematician, a symmetry of a system is simply the action of a group on it: a set of reversible transformations of the system into itself, closed under composition and inversion. From the point of view of a physicist, however, symmetries often have different standings depending on their specific origin: there are intrinsic symmetries of a system, such as the $U(n)$ symmetry of an n-dimensional quantum system, and there are symmetries induced by the presence of some underlying structure, such as the symmetry induced by space-time on quantum fields. We will take the mathematician's point of view, and define a symmetry to be a group action on a system (representations, when linear structure is present). However, we will pay respect to the physicist's point of view by investigating the physical significance of the mathematical constructs we introduce.

In the context of this work, quantum dynamics will be treated as the special case of quantum symmetries generated by a group which is 1-dimensional in some suitable sense, an approach similar, in spirit, to the one behind Noether's theorem. Depending on the context, by quantum dynamics we might mean discrete periodic dynamics (corresponding to a $\mathbb{Z}_n$ symmetry), continuous periodic dynamics (corresponding to a S^1 symmetry), discrete dynamics (corresponding to a $\mathbb{Z}$ symmetry) or continuous dynamics (corresponding to a $\mathbb{R}$ symmetry). The results we will prove hold for any notion of dynamics which can be modelled by a doubly well-pointed coherent group, and in particular they will be immediately applicable to discrete periodic, discrete and continuous periodic dynamics of finite-dimensional and separable quantum systems. Unfortunately, the continuous case of $\mathbb{R}$ is not going to be treated explicitly in this work: the necessary techniques were only developed recently, and there has been no time to accommodate them in this Thesis. However, we are certain that the results derived here will straightforwardly extend to the continuous case, with minimum modifications necessary.

In fact, a significant number of concrete examples in our treatment of dynamics will focus on discrete periodic dynamics of finite-dimensional quantum systems: this is a simple, accessible family of examples, which nonetheless offers the full spectrum of features traditionally associated with dynamics (in fact, comparing and contrasting the discrete periodic case with the traditional continuous case yields some interesting new insights on the latter). Moreover, the discrete periodic case relates well to the problem of time observables, an interesting open question in the philosophy of quantum theory. Thus said, the same examples can be readily generalised to the discrete, continuous periodic and continuous cases.

3.1.2 Synopsis of this Chapter

3.1.2.1 Coherent Groups

In Section 3.2 we investigate the basic structures and properties recurring throughout our coherent treatment of group symmetries. We begin our investigation with the concrete case of wavefunctions on periodic lattices, where the momentum observable arises naturally from a coherent treatment of the lattice translation symmetry. We identify strong complementarity as the relevant algebraic property relating the position and momentum observables, and we define a notion of coherent groups to capture the basic abstract structures intervening in the coherent approach to group theory.

Just like group algebras can be used to "embed" groups into categories of vector spaces, coherent groups can be used to embed groups into arbitrary †-SMCs, and this generalisation is related to non-commutative geometry and algebraic quantum theory. In the finite-dimensional quantum case of fHilb, coherent groups generalise group algebras by using an arbitrary quantum observable (a symmetric †-qSFA) as the point structure, instead of the non-degenerate quantum observable (a †-SCFA) used in the case of a group algebra. This corresponds to a possibly non-commutative C*-algebra, as opposed to the commutative C*-algebra associated with the standard basis, and coherent groups in fHilb reduce to a special case of compact quantum groups.

There are three main advantages to working with an abstract, diagrammatic, theory-independent formulation of group algebras such as coherent groups. Firstly, the abstract character of our definitions allows us to focus on the core structural and operational features of group algebras which play a role in quantum foundations, quantum algorithms and non-locality arguments, without getting distracted or waylaid by the rich structure of Hilbert space quantum mechanics. Secondly, the diagrammatic formulation makes important physical concepts such as position/momentum duality, quantum symmetries, Hamiltonians and dynamics available within the framework of CQM, and in turn allows methods from CQM to be applied to a much wider variety of physically interesting problems. Finally, the theory-independent approach means that our results (in both foundations and protocols) are not limited to conventional quantum mechanics, but are instead immediately applicable to a vast landscape of quantum-like theories (comprising toy models, variations, and extensions of quantum mechanics).

That said, the joint aim of the results in this Section is to show that coherent groups provide a suitable generalisation of group algebras (and, more generally, certain finite-dimensional compact quantum groups) to arbitrary †-symmetric monoidal categories.

(i) **Theorem 3.11 (p.80)** shows that coherent groups on finite-dimensional Hilbert spaces are a special, well-behaved case of compact quantum groups.

(ii) **Theorems 3.12 (p.81), 3.13 (p.81) and 3.14 (p.82)** show how coherent groups can be used to encode groups into arbitrary †-SMCs.

(iii) **Theorem 3.15 (p.83)** shows that well-pointed coherent groups generalise group algebras on categories of finite-dimensional vector spaces (and certain more general categories of matrices over commutative semirings with involution).

3.1.2.2 Wavefunctions on a periodic lattice

In Section 3.3 we go back to wavefunctions on a periodic lattice, and we show that finite abelian coherent groups capture the salient abstract features of position/momentum observables and their relation to translation/boost symmetry. The narrative of this Section focuses on periodic lattices as a concrete and accessible example, but the results we obtain are fully general. Specifically, we will prove that symmetry-observable duality, the Weyl Canonical Commutation Relations and the weak uncertainty principle are results that hold for all coherent groups, not just for the ones we identify with periodic lattice symmetry.

The joint aim of the results in this Section is to show that the observable associated with the group structure in a coherent group can be suitable interpreted as a momentum observable. Namely, we expect to have symmetry-observable dualities for translation-momentum and boost-position, we expect the position/momentum pair to satisfy the Weyl Canonical Commutation Relations, and we expect some form of the Uncertainty Principle to hold.

(i) It is expected that the momentum eigenstates on a finite periodic lattice generate the lattice translation group G, and are invariant states under lattice translations. **Theorems 3.17 (p.89) and 3.18 (p.91)** show that the classical states for the group structure of a coherent group generate lattice translations, and are invariant states for lattice translations.

(ii) It is expected that the position eigenstates on a finite periodic lattice generate the momentum boost group $G^\wedge$, and are invariant under boosts. **Theorems 3.22 (p.96) and 3.23 (p.96)** show that the position eigenstates generate a group symmetry $G^\wedge$ on the classical states of the group structure, and are invariant states for this symmetry.

(iii) It is expected that the position/momentum pair on a finite periodic lattice satisfy the Weyl Canonical Commutation Relations. **Theorem 3.24 (p.99)** shows that the position observable and the observable associated with the groups structure satisfy the Weyl Canonical Commutation Relations.

(iv) We argue that the full form of the Uncertainty Principle is too strong a requirement for a position momentum pair, as there are theories with reasonable notions of position and momentum observables which cannot satisfy it. **Theorem 3.16 (p.88)** provides a concrete example of failure of the Uncertainty Principle for a position/momentum pair in hyperbolic quantum theory, due to the fact that the former is a local theory.

(v) We argue that position/momentum pairs should satisfy a weaker form of the Uncertainty Principle, postulating that states of complete knowledge about position have completely indeterminate momentum, and vice versa. **Theorem 3.25 (p.101)** shows that the position observable and the observable associated with the group structure satisfy this weaker form of the Uncertainty Principle.

3.1.2.3 Systems with symmetries

In Section 3.4 we extend our coherent approach to general symmetric systems. Following the identification of classical symmetries with unitary representations of groups, we define coherent symmetries as unitary representations of coherent groups. We provide a categorical characterisation of symmetric systems as objects of the Eilenberg-Moore category for a certain monad, and we extend symmetry-observable duality results from coherent groups to their representations. We conclude the Section with a digression on Stone's Theorem, which we rephrase within our framework.

The joint aim of the results in this Section is to show that the unitary representations of coherent groups model systems equipped with coherent symmetries, satisfying a generalised version of symmetry-observable duality.

(i) **Theorem 3.28 (p.106)** relates unitary representations of coherent groups to unitary representations of the classical groups they encode.

(ii) **Subsection 3.4.2 (p.107)** explains how systems with symmetry governed by a coherent group have a natural interpretation as the objects of the Eilenberg-Moore category for a certain strong commutative monad, with equivariant maps as morphisms between them.

(iii) **Theorems 3.35 (p.115), 3.36 (p.116) and 3.37 (p.118)** prove symmetry-observable for general systems with symmetry governed by a coherent group.

(iv) **Subsection 3.4.4 (p.119)** reformulates Stone's theorem on 1-parameter unitary groups in terms of projection-valued measures, and connects it to the results on symmetry-observable duality for symmetric systems established in the rest of the Section.

3.1.2.4 Infinite-dimensional CQM

In Section 3.5 we introduce the framework of infinite-dimensional CQM to deal with the coherent treatment of certain infinite groups in quantum mechanics. We explicitly cover the textbook example of position/momentum observables for 1-dimensional wavefunctions with periodic boundary conditions (with translation symmetry group S^1), but our techniques naturally extend to other compact and discrete abelian groups (e.g. the case of toroidal translation symmetry groups $\mathbb{T}^d$ or lattice translation symmetry groups $\mathbb{Z}^d$). Unfortunately, infinite-dimensional CQM is a very young field, and treatment of locally compact symmetry groups (e.g. the continuous time-translation symmetry group $\mathbb{R}$ or the continuous space-translation symmetry groups $\mathbb{R}^d$) is left to future work. This Section is taken from [GG16].

The joint aim of the results in this Section is to obtain a categorical formulation of separable Hilbert spaces and (possibly unbounded) linear maps between them which features the algebraic ingredients (namely strongly complementary pairs of †-qSFAs) necessary to talk about some infinite groups (such as $\mathbb{Z}^d$ and $\mathbb{T}^d$) in the context of our framework.

(i) **Theorems 3.56 (p.135 and 3.59 (p.137))** define a new †-SMC *Hilb of non-standard separable Hilbert spaces and (possibly unbounded) maps between them, and relate it to the category of separable Hilbert spaces and bounded maps between them.

(ii) **Theorems 3.63 (p.142) and 3.64 (p.143)** show that *Hilb is dagger compact, and has unital †-SCFAs.

(iii) **Subsection 3.5.5 (p.144)** explicitly constructs the non-standard model for wavefunctions in a box with periodic boundary conditions (we cover the 1-dimensional case explicitly, but the treatment straightforwardly extends to boxes with arbitrarily many dimensions). In particular, **Theorem 3.69 (p.149)** shows that there is a doubly well-pointed coherent group corresponding to the position/momentum pair for the wavefunction.

3.1.2.5 Categorical Quantum Dynamics

In Section 3.6 we apply the results from Sections 3.3 and 3.4 to the special case of discrete periodic dynamics, which we see as symmetries governed by finite cyclic groups (1-dim periodic lattices): symmetry-observable duality yields the Hamiltonian, while the defining equation of Eilenberg-Moore algebras turns into Schrödinger's equation. We cover some construction of specific interest in quantum dynamics, such as Feynman's clock and von Neumann's Mean Ergodic Theorem, and we also look at synchronisation, the emergence of quantum clocks, and the existence of time observables. A first version of this Section appeared in [Gog15b].

3.2 Coherent Groups

3.2.1 Wavefunctions on periodic lattices

The simplest Hilbert space endowed with a finite abelian group symmetry is the group algebra $\mathbb{C}[G]$, together with the regular representation of G:

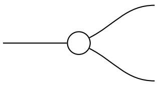
$$U(g) := |h\rangle \mapsto |h \oplus g\rangle \tag{3.1}$$

We will use $\oplus$ to denote the addition operation of a generic abelian group, and 0 for the corresponding unit.[1] When we interpret a finite abelian group $G = \prod_{d=1}^{D} \mathbb{Z}_{n_d}$ as the translation group for a periodic lattice Λ, the group algebra has the very concrete interpretation of a quantum system corresponding to a wavefunction on the lattice. Because of this, we can expect the position and momentum observables to play an important role in the structural characterisation of the group algebra (and indeed this will be the case). More in general, when talking about a quantum system with lattice symmetry we will mean a system $\mathcal{H}$ which comes equipped with a unitary representation of the translation group $\prod_{d=1}^{D} \mathbb{Z}_{n_d}$. From an operational perspective, we can imagine the following scenario: we have a system $\mathcal{H}$, we can transform it reversibly by translation of a lattice Λ, but we know nothing more of its internal structure than what the transformations tell us.

The essence of a group algebra is embodied by the interplay between two kinds of structures: there is the classical data of the group, embedded into the system via a distinguished orthonormal basis (the **standard basis**), and there is the group structure on that classical data. We have already seen that, from a coherent perspective, the classical data embedded in the system is represented by some †-SCFA $\circ_G$, which corresponds to a non-degenerate quantum observable, with 1-dimensional projectors specified by the elements of the translation group. If the latter are identified with the lattice sites (e.g. by fixing a distinguished site), then $\circ_G$ corresponds exactly to the

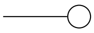
[1] There are four good reasons to use $\oplus$ for the addition in abelian groups, at least within the context of this work. Firstly, the notation is reminiscent of the XOR operation, which is the addition in the abelian group $\mathbb{Z}_2^N$ of N-bit strings and is the most common abelian group operation appearing in quantum computing and protocols. Secondly, while the multiplicative notation would allow a uniform treatment of the abelian and non-abelian cases, it would also result very unfamiliar in the specific instances we are interested in, where group elements are treated as vectors (e.g. the translations of a periodic lattice). Thirdly, the notation can cause no confusion with the direct sum of Hilbert spaces, the most common meaning of $\oplus$ in the context of quantum theory, as direct sums will play no role whatsoever in this work. Finally, the other common additive symbol is $+$, which is already used for superposition in pure-state quantum theory and for convex combination in mixed-state quantum theory and more in general in the context of R-probabilistic theories.

position observable for a wavefunction on the lattice:



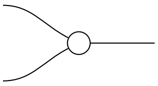
$$= \quad |g\rangle \;\mapsto\; |g\rangle \otimes |g\rangle$$

coherent copy



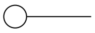
$$= \quad |g\rangle \;\mapsto\; 1$$

coherent delete



$$= \quad |g\rangle \otimes |h\rangle \;\mapsto\; \delta_{g,h}|g\rangle$$

coherent match

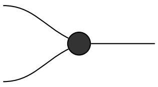


$$= \quad \sum_{g\in G} |g\rangle$$

coherent superposition

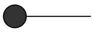
(3.2)

What about the group structure? Do we gain anything by employing a coherent approach in this case? As it will turn out in the rest of this work, we do (and quite a lot). We being by considering the coherent versions of the group multiplication $\oplus$ (also known as *addition*) and group inverse $\ominus$ (as well as the group unit 0, which is already embedded as a distinguished element of the standard basis):



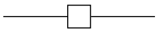
$$= \quad |g\rangle \otimes |h\rangle \;\mapsto\; |g \oplus h\rangle$$

coherent group multiplication



$$= \quad |0\rangle$$

coherent group unit



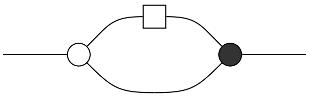
$$= \quad |g\rangle \;\mapsto\; |\ominus g\rangle$$

coherent group inverse

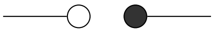
(3.3)

Because of the group structure, these processes come with a number of interesting structural properties; to begin with, the group multiplication and unit form a monoid.

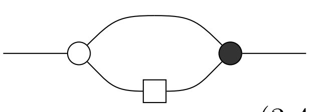
The coherent group inverse is an involution, and it satisfies the following equation known as **Hopf's law**:



$$=$$



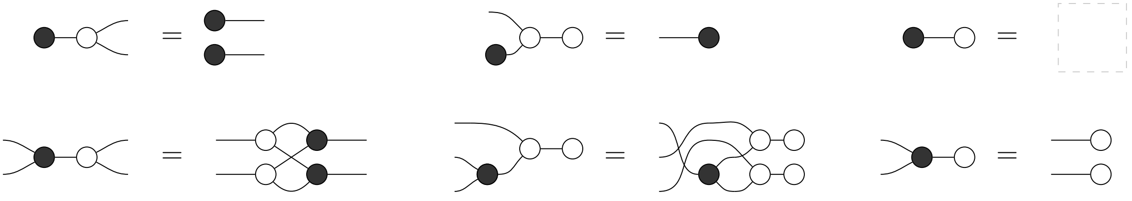
$$=$$



(3.4)

The relation of Hopf's law to the group inverse can be seen by applying both sides of each equation to any ○-classical state $|g\rangle$: on the LHS of the first equation/RHS of the second equation, the state is copied, one copy is inverted, and both copies are added, yielding $|(\ominus g) \oplus g\rangle$ for the first equation and $|g \oplus (\ominus g)\rangle$ for the second equation; on the RHS of the first equation/LHS of the second equation, the state is coherently deleted, and replaced with the state $|0\rangle$; all in all, the equations read $(\ominus g) \oplus g = 0 = g \oplus (\ominus g)$, which is the very definition of group inverse.

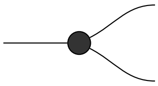
Finally, the coherent group unit is an element of the standard basis (i.e. ●– is a ○-classical state), and application of the coherent multiplication to elements of the standard basis yields elements of the standard basis (i.e. ≻●– is a ○-classical[2] process):



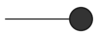
$$(3.5)$$

The top row contains the three conditions (recall from the previous chapter: copy, adjoin and delete) for the coherent group unit to be a ○-classical state, while the bottom row contains the three conditions (again: copy, adjoin and delete) for the coherent group multiplication to be a ○-classical process (which, in particular, maps ○-classical states to ○-classical states).

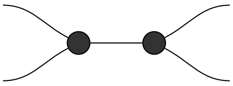
Perhaps the most important property, however, is one which isn't directly inspired by classical groups, and is instead unique to the coherent version of the operations: ≻●– and ●– form the multiplicative fragment of a †-Frobenius algebra:



$$= \quad |g\rangle \;\mapsto \sum_{h\oplus k=g} |h\rangle \otimes |k\rangle$$

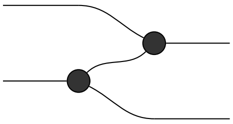


$$= \quad |g\rangle \;\mapsto\; \delta_{g,0}$$



$$= \quad |g\rangle \otimes |h\rangle \;\mapsto \sum_{a\oplus b=g\oplus h} |a\rangle \otimes |b\rangle$$

$$||$$



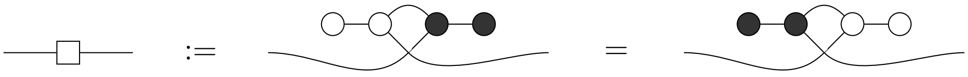
$$= \quad |g\rangle \otimes |h\rangle \;\mapsto \sum_{c\oplus b=h} |g \oplus c\rangle \otimes |b\rangle \qquad (3.6)$$

To be precise, they form a †-qSCFA (commutativity is equivalent to the group being abelian) with normalisation factor $|G|$ (the composite (≻●– ∘ –●≺) sends $|g\rangle$ to $\sum_{h\oplus k=g} |h \oplus k\rangle = |G| \cdot |g\rangle$).

The statement of Frobenius law does not involve the coherent group inverse, and one might therefore imagine that a (commutative) monoid would also give rise to a †-FA on its algebra. On the contrary, it turns out that Frobenius law can only

[2] Henceforth, we will simply use ○-**classical** when referring to ○-to-○ classical processes.

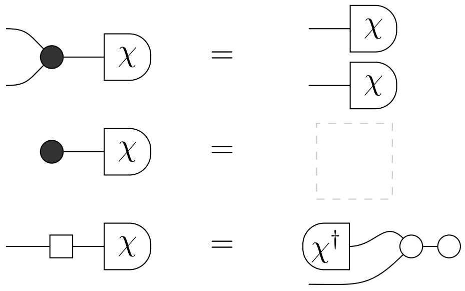
be satisfied when G is a group: for any fixed $g, h \in G$, the sum $\sum_{a \oplus b = g \oplus h} |a\rangle \otimes |b\rangle$ contains a term for $|0\rangle \otimes |g \oplus h\rangle$, which means that the sum $\sum_{c \oplus b = h} |g \oplus c\rangle \otimes |b\rangle$ must also contain a term $|g \oplus c\rangle \otimes |g \oplus h\rangle$ with $g \oplus c = 0$, which in turn means that g must be invertible. Quasi-speciality also depends partially on the fact that G is a group, rather than a monoid: the last equality in the proof above requires each element g to have the same number of pairs (h, k) such that $h \oplus k$, something which is true when G is a group (there are always exactly $|G|$ many such pairs), but need not be true for a general monoid. The apparent absence of the group inverse from the proof of Frobenius law becomes less surprising when we realise that the coherent group inverse, also known as the **antipode**, can always be constructed by only using the †-SCFA ○ and the †-qSCFA ●:



(3.7)

To see that the equalities above hold, apply the three processes to the the state $|g\rangle$ and test them against the effect $\langle h|$, for all $g, h \in G$: the group inverse on the left yields the scalar 1 if $h = \ominus g$ and the scalar 0 otherwise; the process in the middle yields the scalar 1 if $h \oplus g = 0$ and the scalar 0 otherwise; the process on the right yields the scalar 1 if $g \oplus h = 0$ and the scalar 0 otherwise.

Because ● is a †-qSCFA, it is legitimate to ask whether it corresponds to some interesting quantum observable. To find the orthonormal basis associated to it, we want to study the ●-classical states. Equivalently, we can study their adjoints, which are exactly the effects satisfying the following three conditions[3]:



(3.8)

Writing $\chi(g) := \langle \chi | g \rangle$ for any such effect $\langle \chi|$ and any state $|g\rangle$ of the standard basis, we see that the adjoints of the ● classical states correspond to maps $\chi : G \to \mathbb{C}$ satisfying $\chi(g \oplus h) = \chi(g) \cdot \chi(h)$, $\chi(0) = 1$, and $\chi(\ominus g) = \chi(g)^*$, i.e. to the multiplicative characters of the finite abelian group G.

[3] The adjoin condition has been equivalently rewritten in terms of the group inverse, multiplying both sides of the original condition by the symmetric cup corresponding to ○.

In order to understand what this means concretely, observe that the elements $g \in \prod_{d=1}^{D} \mathbb{Z}_{n_d}$ of the translation group for the lattice Λ can be written in terms of components $g = (g_d)_{d=1}^{D}$, where $g_d \in \mathbb{Z}_{n_d}$ for all $d = 1, ..., D$. This makes them look like vectors, and that's not far from true: because they form an abelian group, the translations can always be understood as forming a $\mathbb{Z}$-module. When G is an abelian group, the multiplicative characters always form an abelian group, known as the **Pontryagin dual** of G and denoted $G^{\wedge}$, under pointwise multiplication:

$$\chi \cdot \chi' := g \mapsto \chi(g)\chi'(g) \tag{3.9}$$

The group unit of $G^{\wedge}$ is the **trivial character** $1 := g \mapsto 1$. When G is a finite abelian group, it is always isomorphic to its Pontryagin dual, but not in a canonical way (i.e. there are, in general, many equally legitimate choices of isomorphism $G \cong G^{\wedge}$; more about this later). In the case of $\prod_{d=1}^{D} \mathbb{Z}_{n_d}$, the multiplicative characters can always be written in the following way (here $h \mapsto \chi_h$ is our specific choice of isomorphism $G \cong G^{\wedge}$):

$$\chi_h := g \mapsto e^{-2\pi i\, g \cdot h} \tag{3.10}$$

where the "inner product" $g \cdot h$ in the $\mathbb{Z}$-module $\prod_{d=1}^{D} \mathbb{Z}_{n_d}$ is defined as follows (multiplication $g_d \cdot h_d$ is done modulo n_d):

$$g \cdot h := \sum_{d=1}^{D} \frac{g_d \cdot h_d}{n_d} \tag{3.11}$$

With this explicit characterisation in hand, we are able to write down the orthogonal basis corresponding to the $\bullet$ observable:

$$|\chi_h\rangle = \sum_{g \in G} e^{-2\pi i\, g \cdot h} |g\rangle \tag{3.12}$$

These are the plane waves on a periodic lattice, and hence the quantum observable corresponding[4] to $\bullet$ is exactly the momentum observable.

The result above is an iconic example of what will happen again and again in this Chapter: we treat the classical group symmetry coherently and the observable associated with the corresponding invariant comes out of the framework for free. This is because, contrary to the classical perspective, the coherent perspective is not rigid, and allows us to look at the same primitive from different angles: when looked from the point of view of the position observable, the coherent group multiplication behaves

[4] Implicitly taking into account the fact that the basis states are not normalised.

exactly like the classical group multiplication, but if we switch point of view we can also see as part of an observable in its own right, namely the momentum observable.

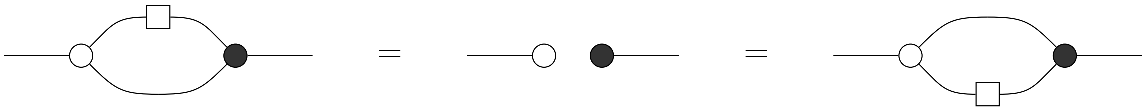
This kind of direct connection between the coherent treatment of a symmetry and the observables corresponding to its conserved quantity is not limited to lattices, or to quantum mechanics; instead, it will be a general result of the framework introduced in this work. The most surprising aspect of this framework will be how it manages to turn few simple ingredients into a whole array of traditional cornerstones of quantum mechanics: we will re-discover familiar results such as position/momentum duality, time/energy duality and the Weyl canonical commutation relations, as well as special cases of Stone's theorem and von Neumann's mean ergodic theorem. Their new formulation in abstract, diagrammatic terms gives us new structural and operational understanding of the reasons behind their validity in quantum theory. At the same time, the abstract and algebraic nature of our definitions and proofs will extend the validity of our results to a much larger spectrum of quantum-like theories, including all those theories based on semiring-valued wavefunctions that we presented at the end of the last Chapter (e.g. real quantum theory, relational quantum theory, modal quantum theory, p-adic quantum theory, etc).

3.2.2 Complementarity and strong complementarity

Hopf's law from 3.4 and the **bialgebra law** from 3.5 (the leftmost equation in the bottom row) are well known in quantum algebra, and make their first appearance in CQM as part of the ZX calculus [CD11]. The ZX calculus focuses on the algebraic relation between the single-qubit Pauli X, Y and Z observables. Both Pauli X and Pauli Y are *complementary*, or *mutually unbiased* to Pauli Z: their eigenstates lie on the equator of the Bloch sphere, an this property is captured by Hopf's law. Amongst the observables complementary to Pauli Z, however, Pauli X plays a special role: if the eigenstates of Pauli Z are taken as the computational basis, the eigenstates of Pauli X are uniquely characterised by the fact that they form the corresponding Fourier basis (they are determined by the multiplicative characters of the finite abelian group $\mathbb{Z}_2$). This special relationship between Pauli Z and Pauli X is known as *strong complementarity*, and is captured by the bialgebra law (and some subset of the equations in 3.5, depending on the specific work [CD11, Bac14, DD16, GK17]).

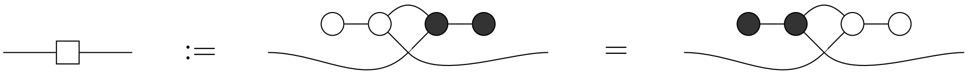
In this Subsection, we define complementarity and strong complementarity in †-SMCs, and prove their general relationship to being mutual unbiased, group structure and the Fourier transform.

Definition 3.1. *Two symmetric †-qSFAs ○ and ● on the same object $\mathcal{H}$ of a †-SMC are said to be* ***complementary*** *(or a* ***complementary pair****) if they satisfy* ***Hopf's Law****:*



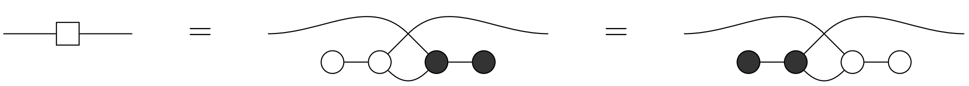
(3.13)

where the ***antipode*** -□- $: \mathcal{H} \to \mathcal{H}$ *is the unitary defined as follows, which we furthermore require to be self-adjoint (or equivalently self-inverse) as part of this definition:*



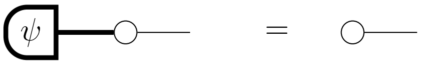
(3.14)

Remark 3.2. *Because the †-qSFAs are chosen to be symmetric, the antipode can furthermore be written in the following additional ways:*



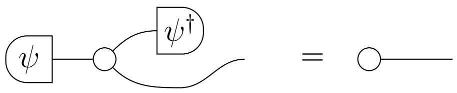
(3.15)

Definition 3.3. *Let ○ be a †-qSFAs in a dagger compact category $\mathcal{C}$. Then a state ψ is a* ***○-unbiased*** *state if the following holds in* $\mathrm{CP}^*[\mathcal{C}]$*:*



(3.16)

Equation 3.16 can be unfolded into the following more general definition, which holds in an arbitrary †-SMC:

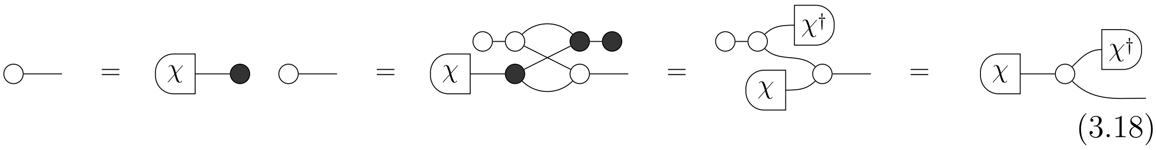


(3.17)

In fHilb, the ○-unbiased states are exactly those which, upon normalisation, yield the uniform distribution when measured in the ○ observable.

Lemma 3.4. *Consider a pair of symmetric †-qSFAs ○ and ● in a †-SMC. If (○,●) is a complementary pair, then the ●-classical states are ○-unbiased, and the ○-classical states are ●-unbiased.*

Proof. We prove that a ●-classical state χ is ○-unbiased:



(3.18)

The first equality is by the delete condition for ●-classical states, the second equality is Hopf's law (together with the self-adjoint requirement for the antipode), the third equality is by the copy condition and adjoint conditions for ●-classical states, the last equality is by Frobenius law and unit law for ○. The proof for ○-classical states is the same, with colours swapped. □

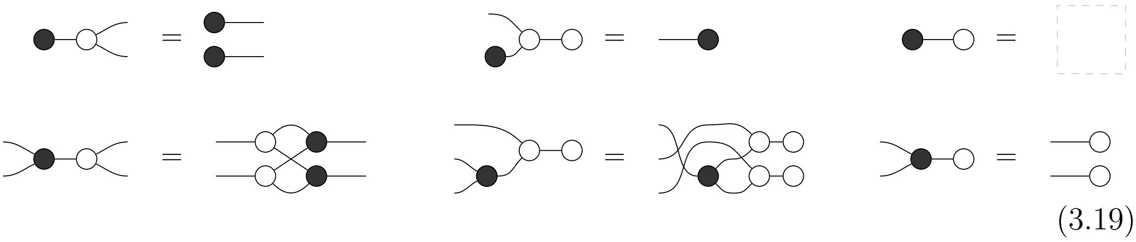
Hence complementarity always results in mutual the observables involved being mutually unbiased, regardless of the specific theory under consideration. We can also prove the converse, that being mutual unbiased implies complementarity (in the sense of Hopf's law and self-adjointness of the antipode), as long as at least one of the two †-qSFAs has enough classical states.

Lemma 3.5. *Consider a pair of symmetric †-qSFAs ○ and ● in a †-SMC. If ○ has enough classical states, and the ○-classical states are ●-unbiased, then* (○, ●) *is a complementary pair. Similarly, if ● has enough classical states, and the ●-classical states are ○-unbiased, then* (○, ●) *is a complementary pair.*

Proof. If ○ has enough classical states, then each equation in 3.18 holds as long as it holds when tested against $\psi^\dagger$, where ψ is an arbitrary ○-classical state. The first equation in the chain is seen to hold by the delete conditions for ○-classical states and ●-classical states. The second equation is seen to hold by applying the copy and adjoin conditions for ○-classical states to the RHS, and then using the fact that ○-classical states are ●-unbiased by hypothesis; an application of Frobenius law and unit laws for ● is necessary to bring the diagram in the form required by the definition of ●-unbiased states (in the form of its adjoint, to be precise). The third equation is seen to hold by the copy and adjoin conditions for ●-classical states. The last equation is seen to hold by Frobenius law and unit laws for ○. □

Variants of Lemmas 3.4 and 3.5 have previously appeared in the literature [CK17].

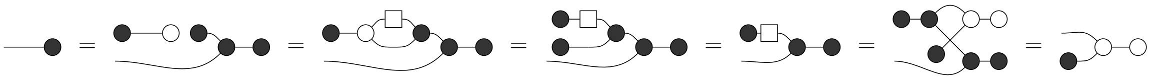
Definition 3.6. *Two symmetric †-qSFAs ○ and ● on the same object $\mathcal{H}$ of a †-SMC are said to be* ***strongly complementary*** *(or a* ***strongly complementary pair****) if they are complementary and furthermore satisfy the following equations*[5]*:*



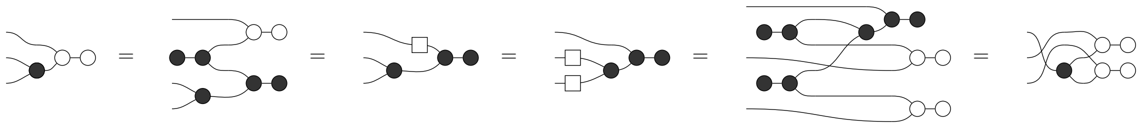
(3.19)

[5] The empty diagram on the RHS of the top right equation is the scalar 1.

Remark 3.7. *The central equations of the top and bottom rows of 3.19 are a consequence of Hopf's law, self-adjointness of the antipode, and the other four equations:*



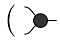
(3.20)

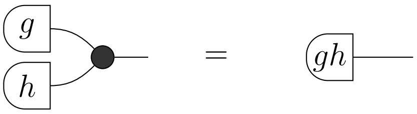


(3.21)

Their corresponding colour-swapped versions are proven similarly. This is why previous presentations of strong complementarity often include only the remaining four equations (together with Hopf's law and either one of: (i) self-adjointness of the antipode, or (ii) the central equation of the top row together with its colour-swapped version). As a consequence, strong complementarity as a property is symmetric in ○ and ● (i.e. we could have equivalently stated it with the colour-swapped versions of the equations above).

In the specific case of quantum mechanics, the relation between strong complementarity and the quantum Fourier transform is given by the following results, some bits of which already appeared in [CDKW12, Kis12] (for the abelian case only).

Lemma 3.8. *Let ○ and ● be a †-SCFA and a †-FA on the same finite-dimensional Hilbert space $\mathcal{H}$. Then ○ and ● are strongly complementary iff there exists a finite group G such that (*  *,* *) endows the set of ○-classical states with the group structure of G. Concretely, this means that we can label the ○-classical states as $(|g\rangle)_{g\in G}$ in a way such that:*



(3.22)

If ○ and ● are strongly complementary, then ● is a †-qSFA with normalisation factor $|G|$, and it is commutative if and only if the group G is.

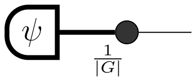
Proof. By definition of strong complementarity, if (○, ●) is a strongly complementary pair, then the set of ○-classical states is always endowed with the structure of some group G which is finite because any †-SCFA ○ can only have finitely many classical states in fHilb. Conversely, if the the set of ○-classical states is endowed by (,) with the structure of some group G, then in particular is a ○-classical process, and is a ○-classical state: this means that the Equations 3.19 always hold when applied to ○-classical states, and hence they hold altogether because any †-SCFA in fHilb always has enough classical states.

It is immediate to see that $(K(\circ),$ >●- , ●- $)$ is abelian if and only if >●- is commutative. Furthermore, the composite >●- ∘ -●< sends an ○-classical state $|g\rangle$ to $\sum_{hk=g} |hk\rangle = |G| \cdot |g\rangle$: because ○ has enough classical states, then this implies that ● is quasi-special, with normalisation factor $|G|$. □

Lemma 3.9. *Let ○ and ● be a strongly complementary pair of a †-SCFA and a †-qSFA on the same finite-dimensional Hilbert space $\mathcal{H}$. Then the ●-classical states are labelled by the multiplicative characters $\chi : G \to S^1$ of the group $G := (K(\circ),$ >●- , ●- $)$, and take the following form in terms of the ○-classical states:*

$$|\chi\rangle := \sum_{g \in G} \chi(g)|g\rangle \tag{3.23}$$

If ● is commutative, then it has enough classical states, and measurement in the ● observable provides the quantum Fourier transform:



$$= \left(\tfrac{1}{|G|}\langle\chi|\psi\rangle\langle\psi|\chi\rangle\right)_{\chi \in G^\wedge} \tag{3.24}$$

$$= \left(\tfrac{1}{|G|}\Big|\sum_{g \in G} \chi(g)^* \psi_g\Big|^2\right)_{\chi \in G^\wedge}$$

Proof. The adjoints of the ●-classical states satisfy Equations 3.8: when restricted to the ○-classical states, the equations are equivalent to those defining the multiplicative characters $\chi \in G^\wedge$ of the finite abelian group $(G, \oplus, 0)$ induced by (>●- , ●-) on the ○-classical states. Hence, they take the desired form. If ● is commutative, then G is abelian, and the ●-classical states form an orthogonal basis.

When ● has enough classical states, $(\mathcal{H}, \bullet)$ is a classical system in CP*[fHilb]. The fact that -●< $= \sum_{\chi \in G^\wedge} |\chi\rangle \otimes |\chi\rangle \otimes \langle\chi|$, together with Equation 3.23, yields the desired result. □

More results about complementarity and strong complementarity, and their relation to the group of phase gates, will be presented in the next Chapter, in regards to Mermin-type non-locality arguments and the abelian Hidden Subgroup Problem.

3.2.3 Coherent Groups

In the fHilb results we have seen above, strong complementarity captures exactly the concept of group algebra. In one direction, a group algebra $\mathbb{C}[G]$ always give rise to a strongly complementary pair, by considering the †-SCFA associated with the standard basis and the †-qSFA generated by the coherent group multiplication and unit. In the other direction, consider a strongly complementary pair of a †-SCFA ○ and a †-qSFA ● on a finite-dimensional Hilbert space $\mathcal{H}$: by Theorem 3.8, there always is a finite group G and a unique isomorphism $\mathcal{H} \cong \mathbb{C}[G]$ which sends the ○-classical states to the elements of the standard basis of $\mathbb{C}[G]$, and that isomorphism turns ≻●- into the coherent group multiplication on $\mathbb{C}[G]$.

We take strongly complementary pairs as our starting point to generalise the coherent treatment of group-theoretic primitives away from the quantum case.

Definition 3.10. *By a* ***coherent group*** *in †-SMC we will mean a strongly complementary pair* (○, ●) *of two symmetric †-qSFAs. We will refer to* ○ *as the* ***point structure****, and to its classical states as the* ***points*** *of the coherent group. We will refer to* ● *as the* ***group structure****.*

We will use (coherent) **copy** and (coherent) **deletion** to refer to the comultiplication and counit of the point structure, and (coherent) **multiplication** and **unit** to refer to the multiplication and unit of the group structure.

Although the underlying definition of the strongly complementary pair (○, ●) is symmetric in ○ and ●, this symmetry is broken in our definition of the coherent group (○, ●) by assigning distinct names to the two †-qSFAs involved. However, the symmetry can be recovered by considering the coherent group (●, ○), which we refer to as the **dual** of (○, ●). Because the two structures play different roles, we will be interested in different properties for each. For example, we will say that a coherent group is **well-pointed** (or that it has **enough points**) if the *point* structure has enough classical states (in which case it is also necessarily commutative), and we will say that a coherent group is **finite** if it is well-pointed with finitely many points. On the other hand, we will say that a coherent group is **commutative**, or **abelian**, if the *group* structure is commutative.

We will take coherent groups on a given †-SMC $\mathcal{C}$ to be the objects of a new SMC QG $[\mathcal{C}]$, which we define as follows:

(i) the objects of QG $[\mathcal{C}]$ are the coherent groups on objects of $\mathcal{C}$;

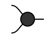
(ii) if (○, ●) and (◌, ◉) are coherent groups on objects $\mathcal{H}$ and $\mathcal{K}$ respectively, then the morphisms $f : (○, ●) \to (◌, ◉)$ of QG $[\mathcal{C}]$, which we will refer to as **coherent group homomorphisms**, are the morphisms $f : \mathcal{H} \to \mathcal{K}$ which are both ○-to-◌ classical and monoid homomorphisms ($\mathcal{H}$, ≻●- , ●-) $\to$ ($\mathcal{K}$, ≻◉- , ◉-)

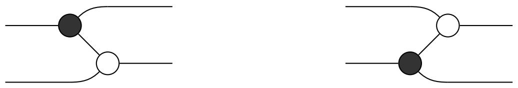
(iii) the tensor product on morphisms is inherited from $\mathcal{C}$, while the tensor product on objects is given by taking the tensor product of the two point structures as the new point structure, and the tensor product of the two group structures as the new group structure $(○, ●) \otimes (○, ◍) := (○ \otimes ○, ● \otimes ◍)$.

Unfortunately, $\mathrm{QG}[\mathcal{C}]$ does not come with a natural dagger. However, dual coherent groups and the dagger of $\mathcal{C}$ can be combined into a well-defined involutive automorphism $^\wedge : \mathrm{QG}[\mathcal{C}] \to \mathrm{QG}[\mathcal{C}]^{\mathrm{op}}$, which sends a coherent group $(○, ●)$ to its dual $(○, ●)^\wedge := (●, ○)$, and a coherent group homomorphism f to $f^\wedge := f^\dagger$. There is also a faithful functor of SMCs $\mathrm{QG}[\mathcal{C}] \to \mathcal{C}$ which sends each coherent group to its underlying object in $\mathcal{C}$, and is the identity on morphisms.

The name *quantum group* is used in the literature to refer to a variety of inequivalent algebraic objects [Dri87, Kas95, Maj00, Str07, Wor87, Wor98], sharing a common conceptual flavour but differing in their actual mathematical implementation. The coherent groups used in this work are closely related to quantum groups: first and foremost, they all feature some form of Hopf's law and bialgebra law, and they take direct inspiration from group algebras and their internal structure. Group algebras are often used to treat group theory within the linear framework of vector spaces, over $\mathbb{C}$ or some other field k: some famous results of this linear treatment are (in order of increasing generality) Fourier theory, Pontryagin duality and Tannaka-Krein dualities for modular categories. Quantum groups (at least in some definitions) can be seen as a direct generalisation of group algebras: they keep the algebraic skeleton, but lose the underlying classical structure given by the standard basis (which is the part that makes group algebras "undesirably" rigid). This is conceptually akin to the way in which non-commutative spaces generalise traditional spaces in Non-commutative Geometry [Con94], or the way in which non-commutative C*-algebras and spectral bundles generalise classical observables and configuration spaces in Algebraic Quantum Theory [HLS09].

We will proceed to show that coherent groups in fHilb are closely related to finite-dimensional compact quantum groups [Wor87, Wor98]. In general, a **compact quantum group** is a pair (C, Δ) of a unital separable C*-algebra C and a co-associative unital C*-algebra homomorphism $\Delta : C \to C \otimes C$ satisfying the additional conditions that the sets $(C \otimes 1) \cdot \Delta(C)$ and $(1 \otimes C) \cdot \Delta(C)$ are dense in $C \otimes C$. When the C*-algebra is finite dimensional, it can be written in the form $C = (\mathcal{H}, ⟩○- , ○-)$ for a symmetric †-SFA ○. As a consequence, a compact quantum group in fHilb can be seen as a pair $(\mathcal{H}, ○, -●⟨)$ a symmetric †-SFA ○ (or, without loss of generality, a †-qSFA) and a co-associative $-●⟨ : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$, satisfying the following conditions:

- The comultiplication  is ○-to-(○⊗○) classical (i.e. a C*-algebra homomorphism $C \to C \otimes C$);
- the following linear endomorphisms of $\mathcal{H} \otimes \mathcal{H}$ are invertible[6]:

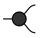


(3.25)

Thanks to this equivalent characterisation, we can prove that coherent groups in fHilb arise as a special, extremely well-behaved case of compact quantum groups on finite-dimensional C*-algebras.

Theorem 3.11 (Coherent groups are compact quantum groups). *There is a bijective correspondence between coherent groups* $(\circ, \bullet)$ *in* fHilb *with* ○ *special and compact quantum groups* $(C,$ $)$ *satisfying the following conditions:*

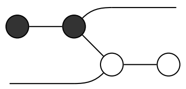
(i) C is a finite-dimensional C-algebra, corresponding to a symmetric †-SFA ○;*

(ii) the comultiplication  *is part of a symmetric †-qSFA ●;*

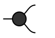
(iii) the unit ●– $: \mathcal{H} \to \mathbb{C}$ *is* ○*-to-*$(\mathbb{C}, \cdot, 1)$ *classical;*

(iv) the two maps depicted in 3.25 are unitaries;

(v) the following map is self-inverse:



(3.26)

Proof. In one direction, consider a coherent group $(\circ, \bullet)$. Then ○ induces a C*-algebra $C = (\mathcal{H},$, ○–$)$, with ● co-associative and ○-to-(○ ⊗ ○) classical (second row of Equations 3.19 in the definition of strong complementarity). The comultiplication  is part of the symmetric †-qSFA ●, and the unit ●– is ○-to-$(\mathbb{C}, \cdot, 1)$ classical (first row of Equations 3.19 in the definition of strong complementarity). The map depicted in 3.26 is the antipode of the coherent group $(\circ, \bullet)$, and it is self-inverse as part of the definition of complementarity. The two maps depicted in 3.25 are unitaries because of complementarity (see Theorem 9 from [ZV14]). In particular, ● is a co-associative C*-algebra homomorphism $C \to (C \otimes C)$ and the two maps depicted in 3.25 are invertible, so that $(C,$ $)$ is a compact quantum group.

[6] In finite dimensions, this is the same as saying that their image is dense.

In the other direction, consider a compact quantum group (C, -●<) on a finite-dimensional C*-algebra C (condition (i)), which always takes the form $C = (\mathcal{H},$ >○- , ○-) for some symmetric †-SFA ○, and assume that the four conditions (ii)-(v) are satisfied. Then >●- is part of a symmetric †-qSFA ● (by condition (ii)) which satisfies Equations 3.19 (because -●< is a C* homomorphism $C \to C \otimes C$ and by condition (iii)). Furthermore, (○, ●) are complementary: they satisfy Hopf's law by condition (iv) and Theorem 9 froms [ZV14], and the associated antipode is self-inverse by condition (v). Hence (○, ●) is a coherent group, with ○ special. □

The following results give a precise meaning to the idea that coherent groups can be used to embed groups in arbitrary †-SMCs. We show that coherent groups always behave as groups on their points, and that well-pointed coherent groups provide a sound generalisation of group algebras to arbitrary †-SMCs.

Theorem 3.12 (**Underlying Group**).
Let (○, ●) *be a coherent group in a †-SMC* $\mathcal{C}$. *Then the multiplication* >●- *and the unit* ●- *endow the points with the structure of a group* (K(○), >●- , ●-).

Proof. The laws of strong complementarity show that ●- ∈ K(○), and that >●- yields a well-defined function K(○) × K(○) → K(○) when restricted to ○-classical states. By associative law and unit laws for ●, we conclude that (K(○), >●- , ●-) is a monoid. Furthermore, the laws of strong complementarity show that if $g \in K$(○) then -□- ∘ $g \in K$(○), and hence the antipode -□- yields a well-defined function K(○) → K(○), which by is furthermore a self-inverse bijection. Finally, Hopf's law implies that for any ○-classical state $g \in K$(○) the ○-classical state -□- ∘ g is an inverse in the monoid (K(○), >●- , ●-), which is therefore a group. □

Theorem 3.13 (**Underlying Homomorphisms**).
Let $\mathbb{G}$:= (○, ●) *and* $\mathbb{H}$:= (⊚, ◍) *be coherent groups on objects* $\mathcal{H}$ *and* $\mathcal{K}$ *of a †-SMC. A coherent group homomorphism* $f : \mathbb{G} \to \mathbb{H}$ *gives rise to a well-defined group homomorphism* f : (K(○), >●- , ●-) → (K(⊚), >◍- , ◍-) *when restricted to the points of* $\mathbb{G}$. *Furthermore, when* $\mathbb{G}$ *is well-pointed, any morphism* $f : \mathcal{H} \to \mathcal{K}$ *which gives rise to a well-defined group homomorphism* f : (K(○), >●- , ●-) → (K(⊚), >◍- , ◍-) *is a coherent group homomorphism* $f : \mathbb{G} \to \mathbb{H}$.

Proof. For the first part, consider a coherent group homomorphism $f : \mathbb{G} \to \mathbb{H}$. The fact that f gives rise to a well-defined function $f : K$(○) → K(⊚) is due to the fact that f is a ○-to-⊚ classical function as part of the definition of coherent group homomorphism. The fact that f is a group homomorphism f : (K(○), >●- , ●-) → (K(⊚), >◍- , ◍-)

follows from the fact that it is a monoid homomorphism as part of the definition of coherent group homomorphism. Conversely, assume that $\mathbb{G}$ is well-pointed, and consider a morphism $f : \mathcal{H} \to \mathcal{K}$ which gives rise to a well-defined group homomorphism $f : (K(○)$, ≻●– , ●–) $\to (K(◍)$, ≻◍– , ◍–). Because it is a function from the ○-classical states to the ◍-classical states, by well-pointedness we conclude that f is ○-to-◍-classical. Because it is a group homomorphism from $(K(○)$, ≻●– , ●–) to $(K(◍)$, ≻◍– , ◍–), it is in particular a monoid homomorphism (≻●– , ●–) to (≻◍– , ◍–). Hence f is a coherent group homomorphism $\mathbb{G} \to \mathbb{H}$. □

Theorem 3.14 (**Underlying Group Functor**).
Let $\mathcal{C}$ be a †-SMC. The following defines a monoidal functor $\llbracket \_ \rrbracket : \mathrm{QG}\left[\mathcal{C}\right] \to \mathrm{Grp}$ from coherent groups to groups:

⟦(○,●)⟧ := (K(○), ≻●– , ●–)

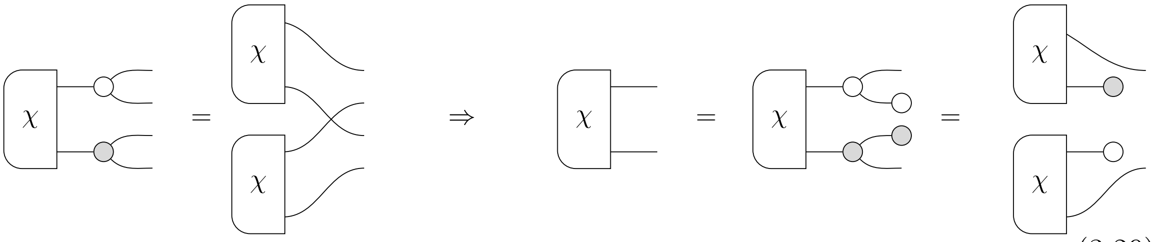
⟦f : (○,●) → (◍,◍)⟧ := f ∘ _ : K(○) → K(◍)   (3.27)

We refer to $\llbracket \_ \rrbracket$ as the ***underlying group functor****. It is faithful when restricted to well-pointed coherent groups.*

Proof. By Theorems 3.12 and 3.13 above, we already know that $\llbracket \_ \rrbracket$ is a well defined functor: all we really need to show is that it is monoidal. Given two coherent groups (○,●) on an object $\mathcal{H}$ and (◍,◍) on an object $\mathcal{K}$, the product coherent group on object $\mathcal{H} \otimes \mathcal{K}$ is given by (○ ⊗ ◍, ● ⊗ ◍). Hence we get the following underlying group for the product coherent group:

⟦(○ ⊗ ◍, ● ⊗ ◍)⟧ = (K(○ ⊗ ◍), ≻●– ⊗ ≻◍– , ●– ⊗ ◍–)   (3.28)

If we can show that all classical states for ○ ⊗ ◍ are in the form $\psi \otimes \phi$ fo a ○-classical state ψ and a ◍-classical state ϕ, then we get $K(○ \otimes ◍) = K(○) \times K(◍)$ and the product is monoidal as desired. The fact that the classical states of a product †-FA are the products of the individual classical states is straightforward consequence of the following observation:



(3.29)

Finally, the functor is faithful when restricted to well-pointed coherent groups because a coherent group homomorphism from a well-pointed coherent group is entirely defined by its action on the underlying group. □

Theorem 3.15 (Group algebras are well-pointed coherent groups). *Let $(R,^\dagger)$ be a cancellative involutive semiring such that the †-SMC R-*Mat *has non-degenerate inner product. If G is any finite group such that $|G| = n^\dagger n$, for some invertible $n \in R$*[7]*, then the group algebra $R[G]$ in R-*Mat *always gives rise to a well-pointed coherent group $(\circ, \bullet)$ (which we also denote by $R[G]$, when no confusion can arise): the point structure $\circ$ is the †-SCFA determined by the standard basis of the group algebra $R[G]$, and the group structure is given by the coherent group multiplication and unit on $R[G]$. Conversely, if $(\circ, \bullet)$ is a well-pointed coherent group in R-*Mat*, then there is a coherent group isomorphism $(\circ, \bullet) \cong R[G]$ for some G.*

Proof. Consider a group algebra $R[G]$, with standard orthonormal basis $\big(|g\rangle\big)_{g\in G}$. A †-SCFA with the standard basis as its set of classical states is given by the following R-linear maps, defined on the standard basis:

$$\begin{aligned} \text{-○<} &:= |g\rangle \mapsto |g\rangle \otimes |g\rangle \\ \text{-○} &:= |g\rangle \mapsto 1 \end{aligned} \tag{3.30}$$

If we take (>●- , ●-) to be the coherent group multiplication and unit for the group algebra $R[G]$, then Frobenius law, the quasi-speciality law, the laws of complementarity and strong complementarity for the pair $(\circ, \bullet)$ all hold when applied to ○-classical states. Because $\circ$ has enough classical states, Frobenius law and the quasi-speciality law hold in generality, making (>●- , ●-, -●< , -●) a †-qSFA, and so do the laws of complementarity and strong complementarity, making $(\circ, \bullet)$ a well-pointed coherent group. Conversely, take a well-pointed coherent group $(\circ, \bullet)$ on an object A of R-Mat, and let $G := (K(\circ),$ >●- , ●- $)$ by the group given by Theorem 3.12. Because the semiring is cancellative and the inner product is non-degenerate, the points of the coherent group form an orthogonal basis for A, and have all the same square norm M (where $M = m^\dagger m$ is the normalisation factor of the point structure). In particular, there can only be finitely many points, so $R[G]$ is a well-defined group algebra in R-Mat and $id_A = \frac{1}{N}\sum_{g\in K(\circ)} g \circ g^\dagger$. Define the following linear map (where $g^\dagger : A \to I$ and $|g\rangle : I \to R[G]$):

$$U := \frac{1}{n} \sum_{g\in K(\circ)} |g\rangle \circ g^\dagger : A \to R[G] \tag{3.31}$$

[7] Semirings in which this is true for all groups G include the rational, real and complex numbers.

Because $id_A = \frac{1}{N}\sum_{g \in K(\bigcirc)} g \circ g^{\dagger}$ and $id_{R[G]} = \sum_{g \in K(\bigcirc)} |g\rangle\langle g|$, the linear map U is a unitary. Furthermore, it is immediate to see that U is a well-defined group homomorphism when restricted to the points of $(\circ, \bullet)$, and hence a coherent group homomorphism by Theorem 3.13. $\square$

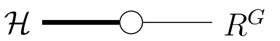
As a closing remark, it should be noted that in R-Mat, e.g. for $R = \mathbb{R}^{+}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$, all finite groups arise from (well-pointed) coherent groups, but that this is not true in general †-SMCs. It is furthermore true that any two well-pointed coherent groups in R-Mat corresponding to the same finite group are connected by a coherent group isomorphism, but again this need not hold in general †-SMCs.

3.3 Wavefunctions on a periodic lattice

We turn our attention back to the treatment of wavefunctions on a periodic lattice, but this time from the abstract perspective of coherent groups on some object $\mathcal{H}$ of some †-SMC $\mathcal{C}$. For the rest of this section, we will work with a well-pointed abelian coherent group $\mathbb{G} := (\circ, \bullet)$ having finitely many points. By Theorem 3.12, $G := (K(\circ),$ ≻●– , ●– $)$ is a finite abelian group, and we fix an isomorphism $G \cong \prod_{d=1}^{D} \mathbb{Z}_{n_d}$ allowing us to interpret G as the translation group of a D-dimensional lattice Λ.

3.3.1 What we look for in a momentum observable

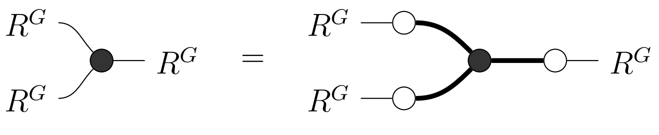
The identification of the position observable with the point structure $\circ$ shouldn't come as a surprise: if we fix a distinguished site λ_0 on the lattice Λ, then lattice sites are naturally identified with elements of G, i.e. points of the coherent group, by the bijection $g \mapsto g(\lambda_0)$. If CP$^*[\mathcal{C}]$ is R-probabilistic, then the following is the desired lattice **position measurement** (where R^G is the space of R-distributions over G):



(3.32)

position measurement

The multiplicative fragment (≻●– , ●–) of the group structure for $\mathbb{G}$ acts as the (coherent) lattice translation on the points/lattice sites, with the unit ●– corresponding to the distinguished site λ_0. The position measurement, together with the corresponding preparation, can then be used to obtain the classical translation group on the lattice[8] from the coherent one, confirming that the outcomes of the position measurement defined above are naturally endowed with lattice structure:



(3.33)

From our experience with fHilb, we expect the momentum observable to arise as the group structure $\bullet$. But what does it mean to be the momentum observable in an abstract setting such as ours? What are the structural and operational features that would allow us to conclude, beyond reasonable doubt, that $\bullet$ behaves as the momentum observable? To understand this, we look at some of the defining characteristics of position and momentum observables in the traditional formulation of quantum mechanics.

[8] Or, to be more precise, its extension to the space of R-distributions over the lattice.

Consider a wavefunctions on the periodic lattice Λ, living in the group algebra $\mathbb{C}[G]$. The translation symmetry on Λ is encoded by a unitary group action $(U_g)_{g \in G}$ of G on $\mathbb{C}[G]$, and the momentum eigenstates $\frac{1}{\sqrt{|G|}}|\chi\rangle$ are the states invariant under this action. Hence the momentum eigenstates generate the group action in following sense:

$$U_g := \frac{1}{|G|} \sum_{\chi} \chi(g) |\chi\rangle\langle\chi| \tag{3.34}$$

The momentum eigenstates come themselves with an abelian group symmetry, the **boost symmetry** on Λ, which is encoded by a unitary group action $(V_\chi)_{\chi \in G^\wedge}$ of the Pontryagin dual $G^\wedge$ of the translation symmetry group. The position eigenstates turn out to be exactly the states invariant under boost symmetry, and generate its group action the following sense:

$$V_\chi := \sum_{g \in G} \chi(g) |g\rangle\langle g| \tag{3.35}$$

We will take this as our first structural description of the relationship between the position and momentum observables: there is a symmetry-observable duality, with the momentum observable corresponding to the translation symmetry (the symmetry of position eigenstates), and the position observable corresponding to the boost symmetry (the symmetry of momentum eigenstates).

In the continuous case of wavefunctions over $\mathbb{R}^n$ (with positions $x \in \mathbb{R}^n$ and momenta indexed by $p \in \mathbb{R}^n$ as $\chi_p := x \mapsto e^{ipx}$), the relationship between the translation and boost symmetries is fully captured by the **Weyl Canonical Commutation Relations**:

$$V_p U_x = e^{i\hbar p \cdot x}\, U_x V_p \tag{3.36}$$

Note that we chose the Weyl CCRs, which refer to the translation and boost symmetries, instead of the more common Heisenberg CCRs $[\mathbf{x}, \mathbf{p}] = i\hbar\; id_{\mathcal{H}}$, which refer to the infinitesimal generators $\mathbf{x}$ and $\mathbf{p}$ for the symmetries (usually referred to as the position and momentum observables). There are two reasons for this choice. Firstly, the Heisenberg CCRs are known not to hold in finite dimensions, for any choice of operators $\mathbf{x}$ and $\mathbf{p}$:

$$\mathrm{Tr}\left(\mathbf{xp} - \mathbf{px}\right) = \mathrm{Tr}\left(\mathbf{xp}\right) - \mathrm{Tr}\left(\mathbf{px}\right) = 0 \neq i\hbar \dim \mathcal{H} = \mathrm{Tr}\left(i\hbar\; id_{\mathcal{H}}\right) \tag{3.37}$$

On the contrary, the Weyl CCRs are easily formulated in our finite-dimensional setting:

$$V_\chi U_g = \chi(g)\; U_g V_\chi \tag{3.38}$$

Secondly, the Heisenberg CCRs focus on infinitesimal generators $\mathbf{x}$ and $\mathbf{p}$, which are mere mathematical constructs arising from Stone's Theorem, while the Weyl CCRs focus on the symmetries associated with position and momentum, which have direct physical significance. The issues with identifying self-adjoint operators and observables are fleshed out in full detail in Subsection 2.4.3 below: the conclusion will be that it makes no sense to look for an analogue of $\mathbf{x}$ and $\mathbf{p}$ in our abstract framework, and as a consequence the Heisenberg form of the CCRs should not be used. We will take the Weyl CCRs, together with an appropriately revised formulation of the Stone-von Neumann Theorem, as our second structural description of the relationship between the position and momentum observables. Despite our departure from the Heisenberg CCRs, we will still be able to formulate a suitable version of Stone's Theorem (in Subsection 3.4.4 below), further strengthening our claims.

The Uncertainty Principle is unarguably the most iconic operational feature of position and momentum in quantum mechanics. The most common formulation of the principle is due to Kennard and Weyl, and involves the standard deviations σ_x and σ_p for the position and momentum observables of a wavefunction on the continuous 1-dimensional space $\mathbb{R}$:

$$\sigma_x \sigma_p \geq \frac{\hbar}{2} \tag{3.39}$$

There is also an entropic formulation of the principle [Bec75, BM75], which involves the entropies H_x and H_p of the probability distributions on outcomes of position and momentum measurements of a same state:

$$H_x + H_p \geq \log(e/2) \tag{3.40}$$

Unfortunately, neither form of the uncertainty principle is suitable for our purposes: while some of its implications truly characterise the abstract relationship between position and momentum observables, other implications, such as the necessarily ensuing non-locality, seem to pertain more to quantum mechanics in general rather than to position and momentum specifically. Indeed there are quantum-like theories which have sensible notions of position/momentum observables[9] while at the same time being entirely local: a stunning example is given by hyperbolic quantum theory, a quasi-probabilistic theory which admits non-trivial examples of position/momentum duality (e.g. for the finite periodic lattices $\mathbb{Z}_2^N$ and for the infinite lattices $\mathbb{Z}^N$), but at

[9] By which we mean coherent groups with each observable having an orthonormal basis of classical states, so that the position/momentum measurements are well defined with non-deterministic classical outcomes.

the same time fails to satisfy either formulation of the uncertainty principle (not a surprise, since the theory is local).

Consider a qubit in hyperbolic quantum theory. Let $\circ$ be the †-SCFA associated with the Pauli Z orthonormal basis $|0\rangle, |1\rangle$, and $\bullet$ be the †-qSCFA associated with the Pauli X orthogonal basis $|\pm\rangle := |0\rangle \pm |1\rangle$. Then $(\circ, \bullet)$ is a coherent group corresponding to the position/momentum pair for a 1-dimensional periodic lattice with points $\mathbb{Z}_2$: the position eigenstates $|0\rangle, |1\rangle$ are unbiased for the momentum measurement, and conversely the (normalised) momentum eigenstates $\frac{1}{\sqrt{2}}|+\rangle, \frac{1}{\sqrt{2}}|-\rangle$ are unbiased for the position measurement. However, both the Kennard-Weyl and the entropic uncertainty principles fail.

Theorem 3.16 (**Hyperbolic quantum theory fails the uncertainty principle**). *There is a mixed state ρ of the qubit in hyperbolic quantum theory which gives outcome $|0\rangle$ with certainty when measured in the Pauli Z observable, and outcome $|+\rangle$ with certainty when measured in the Pauli X observable.*

Proof. Let $a := \sqrt{2}$ and $b := \frac{1}{\sqrt{2}} + j\frac{\sqrt{3}}{\sqrt{2}}$, and consider the pure qubit state $|\psi\rangle := a|0\rangle + b|1\rangle$, which is normalised:

$$\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 2 + (\frac{1}{2} - \frac{3}{2}) = 1 \tag{3.41}$$

Now consider the normalised mixed state $\rho := \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|1\rangle\langle 1|$. Upon measurement in the Pauli Z observable, the state ρ results in the outcome $|0\rangle$ with certainty:

$$\begin{aligned}\langle 0|\rho|0\rangle &= \frac{1}{2}|\langle 0|\psi\rangle|^2 + \frac{1}{2}|\langle 0|1\rangle|^2 = \frac{1}{2}\cdot 2 + \frac{1}{2}\cdot 0 = 1\\ \langle 1|\rho|1\rangle &= \frac{1}{2}|\langle 1|\psi\rangle|^2 + \frac{1}{2}|\langle 1|1\rangle|^2 = \frac{1}{2}\cdot(-1) + \frac{1}{2}\cdot 1 = 0\end{aligned} \tag{3.42}$$

Upon measurement in the Pauli X observable, the state ρ also results in the outcome $|+\rangle$ with certainty:

$$\begin{aligned}\frac{1}{2}\langle +|\rho|+\rangle &= \frac{1}{4}|\langle +|\psi\rangle|^2 + \frac{1}{4}|\langle +|1\rangle|^2\\ &= \frac{1}{4}(|a|^2 + ab^* + a^*b + |b|^2) + \frac{1}{4}\cdot 1 = \frac{1}{4}\big((2 + 2\frac{\sqrt{2}}{\sqrt{2}} - 1) + 1\big) = 1\\ \frac{1}{2}\langle -|\rho|-\rangle &= \frac{1}{4}|\langle -|\psi\rangle|^2 + \frac{1}{4}|\langle -|1\rangle|^2\\ &= \frac{1}{4}(|a|^2 - ab^* - a^*b + |b|^2) + \frac{1}{4}\cdot 1 = \frac{1}{4}\big((2 - 2\frac{\sqrt{2}}{\sqrt{2}} - 1) + 1\big) = 0\end{aligned} \tag{3.43}$$

Hence the state ρ is sharp in both the Pauli Z (lattice position) and Pauli X (lattice momentum) observables, and the conventional form of the uncertainty principle necessarily fails. □

The example of hyperbolic quantum theory is not isolated: there are many other theories admitting sensible notions of position and momentum observables (finite-field and p-adic quantum theories another examples), but which at the same time are local, and hence necessarily fail to satisfy either formulation of the uncertainty principle. As a consequence, we will choose to take a restricted version of the uncertainty principle as our third structural description of the relationship between the position and momentum observables: namely, that states of definite position have completely indeterminate momentum, and vice versa that states of definite momentum have completely indeterminate position.

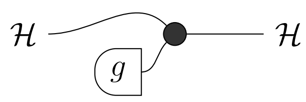
3.3.2 Momenta generate translation symmetry

In the first part of this Section, we have set out a number of structural and operational criteria that would help identifying ● with the momentum observable: (i) the relationship between the position/momentum observables and the translation/boost symmetries; (ii) the Weyl canonical commutation relations; (iii) the (restricted version of the) uncertainty principle. In the remainder of this Section we will prove that the observable ● satisfies all those criteria, and conclude that it is indeed the lattice momentum observable we were looking for.

We begin by observing that the unitary translation symmetry action $(U_g)_{g \in G}$ on $\mathcal{H}$ is obtained by evaluating ≻●– on the points of the coherent group.

Theorem 3.17 (Momenta generate translations).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{H}$ of a †-SMC $\mathcal{C}$, and let $G := (K(\circ),$ ≻●– , ●– $)$. Define a family $(U_g)_{g \in G}$ of endomorphisms of $\mathcal{H}$ as follows:

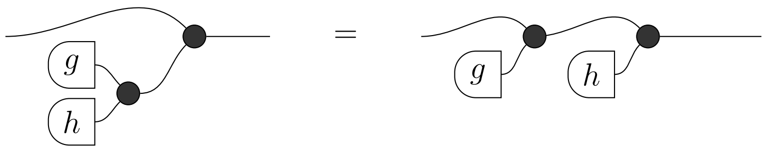
$U_g \quad :=$



(3.44)

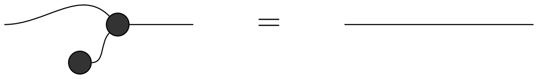
Then $(U_g)_{g \in G}$ gives a unitary action of the group G on $\mathcal{H}$, restricting to the left regular action of the translation group G on the points of $\mathbb{G}$.

Proof. To show that this defines a unitary group action, we need to check that $U_{g \oplus h} = U_h U_g$, that $U_0 = id_{\mathcal{H}}$, and that $U_g^\dagger U_g = id_{\mathcal{H}} = U_g U_h^\dagger$. The first claim follows by the associative law for ●, together with the fact that it acts as the group G on the points of the coherent group:



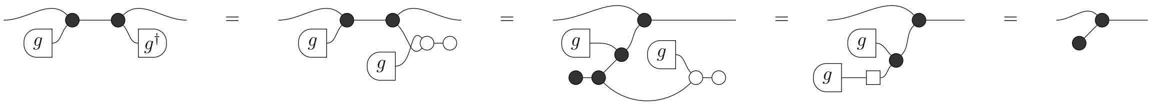
(3.45)

The second claim follows from the unit law for ●:



(3.46)

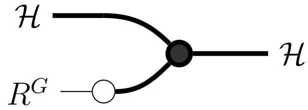
The third claim has a slightly more complicated proof, which involves Frobenius and unit laws for ●, the adjoin condition for ○-classical states, and Hopf's law:



(3.47)

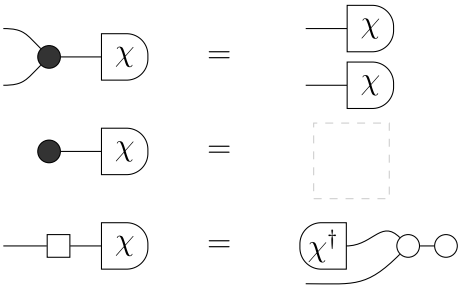
The proof that $U_gU_g^\dagger = id_{\mathcal{H}}$ goes along the same lines. □

We deduce that, when CP*[$\mathcal{C}$] is R-probabilistic and $\mathbb{G}$ is well-pointed, the following defines the controlled unitary corresponding to the symmetry group action:



(3.48)

We define the **multiplicative characters** for the coherent group $\mathbb{G}$ to be the effects $\chi : \mathcal{H} \to I$ satisfying the following three equations:

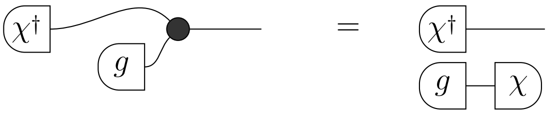


(3.49)

When restricted to the points of $\mathbb{G}$, the three equation above mimic the defining properties of multiplicative characters for classical groups: $\chi(g \oplus h) = \chi(g)\chi(h)$, $\chi(0) = 1$, and $\chi(\ominus g) = \big(\chi(g)\big)^\dagger$ (where the last one made use of the adjoint condition for ○-classical states); indeed, we already encountered them at the beginning of the chapter. It is easy to show that, just like in fHilb, the multiplicative characters for $\mathbb{G}$ are exactly the adjoints of the ●-classical states (which we wish to interpret as momentum eigenstates): the first two equations in 3.49 correspond to the copy and delete conditions for the state $\chi^\dagger$, while the third one can be easily turned into the adjoin condition by applying the symmetric cup corresponding to ○ (and recalling the definition of the antipode).

We now show that the ●-classical states are exactly the states invariant under the translation symmetry action on $\mathcal{H}$.

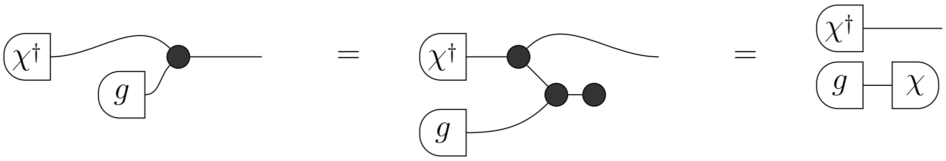
Theorem 3.18 (Momenta invariant under translation).
Let $\mathbb{G} := (\circ, \bullet)$ *be a coherent group on an object* $\mathcal{H}$ *of a* †*-SMC* $\mathcal{C}$*, and let* $G :=$ $(K(\circ),$ ⟩●- , ●- $)$*. The adjoints of the multiplicative characters (i.e. the* ●*-classical states) are invariant under the translation symmetry action, up to a scalar:*



(3.50)

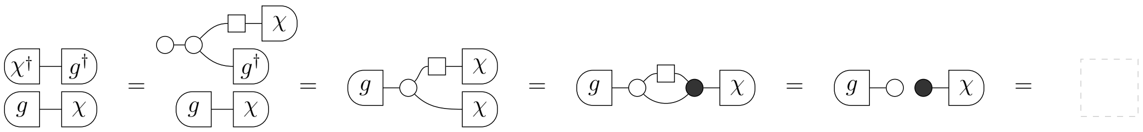
Furthermore, the scalar $\chi(g) := \chi \circ g$ *satisfies* $\chi(g)^\dagger \cdot \chi(g) = 1$*. Finally, assume that* $\mathbb{G}$ *is well-pointed, and consider a state* $\chi^\dagger$*: if both (i) Equation 3.50 holds for all points* g*, and (ii)* $\chi($ ●- $)^\dagger \cdot \chi($ ●- $) = 1$*, then* $\chi^\dagger$ *must be a* ●*-classical state.*

Proof. First we show that the adjoint $\chi^\dagger$ of a multiplicative character χ of the coherent group satisfies Equation 3.50:



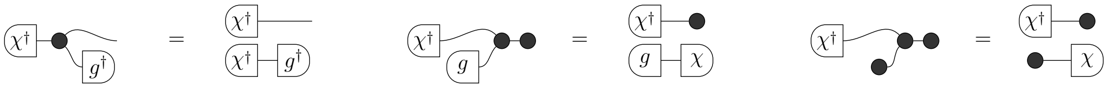
(3.51)

Then we show that the scalar $\chi(g)$ satisfies $\chi(g)^\dagger \cdot \chi(g) = 1$:



(3.52)

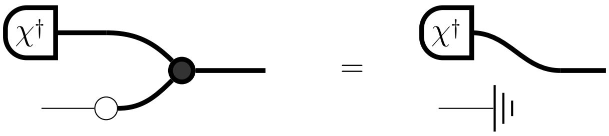
Finally, assume that $\chi^\dagger$ is some state satisfying Equation 3.50. Then we can quickly derive following three equations:



(3.53)

The rightmost equation together with the requirement that $\chi($ ●- $)^\dagger \cdot \chi($ ●- $) = 1$ implies the delete condition for ●-classical states. Because $\mathbb{G}$ is well-pointed, the middle equation together with the delete condition implies the adjoin condition for ●-classical states, while the left equation implies the copy condition. □

We deduce that, when $\mathrm{CP}^*[\mathcal{C}]$ is R-probabilistic, the adjoints of the multiplicative characters are invariant under the controlled unitary associated with the translation symmetry action:



(3.54)

Having checked that the ●-classical states are the invariant states for the translation symmetry action, the next task on our list is to show that they actually generate the symmetry action itself. In the quantum mechanics of wavefunctions on $\mathbb{R}$, the self-adjoint momentum operator $\mathbf{p}$ is traditionally obtained from the translation symmetry action $(U_x)_{x\in\mathbb{R}}$ by using Stone's theorem on 1-parameter unitary groups [Sto30, Sto32]:

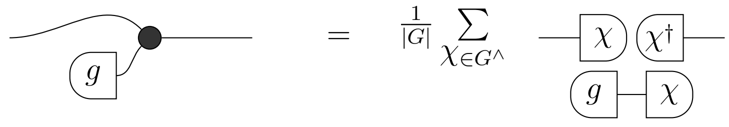
$$U_x := e^{ix\mathbf{p}} = \sum_p e^{ixp}|p\rangle\langle p| \tag{3.55}$$

We have already seen that taking infinitesimal generators does not yield a well defined self-adjoint momentum operator when working on periodic lattices, not even in the traditional quantum mechanical formalism. Hence we will aim for something like Equation 3.34:

$$U_g := \frac{1}{|G|}\sum_\chi \chi(g)|\chi\rangle\langle\chi|$$

Unfortunately, we don't have the luxury of sums. We need to look for a more structural way of phrasing Equation 3.34, one which we can formulate, and hopefully prove, in our more abstract framework. As it turns out, Theorem 3.17 already provides us with such an alternative phrasing, since in quantum mechanics the following is true:

U_g :=



(3.56)

As a consequence, Theorem 3.17 already proved that the momentum observable, seen as the †-qSFA ●, generates the translation symmetry action.

3.3.3 Positions generate boost symmetry

Having completed our description of the connection between ●, our candidate momentum observable, and the translation symmetry action, we now characterise the dual relationship between the position observable, embodied by ○, and the boost symmetry action. To begin with, we need to formalise what we mean by boost symmetry.

In the quantum mechanical case of $\mathbb{C}[G]$, momentum eigenstates $|\chi\rangle$ correspond to multiplicative characters $\chi : G \to \mathbb{C}$. Any multiplicative character χ can be written as χ_h in the following form, for some (non-unique) $h = (h_d)_{d=1}^D \in G \cong \prod_{d=1}^D \mathbb{Z}_{n_d}$:

$$\chi_h = g \mapsto e^{2\pi i\, g\cdot h} \tag{3.57}$$

where $g \cdot h := \sum_{d=1}^D \frac{g_d \cdot h_d}{n_d}$, and each product $g_d \cdot h_d$ is taken modulo n_d. An element $h = (h_d)_{d=1}^D \in G$ is a vector, describing some direction and magnitude on the lattice:

as a consequence we can think of $|\chi\rangle$ as the momentum eigenstate associated with "moving with momentum h on the lattice". Contrary to the case of wavefunctions over $\mathbb{R}$, there is no canonical choice for h in the periodic lattice case, and hence it is best to work directly with the multiplicative character χ.

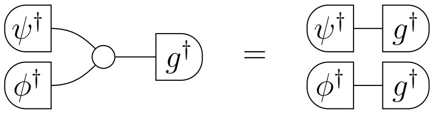
We've already seen that the multiplicative characters $\chi : G \to \mathbb{C}$ of the finite abelian group G form the Pontryagin dual group $G^\wedge$ under pointwise multiplication, but what does this have to do with boosts? To see exactly what's going on, we need to observe the effect of pointwise multiplication $\chi_h \cdot \chi_{\delta h}$ on the explicit form given by Equation 3.57:

$$\chi_h \cdot \chi_{\delta h} = g \mapsto e^{2\pi i\, g\cdot h} e^{2\pi i\, g\cdot \delta h} = e^{2\pi i\, g\cdot (h\oplus\delta h)} \tag{3.58}$$

Hence, if we interpret χ_h as moving with momentum h on the lattice, and $\chi_{\delta h}$ as moving with momentum δh on the lattice, then $\chi_h \cdot \chi_{\delta h}$ should be interpreted as moving with momentum $h \oplus \delta h$ on the lattice. This is why the Pontryagin dual group structure on the multiplicative characters is referred to as the **boost symmetry**.

Perhaps unsurprisingly, the Pontryagin duality between the translation symmetry group and the boost symmetry group in quantum mechanics lifts to a duality between corresponding coherent groups. Perhaps more surprisingly, the duality on the coherent group side has a much simpler characterisation than Pontryagin duality. Theorem 3.19 introduces the notion of dual coherent group, while Theorem 3.20 gives a first bout of legitimacy to the idea that duality of coherent groups generalises Pontryagin duality (the two coincide in the case of well-pointed abelian coherent groups in fHilb).

Theorem 3.19 (Dual coherent group).
*Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{H}$ of a $\dagger$-SMC $\mathcal{C}$. Then the **dual coherent group** $\mathbb{G}^\wedge := (\bullet, \circ)$ is also a coherent group, with the adjoints $\chi^\dagger$ of the multiplicative character of $\mathbb{G}$ as its points. The multiplicative structure $\circ$ of $\mathbb{G}^\wedge$ acts by pointwise composition:*

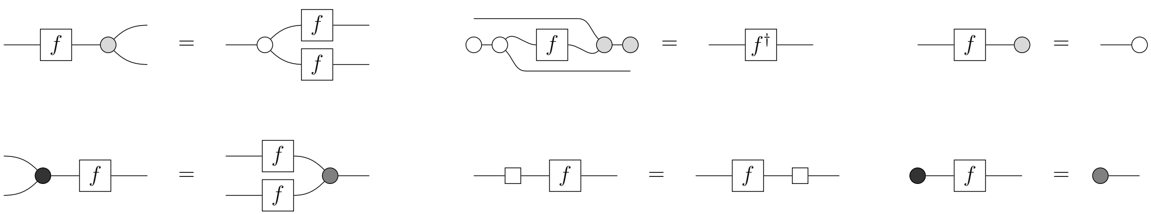


(3.59)

Finally, the following defines an involutive monoidal functor $\wedge : \mathrm{QG}\left[\mathcal{C}\right] \to \mathrm{QG}\left[\mathcal{C}\right]^{\mathrm{op}}$ on coherent groups in a $\dagger$-SMC $\mathcal{C}$:

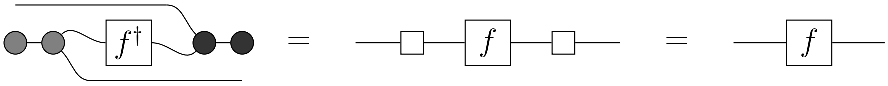
$$\begin{aligned} (\circ, \bullet)^\wedge &:= (\bullet, \circ) \\ f^\wedge &:= f^\dagger \end{aligned} \tag{3.60}$$

Proof. The conditions defining a coherent group $\mathbb{G} := (○, ●)$ are symmetric in ○ and ● (see Definition 3.6 and Remark 3.7), so $\mathbb{G}^\wedge := (●, ○)$ satisfies the same conditions and is a coherent group. We have also already observed that the ●-classical states coincide with the multiplicative characters of $\mathbb{G}$, and the pointwise multiplication action of ○ on them is a consequence of the copy condition for the points of $\mathbb{G}$, which are ○-classical states. We now need to show that $^\wedge$ is an involutive monoidal functor. It is definitely involutive and monoidal, as long as we can show that it is a well-defined functor. We just showed that if (○, ●) is a coherent group, then so is its dual (●, ○), so the functor $^\wedge$ is well-defined on objects. Because the dagger is a functor, all we need to show is that if $f : (○, ●) \to (○, ●)$ is a coherent group homomorphism, then $f^\dagger : (●, ○) \to (●, ○)$ is also a coherent group homomorphism. Below we present the six equations that define f as a coherent group homomorphism:



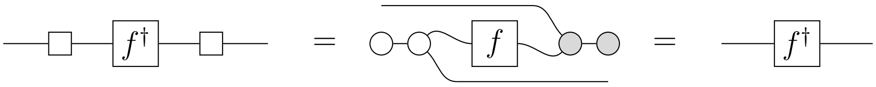
(3.61)

Taking adjoints of the two leftmost equations for f yields the two leftmost equations for $f^\dagger$, and similarly taking adjoints of the two rightmost equations for f implies the two rightmost equations for $f^\dagger$. All we need to show is that the central two equations for f imply the central two equations for $f^\dagger$. First we prove the adjoint condition for $f^\dagger$, using the central two equations for f:



(3.62)

Then we use the central two equations for f and the top central equation for $f^\dagger$ we have just obtained to prove the bottom central equation for $f^\dagger$ (recall that the antipode is self-inverse):



(3.63)

This concludes the proof, showing that $^\wedge$ is an involutive monoidal functor. □

We will often refer to the underlying group $[\![\mathbb{G}^\wedge]\!] = (K(●),$ ⊱ , ○– $)$ in terms of multiplicative characters of $\mathbb{G}$, in which case we will write its operation as $\cdot$ (*pointwise multiplication*) and its unit as $\mathbb{1}$ (the *trivial character*).

Lemma 3.20. *Let* wpAbQG [fHilb] *be the category of well-pointed, abelian coherent groups in* fHilb*, a full subcategory of* QG [fHilb]*. Then the functor* $[\![\_]\!]$: wpAbQG [fHilb] → fAbGrp *is well-defined, induces an equivalence of categories, and makes the following diagram commute:*

$$\begin{tikzcd}
\mathrm{wpAbQG}\,[\mathrm{fHilb}] \arrow[r, "\wedge"] \arrow[d, "{[\![\_]\!]}"'] & \mathrm{wpAbQG}\,[\mathrm{fHilb}]^{\mathrm{op}} \arrow[d, "{[\![\_]\!]^{op}}"] \\
\mathrm{fAbGrp} \arrow[r, "\wedge"] & \mathrm{fAbGrp}^{\mathrm{op}}
\end{tikzcd} \tag{3.64}$$

This shows that Pontryagin duality $^\wedge$ *for finite abelian groups corresponds exactly to the duality* $^\wedge$ *on well-pointed abelian coherent groups in* fHilb*.*

Proof. The underlying group functor $[\![\_]\!]$: wpAbQG [fHilb] → fAbGrp is full, faithful and essentially surjective because of Theorem 3.15. We've already observed that in fHilb the multiplicative characters of an abelian coherent group $(\circ, \bullet)$ are the multiplicative characters of the underlying group: hence $[\![\mathbb{G}^\wedge]\!] = [\![\mathbb{G}]\!]^\wedge$ in fHilb, and the diagram commutes on objects. To see that it also commutes on morphisms, consider a coherent group homomorphism f with $[\![f]\!] : G \to H$ for some finite abelian groups G, H. Then we have that both $[\![f^\wedge]\!]^{op}$ and $[\![f]\!]^\wedge$ are morphisms $H^\wedge \to G^\wedge$, with the following explicit expressions:

$$\begin{aligned} [\![f^\wedge]\!]^{op} &= \chi \mapsto (f^\wedge \circ \chi^\dagger)^\dagger = \chi \circ f \\ [\![f]\!]^\wedge &= \chi \mapsto \chi \circ f \end{aligned} \tag{3.65}$$

The two expressions coincide, showing that Diagram 3.64 also commutes on morphisms. □

Remark 3.21. *We might try to generalise the Pontryagin duality side of Theorem 3.20 as follows. Given a group G and another group K, we can define the* ***dual*** *$G^{\wedge_K}$ of G with respect to K to be the group*[10] *of homomorphisms $G \to K$ (the* ***K-valued multiplicative characters****) under pointwise multiplication (the inverse of $\chi : G \to K$ is given by $g \mapsto \chi(g^{-1})$). When $K = S^1$ and G is abelian, $G^{\wedge_{S^1}}$ is the*

[10] Abelian when either one of K or G is commutative.

usual Pontryagin dual of G. We can turn $^{\wedge_M}$ into a functor $^{\wedge_M} : \mathrm{Grp} \to \mathrm{Grp}$ by setting $f^{\wedge_M} := \_ \circ f$, exactly as in the usual $M = S^1$ case.

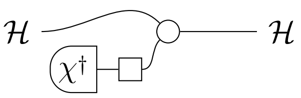
Now consider coherent groups in a †-SMC $\mathcal{C}$, and let K be the group of ***units*** *in $\mathcal{C}$, i.e. those scalars x such that $x^\dagger x = 1$. The Diagram 3.64, where Pontryagin duality $^\wedge : \mathrm{fAbGrp} \to \mathrm{fAbGrp}^{\mathrm{op}}$ is replaced by $^{\wedge_K} : \mathrm{Grp} \to \mathrm{Grp}$, still commutes on morphisms: we have $[\![f^\wedge]\!] = [\![f]\!]^{\wedge_K}$ for all coherent group homomrphisms f. However, the new Diagram need not commute on objects: we always have that $[\![\mathbb{G}^\wedge]\!] \leq [\![\mathbb{G}]\!]^{\wedge_K}$, but equality need not hold. Further investigation is left to future work.*

Recall that the group of position eigenstates under translation symmetry for the coherent group $\mathbb{G} = (\circ, \bullet)$ is given by the underlying group $G = [\![\mathbb{G}]\!] = (K(\circ), \succ\!\bullet\!- , \bullet\!-)$: the discussion until this point makes it clear that the correct choice for the group of momentum eigenstates under boost symmetry should be the underlying group $[\![\mathbb{G}^\wedge]\!] = (K(\bullet), \succ\!\circ\!- , \circ\!-)$ of the dual coherent group $\mathbb{G}^\wedge = (\bullet, \circ)$.

Now that we have figured out what boost symmetry in our generalise setting should be, we need to confirm that it relates as expected to the position observable: need to show that positions generate our choice of boost symmetry (in the same sense as momenta generating translation symmetry in Theorem 3.17), and that they are the invariant states for boost symmetry (in the same sense as momenta being the invariant states of translation symmetry in Theorem 3.18).

Theorem 3.22 (**Positions generate boosts**).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{H}$ of a †-SMC $\mathcal{C}$, and let $X := (K(\bullet), \succ\!\circ\!- , \circ\!-)$ be the underlying group for the dual $\mathbb{G}^\wedge$. Define a family $(V_\chi)_{\chi^\dagger \in X}$ of endomorphisms of $\mathcal{H}$ as follows:

$V_\chi \quad :=$



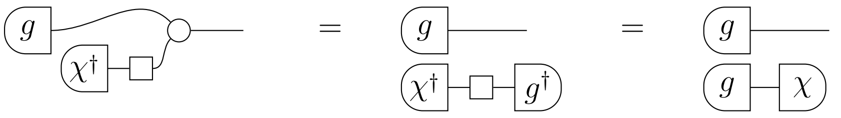
(3.66)

Then $(V_\chi)_{\chi^\dagger \in X}$ gives a unitary action of the group X on $\mathcal{H}$, restricting to the left regular action of the boost symmetry group $[\![\mathbb{G}^\wedge]\!]$ on the points of the dual coherent group $\mathbb{G}^\wedge$.

Proof. This is nothing but Theorem 3.17 applied to the dual coherent group $\mathbb{G}^\wedge$. □

Theorem 3.23 (**Positions invariant under boost**).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{H}$ of a †-SMC $\mathcal{C}$, and let $X :=$

$(K(\bullet)$, ⟩○– , ○– $)$ be the underlying group of the dual coherent group $\mathbb{G}^\wedge$. The points of $\mathbb{G}$ are invariant under the boost symmetry action, up to a scalar:



(3.67)

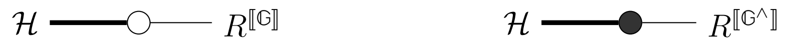
Furthermore, the scalar $\chi(g) = \chi \circ g$ satisfies $\chi(g)^\dagger \cdot \chi(g) = 1$. Finally, assume that the dual coherent group $\mathbb{G}^\wedge$ is well-pointed, and consider a state g: if both (i) Equation 3.67 holds for all multiplicative characters χ of $\mathbb{G}$, and (ii) –○ $(g)^\dagger \cdot$ –○ $(g) = 1$, then g must be a point of $\mathbb{G}$.

Proof. This is nothing but Theorem 3.18 applied to the dual coherent group $\mathbb{G}^\wedge$. □

Looking at the assumptions of Theorem 3.23, we see a problem arise: while position eigenstates (the points of the coherent group $\mathbb{G}$) are always invariant under boost symmetry and generate it, Theorem 3.23 does not guarantee that they will be the *only* invariant states unless the dual coherent group $\mathbb{G}^\wedge$ is itself well-pointed. This is always true for a well-pointed abelian coherent group $\mathbb{G}$ in fHilb, because the points of the dual $\mathbb{G}^\wedge$ correspond exactly to the multiplicative characters of the underlying abelian group $[\![\mathbb{G}]\!]$: the latter form a basis, and hence $\mathbb{G}^\wedge$ is itself well-pointed. However, it need not be true in general.

We will say that a coherent group $\mathbb{G}$ is **doubly well-pointed** if both $\mathbb{G}$ and $\mathbb{G}^\wedge$ are well-pointed. It is worth noting that a doubly well-pointed coherent group is necessarily abelian, and that the dual of a doubly well-pointed coherent group is itself doubly well-pointed. From a physical perspective, well-pointedness models the requirement that there must be enough position eigenstates to distinguish different processes from $\mathcal{H}$: processes are entirely determined by what they do to the position eigenstates. Double well-pointedness models the additional requirement that there must also be enough momentum eigenstates to distinguish different processes from $\mathcal{H}$, i.e. that processes are also entirely determined by what they do to the momentum eigenstates. In the light of these developments, we will henceforth require the coherent group modelling wavefunctions on a periodic lattice to be doubly well-pointed (which, as we mentioned, is a special case of well-pointed abelian). The same requirement will carry through to Sections 3.6 and 3.5.

When $\mathbb{G}$ is doubly well-pointed, we can write both the position measurement and the **momentum measurement** in $\mathrm{CP}^*[\mathcal{C}]$ (which we assume to be R-probabilistic) as processes with output in an appropriate classical system:



position measurement   momentum measurement   (3.68)

Before moving on to the Weyl CCRs, let's go over a brief summary of our work until this point. At the beginning of Section 3.4, we have considered a well-pointed coherent group $\mathbb{G} = (\circ, \bullet)$ having finitely many points as an abstract model of wavefunctions on a periodic lattice. This is because the points $K(\circ)$ of the coherent group form a finite abelian group $[\![G]\!] = (K(\circ), \succ\!\!\bullet\!- , \bullet\!-) \cong \prod_{d=1}^{D} \mathbb{Z}_{n_d}$, which can be interpreted as a D-dimensional periodic lattice Λ endowed with the group structure of translation symmetry.

While $\circ$ is the natural candidate for the position observable, identifying $\bullet$ with the momentum observable is more challenging. In Subsection 3.3.1, we have compiled a list of operational and structural properties characterising the relationship between the position and momentum observables for wavefunctions on periodic lattices in the traditional formulation of quantum mechanics:

(a) that the momentum eigenstates are invariant under the translation symmetry action, and that they generate it;

(b) that the position eigenstates are invariant under the boost symmetry action, and that they generate it;

(c) that the Weyl Canonical Commutation Relations hold;

(d) that the weak form of the uncertainty principle (see Subsection 3.3.1) holds.

In Subsection 3.3.2, we have shown that the classical states $K(\bullet)$ for the $\bullet$ observable, our putative momentum eigenstates, are exactly the invariant states for the translation symmetry action on wavefunctions, which that they furthermore generate. In Subsection 3.3.3, we have identified the boost symmetry in the underlying group $[\![\mathbb{G}^\wedge]\!] = (K(\bullet), \succ\!\!\circ\!- , \circ\!-)$ of the dual coherent group $\mathbb{G}^\wedge = (\bullet, \circ)$. We have then shown that the position eigenstates $K(\circ)$ are invariant states for the boost symmetry action on wavefunctions, which they generate. In order to characterise the position eigenstates as *exactly* the invariant states under the boost symmetry action, we strengthened our requirements on $\mathbb{G}$, assuming that it is doubly well-pointed.

We are half-way through: points (a) and (b) of our list are down, points (c) and (d) remain to be shown. These will be the topic of the next two Subsections.

3.3.4 Weyl Canonical Commutation Relations

We have already mentioned in Equation 3.38 that the Weyl CCRs for wavefunctions on periodic lattices should take the following form:

$$V_\chi U_g = \chi(g)\ U_g V_\chi$$

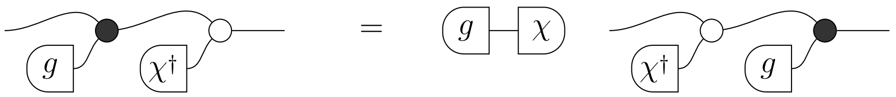
This is in direct analogy with the traditional Weyl CCRs from Equation 3.36:

$$V_p U_x = e^{i\hbar p\cdot x}\ U_x V_p$$

There is a single difference between Equation 3.36 and Equation 3.38: in the former, the momentum eigenstates are labelled by the eigenvalues p of the infinitesimal generator $\mathbf{p}$, while in the latter the momentum eigenstates are labelled by the multiplicative characters χ of the translation symmetry group. As a consequence, the phase in Equation 3.36 is written explicitly as $e^{i\hbar p\cdot x}$, while the phase in Equation 3.38 is obtained more naturally by evaluating the multiplicative character χ labelling the momentum eigenstate on the group element g labelling the position eigenstate. Refer to Subsection 2.4.3 for the reasons behind this choice.

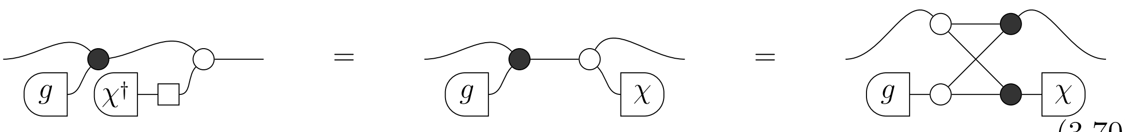
Theorems 3.17 and 3.22 already provide us with an abstract description of the unitaries U_g and V_χ, and of the scalar $\chi(g)$: all we need to show is that they respect Equation 3.38.

Theorem 3.24 (**Weyl Canonical Commutation Relations**).
Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group in a †-SMC $\mathcal{C}$, and define the families of unitaries $(U_g)_{g\in[\![\mathbb{G}]\!]}$ and $(V_\chi)_{\chi^\dagger\in[\![\mathbb{G}^\wedge]\!]}$ as in Equations 3.44 and 3.66. Then the Weyl Canonical Commutation Relations from Equation 3.38 hold:



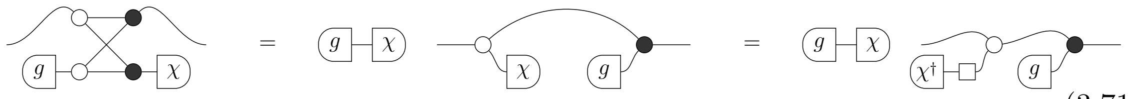
(3.69)

Proof. The proof hinges on the bialgebra law from strong complementarity, on the definition of the antipode, and on the copy/adjoin conditions for $\circ$-classical and $\bullet$-classical states. The first equality below uses the definition of the antipode and the adjoin condition for the $\bullet$-classical state $\chi^\dagger$, while the second equality uses the bialgebra law:



(3.70)

The first equality below uses the copy condition for the ○-classical state g and the ●-classical state -□- $\circ\, \chi$ (because the antipode is a function on ●-classical states), while the second equality uses again the definition of the antipode and the adjoin condition for the ●-classical state χ:



(3.71)

This completes our proof of the Weyl Canonical Commutation Relations. □

In the traditional presentation of quantum mechanics, the Weyl Canonical Commutation Relations make an important appearance as part of the Stone-von Neumann Theorem [Sto30, vN31, Sto32, vN32a]. Consider two jointly irreducible unitary representations $(U_t)_{t\in\mathbb{R}}$ and $(V_s)_{s\in\mathbb{R}}$ of the abelian group $(\mathbb{R}, +, 0)$ on some separable Hilbert Space $\mathcal{H}$: the Stone-von Neumann Theorem states that if they satisfy the Weyl Canonical Commutation Relations from Equation 3.36 then they are jointly unitarily equivalent to the translation and boost symmetry actions on $\mathrm{L}^2[\mathbb{R}]$, i.e. there is some unitary $W : \mathrm{L}^2[\mathbb{R}] \to \mathcal{H}$ such that $W^\dagger U_t W = e^{it\mathbf{x}}$ and $W^\dagger V_s W = e^{is\mathbf{p}}$.

We cannot expect such a direct and precise result in our case, for a variety of reasons. First and foremost, we have as many inequivalent notions of position and momentum as there are periodic lattices: Equation 3.36 gives an explicit braiding relation, with e^{ipx} as phase, while Equation 3.38 gives a braiding relation parametrized on the multiplicative characters, with $\chi(g)$ as phase. However, substituting an explicit form for $\chi(g)$ singles out a unique lattice position/momentum pair: e.g. writing $\chi(g) = e^{i2\pi\frac{pg}{10}}$ in fHilb singles out the position/momentum pair for the 1-dimensional lattice $\mathbb{Z}_{10}$, while writing $e^{i2\pi(\frac{p_1 g_1}{4}+\frac{p_2 g_2}{8})}$ singles out the position/momentum pair for the 2-dimensional lattice $\mathbb{Z}_4 \times \mathbb{Z}_8$. In fact, this is the same for the Stone-von Neumann Theorem in its modern form: the 1-dimensional e^{ipx} case for the group $(\mathbb{R}, +, 0)$ was the first to be proven, but a straightforward generalisation exists for all the groups $(\mathbb{R}^n, +, 0)$, with phases given by $e^{i\sum_{j=1}^{n} p_j x_j}$.

There is a second, structural reason why we cannot expect a result as tight as the Stone-von Neumann Theorem in the general setting of coherent groups on †-SMCs: both the original result and its generalisations to Mackey theory rely both on Pontryagin duality and on a considerable amount of continuous and integrable structure. In an general †-SMC $\mathcal{C}$, the possible choices for a position/momentum pair are classified by the (doubly well-pointed) coherent groups, rather than the underlying groups: the functor $[\![\_]\!]$ on doubly well-pointed coherent groups is faithful, but not necessarily full, and as a consequence it might not be possible to find a suitable subcategory of groups which classify the position/momentum pairs on systems of $\mathcal{C}$.[11]

The search for a suitable extension of the Stone-von Neumann Theorem to coherent groups in arbitrary †-SMCs is left to future work.

3.3.5 Uncertainty principle

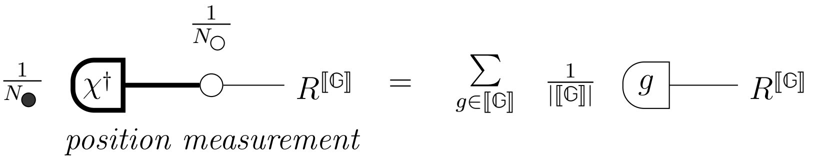
As of this point, we are three fourths of the way to establishing that ● is a suitable momentum observable in a coherent group: we have proven (a) the relationship between momentum observable and translation symmetry; (b) the relationship between position observable and boost symmetry; (c) the Weyl Canonical Commutation Relations. There is one final piece of evidence that we tasked ourselves with finding: item (d), the uncertainty principle.

It was already remarked in Subsection 3.3.1 that the full Kennard-Weyl form of the uncertainty principle from Equation 3.39 is too strong to be considered a characteristic trait of position/momentum duality: it essentially implies contextuality, an operational feature of quantum theory that we believe should not play a direct role in the abstract treatment of mechanics and dynamics. In this light, we proposed that a suitable compromise would involve restricting our attention to the position and momentum observables themselves, and show that position eigenstates have completely indeterminate momentum, and vice versa that momentum eigenstates have completely indeterminate position. But we already know this is going be true: Lemma 3.4 states that any complementary pair is mutually unbiased, and in particular so will be the pair of observables ○ and ● appearing in a coherent group (which by definition must be strongly complementary, and hence complementary).

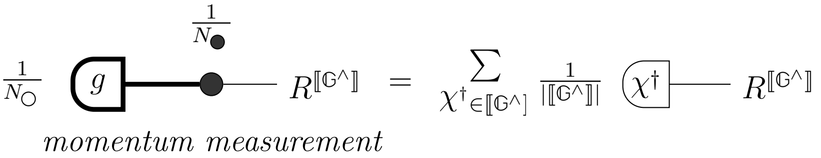
Theorem 3.25 (**Weak uncertainty principle**).
Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group on an object $\mathcal{H}$ of a †-SMC, and let $N_{\circ}$ and $N_{\bullet}$ be the normalisation factors of the †-qSFA ○ and ● respectively. Then the points of $\mathbb{G}$, i.e. the position eigenstates $K(\circ)$, are unbiased for the momentum observable ●. Conversely, the points of the dual coherent group $\mathbb{G}^\wedge$, i.e. the momentum eigenstates $K(\bullet)$, are unbiased for the position observable ○. If $\mathbb{G}$ is doubly well-pointed and ***doubly finite*** *(by which we mean it has finitely many points and multiplicative characters), we get*

[11] Contrary to fHilb, where the functor $[\![\_]\!]$ is full and faithful on doubly well-pointed coherent groups, and essentially surjective onto the subcategory of finite abelian groups.

the following in $\mathrm{CP}^*[\mathcal{C}]$ *(which we assume to be R-probabilistic):*



(3.72)


$\frac{1}{N_\bigcirc}$
$\frac{1}{N_\bullet}$
g
$R^{[\![\mathbb{G}^\wedge]\!]}$
=
$\sum_{\chi^\dagger\in[\![\mathbb{G}^\wedge]\!]}$
$\frac{1}{|[\![\mathbb{G}^\wedge]\!]|}$
$\chi^\dagger$
$R^{[\![\mathbb{G}^\wedge]\!]}$
momentum measurement

(3.73)

Note that the states on the RHS of the two equations above are the states of $R^{[\![\mathbb{G}]\!]}$ *and* $R^{[\![\mathbb{G}^\wedge]\!]}$ *corresponding to elements* $g \in [\![\mathbb{G}]\!]$ *and* $\chi^\dagger \in [\![\mathbb{G}]\!]$*: they correspond to the normalised CPM states* $\frac{1}{N_\bigcirc}$***double***$[g]$ *and* $\frac{1}{N_\bullet}$***double***$\left[\chi^\dagger\right]$ *respectively.*

Proof. Essentially Lemma 3.4, taking into account the normalisation factors of the two †-qSFAs and using the fact that they both have enough classical states (so that both $(\mathcal{H}, \circ)$ and $(\mathcal{H}, \bullet)$ are classical systems in $\mathrm{CP}^*[\mathcal{C}]$). □

We have finally come to the end of our quest: we have shown that the point structure $\circ$ and group structure $\bullet$ in a coherent group $\mathbb{G} := (\circ, \bullet)$ possess the main operational and structural features that we would expect from a position/momentum pair. In particular, doubly well-pointed, doubly finite coherent groups can always be interpreted as defining the position/momentum pair for wavefunctions on a periodic lattice, as made clear by the following summary of the work to this point.

(i) The points $K(\circ)$ of a finite coherent group are endowed with the group structure $\prod_{d=1}^{D} \mathbb{Z}_{n_d}$ of some periodic lattice Λ. They can therefore be interpreted as position eigenstates wavefunctions on the lattice, and $\circ$ can be interpreted as the position observable.

(ii) The processes from a well-pointed coherent group are entirely determined by their action on the position eigenstates, excluding the existence of additional underlying structure.

(iii) The momentum observable $\bullet$ in a well-pointed coherent group generates the translation symmetry action on the wavefunctions, and its classical states $K(\bullet)$ are the invariant states for that action.

(iv) The position observable $\circ$ in a doubly well-pointed coherent group generates the boost symmetry action on the wavefunctions, and its classical states $K(\circ)$ are the invariant states for that action.

(v) The position observable $\circ$ and the momentum observable $\bullet$ in a coherent group always satisfy the Weyl Canonical Commutation Relations.

(vi) The position and momentum observables are always mutually unbiased. In a doubly well-pointed, doubly finite coherent group we can define both a position measurement and a momentum measurement in the CP* category (assuming the latter is R-probabilistic), with outcomes in the classical systems $R^{[\![\mathbb{G}]\!]}$ and $R^{[\![\mathbb{G}^\wedge]\!]}$ respectively. Measuring the position of a (normalised) momentum eigenstate yields the uniform distribution on $R^{[\![\mathbb{G}]\!]}$, proving that momentum eigenstates have completely indeterminate positions. Similarly, measuring the momentum of a (normalised) position eigenstate yields the uniform distribution on $R^{[\![\mathbb{G}^\wedge]\!]}$, proving that position eigenstates have completely indeterminate momentum.

3.4 Systems with symmetries

Up until this moment, we have restricted our attention to the concrete example of wavefunctions on periodic lattices, which we have abstractly identified with doubly well-pointed, doubly finite coherent groups. However, almost none of the results we obtained requires well-pointedness or finiteness: the picture they paint is that coherent groups *in general* have many of the structural properties of position/momentum pairs for wavefunctions on symmetric systems. There are some issues arising when the groups are well-pointed but not doubly well-pointed, such as in the case of non-abelian group algebras in fHilb, which will be covered in future work. There are also some issues with the operational interpretation of non-finite coherent groups, which will be covered in Section 3.5. However, the overall picture as it stands is solid enough, and throughout this Section we will interpret coherent groups as modelling a sensible notion of wavefunctions over symmetry groups.

Just like representations of classical groups yield the notion of physical systems with a classical symmetry, we expect that a suitable notion of representation for coherent groups will yield a suitable notion of physical system with a coherent symmetry. The topic of this section will be the definition and study of said representations.

3.4.1 Unitary representations of coherent groups

In the traditional formalism, a quantum system with periodic lattice symmetry is given by a unitary representation $(U_g)_{g \in G}$ of the translation symmetry group $G = \prod_{d=1}^{D} \mathbb{Z}_{n_d}$ on a Hilbert space $\mathcal{H}$, and wavefunctions on a periodic lattice arise as the special case $\mathcal{H} = \mathbb{C}[G]$ with the regular action $g(|h\rangle) := |g \oplus h\rangle$. In the coherent approach, we consider unitary representations of coherent groups instead, and the physical intuition behind this choice goes as follows. Unitary representations of a group can be seen as controlled unitaries, where the controlling system is classical: in the case of periodic lattice symmetries, the controlling system is the periodic lattice itself (or, equivalently, the classical system of distributions over the lattice). In the passage from the classical to the coherent approach, we wish the states of the controlling system to be wavefunctions over the lattice instead of distributions: as our work to this point shows, this is the same as moving from a (finite abelian) group to a (doubly well-pointed, doubly finite) coherent group.

But what should we take as a unitary representation of a coherent group $\mathbb{G}$ in a generic †-SMC? One possible approach to figuring this out starts from the definition of representations of finite groups in fHilb, and tries to replace all the classical bits and pieces with their coherent counterparts. Recall that a unitary representation $(U_g)_{g\in G}$ of a group[12] (G, m, e, i) on a finite-dimensional Hilbert space $\mathcal{H}$ is a function $\alpha : \mathcal{H} \times G \to \mathcal{H}$, such that $U_g = \alpha(\_\,, g)$ is linear for all $g \in G$ and with α satisfying the following three conditions:

$$\alpha\big(\_\,, m(g,h)\big) = U_{gh} = U_h U_g = \alpha\big(\alpha(\_\,,h), g\big) \tag{3.74}$$

$$\alpha(\_\,, e) = U_e = id_{\mathcal{H}} \tag{3.75}$$

$$\alpha(\_\,, i(g)) = U_{g^{-1}} = U_g^{-1} = U_g^{\dagger} = \Big(\alpha(\_\,, g)\Big)^{\dagger} \tag{3.76}$$

We make the following modifications: instead of the group G and function $\alpha : \mathcal{H} \times G \to \mathcal{H}$, we work with the group algebra $\mathbb{C}[G]$ (which we see as a well-pointed coherent group $\mathbb{G} := (\circ, \bullet))$ and a linear map $\alpha : \mathcal{H} \otimes \mathbb{C}[G] \to \mathcal{H}$. We replace the three conditions above with the following conditions involving the linear extensions $\succ\!\!\bullet\!\!-$, $\bullet\!\!-$ and $-\!\square\!-$ of the multiplication m, unit e and inverse i:

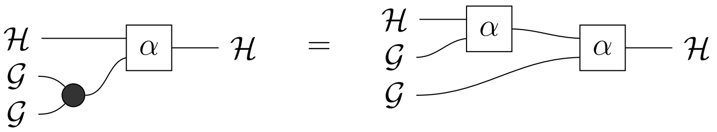
$$\alpha\big(\_\,, \succ\!\!\bullet\!\!- \circ (|g\rangle \otimes |h\rangle)\big) = \alpha\big(\alpha(\_\,, |g\rangle), |h\rangle\big) \tag{3.77}$$

$$\alpha(\_\,, \bullet\!\!-) = id_{\mathcal{H}} \tag{3.78}$$

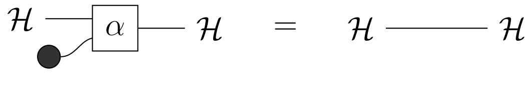
$$\alpha(\_\,, -\!\square\!- |g\rangle) = \Big(\alpha(\_\,, |g\rangle)\Big)^{\dagger} \tag{3.79}$$

As a final step, we get rid of the evaluation over group elements (a very classical thing to do), and obtain a definition which solely involves the coherent group $\mathbb{G}$.

Definition 3.26. *Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let $\mathcal{H}$ be another object of $\mathcal{C}$. A **representation** of $\mathbb{G}$ on $\mathcal{H}$ is a process $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ satisfying the following two requirements:*

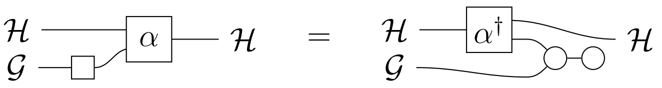


(3.80)



(3.81)

*We say that a representation α is **unitary** if it satisfies the following additional requirement:*



(3.82)

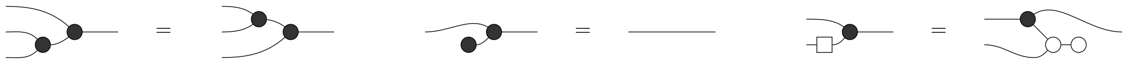
[12] We denote the group multiplication by $m : G \times G \to G$, the group unit by $e : 1 \to G$, and the group inverse by $i : G \to G$.

Equations 3.80 and 3.81 are straightforward graphical translations of Equations 3.77 and 3.78. Equation 3.82 sees, further to Equation 3.79, the introduction of the symmetric cup for the point structure. This is because in Equation 3.79 we take the adjoint of the representation *already evaluated* at $|g\rangle$, and hence from a compositional perspective we are taking the adjoint of $|g\rangle$ as well: this is achieved by using the symmetric cup, as prescribed by the adjoin condition for $\circ$-classical states, which leads to the graphical formulation of Equation 3.82.

To make sure that our definition of coherent symmetries is sensible, we need to check two things: (i) that our definition is consistent with the definition of coherent translation symmetry for wavefunctions on a periodic lattice, and (ii) that our definition yields back the classical symmetries by appropriate use of preparations/measurements. Just to clarify, by a (unitary) representation of a group G on an object $\mathcal{H}$ of a †-SMC we mean a family $(U_g)_{g \in G}$ of (unitary) processes $U_g : \mathcal{H} \to \mathcal{H}$ such that $U_{gh} = U_h U_g$ and $U_e = id_{\mathcal{H}}$.

Lemma 3.27. *Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a †-SMC. Then* *: $\mathcal{G} \otimes \mathcal{G} \to \mathcal{G}$ is a unitary representation of $\mathbb{G}$ on $\mathcal{G}$, which we will refer to as the* ***regular representation*** *of $\mathbb{G}$.*

Proof. The first requirement for a representation of $\mathbb{G}$ is a consequence of associative law, the second requirement for a representation of $\mathbb{G}$ is a consequence of unit law, and the additional requirement for a unitary representation of $\mathbb{G}$ is a consequence of Frobenius law and unit law (once the antipode is expanded in terms of symmetric cap/cap of the point/group structure of $\mathbb{G}$):

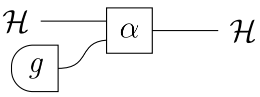


(3.83)

This completes the proof, showing that is indeed a unitary representation of the coherent group $\mathbb{G}$. □

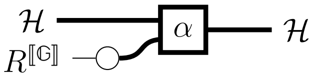
Theorem 3.28 (Underlying group reps from coherent group reps).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a (unitary) representation of $\mathbb{G}$ on an system $\mathcal{H}$ in $\mathcal{C}$. Then the following defines a (unitary) representation $(U_g)_{g \in [\![\mathbb{G}]\!]}$ of $[\![\mathbb{G}]\!]$ on $\mathcal{H}$:

$$U_g \quad :=$$



(3.84)

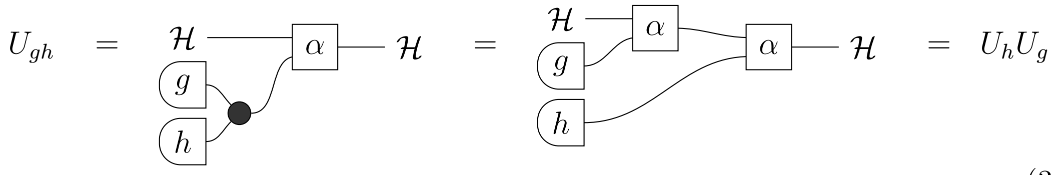
If CP*[$\mathcal{C}$] *is R-probabilistic and* $\mathbb{G}$ *is well-pointed, then we can write the representation of the underlying group* ⟦$\mathbb{G}$⟧ *as the following classically controlled process:*



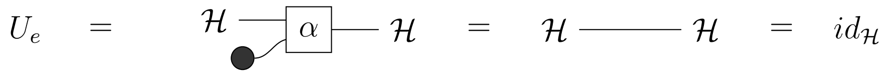
(3.85)

If α *is a unitary representation, then the process above is in fact a controlled unitary.*

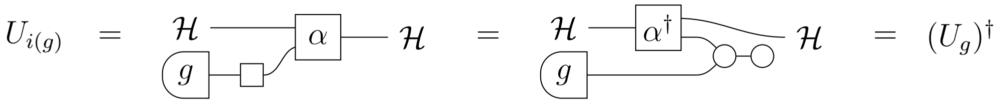
Proof. The first claim follows straightforwardly from the requirements satisfied by a (unitary) representation α for $\mathbb{G}$ and from the definition of the underlying group ⟦$\mathbb{G}$⟧ := (K(○), ⟩●- , ●-):



(3.86)

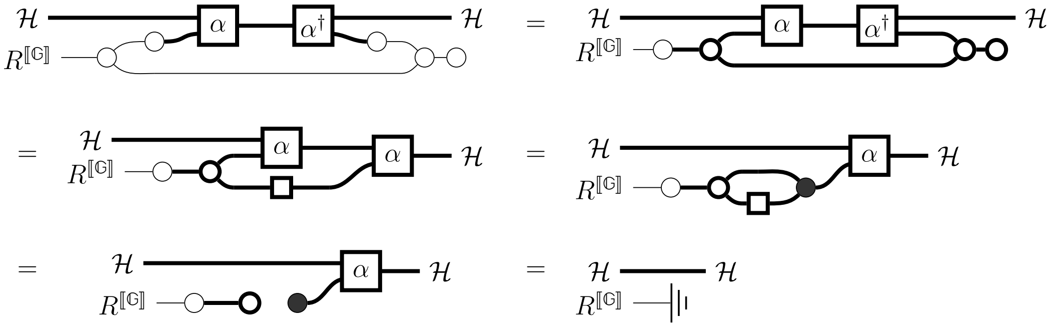


(3.87)



(3.88)

Recasting the representation in the form of Diagram 3.85 is also completely straightforward, but statement that it yields a controlled unitary when α is a unitary representation deserves graphical proof:



(3.89)

The other half of the proof of controlled unitarity goes along the exact same lines. □

3.4.2 The category of representations of a coherent group

Our definition of a coherent group representation is a very concrete one, which we extrapolated directly from the definition of classical group representations. Instead, we would prefer a more categorical characterisation of coherent group representations.

We begin by looking at the following commuting diagrams, involving a representation α of a coherent group $\mathbb{G} := (\circ, \bullet)$ on a system $\mathcal{H}$ of a generic †-SMC $\mathcal{C}$:

$$\begin{tikzcd}
\mathcal{H}\otimes\mathcal{G}\otimes\mathcal{G} \arrow[r, "\alpha\otimes id_{\mathcal{G}}"] \arrow[d, "id_{\mathcal{H}}\otimes \succ\!\bullet\!-"'] & \mathcal{H}\otimes\mathcal{G} \arrow[d, "\alpha"] \\
\mathcal{H}\otimes\mathcal{G} \arrow[r, "\alpha"] & \mathcal{H}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\mathcal{H} \arrow[r, "id_{\mathcal{H}}\otimes \bullet\!-"] \arrow[dr, "id_{\mathcal{H}}"'] & \mathcal{H}\otimes\mathcal{G} \arrow[d, "\alpha"] \\
 & \mathcal{H}
\end{tikzcd} \tag{3.90}$$

To a category theorist, these two diagrams scream "algebra of a monad". This would indeed be a nice categorical definition, but which monad are we talking about? And what is the physical meaning of all of this?

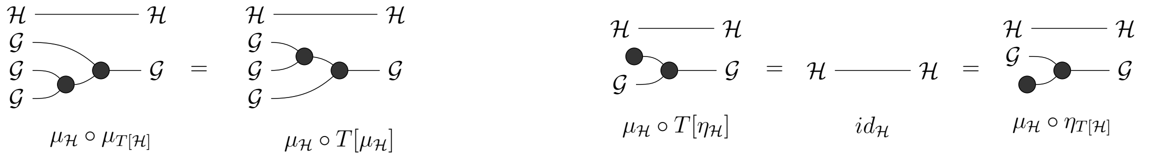
When talking about a system $\mathcal{H}$ with periodic lattice symmetry from a coherent perspective, we are implicitly considering two systems: the system $\mathcal{H}$ itself, and the system $\mathcal{G}$ of wavefunctions on the periodic lattice that control the symmetry (i.e. we are thinking of a specific coherent group $\mathbb{G}$ on it). The concrete process of taking a system $\mathcal{H}$ and considering it jointly with the coherent controlling system $\mathcal{G}$ can be turned into a functor $T : \mathcal{C} \to \mathcal{C}$ (i.e. it can be made properly categorical) as follows:

$$\begin{aligned} T[\mathcal{H}] &:= \mathcal{H}\otimes\mathcal{G} \\ T[f:\mathcal{H}\to\mathcal{H}'] &:= f\otimes id_{\mathcal{G}} : \mathcal{H}\otimes\mathcal{G}\to\mathcal{H}'\otimes\mathcal{G} \end{aligned} \tag{3.91}$$

The functor T can be made into a *monad* by considering the following natural transformations, known as the *multiplication* $\mu : T^2 \to T$ and *unit* $\eta : id_{\mathcal{C}} \to T$:

$$\begin{aligned} \mu_{\mathcal{H}} &:= id_{\mathcal{H}}\otimes \succ\!\bullet\!- \; : T[T[\mathcal{H}]] \to T[\mathcal{H}] \\ \eta_{\mathcal{H}} &:= id_{\mathcal{H}}\otimes \bullet\!- \; : \mathcal{H} \to T[\mathcal{H}] \end{aligned} \tag{3.92}$$

The fact that (T, μ, η) is a monad on $\mathcal{C}$ (in fact it is a *commutative* monad [Koc72]) is a direct consequence of the fact that ($\mathcal{G}$, $\succ\!\bullet\!-$, $\bullet\!-$) is an internal monoid in $\mathcal{C}$, and is summarised by the following graphical equations:


$\mathcal{H}$
$\mathcal{G}$
=
$\mu_{\mathcal{H}}\circ\mu_{T[\mathcal{H}]}$
$\mu_{\mathcal{H}}\circ T[\mu_{\mathcal{H}}]$
$\mu_{\mathcal{H}}\circ T[\eta_{\mathcal{H}}]$
$id_{\mathcal{H}}$
$\mu_{\mathcal{H}}\circ\eta_{T[\mathcal{H}]}$

(3.93)

Monads are the category-theoretic way of talking about abstract operations in algebra[13]. We can think of a monad T as embodying the general principles of an algebraic structure, and of its *algebras* $\alpha : T[A] \to A$ as the concrete realisations of said structure. For example, the *group monad* on Set sends a set X to the underlying set $F[X]$ of the free group on X, and its algebras $\alpha : F[X] \to X$ are all the possible group structures on X. Similar constructions hold for a variety of algebraic theories.

The monad (T, μ, η) we constructed in Equations 3.91 and 3.92 turns out to embody the general structure of representations for a fixed coherent group $\mathbb{G}$ on an object. If $\mathcal{H}$ is an object of $\mathcal{C}$, an **Eilenberg-Moore algebra** (henceforth, **EM algebra**) of the monad (T, μ, η) is a map $\alpha : T[\mathcal{H}] \to \mathcal{H}$ such that $\alpha \circ T[\alpha] = \alpha \circ \mu_{\mathcal{H}}$ and $\alpha \circ \eta_{\mathcal{H}} = id_{\mathcal{H}}$. Expanding the definitions of T, μ and η, we see that the defining equations of an EM algebras for (T, μ, η) are nothing but the two commutative diagrams depicted in 3.90: hence the EM algebras for the monad above, which we will henceforth denote by $\_ \otimes \mathbb{G}$, are exactly the representations of the coherent group $\mathbb{G} := (\circ, \bullet)$.

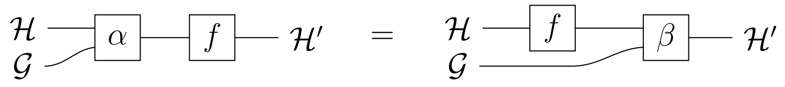
Eilenberg-Moore algebras form a category, the **Eilenberg-Moore category**, which turns out to be really important for our treatment of coherent symmetries:

- the objects of the Eilenberg-Moore category are the EM algebras for the monad;
- the morphisms $f : \alpha \to \beta$ in the Eilenberg-Moore category, where $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ and $\beta : \mathcal{H}' \otimes \mathcal{G} \to \mathcal{H}'$ are EM algebras, are exactly the morphisms $f : \mathcal{H} \to \mathcal{H}'$ in $\mathcal{C}$ which make the following square commute:

$$\begin{tikzcd}
\mathcal{H} \otimes \mathcal{G} \arrow[r, "f \otimes id_{\mathcal{G}}"] \arrow[d, "\alpha"'] & \mathcal{H}' \otimes \mathcal{G} \arrow[d, "\beta"] \\
\mathcal{H} \arrow[r, "f"] & \mathcal{H}'
\end{tikzcd} \tag{3.94}$$

- composition and identities are inherited from $\mathcal{C}$.

The commuting square 3.94 appearing in the definition of EM morphisms can equivalently be written as the following diagrammatic equation:



(3.95)

[13] Monads also arise in the context of functional programming [Mog91] (albeit with a slightly different interpretation), in modal logic, and in a surprising variety of fields of mathematics.

But what is its physical meaning? Looking at Equation 3.95 it is pretty clear that EM morphisms are **equivariant maps** (if thinking of systems with symmetries), or **intertwiners** (if thinking of representations): they are the processes in the base theory $\mathcal{C}$ that respect the coherent symmetries that systems have been endowed with. Because of this, the Eilenberg-Moore category is the natural environment to talk about systems with coherent symmetry given by a fixed coherent group $\mathbb{G}$: since the latter were defined as the *representations* of $\mathbb{G}$, we will refer to the Eilenberg-Moore category as $\mathrm{Rep}\,[\mathbb{G}]$.

Just like any other Eilenberg-Moore category, $\mathrm{Rep}\,[\mathbb{G}]$ comes with a forgetful functor $\mathrm{Rep}\,[\mathbb{G}] \to \mathcal{C}$ sending a representation (i.e. a symmetric system) $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ to the **underlying system** (i.e. a system without symmetry) $\mathcal{H}$, and acting as the identity on processes. The forgetful functor comes with a left adjoint $\mathcal{C} \to \mathrm{Rep}\,[\mathbb{G}]$, sending a system $\mathcal{H}$ to the **free representation** $id_{\mathcal{H}} \otimes \succ\!\!\bullet\!-\; : (\mathcal{H} \otimes \mathcal{G}) \otimes \mathcal{G} \to \mathcal{H} \otimes \mathcal{G}$, and acting as the identity on morphisms.

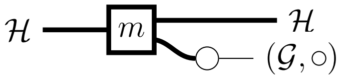
Because in this work we are concerned with *unitary* representations of a coherent group, we will restrict our attention to the full sub-category of $\mathrm{Rep}\,[\mathbb{G}]$ given specified by the unitary representations: we will refer to this subcategory as the **unitary Eilenberg-Moore category**, and denote it by $\mathrm{Rep}^{\dagger}\,[\mathbb{G}]$.

3.4.3 Symmetry-observable duality

In the first part of this section, we have defined a system with coherent symmetry given by a coherent group $\mathbb{G}$ to be a representation α of $\mathbb{G}$. The representation $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ generalises the coherent multiplication $\succ\!\!\bullet\!-\; : \mathcal{G} \otimes \mathcal{G} \to \mathcal{G}$, which endows the space of wavefunctions over the classical group $[\![\mathbb{G}]\!]$ with the symmetry corresponding to the regular representation. We know that the regular representation $\succ\!\!\bullet\!-$ is tightly related to the momentum observable ● of the coherent group $\mathbb{G}$, so a natural question arises: does every representation $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ always yield some sort of momentum measurement for the underlying system $\mathcal{H}$? The answer turns out to be "yes", but first we need to understand what the coherent counterpart of a non-demolition measurement looks like.

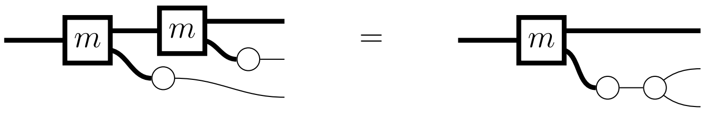
Definition 3.29. *Let* $\mathrm{CP}^*[\mathcal{C}]$ *be an R-probabilistic CP* category, and let* ○ *be a †-SCFA with enough classical states, and finitely many so (i.e.* $(\mathcal{G}, \circ)$ *is a classical system). Then a* ***non-demolition measurement*** *on a system* $\mathcal{H}$ *with outcomes in*

$(\mathcal{G}, \circ)$ is a process m in the following form:



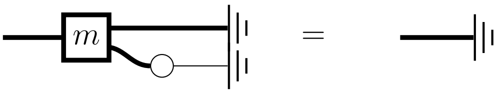
(3.96)

which satisfies the following three requirements:



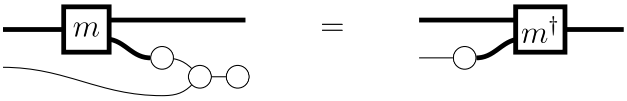
(3.97)

indempotence



(3.98)

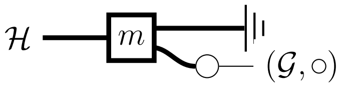
normalisation



(3.99)

self-adjointness

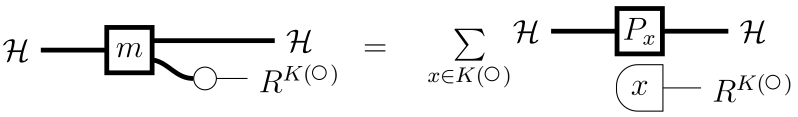
The associated ***demolition measurement*** *takes the following form:*



(3.100)

It's not hard to show that non-demolition measurements always take the familiar form of classically-indexed families of projectors.

Lemma 3.30. *Let $\mathrm{CP}^*[\mathcal{C}]$ be an R-probabilistic CP* category, let $\circ$ be a $\dagger$-SCFA on an object $\mathcal{G}$ in $\mathcal{C}$ having enough classical points, and assume that $K(\circ)$ is finite. Then the non-demolition measurements $m : \mathcal{H} \to \mathcal{H} \otimes (\mathcal{G}, \circ)$ are exactly those taking the following form:*



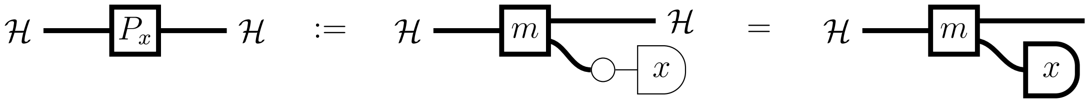
(3.101)

where $(P_x)_{x \in K(\bigcirc)}$ is a complete family of orthogonal projectors in $\mathcal{C}$ (i.e. we have $P_x P_x = P_x$, $P_x^\dagger = P_x$, $P_x P_y = 0$ for $y \neq x$ and $\sum_{x \in K(\bigcirc)}$ ***double***$[P_x]$ *is normalised*[14]*).*

Proof. We begin by defining putative projectors P_x from a non-demolition measurement, and show that they indeed satisfy the requirements for a complete orthogonal

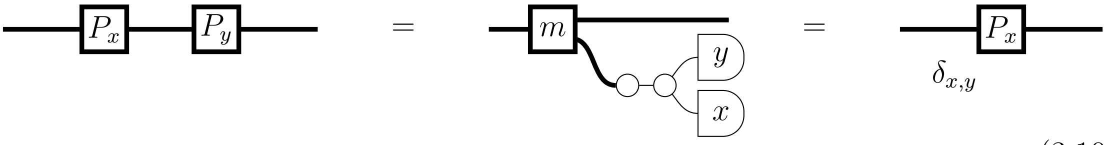
[14] When $\mathcal{C}$ possesses linear structure compatible with that of $\mathrm{CPM}[\mathcal{C}]$, this is the same as the familiar completeness requirement $\sum_x P_x = id_{\mathcal{H}}$.

family of projectors. We define P_x by evaluating against an individual classical outcome $x \in K(\circ)$ for the non-demolition measurement m:



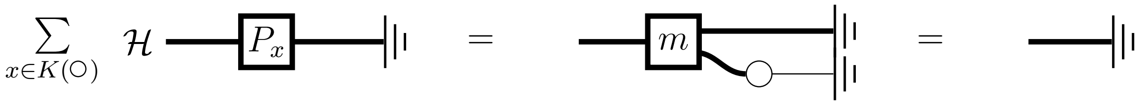
(3.102)

The idempotence and orthogonality of projectors follow from the idempotence requirement for non-demolition measurements:



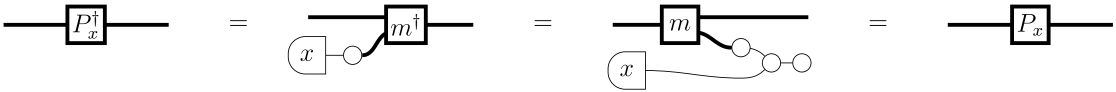
(3.103)

The completeness of the family of projectors follows from the normalisation requirement for non-demolition measurements:



(3.104)

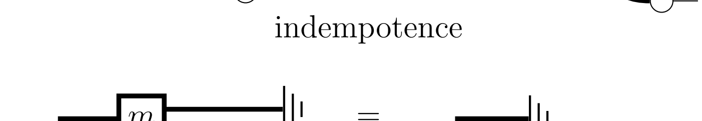
The self-adjointness of the projectors follows from the self-adjointness requirement for non-demolition measurements:



(3.105)

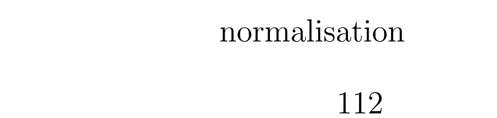
The three equations above can similarly be used to show that the map on the RHS of Equation 3.96 defines a non-demolition measurement. □

In order to figure out what the abstract, coherent counterpart of non-demolition measurements should be, we rewrite the three requirements 3.97, 3.98 and 3.99 so that the only non-pure maps appearing are preparation in ○, measurements in ○, and discarding maps:



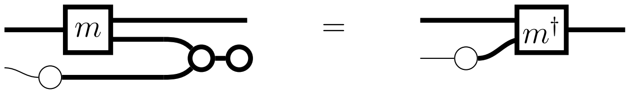
(3.106)

indempotence



(3.107)

normalisation

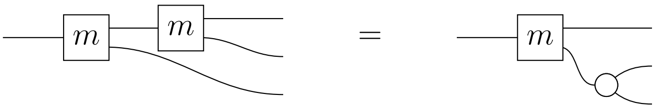


(3.108)

self-adjointness

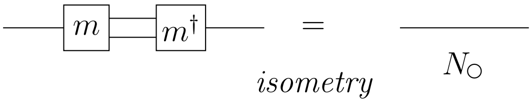
The equations above inspire the following definition of coherent non-demolition measurements.

Definition 3.31. *Let $\mathcal{C}$ be a †-SMC, and ○ be a †-qSFA on an object $\mathcal{G}$ of $\mathcal{C}$, with normalisation factor $N_{\bigcirc}$. A ○-valued* ***coherent non-demolition measurement*** *on an object $\mathcal{H}$ of $\mathcal{C}$ is a process $m : \mathcal{H} \to \mathcal{H} \otimes \mathcal{G}$ which satisfies the following three requirements:*



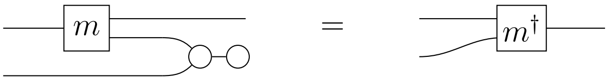
(3.109)

indempotence



(3.110)

isometry

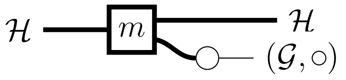


(3.111)

self-adjointness

Remark 3.32. *Note that the isometry requirement involves the normalisation factor $N_{\bigcirc}$ for the †-qSFA ○ on the RHS. This is because in the passage from Equation 3.98 to Equation 3.110 we removed the measurement in ○ from the LHS: when ○ is a generic †-qSCFA, rather than a †-SCFA, this means that we also removed the scalar $\frac{1}{N_{\bigcirc}}$ that comes with the measurement, and hence the RHS of Equations 3.107 and 3.110 will need to carry an extra $N_{\bigcirc}$ factor.*

Lemma 3.33. *Let* $\mathrm{CP}^*[\mathcal{C}]$ *be an R-probabilistic CP* category, and let ○ be a †-SCFA on an object $\mathcal{G}$ of $\mathcal{C}$ having enough classical states, and finitely many of them (so that $(\mathcal{G}, \circ)$ is a classical system). If $m : \mathcal{H} \to \mathcal{H} \otimes \mathcal{G}$ is a ○-valued coherent non-demolition measurement on an object $\mathcal{H}$ of $\mathcal{C}$, then the following is a non-demolition measurement in* $\mathrm{CP}^*[\mathcal{C}]$*:*



(3.112)

Proof. The proof is straightforward: (i) Equation 3.109 for the coherent non-demolition measurement implies Equation 3.106, which is equivalent to Equation 3.97 for the non-demolition measurement; (ii) Equation 3.110 for the coherent non-demolition measurement implies Equation 3.107, which is equivalent to Equation 3.98 for the non-demolition measurement; (iii) Equation 3.111 for the coherent non-demolition measurement implies Equation 3.108, which is equivalent to Equation 3.99 for the non-demolition measurement. □

Remark 3.34. *In Lemmas 3.30 and 3.33 we have restricted our attention to* $\dagger$*-SCFAs, instead of considering more general* $\dagger$*-qSCFAs. This is merely for reasons of clarity, and the results hold just as well when* $\circ$ *is a* $\dagger$*-qSCFA (as long as preparations/measurements are appropriately normalised).*

Having defined coherent non-demolition measurements, we are in a position to answer our original question on the momentum measurement for a symmetric system $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ in $\mathrm{Rep}^{\dagger}[\mathbb{G}]$. We wish to establish that $\alpha^{\dagger}$ yields the coherent momentum measurement[15] of a system α with periodic lattice symmetry (i.e. a unitary representation of a doubly well-pointed, doubly finite coherent group). We will do so by providing the following compelling evidence:

(i) we will show (for all coherent groups) that $\alpha^{\dagger}$ is a $\bullet$-valued coherent measurement on the system $\mathcal{H}$[16];

(ii) we will show (for all coherent groups) that any invariant for the symmetry must commute with $\alpha^{\dagger}$[17]; furthermore, we will show (for abelian coherent groups) that $\alpha^{\dagger}$ is itself an invariant for the symmetry [18];

(iii) we will show (for all coherent groups) that states ψ_{χ} of $\mathcal{H}$ associated with a definite outcome $\chi^{\dagger} \in K(\bullet)$ under $\alpha^{\dagger}$ transform as expected under the translation symmetry (i.e. translation by $g \in K(\circ)$ sends ψ_{χ} to itself times the phase $\chi \circ g$).

We will colloquially refer to $\alpha^{\dagger}$ as the **coherent momentum observable** on a system α with periodic lattice symmetry, generalising the coherent momentum observable $\bullet$ from the case of wavefunctions on the lattice. We exemplified things in the case of periodic lattices, in which case momentum measurement is appropriate, but when

[15] Henceforth, we will write *coherent measurement* for *coherent non-demolition measurement*, since demolition measurements are, almost by definition, not coherent (expect in trivial cases).

[16] From this we can conclude (in the case of doubly well-pointed, doubly finite coherent groups) that the non-demolition and demolition measurements associated to $\alpha^{\dagger}$ have classical outcomes in the set $K(\bullet)$ of possible momenta allowed by the lattice controlling the symmetry.

[17] The momentum measurement is indeed expected to have this property for the translation symmetry, just like it had in the case of wavefunctions on the periodic lattice.

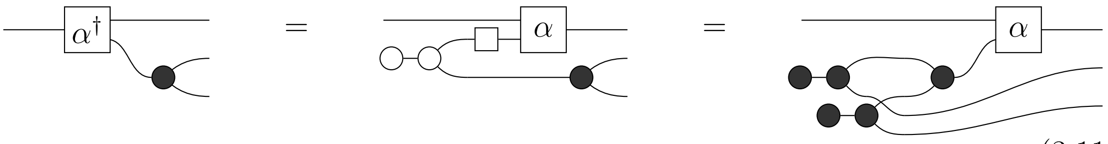
[18] And hence so do the associated non-demolition and demolition measurements.

talking about a generic coherent group we will refer to $\alpha^\dagger$ as the **invariant** associated with the symmetry α.

The fact that the invariant for a symmetric system α can be obtained simply by considering the adjoint $\alpha^\dagger$ is unique to the coherent approach. Indeed, the non-demolition momentum measurement cannot be obtained from the representation of the classical lattice translation group, as they involve measurement/preparation in two complementary observables. In the coherent approach, on the other hand, all the information is preserved, and the distinction between a coherent symmetry α and its invariant $\alpha^\dagger$ is a mere matter of perspective.

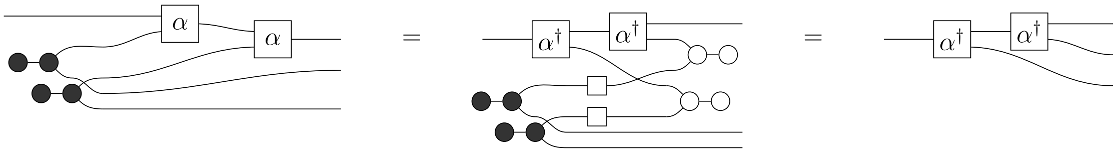
Theorem 3.35 (**Symmetry-observable duality**).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a $\dagger$-SMC $\mathcal{C}$, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. Then $\alpha^\dagger : \mathcal{H} \to \mathcal{H} \otimes \mathcal{G}$ is a $\bullet$-valued coherent measurement on $\mathcal{H}$.

Proof. We begin by showing that the idempotence condition holds. The first equality below is by unitarity of the representation α, while the second equality expands the antipode in its definition and uses the laws of Frobenius algebras:



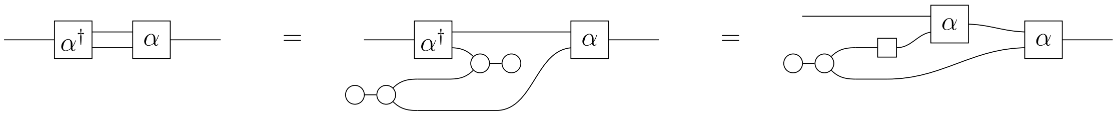
(3.113)

The rightmost diagram above is equal to the leftmost below by the multiplicativity condition for representation α. The first equality below is again by unitarity of α, and the second is again by definition of the antipode and the laws of Frobenius algebras:



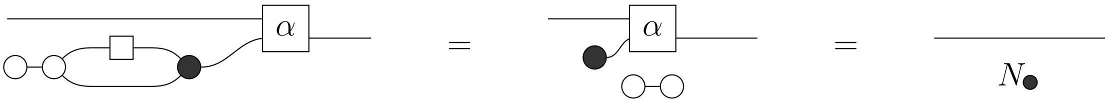
(3.114)

This completes the proof of the idempotence condition for $\alpha^\dagger$. We now move on to prove the isometry condition. The first equality below follows from the laws of Frobenius algebras, while the second equality below is by unitarity of the representation α:



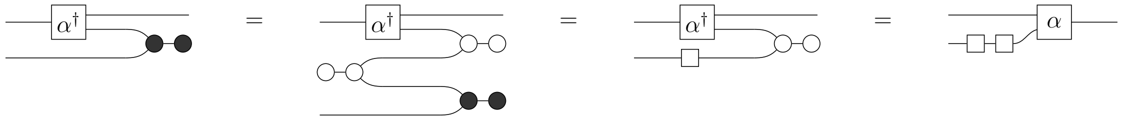
(3.115)

The rightmost diagram above is equal to the leftmost diagram below by the multiplicativity condition for representation α. The first equality below follows from Hopf law, and the second equality below follows from the unit condition for representation α (together with the fact that ○– is a ●-classical state, with squared norm $N_{\bullet}$):



(3.116)

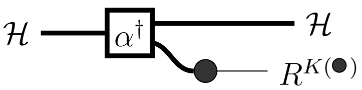
This completes the proof of the isometry condition. Finally, we prove the self-adjointness condition. The first equality below follows from the laws of Frobenius algebras, the second equality by definition of the antipode and the third equality by unitarity of the representation α:



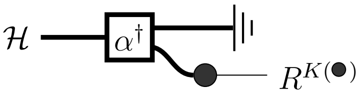
(3.117)

Finally, the antipode is an involution, and hence the rightmost diagram above is nothing but α itself. This completes the proof of the self-adjointness condition. □

When $\mathrm{CP}^*[\mathcal{C}]$ is R-probabilistic and $\mathbb{G}$ is doubly well-pointed and doubly finite, we can write the non-demolition and demolition measurements associated to $\alpha^\dagger$ as follows, with classical outputs in the set $K(\bullet)$:



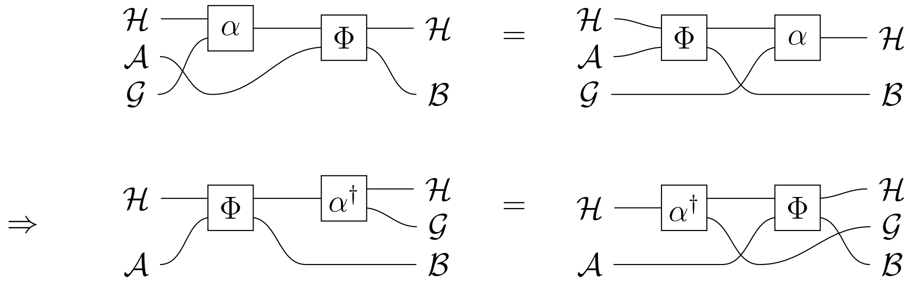
non-demolition measurement



demolition measurement

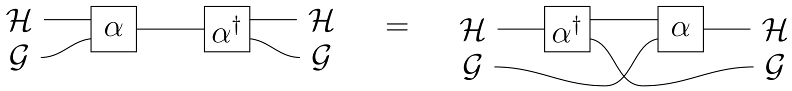
(3.118)

Theorem 3.36 (**Symmetry-invariant duality**).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. Any invariant Φ of α (and in particular every intertwiner $\Phi : \alpha \to \alpha$) must commute with $\alpha^\dagger$:



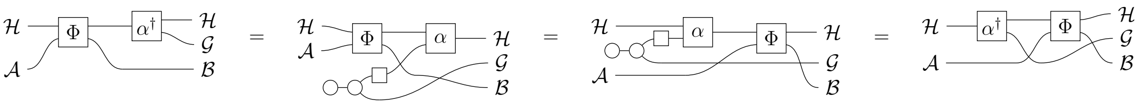
(3.119)

Furthermore, if $\mathbb{G}$ is abelian, then $\alpha^\dagger : \mathcal{H} \to \mathcal{H} \otimes \mathcal{G}$ is itself an invariant for the symmetry α:



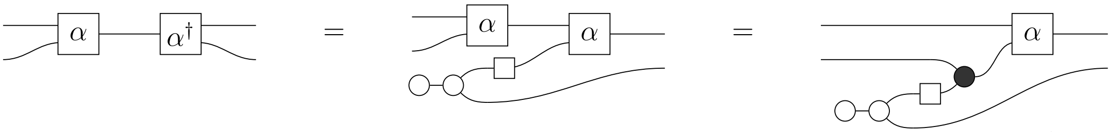
(3.120)

Proof. We begin by proving that any invariant Φ for α must commute with $\alpha^\dagger$. The first and last equalities below are by unitarity of the representation α, while the central equality uses the hypothesis of invariance of Φ:



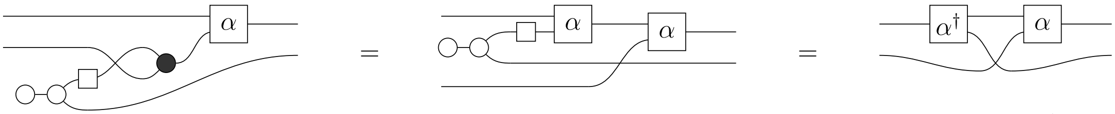
(3.121)

This concludes the proof that any Φ invariant for α must commute with $\alpha^\dagger$. We then prove that, if $\mathbb{G}$ is an abelian coherent group (i.e. if ● is commutative), then $\alpha^\dagger$ itself must be an invariant for the symmetry α. The first equality below is by unitarity of the representation α, while the second equality uses the multiplicativity condition:



(3.122)

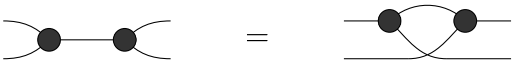
We use commutativity of ● to obtain the leftmost diagram below from the topmost above. The first equality below is again by the multiplicativity condition, and the second equality is again by unitarity:



(3.123)

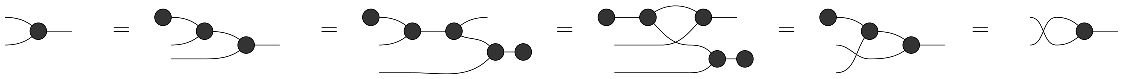
This concludes the proof that, when $\mathbb{G}$ is commutative, $\alpha^\dagger$ is an invariant for the symmetry α. □

The requirement that the coherent group is abelian for $\alpha^\dagger$ to be an invariant for α is a necessary one. Indeed, the multiplication ● is itself a unitary representation, and we have the following consequence of Equation 3.120 holding for all α:



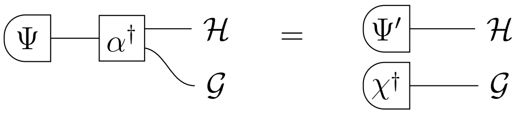
(3.124)

Using the equation above, we can prove that ● is in fact commutative:



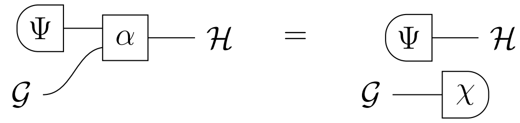
(3.125)

Theorem 3.37 (Invariant states).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an object $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let $\alpha : \mathcal{H}\otimes\mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. Let Ψ be a state of $\mathcal{H}$ associated with a definite outcome $\chi^\dagger \in K(\bullet)$ of the coherent momentum measurement $\alpha^\dagger$, i.e. one such that $\alpha^\dagger\Psi$ separates as $\Psi' \otimes \chi^\dagger$ for some state Ψ':



(3.126)

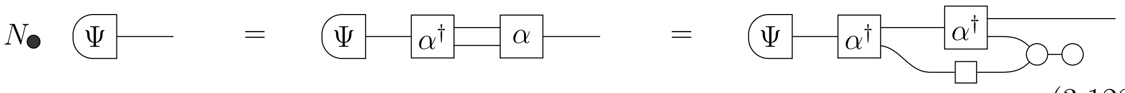
Then we must necessarily have $\Psi = \Psi'$. Furthermore, Ψ transforms as follows under the symmetry action α:



(3.127)

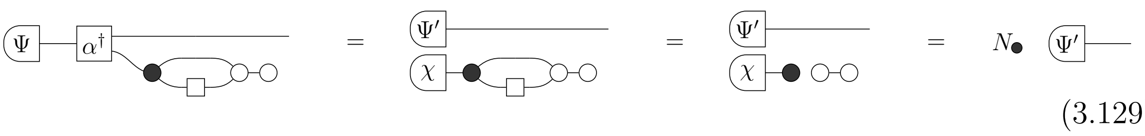
In terms of the classical action $\big(U_g := \alpha \circ (\_ \otimes g)\big)_{g\in[\![\mathbb{G}]\!]}$ of the underlying group, we have $U_g\Psi = \chi(g)\Psi$. Conversely, any state Ψ satisfying the transformation law of Equation 3.127 is associated to a definite outcome $\chi^\dagger$ of $\alpha^\dagger$, as in Equation 3.126.

Proof. We begin by proving that $\Psi = \Psi'$. The first equality below is by the isometry condition for $\alpha^\dagger$, and the second equality by unitarity of α:



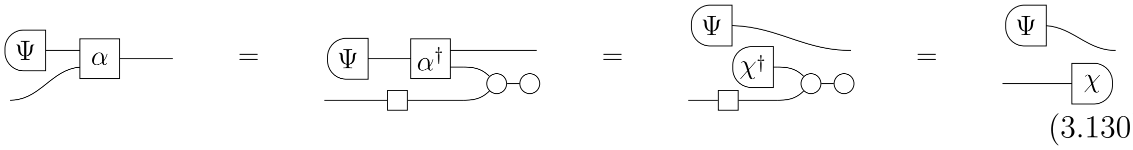
(3.128)

The leftmost diagram below is obtained from the rightmost diagram above by the idempotence condition for $\alpha^\dagger$. The first equality below is by Equation 3.126, the second equality is by Hopf's law, and the third equality follows because $\chi($ ●- $) = 1$ and -○ ∘ ○- $= N_\bullet$:



(3.129)

This completes the proof that $\Psi = \Psi'$. To prove the transformation law of Equation 3.127, we use Equation 3.126 together with the fact that $\Psi = \Psi'$ and unitarity of the representation α:



(3.130)

The proof of the converse statement goes along the exact same lines. □

3.4.4 Stone's theorem revisited

The standard result relating momentum to the translation symmetry of 1-dimensional wavefunctions is known as **Stone's theorem on 1-parameter unitary groups**: it states that the strongly continuous group homomorphisms $x \mapsto U_x$ (the 1-parameter unitary groups) from the additive reals $(\mathbb{R}, +, 0)$ to the unitary operators $U[\mathcal{H}]$ over some separable Hilbert space $\mathcal{H}$ are exactly those in the form $U_x = \exp[ix\mathbf{p}]$ for some (not necessarily bounded) self-adjoint operator $\mathbf{p}$ on $\mathcal{H}$ (the traditional momentum observable). In Theorems 3.35 and 3.36, we saw that the relationship between translation and the momentum observable on periodic lattices is given, in our framework, by adjunction. Throughout this Subsection, we will work in the standard QM formalisms: our aim will be to recast Stone's Theorem for 1-dimensional wavefunctions in a form explicitly compatible with our formulation, i.e. one not involving an infinitesimal generator $\mathbf{p}$.

Theorem 3.38 (**Stone's Theorem** [Sto32])**.**
Let $x \mapsto U_x$ be a strongly continuous group homomorphism $\mathbb{R} \to U[\mathcal{H}]$, where $\mathcal{H}$ is any Hilbert space. Then there exists a unique self-adjoint operator $\boldsymbol{p} : \mathcal{H} \to \mathcal{H}$, not necessarily bounded, such that $U_x = \exp[ix\boldsymbol{p}]$ for all $x \in \mathbb{R}$.

Theorem 3.39 (**Spectral Theorem** [Hal13])**.**
Let $\boldsymbol{p} : \mathcal{H} \to \mathcal{H}$ be a self-adjoint operator. Then there is a measurable space Z, a measure μ and a unitary isomorphism $V : \mathcal{H} \to \mathrm{L}^2[Z, \mu]$ such that $\boldsymbol{p}' := V\boldsymbol{p}V^\dagger$ is a multiplication operator:

$$\begin{aligned} \boldsymbol{p}' : \mathrm{L}^2[Z,\mu] &\to \mathrm{L}^2[Z,\mu] \\ \psi &\mapsto (z \mapsto p_z \psi(z)) \end{aligned} \tag{3.131}$$

*We will refer to the measurable function $p : Z \to \mathbb{R}$ as the **spectrum** of the operator $\boldsymbol{p}$. If $\boldsymbol{p}$ is bounded then p is essentially bounded and we have $||\boldsymbol{p}'|| = ||p||_\infty$.*

This is the usual way to derive the momentum spectrum for 1-dimensional wavefunctions: unfortunately, it turns out not to be canonical. This may seem a merely categorical flaw, but it is in fact related to an important physical fact: valuing momentum in the reals is necessarily subject to a choice of units of measurement.

In the course of this Section, we have established that the canonical space for the momenta associated with a symmetric space (governed by some classical abelian group symmetry G) is given by the Pontryagin dual $G^\wedge$: any attempt to faithfully value momentum in some other space K is equivalent to a choice of group isomorphism

$G^\wedge \cong K$ for some K. Similarly, when the translation symmetry is governed by $G = \mathbb{R}$, we expect any valuation of the momentum in $K = \mathbb{R}$ to be conditional on some choice of units of measurement, i.e. on fixing some isomorphism $\mathbb{R}^\wedge \cong \mathbb{R}$.

Units of measurement, seen as (continuous) group isomorphisms $G^\wedge \overset{\cong}{\to} K$, form a homogeneous space under (transitive and faithful) left regular action of the group automorphisms of K. The action corresponds to changing units, and for $K = \mathbb{R}$ this is the usual multiplication by some non-zero real number. Thus the momentum operator and its spectrum obtained from Theorems 3.38 and 3.39 are subject to an underlying choice of units of measurement $\mathbb{R}^\wedge \xrightarrow{\cong} \mathbb{R}$: Lemma 3.40 below make this statement precise.

Lemma 3.40. *The continuous isomorphisms* $\mathrm{Iso}_{\mathrm{Ab}}[\mathbb{R}^\wedge, \mathbb{R}]$ *form a homogeneous space under the (faithful and transitive) left regular action of* $\mathrm{Aut}_{\mathrm{Ab}}[\mathbb{R}]$*. Also* $\mathrm{Aut}_{\mathrm{Ab}}[\mathbb{R}] \cong_{\mathrm{Ab}} (\mathbb{R}^\times, \cdot, 1)$*, where* $\alpha_c := x \mapsto c \cdot x$ *is the continuous automorphism corresponding to a non-zero real c. As a consequence, the bijection of Theorem 3.38 is non-canonical, and there is instead a homogeneous space of bijections* $U_x = \exp[ix\frac{1}{\hbar}\boldsymbol{p}]$ *between strongly continuous group homomorphisms* $(U_x)_{x\in\mathbb{R}}$ *and self-adjoint operators* $\boldsymbol{p}$*, with fiber isomorphic to the homogeneous space* $\mathrm{Iso}_{\mathrm{Ab}}[\mathbb{R}^\wedge, \mathbb{R}]$ *(except at the singular point* $(U_x)_x = (id_{\mathcal{H}})_x$*). Singling out one such bijection is equivalent to fixing a choice of isomorphism* $\mathbb{R}^\wedge \cong \mathbb{R}$*.*

Proof. The first two observations are standard checks. To see that the bijections form a homogeneous space, all we have to show is that there is an action of $\mathrm{Aut}_{\mathrm{Ab}}[\mathbb{R}]$ on them: the action of a $\frac{\hbar}{\hbar'} : \mathbb{R}^\times$ on the space of bijections is given as follows:

$$\frac{\hbar}{\hbar'} : U_x = \exp[ix\frac{1}{\hbar}\mathbf{p}] \mapsto U_x = \exp[ix\frac{1}{\hbar'}\mathbf{p}] \tag{3.132}$$

□

Taking Theorems 3.38 and 3.39 together, the **momentum spectrum** for a unitary symmetry $(U_x)_{x\in\mathbb{R}}$ is usually defined to be $p : Z \to \mathbb{R}$. However, it is a consequence of Lemma 3.40 that this momentum spectrum is non-canonical, depending instead on a particular choice of unit of measurement: we will denote by $p^\hbar$ the spectrum associated with a particular bijection $U_x = \exp[ix\frac{1}{\hbar}\mathbf{p}]$. We can, however, define a canonical energy spectrum $\hat{p} : Z \to \mathbb{R}^\wedge$.

Theorem 3.41 (**Canonical energy spectrum**).
Let $(U_x)_{x\in\mathbb{R}}$ *be a strongly continuous group homomorphism* $\mathbb{R} \to U[\mathcal{H}]$*. Fix a bijection*

$U_x = \exp[ix\frac{1}{\hbar}\boldsymbol{p}]$, and obtain the[19] *spectral decomposition with $V : \mathcal{H} \to \mathrm{L}^2[Z,\mu]$ and $p^\hbar : Z \to \mathbb{R}$. Define $\hat{p} : \mathrm{L}^2[Z,\mu] \to \mathbb{R}^\wedge$ by:*

$$z \mapsto (x \mapsto \exp[i\frac{1}{\hbar}p^\hbar_z x]) \tag{3.133}$$

*Then $\hat{p}$ is independent of the choice of $\hbar \in \mathbb{R}^\times$ (i.e. it is canonical) and we shall refer to it is as the **canonical momentum spectrum** of $(U_x)_x$.*

Proof. The action defined in Equation 3.132 sends $p^\hbar$ to $p^{\hbar'} = \frac{\hbar'}{\hbar}p^\hbar$. Thus Equation 3.133 is invariant under the action of $\frac{\hbar}{\hbar'} \in \mathbb{R}^\times$. □

Remark 3.42 (**Non-demolition Momentum Measurement?**).
Given a symmetric system $(U_x)_{x\in\mathbb{R}}$ and its canonical momentum spectrum $\hat{p}$, we can "construct" an operator $\hat{p} : \mathrm{L}^2[Z,\mu] \to \mathrm{L}^2[Z,\mu] \otimes \mathrm{L}^2[\mathbb{R}^\wedge]^\star$ similar to the coherent non-demolition measurement by using delta functions:

$$\hat{p} : \int_Z a_z |z\rangle d\mu(z) \mapsto \int_Z a_z |z\rangle \otimes |\hat{p}_z\rangle d\mu(z) \tag{3.134}$$

We denoted by $|z\rangle$ the delta function at $z \in Z$ and by $|\hat{p}_z\rangle$ the delta function at $\hat{p}_z \in \mathbb{R}^\wedge$. Subject to a choice $f : \mathbb{R}^\wedge \overset{\cong}{\to} \mathbb{R}$ of units of measurement, we can also "recover" the momentum operator of Theorem 3.38 from the non-demolition momentum measurement "constructed" above:

$$V\boldsymbol{p}V^\dagger = \left(id_{\mathrm{L}^2[Z,\mu]} \otimes \int_{\mathbb{R}^\wedge} f(\chi)\langle\chi|d\chi\right) \circ \hat{p} \tag{3.135}$$

The operator $\int_{\mathbb{R}^\wedge} f(\chi)\langle\chi|d\chi$ is nothing but f extended linearly on the basis of delta functions for $\mathbb{R}^\wedge$.

The non-demolition Hamiltonian above, however, is not fully rigorous, and we need take a different road to link Stone's Theorem with our periodic lattice symmetries. Recasting the results in terms of projection-valued measures provides a viable alternative.

Lemma 3.43. *Let X, Y be measurable spaces (with sigma-algebras Σ_X and Σ_Y), μ a measure on X and $f : X \to Y$ measurable. Then f determines a projection-valued measure $\pi_f : \Sigma_Y \to \mathrm{B}\left[\mathrm{L}^2[X,\mu]\right]$ by:*

$$\pi_f(U) = \textit{projection onto subspace } \mathrm{L}^2[f^{-1}(U),\mu] \tag{3.136}$$

for all $U \in \Sigma_Y$. If $V : \mathcal{H} \to \mathrm{L}^2[X,\mu]$ is a unitary, then π_f can be seen (giving V as understood) as a projection valued measure $\Sigma_Y \to \mathrm{B}[\mathcal{H}]$ by considering $V^\dagger \pi_f V$.

[19] The decomposition is not really unique. However, the same Z works for all $\hbar$, and the construction of $p^\hbar$ is contravariantly functorial with respect to the choice of Z. So we shall not worry about this any further.

Theorem 3.44 (**Spectral Theorem, projection-valued**).
Let $\boldsymbol{p} : \mathcal{H} \to \mathcal{H}$ be a self-adjoint operator. Let $V : \mathcal{H} \to \mathrm{L}^2[Z,\mu]$ and spectrum $p : Z \to \mathbb{R}$ be given by Theorem 3.39. If π_p is the projection-valued measure defined by Lemma 3.43, then we can reconstruct $\boldsymbol{p}$ as:

$$\boldsymbol{p} = \int_{\mathbb{R}} \lambda \, d\pi_p(\lambda) \tag{3.137}$$

Theorem 3.45 (**Stone's Theorem, projection-valued**).
Let $(U_x)_{x\in\mathbb{R}}$ be a strongly continuous group homomorphism $\mathbb{R} \to U[\mathcal{H}]$. Let $V : \mathcal{H} \to \mathrm{L}^2[Z,\mu]$ unitary isomorphism and $\hat{p} : Z \to \mathbb{R}^\wedge$ canonical momentum spectrum be given by Theorem 3.41. If $\pi_{\hat{p}}$ is the projection-valued measure defined by Lemma 3.43, then we can reconstruct $(U_x)_x$ as:

$$U_x = \int_{\mathbb{R}^\wedge} \chi(t) \, d\pi_{\hat{p}}(\chi) \tag{3.138}$$

Finally, the form of Stone's theorem on 1-parameter unitary groups given by Theorem 3.45 can be extended to the periodic lattice symmetries described in this work, remembering that a symmetry α for a well-pointed abelian[20] coherent group $\mathbb{G}$ on a finite-dimensional Hilbert space $\mathcal{H}$ corresponds to a (necessarily strongly continuous) group homomorphisms $G \to U[\mathcal{H}]$, where G is the (finite abelian) underlying group.

Theorem 3.46 (**Canonical momentum spectrum, finite abelian groups**).
Let $(U_g)_{g\in G}$ be the strongly continuous group homomorphism $G \to U[\mathcal{H}]$ corresponding to a representation $\alpha : \mathcal{H}\otimes\mathcal{G} \to \mathcal{H}$ of a doubly well-pointed abelian coherent group $\mathbb{G}$ in fHilb, *with $G := [\![\mathbb{G}]\!]$ as its (finite abelian) underlying group. Let $\hat{p} := \alpha^\dagger : \mathcal{H} \to \mathcal{H}\otimes\mathcal{G}$, and Z be an orthonormal basis of eigenvalues for $\hat{p}$. Let $V : \mathcal{H} \to \mathrm{L}^2[Z,\mu]$ be the unitary corresponding to the basis, and define the canonical momentum spectrum $\hat{p} : Z \to G^\wedge$ via the multiplicative character basis of $\mathcal{G}$:*

$$\hat{p}(|z\rangle) := [(\langle z| \otimes id_{\mathcal{G}})\, \hat{p}|z\rangle]^\dagger \tag{3.139}$$

Then the projection-valued measure $\pi_{\hat{p}}$ is independent of the choice of basis[21] *and coincides with the complete family of orthogonal projectors defined by $\hat{p}$.*

[20] Recall that well-pointed abelian coherent groups in fHilb are always doubly well-pointed and doubly finite.

[21] Seen as having projections in $\mathrm{B}[\mathcal{H}]$, its correct form would be $V^\dagger \pi_{\hat{p}} V$, where p is dependent on the choice of V. The statement here is that the entire expression $V^\dagger \pi_{\hat{p}} V$ is independent of the choice of V.

The measure provided by Theorem 3.46 can be extended linearly to obtain the invariant $\alpha^\dagger$ for the well-pointed abelian coherent group $\mathbb{C}[G]$, and similarly $(U_g)_{g\in G}$ can be extended linearly to obtain the representation α. In the last section of this Chapter, we will see that this provides a direct link between the (finite abelian groups case of) Stone's Theorem and the symmetry/observable duality results for coherent groups presented in this Section.

3.5 Infinite-dimensional CQM

Throughout the past decade, the framework of CQM has achieved remarkable success in describing the foundations of finite-dimensional quantum theory, and the structures behind quantum information protocols and quantum computation. Unfortunately, attempts to extend the same techniques to the treatment of infinite-dimensional case have so far achieved limited success. Although the work of [AH12a] on H*-algebras provides a characterisation of non-degenerate observables in arbitrary dimensions, the machinery needed to describe coherent groups for separable Hilbert spaces is inevitably lost: strongly complementary pairs do not exist in the category sHilb of separable Hilbert spaces and bounded linear maps for infinite-dimensional spaces. This is a major issue for our coherent framework: it prevents us from being able to talk about one of the textbook examples of position/momentum pairs in quantum mechanics, that of 1-dimensional wavefunctions with periodic boundary conditions. The reason is simple: the translation symmetry group is the compact abelian Lie group $(\mathbb{R}/L\mathbb{Z}, +, 0)$ (where L is the length of the underlying space), while the boost symmetry groups is the infinite discrete abelian group $(\mathbb{Z}, +, 0)$, and sHilb doesn't allow us to formulate coherent groups on $\mathrm{L}^2[\mathbb{Z}]$ or $\mathrm{L}^2[\mathbb{R}/L\mathbb{Z}]$.

In this Section, we resort to non-standard analysis à la Robinson [Rob74] to tackle the issue of infinitesimal and infinite quantities behind unbounded operators, Dirac deltas and plane-waves: these are key ingredients of mainstream quantum mechanics which the categorical framework has thus failed to adequately capture, and we demonstrate how they can be used to recover a great deal of CQM machinery in infinite-dimensions. Applications of non-standard analysis to quantum theory already appeared in the past decades [OO93, Far75], but in a different spirit and with different objectives in mind. In Subsection 3.5.1, we provide a basic summary of the non-standard techniques we will be using. In Subsection 3.5.2, we construct a category *Hilb of non-standard separable Hilbert spaces, and we relate it to the category sHilb of standard separable Hilbert spaces and bounded linear maps. In Subsection 3.5.4, we use our newly defined category to extend CQM from finite to separable Hilbert spaces, and we treat the textbook case of position and momentum observable for 1-dimensional wavefunctions with periodic boundary conditions.

The contents of this Section appeared as a standalone work in QPL 2016 [GG16], and we will follow that treatment here. However, please note that the constructions presented have since been generalised by [GG17] (which includes a new and extended definition of the category *Hilb, as well as a number of explicit constructions).

3.5.1 Non-standard analysis

3.5.1.1 Non-standard models

In this brief introduction to non-standard models, we follow the common lines in the presentations of the original [Rob74] and the more recent [Gol98]. Consider a (first or higher order) theory $\mathbb{T}$, with a standard model M: for example, we could consider the theory of natural numbers, with its standard model $\mathbb{N}$, or the theory of real numbers, with its standard model $\mathbb{R}$. We now proceed to outline the **ultrapower construction**, which is used to produce a non-standard model $^{\star}M$ for the theory[22].

Consider the set $M^{\mathbb{N}}$ of all sequences of elements in M, and extend all operations and relations of $\mathbb{T}$ to $M^{\mathbb{N}}$ by pointwise definition: any algebraic structure of M transfers to $M^{\mathbb{N}}$ this way, but non-algebraic axioms in $\mathbb{T}$ (such as the existence of inverses in a field) need not transfer. For example, $\mathbb{R}^{\mathbb{N}}$ is a commutative ring this way, but it is neither totally ordered nor a field.

Now fix a non-principal ultrafilter $\mathcal{F}$ on the set $\mathbb{N}$, and define an equivalence relation $\equiv$ on $M^{\mathbb{N}}$ as follows:

$$(s_n)_{n\in\mathbb{N}} \equiv (t_n)_{n\in\mathbb{N}} \text{ iff } \{n \in \mathbb{N} \mid s_n = t_n\} \in \mathcal{F} \tag{3.140}$$

We can think of $\equiv$ as equating all sequences which *agree almost everywhere (according to the ultrafilter $\mathcal{F}$)*, and we consider the quotient set $^{\star}M := M^{\mathbb{N}}/\equiv$ (known as the **ultrapower**). Because the equivalence relation $\equiv$ is defined in terms of pointwise equality, the operations and relations of $\mathbb{T}$—which we had already extended from M to $M^{\mathbb{N}}$ by pointwise definition—descend to well-defined operations and relations on the quotient set $^{\star}M$; for example, relations in the quotient $^{\star}M$ hold if and only if their pointwise-defined counterparts hold in $M^{\mathbb{N}}$ almost everywhere (according to $\mathcal{F}$). But a lot more is true: because of the Transfer Theorem (see below), $^{\star}M$ is in fact a model of $\mathbb{T}$, which we refer to as the **non-standard model**. For example, $^{\star}\mathbb{Z}$ is a totally ordered ring, $^{\star}\mathbb{R}$ is a totally ordered field, and $^{\star}\mathbb{C}$ is an algebraically closed field.

Remark 3.47. *The non-standard model obtained via the ultrapower construction is not unique*[23]*. however, all the statements we will make and results we will prove will rely on the Transfer Theorem (see below), and they will apply to any non-standard model $^{\star}M$ obtained via the ultrapower construction. In fact, under the Continuum Hypothesis the choice of $\mathcal{F}$ is entirely irrelevant for the purposes of this work, as all*

[22] Non-standard models are denoted by a prefix $\star$, bearing no relation to complex conjugation.

[23] Nor is it true that all non-standard models of $\mathbb{T}$ need arise this way.

the non-standard models of $\mathbb{R}$ obtained by the ultrapower construction are isomorphic (and a similar statement applies to $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{C}$) [Gol98].

We can define a structure preserving map ${}^\star\_ : M \to {}^\star M$ by sending $x \in M$ to the equivalence class ${}^\star x := [(x, x, x, ...)] \in {}^\star M$ of the constant sequence $(x, x, x, ...) \in M^{\mathbb{N}}$: this is a structure-preserving injective mapping (known as a **universe embedding**), and hence the standard model M is embedded into the non-standard model ${}^\star M$. We refer to the elements of ${}^\star M$ in the form ${}^\star x$ as **standard**, and we will often freely confuse them with the corresponding elements of M (i.e. we will often simply write ${}^\star x$ as x, when no confusion can arise). We refer to the elements of ${}^\star M$ at large as **non-standard**: if M is infinite, then not all elements of ${}^\star M$ are in the form ${}^\star x$, and hence some "truly non-standard" elements exist.

Example 3.48. *Consider the sequence $s := (n)_{n \in N} \in \mathbb{N}^{\mathbb{N}}$, and define $\omega := [s] \in {}^\star\mathbb{N}$. Now take $m \in \mathbb{N}$, and consider ${}^\star m := [(m, m, m, ...)]$: we have that the subset $\{n \in \mathbb{N} \mid m < s_n\} = \{n \in \mathbb{N} \mid m < n\}$ is in any non-principal ultrafilter $\mathcal{F}$, and hence $m < \omega$. Thus in the non-standard model ${}^\star\mathbb{N}$ there is an **infinite natural** ω which satisfies $m < \omega$ for all standard natural numbers $m \in \mathbb{N}$.*

Example 3.49. *Consider the sequence $s := \big(1/(n+1)\big)_{n \in N} \in \mathbb{R}^{\mathbb{N}}$, and define $\epsilon := [s] \in {}^\star\mathbb{R}$. Now take $0 < x \in \mathbb{R}$, and consider ${}^\star x := [(x, x, x, ...)]$: we have that the subset $\left\{n \in \mathbb{N} \,\middle|\, 0 < \frac{1}{n+1} \leq x\right\} = \{n \in \mathbb{N} \mid n + 1 \geq \lceil 1/x \rceil\}$ is in any non-principal ultrafilter $\mathcal{F}$, and hence $0 < \epsilon \leq x$. Thus in the non-standard model ${}^\star\mathbb{R}$ there is an **infinitesimal real** ϵ which satisfies $0 < \epsilon \leq x$ for all positive standard real numbers $0 < x \in \mathbb{R}$.*

Now we consider a **standard** subset $A \subseteq M$, and we construct the a new non-standard subset ${}^\star A \subseteq {}^\star M$ as follows:

$$[(s_n)_{n \in \mathbb{N}}] \in {}^\star A \text{ iff } \{n \in \mathbb{N} \mid s_n \in A\} \in \mathcal{F} \tag{3.141}$$

The set ${}^\star A$ contains A as a subset, and we refer to it as the **enlargement** of A. Furthermore, functions $f : A \to B$ and relations $R \subseteq A \times B$ between standard sets extend to functions ${}^\star f : {}^\star A \to {}^\star B$ and relations ${}^\star R \subseteq {}^\star A \times {}^\star B$ between the corresponding enlargements; we refer to these as the **non-standard extensions** of the corresponding standard function f and relation R. If $\mathcal{M} := (M, Rel_{\mathcal{M}}, Fun_{\mathcal{M}})$ is the full relational structure associated with the standard model[24], when talking about

[24] I.e. the set $Rel_{\mathcal{M}}$ contains all finitary relations on M, and the set $Fun_{\mathcal{M}}$ contains all finitary (partial) functions on M.

the **non-standard** model we will be considering the following structure:

$$^\star\mathcal{M} := \Big({}^\star M, \{ {}^\star R \mid R \in Rel_{\mathcal{M}} \}, \{ {}^\star f \mid f \in Fun_{\mathcal{M}} \} \Big) \tag{3.142}$$

When M is infinite, the structure presented above is not full: we will refer to subsets, relations and functions appearing in $^\star\mathcal{M}$ as **internal**, and to all other subsets, relations and functions of $^\star M$ as **external**.

The fundamental result which relates the standard model M to any non-standard model $^\star M$ obtained by the ultrapower construction is known as **Transfer Theorem**. The Transfer Theorem plays a central role in this work: all our proofs are carried out explicitly appealing to it, and are therefore blind to the underlying construction of non-standard models. Consider a sentence φ in the language $\mathcal{L}_{\mathcal{M}}$ of the standard model M: constants, functions and relations are chosen from those of $\mathcal{M}$, and quantification is on standard subsets of M. Define the **$*$-transform** $^\star\varphi$ of φ by replacing each constant $a \in M$ with $^\star a \in {}^\star M$, each relation $R \subseteq A \times B$ with $^\star R \subseteq {}^\star A \times {}^\star B$, each function $f : A \to B$ with $^\star f : {}^\star A \to {}^\star B$, and each standard set A with its enlargement $^\star A$; in particular, quantification $\forall x \in A$ and $\exists x \in A$ over a standard set A turns into quantification $\forall x \in {}^\star A$ and $\exists x \in {}^\star A$ over its enlargement. Then $^\star\varphi$ is a sentence in the language $\mathcal{L}_{^\star\mathcal{M}}$ of the non-standard model $^\star M$, and the following result holds.

Theorem 3.50 (**Transfer Theorem**).
A sentence φ holds in the standard model M if and only if its $*$-transform $^\star\varphi$ holds in the non-standard model $^\star M$.

We now present a number of sample applications of the Transfer Theorem to the theory of non-standard naturals and reals.

Example 3.51. *Consider the sentence defining predecessors in the natural numbers:*

$$\forall n \in \mathbb{N}. \big[n \neq 0 \Rightarrow [\exists m \in \mathbb{N}. n = m + 1] \big] \tag{3.143}$$

By Transfer Theorem, the following sentence holds in the non-standard model $^\star\mathbb{N}$:

$$\forall n \in {}^\star\mathbb{N}. \big[n \neq 0 \Rightarrow [\exists m \in {}^\star\mathbb{N}. n = m + 1] \big] \tag{3.144}$$

Hence all non-zero non-standard naturals have predecessors.

Example 3.52. *Consider the sentence defining the well-order property for the natural numbers, i.e. saying that every non-empty subset of $\mathbb{N}$ has a minimum:*

$$\forall A \subseteq \mathbb{N}. \Big[A \neq \emptyset \Rightarrow \big[\exists m \in A . \forall a \in A . m \leq a \big] \Big] \tag{3.145}$$

By Transfer Theorem, the following sentence holds in the non-standard model $^\star\mathbb{N}$*:*

$$\forall^\star A \subseteq {}^\star\mathbb{N}. \Big[{}^\star A \neq \emptyset \Rightarrow \big[\exists m \in^\star\! A.\forall a \in^\star\! A.m \leq a\big]\Big] \tag{3.146}$$

Hence all non-empty internal subsets of $^\star\mathbb{N}$ *have a minimum. Now consider the subset* $W \subset {}^\star\mathbb{N}$ *of all infinite non-standard naturals, i.e.* $W := \{k \in^\star\!\mathbb{N} \mid \forall n \in \mathbb{N}.n < k\}$*. The subset* W *cannot have a minimum: if* $m \in W$ *were such a minimum, then* $m \neq 0$ *and hence* $m - 1$ *would exists (by the previous example); but then* $m - 1$ *would be a standard natural, making* m *itself standard and not infinite. Because* W *is non-empty and has no minimum, we infer that it cannot be an internal subset.*

Example 3.53. *Consider the sentence defining multiplicative inverses in* $\mathbb{R}$*:*

$$\forall x \in \mathbb{R}. \big[x \neq 0 \Rightarrow [\exists y \in \mathbb{R}. x \cdot y = 1]\big] \tag{3.147}$$

By Transfer Theorem, the following sentence holds in the non-standard model $^\star\mathbb{R}$*:*

$$\forall x \in^\star\!\mathbb{R}. \big[x \neq 0 \Rightarrow [\exists y \in {}^\star\mathbb{R}. x \cdot y = 1]\big] \tag{3.148}$$

Hence all non-zero non-standard reals have multiplicative inverses. This reasoning can be applied to all axioms making $\mathbb{R}$ *an ordered field, and hence* $^\star\mathbb{R}$ *is an ordered field, with* $\mathbb{R}$ *as a sub-field. In particular, the following holds by Transfer Theorem:*

$$\forall x, y \in^\star\!\mathbb{R}. [x \neq 0 \wedge y \neq 0] \Rightarrow [x < y \Rightarrow 1/x > 1/y] \tag{3.149}$$

Applying this to the infinitesimal real number ϵ *implies that* $1/\epsilon > x$ *for all* $x \in \mathbb{R}$*, i.e. that* $1/\epsilon$ *is an infinite non-standard real number.*

Example 3.54. *Consider the sentence defining the sequence* $s : \mathbb{N} \to \mathbb{R}$ *of partial sums for every sequence* $f : \mathbb{N} \to \mathbb{R}$ *in the standard model* $\mathbb{R}$*:*

$$\forall f : \mathbb{N} \to \mathbb{R}.\exists s : \mathbb{N} \to \mathbb{R}.\big[s(0) = f(0) \wedge [\forall m \in \mathbb{N}.s(m+1) = s(m) + f(m+1)]\big] \tag{3.150}$$

By Transfer Theorem, the following sentence holds in the non-standard model $^\star\mathbb{R}$*:*

$$\forall^\star f :^\star\!\mathbb{N} \to^\star\!\mathbb{R}.\exists^\star s :^\star\!\mathbb{N} \to^\star\!\mathbb{R}.\big[{}^\star s(0) = {}^\star f(0) \wedge [\forall m \in^\star\!\mathbb{N}.{}^\star s(m+1) = {}^\star s(m) + {}^\star f(m+1)]\big] \tag{3.151}$$

Hence every internal sequence $^\star f : {}^\star\mathbb{N} \to {}^\star\mathbb{R}$ *admits a corresponding internal sequence of partial sums* $^\star s : {}^\star\mathbb{N} \to {}^\star\mathbb{R}$*, i.e. the notation* $\sum_{n=0}^{m} {}^\star f(n)$ *is legitimate for all* $m \in {}^\star\mathbb{N}$*. Similarly,* $^\star f$ *admits a corresponding internal sequence of partial products* $^\star p$*, i.e. the notation* $\prod_{n=0}^{m} {}^\star f(n)$ *is legitimate for all* $m \in {}^\star\mathbb{N}$*.*

Example 3.55. *For each $n \in \mathbb{N}$ we can define the lower set $n\!\downarrow := \{m \in \mathbb{N} \mid m \leq n\}$, and given any sequence $f : \mathbb{N} \to \mathbb{R}$ we can define its truncation $f^{(n)} : n\!\downarrow \to \mathbb{R}$ by setting $f^{(n)}(m) = f(m)$ when $m \leq n$ and leaving $f^{(n)}(m)$ undefined otherwise. By Transfer Theorem, for each $\kappa \in {}^\star\mathbb{N}$ there is a corresponding internal set $\kappa\!\downarrow := \{m \in {}^\star\mathbb{N} \mid m \leq \kappa\}$, and each internal function ${}^\star f : {}^\star\mathbb{N} \to {}^\star\mathbb{R}$ has a corresponding internal truncation ${}^\star f^{(\kappa)} : \kappa\!\downarrow \to {}^\star\mathbb{R}$. When talking about the* ***non-standard extension*** *of a standard sequence $f := (a_n)_{n \in \mathbb{N}}$* ***up to an infinite natural*** *κ we will mean the truncation ${}^\star f^{(\kappa)} : \kappa\!\downarrow \to \mathbb{R}$, which we simply denote by $(a_n)_{n=0}^{\kappa}$.*

3.5.1.2 The structure of ${}^\star\mathbb{N}$

The **non-standard naturals** ${}^\star\mathbb{N}$ form a totally ordered semiring, with the **standard naturals** $\mathbb{N}$ as an initial segment. As a totally ordered set, the non-standard naturals are order-isomorphic to $\mathbb{N} + \theta \times \mathbb{Z}$, where θ is a dense order with no maximum nor minimum. We refer to the standard naturals as **finite naturals**, and to the internal naturals in ${}^\star\mathbb{N} - \mathbb{N}$ as **infinite naturals**: this is because any infinite natural κ satisfies $\kappa > n$ for all $n \in \mathbb{N}$. We say that two non-standard naturals n, m have the same **order of infinity** if they differ by a finite natural $|n - m| \in \mathbb{N}$: this gives an equivalence relation, and the set of equivalence classes is in order-preserving bijection with the totally ordered set $\Theta^+ := \{0\} + \theta$. The set Θ^+ also inherits the additive monoid structure of ${}^\star\mathbb{N}$, but not the full semiring structure.

By Transfer Theorem, many properties of $\mathbb{N}$ transfer to ${}^\star\mathbb{N}$: for example, from the fact that every non-empty set of standard naturals has a minimum we conclude that every non-empty internal set of non-standard naturals also has a minimum, and arguments by induction can be carried out on non-empty internal subsets of ${}^\star\mathbb{N}$. If $(a_n)_{n \in \mathbb{N}}$ is a sequence of natural numbers in the standard model, then we can consider the unique corresponding standard sequence $(a_n)_{n \in {}^\star\mathbb{N}}$ in the non-standard model, coinciding with $(a_n)_{n \in \mathbb{N}}$ for all finite naturals. Furthermore, for any $m \in \mathbb{N}$ the naturals $s_m := \sum_{n=0}^{m} a_n$ and $p_m := \prod_{n=0}^{m} a_n$ exist in the standard model, and hence the non-standard naturals s_m and p_m exist in the non-standard model for all $m \in {}^\star\mathbb{N}$.

The **non-standard integers** ${}^\star\mathbb{Z}$ similarly relate to the standard integers $\mathbb{Z}$: they form a totally ordered ring, with $\mathbb{Z}$ as a sub-ring and ${}^\star\mathbb{N}$ as a sub-semiring. As a totally ordered set, they are order-isomorphic to $(\theta + \{0\} + \theta) \times \mathbb{Z}$: they contain the finite integers together two copies of the infinite naturals, one copy above all finite integers (the **positive infinities**) and one copy below all finite integers (the **negative infinities**). The set $\Theta := \theta + \{0\} + \theta$ of orders of infinity for ${}^\star\mathbb{Z}$ again inherits the total order and the additive group structure, but not the ring one.

3.5.1.3 The structure of $^\star\mathbb{R}$

The **non-standard reals** $^\star\mathbb{R}$ form an ordered field, with the **standard reals** $\mathbb{R}$ as a sub-field and the non-standard integers $^\star\mathbb{Z}$ as a subring. They are a non-archimedean field, with a sub-ring M_1 of **infinitesimals**, smaller in absolute value than all positive standard reals. The non-zero infinitesimals have inverses, the **infinite reals**, larger in absolute value than all positive standard integers/reals.

By using the finite integers $\mathbb{Z} \subset {}^\star\mathbb{Z} \subset {}^\star\mathbb{R}$, it is possible to define the sub-ring[25] M_0 of the **finite reals**, given by those $x \in {}^\star\mathbb{R}$ such that $\exists\ n \in \mathbb{Z}\ |x| < n$. The sub-ring M_1 of infinitesimals is a two-sided ideal in M_0, and by using Dedekind cuts it is possible to show that the ring quotient M_0/M_1 is isomorphic to $\mathbb{R}$: we refer to the corresponding surjective ring homomorphism $\mathrm{st}(\_) : M_0 \to \mathbb{R}$ as the **standard part** (which is the identity on the subring $\mathbb{R} \leq M_0$), and we denote the corresponding quotient equivalence relation on M_0 by $x \simeq y \overset{def}{\iff} |x - y|$ is an infinitesimal. The coset of M_1 surrounding any non-standard real $x \in {}^\star\mathbb{R}$ is called the **monad** of x, and when x is finite it contains exactly one standard real $\mathrm{st}(x) \in \mathbb{R}$.

The non-standard reals are Archimedean in a non-standard sense: by the transfer theorem, for any $x \in {}^\star\mathbb{R}$ there is a unique $n \in {}^\star\mathbb{N}$ such that $n \leq |x| < n + 1$.[26] As a consequence, the non-standard rationals $^\star\mathbb{Q}$ are a dense subfield of $^\star\mathbb{R}$. Furthermore, the non-standard reals can be obtained in the familiar way by "gluing" a copy of the (non-standard) unit interval between any two consecutive (non-standard) integers: as a totally ordered additive group, they are then isomorphic to $\Theta \times M_0$.

Any sequence $(a_n)_{n\in\mathbb{N}}$ of reals definable in the standard model has a corresponding non-standard extension $(a_n)_{n\in{}^\star\mathbb{N}}$ by the transfer theorem: it coincides with the original sequence on all finite naturals, but will not in general be valued in the standard reals on infinite naturals. It is possible to show that $\lim_{n\to\infty} a_n = a \in \mathbb{R}$ in the standard model if and only if $a_n \simeq a$ for all infinite naturals n in the non-standard model. Furthermore, $(a_n)_{n\in\mathbb{N}}$ is bounded (say by $|a_n| \leq z \in \mathbb{R}^+$) in the standard model if and only if a_n is a finite real (with $|a_n| \leq z$) for all infinite naturals.

Real-valued functions $f : I \to \mathbb{R}$ in the standard model can similarly be extended by the transfer theorem to real-valued $f : {}^\star I \to {}^\star\mathbb{R}$ in the non-standard model, coinciding with the original function on all standard reals in $^\star I$. Then $\lim_{x\to a} f(x) = c$ in the standard model if and only if in the non-standard model we have $f(x) \simeq c$ for all $x \simeq a$ (except perhaps at $x = a$). As a consequence, f is continuous at $a \in I$ in

[25] In fact, they form a $\mathbb{R}$-vector subspace of $^\star\mathbb{R}$.

[26] Equivalently, for every infinitesimal $\xi \in M_1$ there is a unique non-standard natural $n \in {}^\star\mathbb{N}$ such that $1/(n+1) < |\xi| \leq 1/n$.

the standard model if and only if in the non-standard model we have $f(x) \simeq f(a)$ whenever $x \simeq a$.

The **non-standard complex numbers** ${}^\star\mathbb{C}$ similarly extend $\mathbb{C}$ with infinitesimals and infinities: they also form a field, with both ${}^\star\mathbb{R}$ and $\mathbb{C}$ as sub-fields. As an additive group, they are isomorphic to ${}^\star\mathbb{R}^2$. We will transfer most notations from ${}^\star\mathbb{R}$ to ${}^\star\mathbb{C}$, when no confusion can arise.

3.5.1.4 Non-standard Hilbert spaces

The passage from standard to non-standard models has a two-fold effect on (complex) Hilbert spaces: (i) the scalars change from $\mathbb{C}$ to ${}^\star\mathbb{C}$; (ii) the vectors change from sequences $(a_n)_{n \in \mathbb{N}^+}$ indexed by the standard naturals to sequences $(a_n)_{n \in {}^\star\mathbb{N}^+}$ indexed by the non-standard naturals. Each standard Hilbert space V has a non-standard counterpart ${}^\star V$: the non-standard space ${}^\star V$ contains all vectors of V, known as the **standard vectors**, as a $\mathbb{C}$-linear (but not ${}^\star\mathbb{C}$-linear) subspace. The non-standard space ${}^\star V$ comes with a ${}^\star\mathbb{C}$-valued inner product (extending the standard one on V), and an associated ${}^\star\mathbb{R}^+$-valued norm.

The vectors infinitesimally close to standard vectors are called **near-standard vectors**, and the vectors with infinitesimal norm are called **infinitesimal vectors**: both form $\mathbb{C}$-linear (and M_0-linear) subspaces ${}^\star V_0$ and ${}^\star V_1$ of ${}^\star V$. There is a $\mathbb{C}$-linear map $\mathrm{st}(\_) : {}^\star V_0 \to V$, known as the **standard part**, which sends the near-standard vectors surjectively onto V, acts as the identity on standard vectors and has the infinitesimal vectors V_1 as kernel. The standard part defines an equivalence relation $\simeq$ on near-standard vectors, with $|\psi\rangle \simeq |\phi\rangle$ if and only if $|\psi\rangle - |\phi\rangle$ is an infinitesimal vector.

An interesting class of non-standard vectors can be obtained by the transfer theorem. Consider a standard complex Hilbert space V which is separable, i.e. comes with a complete orthonormal basis $|e_n\rangle_{n \in \mathbb{N}^+}$ which is countable[27]. If $(\psi_n)_{n \in \mathbb{N}^+}$ is a standard sequence of complex numbers, then the vector $|\psi^{(k)}\rangle := \sum_{n=1}^{k} \psi_n |e_n\rangle \in V$ exists for all positive standard naturals $k \in \mathbb{N}^+$: by the transfer theorem, the vector $|\psi^{(\kappa)}\rangle$ exists in ${}^\star V$ for any infinite natural κ, where the corresponding non-standard sequence $(\psi_n)_{n \in {}^\star\mathbb{N}^+}$ is used to provide values. In particular, the vector $\sum_{n=1}^{\kappa} |e_n\rangle \in {}^\star V$ exists, and has squared norm $\kappa \in {}^\star\mathbb{R}^+$.

[27] We index our vectors in the positive naturals $\mathbb{N}^+$ for reasons of convenience: this way a generic vector in a d-dimensional vector space is written cleanly as $\sum_{n=1}^{d} v_n |e_n\rangle$.

The vectors of finite norm are known as **finite vectors** and form a $\mathbb{C}$-linear (and M_0-linear) subspace of V. However, this is where the second effect of non-standard analysis on Hilbert spaces comes into play: there exist finite vectors, such as $|\phi\rangle := \frac{1}{\sqrt{\kappa}} \sum_{n=1}^{\kappa} |e_n\rangle$, which are not near-standard. Indeed, any standard vector $|\psi\rangle$ is infinitesimally close to its truncation in the form $|\psi^{(\kappa)}\rangle := \sum_{n=1}^{\kappa} \psi_n |e_n\rangle$, where ψ_ν is infinitesimal for all infinite naturals ν. We get the following lower bound for the squared norm of the difference $|\phi\rangle - |\psi\rangle$:

$$\begin{aligned} \Big|\Big||\phi\rangle - |\psi\rangle\Big|\Big|^2 \simeq \Big|\Big||\phi\rangle - |\psi^{(\kappa)}\rangle\Big|\Big|^2 &= \sum_{n=1}^{\kappa} \frac{|1-\psi_n|^2}{\kappa} \geq \sum_{n \geq \kappa/M} \frac{|1-\psi_n|^2}{\kappa} \\ &\geq \sum_{n \geq \kappa/M} \frac{1-\epsilon}{\kappa} = (1-\epsilon)(1-\frac{1}{M}) \end{aligned}$$

for all $M \in \mathbb{N}^+$ and $\epsilon \in (0,1)$. This means that $\mathrm{st}(\Big|\Big||\phi\rangle - |\psi^{(\kappa)}\rangle\Big|\Big|) \geq 1$ for all standard vectors $|\psi\rangle$, and hence the vector $|\phi\rangle$ is finite but not near-standard. Finite vectors which are not near-standard are genuinely new, and can be used to do genuinely new things. This is what makes the non-standard approach to quantum mechanics so powerful: in $^\star\mathbb{R}$ and $^\star\mathbb{C}$ finite numbers are all near-standard, and correspond to standard numbers under infinitesimal equivalence, while in a non-standard Hilbert space one gets new things for free, such as normalised plane-waves in $\mathrm{L}^2[\mathbb{Z}]$ and Dirac-deltas in $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$. These will be the fundamental building blocks of our work.

The transfer theorem can similarly be used to define non-standard linear operators (not necessarily continuous/bounded): if $(a_{nm})_{n,m\in\mathbb{N}^+}$ is a doubly-indexed sequence (a.k.a. a matrix) of complex numbers, then the linear operator $\sum_{m,n=0}^{\kappa} a_{mn} |e_m\rangle\langle e_n| : {}^\star V \to {}^\star V$ exists for any infinite natural κ (where $(a_{nm})_{n,m\in{}^\star\mathbb{N}^+}$ is the unique internal non-standard sequence given by the transfer theorem). This is a remarkable result, but it comes with some tricky limitations which will be presented in the next section.

3.5.2 The category *Hilb

The main idea behind our construction is to legitimise, through non-standard analysis, notations such as $\sum_{n\in\mathbb{N}^+} |e_n\rangle\langle e_n|$ for the identity operator, $\sum_{n\in\mathbb{N}^+} |e_n\rangle$ for the unit of an infinite-dimensional Frobenius algebra, $\sum_{n,m\in\mathbb{N}^+} |e_n\rangle a_{nm} \langle a_m|$ for a general matrix $(a_{nm})_{n,m\in\mathbb{N}^+}$. The transfer theorem doesn't allow us to conclude the existence of sums strictly over $\mathbb{N}^+$ (nor over the entirety of $^\star\mathbb{N}$), but it does allow us to sum up to some infinite natural κ: the sums $\sum_{n=1}^{\kappa} |e_n\rangle\langle e_n|$, $\sum_{n=1}^{\kappa} |e_n\rangle$ and $\sum_{n,m=1}^{\kappa} |e_n\rangle a_{nm} \langle e_m|$ all describe well-defined internal linear maps of non-standard Hilbert spaces. Unfortunately,

$P_\kappa := \sum_{n=1}^{\kappa} |e_n\rangle\langle e_n|$ does not behave like the identity over the space of all internal linear maps, but rather it is as a subspace projector: in order to turn these projectors into identities, we use a construction similar to that of the Cauchy/idempotent[28] completion. As it turns out, this procedure preserves all standard bounded operators, and enough non-standard ones to do many of the things we care about in categorical quantum mechanics.

3.5.2.1 Definition of the category

We proceed to define the **category of non-standard separable Hilbert spaces**[29], which we will denote by *Hilb. All proofs of results in this and future sections can be found in the Appendix. As objects we take separable (standard) Hilbert spaces together with a witness of separability, i.e. pairs $\mathcal{H} := \big(V, |e_n\rangle_{n=1}^{\kappa}\big)$ of a standard separable Hilbert space V and a family of vectors $|e_n\rangle_{n=1}^{\kappa}$ defined as follows (for some non-standard natural $\kappa \in {^\star}\mathbb{N}$).

(i) If V is finite-dimensional: we consider a finite orthonormal basis $|e_n\rangle_{n=1}^{\kappa}$, where $\kappa := \dim V \in \mathbb{N}$.

(ii) If V is infinite-dimensional: we fix some infinite natural $\kappa \in {^\star}\mathbb{N}$ (meant to be the non-standard dimension), and we consider the unique extension (by the transfer theorem) up to κ of a complete orthonormal basis $|e_n\rangle_{n\in\mathbb{N}^+}$ for V.

For each object $\mathcal{H} := \big(V, |e_n\rangle_{n=1}^{\kappa}\big)$, let the **truncating projector** $P_\mathcal{H} : \mathcal{H} \to \mathcal{H}$ be the following internal linear map ${^\star}V \to {^\star}V$, where we refer to $\dim \mathcal{H} := \kappa \in {^\star}\mathbb{N}$ as the **dimension** of object $\mathcal{H}$:

$$P_\mathcal{H} := \sum_{n=1}^{\dim \mathcal{H}} |e_n\rangle\langle e_n|. \tag{3.152}$$

We also use notation $|\mathcal{H}| := V$ to refer to the standard separable Hilbert space underlying an object $\mathcal{H}$ of *Hilb. The morphisms in the category *Hilb are then defined as follows:

$$\mathrm{Hom}_{^\star\mathrm{Hilb}}\left[\mathcal{H}, \mathcal{G}\right] := \{\, P_\mathcal{G} \circ F \circ P_\mathcal{H} \;\mid\; F : {^\star}|\mathcal{H}| \to {^\star}|\mathcal{G}| \text{ internal linear map}\}\,. \tag{3.153}$$

Because the truncating projectors for $\mathcal{H}$ and $\mathcal{G}$ are internal linear maps, the composite $P_\mathcal{G} \circ F \circ P_\mathcal{H}$ is an internal linear map ${^\star}|\mathcal{H}| \to {^\star}|\mathcal{G}|$, which we shall denote by $\bar{F}$.

[28] Projectors are self-adjoint idempotents.

[29] We have complex Hilbert spaces in mind, but the construction is identical for real Hilbert spaces.

Composition of morphisms in *Hilb is simply composition of internal linear maps

$$\bar{G}\cdot\bar{F} := \bar{G}\circ\bar{F} = (P_{\mathcal{G}}\circ G\circ P_{\mathcal{H}})\circ(P_{\mathcal{H}}\circ F\circ P_{\mathcal{K}}) = P_{\mathcal{G}}\circ(G\circ P_{\mathcal{H}}\circ F)\circ P_{\mathcal{K}}, \quad (3.154)$$

where we used associativity of composition and idempotence of truncating projectors. Idempotence of the projectors, in particular, means that they provide suitable identity morphisms. Indeed if we define

$$id_{\mathcal{H}} := P_{\mathcal{H}}\circ id_{{}^\star|\mathcal{H}|}\circ P_{\mathcal{H}} = P_{\mathcal{H}}\circ P_{\mathcal{H}} = P_{\mathcal{H}}, \quad (3.155)$$

it is straightforward to check that $id_{\mathcal{G}}\cdot\bar{F} = P_{\mathcal{G}}\circ P_{\mathcal{G}}\circ F\circ P_{\mathcal{H}} = P_{\mathcal{G}}\circ F\circ P_{\mathcal{H}} = \bar{F}$, and similarly for $\bar{F}\cdot id_{\mathcal{H}}$.

Now consider two naturals $\kappa,\nu\in{}^\star\mathbb{N}$, and define the internal map

$$\varsigma_{\kappa,\nu}(n,m) := (n-1)\nu + m, \quad (3.156)$$

which is an internal bijection between $\{1,...,\kappa\}\times\{1,...,\nu\}$ and $\{1,...,\kappa\nu\}$. Also, we will simply write $\varsigma(n,m)$ when no confusion can arise. A tensor product can be defined on the objects of *Hilb as follows, with tensor unit $(\mathbb{C},1)$:

$$\Big(V,|e_n\rangle_{n=1}^{\kappa}\Big)\otimes\Big(W,|f_m\rangle_{m=1}^{\nu}\Big) := \Big(V\otimes W,\big(|e_n\rangle\otimes|f_m\rangle\big)_{\varsigma(n,m)=1}^{\kappa\nu}\Big). \quad (3.157)$$

In order to define the tensor product on morphisms, we need to first note that morphisms $\bar{F}:\mathcal{H}\to\mathcal{G}$ in *Hilb are uniquely determined by certain matrices $\{1,...,\dim\mathcal{G}\}\times\{1,...,\dim\mathcal{H}\}\to{}^\star\mathbb{C}$:

$$\bar{F} = P_{\mathcal{G}}\circ F\circ P_{\mathcal{H}} = \sum_{m=1}^{\dim\mathcal{G}}\sum_{n=1}^{\dim\mathcal{H}}|f_m\rangle\Big(\langle f_m|F|e_n\rangle\Big)\langle e_n|. \quad (3.158)$$

We introduce the notation $\bar{F}_{mn} := \langle f_m|F|e_n\rangle$, and define the tensor product of two morphisms $\bar{F}:\mathcal{H}\to\mathcal{G}$ and $\bar{G}:\mathcal{H}'\to\mathcal{G}'$ to be the familiar tensor product of matrices:

$$\bar{F}\otimes\bar{G} := \sum_{\varsigma(m,m')=1}^{\dim\mathcal{G}\dim\mathcal{G}'}\sum_{\varsigma(n,n')=1}^{\dim\mathcal{H}\dim\mathcal{H}'}|f_m\rangle\otimes|f'_{m'}\rangle\;\bar{F}_{mn}\bar{G}_{m'n'}\;\langle e_n|\otimes\langle e'_{n'}|. \quad (3.159)$$

The map $\bar{F}\otimes\bar{G}$ is an internal linear map ${}^\star|\mathcal{H}|\otimes{}^\star|\mathcal{H}'|\to{}^\star|\mathcal{G}|\otimes{}^\star|\mathcal{G}'|$ by the transfer theorem. Also we have that $P_{\mathcal{H}}\otimes P_{\mathcal{H}'} = P_{\mathcal{H}\otimes\mathcal{H}'}$, and that $\bar{F}\otimes\bar{G} = P_{\mathcal{G}\otimes\mathcal{G}'}\circ\big(\bar{F}\otimes\bar{G}\big)\circ P_{\mathcal{H}\otimes\mathcal{H}'}$. Hence, $\bar{F}\otimes\bar{G}$ is a genuine morphism $\mathcal{H}\otimes\mathcal{H}'\to\mathcal{G}\otimes\mathcal{G}'$. It is straightforward to check that this results in a well defined tensor product, and the following braiding operator turns *Hilb into a symmetric monoidal category (SMC):

$$\sigma_{\mathcal{H}\mathcal{G}} := \sum_{\varsigma(n,m)=1}^{\dim\mathcal{H}\dim\mathcal{G}}|f_m\rangle\otimes|e_n\rangle\;\langle e_n|\otimes\langle f_m|. \quad (3.160)$$

Finally, one can define a dagger on morphisms by taking the conjugate transpose on the **matrix representation** given by (3.158), obtaining the following morphism (by the transfer theorem):

$$(\bar{F})^\dagger := \sum_{n=1}^{\dim \mathcal{H}} \sum_{m=1}^{\dim \mathcal{G}} |e_n\rangle \bar{F}^\star_{mn} \langle f_m|. \tag{3.161}$$

It is straightforward to check that $(\bar{F})^\dagger$ is a morphism $\mathcal{G} \to \mathcal{H}$ whenever $\bar{F}$ is a morphism $\mathcal{H} \to \mathcal{G}$, that the dagger is functorial and that it satisfies all the compatibility requirements with the monoidal structure. The content of this section can thus be summarised by the following result.

Theorem 3.56. *The category* *Hilb *is a* †*-SMC, with tensor product and dagger defined by (3.157, 3.159, 3.161).*

3.5.2.2 Standard bounded linear maps in *Hilb

In order to do categorical quantum mechanics in *Hilb, we have to first establish its relationship with the more traditional arena of standard Hilbert spaces and bounded linear maps. By construction, we don't expect *Hilb to contain all of Hilb, as the objects were explicitly chosen to be separable (rather than arbitrary) Hilbert spaces. We expect, however, that the full subcategory sHilb of separable Hilbert spaces and bounded linear maps will be faithfully embedded in it.

We will refer to morphisms $|\psi\rangle :\equiv \sum_{n=1}^{\dim \mathcal{H}} \psi_n |e_n\rangle : {}^\star\mathbb{C} \to \mathcal{H}$ as **vectors** or **states** in $\mathcal{H}$, and the $^\star\mathbb{C}$-valued inner product induced by the dagger can be written as $\langle \phi | \psi \rangle = \sum_{n=1}^{\dim \mathcal{H}} \phi_n^\star \psi_n$. We will refer to vectors $|\psi\rangle$ having finite squared norm $\langle \psi | \psi \rangle$ as **finite vectors**, and to vectors having infinitesimal squared norm as **infinitesimal vectors**. Difference by infinitesimal vectors gives rise to the following equivalence relation, corresponding to the notion of convergence of vectors in norm:

$$|\phi\rangle \simeq |\psi\rangle \overset{def}{\iff} |\phi\rangle - |\psi\rangle \text{ is infinitesimal.} \tag{3.162}$$

We will say that a morphism $\bar{F} : \mathcal{H} \to \mathcal{G}$ in *Hilb is **continuous** if for any $|\psi_\kappa\rangle, |\phi_\kappa\rangle : {}^\star\mathbb{C} \to \mathcal{H}$ satisfying $|\psi_\kappa\rangle \simeq |\phi_\kappa\rangle$ we have $\bar{F}|\psi_\kappa\rangle \simeq \bar{F}|\phi_\kappa\rangle$. Furthermore, the **operator norm** on some homset $\mathrm{Hom}_{^\star\mathrm{Hilb}}[\mathcal{H}, \mathcal{G}]$ can be defined as follows[30]:

$$||\bar{F}||_{op} := \sup_{\langle \psi | \psi \rangle = 1} \sqrt{\langle \psi | \bar{F}^\dagger \bar{F} | \psi \rangle}. \tag{3.163}$$

[30] Both the sup and the square root are simply extended from $\mathbb{R}^+$ to $^\star\mathbb{R}^+$ by the transfer theorem, as usual. The definition of the operator norm is independent of the equivalence relation $\simeq$.

We will say that a morphism $\bar{F} : \mathcal{H} \to \mathcal{G}$ is **bounded** if its operator norm $||\bar{F}||_{op}$ is finite. Just as it happens in the case of standard Hilbert spaces, throughout this work we will confuse bounded and continuous, thanks to the following result.

Lemma 3.57. *Let $\bar{F} : \mathcal{H} \to \mathcal{G}$ be a morphism in* *Hilb*. The following are equivalent:*

(i) the operator norm $||\bar{F}||_{op}$ is finite;

(ii) $\bar{F}|\xi_\kappa\rangle : {}^\star\mathbb{C} \to \mathcal{G}$ is infinitesimal whenever $|\xi_\kappa\rangle : {}^\star\mathbb{C} \to \mathcal{H}$ is infinitesimal;

(iii) if $|\psi_\kappa\rangle, |\phi_\kappa\rangle : {}^\star\mathbb{C} \to \mathcal{H}$ satisfy $|\psi_\kappa\rangle \simeq |\phi_\kappa\rangle$, then we have $\bar{F}|\psi_\kappa\rangle \simeq \bar{F}|\phi_\kappa\rangle$.

Proof. (i) implies (ii): let $\zeta := \langle\xi_\kappa|\xi_\kappa\rangle$ be an infinitesimal; then we have $\langle\xi_\kappa|\bar{F}^\dagger\bar{F}|\xi_\kappa\rangle \leq \zeta||\bar{F}||_{op}$, which is infinitesimal since $||\bar{F}||_{op}$ is finite. *(ii) implies (i)*: if $||\bar{F}||_{op}$ is infinite, then for some $|\psi_\kappa\rangle$ of unit norm we have $\langle\psi_\kappa|\bar{F}^\dagger\bar{F}|\psi_\kappa\rangle = \theta$ infinite; but then $\langle\psi_\kappa|\frac{1}{\sqrt{\theta}}\bar{F}^\dagger\bar{F}\frac{1}{\sqrt{\theta}}|\psi_\kappa\rangle = 1$ is not infinitesimal, with $\frac{1}{\sqrt{\theta}}|\psi_\kappa\rangle$ infinitesimal. *(ii) equivalent to (iii)*: by linearity of $\bar{F}$. □

The following equivalence relation embodies the notion of convergence in operator norm:

$$\bar{F} \sim \bar{F}' \overset{def}{\iff} ||\bar{F} - \bar{F}'||_{op} \text{ is infinitesimal.} \tag{3.164}$$

This equivalence relation is $\mathbb{C}$-linear, by triangle inequality, and it commutes with the dagger. It also commutes with composition and tensor product, as long as we restrict ourselves to continuous operators.

Lemma 3.58. *Suppose that $\bar{F}$, $\bar{F}'$, $\bar{G}$ and $\bar{G}'$ are all continuous. Then the following statements hold:*

$$\begin{aligned} \bar{G}\cdot\bar{F} \sim \bar{G}'\cdot\bar{F}' &\text{ whenever both } \bar{F} \sim \bar{F}' \text{ and } \bar{G} \sim \bar{G}', \\ \bar{G}\otimes\bar{F} \sim \bar{G}'\otimes\bar{F}' &\text{ whenever both } \bar{F} \sim \bar{F}' \text{ and } \bar{G} \sim \bar{G}'. \end{aligned} \tag{3.165}$$

Proof. Bi-linearity of composition and tensor product, together with the triangle inequality, imply that the only statements we need to prove are the following:

$$\begin{aligned} &||\bar{G}\cdot\xi_\kappa||_{op} \text{ infinitesimal whenever } \bar{G} \text{ continuous and } \xi_\kappa \text{ infinitesimal;} \\ &||\zeta_\kappa\cdot\bar{F}||_{op} \text{ infinitesimal whenever } \bar{F} \text{ continuous and } ||\zeta_\kappa||_{op} \text{ infinitesimal;} \\ &||\bar{G}\otimes\xi_\kappa||_{op} \text{ infinitesimal whenever } \bar{G} \text{ continuous and } ||\xi_\kappa||_{op} \text{ infinitesimal.} \end{aligned} \tag{3.166}$$

The first statement follows from the fact that $||\bar{G}\xi_\kappa||_{op} \leq ||\bar{G}||_{op}||\xi_\kappa||_{op}$, which is infinitesimal because $||\bar{G}||_{op}$ is finite. The second statement goes similarly. The third statement is slightly trickier. Let $|\psi_\kappa\rangle$ be unit norm, and write $|\psi_\kappa\rangle = \sum_n |\phi_\kappa^{(n)}\rangle|e_n\rangle$ (where $(|e_n\rangle)_n$ is the chosen orthonormal basis for the domain of ξ_κ). Then we have the following

$$\langle\psi_\kappa|(\bar{G}\otimes\xi_\kappa)^\dagger(\bar{G}\otimes\xi_\kappa)|\psi_\kappa\rangle \leq \sum_{n'}\sum_n \langle\phi_\kappa^{(n)}|\phi_\kappa^{(n)}\rangle||\bar{G}||_{op}|(\xi_\kappa)_{n'n}|^2 \leq ||\bar{G}||_{op}||\xi_\kappa||_{op}, \tag{3.167}$$

where the last product is infinitesimal because $||\bar{G}||_{op}$ is finite. □

We say that a morphism $\bar{G}$ is **near-standard** (in the operator norm) if it satisfies $\bar{G}\sim\bar{f}$ for some standard bounded linear map f. From now on, we will always use lowercase letters to denote standard bounded linear maps. Near-standard morphisms are in particular continuous, and form a sub-†-SMC of *Hilb, which we shall denote by $^\star\text{Hilb}^{(std)}$. If ω is some infinite natural, we denote by $^\star\text{Hilb}^{(std)}_\omega$ the full sub-category of $^\star\text{Hilb}^{(std)}$ having objects which are either finite-dimensional or have dimension ω. By Lemma 3.58 both $^\star\text{Hilb}^{(std)}$ and $^\star\text{Hilb}^{(std)}_\omega$ can be enriched to become a strict †-symmetric monoidal 2-categories. This observation finally allows us to relate our newly introduced category *Hilb to the more familiar sHilb.
We define a strict **standard part** functor $\text{st}(\_) : {}^\star\text{Hilb}^{(std)} \to \text{sHilb}$ as follows:

(i) $\text{st}(V, |e_n\rangle_{n=1}^\kappa) := V$;

(ii) $\text{st}(\bar{F}) :=$ the unique f such that f is standard bounded and $\bar{F}\sim\bar{f}$.

We fix an infinite non-standard natural ω, and define a weak **lifting functor**, denoted by $\text{lift}_\omega : \text{sHilb} \to {}^\star\text{Hilb}^{(std)}$, as follows (with functoriality only up to $\sim$):

(i) $\text{lift}_\omega[V] := (V, (|e_n\rangle)_n)$, where the orthonormal bases are chosen in such a way as to respect tensor product of $^\star\text{Hilb}^{(std)}$ (see the [GG16] for details);

(ii) we have that $\text{lift}_\omega[f] := \bar{f}$ on morphisms, and Lemma 3.58 guarantees that $\text{lift}_\omega[G\cdot F] \sim \text{lift}_\omega[G]\cdot\text{lift}_\omega[F]$.

For any fixed infinite natural ω, the standard part functor restricts to a functor $\text{st}(\_) : {}^\star\text{Hilb}^{(std)}_\omega \to \text{sHilb}$, and the lifting functor restricts to a well-defined weak functor $\text{lift}_\omega : \text{sHilb} \to {}^\star\text{Hilb}^{(std)}_\omega$.

Theorem 3.59. *The following results relate* $^\star\text{Hilb}^{(std)}_\omega$ *and* sHilb*:*

(i) $\text{st}(\_)$ *is a strict full functor of* †*-SMCs, which is surjective on objects;*

(ii) lift_ω *is a weak faithful functor from a* †*-SMC to a* †*-symmetric monoidal 2-category, which is essentially surjective on objects; its restriction to the subcategory* fHilb *is strictly functorial;*

(iii) $\mathrm{st}(\mathrm{lift}_\omega[f]) = f$*, for all standard bounded morphisms* f*;*

(iv) $\mathrm{st}(\mathrm{lift}_\omega[V]) = V$*, for all objects* V *of* sHilb*;*

(v) For all objects $\mathcal{H}$ *of* $^\star\mathrm{Hilb}_\omega^{(std)}$*, there is a (unique) standard unitary* $\bar{u}_\mathcal{H} : \mathcal{H} \to \mathrm{lift}_\omega[\mathrm{st}(\mathcal{H})]$ *such that* $\mathrm{st}(\bar{u}_\mathcal{H}) = id_{\mathrm{st}(\mathcal{H})}$*.*

(vi) $\bar{u}_\mathcal{G}^\dagger \, \mathrm{lift}_\omega[\mathrm{st}(\bar{F})]\bar{u}_\mathcal{H} \sim \bar{F}$ *for all morphisms* $\bar{F} : \mathcal{H} \to \mathcal{G}$ *in* $^\star\mathrm{Hilb}_\omega^{(std)}$

Proof. Existence and uniqueness of definition of $\mathrm{st}(\bar{F})$*.* By definition, if $\bar{F}$ is near-standard, at least one standard bounded linear map f' exists such that $\bar{F} \sim \bar{f}'$. Now take two such standard bounded linear maps f' and f'': by transitivity we get that $f' \sim f''$, i.e. that $||\bar{f}' - \bar{f}''||_{op}$ is infinitesimal; define $g := f' - f''$, standard bounded linear map. By transfer theorem (both directions), $\sqrt{\langle\psi|g^\dagger g|\psi\rangle}$ is bounded above (by a standard constant $c \in \mathbb{R}^+$, for all standard $|\psi\rangle$ satisfying $\langle\psi|\psi\rangle = 1$), if and only if $\sqrt{\langle\psi|g^\dagger g|\psi\rangle}$ is also bounded above (by the same standard constant c, for all internal $|\psi\rangle$ such that $\langle\psi|\psi\rangle = 1$). Because g is standard and bounded, $\sqrt{\langle\psi|g^\dagger g|\psi\rangle}$ and $\sqrt{\langle\psi|\bar{g}^\dagger\bar{g}|\psi\rangle}$ are infinitesimally close: as a consequence, if $||\bar{f}' - \bar{f}''||_{op}$ is infinitesimal, then it is bounded above by all standard reals $c > 0$, and hence by the transfer theorem so is $||f' - f''||_{op}$. This proves that $||f' - f''||_{op} = 0$, and we conclude that $f' = f''$.

Choice of orthonormal bases for lift_ω*.* Up to equivalence of categories, we can consider sHilb as having objects given by all finite (possibly empty) tensor products of the following basic objects: the finite-dimensional Hilbert spaces $\mathbb{C}^p$ for all primes p, and the separable space $\ell^2[\mathbb{N}^+]$. Choose any orthonormal basis for each of the basic objects; denote them by $|e_n^{(p)}\rangle_{n=1}^p$ and $|e_n^{(\infty)}\rangle_{n=1}^\infty$. On basic objects, define $\mathrm{lift}_\omega[\mathbb{C}^p] := (\mathbb{C}^p, |e_n^{(p)}\rangle_{n=1}^p)$ and $\mathrm{lift}_\omega[\ell^2[\mathbb{N}^+]] := (\ell^2[\mathbb{N}^+], |e_n^{(\infty)}\rangle_{n=1}^\omega)$. Extend the definition to finite tensor products by using the tensor product of *Hilb (or, equivalently, by using the bijection ς from Equation (3.156) to explicitly construct a basis).

Proof that $f \mapsto \bar{f}$ *is an injection.* Let f, g be standard bounded linear maps, defined by matrices $(a_{nm})_{n,m\in\mathbb{N}^+}$ and $(b_{nm})_{n,m\in\mathbb{N}^+}$ respectively. The matrices can be extended by the transfer theorem to non-standard indices, and $\bar{f}$ and $\bar{g}$ have matrices $(a_{nm})_{\varsigma(n,m)=1}^{\kappa\nu}$ and $(b_{nm})_{\varsigma(n,m)=1}^{\kappa\nu}$. If $\bar{f} = \bar{g}$, then we have that $(a_{nm})_{\varsigma(n,m)=1}^{\kappa\nu} = (b_{nm})_{\varsigma(n,m)=1}^{\kappa\nu}$ as matrices, and in particular $a_{nm} = b_{nm}$ for all $n, m \in \mathbb{N}^+$, proving that $f = g$ in the first place.

Weak functoriality of lift_ω. We begin by covering weak functoriality of lift_ω, as it makes an interesting point by itself. Note that $\mathrm{lift}_\omega[g] \cdot \mathrm{lift}_\omega[f] = P_{\mathcal{G}} \circ g \circ P_{\mathcal{H}} \circ f \circ P_{\mathcal{K}}$, and that $\mathrm{lift}_\omega[g \cdot f] = P_{\mathcal{G}} \circ g \circ f \circ P_{\mathcal{K}}$. In the infinite-dimensional case, if f, g are standard bounded linear maps, then the standard series $a_{ln} := \sum_{m=0}^{\infty} g_{lm} f_{mn}$ converges for all fixed l, n, and the non-standard complex number $\sum_{m=0}^{\kappa} g_{lm} f_{mn}$ is infinitesimally close to the standard complex number a_{ln}. Hence $g \circ P_{\mathcal{H}} \circ g \sim g \circ f$, when seen as internal morphisms of non-standard Hilbert spaces. In the finite-dimensional case, there is no issue of truncation, and lift_ω is strictly functorial.

Proof of the main results. Proof of (i). The map $\mathrm{st}(\_)$ is well-defined and monoidally functorial by Lemma 3.58. It is full by the proof of existence/uniqueness given above, and surjective on objects by construction of $^\star\mathrm{Hilb}$ and sHilb. *Proof of (ii).* The map $\mathrm{lift}_\omega[\_]$ is weakly functorial by the argument given at the beginning of this proof (strictly functorial when restricted to fHilb), and monoidally so by Lemma 3.58 and the choice of orthonormal bases presented above. Faithfulness was proven above (by showing that $f \mapsto \bar{f}$ is an injection), and essential surjectivity follows from point (v) below. *Proof of (iii).* We know from above that lift_ω is faithful, i.e. that $f \mapsto \bar{f}$ is an injection. If f is a standard bounded linear map, then the morphism $\mathrm{st}(\mathrm{lift}_\omega[f])$ of sHilb is the unique standard bounded linear map which is infinitesimally close (in operator norm) to $\bar{f}$, i.e. it is f itself. *Proof of (iv).* By definition of the two functors. *Proof of (v).* By (iii), one such standard unitary $\bar{u}_{\mathcal{H}}$ exists, namely by taking $u := id_{\mathcal{H}}$. Uniqueness follows because any such unitary must be infinitesimally close to the standard unitary $\bar{u}_{\mathcal{H}}$ define above, and at most one such standard linear map exists. *Proof of (vi).* The morphism $\bar{u}_{\mathcal{G}}^{\dagger} \, \mathrm{lift}_\omega[\mathrm{st}(\bar{F})]\bar{u}_{\mathcal{H}}$ is infinitesimally close to its image under $\mathrm{st}(\_)$, which is $\mathrm{st}(\bar{F})$ by points (iii) and (v) above. Similarly, $\bar{F}$ is infinitesimally close to its image under $\mathrm{st}(\_)$, which is also $\mathrm{st}(\bar{F})$. We conclude by transitivity/symmetry of $\sim$. □

3.5.3 How to use *Hilb for standard purposes

The essence of Theorem 3.59 is that sHilb is equivalent to the subcategory $^\star\mathrm{Hilb}^{(std)}$ of *Hilb given by near-standard morphisms in the operator norm, as long as we take care to equate morphisms which are infinitesimally close. The equivalence allows one to prove results about sHilb by working in *Hilb and taking advantage of the CQM machinery introduced in the next Section. In a typical scenario, one might follow the following procedure, which is conceptually akin to using the two directions of the transfer theorem to prove results of standard analysis using non-standard methods:

(i) start from sHilb;

(ii) lift to ${}^\star\mathrm{Hilb}^{(std)}$ via the lifting functor;

(iii) work in *Hilb to obtain a near-standard result (living again in ${}^\star\mathrm{Hilb}^{(std)}$);

(iv) descend again to sHilb via the standard part functor.

When proving equalities in sHilb, it is in fact sufficient to lift both sides via lift_ω, and prove the equality in *Hilb without further constraints (this is because both sides will necessarily be lifted to ${}^\star\mathrm{Hilb}^{(std)}$).

The arbitrary choice of infinite natural ω in the "lifting phase" might seem unnatural at first, as the objects $\mathrm{lift}_\omega[V]$ and $\mathrm{lift}_{\omega'}[V]$ are not isomorphic in *Hilb for different infinite naturals $\omega \neq \omega'$. However, this is not actually an issue: from the perspective of sHilb, the two spaces are equivalent for all intents and purposes, because any proof that can be performed in one space can also be performed in the other. The following result makes this statement categorically precise.

Lemma 3.60. *Let $\omega, \omega' \in {}^\star\mathbb{N}$ be infinite natural numbers. Then the categories ${}^\star\mathrm{Hilb}^{(std)}_\omega$ and ${}^\star\mathrm{Hilb}^{(std)}_{\omega'}$ are weakly equivalent over* sHilb*, in the sense that there is a weak functor $\Phi_{\omega,\omega'} :{}^\star \mathrm{Hilb}^{(std)}_\omega \rightarrow{}^\star \mathrm{Hilb}^{(std)}_{\omega'}$ such that:*

$$\begin{aligned}\Big(\Phi_{\omega',\omega} \circ \Phi_{\omega,\omega'}\Big)(\mathcal{H}) &= \mathcal{H} \textit{ for all objects } \mathcal{H} \textit{ of } {}^\star\mathrm{Hilb}^{(std)}_\omega \\ \Big(\Phi_{\omega',\omega} \circ \Phi_{\omega,\omega'}\Big)(\bar{F}) &\sim \bar{F} \textit{ for all morphisms } \bar{F} \textit{ of } {}^\star\mathrm{Hilb}^{(std)}_\omega\end{aligned}$$

In particular, from the standard point of view of sHilb *we have that* $\mathrm{st} \circ \Phi_{\omega,\omega'} = \mathrm{st}$*, so that the categories ${}^\star\mathrm{Hilb}^{(std)}_\omega$ and ${}^\star\mathrm{Hilb}^{(std)}_{\omega'}$ are indistinguishable for standard purposes.*

Proof. Define the functor $\Phi_{\omega,\omega'}$ as follows:

$$\Phi_{\omega,\omega'}(V, |e_n\rangle_{n=1}^{\omega}) := (V, |e_n\rangle_{n=1}^{\omega'}) \qquad \Phi_{\omega,\omega'}(\bar{F}) := \bar{F} \tag{3.168}$$

Because all morphisms $\bar{F}$ of ${}^\star\mathrm{Hilb}^{(std)}_\omega$ are near-standard, this is clearly a weak functor of symmetric monoidal 2-categories: it respects composition and tensor product of morphisms only up to infinitesimal equivalence $\sim$, because the truncation $\bar{F}$ is performed with different truncating projectors in ${}^\star\mathrm{Hilb}^{(std)}_\omega$ and ${}^\star\mathrm{Hilb}^{(std)}_{\omega'}$. By their very definition, $\Phi_{\omega,\omega'}$ and $\Phi_{\omega',\omega}$ establish a weak equivalence between ${}^\star\mathrm{Hilb}^{(std)}_\omega$ and ${}^\star\mathrm{Hilb}^{(std)}_{\omega'}$, and the equation $\mathrm{st} \circ \Phi_{\omega,\omega'} = \mathrm{st}$ is also a straightforward check. □

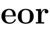
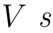
There are two main kinds of proofs that can be performed using *Hilb.

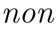
- In one kind of proof, we have standard maps which can be expressed as compositions of non-standard maps with nicer algebraic/diagrammatic properties. This is the case, for example, of the proof of the Weyl Canonical Commutation Relations: the time-translation unitary (standard) is expressed as composition of the Frobenius algebra multiplication for the momentum observable (standard) and a position eigenstate (not near-standard), while the the momentum-boost unitary (standard) is expressed as composition of the Frobenius algebra multiplication for the position observable (not near-standard) and a momentum eigenstate (standard). This is also the case in the proof of Stone's Theorem on 1-parameter unitary groups (in the case of continuous periodic dynamics, where a symmetric cup is used to turn the unitary dynamics into the observable associated with their invariant.
- In the other kind of proof, we have equalities between standard maps which involve limits: these are lifted to equalities between non-standard maps where the limits have been absorbed into appropriate limiting objects (not necessarily near-standard), allowing the proof to be carried out algebraically. This is the case, for example, of the proofs of von Neumann's Mean Ergodic Theorem and Stone's Theorem on 1-parameter unitary groups (in the case of continuous periodic dynamics) : in both cases, the limit of a sum of standard maps is replaced by composition with the (not near-standard) counit of a Frobenius algebra, so that the proof can be carried out algebraically.

Despite the remarks above, one should not necessarily discount *Hilb as just being a category of handy mathematical tricks: a number of objects of concrete interest in the everyday practice of quantum mechanics (such as the position/momentum observables and eigenstates) are native to that richer environment, and help confer it its own independent dignity. Of course, the existence of multiple inequivalent choices of infinite natural dimension raises concerns with the physical interpretation of these non-standard objects, but Lemma 3.60 guarantees an essential equivalence of different choices of infinite natural dimension ω from the point of view of standard quantum theory. The same limiting objects (e.g. Diract deltas or plane-waves) for different choices of ω should effectively be treated as incarnations of the same conceptual objects corresponding to different choices of "infinite cutoff". This point of view is more evident in the recent work of [GG17].

3.5.4 Infinite-dimensional categorical quantum mechanics

The main motivation behind our use of non-standard analysis comes from the work of [AH12a] on commutative $H^\star$-algebras, a particular class of non-unital special commutative †-Frobenius algebras[31] (non-unital †-SCFAs, in short). It is an established result that approximate units for the algebras exist in separable Hilbert spaces: we will show that, in our non-standard framework, they can be made truly unital.

Theorem 3.61 (From [AH12a])**.** *A non-unital †-SCFA* ( ,) *on an object V of* sHilb *is an $H^\star$-algebra if and only if it corresponds to an orthonormal basis $|e_n\rangle_{n\in\mathbb{N}^+}$ of V such that*  $\circ\, |e_n\rangle = |e_n\rangle|e_n\rangle$*.*

Theorem 3.62 (From [AH12a, Amb45])**.** *A non-unital †-SCFA* ( ,) *on an object V of* sHilb *is an $H^\star$-algebra if and only if there is a sequence $|E_n\rangle_{n\in\mathbb{N}^+}$ such that for all $|a\rangle : \mathbb{C} \to V$ we have:*

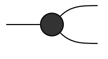
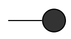
(i) $\circ\, (|E_n\rangle \otimes |a\rangle)$ *converges to $|a\rangle$;*

(ii) $(id_V \otimes \langle a|) \circ$ $\circ\, |E_n\rangle$ *converges.*

If this is so, then we can take $|E_n\rangle =: \sum_{n' \leq n} |e_{n'}\rangle$.

The sequence $|E_n\rangle_{n\in\mathbb{N}^+}$ itself doesn't converge in sHilb, because the state $\sum_{n\in\mathbb{N}^+} |e_n\rangle$ would have infinite norm. In our non-standard context, however, the state $\sum_{n=1}^{\kappa} |e_n\rangle$ is a well-defined, internal state for $\mathcal{H} = (V, |e_n\rangle_{n=1}^{\kappa})$. This opens the way to the definition of unital †-SCFAs on all objects of *Hilb.

Theorem 3.63. *Let $\mathcal{H} = (V, |e_n\rangle_{n=1}^{\kappa})$ be an object in* *Hilb*, and $|f_n\rangle_{n\in\mathbb{N}^+}$ be a standard orthonormal basis for V. Then the following comultiplication and counit define a* ***weakly unital****,* ***weakly special*** *commutative †-Frobenius algebra on $\mathcal{H}$ (i.e. one where the Unit and Speciality laws hold only up to $\sim$):*

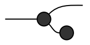
 $$:= \sum_{n=1}^{\kappa} |f_n\rangle \otimes |f_n\rangle \langle f_n|$$  $$:= \sum_{n=1}^{\kappa} \langle f_n| \qquad (3.169)$$

We refer to it as the ***classical structure***[32] *for $|f_n\rangle_n$. When $|f_n\rangle_n$ is the* ***chosen orthonormal basis*** *$|e_n\rangle_n$ for $\mathcal{H}$, the algebra is strictly unital and strictly special, i.e. a unital †-SCFA.*

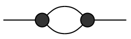
[31] In [AH12a], non-unital special commutative †-Frobenius algebras are simply referred to as *Frobenius algebras*. We refer to them in full as special commutative †-Frobenius algebras, and we will specify *non-unital* or *unital* explicitly.

[32] The terminology *classical structure*, in the context of *Hilb, will refer to weakly unital, weakly special, commutative †-Frobenius algebras. This is in accordance with the weak functoriality of lift_ω seen in the previous section.

Proof. Associativity and Frobenius laws hold with strict equalities (not up to $\sim$, despite involving composition of standard bounded linear maps), exactly as shown in [AH12a]. Commutativity also holds with strict equality. The only things left to check are a Unit law and the Speciality law.



$$= (id_{\mathcal{H}} \otimes \sum_{m=1}^{\kappa} \langle f_m |) \cdot \sum_{n=1}^{\kappa} |f_n\rangle \otimes |f_n\rangle \; \langle f_n|$$
$$\sim \sum_{m=1}^{\kappa} \sum_{n=1}^{\kappa} |f_n\rangle\langle f_m|f_n\rangle\langle f_n| = \sum_{n=1}^{\kappa} |f_n\rangle\langle f_n| \sim id_{\mathcal{H}} \qquad (3.170)$$

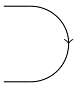


$$= (\sum_{m=1}^{\kappa} |f_m\rangle \; \langle f_m| \otimes \langle f_m|) \cdot (\sum_{n=1}^{\kappa} |f_n\rangle|f_n\rangle\langle f_n|)$$
$$\sim \sum_{m=1}^{\kappa} \sum_{n=1}^{\kappa} |f_m\rangle\langle f_m|f_n\rangle^2\langle f_n| = \sum_{n=1}^{\kappa} |f_n\rangle\langle f_n| \sim id_{\mathcal{H}} \qquad (3.171)$$

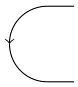
Finally, if $|f_n\rangle_n$ is the chosen orthonormal basis $|e_n\rangle_n$ for $\mathcal{H}$, then the $\sim$ in the previous equations are in fact $=$, and the classical structure is a strictly unital, strictly special commutative †-Frobenius algebra[33]. □

In fact, it is not hard to show that *Hilb is a dagger compact category.

Theorem 3.64. *The category* *Hilb *is compact closed. The* ***dual*** *of an object* $\mathcal{H} = (V, |e_n\rangle_{n=1}^{\kappa})$ *is defined by* $\mathcal{H}^* := (V^*, |\xi_n\rangle_{n=1}^{\kappa})$*, where* $|\xi_n\rangle$ *is the adjoint of* $|e_n\rangle$ *seen as a state of* V^**. The* ***cap*** *and* ***cup*** *on* $\mathcal{H}$ *are defined as follows:*



$$:= \sum_{n=1}^{\kappa} \langle e_n| \otimes \langle \xi_n|$$



$$:= \sum_{n=1}^{\kappa} |\xi_n\rangle \otimes |e_n\rangle \qquad (3.172)$$

More in general, any classical structure in *Hilb *can be used to define a* ***(weak) symmetric cap*** *and a* ***(weak) symmetric cup****, satisfying (weak)*[34] *yanking equations.*

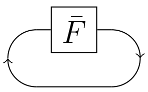
Proof. Weak yanking equations follow from the Frobenius law and weak Unit laws of any classical structure in *Hilb. When the classical structure is that of the chosen orthonormal basis, the strict Unit laws result in strict yanking equations, yielding legitimate cups and caps (again because of the exact resolution of the identity into $id_{\mathcal{H}} = \sum_{n=1}^{\kappa} |f_n\rangle\langle f_n|$). □

[33] The $\sim$ become $=$ because the identity takes the exact form $id_{\mathcal{H}} = \sum_{n=1}^{\kappa} |f_n\rangle\langle f_n|$, rather than the approximate form $id_{\mathcal{H}} \sim \sum_{n=1}^{\kappa} |f_n\rangle\langle f_n|$, when $|f_n\rangle_{n=1}^{\kappa}$ is the chosen ort'l basis.

[34] By a **weak** equation we will henceforth mean one which is satisfied only up to $\sim$.

The compact closed structure gives rise to a **trace** in the usual way:

$$\mathrm{Tr}\ \bar{F} \quad = \quad$$



$$= \quad \sum_{n=1}^{\kappa} \bar{F}_{nn} \tag{3.173}$$

In particular, we see that the notation $\dim \mathcal{H} := \kappa$ for $\mathcal{H} = (V, |e_n\rangle_{n=1}^{\kappa})$ was well chosen: $\mathrm{Tr}\ id_{\mathcal{H}} = \sum_{n=1}^{\kappa} 1 = \kappa = \dim \mathcal{H}$. The trace can also be used to endow the homset $\mathrm{Hom}_{^\star\mathrm{Hilb}}\left[\mathcal{H}, \mathcal{G}\right]$, which we have already seen to be a ${}^\star\mathbb{C}$-vector space, with the following ${}^\star\mathbb{C}$-valued **Hilbert-Schmidt inner product**:

$$\left(\bar{G}, \bar{F}\right) := \mathrm{Tr}\ \bar{G}^\dagger \bar{F} = \sum_{m=1}^{\dim \mathcal{G}} \sum_{n=1}^{\dim \mathcal{H}} \bar{G}^\star_{mn} \bar{F}_{mn}. \tag{3.174}$$

This is exactly the inner product that one would get by enriching the category *Hilb in itself via compact closure.

3.5.5 Wavefunctions with periodic boundaries

As a sample application of the structures presented above, we cover the theory of wavefunctions on a 1-dimensional space with periodic boundary conditions: these live in $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})] \cong \mathrm{L}^2[S^1]$, where L is the length of the underlying space. The **momentum eigenstates**, or **plane-waves**, form a countable orthogonal basis for $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$, indexed by $n \in \mathbb{Z}$ (in this section, n, m, k, h will range over integers):

$$\chi_n := x \mapsto e^{-i(2\pi/L)nx}. \tag{3.175}$$

The plane-wave $|\chi_n\rangle$ is the eigenstate of momentum $n\hbar$. Let $\theta(n) := |2n| + \frac{1-\mathrm{sign}(n)}{2}$ (with $\mathrm{sign}(0) := -1$) be a bijection $\mathbb{Z} \to \mathbb{N}^+$. We can obtain a countable orthonormal basis $|e_l\rangle_{l \in \mathbb{N}^+}$ for $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$ as follows:

$$|e_{\theta(n)}\rangle := \frac{1}{\sqrt{L}} |\chi_n\rangle \text{ for all } n \in \mathbb{Z}. \tag{3.176}$$

Now we shift our attention to the object $(\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})], |e_l\rangle_{l=1}^{\kappa})$ of *Hilb, with $\kappa = 2\omega + 1$ some odd infinite natural[35]. As a shorthand for $\sum_{l=1}^{\kappa} |\chi_{\theta^{-1}(l)}\rangle$, and other cases where the index is bijected to the integers, we will simply re-index over the non-standard integers $\{-\omega, ..., +\omega\}$ (such as in $\sum_{n=-\omega}^{+\omega} |\chi_n\rangle$). In particular, we will write our chosen object as $(\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})], \frac{1}{\sqrt{L}} |\chi_n\rangle_{n=-\omega}^{+\omega})$, or simply $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$ when no confusion can

[35] The notions of oddness and evenness extend from $\mathbb{N}$ to ${}^\star\mathbb{N}$ by the transfer theorem, and by saying that some infinite non-standard natural $\kappa \in {}^\star\mathbb{N}$ is odd we mean exactly that $\kappa = 2\omega + 1$ for some (necessarily infinite) non-standard natural $\omega \in {}^\star\mathbb{N}$. Note that the infinite natural ω here has nothing to do with the ordinal ω from set theory.

arise. Now that we established the role of momentum eigenstates in our framework, it is time to turn our attention to position eigenstates. On a continuous space, position eigenstates are given by Dirac delta functions, and as a consequence are not associated with well-defined standard vectors. Here, we will define them in terms of the basis of momentum eigenstates, and then show that they coincide with their more traditional formulation in terms of Dirac deltas. Let $x_0 \in {}^\star\big(\mathbb{R}/(L\mathbb{Z})\big)$ be a point of the underlying space, then we define the **position eigenstate** at x_0 to be the following non-standard state:

$$|\delta_{x_0}\rangle := \frac{1}{\sqrt{L}} \sum_{n=-\omega}^{+\omega} \chi_n(x_0)^* \frac{1}{\sqrt{L}} |\chi_n\rangle. \tag{3.177}$$

Theorem 3.65. *The position eigenstates are weakly orthogonal at standard points. Furthermore, they behave as* ***Dirac deltas****, i.e. they satisfy $\langle \delta_{x_0}|f\rangle \simeq f(0)$ for all standard smooth $f \in \mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$ and all standard points $x_0 \in \mathbb{R}/(L\mathbb{Z})$. The position eigenstates are also unbiased with respect to the momentum eigenstates, in the sense that $|\langle \delta_{x_0}|\chi_n\rangle| = 1$ independently of n or x_0.*

Proof. The proof that the state $|\delta_{x_0}\rangle$ satisfies $\langle \delta_{x_0}|f\rangle \simeq f(0)$ for all standard smooth $f \in \mathrm{L}^2[\mathbb{R}/L\mathbb{Z}]$ hinges on the transfer theorem, together with the following standard result from Fourier theory:

$$\frac{1}{\sqrt{L}} \sum_{n=-N}^{N} e^{-i(2\pi/L)x_0 n} \frac{1}{\sqrt{L}} \langle \chi_n|f\rangle = \frac{1}{L} \int_{\mathbb{R}/L\mathbb{Z}} \Big(\sum_{n=-N}^{N} e^{i(2\pi/L)(x-x_0)n} \Big) f(x) dx \overset{N\to\infty}{\longrightarrow} f(x_0). \tag{3.178}$$

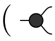
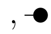
To show orthogonality, we repeat the reasoning above in the special case of $|f\rangle := \sum_{m=-M}^{M} \big(\frac{1}{L} e^{i(2\pi/L)x_1 m}\big)|\chi_m\rangle$, for some $x_1 \neq x_0$. Two limits and two applications of the transfer theorem yield the desired result (we cannot do $\langle \delta_{x_0}|\delta_{x_1}\rangle \simeq 0$ directly because $|\delta_{x_1}\rangle$ is not a standard smooth function):

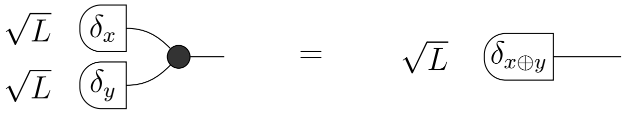
$$\begin{aligned} &\frac{1}{\sqrt{L}} \sum_{n=-N}^{N} \frac{1}{\sqrt{L}} \sum_{m=-M}^{M} \big(e^{-i(2\pi/L)x_0 n} \frac{1}{\sqrt{L}}\big) \langle \chi_n|\chi_m\rangle \big(e^{i(2\pi/L)x_1 m} \frac{1}{\sqrt{L}}\big) = \\ =&\frac{1}{L^2} \int_{\mathbb{R}/L\mathbb{Z}} \Big(\sum_{n=-N}^{N} \sum_{m=-M}^{M} e^{i(2\pi/L)\big((x-x_0)n+(x-x_1)m\big)} \Big) dx \overset{N,M\to\infty}{\longrightarrow} 0. \end{aligned} \tag{3.179}$$

Finally, the position eigenstates are clearly unbiased for the momentum eigenstates: by the first part of this proof, any given position eigenstate $|\delta_{x_0}\rangle$ satisfies $|\langle \delta_{x_0}|\chi_n\rangle|^2 \simeq 1$ for all momentum eigenstates $|\chi_n\rangle$, independently of n. □

In the first part of this Chapter, we have defined coherent groups starting from the position observable ○ and translation symmetry, and we have proven that ● is the momentum observable. In this Section, we will take the opposite approach: we will start from the momentum observable ● given by the plane-waves, then define the boost symmetry on momentum eigenstates, and finally prove that there is a corresponding position observable ○ given by the Dirac deltas defined above (strongly complementary to the momentum observable).

We begin by showing explicitly that momenta generate the translation action of ${}^{\star}\big(\mathbb{R}/(L\mathbb{Z})\big)$ on the Dirac deltas.

Theorem 3.66. *Let (*  *,*  *,* *,* *) be the classical structure for the chosen orthonormal basis of normalised momentum eigenstates. Then the monoid (* *,* *) endows the set* $\Big\{\sqrt{L}|\delta_x\rangle \;\Big|\; x \in {}^{\star}\big(\mathbb{R}/(L\mathbb{Z})\big)\Big\}$ *of position eigenstates with the abelian group structure of position-space translation* $\Big({}^{\star}\big(\mathbb{R}/(L\mathbb{Z})\big), \oplus, 0\Big)$*:*



(3.180)

This can be equivalently written in the following form:

$$|\delta_{x\oplus y}\rangle = \Big[\frac{1}{\sqrt{L}^2}\sum_{n=-\omega}^{+\omega} \chi_n(x)^*|\chi_n\rangle\langle\chi_n|\Big]|\delta_y\rangle, \tag{3.181}$$

Note that $\chi_n(x)^* = \langle\chi_n|\delta_x\rangle$ *is nothing but* $\exp[i\frac{xp}{\hbar}]$ *for a given (quantised) momentum eigenvalue* $p = (n\hbar)/L$ *and corresponding momentum eigenstate* $|\chi_n\rangle$*.*

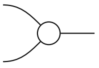
Proof. Using the definition of the classical structure for momentum eigenstates, together with the definition of the position eigenstates, we obtain the desired equalities:

$$\begin{aligned} \circ\,(\sqrt{L}|\delta_x\rangle\sqrt{L}|\delta_y\rangle) &= \Big[\frac{1}{\sqrt{L}^3}\sum_{n=-\omega}^{+\omega} |\chi_n\rangle\langle\chi_n|\langle\chi_n|\Big]\sqrt{L}|\delta_x\rangle\sqrt{L}|\delta_y\rangle \\ &= \Big[\frac{1}{\sqrt{L}^2}\sum_{n=-\omega}^{+\omega} \chi_n(x)^*|\chi_n\rangle\langle\chi_n|\Big]\sqrt{L}|\delta_y\rangle \\ &= \frac{1}{\sqrt{L}}\sum_{n=-\omega}^{+\omega} \chi_n(x)^*\chi_n(y)^*|\chi_n\rangle \\ &= \frac{1}{\sqrt{L}}\sum_{n=-\omega}^{+\omega} \chi_n(x\oplus y)^*|\chi_n\rangle = \sqrt{L}|\delta_{x\oplus y}\rangle. \end{aligned} \tag{3.182}$$

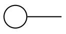
□

While the momentum observable is embedded in our very definition of the object $\left(\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})], |e_l\rangle_{l=1}^{\kappa}\right)$, the definition of a position observable is not as straightforward, because the position eigenstates don't form a *countable* orthonormal basis. Instead of defining the observable directly, we appeal to our understanding of symmetry-observable duality in coherent groups: we first define the boost symmetry $(K(\bullet)$, ,) on momentum eigestates, and only then we show that it is a unital †-qSCFA behaving as expected from the position observable.

Consider the binary function $a \oplus b := a + b \pmod{2N+1}$, where representatives for the $2N+1$ remainder classes are chosen in the set $\{-N, ..., +N\}$: for every N, this function is defined in the standard theory of $\mathbb{Z}$, and endows $\{-N, ..., +N\}$ with the group structure of $\mathbb{Z}_{2N+1}$. By transfer theorem, a similar group operation exists on the internal set $\{-\omega, ..., +\omega\}$ of $^\star\mathbb{Z}$, endowing it with the group structure of $^\star\mathbb{Z}_{2\omega+1}$. Remarkably, for any two finite integers $n, m \in \mathbb{Z}$ we have $n \oplus m = n + m$ (because $n, m < \omega$ implies $n + m < \omega$, so no modular reduction occurs). Now consider the following morphisms of *Hilb:

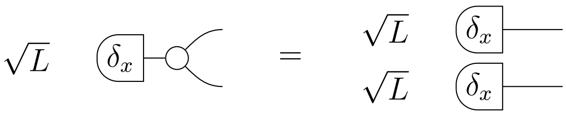


$$:= \quad \frac{1}{\sqrt{L}^3} \sum_{n=-\omega}^{+\omega} \sum_{m=-\omega}^{+\omega} |\chi_{n\oplus m}\rangle \langle\chi_n| \otimes \langle\chi_m| \tag{3.183}$$

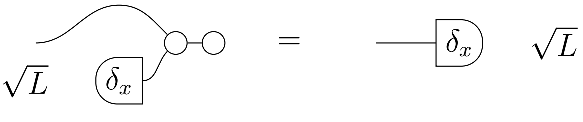


$$:= \quad \frac{1}{\sqrt{L}}|\chi_0\rangle$$

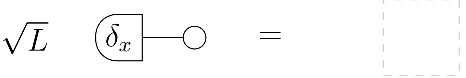
Theorem 3.67. (, , ,) *is a unital commutative †-Frobenius algebra, the* ***group algebra*** *of* $^\star\mathbb{Z}_{2\omega+1}$*. It is quasi-special, with normalisation factor* $N_{\bigcirc} = (2\omega+1)$*. Furthermore, it coherently copies, adjoins and deletes the (rescaled) position eigenstates, as long as the position* x *takes the form* $x = j\frac{L}{2\omega+1} \in \mathrm{st}(\mathbb{R}/(L\mathbb{Z}))$ *for some* $j \in {}^\star\mathbb{Z}_{2\omega+1}$ *(i.e. we have that* $x \in \frac{L}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$*)*[36]*:*



(3.184)



(3.185)



(3.186)

As a consequence, we will also refer to it as the ***classical structure for position eigenstates****, or as the* ***position observable****.*

[36] Note the very interesting duality which emerges between the large-scale cutoff on the momentum k (which has magnitude bounded above by ω) and the small-scale cutoff on the position x (which must be an integer multiple of $\frac{L}{2\omega+1}$).

Proof. Commutative, Associative and Unit laws can be proven on the monoid using the corresponding laws for $(\oplus, 0)$. Frobenius law follows from the following re-indexing, with $k' := k \oplus n$:

$$\begin{aligned}(\succ\!\!- \otimes id) \circ (id \otimes -\!\!\prec) &= \frac{1}{\sqrt{L}^4} \sum_{n=-\omega}^{+\omega} \sum_{m=-\omega}^{+\omega} \Big[\sum_{k \oplus h = m} |\chi_{n\oplus k}\rangle \otimes |\chi_h\rangle \, \langle \chi_n| \otimes \langle \chi_m| \Big] = \\ &= \frac{1}{\sqrt{L}^4} \sum_{n=-\omega}^{+\omega} \sum_{m=-\omega}^{+\omega} \Big[\sum_{k' \oplus h = n \oplus m} |\chi_{k'}\rangle \otimes |\chi_h\rangle \, \langle \chi_n| \otimes \langle \chi_m| \Big] \\ &= -\!\!\prec \circ \succ\!\!- \end{aligned} \tag{3.187}$$

The algebra is obviously a group algebra, and hence it is quasi-special with normalisation factor $(2\omega + 1)$. The fact that position eigenstates are copied is a straightforward check, with a re-indexing $n' := n \ominus k$ in the second-to-last step:

$$\begin{aligned} -\!\!\prec \circ \big(\sqrt{L}|\delta_x\rangle\big) &= \frac{1}{\sqrt{L}^2} \sum_{n=-\omega}^{+\omega} \sum_{k=-\omega}^{+\omega} |\chi_k\rangle \otimes |\chi_{n\ominus k}\rangle \, \langle \chi_n | \delta_x\rangle = \\ &= \frac{1}{\sqrt{L}^2} \sum_{n=-\omega}^{+\omega} \sum_{k=-\omega}^{+\omega} |\chi_k\rangle \otimes |\chi_{n\ominus k}\rangle \, \chi_n(x)^* = \\ &= \frac{1}{\sqrt{L}^2} \sum_{n=-\omega}^{+\omega} \sum_{k=-\omega}^{+\omega} |\chi_k\rangle \otimes |\chi_{n\ominus k}\rangle \, \chi_k(x)^* \chi_{n\ominus k}(x)^* e^{i2\pi \frac{2\omega+1}{L} sx} = \\ &= \Big[\frac{1}{\sqrt{L}} \sum_{n'=-\omega}^{+\omega} \chi_{n'}(x)^* |\chi_{n'}\rangle\Big] \otimes \Big[\frac{1}{\sqrt{L}} \sum_{k=-\omega}^{+\omega} \chi_k(x)^* |\chi_k\rangle\Big] = \\ &= \sqrt{L}|\delta_x\rangle \otimes \sqrt{L}|\delta_x\rangle. \end{aligned} \tag{3.188}$$

In the third line, the extra phase $e^{i2\pi \frac{2\omega+1}{L} s_{n,k} x}$ appears because χ_n is a character of $\mathbb{Z}$, not of ${}^\star\mathbb{Z}_{2\omega+1}$: the value of $s_{n,k} \in \{-1, 0, +1\}$ keeps track of whether some modular reduction was necessary to go from $k \oplus (n \ominus k)$ to n. It is cancelled out if and only if we require x to be in the form $x = j\frac{L}{2\omega+1}$, for some $j \in {}^\star\mathbb{Z}_{2\omega+1}$: hence a duality between the large-scale cutoff of momentum and the small-scale cutoff of position arises as a consequence of a purely algebraic requirement in the non-standard framework. The adjoint and delete conditions have proofs that go along similar lines. □

Remark 3.68. *Because the position eigenstates act as Dirac deltas on the smooth standard functions, the delete condition above means that the rescaled counit* $\sqrt{L}$–○ *defines the* ***integral operator****:* $\sqrt{L}$–○ $= |\bar{f}\rangle \mapsto \int_{\mathbb{R}/(L\mathbb{Z})} f(x)dx$*. Furthermore, the position eigenstates are actually orthogonal (and not only for standard points): this is because they are the classical states of a quasi-special commutative †-Frobenius algebra in a SMC with scalars forming a field [CPV13].*

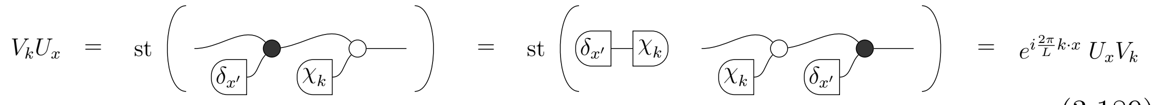
Theorem 3.69. *The position and momentum observables defined above form a doubly well-pointed coherent group* $(\circ, \bullet)$*.*

Proof. We begin by observing that both ● and ○ have enough classical states: the †-SCFA ● has enough classical states by construction, while the †-qSCFA ○ can be seen to have enough classical states because the position eigenstates are enough to distinguish all momentum eigenstates. Then the laws of complementarity and strong complementarity follow immediately from the fact that: (i) the momentum and position eigenstates are mutually unbiased (by Theorem 3.65), (ii) the momentum eigenstates form group under (>○- , ○-) (by the very definition of the group algebra for ${}^{\star}\mathbb{Z}_{2\omega+1}$), and (iii) position eigenstates form group under (>●- , ●-) (by Thm 3.66). □

Corollary 3.70 (Weyl CCRs).
For all $x \in \mathbb{R}/(L\mathbb{Z})$*, let* U_x *be the unitary on* $\mathrm{L}^2[\mathbb{R}/(L\mathbb{Z})]$ *corresponding to space-translation of wavefunctions (with periodic boundary conditions) by* x*. For all* $k \in \mathbb{Z}$*, let* V_k *be the unitary corresponding to momentum-boost by* $k\hbar$*. Then the following braiding relations hold between the two unitaries:*

$$V_k U_x = e^{i\frac{2\pi}{L}k\cdot x}\, U_x V_k$$

Proof. The proof is a straightforward consequences of Theorems 3.24 and 3.69, and exemplifies an application of tools from *Hilb to obtain a simple algebraic proof of an iconic result of standard quantum mechanics. Indeed, if $x' := j\frac{L}{2\omega+1} \in {}^{\star}\mathbb{R}/(L\mathbb{Z})$ is any near-standard point such that $x' \simeq x$, then the following holds:



(3.189)

□

Remark 3.71. *The methods presented here can be extended to the case of wavefunctions on spaces with a compact or discrete abelian group of translations (such as tori or lattices). A further extension is possible to certain locally compact groups, such as* $(\mathbb{R}, +, 0)$*, albeit requiring some additional finesse. These developments are detailed in the recent [GG17].*

3.6 Quantum dynamics

3.6.1 A traditional perspective on quantum dynamics

In the traditional formulation of quantum mechanics, a quantum dynamical system is a quantum system $\mathcal{H}$ equipped with a prescribed Hamiltonian $\mathbf{H}$. By Stone's Theorem, this is the same as saying that it is a quantum system equipped with a 1-parameter unitary group $(U_t)_{t \in \mathbb{R}}$: as such, dynamics can be treated as a special case of symmetry, where the symmetry group is chosen to be $(\mathbb{R}, +, 0)$.

More general kinds of dynamics can be studied by considering different symmetry groups. The ones generally deemed of interest in physics and computer science are:

(i) **continuous** dynamics, corresponding to symmetry group $(\mathbb{R}, +, 0)$;

(ii) **continuous periodic** dynamics, corresponding to symmetry group $(\mathbb{R}/(T\mathbb{Z}), \oplus, 0)$;

(iii) **discrete** dynamics, corresponding to symmetry group $(\mathbb{Z}, +, 0)$;

(iv) **discrete periodic** dynamics, corresponding to symmetry group $(\mathbb{Z}_T, \oplus, 0)$.

In this opening Subsection, we will briefly recap the basics of all four notions of dynamics in the traditional formulation of finite-dimensional quantum theory: when making general statements about all four notions, we will used $(G, \oplus, 0)$ to denote the generic time-translation symmetry group.

3.6.1.1 Quantum dynamical systems

A quantum dynamical system is a finite-dimensional Hilbert space $\mathcal{H}$ endowed with a unitary representation $(U_t)_{t \in G}$ of the time-translation symmetry group $(G, \oplus, 0)$, where $(U_t)_{t \in G}$ is a strongly continuous family (a condition which is trivially satisfied in the case of discrete dynamics). As mentioned above and discussed in further detail below, this perspective is entirely equivalent to the perspective involving Hamiltonians and Schrödinger's equation.

When talking about the dynamics of a system $\mathcal{H}$, we are often interested in the evolution of an initial state ψ_0 under time-translation. Classically, we can look at the trajectory of ψ_0 in $\mathcal{H}$ as the function $\Psi : G \rightarrow \mathcal{H}$ which traces the history of the initial state as it evolves in time, i.e. the one defined by $\Phi := t \mapsto U_t|\psi_0\rangle$.

The classical trajectory of ψ_0 under $\mathbb{Z}_T$ is not just a function $\mathbb{Z}_T \rightarrow \mathcal{H}$: it is an equivariant function, by which we mean that $U_{\delta t}\Phi(t) = \Phi(t + \delta t)$, and hence it is a structurally sound way of seeing the time-translation symmetry group (a dynamical system itself, under the regular action) into the dynamical system $\mathcal{H}$.

3.6.1.2 Hamiltonian and energy measurement

In the continuous case, the Hamiltonian is the unique self-adjoint operator, given by Stone's Theorem on 1-parameter unitary groups, such that $U_t = e^{-i\frac{\mathbf{H}}{\hbar}t}$. In the previous Chapter, we have discussed a number of issues with the identification of quantum mechanical observables with self-adjoint operators: as a consequence, we will instead take the Hamiltonian to be a PVM (Projector-Valued Measure) $\big(\pi(\chi)\big)_{\chi \in \mathbb{R}^\wedge}$, or equivalently a PVM $\big(\pi(E)\big)_{E \in \mathbb{R}}$, where we have fixed an isomorphism $\mathbb{R}^\wedge \cong \mathbb{R}$ (by choosing a constant $\hbar$). Stone's Theorem in its PVM version takes the following form:

$$U_t = \int_{\mathbb{R}^\wedge} \chi(t) d\pi(\chi) = \int_{\mathbb{R}} e^{-i\frac{E}{\hbar}t} d\pi(E) \tag{3.190}$$

The PVM $(\pi(E))_{E\in\mathbb{R}}$ itself specifies the energy measurement for the system: if the quantum system is in state ρ (pure or mixed) and $S \subseteq \mathbb{R}$ is any measurable subset, then the probability of an energy measurement resulting in an outcome in S is given by $\operatorname{Tr} \pi(S)\rho$ (where $\pi(S)$ is the projector on the subspace of pure states spanned by the energy eigenstates $|\psi_E\rangle$ with $E \in S$, as specified by the PVM).

Once we let go of the self-adjoint operator point of view on the Hamiltonian, all four cases of dynamics enumerated in the introduction to this Section can be tackled uniformly. The Hamiltonian is always PVM $\big(\pi(\chi)\big)_{\chi \in G^\wedge}$: for the continuous case, $G \cong \mathbb{R}$ and $G^\wedge \cong \mathbb{R}$; for the continuous periodic case, $G \cong \mathbb{R}/(T\mathbb{Z})$ and $G^\wedge \cong \mathbb{Z}$; for the discrete case, $G \cong \mathbb{Z}$ and $G^\wedge \cong \mathbb{R}/\mathbb{Z}$; for the discrete periodic case, $G \cong \mathbb{Z}_T$ and $G^\wedge \cong \mathbb{Z}_T$. The PVM version of Stone's Theorem takes the same form for all four cases (in the periodic cases we can think of $E = nh$):

$$U_t = \int_{\mathbb{R}^\wedge} \chi(t) d\pi(\chi) = \int_{\mathbb{R}} e^{-i2\pi\frac{Et}{h}} d\pi(E) \text{ for all } t \in \mathbb{R} \tag{3.191}$$

$$U_t = \int_{(\mathbb{R}/(T\mathbb{Z}))^\wedge} \chi(t) d\pi(\chi) = \sum_{n\in\mathbb{Z}} e^{-i2\pi\frac{nt}{T}} \pi(n) \text{ for all } t \in \mathbb{R}/(T\mathbb{Z}) \tag{3.192}$$

$$U_t = \int_{\mathbb{Z}^\wedge} \chi(t) d\pi(\chi) = \int_{\mathbb{R}/\mathbb{Z}} e^{-i2\pi\frac{Et}{h}} d\pi(E) \text{ for all } t \in \mathbb{Z} \tag{3.193}$$

$$U_t = \int_{\mathbb{Z}_T^\wedge} \chi(t) d\pi(\chi) = \sum_{n\in\mathbb{Z}_T} e^{-i2\pi\frac{nt}{T}} \pi(n) \text{ for all } t \in \mathbb{Z}_T \tag{3.194}$$

The energy measurements can similarly be expressed in the same form for all four cases (the top expression is for the two continuous cases[37], while the bottom expression

[37] There are some (weak) caveats on the PVM in order for the integral expression to apply.

applies to the two discrete cases, where again we think of $E = nh$):

$$\mathbb{P}[E \in S|\rho] = \mathrm{Tr}\, \pi(S)\rho \overset{*}{=} \int_S \mathrm{Tr}\, [\pi'(E)\rho] dE \tag{3.195}$$

$$\mathbb{P}[n \in S|\rho] = \mathrm{Tr}\, \pi(S)\rho = \sum_{n \in S} \mathrm{Tr}\ \pi(n)\rho \tag{3.196}$$

3.6.1.3 Schrödinger's Equation

In its traditional formulation for continuous quantum dynamics, the **time-independent Schrödinger Equation** for an energy eigenstate $|\psi_E\rangle$ of a quantum dynamical system can be written as follows, where $\mathbf{H}$ is the traditional Hamiltonian observable (the self-adjoint operator given by Stone's Theorem) and $|\psi_E\rangle$ is an energy eigenstate for energy level $E \in \mathbb{R}$:

$$\mathbf{H}|\psi_E\rangle = E|\psi_E\rangle \tag{3.197}$$

The full **Schrödinger Equation** takes the following differential form:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = \mathbf{H}|\psi(t)\rangle \tag{3.198}$$

Because we do not want to work with self-adjoint operators and differentiation, we instead consider the following, equivalent formulation of Equations 3.197 and 3.198, known as the **exponentiated Schrödinger Equation** (here $h = 2\pi\hbar$):

$$U_t|\psi_E\rangle = e^{-i2\pi\frac{Et}{h}}|\psi_E\rangle \tag{3.199}$$

To a practising physicist, the exponentiated formulation may feel further from the spirit of dynamics than the traditional formulation, because it replaces instantaneous states and differential evolution with a global, non-differential description in terms of a 1-parameter unitary group. In this work, however, we choose to adopt a more holistic point of view: the two equations are after all mathematically equivalent, and preferring one formulation over the other depends on the specific application and on the mathematical tools available to solve the equation itself. Because this work is concerned with the study of dynamics as a symmetry, and not with the solution of the equations of motion for some specific dynamical system, the exponentiated formulation in terms of 1-parameter unitary groups will be the undisputed favourite.

Aside from conceptual stances, the exponentiated version of Schrödinger Equation has another, clear-cut advantage over the differential one when it comes to this work: it has a direct translation to those dynamical systems, such as the discrete periodic ones that will occupy large parts of this section, which don't admit infinitesimal generators for their dynamics. Below we write the exponentiated Schrödinger Equation for all four cases of dynamics considered in the introduction to this Section:

$$U_t|\psi_\chi\rangle = \chi(t)|\psi_\chi\rangle = e^{-i2\pi\frac{Et}{h}}|\psi_\chi\rangle \text{ for all } \chi \in \mathbb{R}^\wedge \leftrightarrow E/h \in \mathbb{R} \tag{3.200}$$

$$U_t|\psi_\chi\rangle = \chi(t)|\psi_\chi\rangle = e^{-i2\pi\frac{nt}{T}}|\psi_\chi\rangle \text{ for all } \chi \in (\mathbb{R}/(T\mathbb{Z}))^\wedge \leftrightarrow n = E/h \in \mathbb{Z} \tag{3.201}$$

$$U_t|\psi_\chi\rangle = \chi(t)|\psi_\chi\rangle = e^{-i2\pi\frac{Et}{h}Et}|\psi_\chi\rangle \text{ for all } \chi \in \mathbb{Z}^\wedge \leftrightarrow E/h \in \mathbb{R}/\mathbb{Z} \tag{3.202}$$

$$U_t|\psi_\chi\rangle = \chi(t)|\psi_\chi\rangle = e^{-i2\pi\frac{nt}{T}}|\psi_\chi\rangle \text{ for all } \chi \in \mathbb{Z}_T^\wedge \leftrightarrow n \in \mathbb{Z}_T \tag{3.203}$$

In all four cases, we have explicitly fixed a correspondence between the canonical energy levels $\chi \in G^\wedge$ and non-canonical values of more direct physical significance.

3.6.1.4 von Neumann's mean ergodic theorem

von Neumann's Mean Ergodic Theorem is a cornerstone result in quantum dynamics, and its generalisation provides a statement which is dual, in a very specific sense, to the PVM formulation of Stone's Theorem for discrete dynamics.

Theorem 3.72 (**von Neumann's Mean Ergodic Theorem (discrete)** [vN32b]**).**

Let $U : \mathcal{H} \to \mathcal{H}$ be a unitary operator on a Hilbert space $\mathcal{H}$, and let $(U_t)_{t\in\mathbb{Z}}$ be the discrete dynamics it generates, i.e. $U_t := U^t$. Let $P : \mathcal{H} \to \mathcal{H}$ be the orthogonal projector on the invariant subspace for U, i.e. the subspace given by those vectors $|\phi\rangle$ such that $U|\phi\rangle = |\phi\rangle$. Then the following limit holds in the strong operator topology:

$$\lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U_t = P_1 \tag{3.204}$$

Corollary 3.73. *Let $U : \mathcal{H} \to \mathcal{H}$ be a unitary operator on a Hilbert space $\mathcal{H}$, and let $(U_t)_{t\in\mathbb{Z}}$ be the discrete dynamics it generates, i.e. $U_t := U^t$. For each $\chi \in \mathbb{Z}^\wedge$, write $P_\chi : \mathcal{H} \to \mathcal{H}$ be the orthogonal projector on the subspace given by those vectors $|\phi\rangle$ such that $U|\phi\rangle = \chi(1)|\phi\rangle$.*[38] *Then the following limit holds in the strong operator topology:*

$$\lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \chi(t)^* U_t = P_\chi \tag{3.205}$$

Proof. Apply Theorem 3.72 to $U' := \chi(1)^*U$, observing that $\chi(t) = \chi(1)^t$, and that the condition $U'|\psi\rangle = |\psi\rangle$ used in Theorem 3.72 is equivalent to the condition $U|\psi\rangle = \chi(1)|\psi\rangle$ used in this Corollary. □

[38] Note that the $\chi \in \mathbb{Z}^\wedge$ are exactly those in the form $\chi := t \mapsto \zeta^t$ for some complex phase ζ, so that the values $\chi(1)$ cover exactly all the possible eigenvalues for unitary operators.

From Corollary 3.73, we can see how von Neumann's Mean Ergodic Theorem is dual to Stone's Theorem on discrete dynamics. Stone's Theorem, in its PVM formulation for discrete dynamics, shows that unitary dynamics can be reconstructed by integrating the projectors of the Hamiltonian observable multiplied by phases given by the canonical energy spectrum; von Neumann's Theorem, in its generalised formulation, shows that the projectors of the Hamiltonian observable can be reconstructed by averaging the unitary dynamics across time, multiplied by phases given by the canonical energy spectrum. This suggests a somewhat different point of view on quantum dynamical ergodicity: rather than being about invariant measures and the coincidence of time and space averages, as is the case in classical dynamical systems, the ergodic theorem in quantum dynamical systems is a manifestation of symmetry-observable duality, proving how time-translation symmetry and the Hamiltonian observable can be reconstructed one from the other.

A generalised version of von Neumann's Mean Ergodic Theorem can be formulated for continuous dynamics [vN32b], continuous periodic dynamics and discrete periodic dynamics (as corollaries), and is summarised below.

Theorem 3.74 (**Generalised von Neumann's Mean Ergodic Theorem**). *Let $(G, \oplus, 0)$ be one of $(\mathbb{R}, +, 0)$, $(\mathbb{R}/(T\mathbb{R}), \oplus, 0)$, $(\mathbb{Z}, +, 0)$, or $(\mathbb{Z}_T, \oplus, 0)$. Let $(U_t)_{t\in G}$ be a unitary dynamic on a Hilbert space $\mathcal{H}$ (i.e. a strongly continuous 1-parameter unitary group). For all $\chi \in G^\wedge$, let $P_\chi : \mathcal{H} \to \mathcal{H}$ be the orthogonal projector on the invariant subspace for U, i.e. the subspace given by those vectors $|\phi\rangle$ such that $U_t|\phi\rangle = \chi(t)|\phi\rangle$. Then the following limit holds in the strong operator topology:*

$$\lim_{T\to\infty} \frac{1}{T} \int\limits_{t=0}^{T} \chi(t)^* U_t dt = P_\chi \tag{3.206}$$

It is immediately clear from Equation 3.206 that the four generalised versions of von Neumann's Theorem—for continuous, continuous periodic, discrete and discrete periodic dynamics, respectively—provide exact duals for the four versions of Stone's Theorem presented earlier on.

3.6.1.5 The issue with time observables

The problem of time observables is a long standing open problem in the philosophy of quantum theory. The history of time observables is turbulent, and extremely interesting: we will only mention some of the headlines in the coming paragraphs, and we refer the interested reader to [Hil05, Pas15, Rob12, But14].

Our story begins in 1926, when Dirac introduces time in quantum mechanics as a dynamical variable t, with associated "conjugate momentum" W satisfying the Kennard-Weyl form $tW - Wt = -i\hbar$ of the CCRs (technically, the conjugate momentum is $-W$). Heisenberg follows in 1927 with the time-energy uncertainty principle $Et - tE = -i\hbar$ (note the sign!) for Stern-Gerlach experiments, and Bohr proposes in 1928 the uncertainty relation $\Delta t \Delta E \geq h$ for wave-packets (although he talks of complementarity, rather than uncertainty relations). Both Dirac and Heisenberg later revise their position, and start treating t as a parameter.

The first real issues with the notion of time observable are raised by Schrödinger in 1931: he posits that a quantum time observable t would be measured by observing an ideal quantum clock, and concludes that the resulting state of the system would be "physically meaningless", as it would have completely uncertain energy. Pauli in 1933 makes this claim rigorous, in what would become known as "Pauli's Theorem"[39]. Using the Stone-von Neumann Theorem, one deduces that a time observable t and a Hamiltonian H satisfying the Weyl CCRs for the group $(\mathbb{R}, +, 0)$ would force H to have continuous, unbounded-below spectrum. Since this contradicts real-world observations, Pauli concludes time observables to be physically meaningless.

Putting together Schrödinger's remarks and Pauli's result, we immediately spot a problem: what they are measuring is the *clock* time observable and the *system* energy. Looking at a synchronised clock-system state, it is easy to see that the energy measurement on the system, obtained from the coherent Hamiltonian, always commutes with the clock time measurement. What *really* comes out of Schrödinger's and Pauli's arguments is an issue with the quantum clocks themselves, not with the quantum dynamical systems.

When you think a little more about what the clock does, however, things are not as ludicrous as they might seem. It is true that if you "freeze" the clock in a definite clock time state (by measuring it) you lose all information about the the clock energy. However, we have seen in the previous Subsection that the clock energy is only relevant for the dynamical systems governed by the quantum clock, not for the clock itself: if one wishes to see the clock as a dynamical system governed by some notion of time other than the one it is ticking itself, then the resulting Hamiltonian for the clock need not have anything to do with the clock energy observable. Indeed, this is exactly what happens when we try to apply Schrödinger's and Pauli's arguments to

[39] His remarks are not really a theorem: he originally used the Kennard-Weyl form of the CCR, while the Stone-von Neumann Theorem requires the Weyl form.

the quantum clocks themselves, and the physical absurdity stems from the incorrect identification between two different “energy” observables:

(i) the clock energy observable, which is only relevant for the quantum dynamical systems governed by the clock, and which becomes completely undetermined upon measurement in the clock time observable;

(ii) the physical Hamiltonian, which instead corresponds to seeing the quantum clock as a dynamical system governed by some other, larger clock, and which need not be affected at all by the measurement of the clock time observable.

It would be tempting to conclude the discussion above by positing the existence of some large, universal quantum clock ticking time (with time-translation group $\mathbb{R}$) for all quantum clocks, but attempts to consider such an object have so far fallen back into the usual routine: either (i) the clock is an accessible physical system, in which it also governs itself and has an unbounded below, physically meaningless Hamiltonian, or (ii) it is external to the theory, in which case time is an external parameter and we get to the same conclusion of Schrödinger, Pauli and many quantum physicists after them. In fact, even if we accepted the existence of Hamiltonians unbounded below, the first option would be physically meaningless: there would exists a system which we can measure and which freezes time for the entire universe. What nonsense! In Subsection 3.6.10 below, we will approach this problem from a different direction: we will develop the tool to define a notion of quantum dynamics based on hierarchies of (locally) synchronised quantum clocks, which can be made inaccessible without the need for time to reduce to an external parameter. We will argue that this can be used to construct a (toy?) model of emergent global time without any need for an accessible universal quantum clock, but we will leave the detailed construction to future work.

3.6.1.6 Quantum dynamics within the coherent group framework

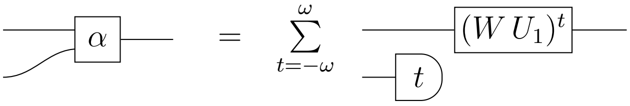
The techniques we have developed in the previous Sections allow us to treat three special cases of quantum dynamics: those which are discrete, periodic, or both. These are associated, respectively, with the symmetry groups $\mathbb{Z}$, $\mathbb{R}/T\mathbb{Z}$ (where time flows continuously, with period T), and $\mathbb{Z}_T$ (where time ticks at regular discrete intervals, with period T). Unfortunately, it will not be possible to cover the continuous aperiodic case of dynamics governed by $\mathbb{R}$ in this work: the treatment of $\mathrm{L}^2[\mathbb{R}]$ in the non-standard framework was introduced only recently [GG17], and the techniques developed here will be extended to continuous dynamics in the near future.

Discrete periodic case. Discrete periodic quantum dynamics are unitary representations of the finite cyclic groups $\mathbb{Z}_T$ (where T is the period). In our coherent framework, they are the representations of those doubly well-pointed, doubly finite coherent groups $\mathbb{G} = (\circ, \bullet)$ in fHilb which have $[\![G]\!] \cong \mathbb{Z}_T$.

Discrete case. Discrete quantum dynamics are unitary representations of the group $\mathbb{Z}$. In order to deal with them within our coherent framework, we consider the object $\mathcal{G} := \Big(\mathbb{R}/(T\mathbb{Z}), \frac{1}{\sqrt{T}}|\chi_n\rangle_{n=-\omega}^{\omega}\Big)$ of *Hilb constructed in Section 3.5, together with the doubly well-pointed coherent group $\mathbb{G} := (\circ, \bullet)$ on $\mathcal{G}$ corresponding to the momentum/position pair for wavefunctions in a 1-dimensional box of side $T > 0$ with periodic boundary conditions. The underlying group $[\![\mathbb{G}]\!]$ for $\mathbb{G}$ is ${}^\star\mathbb{Z}_{2\omega+1}$, which has $\mathbb{Z}$ as its subgroup of standard elements.

In order to talk about standard discrete quantum dynamics within the non-standard framework, we will be interested in those unitary representations $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ of the coherent group $\mathbb{G}$ such that $\bar{U}_t := \alpha \circ (id_{\mathcal{H}} \otimes |t\rangle)$ is near-standard for all $t \in \mathbb{Z}$ (it is in fact enough to ask for $\bar{U}_1$ to be near-standard, as $\bar{U}_t = (\bar{U}_1)^t$). Given a standard discrete unitary dynamics $(U_t)_{t\in\mathbb{Z}}$ on some separable Hilbert space V, the following result shows how to find an α such that $\mathrm{st}(\bar{U}_t) = U_t$ for all $t \in \mathbb{Z}$.

Theorem 3.75. *Let $\mathcal{H} := (V, |e_d\rangle_{d=1}^{D})$ be a space in *Hilb, with dimension $D \in {}^\star\mathbb{N}$. Consider a discrete dynamic $(U_t)_{t\in\mathbb{Z}}$ on the separable standard Hilbert space V, and denote by $(U_t)_{t\in{}^\star\mathbb{Z}}$ its non-standard extension. Then any near-standard unitary $W \sim id_{\mathcal{H}}$ such that $(WU_1)^{2\omega+1} = id_{\mathcal{H}}$ induces a unitary representation $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ of the coherent group $\mathbb{G}$ as follows:*



(3.207)

The unitary representations α of $\mathbb{G}$ which arise this way are exactly those such that $\alpha\circ(id_{\mathcal{H}}\otimes|1\rangle)$ is near-standard. Equivalently, $\alpha\circ(id_{\mathcal{H}}\otimes|t\rangle)$ is near-standard for all $t \in \mathbb{Z}$, and the original standard discrete dynamics is recovered as $U_t := \mathrm{st}(\alpha \circ (id_{\mathcal{H}} \otimes |t\rangle))$.

Proof. Any discrete standard dynamic $(U_t)_{t\in\mathbb{Z}}$ satisfies $U_t = (U_1)^t$ for all $t \in \mathbb{Z}$, and hence by Transfer Theorem its non-standard extension must satisfy $U_t = (U_1)^t$ for all $t \in \{-\omega, ..., +\omega\}$. But the family $(U_t)_{t=-\omega}^{+\omega}$ is not in general a representation of ${}^\star\mathbb{Z}_{2\omega+1}$: it need not satisfy $U_{2\omega+1} = id_{\mathcal{H}}$. We now construct some near-standard unitary $W \sim id_V$ commuting with U_1 and such that $W^{2\omega+1} = U_{-2\omega-1}$. Diagonalise the unitary U_1 and let its eigenvalues be $(e^{i2\pi\,\alpha_d})_{d=1}^{D}$: then $U_{-2\omega-1}$ is necessarily near-standard, with eigenvalues $(e^{i2\pi\beta_d})_{d=1}^D$, where β_d is the unique non-standard real $0 \leq \beta_d < 1$ satisfying $\beta_d = (2\omega+1)\alpha_d \pmod 1$. Some unitaries W satisfying the requirements above are the ones with the same eigenvectors as U_1 and with eigenvalues $(e^{i2\pi\gamma_d})_{d=1}^D$, where $\gamma_d := (\beta_d + k)/(2\omega+1)$ and $k \in {}^\star\mathbb{Z}$ is such that $k/(2\omega+1)$ is infinitesimal. If we now let $U'_t := (WU_1)^t$ for one such W, then $(U'_t)_{t\in{}^\star\mathbb{Z}_{2\omega+1}}$ is a representation of ${}^\star\mathbb{Z}_{2\omega+1}$, because the following equation now holds:

$$U'_{2\omega+1} = (WU_1)^{2\omega+1} = id_{\mathcal{H}} \tag{3.208}$$

Now consider a unitary representation of $\mathbb{G}$, write $U'_1 := \alpha \circ (id_{\mathcal{H}} \otimes |1\rangle)$ and let U be a standard unitary such that $U'_1 \sim U$. If we define $W := U'_1 U^{-1}$, then W is by definition a near-standard unitary such that $W \sim id_{\mathcal{H}}$ and satisfying:

$$(WU)^{2\omega+1} = (U'_1)^{2\omega+1} = id_{\mathcal{H}} \tag{3.209}$$

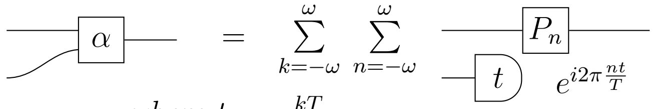
Hence α is in the required form, for a W satisfying the required conidtions. Finally, note that $\alpha \circ (id_{\mathcal{H}} \otimes |t\rangle) \sim U^t$ for finite integers $t \in \mathbb{Z}$, and hence letting $U_t := \mathrm{st}(\alpha \circ (id_{\mathcal{H}} \otimes |t\rangle)) = U^t$ defines a unitary representation of $\mathbb{Z}$ on V. □

Continuous periodic case. Continuous periodic quantum dynamics are unitary representations of the group $\mathbb{R}/(T\mathbb{Z})$. In order to deal with them within our coherent framework, we consider the object $\mathcal{G} := \left(\mathbb{R}/(T\mathbb{Z}), \frac{1}{\sqrt{T}}|\chi_n\rangle_{n=-\omega}^{\omega}\right)$ of *Hilb constructed in Section 3.5, together with the doubly well-pointed coherent group $\mathbb{G} := (\bullet, \circ)$ on $\mathcal{G}$ corresponding to the position/momentum pair for wavefunctions in a 1-dimensional box of side $T > 0$ with periodic boundary conditions.

The underlying group $[\![\mathbb{G}]\!]$ for $\mathbb{G}$ is $\frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$, with elements in the form $x = \frac{kT}{2\omega+1}$ for $k \in {}^\star\mathbb{Z}_{2\omega+1}$, and taking the standard part corresponds to a quotient group homomorphism $\mathrm{st} : \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1} \to \mathbb{R}/(T\mathbb{Z})$. This means that every element of $\mathbb{R}/(T\mathbb{Z})$ can be approximated to within infinitesimal distance by elements of $[\![\mathbb{G}]\!]$, with the elements $\mathrm{st}^{-1}(y) \subset [\![\mathbb{G}]\!]$ approximating a given $y \in \mathbb{R}/(T\mathbb{Z})$ forming a coset of the elements $\mathrm{st}^{-1}(0) \subset [\![\mathbb{G}]\!]$ approximating the group unit $0 \in \mathbb{R}/(T\mathbb{Z})$.

In order to talk about standard continuous periodic quantum dynamics within the non-standard framework, we will be interested in those unitary representations $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ of the coherent group $\mathbb{G}$ such that $\bar{U}_t := \alpha \circ (id_{\mathcal{H}} \otimes |t\rangle)$ is near-standard for all $t \in \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$. Given a standard continuous periodic unitary dynamics $(U_t)_{t\in\mathbb{Z}}$ on some separable Hilbert space V, the following result shows how to find an α such that $\mathrm{st}(\bar{U}_t) = U_{\mathrm{st}(t)}$ for all $t \in \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$, where we used again the notation $\bar{U}_t := \alpha \circ (id_{\mathcal{H}} \otimes |t\rangle)$.

Theorem 3.76. *Consider a continuous periodic dynamic $(U_t)_{t\in\mathbb{R}/(T\mathbb{Z})}$ on a separable standard Hilbert space V, let $(P_n)_{n\in\mathbb{Z}}$ be the complete family of orthogonal projectors for the Hamiltonian observable, and let $(P_n)_{n\in{}^\star\mathbb{Z}}$ be its non-standard extension. Consider the space $\mathcal{H} := (V, |e_d\rangle_{d=1}^D)$ in *Hilb, where without loss of generality we have picked the basis $|e_d\rangle_{d=1}^D$ to consist of energy eigenstates, and we have chosen the dimension $D \in {}^\star\mathbb{N}$ such that $\sum_{n=-\omega}^{+\omega} P_n = \sum_{d=1}^D |e_d\rangle\langle e_d|$. Then the following is a unitary representation $\alpha : \mathcal{H}\otimes\mathcal{G}\to\mathcal{G}$ of the coherent group $\mathbb{G}$:*



(3.210)

where $t := \frac{kT}{2\omega+1}$

Furthermore, we have that $\mathrm{st}(\bar{U}_t) = U_{\mathrm{st}(t)}$ *for all* $t \in \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$.

Proof. For each given $t \in \mathbb{R}/(T\mathbb{Z})$, by PVM version of Stone's Theorem we have that:

$$U_t = \sum_{n\in\mathbb{Z}} e^{i2\pi\frac{nt}{T}} P_n \tag{3.211}$$

As a consequence, it should not be too surprising that for a given $t \in \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$ we have defined:

$$\bar{U}_t := \sum_{n=-\omega}^{+\omega} e^{i2\pi\frac{nt}{T}} P_n \tag{3.212}$$

Because $(P_n)_{n\in\mathbb{Z}}$ is a complete family of orthogonal projectors, then so is $(P_n)_{n\in{}^\star\mathbb{Z}}$. As a consequence, we have that:

$$\bar{U}_0 = \sum_{n=-\omega}^{+\omega} P_n = id_{\mathcal{H}} \tag{3.213}$$

$$\bar{U}_t\bar{U}_s = \sum_{n=-\omega}^{+\omega}\sum_{m=-\omega}^{+\omega} e^{i2\pi\frac{nt+ms}{T}} P_nP_m = \sum_{n\in\mathbb{Z}} e^{i2\pi\frac{n(t+s)}{T}} P_n = \bar{U}_{t\oplus s} \tag{3.214}$$

Furthermore, for any infinite $m \in {}^\star\mathbb{Z}$ we must have that $\mathrm{st}(P_m) = 0$, because $P_mP_n = 0$ for all finite $n \in \mathbb{Z}$. As a consequence, for any $t \in \frac{T}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$ we have:

$$\mathrm{st}(\bar{U}_t) = \sum_{n=-\omega}^{+\omega} e^{i2\pi\frac{n\,\mathrm{st}(t)}{T}}\,\mathrm{st}(P_n) = \sum_{n\in\mathbb{Z}} e^{i2\pi\frac{n\,\mathrm{st}(t)}{T}} P_n = U_{\mathrm{st}(t)} \tag{3.215}$$

□

The way forward. For the remainder of this Section, we will try to deal with quantum dynamics in full generality, by working with some generic doubly well-pointed coherent group $\mathbb{G} := (\circ, \bullet)$ which we interpret as encoding time-translation symmetry. We will take $[\![\mathbb{G}]\!] = (K(\circ), \succ\!\bullet\!-, \bullet\!-)$ to mark the states of definite time, and deduce that $(K(\bullet), \succ\!\circ\!-, \circ\!-)$ marks the states of definite energy, but for the most part we will not be concerned with the specific structure of $\mathbb{G}$: as a consequence, our results will apply to all those dynamics which can be modelled by coherent groups within our framework[40]. We will make it explicitly clear when a specific underlying group structure is used to derive some result, or at certain points in the discussion.

3.6.2 Quantum clocks

We consider a doubly well-pointed coherent group $\mathbb{G} = (\circ, \bullet)$, and we interpret the underlying group $[\![\mathbb{G}]\!]$ to be the time-translation symmetry group of a classical **clock** governing the dynamical systems which we are interested in. From an operational perspective, when saying that a clock "governs" a dynamical system we will merely mean that the two are "perfectly synchronised": this perspective will be covered in detail later in this Section.

If we understand the underlying group $[\![\mathbb{G}]\!]$ as a classical clock, then the coherent group $\mathbb{G}$ is exactly what Schrödinger would refer to as a **quantum clock** [Hil05]: the quantum system of wavefunctions over the classical clock states, together with the appropriate time-translation symmetry structure. By construction, the point structure $\circ$ of a quantum clock is associated with the **clock time** observable, and the group structure endows the set $K(\circ)$ of **clock time states** with the relevant time-translation structure: after all, the quantum clock always governs its own dynamics, as it is necessarily synchronised with itself. what is the physical meaning of the observable associated with the group structure $\bullet$? Is it energy, in a certain sense? To understand its role, we need to look at the dynamical systems governed by the quantum clock.

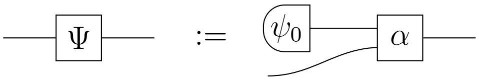
3.6.3 Quantum dynamical systems

Because we understand dynamics as time-translation symmetry, a **quantum dynamical system** governed by a quantum clock $\mathbb{G}$ is simply a unitary representation α of

[40] At present, this includes discrete, continuous periodic and discrete periodic dynamics. Continuous dynamics will be added to this list in the near future, thanks to the recent work of [GG17].

$\mathbb{G}$. As a consequence, the unitary Eilenberg-Moore category $\mathrm{Rep}^{\dagger}[\mathbb{G}]$ is the category of quantum dynamical systems governed by $\mathbb{G}$.

In the coherent perspective, the evolution of an initial state ψ_0 under time-translation is given by its **coherent history** in the quantum dynamical system $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$, which is defined to be the following process $\Psi : \mathcal{G} \to \mathcal{H}$:

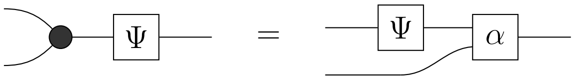


(3.216)

A similar construction can be done for arbitrary coherent groups, not necessarily with dynamical semantics, in which case we will say that Ψ is the **coherent orbit** of ψ_0 in the symmetric system α.

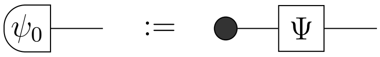
Just like classical trajectories can be characterised as certain equivariant functions (e.g. $\mathbb{R} \to \mathcal{H}$, in the continuous case), so coherent histories can be characterised as certain Eilenberg-Moore morphisms.

Theorem 3.77 (Coherent orbits are EM morphisms).
Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group on a system $\mathcal{G}$ of a †-SMC, let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. If Ψ is the coherent orbit of an initial state ψ_0 in α, then it is also an Eilenberg-Moore morphism Ψ : *$\to \alpha$ from the coherent group (seen as the regular representation) to α:*



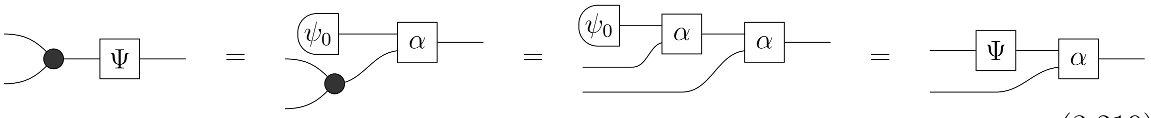
(3.217)

Conversely, if Ψ : *$\to \alpha$ is an Eilenberg-Moore morphism, then it is the coherent orbit of the following initial state ψ_0:*



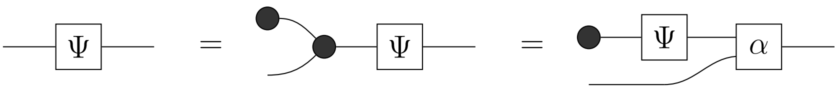
(3.218)

Proof. First we prove that the coherent orbit of an initial state ψ_0 in α is an EM morphism:



(3.219)

Conversely, we prove that an EM morphism is the coherent orbit of the initial state ψ_0 specified by Equation 3.218:



(3.220)

□

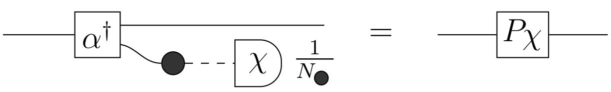
3.6.4 The coherent Hamiltonian

In order to understand the role of the group structure $\bullet$ in the quantum clock, we turn our attention to the states which are invariant under the coherent dynamics: from Theorem 3.37, we know that an invariant state of a quantum dynamical system α is associated with a definite outcome $\chi^\dagger \in K(\bullet)$ of the coherent measurement $\alpha^\dagger$, and that the phase at time $t \in \mathbb{Z}_T$ of its evolution is given by the scalar $\chi \circ t$. But this is exactly what happens with energy eigenstates in traditional quantum mechanics!

The admissible energy levels for a generic continuous quantum dynamical system $(U_t)_{t\in\mathbb{R}}$, are traditionally labelled by the real numbers, and the phase acquired over time $t \in \mathbb{R}$ by an eigenstate $|\psi_E\rangle$ of energy $E \in \mathbb{R}$ is given by $\chi_{E/h}(t) := e^{i2\pi\frac{Et}{h}}$. The admissible energy levels for a continuous periodic dynamical system $(U_t)_{t\in\mathbb{R}/(T\mathbb{Z})}$ are discretised by periodicity, and are traditionally labelled by nh, where $n \in \mathbb{Z}$. The phase acquired over time $t \in \mathbb{R}/(T\mathbb{Z})$ by an eigenstate $|\psi_{n\hbar}\rangle$ of energy nh is given by $\chi_n(t) := e^{i2\pi\frac{nt}{T}}$. The admissible energy levels for a discrete quantum dynamical system $(U_t)_{t\in\mathbb{Z}}$ are continuous, but they are made periodic by the discrete nature of the dynamics. If we label the energy levels as $E \in \mathbb{R}/(h\mathbb{Z})$, then the phase acquired over time $t \in \mathbb{Z}$ by an eigenstate $|\psi_E\rangle$ of energy E is given by $\chi_{E/h}(t) := e^{i2\pi\frac{Et}{h}}$. The admissible energy levels for a discrete periodic quantum dynamical system $(U_t)_{t\in\mathbb{Z}_T}$ are both discrete and periodic: we can label them by nh as in the discrete case, but with $n \in \mathbb{Z}_T$ in this case. The phase acquired over time $t \in \mathbb{Z}_T$ by an eigenstate $|\psi_{nh}\rangle$ of energy nh is given by $\chi_n(t) := e^{i2\pi\frac{nt}{T}}$.

In all four cases above, we could equivalently label the energy levels for dynamics governed by a time-translation group G in a canonical way by using the multiplicative characters in $G^\wedge$. Indeed, an energy level is always uniquely identified with the time evolution of phases for its eigenstates: the two notions can be made to coincide, and in doing so we obtain a labelling of energy levels which is independent of choices of units of measurement for energy (and in particular of Planck constant h).

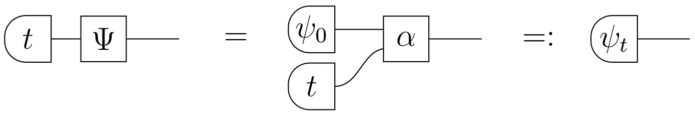
From the discussion above, it is clear that the $\bullet$-classical states can be identified with the admissible energy levels for quantum dynamical systems governed by the given quantum clock $(\circ, \bullet)$. As a consequence, we will refer to $\bullet$ as the **clock energy** observable, and to $\alpha^\dagger$ as the **coherent Hamiltonian** of the quantum dynamical system α. Hence, the non-demolition and demolition measurements associated with $\alpha^\dagger$ correspond to the non-demolition and demolition measurements for the energy of the quantum dynamical system α, where P_χ is the projector for energy level χ:



(3.221)

3.6.5 Schrödinger's Equation

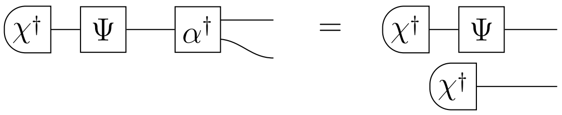
Just as a representation of a coherent group carries a lot more information than the corresponding representation of the underlying classical group, the coherent history of a state in a quantum dynamical system α carries a lot more information than the corresponding history under the classical clock $[\![\mathbb{G}]\!]$. When evaluating the coherent history $\Psi : \mathcal{G} \to \mathcal{H}$ of an initial state ψ_0 at a clock time state t, we obtain the state ψ_t corresponding to the evolution of the system at that time:



(3.222)

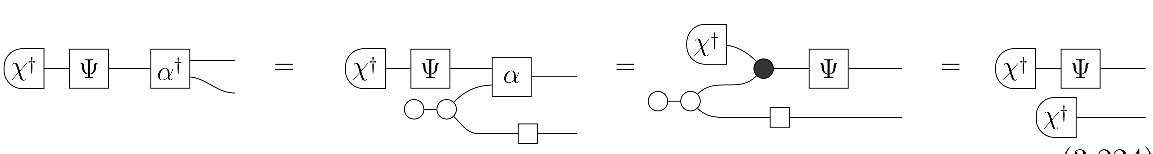
Thanks to the coherent approach, however, we could instead choose to evaluate the coherent history at a clock energy state $\chi^\dagger$. As the following result shows, this yields the component of ψ_0 corresponding to energy level $\chi^\dagger$.

Lemma 3.78. *Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group on a system $\mathcal{G}$ of a $\dagger$-SMC, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. Let ψ_0 be a state of $\mathcal{H}$, and let $\Psi : \mathcal{G} \to \mathcal{H}$ be the associated coherent history. If $\chi^\dagger \in \bullet$, then the following holds:*



(3.223)

Proof. The proof is straightforward, by unpacking the definition of Ψ and using idempotence of α and $\bullet$-classicality of $\chi^\dagger$:

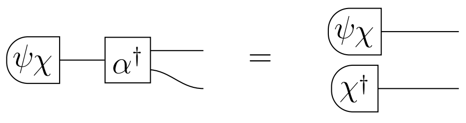


(3.224)

□

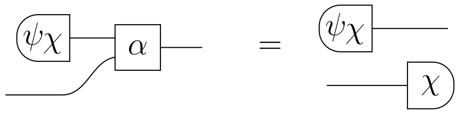
The same idea—using coherence to evaluate something that is classically a function of clock time states on a clock energy state instead—can be used to derive Schrödinger's Equation for a quantum dynamical system α from the defining equation of Eilenberg-Moore morphisms ⟩●– $\to \alpha$. From a categorical perspective, this is an extremely neat result: the fundamental equation of traditional quantum dynamics finds its natural counterpart in the fundamental equation defining evolution of states within the categorical framework (see Theorem 3.77).

Theorem 3.79 (Schrödinger Equation).
Let $\mathbb{G} = (\circ, \bullet)$ be a coherent group on a system $\mathcal{G}$ of a $\dagger$-SMC, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a unitary representation of $\mathbb{G}$. Suppose that ψ_χ is an energy eigenstate of α corresponding to clock energy level $\chi^\dagger \in K(\bullet)$:



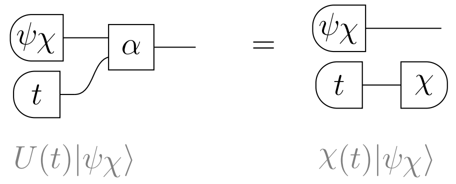
(3.225)

Then ψ_χ satisfies the following Equation :



(3.226)

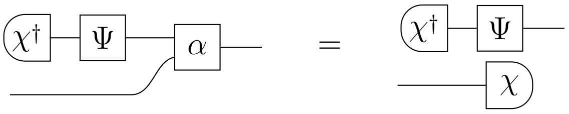
When evaluated on clock time states, Equation 3.227 is easily seen to be an abstract counterpart to Equation 3.199:



(3.227)

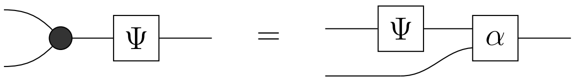
From this point onwards, we will refer to Equation 3.226 as ***Schrödinger's Equation*** *in our framework. Now assume that $\mathbb{G}$ is doubly well-pointed, and consider any process $\Psi : \mathcal{G} \to \mathcal{H}$. Then the following two conditions are equivalent:*

- *the states $\psi_\chi := \Psi \circ \chi^\dagger$ satisfy Schrödinger's Equation for all $\chi^\dagger \in K(\bullet)$:*



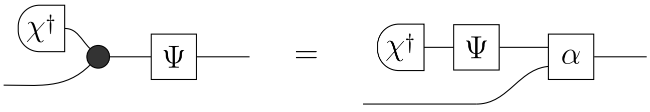
(3.228)

- *the process Ψ is a coherent history, i.e. it satisfies the defining equation for Eilenberg-Moore morphisms* *$\to \alpha$:*



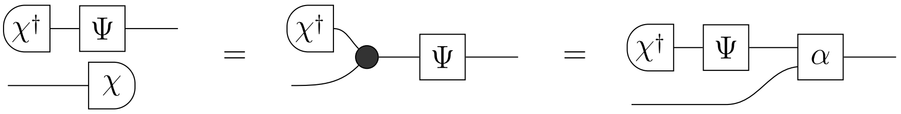
(3.229)

Proof. Proving that Schrödinger's Equation (Equation 3.226) is satisfied by energy eigenstates is a straightforward application of unitarity for α and $\bullet$-classicality of $\chi^\dagger$. Now we want to prove that Equation 3.226 holding for all ψ_χ is equivalent to Ψ satisfying the defining equation for EM algebras. Because the coherent group is doubly well-pointed, the defining equation for EM algebras holds if and only if it holds when evaluated on all $\chi^\dagger \in K(\bullet)$:



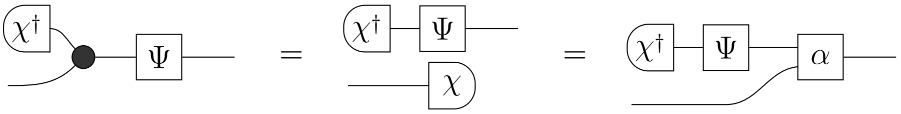
(3.230)

If Equation 3.230 holds for all $\chi^\dagger$, then so does Equation 3.226:



(3.231)

Conversely, if Equation 3.226 holds for all $\chi^\dagger$, then so does Equation 3.230:



(3.232)

□

3.6.6 von Neumann's mean ergodic theorem

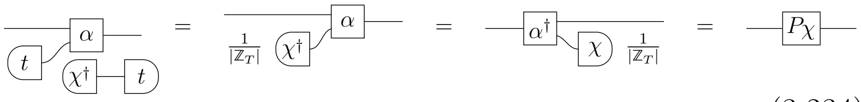
We will now use symmetry-observable duality for coherent quantum dynamics to provide concise proofs of von Neumann's mean ergodic theorem in the discrete periodic, discrete and continuous periodic cases (using the coherent groups we introduced at the beginning of this Section). The same proof method applies—essentially unchanged—to the continuous case, using the coherent group on $\mathrm{L}^2[\mathbb{R}]$ introduced in [GG17]; however, a fully detailed treatment of the continuous case is left to future work.

Theorem 3.80 (**Mean Ergodic Theorem (discrete periodic)**). *Let $(U_t)_{t\in\mathbb{Z}_T}$ be a unitary representation of $\mathbb{Z}_T$ on a finite-dimensional Hilbert space $\mathcal{H}$, and let $P_\chi : \mathcal{H} \to \mathcal{H}$ be the orthogonal projector on the energy eigenspace corresponding to energy level $\chi \in \left(\mathbb{Z}_T\right)^\wedge$. Then the following equality holds:*

$$\frac{1}{T}\sum_{t=0}^{T-1} \chi(t)^* U_t = P_\chi \tag{3.233}$$

Proof. Symmetry-observable duality for systems with coherent symmetries can be invoked to obtain the following one-line proof:

$$\tfrac{1}{T}\sum_{t=0}^{T-1} \chi(t)^* U_t = \tfrac{1}{T}\sum_{t=0}^{T-1}$$



(3.234)

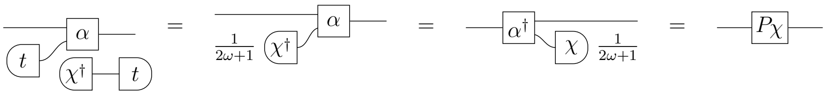
□

Theorem 3.81 (**Mean Ergodic Theorem (discrete)**).
Let $(U_t)_{t\in\mathbb{Z}}$ be a unitary representation of $\mathbb{Z}$ on a separable Hilbert space V, and let $P_\chi : V \to V$ be the orthogonal projector on the energy eigenspace corresponding to energy level $\chi \in \mathbb{Z}^\wedge$. Then the following equality holds:

$$\lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \chi(t)^* U_t = P_\chi \tag{3.235}$$

Proof. Symmetry-observable duality for systems with coherent symmetries can be invoked to obtain the following chain of equations:

$$\frac{1}{2\omega+1}\sum_{t=-\omega}^{+\omega} \chi(t)^* U_t \;=\; \frac{1}{2\omega+1}\sum_{t=-\omega}^{+\omega}$$



(3.236)

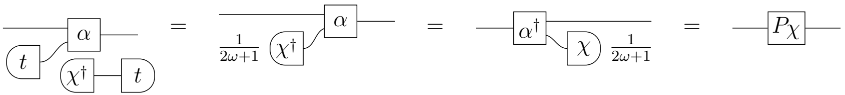
Because ω is an arbitrary infinite integers, we have that $\lim_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\chi(t)^*U_t \sim \frac{1}{2\omega+1}\sum_{t=-\omega}^{+\omega}\chi(t)^*U_t$, and by taking the standard part we obtain the desired result. □

Theorem 3.82 (**Mean Ergodic Theorem (continuous periodic)**).
Let $(U_t)_{t\in\mathbb{R}/(T\mathbb{Z})}$ be a unitary representation of $\mathbb{R}/(T\mathbb{Z})$ on a separable Hilbert space V, and let $P_\chi : V \to V$ be the orthogonal projector on the energy eigenspace corresponding to energy level $\chi \in \big(\mathbb{R}/(T\mathbb{Z})\big)^\wedge$. Then the following equality holds:

$$\frac{1}{T}\int_{t=0}^{T} \chi(t)^* U_t dt = P_\chi \tag{3.237}$$

Proof. Symmetry-observable duality for systems with coherent symmetries can be invoked to obtain the following chain of equations, where we used the non-standard extension $(U_t)_{t\in{}^\star(\mathbb{R}/(T\mathbb{Z}))}$ and we had defined the shorthand $t := \frac{kT}{2\omega+1}$ in the two leftmost expressions:

$$\frac{1}{2\omega+1}\sum_{k=-\omega}^{+\omega} \chi(t)^* U_t = \frac{1}{2\omega+1}\sum_{t=0}^{T-1}$$



(3.238)

It is a standard result of non-standard analysis that the integral $\int_{t=0}^{T}\chi(t)^*U_t dt$ can be approximated, up to infinitesimals, by the infinite sum $\sum_{k=-\omega}^{+\omega}\big(\chi(t)^*U_t\frac{T}{2\omega+1}\big)$: hence the chain of equations above reads $\frac{1}{T}\int_{t=0}^{T}\chi(t)^*U_t dt \sim P_\chi$, and by taking the standard part we obtain the desired result. □

3.6.7 Stone's Theorem

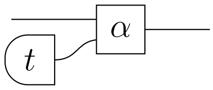
We will use symmetry-observable duality for coherent quantum dynamics once more, this time to provide concise proofs of Stone's Theorem in the discrete periodic, discrete and continuous periodic cases (using the coherent groups we introduced at the beginning of this Section). These proofs are essentially the duals of the proofs for von Neumann's Mean Ergodic Theorem presented above, but they're presented in full for instructive reasons. Again, he same proof method applies—essentially unchanged—to the continuous case, using the coherent group on $\mathrm{L}^2[\mathbb{R}]$ introduced in [GG17]; however, a fully detailed treatment of the continuous case is left to future work.

Theorem 3.83 (**Stone's Theorem (discrete periodic)**).
Let $(U_t)_{t\in\mathbb{Z}_T}$ be a unitary representation of $\mathbb{Z}_T$ on a finite-dimensional Hilbert space $\mathcal{H}$, and let $(P_\chi)_{\chi\in(\mathbb{Z}_T)^\wedge}$ be the complete family of orthogonal projectors associated to the Hamiltonian observable. Then the following equality holds:

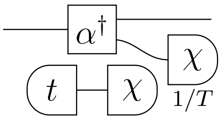
$$U_t = \sum_{\chi\in(\mathbb{Z}_T)^\wedge} \chi(t) P_\chi \tag{3.239}$$

Proof. Symmetry-observable duality for systems with coherent symmetries can be invoked to obtain the following on-line proof:

U_t =



= $\sum_{\chi\in(\mathbb{Z}_T)^\wedge}$



= $\sum_{\chi\in(\mathbb{Z}_T)^\wedge} \chi(t)P_\chi$

(3.240)

□

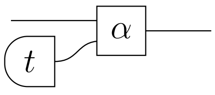
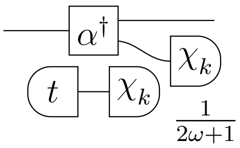
Theorem 3.84 (**Stone's Theorem (discrete)**).
Let $(U_t)_{t\in\mathbb{Z}}$ be a unitary representation of $\mathbb{Z}$ on a separable Hilbert space V, and let $\big(\pi(S)\big)_{S\subseteq\mathbb{Z}^\wedge}$ be the PVM associated to the Hamiltonian observable[41]. *Then the following equality holds:*

$$U_t = \int_{\mathbb{Z}^\wedge} \chi(t) d\pi(\chi) \tag{3.241}$$

Proof. We have $\mathbb{Z}^\wedge \cong \mathbb{R}/\mathbb{Z}$, which corresponds to ${}^\star\mathbb{Z}_{2\omega+1}{}^\wedge \cong \frac{1}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$ in the non-standard framework. For each $\frac{k}{2\omega+1} \in \frac{1}{2\omega+1}{}^\star\mathbb{Z}_{2\omega+1}$, we write χ_k for the corresponding element of ${}^\star\mathbb{Z}_{2\omega+1}{}^\wedge$. Symmetry-observable duality for systems with coherent

[41] Note that $\mathbb{Z}^\wedge \cong \mathbb{R}/\mathbb{Z}$, so we need to consider a PVM instead of a complete family of orthogonal projectors as we do in the other cases.

symmetries can then be invoked to obtain the following chain of equations:

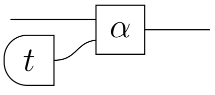
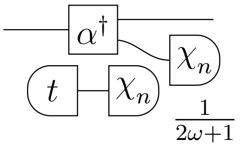
$U_t \quad =$  $= \quad \sum_{k=-\omega}^{+\omega}$  $= \quad \sum_{k=-\omega}^{+\omega} \chi(t) P_{\chi_k}$ (3.242)

The projectors P_{χ_k} are infinitesimal, i.e. they can be seen to satisfy the following property: if $x, y \in \mathbb{R}/\mathbb{Z}$ and $h, k \in {}^\star\mathbb{Z}_{2\omega+1}$ are such that $x \simeq \frac{k_x}{2\omega+2}$ and $y \simeq \frac{k_y}{2\omega+2}$, then we have $\int_x^y d\pi(\chi) \sim \sum_{k=k_x}^{k_y} P_{\chi_k}$. As a consequence, we have $\int_{\mathbb{Z}^\wedge} \chi(t) d\pi(\chi) \sim \sum_{k=-\omega}^{+\omega} \chi(t) P_{\chi_k}$, and taking the standard part completes our proof. □

Theorem 3.85 (Stone's Theorem (continuous periodic)).
Let $(U_t)_{t \in \mathbb{R}/(T\mathbb{Z})}$ be a unitary representation of $\mathbb{R}/(T\mathbb{Z})$ on a separable Hilbert space V, and let $(P_\chi)_{\chi \in (\mathbb{R}/(T\mathbb{Z}))^\wedge}$ be the complete family of orthogonal projectors associated to the Hamiltonian observable[42]*. Then the following equality holds:*

$$U_t = \sum_{\chi \in (\mathbb{R}/(T\mathbb{Z}))^\wedge} \chi(t) P_\chi \tag{3.243}$$

Proof. Symmetry-observable duality for systems with coherent symmetries can be invoked to obtain the following chain of equations, where we have used the non-standard extension $(U_t)_{t \in {}^\star(\mathbb{R}/(T\mathbb{Z}))}$ and the shorthand $t := \frac{kT}{2\omega+1} \in \frac{T}{2\omega+1} {}^\star\mathbb{Z}_{2\omega+1}$:

$U_t \quad =$  $= \quad \sum_{n=-\omega}^{\omega}$  $= \quad \sum_{n=-\omega}^{+\omega} \chi(g) P_{\chi_n}$ (3.244)

We obtain our desired result by taking the standard part of the leftmost and rightmost expression, by observing that $\mathrm{st}(U_t) = U_{\mathrm{st}(t)}$ and that $\mathrm{st}(P_{\chi_n}) = 0$ for all infinite non-standard integers n. □

3.6.8 Feynman's clock

Given a quantum circuit composed of unitary gates, the Feynman clock construction [Fey82, Fey86] provides a Hamiltonian with ground states characterising the entire computation. More precisely, if $(V^{(t)})_{t=0,\dots,n}$ is some finite sequence of unitary gates

[42] Note that $\big(\mathbb{R}/(T\mathbb{Z})\big)^\wedge \cong \mathbb{Z}$, so we can work directly with a complete family of orthogonal projectors in this case.

on a quantum system $\mathcal{H}$, then the construction produces a Hamiltonian with the following ground states:

$$\left[\sum_{t=0,...,n} |\psi_t\rangle \otimes |t\rangle\right] \text{ s.t. } V^{(t)}|\psi_t\rangle = |\psi_{t+1}\rangle \tag{3.245}$$

The problem of performing the quantum computation is then reduced to the problem of finding a ground state for the Hamiltonian. This construction can be straightforwardly applied to the parallel-in-time simulation of discrete quantum dynamics (i.e. the one-step computation of a coherent history for the system) by seeing $U^{(t)}$ as the time evolution operator from time t to time $t+1$ [MPAG13].

The relation between the Feynman clock construction and discrete periodic dynamics comes from the following observation: any linear circuit $(V^{(t)})_{t=0,...,T-1}$ can be turned into an appropriate cyclic circuit $(U^{(t)})_{t\in\mathbb{Z}_{2T}}$ by setting $U^{(t)} := V^{(t)}$ for all $t = 0, ..., T-1$ and $U^{(t)} := V^{(2T-t-1)}$ for $t = T, ..., 2T-1$, and the cyclic circuit can be seen as a discrete periodic quantum dynamical system possessing a time-dependent Hamiltonian. The problem of finding the ground energy state for the original linear circuit is evidently equivalent to the problem of finding the ground energy state for the cyclic circuit, and hence the two circuits can be used interchangeably for the purposes of the Feynman clock construction. We will henceforth be considering a generic cyclic circuit, i.e. some family $(U^{(t)})_{t\in\mathbb{Z}_T}$ of unitaries such that $\prod_{t=0}^{T-1} U^{(t)} = id$.

The main obstacle to treating the Feynman clock construction within our framework would appear to be that a generic cyclic circuit $(U^{(t)})_{t\in\mathbb{Z}_T}$ need not correspond to discrete periodic dynamics, in the sense used in this work up to this moment: in a representation $(U_t)_{t\in\mathbb{Z}_T}$ of the finite cyclic group $\mathbb{Z}_T$ we have $U_t = (U_1)^t$, while the operators $U^{(t)}$ are completely arbitrary. From a physical perspective, our symmetry approach models the the time-translation symmetry of quantum dynamical systems with a time-independent Hamiltonian, while the Feynman clock construction allows for potentially different time evolution operators $U^{(t)}$ at each different time t.

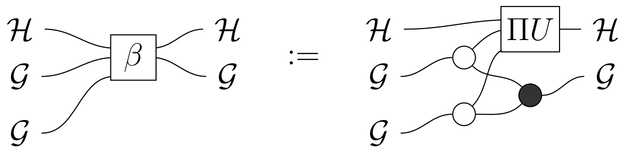
However, this does not turn out to be such a mighty obstacle after all, because time-dependent dynamics can be easily accommodated in the time-independent symmetry perspective. Instead of a representation of $\mathbb{Z}_T$ on $\mathcal{H}$, we consider the following representation $(W_t)_{t\in\mathbb{Z}_T}$ of $\mathbb{Z}_T$ on $\mathcal{H} \otimes \mathbb{C}[\mathbb{Z}_T]$:

$$W_{\delta t}\big(|\psi\rangle \otimes |t\rangle\big) := \left[\left(\prod_{j=t}^{t+\delta t-1} U^{(j)}\right)|\psi\rangle\right] \otimes |t \oplus \delta t\rangle \tag{3.246}$$

where the product is expanded to the left. This representation is essentially the *propagator* for the discrete quantum dynamical system: given an interval of time δt, the time-translation action of the propagator evolves the state ψ_t at time t to the corresponding state $\psi_{t\oplus\delta t}$ at time $t \oplus \delta t$. If we interpret $\mathcal{H}$ as the quantum system of wavefunctions over some space, then $\mathcal{H}\otimes\mathcal{G}$ (here $\mathcal{G} = \mathbb{C}[\mathbb{Z}_T]$) can be interpreted as the quantum system of wavefunctions over the corresponding (non-relativistic) space-time.

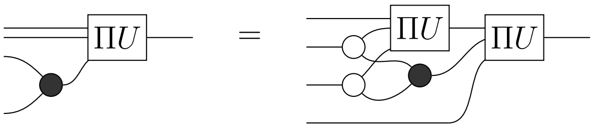
With a little work to formalise that expanding product, we can turn this iterated product construction into a general result about unitary representations of coherent groups, and as a consequence we will be able to model quantum dynamical systems with time-dependent Hamiltonians within our framework.

Theorem 3.86 (**Propagators**).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an system $\mathcal{G}$ of a †-SMC $\mathcal{C}$. Consider a process $\Pi U : (\mathcal{H}\otimes\mathcal{G})\otimes\mathcal{G} \to \mathcal{G}$, and construct a process $\beta : (\mathcal{H}\otimes\mathcal{G})\otimes\mathcal{G} \to \mathcal{H}\otimes\mathcal{G}$ as follows:

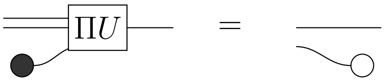


(3.247)

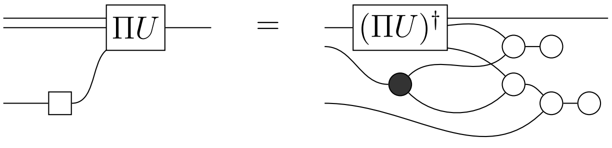
Then β is a unitary representation of the coherent group $\mathbb{G}$ on the composite system $\mathcal{H}\otimes\mathcal{G}$ if and only if the process ΠU satisfies the following requirements:



(3.248)



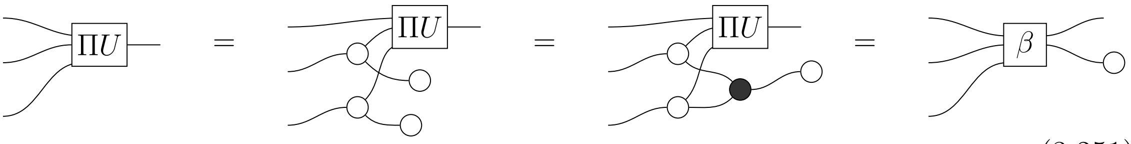
(3.249)



(3.250)

When β is a unitary representation the form above, we refer to it as a ***propagator****.*

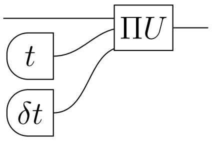
Proof. The entire proof essentially depends on the fact that the process ΠU can be recovered from the propagator β by coherently deleting the time output of the latter:



(3.251)

Checking the various implications (six in total) is a tedious but entirely straightforward application of the laws of strong complementarity and Frobenius algebras. □

In fHilb, the process ΠU captures all the possible iterated products of unitaries in the following way:



$$= \prod_{j=t}^{t+\delta t-1} U^{(j)} \tag{3.252}$$

Equation 3.248 (similarly evaluated on clock time states t and δt) corresponds to the following property of the iterated products:

$$\prod_{j=t}^{t+\delta t+\delta t'-1} U^{(j)} = \Big(\prod_{j=t+\delta t}^{t+\delta t+\delta t'-1} U^{(j)} \Big) \Big(\prod_{j=t}^{t+\delta t-1} U^{(j)} \Big) \tag{3.253}$$

Equation 3.249 corresponds to the following property of the iterated products:

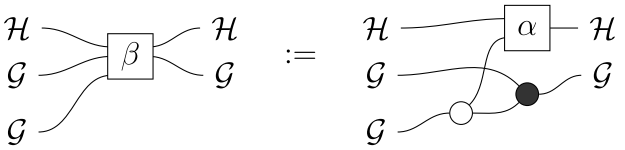
$$\prod_{j=t}^{t-1} U^{(j)} = id \tag{3.254}$$

Equation 3.250 defines what it means to take an iterated product "going backwards":

$$\prod_{j=t}^{t-\delta t-1} U^{(j)} := \Big(\prod_{j=t-\delta t}^{t-1} U^{(j)} \Big)^{\dagger} = \big(U^{(t-\delta t)}\big)^{\dagger} \circ \big(U^{(t-\delta t+1)}\big)^{\dagger} ... \circ \big(U^{(t-2)}\big)^{\dagger} \circ \big(U^{(t-1)}\big)^{\dagger} \tag{3.255}$$

Equation 3.250 furthermore proves that the product is in fact a product of unitaries. Theorem 3.86 is stated for a generic coherent group, but in the special case of discrete periodic dynamics Equation 3.250 also proves that the family of unitaries involved in the product is in fact a cyclic circuit.

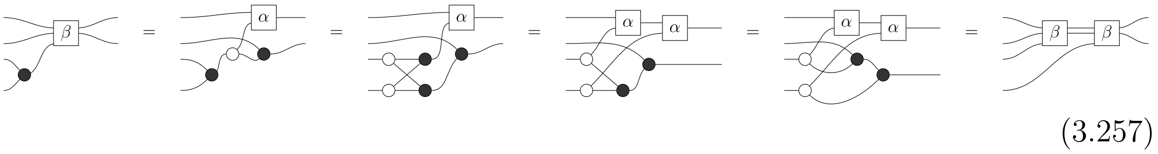
Corollary 3.87 (Time-translationally invariant propagators).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an system $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let α be a unitary representation of $\mathbb{G}$ on $\mathcal{H}$. Then the following process β is a propagator:



(3.256)

We refer to these as ***time-translationally invariant propagators****.*

Proof. The proof involves another series of straightforward checks using the laws of strong complementarity. For example, the following chain of equalities proves the multiplication condition for β using that for α:



(3.257)

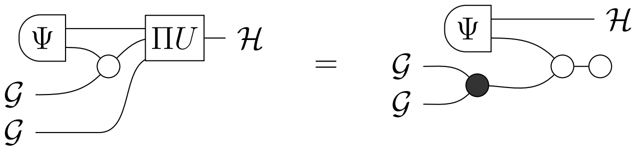
□

We are now in a position to prove correctness of the Feynman Clock construction within our framework. The next result is proven for general coherent groups, but in the special case where $\mathbb{G}$ is a quantum clock we have that $\beta^\dagger$ is the coherent Hamiltonian, and that the states Ψ of Equation 3.245 are the ground energy eigenstates. The result can be understood by observing that Equation 3.259 is the abstract version of the following generalisation of the condition appearing in Equation 3.245:

$$\forall t . \forall \delta t . \; \Big(\prod_{j=t}^{t+\delta t-1} U^{(j)} \Big) |\psi_t\rangle = |\psi_{t+\delta t}\rangle \tag{3.258}$$

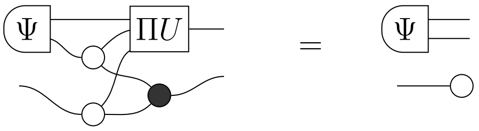
Hence Theorem 3.88 yields, in the special case of discrete periodic quantum dynamics, a proof of correctness for the traditional Feynman clock construction.

Theorem 3.88 (Feynman's Clock).
Let $\mathbb{G} := (\circ, \bullet)$ be a coherent group on an system $\mathcal{G}$, and let $\beta : (\mathcal{H} \otimes \mathcal{G}) \otimes \mathcal{G} \to \mathcal{H} \otimes \mathcal{G}$ be a propagator for $\mathbb{G}$. Then the eigenstates of $\beta^\dagger$ corresponding to the definite outcome ○– $\in K(\bullet)$ are exactly the states Ψ of $\mathcal{H} \otimes \mathcal{G}$ satisfying the following condition:



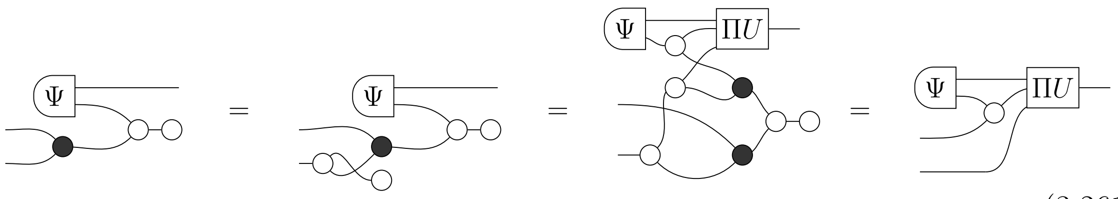
(3.259)

Proof. If Ψ is an eigenstate corresponding to definite outcome ○–, then we have the following equality (by the definition of β as a propagator):



(3.260)

As a consequence we also have the following chain of equalities, where the rightmost equality is obtained by applying the laws of strong complementarity (central rule of the bottom row) and Hopf's law:



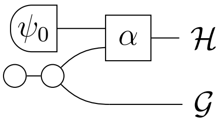
(3.261)

□

3.6.9 Clock-system synchronisation

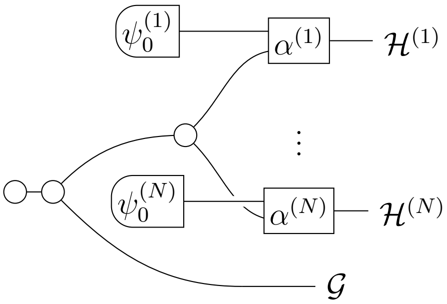
Up to this point, we have described quantum dynamical systems in terms of unitary representations. Although appealing from an algebraic and categorical perspective, this formulation lacks an immediate physical interpretation. To fix this, we shift point of view from the *action* of a quantum clock on a quantum system, to the *synchronisation* of the quantum clock and quantum dynamical system. The algebraic perspective corresponds to saying that a clock time state $|\delta t\rangle$ sends state $|\psi_t\rangle$ of a quantum dynamical system α to the corresponding evolved state $|\psi_{t \oplus \delta t}\rangle$. The synchronisation perspective corresponds to saying that whenever the clock is measured to be in clock time state $|t\rangle$, the quantum dynamical system is necessarily in state $|\psi_t\rangle$.

When talking about a **synchronised clock-system state** for a unitary representation α of coherent group $\mathbb{G} = (\circ, \bullet)$, we will mean a state in the following form, and we will refer to ψ_0 as the **initial state** for α:



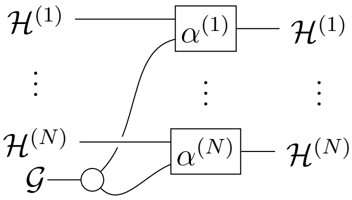
(3.262)

Note that a synchronised clock-system state for α is a stationary state for the time-translationally invariant propagator β associated with α (the one given by Equation 3.256). There is an obvious generalisation to multiple quantum dynamical systems $\alpha^{(1)}, ..., \alpha^{(N)}$ governed by $\mathbb{G}$ and mutually synchronised:



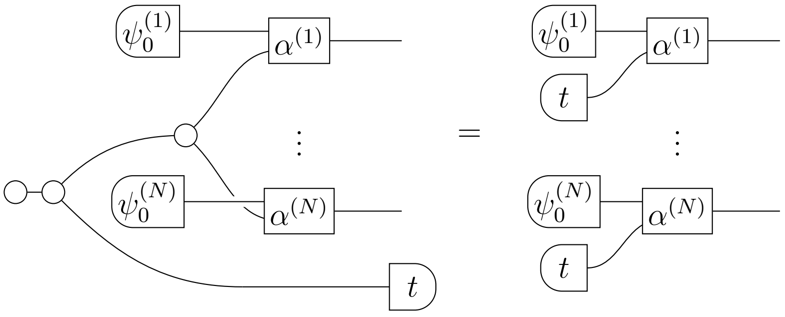
(3.263)

In fact, this is not really a generalisation of the notion of synchronised clock-system state, but rather a special case of it. Indeed, we can obtain Diagram 3.263 from Diagram 3.262 by choosing α to be the following **joint dynamical system** of $\alpha^{(1)}, ..., \alpha^{(N)}$:



(3.264)

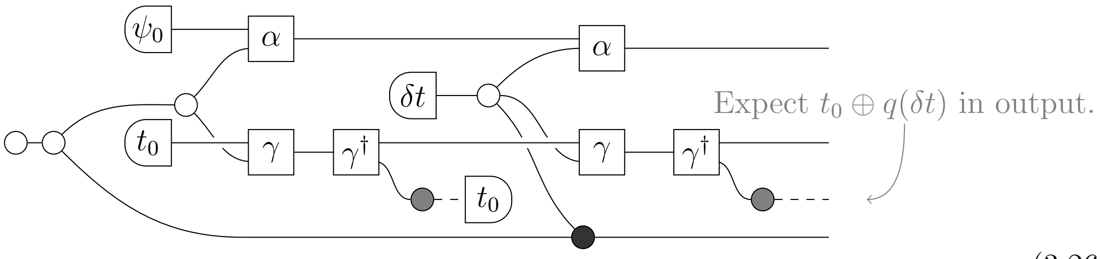
A measurement of the quantum clock $\mathbb{G}$ in the clock time observable results in each systems $\alpha^{(j)}$ collapsing to state $\psi_t^{(j)}$, as one would expect:



(3.265)

One should note that Equation 3.265 is a post-selection on a definite clock time state, and does not necessarily reflect the intuition of looking at a clock to find out what time it is. In short, the situation can be summarised as follows: in the real world, both the quantum system and the quantum clock can be thought to be in turn synchronised with some inaccessible quantum clock ticking time for both of them. Real world clocks, for example, are finite: they model the discrete periodic time of $\mathbb{Z}_T$, ticked at regular intervals and starting again from zero when the clock has gone through all its T time states. With respect to that same regular interval, we could think of an inaccessible external quantum clock as ticking the discrete time of $\mathbb{Z}$, so that synchronisation between the clock and the external clock corresponds to the action $\mathbb{Z} \times \mathbb{Z}_T \to \mathbb{Z}_T$ given by $(\delta t, t_0) \mapsto t_0 \oplus q(\delta t)$, where $q : \mathbb{Z} \to \mathbb{Z}_T$ is the group quotient homomorphism defined by $q(1) = 1 \pmod{T}$. Similarly, the continuous case would involve finite clocks ticking $\mathbb{R}/(T\mathbb{Z})$ time and the external clock ticking $\mathbb{R}$ time, with synchronisation between the two given by the corresponding quotient group homomorphism $q : \mathbb{R} \to \mathbb{R}/(T\mathbb{Z})$.

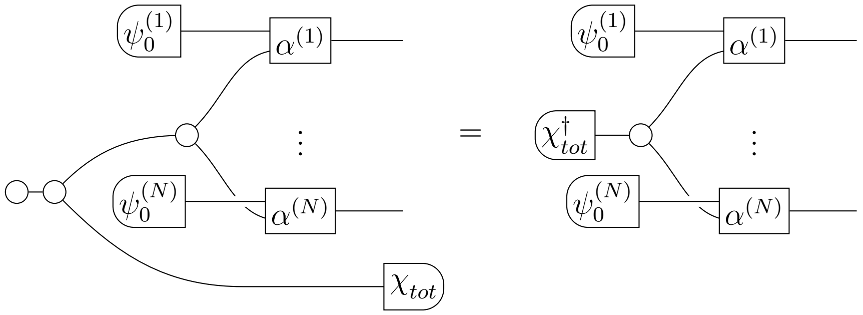
When thinking of a real world synchronised clock-system scenarios, we sometimes have to explicitly consider the inaccessible external clock. For example, consider the following situation (e.g. with the clock ticking $\mathbb{Z}_T$ and the external clock ticking $\mathbb{Z}$ as before). At some point in the external clock time, the (internal) clock is measured to be in clock time state t_0, so that the synchronised system is inferred to be in state $|\psi_{t_0}\rangle$. A certain amount δt of external clock time is then allowed to pass, and the clock is measured again: in a correct modelling of this situation, the clock should be found in clock time state $t_0 \oplus q(\delta t)$, and the system should be inferred to be in state $|\psi_{t_0 \oplus q(\delta t)}\rangle$. This scenario cannot be modelled simply by post-selecting clock time states, because post-selection is a static process and the clock needs to evolve between successive measurements. The correct modelling of this situation goes as follows, where γ is the quantum dynamical system corresponding to the discrete periodic clock (described by the action of $\mathbb{Z}$ on $\mathbb{Z}_T$ above) and α is the quantum dynamical system synchronised with it:



Expect $t_0 \oplus q(\delta t)$ in output.

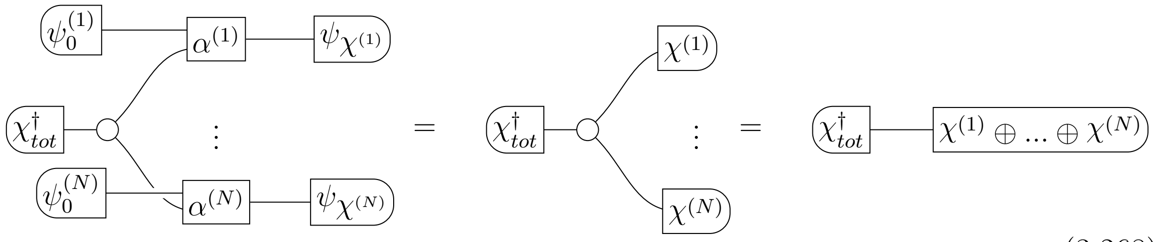
(3.266)

We have given an interpretation to measurement of the quantum clock $\mathbb{G}$ in clock time states. But what if instead we measured a quantum clock, synchronised with one or many systems, in the clock energy observable? We claim that this results in the synchronised systems finding themselves in a global state of definite total energy χ_{tot} given by the outcome of the clock energy measurement:



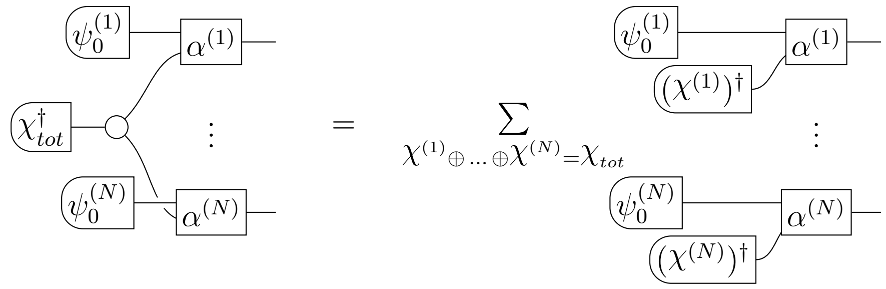
(3.267)

To simplify our life in proving that this interpretation is sound in general, we will (this time only) assume that the energy levels are orthogonal. If we perform a Hamiltonian measurement on systems $\alpha^{(1)}, ..., \alpha^{(N)}$ and obtain energy levels $\chi^{(1)}, ..., \chi^{(N)}$, then a global state in the form of 3.267 imposes the constraint $\chi^{(1)} \oplus ... \oplus \chi^{(N)} = \chi_{tot}$, proving that χ_{tot} behaves exactly like we would expect the total energy of the global dynamical system to behave:



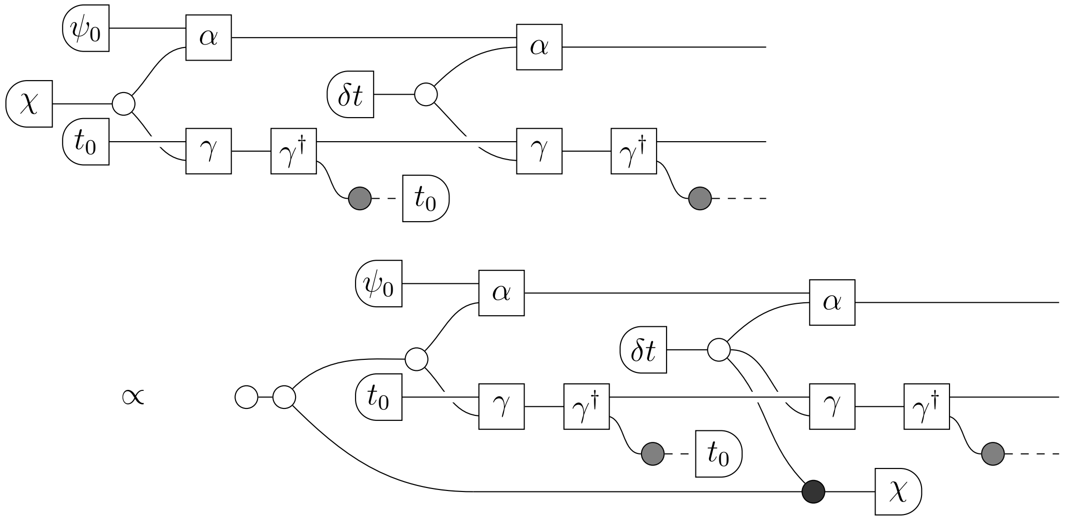
(3.268)

In fHilb, the state of definite total energy given by Equation 3.267 is a superposition of all possible combinations of states of definite energies $\chi^{(1)}, ..., \chi^{(N)}$ for the individual systems, exactly as would be expected:



(3.269)

This whole business of measuring a quantum clock in the clock energy observable also answer a pending question about the inaccessible external clocks we have talked so much about: what is a good way to denote their inaccessibility in the diagrammatic formalism? The answer turns out to lie in the clock energy measurement. For example, we should not have access to the time state of a universal clock (a particularly extreme case of external clock), but we sure can certainly impose the total energy that systems governed by said universal clock should have. Hence the act of making an external clock inaccessible coincides with the act of setting the total energy χ_{tot} for a group of synchronised dynamical systems, as done in Equation 3.267. Indeed, the time translations required to model the incessant marching of universal time can still be performed under post-selection on a total energy state, as long as we are willing to ignore the ensuing global phase:



(3.270)

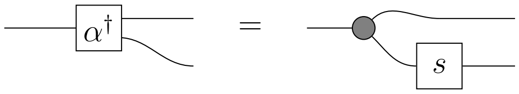
This shows that there is a third way to address the issue of universal clocks: it may well be inevitable that they be made inaccessible in the modelling of any operational scenario, but the discussion above shows that this can be achieved without necessarily turning time into an external classical parameter.

3.6.10 Time observables

The introduction of synchronised clock-system states as modelling the relationship between a quantum dynamical system and the quantum clock governing its dynamics can be related to the problem of time observables. We have seen in the beginning of this Section that positing the existence of a universal quantum clock poses severe issues from both a philosophical and a physical perspective In the previous Subsection we have discussed how such a problem may be solved within our coherent framework, by positing the existence of inaccessible quantum clocks which govern the joint dynamics of the quantum dynamical systems in the various scenarios we might be interested in.

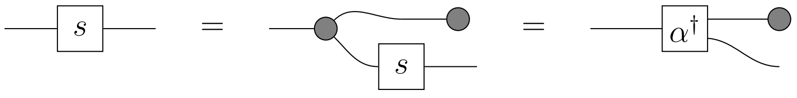
This approach leaves one important question open: how do quantum clocks emerge in the first place? How are they related between themselves? To answer these questions, we will show that certain quantum dynamical systems possess an "internal" time observables, strongly complementary (in a suitable sense) to their Hamiltonian, and that these systems can be turned into quantum clocks governing all other systems in the global synchronised state.

To begin with, if $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{G}$ is a unitary representation of a coherent group $\mathbb{G}$ on an object $\mathcal{H}$, we say that a symmetric †-qSFA ● on $\mathcal{H}$ **internalises** $\alpha^\dagger$ if there is a ●-to-● classical process $s : \mathcal{H} \to \mathcal{G}$ such that:



(3.271)

In fact, if one such s exists then it is necessarily unique:



(3.272)

In the context of quantum dynamical systems, ● will called be an **internal Hamiltonian observable**, or **internal energy observable**: in fHilb, this †-qSFA corresponds to the traditional Hamiltonian observable. If s is an isometry, then we will refer to ● as a **non-degenerate** internal energy observable, because the isometry condition means that the quantum dynamical system has non-degenerate energy eigenspaces. The process s simply maps the energy eigenstates, which act as internal labels for the energy levels of the dynamical system, to the corresponding clock energy states, which are the canonical labels for the energy levels of the dynamical system.

Now that we have candidate clock energy observable for the dynamical system α, we need to find an appropriate clock time observable to match it.

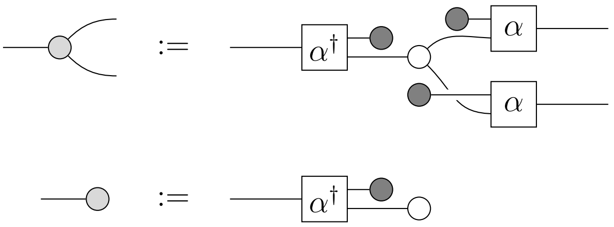
Theorem 3.89 (Internal time observables).
Let $\mathbb{G} := (○, ●)$ be a doubly well-pointed coherent group on a system $\mathcal{G}$ of a †-SMC $\mathcal{C}$, and let α be a unitary representation of $\mathbb{G}$ on a system $\mathcal{H}$. Assume that there is a non-degenerate internal energy observable ◉ having enough classical states. Then the following implications both hold.

(i) If the function $s : K(◉) \to K(●)$ has image which is a subgroup H of $(K(●), ≻○– , ○–)$, then there is a symmetric †-qSCFA ◍ on $\mathcal{H}$ such that $\mathbb{H} = (◍, ◉)$ is a doubly well-pointed coherent group on system $\mathcal{H}$ and $s^\dagger$ is a coherent group homomorphism $s^\dagger : (○, ●) \to (◍, ◉)$.

(ii) Conversely, if $\mathbb{H} = (◍, ◉)$ is a doubly well-pointed coherent group on system $\mathcal{H}$ such that $s^\dagger$ is a coherent group homomorphism $s^\dagger : (○, ●) \to (◍, ◉)$, then $s : K(◉) \to K(●)$ has image which is a subgroup H of $(K(●), ≻○– , ○–)$.

In both cases, $s^\dagger$ restricts to a quotient group homomorphism $s^\dagger : (K(○), ≻●– , ●–) \to (K(◍), ≻◉– , ◉–)$, showing that $(K(◍), ≻◉– , ◉–) \cong (K(○), ≻●– , ●–)/H^\wedge$.

Proof. We begin by proving implication (i). Define –◍≺ and –◍ as follows:



(3.273)

The †-qSCFA ◉ has enough classical states, s is a classical injection on ◉-classical states (because it is an isometry) and it has a subgroup H of $(K(●), ≻○– , ○–)$ as its image. As a consequence, it is immediate to check that –◍≺ and –◍ form, together with their adjoints, a symmetric †-qSFA ◍: one evaluates the equations on ◉-classical states, pushes the states through the classical injection, and checks the validity of the equations for ○, which satisfies all of them because it is a †-qSCFA.

Since the image of the classical map s is a subgroup H of $(K(●), ≻○– , ○–)$, it is also immediate to check that $(≻◍– , ◍–)$ endows $K(◉)$ with the structure of a group: but ◉ has enough classical states, and hence $(◍, ◉)$ is a coherent group. A similar argument can be used to prove that s is a coherent group homomorphism $s : (◉, ◍) \to (●, ○)$, and as a consequence $s^\dagger$ is a coherent group homomorphism $s^\dagger : (○, ●) \to (◍, ◉)$. Finally, ◍ has enough classical states because: (a) $s^\dagger$ is ○-to-◍ classical and surjective on ◍-classical states; (b) ○ has enough classical states; (c) s is an isometry.

The proof of implication (ii) goes along similar lines: if (○, ◍) is a coherent group on $\mathcal{H}$ and $s^\dagger$ is a coherent group homomorphism $s^\dagger$: (○, ●) → (○, ◍), then s must be a coherent group homomorphism s : (◍, ○) → (●, ○), and hence the image of s must be a subgroup H of (K(●), ⟩○– , ○–).

In both cases, $s^\dagger$ restricted to ○-classical states must be a surjective group homomorphism $s^\dagger$: (K(○), ⟩●– , ●–) → (K(○), ⟩◍– , ◍–), hence proving that (K(○), ⟩◍– , ◍–) ≅ (K(○), ⟩●– , ●–)$/H^\wedge$. □

Theorem 3.89 is an extremely important result for this framework: it gives a characterisation of certain quantum dynamical systems which can be taken to behave as quantum clocks, i.e. which can be endowed with the structure of a coherent group which is compatible (via the coherent group homomorphism $s^\dagger$) with the original dynamics. We work out the details of the most general example of this phenomenon in fHilb, for discrete periodic dynamics.

Consider a discrete periodic quantum clock $\mathbb{G}$ in fHilb, given in its most general form by the group algebra $\mathcal{G} := \mathbb{C}[\mathbb{Z}_T]$ for some T, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a quantum dynamical system governed by $\mathbb{G}$, associated to a unitary representation $(U_t)_{t \in \mathbb{Z}_T}$ of $\mathbb{Z}_T$ on $\mathcal{H}$. A non-degenerate internal energy observable ◍ (a †-qSCFA with normalisation factor $N_{◍} = |\mathbb{Z}_T| = |H||H^\wedge|$ fixed by the requirement that $s^\dagger$ be an isometry) exists if we have the following decomposition for the representation, where $H \subseteq \mathbb{Z}_T^\wedge$ is any non-empty subset and $(|\psi_\chi\rangle)_{\chi \in H}$ is an orthogonal basis (the classical states for ◍):

$$U_t := \sum_{\chi \in H} \chi(t) \frac{1}{|H||H^\wedge|} |\psi_\chi\rangle\langle\psi_\chi| \tag{3.274}$$

When H is a subgroup, we can consider the quotient $G' := \mathbb{Z}_T/H^\wedge$, and we label the elements of the quotient by the cosets $t \oplus H^\wedge$ of $H^\wedge$ in $\mathbb{Z}_T$. We can then consider the following family $(|t \oplus H^\wedge\rangle)_{(t \oplus H^\wedge) \in G'}$ of states:

$$|t \oplus H^\wedge\rangle := \sum_{\chi \in H} \chi(t) \frac{1}{|H||H^\wedge|} |\psi_\chi\rangle \tag{3.275}$$

It is not hard to check that the family is an orthogonal basis corresponding to a †-qSCFA ○ on $\mathcal{H}$ (with normalisation factor $N_{○} = 1/|H^\wedge|$ fixed by the requirement that $s^\dagger$ be an isometry):

$$\begin{aligned}\langle s \oplus H^\wedge | t \oplus H^\wedge \rangle &= \sum_{\chi, \chi' \in H} (\chi')^*(s)\chi(t) \frac{1}{|H||H^\wedge|} \frac{1}{N_{◍}} \langle \psi_{\chi'} | \psi_\chi \rangle = \\ &= \frac{1}{|H||H^\wedge|} \sum_{\chi \in H} \chi(t \ominus s) = \begin{cases} \frac{1}{|H^\wedge|} \text{ if } s \oplus H = t \oplus H \\ 0 \text{ otherwise} \end{cases}\end{aligned} \tag{3.276}$$

We want the unit $\bullet\!-$ to be the state $|0 \oplus H^\wedge\rangle$, and indeed our choice of normalisation factors yields the following equality:

$$|H^\wedge|\, {-}\!\bullet \;\circ |t \oplus H^\wedge\rangle = \frac{1}{|H|}\sum_{\chi\in H}\chi(t) = \begin{cases} 1 \text{ if } t = 0 \\ 0 \text{ otherwise} \end{cases} \tag{3.277}$$

The multiplication $\succ\!\!\bullet\!-$ acts as the group multiplication of G' on the family:

$$\succ\!\!\bullet\!- \;\circ \left(|t \oplus H^\wedge\rangle \otimes |s \oplus H^\wedge\rangle\right) = \frac{1}{|H||H^\wedge|}\sum_{\chi\in H}\chi(s\oplus t)|\psi_\chi\rangle = |(s \oplus t) \oplus H^\wedge\rangle \tag{3.278}$$

As a consequence, the pair $\mathbb{G}' := (\circ, \bullet)$ is a doubly well-pointed coherent group on $\mathcal{H}$, with underlying group $[\![\mathbb{G}']\!] = G'$. The map $s^\dagger$ specified by Equation 3.272 is given explicitly as follows, and restricts to the quotient group homomorphism $\mathbb{Z}_T \to \mathbb{Z}_T/H^\wedge$ when evaluated on $\circ\!-$classical states:

$$\begin{aligned} s^\dagger &= \frac{1}{N_\bullet}\sum_{t\in\mathbb{Z}_T}\sum_{\chi\in H}\chi(t)|\psi_\chi\rangle\langle t| = \frac{1}{N_\bullet}\sum_{(t\oplus H^\wedge)\in G'}\;\sum_{t'\in(t\oplus H^\wedge)}\;\sum_{\chi\in H}\chi(t')|\psi_\chi\rangle\langle t'| = \\ &= \sum_{(t\oplus H^\wedge)\in G'}\;\sum_{\chi\in H}\chi(t)\frac{1}{|H||H^\wedge|}|\psi_\chi\rangle\sum_{t'\in(t\oplus H^\wedge)}\langle t'| \;=\; \sum_{(t\oplus H^\wedge)\in G'}|t\oplus H^\wedge\rangle\Big(\sum_{t'\in(t\oplus H^\wedge)}\langle t'|\Big) \end{aligned} \tag{3.279}$$

Theorem 3.89 is a rather general result, but by itself it does not cover all interesting cases of internal time observables: the relationship between external and internal time only involves a quotient, with no space for any kind of "coarsening" of the time being ticket. Indeed, consider consider the following setup with two synchronised clocks: one is a wall clock, ticking 12 hours in intervals of one minute, and one is a chronograph, ticking 24 hours in intervals of 1/100 of a second. It is sensible to say that the wall clock is a dynamical system governed by the chronograph in some appropriate sense, but the relationship between wall clock (internal) time and chronograph (external) time is not simply given by a quotient: first one needs to discretise the chronograph to a digital clock, ticking 24 hours in intervals of one second, and only at that point a quotient can be taken. Mathematically, this amounts to first considering the subgroup $\mathbb{Z}_{86{,}400} \trianglelefteq \mathbb{Z}_{8{,}640{,}000}$ (going from $8,640,000$ 1/100 seconds in 24h to $86,400$ seconds in 24 hours), and then considering the quotient $\mathbb{Z}_{86{,}400} \to \mathbb{Z}_{43{,}200}$ (going from $86,400$ seconds in 24 hours to $43,200$ seconds in 12 hours).

Consider two coherent groups $\mathbb{G}, \mathbb{G}'$ on objects $\mathcal{G}, \mathcal{G}'$ of a †-SMC, and a coherent group homomorphism $f : \mathbb{G}' \to \mathbb{G}'$. If $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ is a unitary representation of $\mathbb{G}$ on $\mathcal{H}$, then it is easy to check that $\gamma := \alpha \circ (id_{\mathcal{H}} \otimes f)$ is a unitary representation of $\mathbb{G}'$

on $\mathcal{H}$. It is possible, therefore, that the assumptions of Theorem 3.89 might not apply to α and $\mathbb{G}$, because H is not a subgroup of $\llbracket \mathbb{G} \rrbracket$, but that the assumptions do apply once we move to γ and $\mathbb{G}'$: in the wall-clock vs chronograph example above, α is the wall clock seen as a system governed by the chronograph $\mathbb{G}$, and γ is the wall clock seen as a system governed by the digital clock $\mathbb{G}'$, a coarsening of the chronograph. We work out the details of this phenomenon in fHilb, for discrete periodic dynamics.

Consider again a discrete periodic doubly well-pointed quantum clock $\mathbb{G}$ in fHilb, given in its most general form by the group algebra $\mathcal{G} := \mathbb{C}[\mathbb{Z}_T]$ for some T, and let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a quantum dynamical system governed by $\mathbb{G}$, associated to a unitary representation $(U_t)_{t \in \mathbb{Z}_T}$ of $\mathbb{Z}_T$ on $\mathcal{H}$. Consider again a non-degenerate internal energy observable $\bullet$ (a †-qSCFA with normalisation factor $N_{\bullet}$) with $H \subseteq \mathbb{Z}_T^{\wedge}$ any non-empty subset and $(|\psi_\chi\rangle)_{\chi \in H}$ the orthogonal basis of classical states for $\bullet$:

$$U_t := \sum_{\chi \in H} \chi(t) \frac{1}{N_{\bullet}} |\psi_\chi\rangle\langle\psi_\chi| \tag{3.280}$$

In this more general case, H is not necessarily a subgroup of $\mathbb{Z}_T^{\wedge}$. Assume, however, that there is a subgroup injection $i : \mathbb{Z}_{T'} \to \mathbb{Z}_T$ (i.e. $T = mT'$ for some $m \in \mathbb{N}^+$), and assume that $H' := \{\chi \circ i \mid \chi \in H\}$ is a subgroup of $\mathbb{Z}_{T'}^{\wedge}$, where we have:

$$\big(\chi \circ i\big)(t') = \chi(m\,t') \tag{3.281}$$

In this context, we could apply Theorem 3.89 to the quantum dynamical system $\gamma := \alpha \circ (id_{\mathcal{H}} \otimes i)$ governed by the quantum clock $\mathbb{G}'$ specified by the group algebra $\mathbb{C}[\mathbb{Z}_{T'}]$ (we have written $i : \mathbb{G}' \to \mathbb{G}$ for the coherent group homomorphism specified by the subgroup injection $i : \mathbb{Z}_{T'} \to \mathbb{Z}_T$).

As a concrete example, we consider the quantum clocks associated with the wall-clock, chronograph and digital clock examples given above. The chronograph corresponds to a quantum clock $\mathbb{G}$ with underlying group $\mathbb{Z}_T$ for $T = 8,640,000$, while the digital clock corresponds to a quantum clock $\mathbb{G}'$ with underlying group $\mathbb{Z}_{T'}$ for $T' = 86,400$. The wall clock as a quantum dynamical system α governed by the chronograph is given by the following unitary representation $(U_t)_{t \in \mathbb{Z}_T}$ (where $(|\psi_k\rangle)_{k=0}^{43,200-1}$):

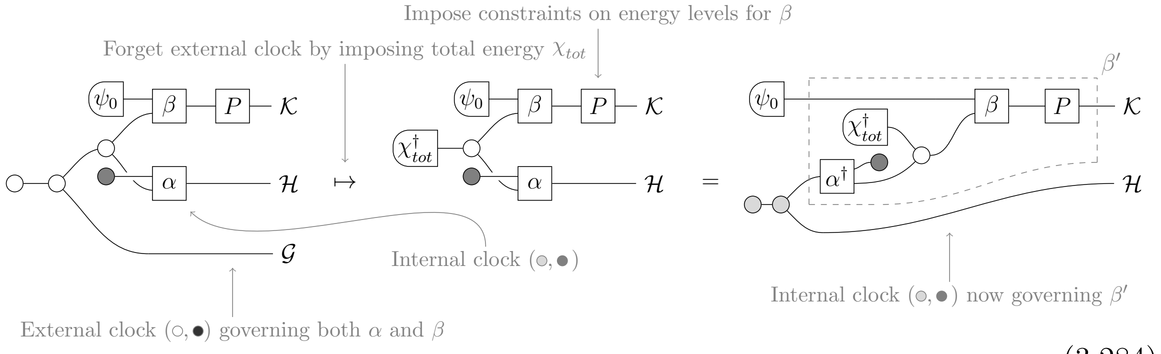
$$U_t := \sum_{k=0}^{43,200-1} e^{i2\pi\frac{2kt}{8,640,000}} |\psi_k\rangle\langle\psi_k| \tag{3.282}$$

The subset $H := \left\{ t \mapsto e^{i2\pi\frac{2kt}{8,640,000}} \,\middle|\, k = 0, ..., 43,200-1 \right\}$ is not a subgroup of $\mathbb{Z}_T$. The wall clock as a quantum dynamical system β governed by the chronograph is given by the following unitary representation $(V_{t'})_{t' \in \mathbb{Z}_{T'}}$:

$$V_{t'} := \sum_{k=0}^{43,200-1} e^{i2\pi \frac{2kt'}{86,400}} |\psi_k\rangle\langle\psi_k| \tag{3.283}$$

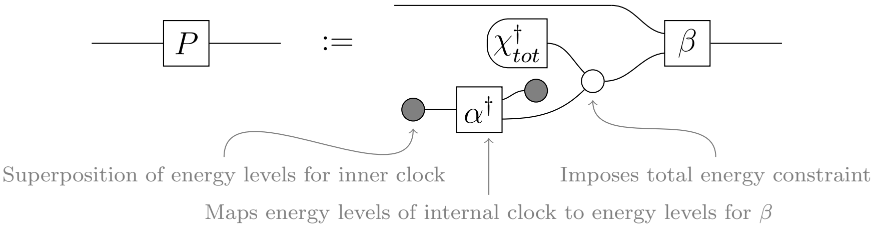
The subset $H' := \left\{ t \mapsto e^{i2\pi \frac{2kt}{86,400}} \;\middle|\; k = 0, ..., 43, 200 - 1 \right\}$ is a subgroup of $\mathbb{Z}_{T'}$, with $(H')^\wedge \cong \mathbb{Z}_2$. We can apply Theorem 3.89 to the wall clock γ governed by the digital clock $\mathbb{G}'$, and we conclude that the wall clock is a quantum clock itself, with underlying group $\mathbb{Z}_{86,400}/\mathbb{Z}_2 \cong \mathbb{Z}_{43,200}$.

We have established above that under certain conditions quantum dynamical systems are quantum clocks, but what use is a clock if it is not synchronised with other dynamical systems? In other words: we have established that certain quantum dynamical systems *have the algebraic structure of* quantum clocks, but we have not yet shown that they *behave operationally as quantum clocks*. Consider the general scenario of Equation 3.267, where quantum dynamical systems $\alpha^{(1)}, ..., \alpha^{(N)}$ are synchronised between themselves and governed by some inaccessible clock, which has been forgotten by setting a total energy χ_{tot} for the systems. If one of the dynamical systems, say $\alpha^{(N)}$, can be turned into a quantum clock by virtue of Theorem 3.89, then we would expect it to govern the remaining dynamical systems $\alpha^{(1)}, ..., \alpha^{(N-1)}$ (we can treat the latter as a single quantum dynamical system β, and we will simply write α for the quantum dynamical system $\alpha^{(N)}$ being promoted to the role of clock). Theorem 3.90 below shows that this is indeed the case, and hence completes the picture on the emergence of quantum clocks: quantum clocks begin their lives as quantum dynamical systems, and rise to the challenge when the quantum clock originally governing their dynamics is forgotten (by imposing a total energy constraint).


Impose constraints on energy levels for β
Forget external clock by imposing total energy χ_{tot}
β'
ψ_0
β
P
$\mathcal{K}$
α
$\mathcal{H}$
$\mathcal{G}$
$\mapsto$
$\chi^\dagger_{tot}$
$=$
$\alpha^\dagger$
Internal clock (◦, •)
Internal clock (◦, •) now governing β'
External clock (○, ●) governing both α and β

(3.284)

In order for this to happen, however, one must first ensure that the quantum dynamical system β is restricted to energy levels which are compatible with the internal clock. This is achieved by the introduction of a projector P onto the subspace spanned by the energy eigenstates for β corresponding to energy levels of the internal clock α (seen as a subgroup of the energy levels of the external clock):


P
$:=$
$\chi^\dagger_{tot}$
β
$\alpha^\dagger$
Superposition of energy levels for inner clock
Imposes total energy constraint
Maps energy levels of internal clock to energy levels for β

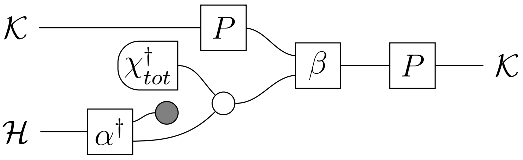
(3.285)

In order to treat the constraint enforced by the projector P in a categorical fashion, we work in the **†-Karoubi envelope** $\mathrm{Split}^\dagger[\mathcal{C}]$ of our original †-SMC $\mathcal{C}$:

1. objects are now pairs $(\mathcal{H}, p)$ where $\mathcal{H}$ is an object of the original category $\mathcal{C}$ and $p : \mathcal{H} \to \mathcal{H}$ is a self-adjoint idempotent (i.e. a projector);
2. morphisms $f : (\mathcal{H}, p) \to (\mathcal{K}, q)$ are exactly the morphisms $f : \mathcal{H} \to \mathcal{K}$ in $\mathcal{C}$ which are invariant under the projectors, i.e. those satisfying $f = q \circ f \circ p$.

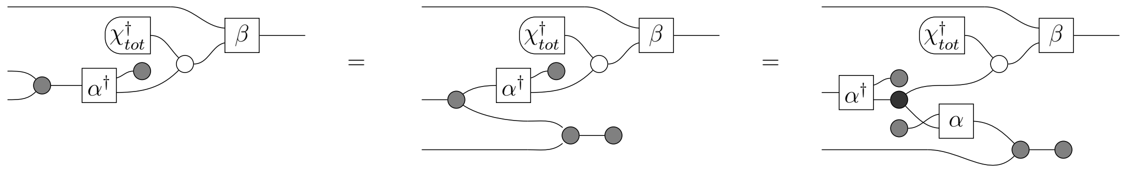
The †-Karoubi envelope is itself a †-SMC, and we can see $\mathcal{C}$ canonically as the full sub-†-SMC of $\mathrm{Split}^\dagger[\mathcal{C}]$ given by objects in the form $(\mathcal{H}, id_{\mathcal{H}})$, which we will simply write as $\mathcal{H}$ when no confusion can arise. In particular, quantum dynamical systems and quantum clocks in $\mathcal{C}$ are also quantum dynamical systems and quantum clocks in $\mathrm{Split}^\dagger[\mathcal{C}]$. Working in $\mathrm{Split}^\dagger[\mathcal{C}]$ is the same as working in $\mathcal{C}$ while additionally enforcing constraints on states (or effects, or processes) specified by the projectors.

Theorem 3.90 (Emerging quantum clocks).
Assume that the "external" quantum clock $\mathbb{G} := (\circ, \bullet)$, the quantum dynamical system α and the associated "internal" quantum clock $\mathbb{H} := (\circ, \bullet)$ are as in Theorem 3.89. Let $\beta : \mathcal{K} \otimes \mathcal{G} \to \mathcal{K}$ be another quantum dynamical system governed by $\mathbb{G}$, and let $P : \mathcal{H} \to \mathcal{H}$ be the map defined by Diagram 3.285. Then P is a self-adjoint idempotent (i.e. a projector), which commutes with β. Furthermore, the following is a quantum dynamical system governed by $\mathbb{H}$ on the object $(\mathcal{K}, P)$ of the †-Karoubi envelope, for all possible choices of total energy $\chi^\dagger \in K(\bullet)$.

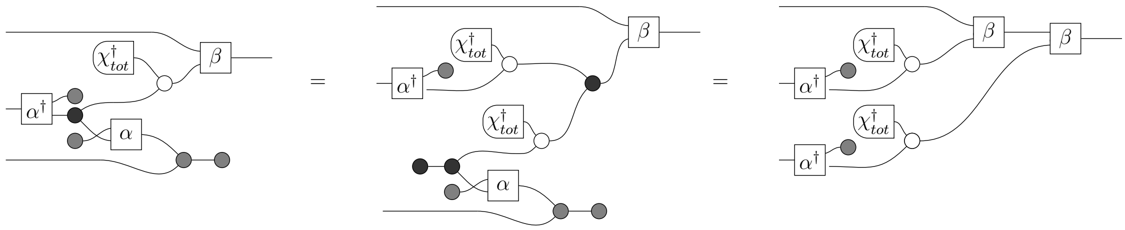


(3.286)

Proof. We being by proving the following multiplicativity result:

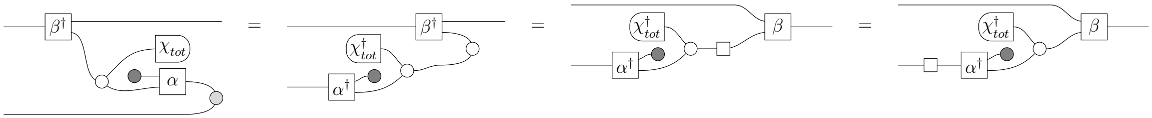


(3.287)



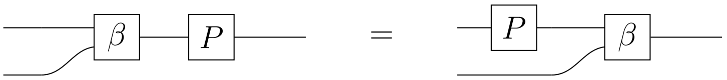
(3.288)

Similarly, we can prove the following inversion result:



(3.289)

Using the results above (and the unit laws for ●), the map P defined in Diagram 3.285 is seen to be a self-adjoint idempotent (i.e. a projector). Similarly, the projector P can be seen to commute with the representation β, in the following sense:



(3.290)

Putting the results above together, we conclude that the map of Diagram 3.286 is a unitary representation of the quantum group $\mathbb{H}$ on the object $(\mathcal{K}, P)$ of the †-Karoubi envelope. □

Once again, we work out the details of this phenomenon in fHilb, for discrete periodic dynamics. Consider a discrete periodic quantum clock $\mathbb{G} := (○, ●)$ in fHilb, given in its most general form by the group algebra $\mathcal{G} := \mathbb{C}[\mathbb{Z}_T]$ for some T. Let $\alpha : \mathcal{H} \otimes \mathcal{G} \to \mathcal{H}$ be a quantum dynamical system governed by $\mathbb{G}$, which is itself a quantum clock $\mathbb{H} := (○, ●)$ given by the group algebra $\mathcal{H} = \mathbb{C}[\mathbb{Z}_{T'}]$ for $T = mT'$, and is related to $\mathbb{G}$ by the quotient group homomorphism $\mathbb{Z}_T \to \mathbb{Z}_{T'}$. Let $\beta : \mathcal{K} \otimes \mathcal{G} \to \mathcal{K}$ be another quantum dynamical system governed by $\mathbb{G}$, associated to a unitary representation $(U_t)_{t \in \mathbb{Z}_T}$ which we write in its most general form as follows:

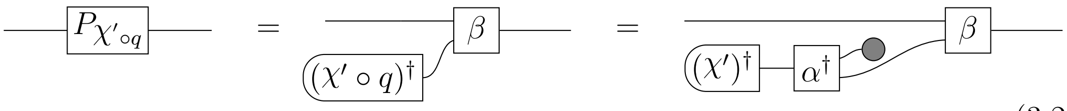
$$U_t := \sum_{\chi \in \mathbb{Z}_T^\wedge} \chi(t) P_\chi \tag{3.291}$$

Now we look at the quantum dynamical system of Diagram 3.286, governed by the quantum clock $\mathbb{H}$; we set total energy $\chi_{tot} \in \mathbb{Z}_T^\wedge$. In terms of energy eigenstates, the map $s : \mathcal{H} \to \mathcal{G}$ takes the following form:

$$s := \frac{1}{T} \sum_{\chi' \in \mathbb{Z}_{T'}^\wedge} |\chi' \circ q\rangle\langle\chi| \qquad (3.292)$$

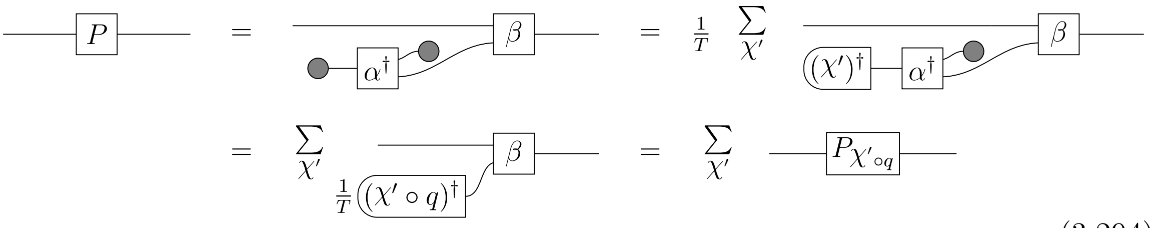
Seen another way, $s : K(\bullet) \to K(\bullet)$ corresponds to the injective group homomorphism $q^\wedge : \mathbb{Z}_{T'}^\wedge \to \mathbb{Z}_T^\wedge$ given by $q^\wedge := \chi' \mapsto \chi' \circ q$, where $q : \mathbb{Z}_T \to \mathbb{Z}_{T'}$ is the quotient group homomorphism given by $q := t \mapsto (t \pmod{T'})$ (recall that the normalisation factor for $K(\bullet)$ is fixed to $N_\bullet = T$, so that $\frac{1}{T}\langle\chi'|\chi''\rangle = \delta_{\chi',\chi''}$).

Without loss of generality and to simplify the discussion, we will take χ_{tot} to be the ground energy level (the general case simply involves a translation $\chi' \circ q \mapsto \chi' \circ q \oplus \chi_{tot}$ of the energy levels for β by χ_{tot}). Consider those energy level $\chi' \circ q$ of the external quantum clock $\mathbb{G}$ which are compatible with some energy level $\chi' \in \mathbb{Z}_{T'}^\wedge$ of the inner quantum clock $\mathbb{H}$. We have the following expression for the projectors onto the eigenspaces of the quantum dynamical system β corresponding to those energy levels:



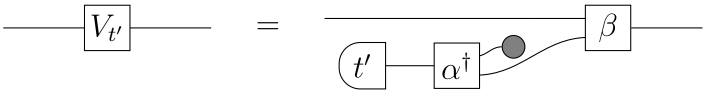
(3.293)

As a consequence, it is immediate to see that the projector P defined by Diagram 3.285 corresponds to the subspace spanned by all the eigenstates of β corresponding to energy levels compatible with the inner quantum clock $\mathbb{H}$:



(3.294)

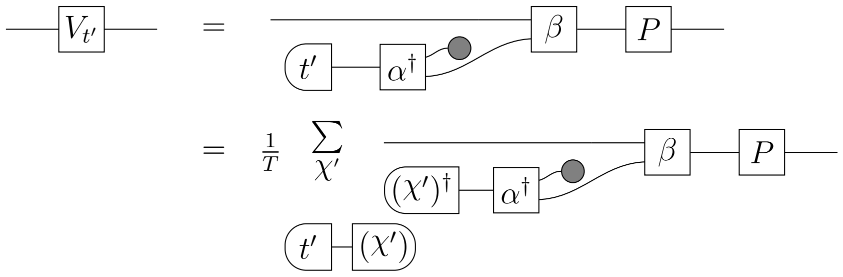
Now write $(V_{t'})_{t' \in \mathbb{Z}_{T'}}$ for the unitary representation of $\mathbb{Z}_{T'}$ on $\mathcal{K}$ corresponding to the quantum group representation given by Diagram 3.286:



(3.295)

Then we get the following explicit expression for the unitary representation $(V_{t'})_{t' \in \mathbb{Z}_{T'}^\wedge}$

describing the quantum dynamical system as governed by the internal quantum clock:



(3.296)

$$= \sum_{\chi'} \chi'(t') P P_{\chi' \circ q} \quad = \quad \sum_{\chi'} \chi'(t') P_{\chi' \circ q}$$

Luckily, this is exactly what we would have expected from Stone's Theorem!

We believe that Theorems 3.89 and 3.90, together with the worked out examples that follow them, provide an interesting new perspective on time observables in quantum theory: they show a sense in which time observables do indeed exist, and how quantum clocks can be seen to emerge from synchronised quantum dynamical systems under appropriate conditions. In particular, we believe to have shed some light on Schrödinger's 1931 conundrum: when a quantum clock $\mathbb{H}$ arises by synchronisation with a ("forgotten", or "inaccessible") external quantum clock $\mathbb{G}$, the dynamics of $\mathbb{H}$ are governed by the external clock energy observable on $\mathbb{G}$, which commutes with the internal time observable on $\mathbb{H}$. In particular, joint eigenstates for the two observables exist, so that the quantum clock $\mathbb{H}$ can be in a definite external clock energy state and a definite internal time state at the same time, exactly as Schrödinger desired.

In describing the mechanism of emergence of quantum clocks, we have provided ways to relate synchronised quantum clocks by increased periodicity and increased discretisation. In our exemplification on finite-dimensional quantum systems with discrete periodic dynamics, increased periodicity corresponds to a group quotient $q : \mathbb{Z}_T \to \mathbb{Z}_{T'}$, while increased discretisation corresponds to a subgroup injection $i : \mathbb{Z}_{T'} \to \mathbb{Z}_T$. The techniques and results we have proven are fully general, and can be straightforwardly extended to other notions of dynamics (e.g. using the non-standard framework for infinite-dimensional CQM presented earlier in this chapter).

Remark 3.91. *As the very last remark to this Section and Chapter, we sketch a brief argument in favour of the construction of a toy model of emergent quantum time for finite-dimensional quantum systems based on discrete periodic dynamics alone: we do so in the hope that it will provide further evidence that the discrete periodic case is worthy of study in itself. The detailed construction of this toy model, including its abstraction and categorification, will be the subject of future work.*

Consider a d-dimensional quantum dynamical system α governed by continuous dynamics, corresponding to a 1-parameter unitary group $(U_t)_{t\in\mathbb{R}}$. Use Stone's Theorem to write the unitary group in the following form, for some $\omega_1, ..., \omega_J \in \mathbb{R}$ and a complete family of orthogonal projectors $(P_j)_{j=1}^J$:

$$U_t = \sum_{j=1}^{J} e^{i2\pi\omega_j t} P_j \tag{3.297}$$

Now consider two strictly increasing sequences of non-zero natural numbers $(Q^{(k)})_{k\in\mathbb{N}}$ and $(R^{(k)})_{k\in\mathbb{N}}$, such that $Q^{(k)}|Q^{(k+1)}$ and $R^{(k)}|R^{(k+1)}$ for all $k \in \mathbb{N}$, and define the following coefficients:

$$a_j^{(k)} := \lfloor \omega_j Q^{(k)} \rfloor \tag{3.298}$$

Now, consider the following families of unitary representations $(U_t^{(k)})_{t\in\mathbb{Z}_{T^{(k)}}}$, $(V_t^{(k)})_{t\in\mathbb{Z}_{S^{(k)}}}$ and $(W_t^{(k)})_{t\in\mathbb{Z}_{S^{(k)}}}$, where $T^{(k)} := Q^{(k)}R^{(k)}$ and $S^{(k)} := Q^{(k+1)}R^{(k)}$:

$$U_t^{(k)} := \sum_{j=1}^{J} e^{i2\pi \frac{a_j^{(k)}}{Q^{(k)}} \frac{t}{R^{(k)}}} P_j \tag{3.299}$$

$$V_t^{(k)} := \sum_{j=1}^{J} e^{i2\pi \frac{a_j^{(k+1)}}{Q^{(k+1)}} \frac{t}{R^{(k)}}} P_j \tag{3.300}$$

$$W_t^{(k)} := \sum_{j=1}^{J} e^{i2\pi \frac{a_j^{(k)}}{Q^{(k)}} \frac{t}{R^{(k)}}} P_j \tag{3.301}$$

Designate by $\alpha_U^{(k)}$, $\alpha_V^{(k)}$ and $\alpha_W^{(k)}$ the corresponding quantum dynamical system, governed by the quantum clocks $\mathbb{C}[\mathbb{Z}_{T^{(k)}}]$ and $\mathbb{C}[\mathbb{Z}_{S^{(k)}}]$. Then the quantum dynamical systems $\alpha_U^{(k)}$ are converging approximations of the quantum dynamical system α, in the sense that as $k \to \infty$ and $t^{(k)}/R^{(k)} \to t \in \mathbb{R}$ we get that $U_{t^{(k)}}^{(k)} \to U_t$ in operator norm.

Consider a scenario in which the quantum clock $\mathbb{C}[\mathbb{Z}_{S^{(k)}}]$ is related to the quantum clock $\mathbb{C}[\mathbb{Z}_{T^{(k+1)}}]$ by increased discretisation, via the subgroup injection $\mathbb{Z}_{Q^{(k+1)}R^{(k)}} \to \mathbb{Z}_{Q^{(k+1)}R^{(k+1)}}$. From the discussion following Theorems 3.89 and 3.90, it is easy to check that quantum dynamical system $\alpha_U^{(k+1)}$, governed by quantum clock $\mathbb{C}[\mathbb{Z}_{T^{(k+1)}}]$, descends to the quantum dynamical system $\alpha_V^{(k)}$, governed by the quantum clock $\mathbb{C}[\mathbb{Z}_{S^{(k)}}]$.

For each value of $t \in \mathbb{Z}_{S^{(k)}}$, the operator norm distance between $V_t^{(k)}$ and $W_t^{(k)}$ is bounded above by $\epsilon^{(k)} := d\frac{1}{Q^{(k)}}$, and tends to zero as k diverges. Hence we can think of $\alpha_W^{(k)}$ as an increasingly precise approximation of $\alpha_V^{(k)}$. Now consider a scenario in which the quantum clock $\mathbb{C}[\mathbb{Z}_{T^{(k)}}]$ is related to the quantum clock $\mathbb{C}[\mathbb{Z}_{S^{(k)}}]$ by increased periodicity, via the group quotient $\mathbb{Z}_{Q^{(k+1)}R^{(k)}} \to \mathbb{Z}_{Q^{(k)}R^{(k)}}$. Again from the discussion *following Theorems 3.89 and 3.90, it is easy to check that quantum dynamical system* $\alpha_W^{(k)}$*, governed by the quantum clock* $\mathbb{C}[\mathbb{Z}_{S^{(k)}}]$ *and* $\epsilon^{(k)}$*-close to* $\alpha_V^{(k)}$*, descends to quantum dynamical system* $\alpha_U^{(k)}$ *governed by quantum clock* $\mathbb{C}[\mathbb{Z}_{T^{(k)}}]$*.*

In conclusion, we have seen that—up to an error in operator norm which vanishes exponentially fast as k *diverges—the quantum dynamical systems* $\alpha^{(k)}$ *form a hierarchy of approximations to the original quantum dynamical system* α*, governed by a hierarchy* $\mathbb{C}[\mathbb{Z}_{T^{(k)}}]$ *of quantum clocks related by progressive increase in discretisation and periodicity, as described by Theorems 3.89 and 3.90.*

Chapter 4

Strong Complementarity in Quantum Algorithms

In the previous Chapter, we have explored the relevance of strong complementarity and the coherent treatment of group and representation theory to the foundations of quantum mechanics; more specifically, we have focused our attention on the symmetry-observable duality following from strong complementarity. In this Chapter, we will develop two new facets of this versatile algebraic property, in their applications to quantum algorithms and protocols.

In Section 4.1, taken from [GK17], we put the connection between strong complementarity and the quantum Fourier transform to work in the first fully diagrammatic, theory-independent proof of correctness for the quantum subroutine of the algorithm solving the Hidden Subgroup Problem (HSP). The abstract nature of our proof allows us to interpret it directly in categories other than fHilb, and our results will provide compelling evidence that strong complementarity is the structural feature powering the quantum subroutine for the abelian HSP. We also obtain interesting new results by interpreting our proof in real quantum theory, hyperbolic quantum theory, finite-field quantum theory and non-standard infinite-dimensional quantum theory.

In Section 4.2, we investigate the special standing of the points $K(\bullet)$ of a well-pointed coherent group $(\bullet, \circ)$ within the larger set of unbiased states for the group structure $\circ$. We put this to work in a broad generalisation of Mermin's non-locality argument for GHZ states, and we provide an exact characterisation of the connection between non-locality and phase groups, bringing the programme started by [CDKW12, CES10] to a close. We relate our findings to the framework of All-vs-Nothing arguments [ABK$^+$15] (a different generalisation of Mermin's argument), and we formulate a non-trivial extension of the quantum-classical secret sharing scheme of Hillery, Bužek and Berthiaume [HBB99] (together with novel device-independent guarantees).

4.1 Hidden Subgroup Problem

The advent of quantum computing promises to solve a number number of problems which have until now proven intractable for classical computers. Amongst these, one of the most famous is Shor's algorithm [Sho95, EJ96]: implemented on a quantum computer, it allows for an efficient solution of the integer factorisation problem and the discrete logarithm problem, the hardness of which underlies many of the cryptographic algorithms which we currently entrust with our digital security (such as RSA and Diffie-Hellman Key Exchange). Integer factorisation and the discrete logarithm, together with Simon's problem [Sim97], Deutsch original algorithm and a number of other number-theoretic questions, turn out to be special cases of the much more general abelian Hidden Subgroup Problem (HSP) [Joz01], and can all be tackled by quantum computers using the same strategy.

The reformulation of Shor's algorithm as a special case of the abelian HSP [Joz01] makes the core issue of order-finding pop out as a group-theoretic question, and highlights the role played by the quantum Fourier transform in solving it [Joz97]. However, it is only with the compelling diagrammatic work of [Vic12b] that the structures and information flow behind the quantum solution to the HSP become apparent: the unitary oracle used in the algorithm is decomposed into its algebraic building blocks, namely certain †-Frobenius algebras, providing a clear topological account of why the procedure works. In this Section, taken from [GK17], we present (Theorem 4.1) the first[1] fully diagrammatic[2] proof of correctness for the quantum algorithm solving the abelian HSP, providing compelling evidence that strong complementarity is indeed the structural feature powering the quantum algorithm.

Furthermore, we exploit the theory independent formulation of our proof to obtain new results in theories other than finite-dimensional quantum theory. We show that Simon's Problem can be efficiently solved in real quantum theory and in hyperbolic quantum theory: the latter result is perhaps more surprising than the former, as hyperbolic quantum theory is a local quasi-probabilistic theory. Theorem 4.2 uses the non-standard infinite-dimensional CQM framework to show that the infinite abelian HSP for $\mathbb{Z}^N$ can be efficiently solved (under suitable assumptions).

[1] The diagrammatics in the proof of [Vic12b] are nothing but straightforward graphical transcriptions of results obtained via traditional representation theory.

[2] Technically, our proof involves a classically-indexed family of diagrams, but this is an accepted standard for fully-diagrammatic treatments of quantum protocols [CK17].

4.1.1 The Hidden Subgroup Problem

The **Hidden Subgroup Problem** (HSP) can be phrased as follows:

(i) a finite group G is fixed;

(ii) we are given an oracle implementing a **subgroup hiding function** $f : G \to \mathbb{Z}_2^N$, which associates to each element of G a **label** in the form of an N-bit string;

(iii) we are promised that the function is constant on (left) cosets of some subgroup $H \leq G$, and associates different labels to different cosets; equivalently, we are promised that f factorises as follows for some injective function s and the quotient group homomorphism q (we refer to this as the **factorisation promise**):

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "q"'] & & \mathbb{Z}_2^N \\ & G/H \arrow[ur, "s"'] & \end{tikzcd} \tag{4.1}$$

(iv) we are asked to find the **hidden subgroup** H.

In the **abelian** HSP we are also promised that G is abelian, while in the more general **normal** HSP we are promised that H is a normal subgroup (a fact which always holds in the abelian HSP). In order for a quantum treatment to be possible at all, one imposes additional requirement on the oracle encoding the subgroup hiding function:

(e) the oracle is given *coherently*, as the following unitary $U_f \in U\left[\mathbb{C}[G] \otimes \mathbb{C}[\mathbb{Z}_2^N]\right]$:

$$U_f := |g\rangle \otimes |t\rangle \mapsto |g\rangle \otimes |f(g) \oplus t\rangle \tag{4.2}$$

where by $\oplus$ we denoted the bit-wise XOR operation on N-bit strings.

A number of important problems arise as special instances of the abelian HSP. In the Discrete Logarithm problem, one is given a prime number p, a primitive root g mod p, and a number a such that $a = g^b \pmod{p}$ for some unknown b to be found. This is an instance of the abelian HSP with group $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, hidden subgroup $H = \mathbb{Z}_{p-1} \cdot (b, 1) \trianglelefteq G$ and subgroup hiding function $f(x, y) = g^x a^{-y} \pmod{p}$.

In the Integer Factorisation problem, one is given a composite number N and is asked to provide a non-trivial factorisation for it. Shor's algorithm solves the problem efficiently on quantum computers: its core is the order-finding subroutine, which considers an integer a coprime[3] with N, and asks for the order of a as a multiplicative unit modulo N. The order-finding subroutine is an instance of the abelian HSP with group $G = \mathbb{Z}_N^\times$ (the abelian group of multiplicative units modulo N)[4], hidden subgroup

[3] If $a \in \{2, ..., N-1\}$ is not coprime with N, then we already have a non-trivial factorisation of N.

[4] In practice one uses $\mathbb{Z}_{2^M}$: if $M \gg \log_2 N$, the errors due to the inexact period of a will be small.

$H = \langle a \rangle \cong \mathbb{Z}_{\mathrm{ord}(a)}$ and subgroup hiding function $f(x) = a^x \pmod N$.

In Simon's problem, one is given a function $f : \mathbb{Z}_2^N \to \mathbb{Z}_2^N$ with the promise that the stabilizer subgroup for f has order 2: there is a unique non-zero string $z \in \mathbb{Z}_2^N$, which we are asked to find, such that for any two N-bit strings $x, y \in \mathbb{Z}_2^N$ we have that $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus z$. The importance of Simon's problem in the complexity of quantum computing lies in a result [BV97] stating that, relative to oracles with the promise above, Simon's problem separates BQP (the class of bounded-error quantum polynomial time problems) from BPP (the class of bounded-error classical polynomial time problems). Simon's problem is clearly an instance of the abelian HSP, with $G = \mathbb{Z}_2^N$, hidden subgroup $H = \langle z \rangle = \{0, z\}$ and subgroup hiding function f.

4.1.2 The Quantum Algorithm

For the fully diagrammatic version of the proof, we replace the concrete Hilbert space setting with four assumptions about the †-SMC $\mathcal{C}$ we want to implement the protocol in, and the strongly complementary pairs that it possesses.

(a) There exist strongly complementary pairs encoding the four relevant finite abelian groups: the group G, the hidden subgroup H, the quotient group G/H and the group of N-bit strings $\mathbb{Z}_2^N$. That is, there exists a strongly complementary pair $(\circ_K, \bullet_K)$ on object $\mathcal{H}_K$ such that $K \cong (K(\circ_K), \succ\!\!\bullet\!-_K, \bullet\!-_K)$, for each $K = G, H, G/H, \mathbb{Z}_2^N$.

(b) The †-SMC we are working with has an absorbing scalar 0, i.e. we can define a sensible notion of impossibility in it.

(c) $\circ_H$ and $\circ_{G/H}$ have enough classical states.

(d) $\bullet_G$ and $\circ_{\mathbb{Z}_2^N}$ have enough classical states, and their classical states are orthogonal—this is so that measurement in either observable can be properly interpreted as a process with classical output in the CP* category CP*[$\mathcal{C}$] modelling the full quantum-classical theory[5].

As a matter of convenience, we also assume the point structures $\circ_K$ to be special, though this is not crucial to the proof. We denote by $\xi_K^\dagger \xi_K$ the normalisation factor of the group structures $\bullet_K$ (which are quasi-special).

[5] Because the procedure results in uniform sampling, we don't really need to ask for any specific semiring structure on the space of measurement outcomes.

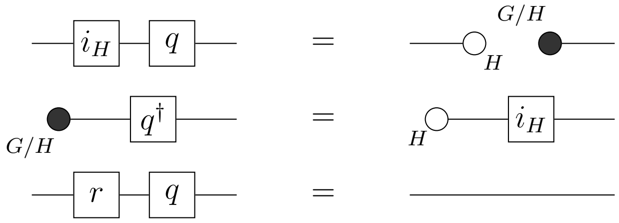
Much of the proof relies on the fact that the quotient map $q : G \to G/H$ is a very specific group homomorphism, defined by the following three properties:

(a) q identifies enough elements of G to send all of H to the group unit;

(b) q does not send any elements other than those in H to the group unit;

(c) q is surjective.

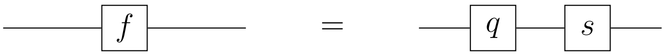
As a consequence, we require that there exists a morphism $q : \mathcal{H}_G \to \mathcal{H}_{G/H}$ satisfying the three graphical properties below, where $r : \mathcal{H}_{G/H} \to \mathcal{H}_G$ is a $\circ_{G/H}$-to-$\circ_G$ classical isometry (a section for q, witnessing its surjectivity), and $i_H : \mathcal{H}_H \to \mathcal{H}_G$ is a $\circ_H$-to-$\circ_G$ classical isometry (modelling the group homomorphism injecting H into G):



(4.3)

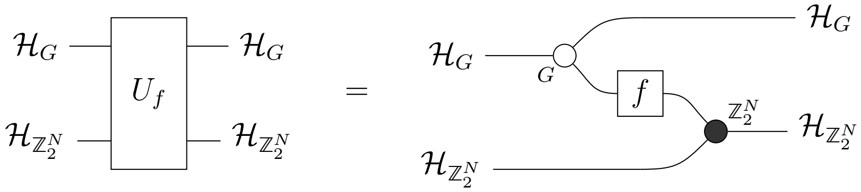
Again as a matter of notational convenience, we will henceforth choose coset representatives so that the map r sends the $\circ_{G/H}$-classical state corresponding to coset $g_b H \in G/H$ to the $\circ_G$-classical state corresponding to element $g_b \in G$.

We begin by constructing an abstract version of the unitary oracle U_f given in Equation 4.2. We replace the subgroup hiding function $f : G \to \mathbb{Z}_2^N$ (or, to be precise, its linear extension $f : \mathbb{C}[G] \to \mathbb{C}[\mathbb{Z}_2^N]$) with a $\circ_G$-to-$\circ_{\mathbb{Z}_2^N}$-classical map $f : \mathcal{H}_G \to \mathcal{H}_{\mathbb{Z}_2^N}$, which is required to satisfy an appropriate factorisation promise, where q is the quotient map defined above and $s : \mathcal{H}_{G/H} \to \mathcal{H}_{\mathbb{Z}_2^N}$ is a $\circ_{G/H}$-to-$\circ_{\mathbb{Z}_2^N}$-classical isometry (modelling the subgroup labelling function, which was originally injective)



(4.4)

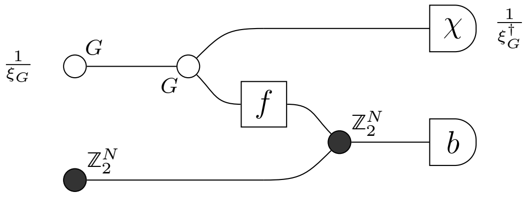
The unitary oracle U_f can then be decomposed as follows, in terms of a coherent copy operations for G, a coherent multiplication operations for $\mathbb{Z}_2^N$, and the coherent subgroup hiding function f:


$\mathcal{H}_G$
U_f
$\mathcal{H}_G$
$\mathcal{H}_{\mathbb{Z}_2^N}$
$\mathcal{H}_{\mathbb{Z}_2^N}$
=
$\mathcal{H}_G$
$\mathcal{H}_G$
G
f
$\mathbb{Z}_2^N$
$\mathcal{H}_{\mathbb{Z}_2^N}$
$\mathcal{H}_{\mathbb{Z}_2^N}$

(4.5)

The process U_f defined above is always unitary, and on finite-dimensional quantum systems it coincides with the oracle we explicitly defined in Equation 4.2 [Vic12b].

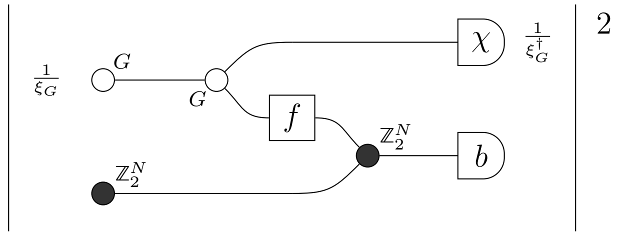
The following diagram presents the quantum subroutine in its entirety: the initial state is prepared, the unitary oracle is applied, and two outcomes $b \in \mathbb{Z}_2^N$ and $\chi \in G^\wedge$ are obtained from the measurements performed on the two parts of the resulting state:



(4.6)

The diagram given above is a scalar $c_{b,\chi}$, and we interpret its square absolute value as the probability $\mathbb{P}(b, \chi) = c_{b,\chi}^\dagger c_{b,\chi}$ of obtaining the joint measurement outcome (b, χ). We will now provide a fully diagrammatic proof that the probability must be zero if $b \notin \operatorname{im} s$ or if $\chi \notin \operatorname{Ann}[H]$, and it must otherwise be non-zero and independent of b and χ. In other words, we wish to show that the procedure produces a uniformly random sampling of the annihilator of H.

Theorem 4.1 (Abelian HSP in †-SMCs).
The quantum subroutine for the (abelian) HSP can be carried out in any †-SMC satisfying the assumptions presented above:



$$= \begin{cases} \frac{(\xi_H^\dagger \xi_H)^2}{(\xi_G^\dagger \xi_G)^2} & \textit{if } b \in \operatorname{im} s,\ \chi \in \operatorname{Ann}[H] \\ 0 & \textit{otherwise} \end{cases}$$

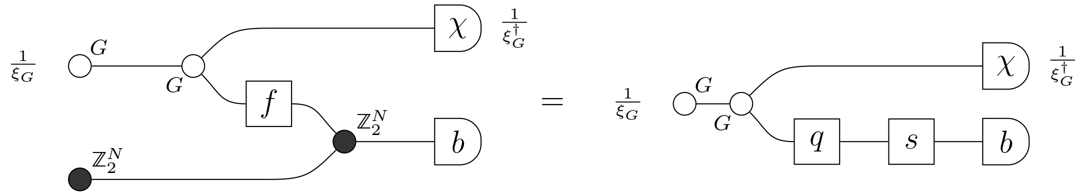
(4.7)

In the case of finite-dimensional quantum systems, we have $\xi_K^\dagger \xi_K = |K|$ for any finite group K, and hence the scalar appearing on the RHS is $|H|^2/|G|^2$.[6]

Proof. We divide the proof into several steps: (i) we use the factorisation promise to break f into its constituent components q and s, and we eliminate the coset label $b \in \mathbb{Z}_2^N$ by assuming it is into the image of s; (ii) we show that non-annihilator outcomes $\chi \notin \operatorname{Ann}[H]$ are impossible; (iii) in the case of annihilator outcomes $\chi \in \operatorname{Ann}[H]$, we explicitly introduce the abstract equivalents of the coset states $|\chi\rangle := \sum_{g \in G} \chi(g)|g\rangle$ appearing in the original quantum version; (iv) we annihilate the coset states and obtain the final probabilities.

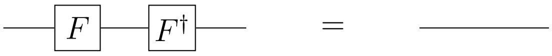
[6] This is what we expect: there are $|G/H| = |G|/|H|$ distinct b in the image of $s : G/H \to \mathbb{Z}_2^N$ (because s is injective), and the annihilator of H itself has size $|G|/|H|$, leading to a total of $|G|^2/|H|^2$ possible joint measurement outcomes (b, χ).

Using the Factorisation Promise. As our first manipulation step, we can substitute the promised factorisation of f into $s \circ q$, and use the unit law to remove the †-qSCFA $\bullet_{\mathbb{Z}_2^N}$ from the diagram:



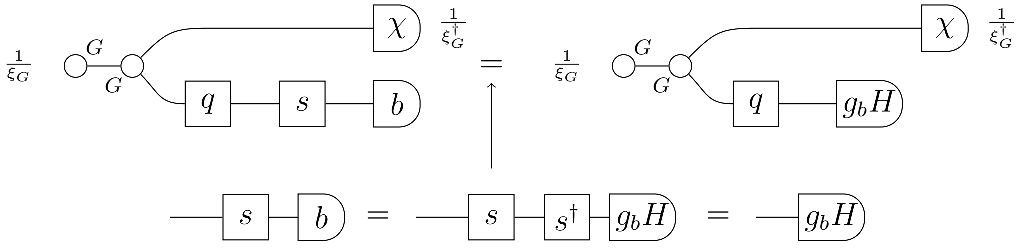
(4.8)

The property of process $s : \mathcal{H}_{G/H} \to \mathcal{H}_{\mathbb{Z}_2^N}$ being an isometry can be readily formulated diagrammatically as follows:



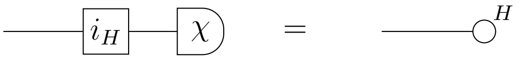
(4.9)

Because s is a $\circ_{G/H}$-to-$\circ_{\mathbb{Z}_2^N}$ classical map, and because $\circ_{G/H}$ has enough classical states and the classical states of $\circ_{\mathbb{Z}_2^N}$ are orthogonal, then we have the following: a $\circ_{\mathbb{Z}_2^N}$-classical state b is either in the image of s, i.e. $b = s \circ (g_b H)$ for some classical state $g_b H$, or we have that $b^\dagger \circ s = 0$ is the impossible process, i.e. b is never observed as outcome. Our second manipulation step then assumes that the outcome $b \in \mathbb{Z}_2^N$ is in the image of s, and uses the isometry property to remove s from the diagram altogether:



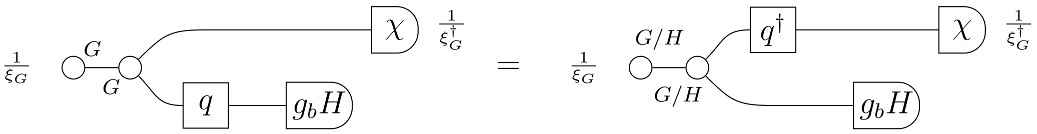
(4.10)

Excluding the Non-Annihilator Outcomes. As our next step, we want to show that the diagram evaluates to 0 whenever χ is not in the annihilator of H. To do so, we first need a graphical definition of what it means for a character χ to annihilate H:



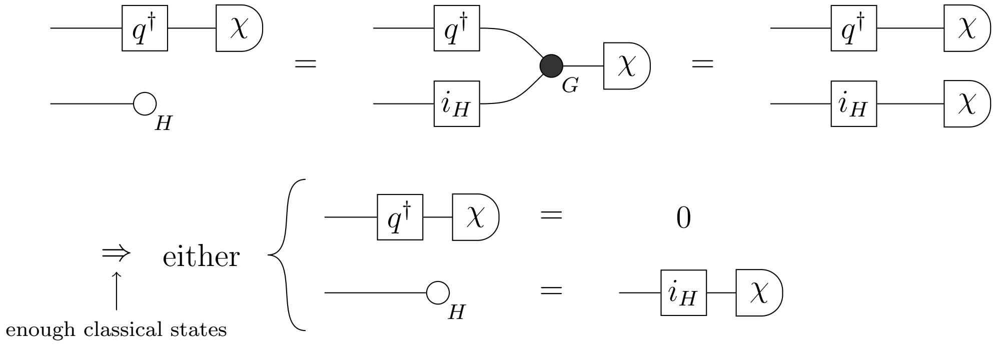
(4.11)

We begin by moving q from the lower to the upper branch, by using the fact that it is $\circ_G$-to-$\circ_{G/H}$ classical:



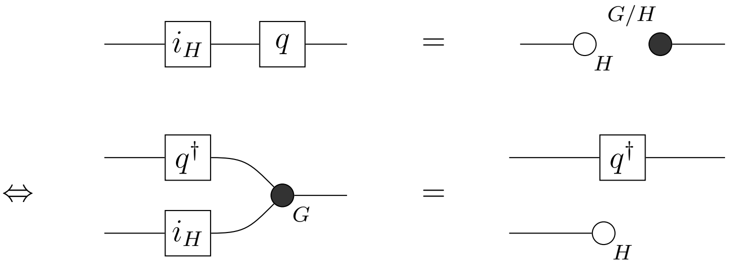
(4.12)

We then proceed to show, by case analysis, that either $\chi^\dagger \circ q^\dagger = 0$ (and hence that the entire diagram vanishes), or that the character χ is in the annihilator of H (according to the graphical definition of Equation 4.11):



(4.13)

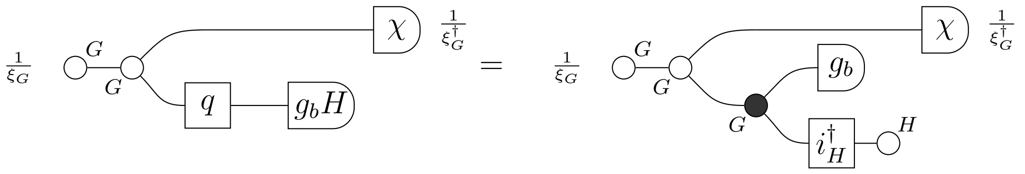
The first equality is a consequence of the following equivalent reformulation of a defining property of the quotient map q:



(4.14)

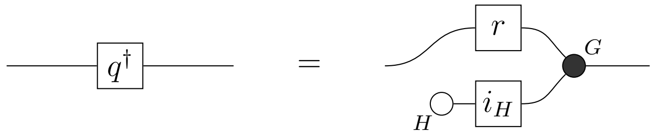
The equivalence between the two versions can be proven by using the same general technique which is used in Equation 4.18 below.

Introducing the Coset States. Having excluded the case where $\chi \notin \mathrm{Ann}[H]$ (a fact which won't really be needed until the next subsection), our third manipulation step goes as follows:



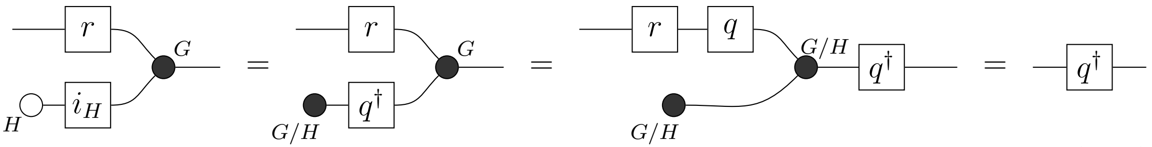
(4.15)

We removed both $q^\dagger$ and the state $g_b H$ of $\mathcal{H}_{G/H}$ from the diagram, and replaced them with an abstract version of the **coset state** $\sum_{h \in H} |g_b \cdot h\rangle$ of $\mathcal{H}_G$, by using the following result:



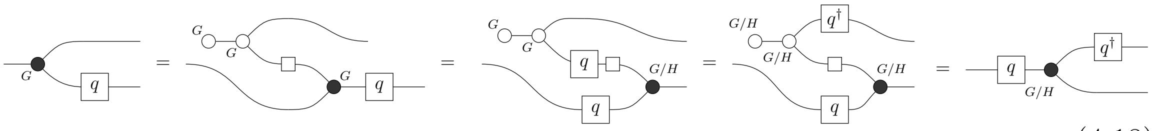
(4.16)

The equality above can be proven diagrammatically using the defining properties of q:



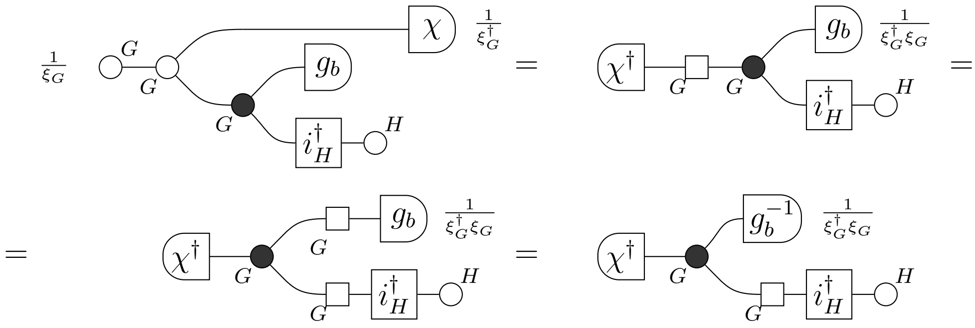
(4.17)

More in detail, the second equation in the chain is proven by using the fact that q is a $(\circ_G, \bullet_G)$-to-$(\circ_{G/H}, \bullet_{G/H})$ homomorphism, by replacing the antipode with its definition, and by appealing to the fact that the antipode is self-inverse:

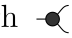


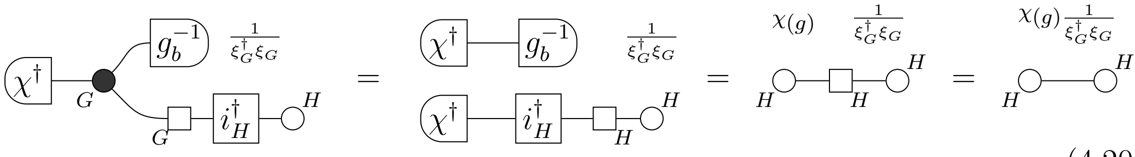
(4.18)

Annihilating the Coset States. We are now in the situation where χ is in the annihilator of H, and we have rewritten our diagram explicitly in terms of coset states. As our fourth manipulation step, we turn the character around to obtain (the adjoint of) a diagram involving a character evaluated on a coset state:



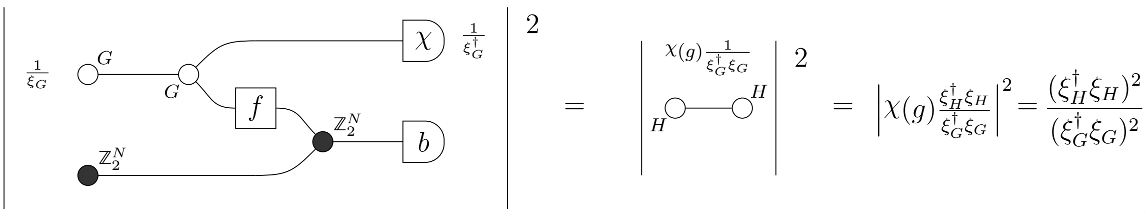
(4.19)

Because the character is multiplicative (its adjoint is a $\bullet_G$-classical state), we can copy it through  $_G$. Evaluating against g_b^{-1} removes the first copy to give some phase $\chi(g)$, satisfying $\chi(g)^\dagger \chi(g) = 1$, while the definition of the annihilator removes the second copy together with $i_H^\dagger$:


$\chi^\dagger$
G
g_b^{-1}
$\frac{1}{\xi_G^\dagger \xi_G}$
G
$i_H^\dagger$
H
=
$\chi^\dagger$
g_b^{-1}
$\frac{1}{\xi_G^\dagger \xi_G}$
$\chi^\dagger$
$i_H^\dagger$
H
H
=
$\chi(g)$
$\frac{1}{\xi_G^\dagger \xi_G}$
H
H
H
=
$\chi(g)$
$\frac{1}{\xi_G^\dagger \xi_G}$
H
H

(4.20)

We are left with a bunch of explicit scalars, and we can finally evaluate the square absolute value of Diagram 4.6 to obtain our desired result:


$\frac{1}{\xi_G}$
G
G
χ
$\frac{1}{\xi_G^\dagger}$
f
$\mathbb{Z}_2^N$
$\mathbb{Z}_2^N$
b
2
=
$\chi(g)\frac{1}{\xi_G^\dagger\xi_G}$
H
H
2
$= \left|\chi(g)\frac{\xi_H^\dagger\xi_H}{\xi_G^\dagger\xi_G}\right|^2 = \frac{(\xi_H^\dagger\xi_H)^2}{(\xi_G^\dagger\xi_G)^2}$

(4.21)

The evaluation of the square norm ○–$^\dagger_H$ ∘ ○–$_H$ to $\xi_H^\dagger\xi_H$ comes from the fact that ○–$_H$ is ●$_H$-classical, and the latter has $\xi_H^\dagger\xi_H$ as normalisation factor.

□

4.1.3 Non-abelian HSP

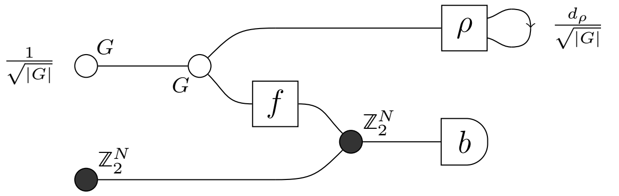
Quantum algorithms to solve the HSP have been studied beyond the abelian case. An extension of the efficient quantum solution to the case of normal subgroups of non-abelian groups is given by [HRTS00], while [MRS08, HRS10] provide a no-go theorem showing that the same techniques cannot be used to formulate an efficient quantum solution to the general non-abelian case. The general non-abelian case is important because two interesting problems of classical computational complexity arise as special cases: the Graph Isomorphism Problem arises as a special case of the HSP on symmetric groups [HRTS00], while the Unique Shortest Vector Problem (uSVP) arises as a special case of the HSP on dihedral groups [Reg04b]. The latter forms the basis of a public key cryptosystem [Reg04a] which, subject to quantum intractability of the HSP on dihedral groups, is a candidate to replace RSA in post-quantum cryptography (as are many other lattice-based cryptographic algorithms).

Nowhere in our proof above we have explicitly used commutativity of the †-qSCFAs (equivalently, the fact that G and H are abelian), and our approach naturally generalises to the case where G is a finite group and H a normal subgroup (a necessary requirement in this approach, which explicitly uses a group structure on G/H). For the sake of simplicity, and because no hard result will be proven, we will stick to the case of finite-dimensional Hilbert spaces for the remainder of this Section.

Going from commutative to general quasi-special †-Frobenius algebras (†-qSFA) has the following implication: the classical states are still the multiplicative characters, and they are still orthogonal, but they no longer form a basis. Instead, the †-qSFA is now associated with a potentially degenerate observable: sampling it will produce, as classical output, the character χ_ρ of an irreducible representation ρ of G, with the following probability (where d_ρ is the dimension of representation ρ):

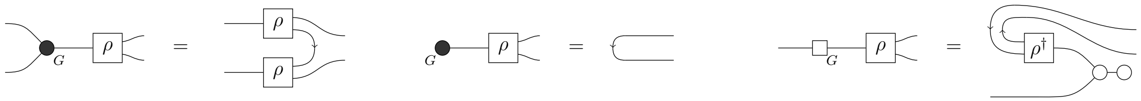
$$\mathbb{P}[b, \chi_\rho] = \begin{cases} \frac{|H|^2}{|G|^2} d_\rho^2 & \text{if } \rho(h) = 0 \text{ for all } h \in H \\ 0 & \text{otherwise} \end{cases} \tag{4.22}$$

For our graphical proof to go through, Diagram 4.6 needs to be modified as follows:



(4.23)

where we used the dagger-compact structure to take the trace of the irreducible representation $\rho : \mathbb{C}[G] \to V_\rho^* \otimes V_\rho$ (technically, its linear extension from G to $\mathbb{C}[G]$). The defining properties of multiplicative characters generalise to representations, as shown by [Vic12b]:



(4.24)

However, the generalisation from the abelian to the non-abelian case encounters a much bigger hurdle in the classical post-processing: the logarithmic dependency of the number of generators on the size of the group only need to hold in the abelian case, and the number of samples required is in general linear in the size of the group (and hence exponential in the size of its description) [HRS10]. This is a separate problem, interesting in its own right, and is beyond the scope of this work.

4.1.4 Toy quantum theories

The fully diagrammatic, abstract character of our approach means that our results can be directly applied to theories other than quantum theory, as long as they feature the relevant algebraic structure. Specifically, we consider theories of wavefunctions valued in some commutative involutive semirings S (generalising the complex-valued wavefunctions of ordinary quantum theory). This is a large family, and a number of concrete examples were given in Chapter 2.

In order for the quantum HSP algorithm for some finite group G to be implementable in S-Mat, we need two conditions to be satisfied:

(i) we need G, H, G/H and $\mathbb{Z}_2^N$ to all admit strongly complementary pairs in S-Mat, with enough points in the case of H, G/H and $\mathbb{Z}_2^N$;

(ii) we need $\bullet_G$ to have enough classical states: this is a non-trivial condition, depending entirely on the structure of S-valued multiplicative characters for the group G (it is still necessary for G to be abelian, but no longer sufficient).

Even when the quantum algorithm can be implemented, it is worth noting that the S-valued multiplicative characters arising in S-Mat may be very different from the complex-valued ones arising in the traditional implementation, and it is in general non-trivial to check that the classical post-processing part of the algorithm will go through as expected.

4.1.4.1 Real quantum theory

Real quantum theory is the theory $\mathbb{R}$-Mat of real-valued wavefunctions, where $\mathbb{R}$ is equipped with the identity as its involution. Because $\mathbb{R}$ is a field, every finite group K admits a strongly complementary pair $(\circ_K, \bullet_K)$ in $\mathbb{R}$-Mat with enough points. The real-valued characters of a group G are a subset of the complex valued ones, an observation which has two consequences: (i) the finite abelian groups G which admit an implementation of the quantum algorithm to solve the HSP are those possessing only real-valued multiplicative characters, i.e. those in the form $G \cong \mathbb{Z}_2^N$; (ii) the classical post-processing goes through as in the traditional implementation, without additional issues.

Hence real quantum theory admits efficient solutions to the HSP on $\mathbb{Z}_2^N$, and in particular to Simon's problem. This furthermore implies that the class $\mathrm{BQP}_{\mathbb{R}}$ (by which we mean BQP for Real Quantum Theory) is separated from BPP relative to oracles with the appropriate promise (see [DeB14] for a detailed study of computational complexity in some toy quantum theories modelled by S-Mat constructions).

4.1.4.2 Hyperbolic quantum theory

Hyperbolic quantum theory is the theory $\mathbb{C}[\sqrt{1}]$-Mat of wavefunctions valued in the *split complex numbers* $\mathbb{C}[\sqrt{1}] := \mathbb{R}[X]/(X^2 - 1)$, a two-dimensional real algebra. Split complex numbers take the form $(x + jy)$, where $x, y \in \mathbb{R}$ and $j^2 = 1$; in particular, they have non-trivial zero-divisors in the form $a(1 \pm j)$, because $(1+j)(1-j) = 1 - j^2 = 0$. They come with the involution $(x + jy)^* := x - jy$, making Hyperbolic Quantum Theory a quasi-probabilistic theory (i.e. it has signed probabilities) and a local theory (because its scalars form a field).

The split complex numbers contain $\mathbb{R}$ as a subfield fixed by the involution, and hence all protocols which can be implemented in real quantum theory can also be implemented in hyperbolic quantum theory. In particular, the HSP on $\mathbb{Z}_2^N$ can be efficiently solved in hyperbolic quantum theory. There are no other finite abelian groups for which the HSP can be solved efficiently; however, hyperbolic quantum theory admits—similarly to ordinary quantum theory and in contrast to real quantum theory—implementations of the HSP for the infinite abelian groups $\mathbb{Z}^N$.

4.1.4.3 Finite-field quantum theory

If $\mathbb{F}_{p^n}$ is a finite field (with p odd) and ε is a primitive element, then we can consider the ring $\mathbb{F}_{p^n}[\sqrt{\varepsilon}] := \mathbb{F}_{p^n}[X^2 - \varepsilon]$, equipped with the involution $(x + y\sqrt{\varepsilon})^* := (x - y\sqrt{\varepsilon})$. Because ε is a primitive element, $\mathbb{F}_{p^n}(\sqrt{\varepsilon}) \cong \mathbb{F}_{p^{2n}}$ is a field. We are thus working with the quadratic extension of fields $\mathbb{F}_{p^n}(\sqrt{\varepsilon})/\mathbb{F}_{p^n}$, equipped with the usual involution and (squared) norm from Galois theory:

$$\left|x + y\sqrt{\varepsilon}\right|^2 = (x - y\sqrt{\varepsilon})(x + y\sqrt{\varepsilon}) = x^2 - \varepsilon y^2 \tag{4.25}$$

The finite abelian groups K admitting a strongly complementary pair $(\circ_K, \bullet_K)$ with enough points in $\mathbb{F}_{p^n}(\sqrt{\varepsilon})$-Mat are exactly those with order not divisible by p. Furthermore, the group of phases in finite-field quantum theory is isomorphic to the finite abelian group $\mathbb{Z}_{p^n+1}$: as a consequence, the finite abelian groups G such that $\bullet_G$ has enough classical states are exactly those in the form $G \cong \prod_{k=1}^{K} \mathbb{Z}_{p_k^{e_k}}$, with $p_k^{e_k} | p^n + 1$ for all $k = 1, ..., K$ (which, in particular, have order not divisible by p). Finally, the $\mathbb{F}_{p^n}(\sqrt{\varepsilon})$-valued multiplicative characters can be easily interpreted as complex-valued multiplicative characters (using the subgroup $\mathbb{Z}_{p^n+1}$ of the circle group given by the $(p^n + 1)$-th roots of unity), and the classical post-processing phase of the algorithm goes through without additional issues.

4.1.4.4 p-adic quantum theory

The phases in p-adic quantum theory form a multiplicative abelian group C_ε isomorphic to the additive group $\mathbb{Z}_{p+1} \times pZ_p$, where $(\mathbb{Z}_{p+1}, +, 0)$ are the integers modulo $p + 1$, while $(pZ_p, +, 0)$ is the additive subgroup of Z_p formed by those p-adic integers which are divisible by p. As a consequence, a finite abelian group G gives rise to a group structure $\bullet_G$ with enough classical states if and only if $G \cong \prod_{k=1}^{K} \mathbb{Z}_{p_k^{e_k}}$, with $p_k^{e_k} | p+1$ for all $k = 1, ..., K$—just as in the finite-field quantum theory $\mathbb{F}_p(\sqrt{\varepsilon})$-Mat. Similarly, the $Q_p(\sqrt{\varepsilon})$-valued multiplicative characters can be easily interpreted as complex-valued, and the classical post-processing of the algorithm for the HSP goes through as in the traditional case.

4.1.4.5 Relational quantum theory

Relational quantum theory is the theory of boolean-valued wavefunctions, or more generally of wavefunctions valued in a locale Ω (with the identity as involution). It is modelled by the dagger compact category Ω-Mat, and in the boolean case it coincides with the category fRel of finite sets and relations. For any finite group K, the scalar $|K|$ in Relational Quantum Theory is simply the scalar 1 (because $|K| = 1 + 1 + 1 + ... + 1$, and 1 is additively idempotent in any locale), and hence all finite groups admit a strongly complementary pair with enough points. However, the phase group in relational quantum theory is the trivial group $\{1\} \cong \mathbb{Z}_1$, and the only group K such that $\bullet_K$ has enough classical states is the trivial group $\mathbb{Z}_1$ itself. Hence there are no non-trivial implementations of the quantum algorithm for the HSP in relational quantum theory. However, this does not necessarily mean that no efficient solution to the HSP can be obtained in relational quantum theory, and the study of relational formulations of quantum algorithms is a busy open field (especially in the context of Spekkens' Toy Model [Spe07, CE12, BD15, Zen15, DM16, CB17]).

4.1.4.6 Infinite-dimensional HSP

The category Hilb of infinite-dimensional Hilbert spaces and bounded linear maps does not admit Frobenius algebras, and as a consequence it cannot be used to extend our abstract setup to infinite abelian groups. However, we have seen in Chapter 2 that tools from non-standard analysis can be used to construct a well-defined category *Hilb of infinite-dimensional separable Hilbert spaces, including both bounded and unbounded linear maps, as well as a number of commonplace features of quantum mechanics (such as Dirac deltas and plane-waves). This opens the way to infinite generalisations of the abelian HSP.

Theorem 4.2 (HSP for $\mathbb{Z}^N$ with a particle in a box).
Consider a particle in an N-dimensional box with periodic boundary conditions. Assume that preparations and measurements in the position observable can be performed with arbitrarily high precision. Then it is possible to efficiently solve the HSP for the infinite abelian group $\mathbb{Z}^N$.

Proof. In Chapter 2 we have seen that that the category *Hilb possesses suitable strongly complementary pairs corresponding to the discrete groups $\mathbb{Z}^N$ of translations of lattices and the compact groups $\mathbb{T}^N$ of translations of tori; all the observables concerned are quasi-special or special, commutative, and have enough classical states.

These observables have direct physical relevance, as they correspond to the momentum/position observable pairs for particles in N-dimensional boxes with periodic boundary conditions. As a consequence, our scheme straightforwardly extends to a quantum subroutine for the HSP on the infinite abelian groups $G = \mathbb{Z}^N$. The classical subroutine requires no adjustment for the case of $\mathbb{Z}^N$, because all the possible quotients G/H are in the form $\mathbb{Z}^J \times \prod_{k=1}^{K} \mathbb{Z}_{n_k}$: hence all the possible annihilators $\mathrm{Ann}[H]$ are in the form $\mathbb{T}^J \times \prod_{k=1}^{K} \mathbb{Z}_{n_k}$, and can be efficiently sampled (infinite precision notwithstanding).

For the sake of physical implementation, this setup corresponds to fixing the computational basis $\circ_G$ to be the basis of momentum eigenstates (valued in $\mathbb{Z}^N$) of a particle in an N-dimensional box with periodic boundary conditions, and performing the $\bullet_G$ measurement corresponding to its position observable (valued in T^N). The oracle is a standard unitary, but the particle needs to be prepared in the exact position eigenstate $\frac{\sqrt{L}^N}{\sqrt{(2\omega+1)^N}} \circ\!\!- \,_G$, and then measured in the position observable with infinite precision (i.e. with continuous-valued outcomes in $\mathbb{T}^N$). Hence we can efficiently solve HSPs on the infinite abelian groups $\mathbb{Z}^N$ as long as we can perform exact preparations and measurements in the position observable.

In fact, being able to perform preparations and measurements in the position observable with arbitrary finite precision turns out to be sufficient. Indeed, consider the family of processes, indexed by $t \in \{1, ..., \omega\}$, which involves preparation in the following approximate position eigenstate:

$$\frac{\sqrt{L}^N}{\sqrt{(2\omega+1)^N}} |\delta_0^{(t)}\rangle := \frac{1}{\sqrt{(2\omega+1)^N}} \sum_{k_1=-t}^{t} \cdots \sum_{k_N=-t}^{t} \frac{1}{\sqrt{L}^N} |\chi_{\underline{k}}\rangle \tag{4.26}$$

This results in a sequence of conditional probability distributions $\mathbb{P}_t(x|b)$ on position measurement outcomes $x \in \frac{1}{(2\omega+1)}{}^{\star}\mathbb{Z}_{2\omega+1}^N$, indexed by the parameter $t \in \{1, ..., \omega\}$. The choice of infinite natural ω is arbitrary, and hence the main proof of this Section shows that $\mathbb{P}_t(x|b) \simeq 0$ for all t infinite and all $x \notin \mathrm{Ann}[H]$. As a consequence, we must have have the following standard result, where now we restrict our attention to $t \in \mathbb{N}^+$:

$$\lim_{t \to \infty} \mathbb{P}_t(\mathrm{st}(x)|b) = 0 \text{ for all } x \notin \mathrm{Ann}[H] \tag{4.27}$$

This shows that arbitrary precision position preparations plus exact position measurements are enough. However, all quotients of $\mathbb{Z}^N$ take the form $\mathbb{T}^J \times \prod_{k=1}^{K} \mathbb{Z}_{n_j} \leq \mathbb{T}^N$, and as a consequence approximate position measurements with sufficiently high precision always suffice. b □

4.2 Mermin-type non-locality scenarios

Non-locality is a defining feature of quantum mechanics, and its connection to the structure of phase groups is a key foundational question. A particularly crisp example of this connection is given by Mermin's argument for qubit GHZ states [Mer90], which finds practical application in the HBB quantum secret sharing protocol.

In Mermin's argument, N qubits are prepared in a Pauli Z GHZ state, then a controlled phase gate is applied to each, followed by measurement in the Pauli X observable. Even though the N outcomes (valued in $\mathbb{Z}_2$) are probabilistic, their parity turns out to satisfy certain deterministic equations. Mermin shows that the existence of a local hidden variable model would imply a joint solution for the equations: however, the latter form an inconsistent system, and Mermin concludes that the scenario is non-local. Mermin's argument has sparked a number of lines of enquiry, and this work is concerned with two in particular: one leading to All-vs-Nothing arguments, and the other investigating the role played by strong complementarity. All-vs-Nothing arguments [ABK$^+$15] arise in the context of the sheaf-theoretic framework for non-locality and contextuality [AB14], and generalise the idea of a system of equations which is locally consistent but globally inconsistent. The second line of research is brought forward within the framework of categorical quantum mechanics, and it focuses on the algebraic characterisation of the structures involved.

A detailed analysis of Mermin's argument shows that the special relationship between the Pauli X and Pauli Z observables powering the argument is nothing but strong complementarity. A pair of complementary observables corresponds to mutually unbiased orthonormal bases: for example, both Pauli X and Pauli Y are complementary to Pauli Z. Strong complementarity amounts to a strictly stronger requirement: if one observable is taken as the computational basis, the other must correspond to the Fourier basis for some finite abelian group. Pauli X fits the bill, for the abelian group $\mathbb{Z}_2$, but Pauli Y doesn't (in fact, Pauli X is the only one for qubits).

In [CDKW12], Mermin's argument is completely reformulated in terms of strongly complementary observables (†-Frobenius algebras) and abstract phase gates. It can therefore be tested on theories different from quantum mechanics, to better understand the connection between non-locality and the structure of phase groups. A particularly insightful comparison is given by qubit stabiliser quantum mechanics [CD11, Bac14] vs Spekkens' toy model [Spe07, CE12]: both theories sport very similar operational and algebraic features, but the difference in phase groups ($\mathbb{Z}_4$ for the former vs $\mathbb{Z}_2 \times \mathbb{Z}_2$ for the latter) results in the former being non-local and the latter being local (both models have $\mathbb{Z}_2$ as group of measurement outcomes, like Mermin's original argument). The picture arising from comparing qubit stabiliser quantum mechanics and Spekkens' toy model is iconic, and provides a first real glimpse into the connection between phase groups and non-locality [CES10].

While presenting an extremely compelling case for stabiliser qubits and Spekkens' toy qubits, the work of [CDKW12, CES10] does not treat the general case (i.e. beyond $\mathbb{Z}_2$ as group of measurement outcomes), nor does it provide a complete algebraic characterisation of the conditions guaranteeing non-locality. In this Section, taken from [GZ17], we fully generalise Mermin's arguments (Definition 4.14) from $\mathbb{Z}_2$ to arbitrary finite abelian groups, in arbitrary theories and for arbitrary phase groups (we will refer to these as **generalised Mermin-type arguments**). We also provide exact algebraic conditions for non-locality to be exhibited by our generalised Mermin-type arguments (Theorem 4.16), thus completing the line of research on the connection of phases and non-locality initiated by [Coe12, CES10].

We proceed to make contact with the All-vs-Nothing line of enquiry [ABK$^+$15], showing that the non-local generalised Mermin-type arguments yield a new hierarchy of quantum-realisable All-vs-Nothing empirical models, and hence that they are strongly contextual (Theorem 4.17 proves that the arguments are quantum realisable, while Theorem 4.18 proves the non-local arguments are All-vs-Nothing). As a consequence, we show that the hierarchy of quantum-realisable All-vs-Nothing models over finite fields does not collapse (Theorem 4.20).

Mermin's argument for the qubit GHZ states also finds practical application in the quantum-classical secret sharing scheme of Hillery, Bužek and Berthiaume [HBB99], and we provide a non-trivial extension of the scheme to our generalised Mermin-type arguments. We also use the strong contextuality deriving from our All-vs-Nothing characterisation to provide some device-independent security guarantees (Theorem 4.22), which apply to the original HBB scheme as a special case.

The results in this Section are also related to the recent work of [RLZL13], and previous work by [LLK06, CMP02, KZ02, ZK99]. The construction adopted in [RLZL13] is similar to the one we will derive in this Section for the special case of cyclic groups $K := \mathbb{Z}_D$, and the relationship between the dimension D of the quantum systems and the allowed numbers N of parties are the same in both works (i.e. $\gcd(N, D) = 1$). The References presented above feature explicit constructions, but are not concerned with investigating the general connection between Mermin-type non-locality and the structure of phase groups (which is the stated aim of the line of research of [Coe12, CES10], brought forward by this Section).

4.2.1 Mermin's Original Argument

4.2.1.1 The parity argument

In the original [Mer90], Mermin considers a 3-qubit GHZ state in the computational basis, the basis of eigenstates for the single-qubit Pauli Z observable, together with the following four joint measurements[7]:

(a) the GHZ state is measured in the observable $X_1 \otimes X_2 \otimes X_3$;

(b) the GHZ state is measured in the observable $Y_1 \otimes Y_2 \otimes X_3$;

(c) the GHZ state is measured in the observable $Y_1 \otimes X_2 \otimes Y_3$;

(d) the GHZ state is measured in the observable $X_1 \otimes Y_2 \otimes Y_3$.

We will denote the eigenstates of the Pauli Z observable by $|z_0\rangle, |z_1\rangle$, the eigenstates of the Pauli X observable by $|\pm\rangle := \frac{1}{\sqrt{2}}(|z_0\rangle \pm |z_1\rangle)$ and the eigenstates of the Pauli Y observable by $|\pm i\rangle := \frac{1}{\sqrt{2}}(|z_0\rangle \pm i|z_1\rangle)$. Mermin's argument is a parity argument, where measurement outcomes are valued in the abelian group $\mathbb{Z}_2 = \{0, 1\}$ according to the following bijections:

(i) for the X observable, $|+\rangle \mapsto 0$ and $|-\rangle \mapsto 1$

(ii) for the Y observable, $|+i\rangle \mapsto 0$ and $|-i\rangle \mapsto 1$

The argument then proceeds as follows. While the joint measurement outcomes are probabilistic, the $\mathbb{Z}_2$ sum of the three outcomes turns out to be deterministic, yielding the following system of equations ($\oplus$ here denotes the sum in $\mathbb{Z}_2$):

$$\begin{cases} X_1 \oplus X_2 \oplus X_3 &= 0 \\ Y_1 \oplus Y_2 \oplus X_3 &= 1 \\ Y_1 \oplus X_2 \oplus Y_3 &= 1 \\ X_1 \oplus Y_2 \oplus Y_3 &= 1 \end{cases} \tag{4.28}$$

If there was a non-contextual assignment of outcomes for all measurements (i.e. X_1, X_2, X_3, Y_1, Y_2 and Y_3), i.e. if there existed a non-contextual hidden variable model, then System 4.28 would have a solution in $\mathbb{Z}_2$, and in particular it would have to be consistent. However, the sum of the left hand sides yields 0 in $\mathbb{Z}_2$:

$$2X_1 \oplus 2X_2 \oplus ... \oplus 2Y_3 = 0X_1 \oplus ... \oplus 0Y_3 = 0 \tag{4.29}$$

[7] Where X_j and Y_j are the single-qubit Pauli X and Y observables on qubit j, for $j = 1, 2, 3$.

while the sum of the right hand sides yields $0 \oplus 1 \oplus 1 \oplus 1 = 3 = 1$ in $\mathbb{Z}_2$. This shows the system to be inconsistent. Equivalently, one could observe that the sum of the LHSs from Equation 4.29 can be written as $2(Y_1 \oplus Y_2 \oplus Y_3)$, and that inconsistency of the system is witnessed by the fact that the equation $2y = 1$ has no solution in $\mathbb{Z}_2$.

The first point of view, where contextuality is witnessed by an inconsistent system where each equation individually admits a solution, is behind the generalisation of Mermin's argument to All-vs-Nothing arguments, presented in [ABK+15]. The second point of view, where contextuality is witnessed by the single unsatisfiable equation $2y = 1$, will inspire the generalisation presented in this work.

4.2.1.2 The role of phases

To understand the role played by the equation $2y = 1$ in the original Mermin argument, we need to take a step back. First of all, we observe that the Pauli Y measurement can be equivalently obtained as a Pauli X measurement preceded by an appropriate unitary. A single-qubit **phase gate**, in the computational basis (the Pauli Z observable), is a unitary transformation in the following form:

$$P_\alpha := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{4.30}$$

where we eliminated global phases by setting the first diagonal element to 1. Measuring in the single-qubit Y observable is equivalent to first applying the single-qubit phase gate $P_{\frac{\pi}{2}}$, and then measuring in the Pauli X observable.

Because they pairwise commute, phase gates come with a natural abelian group structure given by composition, resulting in an isomorphism $\alpha \mapsto P_\alpha$ between them and the abelian group[8] $\mathbb{R}/(2\pi\mathbb{Z})$. Of all the phase gates, P_0 (the identity element of the group) and P_π stand out because of their well-defined action on the (unnormalised) eigenstates of the Pauli X observable:

$$\begin{aligned} P_0 &= |\pm\rangle \mapsto |\pm\rangle \\ P_\pi &= |\pm\rangle \mapsto |\mp\rangle \end{aligned} \tag{4.31}$$

If we see $|\pm\rangle$ as the subgroup[9] $\{0, \pi\} < \mathbb{R}/(2\pi\mathbb{Z})$, then Equation 4.31 looks a lot like the regular action of $\{0, \pi\}$ on itself. This is not a coincidence. Each phase gate P_α can be (faithfully) associated the unique **phase state** $|\alpha\rangle := |z_0\rangle + e^{i\alpha}|z_1\rangle$ obtained

[8] The abelian group $\mathbb{R}/(2\pi\mathbb{Z})$ is isomorphic to the circle group S^1. We prefer the former because of its additive notation, as opposed to the traditionally multiplicative notation of the latter (which is a subgroup of the non-zero multiplicative complex numbers $\mathbb{C}^\times$).

[9] Corresponding to $\{\pm 1\} < S^1$ in the circle group.

from its diagonal, and these phase states can be abstractly characterised in terms of the Pauli Z observable, with no reference to the phase gates they came from (See Subsection 4.2.2). The phase states inherit the abelian group structure of the phase gates, and their regular action coincides with the action of the group of phase gates on them. In particular, the phase gates P_0 and P_π have orthogonal eigenstates of the Pauli X observable as their associated phase states $|0\rangle$ and $|\pi\rangle$, which coincide with $\sqrt{2}|+\rangle$ and $\sqrt{2}|-\rangle$ respectively: this endows the outcomes of Pauli X measurements with the natural $\mathbb{Z}_2$ abelian group structure arising[10] from the inclusion $\{0, \pi\} < \mathbb{R}/(2\pi\mathbb{Z})$. We will henceforth refer to the group of phase states as the **group of Z-phase states**, and to the subgroup $\{0, \pi\}$ as the **subgroup of X-classical states**; the latter will also be used to label the corresponding measurement outcomes.

In order to pave the way to our generalisation, we now proceed to show how Mermin's original argument can be re-constructed from the following statement:

> *the equation $2y = \pi$ has no solution in the subgroup $\{0, \pi\}$ of X-classical states, but a solution[11] $y = \frac{\pi}{2}$ can be found in the larger group $\mathbb{R}/(2\pi\mathbb{Z})$ of Z-phase states.*

We begin by observing that tripartite qubit GHZ state used in Mermin's argument has a special property when it comes to the application of phase gates followed by measurements in the Pauli X observable.

Lemma 4.3 ([CDKW12]). *If $\alpha_j \in \mathbb{R}/(2\pi\mathbb{Z})$, denote by $X_j^{\alpha_j}$ the measurement outcome on qubit j obtained by first applying phase gate P_{α_j}, and then measuring in the Pauli X observable. If $\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = 0$ or π (mod 2π), then $X_1^{\alpha_1} \oplus X_2^{\alpha_2} \oplus X_3^{\alpha_3} = 0$ or π (mod 2π) respectively.*

Now consider System 4.28 again, with values on the the RHS now obtained by applying Lemma 4.3 to $X_j := X_j^0$ and $Y_j := X_j^{\frac{\pi}{2}}$ (and valued in $\{0, \pi\}$ instead of $\mathbb{Z}_2$):

$$\begin{cases} X_1^0 \oplus X_2^0 \oplus X_3^0 & = 0, \text{ the control} \\ X_1^{\frac{\pi}{2}} \oplus X_2^{\frac{\pi}{2}} \oplus X_3^0 & = \pi, \text{ the first variation} \\ X_1^{\frac{\pi}{2}} \oplus X_2^0 \oplus X_3^{\frac{\pi}{2}} & = \pi, \text{ the second variation} \\ X_1^0 \oplus X_2^{\frac{\pi}{2}} \oplus X_3^{\frac{\pi}{2}} & = \pi, \text{ the third variation} \end{cases} \tag{4.32}$$

There are two complementary parts to the Mermin non-locality argument: (i) System 4.32 above must be inconsistent, to rule out the existence of a non-contextual hidden

[10] Natural because there is a unique isomorphism $\mathbb{Z}_2 \cong \{0, \pi\}$.

[11] Corresponding to $y = e^{i\frac{\pi}{2}} = +i$ in the circle group S^1.

variable model, and (ii) joint measurements yielding the individual equations must be possible (in quantum theory). For the first part, inconsistency of the system is witnessed by the fact that the equation $2y = \pi$ has no solution in the subgroup of X-classical states. For the second part, notice that only measurements in the Y observable contribute to the sum for each equation, as measurements in the X observable are associated with the group unit 0 of the group of Z-phase states. As a consequence, the existence of measurements implementing each individual equation reduces to the existence of a Z-phase state $|y\rangle$ satisfying equation $2y = \pi$: the Y observable is chosen exactly because $y = \pi/2$ gives one such Z-phase state.

The following steps summarise the skeleton of the argument, and open the way to our generalisation:

1. consider a non-degenerate observable, call it Z, on an arbitrary quantum system;
2. consider a non-degenerate observable, call it X, such that the X-classical states are a subgroup (call it K) of the abelian group of Z-phase states (call it P);
3. consider an equation in the following form, generalising $2y = \pi$:
$$n_1 y_1 \oplus ... \oplus n_M y_M = a \tag{4.33}$$
(here $a \in K$, $n_1, ..., n_M$ are integers[12], and $\oplus$ is the group addition in P);
4. construct an appropriate system of equations, generalising System 4.32, with inconsistency witnessed by non-existence of solutions for Equation 4.33 in K, and consistency of the individual equations witnessed by the existence of solutions in P;
5. a measurement scenario is implementable if and only if a solution exists in P;
6. a measurement scenario is contextual if and only if no solutions exist in K.

To give a first example of how such an appropriate system of equations might be constructed, we consider the simple generalisation of the argument from a 3-partite to an N-partite GHZ state, for appropriate values of $N \geq 2$. Our requirements are:

(i) we want the phases in the control to sum to 0, and hence we will take them all to be 0 (i.e. X measurements), just as in the original argument;

[12] This is a general equation in abelian groups, seen equivalently as $\mathbb{Z}$-modules.

(ii) we also want the phases in each variation to sum to π, and hence we will take two measurements in each variation to be with phase $\pi/2$ (i.e. measurements in the Y observable), and all the other ones to be with phase 0;

(iii) we want an odd number V of variations, in order to ensure that the RHSs will sum to $0 \oplus V\pi = \pi$;

(iv) we want the LHSs to sum to an even multiple of $X_1^{\frac{\pi}{2}} \oplus ... \oplus X_N^{\frac{\pi}{2}}$;

An appropriate choice is given by the following system of equations, where $V := N$ and all variations are cyclic permutations of the first one:

$$\begin{cases} X_1^0 \oplus X_2^0 \oplus X_3^0 \oplus \quad ... \quad \oplus X_{N-1}^0 \oplus X_N^0 & = 0, \text{ the control} \\ X_1^{\frac{\pi}{2}} \oplus X_2^{\frac{\pi}{2}} \oplus X_3^0 \oplus \quad ... \quad \oplus X_{N-1}^0 \oplus X_N^0 & = \pi, \text{ the } 1^{st} \text{ variation} \\ X_1^{\frac{\pi}{2}} \oplus X_2^0 \oplus \ ... \ \oplus X_{N-2}^0 \oplus X_{N-1}^0 \oplus X_N^{\frac{\pi}{2}} & = \pi, \text{ the } 2^{nd} \text{ variation} \\ \qquad\qquad \vdots & \\ X_1^0 \oplus X_2^{\frac{\pi}{2}} \oplus X_3^{\frac{\pi}{2}} \oplus \quad X_4^0 \quad \oplus \quad ... \quad \oplus X_N^0 & = \pi, \text{ the } N^{th} \text{ variation} \end{cases} \tag{4.34}$$

As long as $N = 1 \pmod{k}$, where $k = 2$ is the exponent[13] of K, the RHSs will sum to π in K. Having chosen our variations by cyclic permutation also makes for the desired sum of the LHSs, since each $X_j^{\pi/2}$ will be counted exactly twice:

$$\underset{\text{control}}{\left(X_1^0 \oplus ... \oplus X_N^0\right)} \quad \oplus \quad \underset{X_j^{\frac{\pi}{2}}\text{s from the variations}}{2 \cdot \left(X_1^{\frac{\pi}{2}} \oplus ... \oplus X_N^{\frac{\pi}{2}}\right)} \quad \oplus \quad \underset{X_j^0\text{s from the variations}}{(N-2) \cdot \left(X_1^0 \oplus ... \oplus X_N^0\right)}$$

Writing x for $X_1^0 \oplus ... \oplus X_N^0$ and y for $X_1^{\frac{\pi}{2}} \oplus ... \oplus X_N^{\frac{\pi}{2}}$, the sum above can be rearranged to take the form $(N-1)x \oplus 2y$, which is equal to $2y$ in K (since $(N-1) = 0 \pmod{k}$)[14]. Hence summing all the LHSs and RHSs leaves us with the equation $2y = \pi$, which we know to be unsatisfiable in K.

4.2.2 The phase group

Mermin's parity argument is fundamentally group-theoretic, and it depends almost entirely on the special relationship between the Pauli Z and Pauli X observables. Fixing the eigenstates of the Pauli Z observable as the computational basis, the requirement that the X-classical states are Z-phase states is satisfied by the Pauli X observable, but also by the Pauli Y: in fact, the Z-phase states are exactly the

[13] The smallest positive integer such that $kx = 0$ for all $x \in K$.

[14] In this specific case, it is also true that $2 = 0 \pmod{k}$, but this is not key to the argument.

unbiased states for the Pauli Z observables, the states lying on the equator of the Bloch sphere, and hence any observable **complementary**, or **mutually unbiased**, to Pauli Z would do the trick; because their eigenstates lie on the equator of the Bloch sphere, we refer to these as **equatorial observables**.

Complementarity however, is not sufficient for Mermin's argument: Lemma 4.3 only holds if we measure the GHZ state in the Pauli X observable, not in any other equatorial observable. The algebraic relationship between the Pauli X, Y and Z observables is vividly captured by the ZX calculus [CD11]: there, the special property relating the Pauli Z and X observables is axiomatised under the name of **strong complementarity**, to distinguish it from the complementarity of Pauli Z and any other equatorial observable (such as Pauli Y). Strong complementarity is behind the proof of Lemma 4.3, which lies at core of the fully diagrammatic treatment of Mermin's original argument appearing in [CDKW12].

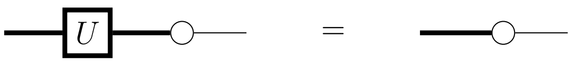
Remark 4.4. *The Pauli X and Y observables on physical qubits are physically indistinguishable, as they can be turned into one another by a unitary which fixes the Pauli Z observable (i.e. a Pauli Z phase gate). As a consequence, it seems somewhat disturbing that X and Y could be distinguished by an abstract, basis-independent property such as strong complementarity.*

An extremely detailed description of the (inexact) correspondence between quantum observables, orthonormal bases of vectors and classical structures is given in Section 5 of [CD11], where the concept of strong complementarity was originally introduced. In particular, the discussion explains why strong complementarity picks Pauli X and not Pauli Y. The point is that the classical structure ○ for Pauli Z picks out two vector representatives $|z_0\rangle, |z_1\rangle$ for the Pauli Z eigenstates (which are complex projective lines), and in doing so it imposes a specific group structure (⟩○– , ○–) on the set of equatorial states.

Physically, Pauli X can be turned into Pauli Y by a rotation of $\pi/2$ around the positive Z axis, and this transformation leaves the Pauli Z physical observable invariant. However, it turns out to change the Pauli Z classical structure, in the following way: keeping $|z_0\rangle$ fixed (without loss of generality), it sends $|z_1\rangle$ to $i|z_1\rangle$ (same physical state, different vector), so that the unit ○– changes from the Pauli X $+1$-eigenstate $|+\rangle := |z_0\rangle + |z_1\rangle$ to the Pauli Y $+1$-eigenstate $|+i\rangle := |z_0\rangle + i|z_1\rangle$; the multiplication changes as well, to reflect the fact that the unit of the group of equatorial states has rotated from $|+\rangle$ to $|+i\rangle$.

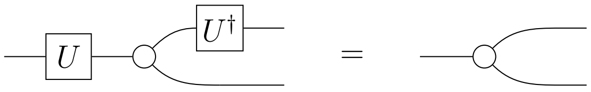
The importance of strong complementarity for the Hidden Subgroup Problem lied in its connection to the quantum Fourier transform. The situation with Mermin-type arguments, however, is different: the relevant facet of strong complementarity will be the special relationship between ●-classical points and ○-phase states, explored in detail in this Subsection. If strong complementarity is the fundamental algebraic property at work in Mermin's argument, phase gates and GHZ states are the operational components key to its implementation. Phase gates arise in the context of quantum-to-classical transitions, where they provide a characterisation, in the spirit of groups and symmetries, of how much information is lost by performing a (demolition) measurement in a non-degenerate observable.

Definition 4.5. *Let ○ be a †-qSFA on an object $\mathcal{H}$ of a dagger compact category. Then the ○-**phase gates** are the unitaries $U : \mathcal{H} \to \mathcal{H}$ which are annihilated by the measurement in the ○ observable:*



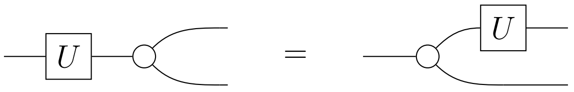
(4.35)

Equation 4.35 can be unfolded into the following equivalent definition, which extends to an arbitrary †-SMC:

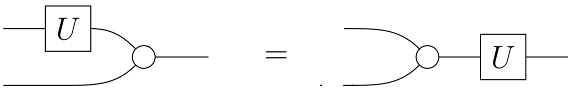


(4.36)

A simpler algebraic characterisation of phase gates is given by the following two equations, which are equivalent to Equation 4.36 (because U is assumed to be unitary):



(4.37)



(4.38)

Both equations will play a pivotal role in this section: Equation 4.37 will features shortly in Lemma 4.8, the result relating phase gates and GHZ states, while Equation 4.38 will feature in Theorem 4.9, the result relating phase gates and unbiased states.

From Equation 4.35, it is not hard to see that ○-phase gates form a group: we will refer to this as the **○-phase group**, and we will denote it by $P(\circ)$. If ○ is a symmetric †-SFA on a finite-dimensional Hilbert space $\mathcal{H}$, associated with a direct sum decomposition $\mathcal{H} = \bigoplus_j \mathcal{H}_j$, then the phase group $P(\circ)$ is given by the corresponding direct sum of unitary groups, modulo a global phase:

$$P(\circ) = \Big(\bigoplus_j U(\mathcal{H}_j)\Big)/S^1 \tag{4.39}$$

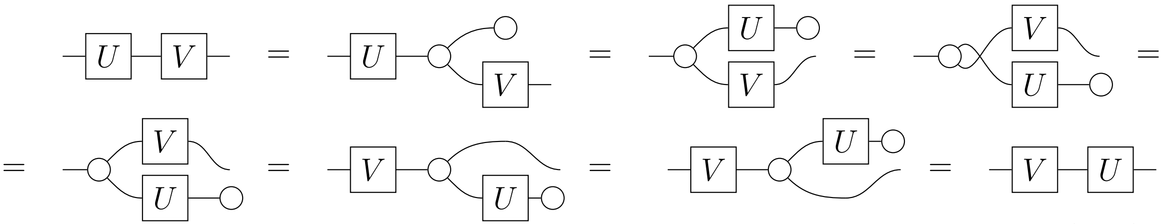
In the special case where $\circ$ is a †-SCFA on $\mathcal{H}$, i.e. when all $\mathcal{H}_j$ subspaces are 1-dimensional, the phase group is abelian, the translation group of a torus:

$$P(\circ) = \Big(\bigoplus_{j=1}^{\dim \mathcal{H}} U(1)\Big)/S^1 \cong T^{\dim \mathcal{H} - 1} \tag{4.40}$$

The connection between abelian phase groups and commutative Frobenius algebras generalises from fHilb to arbitrary dagger compact categories. The following result shows that the phase group of a commutative Frobenius algebra is always abelian, while the converse will be proven later on in Corollary 4.12 (conditional to the existence of enough unbiased states)

Lemma 4.6. *Let $\circ$ be a †-qSFA on an object $\mathcal{H}$ of a dagger compact category. If $\circ$ is commutative, then the $\circ$-phase group $P(\circ)$ is abelian.*

Proof.

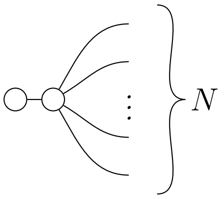


(4.41)

The first equality is by unit law for $\circ$; the second equality is by Equation 4.37; the third equality is some topological manipulation; the fourth equality (top right to bottom left) is by commutativity of $\circ$; the fifth equality is by Equation 4.37; the sixth equality is commutativity of $\circ$; the seventh and last equality is by Equation 4.37, followed by unit law for $\circ$. □

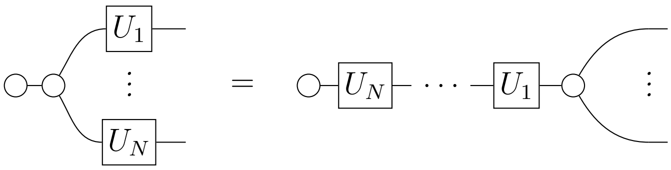
Having defined the phase group and proven Lemma 4.6, we are now in a position to state the first important result of this Subsection. Lemma 4.8 below will characterise the states that can be obtained by application of phases gates to a GHZ state: in the context of our generalised Mermin-type arguments, it will play the same role that Lemma 4.3 played in Mermin's original argument.

Definition 4.7. *If ○ is a †-qSFA on an object $\mathcal{H}$ of a dagger compact category, the N**-partite ○-GHZ state** is the following state of $\mathcal{H}^{\otimes N}$:*



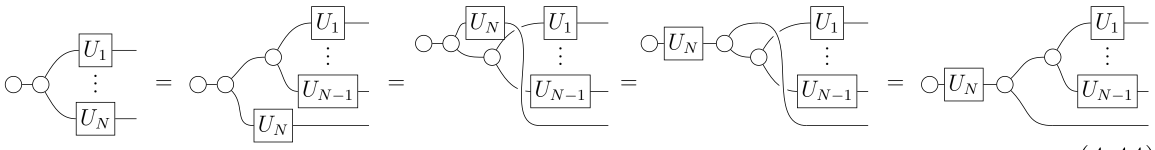
(4.42)

Lemma 4.8. *Let ○ be a †-qSCFA on an object $\mathcal{H}$ of a dagger compact category. Then the state obtained by applying ○-phase gates $U_1, ..., U_N$ to the N-partite ○-GHZ state only depends on the composition $U_1 \cdot ... \cdot U_N$ of the phase gates:*



(4.43)

Proof. Each ○-phase gate is pushed down by using Equation 4.37 and commutativity of ○. Formally, the proof is by induction, with inductive step given by the following equality:

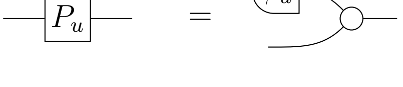


(4.44)

□

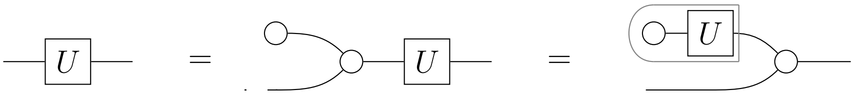
We have remarked before that the phase gates in Mermin's original argument are associated to certain phase states, extracted from their diagonalisation, which are also unbiased states for the relevant observable. As Theorem 4.9 below shows, the connection between ○-phase gates and ○-unbiased states holds true in full generality, and as a consequence we will also refer to ○-unbiased states as **○-phase states**. In the case of fHilb, the decomposition of a ○-phase gate U given by Equation 4.45 below for a †-SCFA ○ is equivalent to saying that U is diagonal in the orthonormal basis $(|x\rangle)_x$ associated with ○, and has diagonal encoded by ○-phase state $|u\rangle$ as $U_{xx} = \langle x|u\rangle$.

Theorem 4.9 (Phase gates, phase states).
Let ○ be a †-qSFA on an object $\mathcal{H}$ of a dagger compact category. Then the ○-phase gates are exactly the maps $P_u : \mathcal{H} \to \mathcal{H}$ taking the following form for some ○-unbiased state ψ_u:



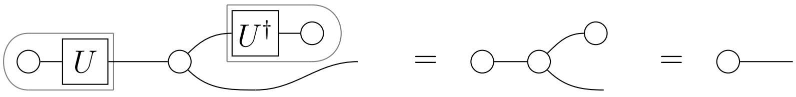
(4.45)

Proof. First we prove that any phase gate U takes the form above, for some ○-unbiased state ψ_u. An appropriate state ψ_u can then be obtained by unit law for ○:



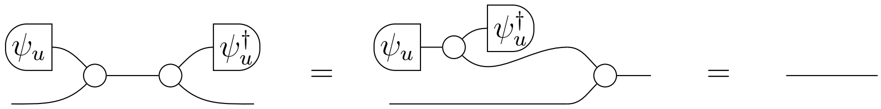
(4.46)

By using Equation 4.36, we can prove that the state we obtained is ○-unbiased:



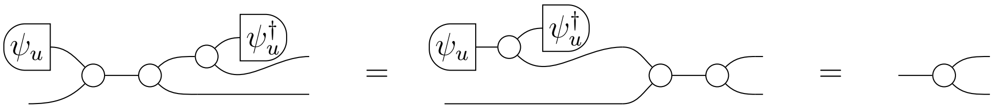
(4.47)

Then we prove that any U in the form above with ψ_u a ○-unbiased state is a unitary:



(4.48)

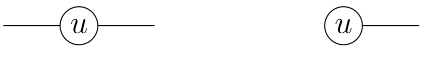
Finally, we prove that any unitary U in the form above with ψ_u a ○-unbiased state is a ○-phase gate:



(4.49)

□

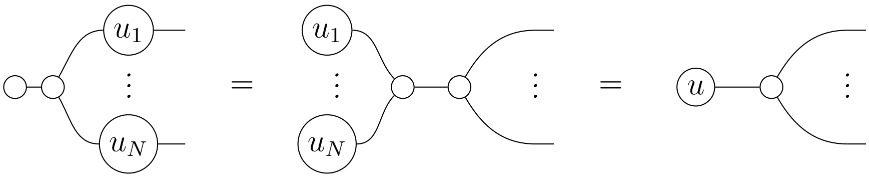
Because of the correspondence above, we will adopt a uniform notation for phase gates and phase states, known in the literature as **decorated spider** notation [CD11, CK17]:



(4.50)

phase gate P_u phase state ψ_u

Corollary 4.10. *Let ○ be a †-qSCFA on an object $\mathcal{H}$ of a dagger compact category. Then the state obtained by applying ○-phase gates $P_{u_1}, ..., P_{u_N}$ to the N-partite ○-GHZ state takes the following form in terms of the corresponding ○-phase states $\psi_{u_1}, ..., \psi_{u_N}$:*



(4.51)

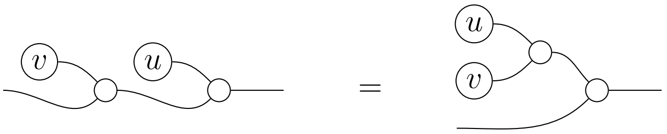
That is, the states that can be obtained by applying ○*-phase gates to the* N*-partite* ○*-GHZ state are exactly those obtained by comultiplying* N*-times some* ○*-unbiased state* u *(specifically, above we have* $u = u_1 \cdot ... \cdot u_N$*, and all* ○*-unbiased states can be obtained this way).*

Proof. From Lemma 4.8, by re-writing each ○-phase gate in terms of the corresponding ○-phase state using Theorem 4.9, and then using associativity to group the ○-phase states together. □

The group structure of phase gates transfers to unbiased states via the correspondence given by Theorem 4.9. Albeit not surprising, this result plays an important role in our generalisation of Mermin-type arguments, where it connects the operational side of phase gates and GHZ states to the algebraic side of strong complementarity (see Theorem 4.13 below).

Lemma 4.11. *Let* ○ *be a* †*-qSFA on an object* $\mathcal{H}$ *of a dagger compact category. Then* (⟩○- , ○–) *endows the set of* ○*-unbiased states with the structure of* $P(○)$*.*

Proof. The ○-phase gate corresponding to the ○-unbiased state ○– is the identity, the unit of $P(○)$, so all we need to show is that composition of phase gates is the same as multiplication under ⟩○- of the corresponding ○-unbiased states:



(4.52)

□

As a bonus, the correspondence between the ○-phase group and the group structure on ○-unbiased states can be used to prove a converse to Lemma 4.6.

Corollary 4.12. *Let* ○ *be a* †*-qSFA on an object* $\mathcal{H}$ *of a dagger compact category, and assume that* ○ *has* ***enough unbiased states***[15]*. Then* ○ *is commutative iff* $P(○)$ *is abelian.*

Proof. We already know from Lemma 4.6 that if ○ is commutative then the ○-phase group $P(○)$ must be abelian. Conversely, if $P(○)$ is abelian then so is the group structure induced by (⟩○- , ○–) on the ○-unbiased states. In particular, this means that ⟩○- is commutative whenever it is applied to ○-unbiased states, and the existence of enough unbiased states allows us to conclude that ○ is always commutative. □

[15] Two morphisms $F, G : \mathcal{H} \to \mathcal{K}$ are equal whenever $F \circ \psi = G \circ \psi$ for all ○-unbiased states ψ.

With Theorem 4.9 we have proven a general correspondence between phase gates and unbiased states, while with Lemma 4.8 and Corollary 4.10 we have characterised the states that can be obtained by applying phase gates to GHZ states. Phase gates and the GHZ state for the Pauli Z observable are the key operational ingredients for Mermin's original argument. However, just as important is the special algebraic standing of those phase gates derived from the eigenstates of the Pauli X observable (an observable strongly complementary to Pauli Z), as opposed to the phase gates derived from other equatorial states (the eigenstates of observables complementary to Pauli Z). The last result of this section, Theorem 4.13, provides a general characterisation of complementarity and strong complementarity in terms of the relation between classical states of one observable and unbiased states of the other. Together with Theorem 4.9 and Corollary 4.10, it will form the basis for the formulation of our generalised Mermin-type arguments in the next Subsection.

Theorem 4.13 (Strong complementarity and phase groups).
Let ○ and ● be symmetric †-qSFA on an object $\mathcal{H}$ of a †-SMC. The following implications always hold:

(i) if ○ and ● are complementary, then the ●-classical states form a subset of the ○-unbiased states, and viceversa;

(ii) if ○ and ● are strongly complementary, then the ●-classical states form a subgroup of the ○-unbiased states, and viceversa.

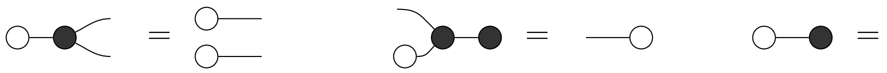
The converse implications hold if ● has enough classical states:

(i) if the ●-classical states form a subset of the ○-unbiased states, then ○ and ● are complementary;

(ii) if the ●-classical states form a subgroup of the ○-unbiased states, then ○ and ● are strongly complementary.

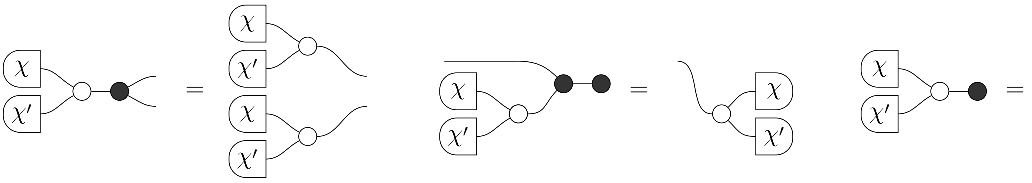
Note that the existence of enough ●-classical states implies the existence of enough ○-unbiased states when the former are a subset/subgroup of the latter.

Proof. Implication (i) is the statement of Lemma 3.4, implication (ii) is the statement of Theorem 3.12, and implication (iii) is the statement of Lemma 3.5. To prove implication (iv) we use the fact that ● has enough classical states by hypothesis, and we work with the colour-swapped versions of the defining equation of strong complementarity (which imply the usual ones, see Remark 3.7). The colour-swapped top row of Equations 4.53 simply states that the unit ○– is a ●-classical state, something which is true when the ●-states are a subgroup of the ○-unbiased states:



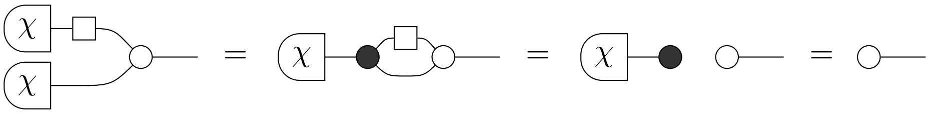
(4.53)

The colour-swapped bottom row of Equations 4.53 holds applied to two ●-classical states if and only if the multiplication under ⟩○– of two ●-classical states is a ●-classical state, something which is always true when the ●-states are a subgroup of the ○-unbiased states



(4.54)

Conditional to (⟩○– , ○–) endowing the ●-classical states with the structure of a monoid, Hopf's law applied to a ●-classical state is equivalent to the antipode acting as group inverse on ●-classical states.



(4.55)

This concludes the proof of implication (iv). □

4.2.3 Generalised Mermin-type Arguments

Armed with the necessary results relating the classical and unbiased states of strongly complementary observables, we are now in a position to formulate our generalised Mermin-type arguments. To do so, we first review the ingredients of Mermin's original parity argument:

(a) a 3-partite qubit GHZ state for the Pauli Z observable;

(b) the abelian group $P(Z) \cong \mathbb{R}/(2\pi\mathbb{Z})$ of phase states for the Pauli Z observable;

(c) the finite subgroup $\{0, \pi\} \cong \mathbb{Z}_2$ given by the eigenstates of the Pauli X observable;

(d) an equation $2x = 1$ with no solution in the subgroup $\{0, \pi\}$ given by the Pauli X eigenstates, but with a solution $\pi/2$ in the group $\mathbb{R}/(2\pi\mathbb{Z})$ of Pauli Z phase states;

(e) measurements in the Pauli X observable.

Similarly, our generalised Mermin-type arguments will involve the following ingredients:

(a) an N-partite GHZ state for a †-qSCFA $\circ$;

(b) the abelian group $(P(\circ), \oplus, 0)$ of $\circ$-phase states[16];

(c) the subgroup $(K(\bullet), \oplus, 0)$, assumed to be finite, of $\bullet$-classical states for a symmetric †-qSFA $\bullet$ strongly complementary to $\circ$;

(d) a finite system of $\mathbb{Z}$-module equations, together with a solution in the group $P(\circ)$;

(e) measurements in the $\bullet$ observable.

The non-existence of a solution in the subgroup $K(\bullet)$ of $\bullet$-classical states is not part of our generalised setup: it will be explicitly characterised as the necessary and sufficient condition for contextuality. Also, N will not be a free parameter, being instead determined by the exponent of the finite abelian group $K(\bullet)$.

Definition 4.14. *Consider an R-probabilistic CPM category $\mathcal{C}$. A* ***generalised Mermin-type argument*** *in $\mathcal{C}$ is specified by the following data:*

(i) a strongly complementary pair $(\circ, \bullet)$ of a canonical †-qSCFA $\circ$ and a canonical †-SCFA $\bullet$ on some object $\mathcal{H}$ of $\mathcal{C}$, such that $\bullet$ has enough classical states; we furthermore assume that the set $K(\bullet)$ of $\bullet$-classical states is finite[17], and that $|K(\bullet)|$ is invertible as an element of the semiring R of scalars of $\mathcal{C}$;

(ii) a finite system $\mathcal{S}$ of $\mathbb{Z}$-module equations[18], with $a^1, ..., a^S \in K(\bullet)$:

$$\mathcal{S} = \begin{cases} \bigoplus_{r=1}^{M} n_r^1 \, y_r = a^1 \\ \quad \vdots \\ \bigoplus_{r=1}^{M} n_r^S \, y_r = a^S \end{cases} \tag{4.56}$$

(iii) a given solution $(y_r := \beta_r)_{r=1}^{M}$ in the abelian group $P(\circ)$ of $\circ$-phase states;

(iv) a positive integer N such that $N \geq \sum_{r=1}^{M} n_r^s$ for all $s = 1, ..., S$, and satisfying $\gcd(N, \exp[K(\bullet)]) = 1$, where $\exp[K(\bullet)]$ is the exponent[19] of $K(\bullet)$.

Therefore a generalised Mermin-type argument is specified by a quintuple $(\circ, \bullet, \mathcal{S}, \beta, N)$.

[16] Isomorphic, by Theorem 4.9, to the $\circ$-phase group, which we will denote by $(P(\circ), \cdot, id)$.

[17] This, together with commutativity of $\circ$, means that $(K(\bullet), \oplus, 0)$ is a finite abelian group.

[18] I.e. equations with integer coefficients $n_r^s \in \mathbb{Z}$ and valued in abelian groups (aka $\mathbb{Z}$-modules).

[19] The smallest positive integer e such that $e \cdot g = 0$ for all $g \in K(\bullet)$.

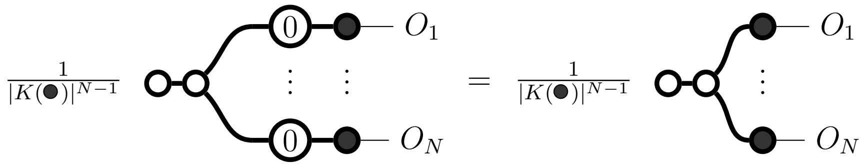
The quintuple $(\circ, \bullet, \mathcal{S}, \beta, N)$ contains all the algebraic and operational ingredients we need to formulate a measurement scenario, which sees N no-signalling parties sharing an N-partied $\circ$-GHZ state. Each party makes a measurement choice $m_j \in \{0, 1, ..., M\}$, applies the phase gate $P_{\beta_{m_j}}$ to her system, and measures it in the $\bullet$ observable (i.e. measurement outcomes are valued in the set $K(\bullet)$ of $\bullet$-classical states).

Not all combinations of measurement choices are needed for the argument, and the measurement contexts will be determined by System 4.56. We begin by zero-padding the system as follows, so that exactly N phase states are involved in each equation:

$$\begin{cases} n_0^0\, y_0 \oplus \quad 0\, y_1 ... \oplus \quad\; 0\, y_M = 0 \\ n_0^1\, y_0 \oplus n_1^1\, y_1 ... \oplus n_M^1\, y_M = a^1 \\ \qquad \vdots \\ n_0^S\, y_0 \oplus n_1^S\, y_1 ... \oplus n_M^S\, y_M = a^S \end{cases} \tag{4.57}$$

where we have defined $a^0 := 0$, $n_0^s := N - \sum_{r=1}^{M} n_r^s$ for all $s = 1, ..., S$, $n_0^0 := N$ and $n_r^0 := 0$ for all $r = 1, ..., M$; we will also extend the given solution by setting $\beta_0 := 0$. The first equation in System 4.57 (which we will refer to by the special value $s = 0$ of the parameter s) will contribute to a single measurement context, the **control**; each further equation (i.e. for each value $s = 1, ..., S$ of the parameter s) will give rise to N measurement contexts, the **variations**, for a total of $1 + S \cdot N$ measurement contexts involved in the scenario.

In the control, all parties choose $m_j^0 = 0$, i.e. perform no phase gate before measuring. They obtain the following global state (where $1/|K(\bullet)|^{N-1}$ is the normalisation factor required to obtain a R-distribution):

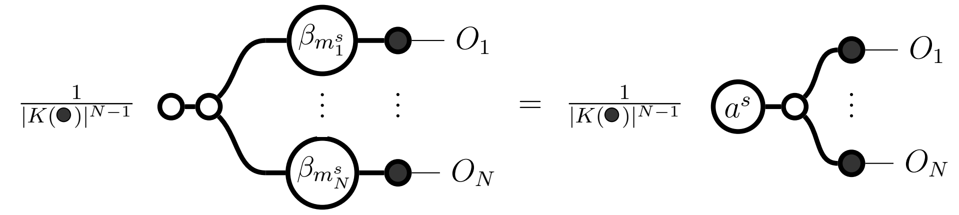

$\frac{1}{|K(\bullet)|^{N-1}}$
0
O_1
0
O_N
=
$\frac{1}{|K(\bullet)|^{N-1}}$
O_1
O_N

(4.58)

The first variation for each value $s = 1, ..., S$ is specified by the corresponding equation in System 4.57: the first n_0^s parties choose $m_j^s = 0$, the next n_1^s parties choose $m_j^s = 1$, the next n_2^s parties choose $m_j^s = 2$ and so on, until the last n_M^s parties choose $m_j^s = M$:

$$m_j^s := \text{the largest } m \in \{0, ..., M\} \text{ such that } j \geq \sum_{r=0}^{m-1} n_r^s \tag{4.59}$$

They obtain the following global state, where the equality results from an application of Corollary 4.10, using the relevant equation from System 4.57:



$\frac{1}{|K(\bullet)|^{N-1}}$
$\beta_{m_1^s}$
O_1
$\beta_{m_N^s}$
O_N
=
$\frac{1}{|K(\bullet)|^{N-1}}$
a^s
O_1
O_N

(4.60)

For each fixed value of s, the next $N-1$ variations are cyclic permutations of the first. The measurement choice for the j^{th} party at the k^{th} variation of a given s is $m^s_{j+(k-1)}$, where the sum $j+(k-1)$ is taken modulo N:

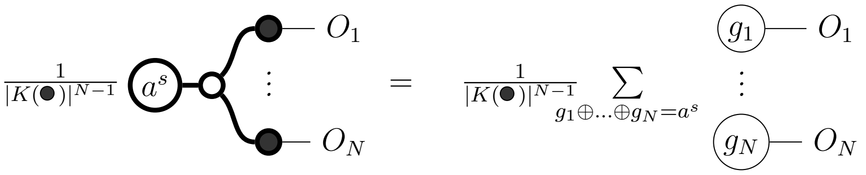
Parties:	1	2	...	$N-1$	N
1^{st} variation for s	m_1^s	m_2^s	...	m_{N-1}^s	m_N^s
2^{nd} variation for s	m_2^s	m_3^s	...	m_N^s	m_1^s
3^{rd} variation for s	m_3^s	m_4^s	...	m_1^s	m_2^s
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
N^{th} variation for s	m_N^s	m_1^s	...	m_{N-2}^s	m_{N-1}^s

(4.61)

Because ○ is commutative, the global state obtained is the same as that for the first variation for that value of s (shown on the RHS of Equation 4.60).

By using strong complementarity and Theorem 4.13, we rewrite the global state obtained by the N parties in the control and variations, obtaining an explicit R-distribution over the set $K(\bullet)^N$ of joint measurement outcomes (from now on, the parameter s can take any value in $\{0, 1, ..., S\}$, unless otherwise specified).

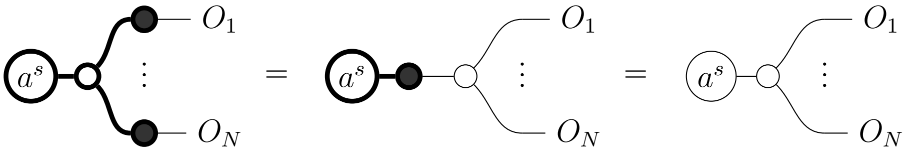
Lemma 4.15.



$\frac{1}{|K(\bullet)|^{N-1}}$
a^s
O_1
O_N
=
$\frac{1}{|K(\bullet)|^{N-1}}$
$\sum_{g_1\oplus...\oplus g_N=a^s}$
g_1
O_1
g_N
O_N

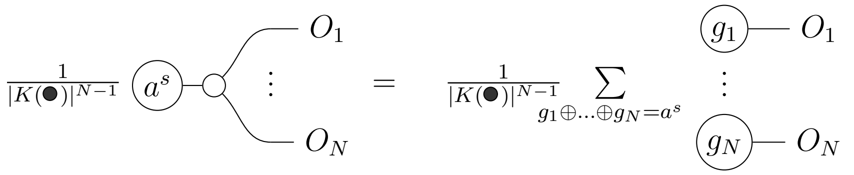
(4.62)

Proof. Strong complementarity can be used to swap ○ and ●, as shown in Corollary 4.1 of [CDKW12], and then a^s can be pushed through because it is a ●-classical state (we have left normalisation aside, and we use $a^0 := 0$ to treat control and variations uniformly):



(4.63)

Using fact that ● has enough classical states, and recalling from Theorem 4.13 that (≻- , ○-) acts as the group multiplication of $K(\bullet)$ when restricted to the ●-classical states, we can further decompose the state on the RHS of Equation 4.63 into an R-distribution over the set $K(\bullet)^N$:



$\frac{1}{|K(\bullet)|^{N-1}}$
a^s
O_1
O_N
=
$\frac{1}{|K(\bullet)|^{N-1}} \sum_{g_1 \oplus ... \oplus g_N = a^s}$
g_1
O_1
g_N
O_N

(4.64)

□

The joint outcome of measurements for the control is uniformly distributed over the subgroup $H_0 \trianglelefteq K(\bullet)^N$ specified by $H_0 := \{(g_1, ..., g_N) \mid g_1 \oplus ... \oplus g_N = 0\}$, while the joint outcome of any of the N variations for each specific value of s is uniformly distributed over the coset $H_{a_s} := (a^s, 0, ..., 0) \oplus H_0$. For each $s, s' \in \{0, 1, ..., S\}$, the cosets H_{a_s} and $H_{a_{s'}}$ are disjoint if and only if $a^s \neq a^{s'}$. All in all, we get the following empirical model for the generalised Mermin-type argument:

$$\mathbb{P}[(g_1, ..., g_N)|\text{control}] = \begin{cases} \frac{1}{|K(\bullet)|^{N-1}} & \text{if } g_1 \oplus ... \oplus g_N = 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.65}$$

$$\mathbb{P}[(g_1, ..., g_N)|k^{th} \text{ variation for } s] = \begin{cases} \frac{1}{|K(\bullet)|^{N-1}} & \text{if } g_1 \oplus ... \oplus g_N = a^s \\ 0 & \text{otherwise} \end{cases} \tag{4.66}$$

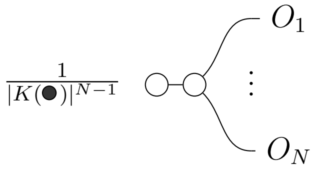
One of the catchy features of Mermin's original argument is that it is entirely deterministic: instead of relying on the violation of some probabilistic inequality, the proof of contextuality shows that the existence of a local hidden variable (LHV) model would lead to the existence of solutions to an unsatisfiable parity equation (i.e. one which doesn't admit solutions in the finite abelian group $\mathbb{Z}_2$). The proof of contextuality for our generalised Mermin-type arguments goes by similar lines, showing that the existence of a LHV model is equivalent to System 4.56 admitting solutions in the finite abelian group $K(\bullet)$.

Theorem 4.16 (**Mermin-type contextuality**).
Consider an R-probabilistic CPM category $\mathcal{C}$, and let $(\circ, \bullet, \mathcal{S}, \beta, N)$ be a generalised Mermin-type argument in it. If the associated empirical model is contextual, then the system $\mathcal{S}$ admits no solution in the finite abelian group $K(\bullet)$. Conversely, if the system $\mathcal{S}$ admits no solution in $K(\bullet)$ and R is a positive semiring, then the empirical model is contextual.

Proof. The proof comes in two parts: (⇒) we show that any solution in $K(\bullet)$ can be turned into a LHV model; (⇐) we show that, as long as R is a positive semiring, any LHV model can be turned into a solution in $K(\bullet)$.

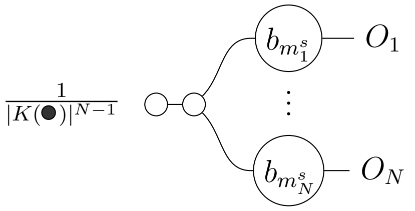
Proof of ($\Rightarrow$). Assume that the system $\mathcal{S}$ (in the form of System 4.56) admits a solution $(y_r := b_r)_{r=1}^{M}$, and define $b_0 := 0$. A LHV model can be obtained as follows:

(i) the uniform R-distribution on $H_0 \trianglelefteq K(\bullet)^N$ is taken as a shared classical state amongst the N parties:



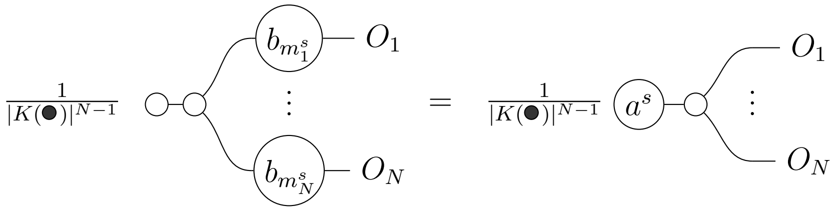
(4.67)

(ii) upon measurement choice $m_j \in \{0, 1, ..., M\}$ for the j^{th} party, a translation by b_{m_j} in the group $K(\bullet)$ is applied to the respective classical subsystem, independently of the measurement choices of the other parties:



(4.68)

All we need to show is that the procedure above produces the same R-distributions on $K(\bullet)^N$ as those given by the empirical model of Equations 4.65 and 4.66. To do so, we simply observe that the global state obtained with the procedure above is the same as the global states obtained in the control 4.58 and in the variations 4.60 (which we treat uniformly by considering $s = 0, 1, ..., S$), because $b_0, b_1, ..., b_N$ satisfy the same equations satisfied by the phases $\beta_0, \beta_1, ..., \beta_N$:



(4.69)

Proof of ($\Leftarrow$). Now assume that R is a positive semiring, and that the scenario admits a LHV model:

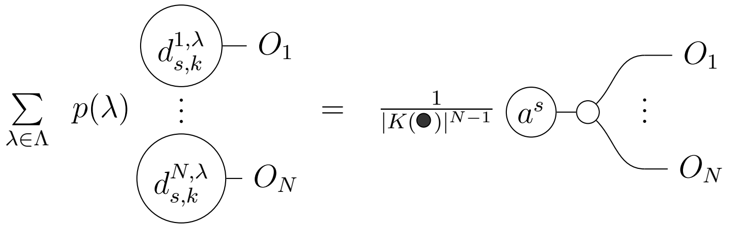
(i) there is a some finite set Λ, the set of values for the hidden variable, coming with an R-distribution $p : \Lambda \to R$;

(ii) for each possible measurement choice $r = 0, 1, ..., M$ that each party $i = 1, ..., N$ can make, there is a family $(c_r^{i,\lambda})_{\lambda \in \Lambda}$ of $\bullet$-classical states, the deterministic local outcomes for each value of the hidden variable;

(iii) for each measurement context (either $s = 0$, $k = 1$ for the control, or $(s, k) \in \{1, ..., S\} \times \{1, ..., N\}$ for the $N \cdot S$ variations), a definite $\bullet$-classical outcome $d^{i,\lambda}_{s,k}$ is obtained by each party $i = 1, ..., N$ at each definite value $\lambda \in \Lambda$ of the hidden variable:

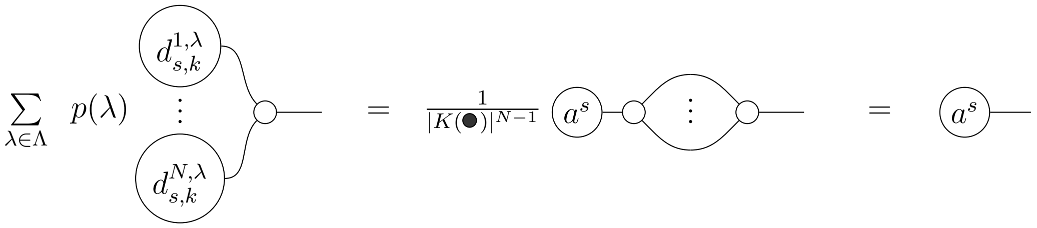
$$d^{i,\lambda}_{s,k} := c^{i,\lambda}_{m^s_{i+(k-1)}} \tag{4.70}$$

(iv) if these definite $\bullet$-classical global states are weighted based on the R-distribution p on Λ, one obtains the same R-distribution on joint measurement outcomes that would be expected from the measurement context:



(4.71)

Given a LHV model, we can sum up all N outcomes of each side of Equation 4.71 in $(K(\bullet), \oplus, 0)$ to obtain an equation between R-distribution over $K(\bullet)$:



(4.72)

The last equation used the fact that $\bullet$ was chosen to be special[20], and hence the normalisation factor for the †-qSCFA $\circ$ is $|K(\bullet)|$ (because $\bullet$ has enough classical states)[21]. Equation 4.72 can be turned into the following conditions on the LHV:

$$\sum_{\lambda \text{ s.t. } \bigoplus_{i=1}^N d^{i,\lambda}_{s,k} = a^s} p(\lambda) = 1 \qquad\qquad \sum_{\lambda \text{ s.t. } \bigoplus_{i=1}^N d^{i,\lambda}_{s,k} \neq a^s} p(\lambda) = 0 \tag{4.73}$$

Because R is a positive semiring, $p(\lambda) = 0$ for any λ such that $\oplus_{i=1}^N d^{i,\lambda}_{s,k} \neq a^s$ for some s. Conversely, picking any λ_+ such that $p(\lambda_+) > 0$ (and at least one such λ_+ exists, because p is an R-distribution) yields a family $(d^{i,\lambda_+}_{s,k})_{s,k,i}$ such that $\oplus_{i=1}^N d^{i,\lambda_+}_{s,k} = a^s$ for all s and k. For the control ($s = 0$ and $k = 1$), we obtain the following equation:

$$\oplus_{i=1}^N c^{i,\lambda_+}_0 = 0 \tag{4.74}$$

[20] The special $\bullet$ could have been replaced by a more general †-qSCFA, but at the price of an additional normalisation factor in all global states.

[21] The normalisation factor $|K(\bullet)|$ refers to two wires: each additional wire is an additional copy of $|K(\bullet)|$, for a total of $|K(\bullet)|^{N-1}$ in the N-wire case here.

For each variation $(s,k) \in \{1,...,S\} \times \{1,...,N\}$, we obtain the following equation:

$$\oplus_{i=1}^{N} c^{i,\lambda_+}_{m^s_{i+(k-1)}} = a^s \tag{4.75}$$

If c^{i,λ_+}_r were independent of the party i for all $r = 1,...,M$, this equation would yield a solution to system $\mathcal{S}$ in the form of $b_r := c^{i,\lambda_+}_r$ for any i; unfortunately, this need not be the case. This is where our cyclic definition of the N variations for each value of s comes into play. For each fixed value of s, we add up the N equations for $k = 1,...,N$:

$$\oplus_{k=1}^{N} \oplus_{i=1}^{N} c^{i,\lambda_+}_{m^s_{i+(k-1)}} = N a^s \tag{4.76}$$

Because $\gcd(N, \exp[K(\bullet)]) = 1$, the equation above has solutions if and only if the equation below does:

$$\oplus_{k=1}^{N} \oplus_{i=1}^{N} c^{i,\lambda_+}_{m^s_{i+(k-1)}} = a^s \tag{4.77}$$

Now refer to the Table 4.61 defining the N variations for s and to the Equation 4.59 defining the measurement choices. The LHS of Equation 4.76 is a sum by rows of the N^2 measurement choices in Table 4.61: each $r = 0,1,...,M$ appears n^s_r times in each row, but the changing value of i along each row stops us from turning it into a solution to system $\mathcal{S}$. However, we can switch the summations in Equation 4.76 to obtain a sum by columns of the table, where each $r = 0,1,...,M$ still appears n^s_r times in each column (by the cyclic definition), but now i is constant along each column:

$$\oplus_{i=1}^{N} \oplus_{k=1}^{N} c^{i,\lambda_+}_{m^s_{i+(k-1)}} = \oplus_{i=1}^{N} \oplus_{r=0}^{M} n^s_r c^{i,\lambda_+}_r \tag{4.78}$$

We can then sum up all $(c^{i,\lambda_+}_r)_{i=1}^N$ for each $r = 0,1,...,M$, and use Equation 4.76 (together with Equation 4.74 to cancel out the contribution from $r = 0$) to finally obtain the desired solution $(b_r)_{r=1}^M$ to system $\mathcal{S}$:

$$\oplus_{r=1}^{M} n^s_r \underbrace{\left(\oplus_{i=1}^{N} c^{i,\lambda_+}_r\right)}_{b_r} = a^s \tag{4.79}$$

□

4.2.4 Quantum realisability

In quantum theory, i.e. in the $\mathbb{R}^+$-probabilistic CPM category CPM[fHilb], many of the requirements of generalised Mermin-type arguments are automatically satisfied: canonical †-SCFA in CPM[fHilb] (i.e. †-SCFA in fHilb) always have enough classical states (and finitely many so), the semiring $\mathbb{R}^+$ of scalars is positive, and any non-zero integer is invertible in it. Hence, only strong complementarity is required in point (i) of the definition generalised Mermin-type arguments, and Theorem 4.16 establishes an unconditional equivalence between contextuality of a generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$ and the existence of solutions to system $\mathcal{S}$ in the finite abelian group $K(\bullet)$ of $\bullet$-classical states.

The remarks above show that the correspondence between systems of equations in finite abelian groups and generalised Mermin-type arguments is particularly tight in the case of quantum theory, but an important question remains unanswered: which systems of $\mathbb{Z}$-module equations lead to arguments which can be realised in quantum theory? As it turns out, all of them (but an obvious caveat applies).

Theorem 4.17 (**Quantum Realisability**).
Let $(K, \oplus, 0)$ be a finite abelian group, and $\mathcal{S}$ be a finite system of $\mathbb{Z}$-module equations in the following form, with $a^1, ..., a^S \in K$:

$$\mathcal{S} = \begin{cases} \bigoplus_{r=1}^{M} n_r^1\, y_r = a^1 \\ \quad\vdots \\ \bigoplus_{r=1}^{M} n_r^S\, y_r = a^S \end{cases} \tag{4.80}$$

*Assume that the system is **consistent** in the following sense, where by $\underline{n}^s \in \mathbb{Z}^M$ we denoted the row vectors of System 4.80:*

$$\bigoplus_{s=1}^{S} c_s \cdot \underline{n}^s =_{\mathbb{Z}^M} \underline{0} \implies \bigoplus_{s=1}^{S} c_s \cdot a^s =_K 0, \tag{4.81}$$

Then for every $|K|$-dimensional quantum system $\mathcal{H}$ and every $\dagger$-qSCFA $\circ$ on $\mathcal{H}$ with normalisation factor $|K|$, there exists a generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$ corresponding to System 4.80, i.e. we can always find:

(i) a $\dagger$-SCFA $\bullet$, strongly complementary to $\circ$, such that $(K(\bullet), \rangle\!\!\circ\!\!-\ , \circ\!\!-\ ) \cong (K, \oplus, 0)$;

(ii) a solution $(y_r := \beta_r)_{r=1}^{M}$ to $\mathcal{S}$ in $P(\circ) \cong T^{|K|-1}$;

(iii) a positive integer N (infinitely many, in fact) such that $N \geq \sum_{r=1}^{M} n_r^s$ for all $s = 1, ..., S$, and such that $\gcd(N, \exp[K(\bullet)]) = 1$.

Proof. Point (iii) is trivial: there are infinitely many positive integers N such that $\gcd(N, \exp[K]) = 1$, and hence we can always find one such that $N \geq \sum_{r=1}^{M} n_r^s$ for all $s = 1, ..., S$. Point (i) is more interesting, and relies on the characterisation of strong complementarity in fHilb and Pontryagin duality for finite abelian groups. Point (ii) is perhaps the most interesting, and relies on the possibility of solving consistent systems of $\mathbb{Z}$-module equations in the torus $T^{|K|-1}$.

Proof of point (i). Because $\circ$ is a †-qSCFA with normalisation factor $|K|$ on a $|K|$-dimensional Hilbert space $\mathcal{H}$, it is associated with a basis of $|K|$ vectors, each having norm $\sqrt{|K|}$. Label the basis vectors by the $|K|$ multiplicative characters $\chi \in K^\wedge$ of the finite abelian group K, and construct an orthonormal basis by using the multiplicative characters $\tau \in (K^\wedge)^\wedge$ of the finite abelian group $K^\wedge$:

$$|\tau\rangle := \frac{1}{|K|} \sum_{\chi \in K^\wedge} \tau(\chi)|\chi\rangle \tag{4.82}$$

By Pontryagin duality, there is a canonical isomorphism $(K^\wedge)^\wedge \cong K$, so that the new orthonormal basis given by Equation 4.82 is canonically labelled by elements of K. Consider the †-SCFA $\bullet$ associated to the orthonormal basis thus defined to obtain the desired $(K(\bullet), \succ\!\!\circ\!\!- , \circ\!\!-) \cong (K, \oplus, 0)$.

Proof of point (ii). The phase group $P(\circ)$ for a canonical †-qSCFA on a $|K|$-dimensional Hilbert space in CPM[fHilb] is isomorphic to the $(|K|-1)$-dimensional torus, an abelian Lie group. To find a solution $(y_r := \beta_r)_{r=1}^M$ to System 4.80, we will show that one can always find solutions to arbitrary consistent systems of $\mathbb{Z}$-module equations in a torus.

While all K-valued systems with solutions in some super-group of K must necessarily be consistent, the converse is not true in general: given a super-group P of K there may be consistent systems with no solutions in P. Certainly if P is finite then at least one such system exists (because of the finite exponent), and certainly if $P = \mathbb{Q}^d$ then no such system exists; in fact, every divisible torsion-free abelian group P is canonically a $\mathbb{Q}$-vector space, and thus every consistent system of $\mathbb{Z}$-modules equations (and, in fact, of $\mathbb{Q}$-vector space equations) valued in a divisible torsion-free abelian group P has solutions in P (e.g. by Gaussian elimination over the field $\mathbb{Q}$). Unfortunately, while tori are divisible, they are not torsion-free, and in particular not $\mathbb{Q}$-vector spaces: as a consequence, the reasoning above does not apply.

However, a more general argument can be used to show that any consistent system of equations can be solved in any divisible abelian group, regardless of whether the group is torsion-free or not [Fuc15] (although uniqueness of solution need not hold for systems with linearly independent row vectors). As tori are divisible abelian groups, all consistent systems of $\mathbb{Z}$-module equations can be solved in them, and in particular we can find our solution $(y_r := \beta_r)_{r=1}^M$ to System 4.80. □

4.2.5 All-vs-Nothing Arguments

Strong contextuality can be reformulated directly in terms of the supports of the distributions. The supports of the global sections, i.e. the $d \in \mathcal{D}_{\mathbb{B}}\mathcal{E}[\mathcal{X}]$ satisfying Equation 2.79 form a (possibly empty) lattice, and thus a probabilistic empirical model is strongly contextual iff the following set is empty:

$$\mathbb{S}[\mathcal{X}] := \left\{ s \in \mathcal{E}[\mathcal{X}] \,\middle|\, s|_C \in \operatorname{supp} \zeta_C \text{ for all } C \in \mathcal{M} \right\} \tag{4.83}$$

For a possibilistic (no-signalling) empirical model $(\zeta_C)_{C \in \mathcal{M}}$, we can define [ABK+15] a **support subpresheaf** $\mathbb{S} \subseteq \mathcal{E}$ by setting:

$$\mathbb{S}[U] := \{ s \in \mathcal{E}[U] \mid s|_{C \cap U} \in \operatorname{supp} \zeta_C|_{U \cap C} \text{ for all } C \in \mathcal{M} \} \tag{4.84}$$

Then a possibilistic empirical model is strongly contextual if and only if $\mathbb{S}[\mathcal{X}] = \emptyset$.

The fundamental observation behind the **All-vs-Nothing arguments** of [ABK+15] is that contextuality of Mermin's original argument follows from the existence of the system of $\mathbb{Z}_2$ equations which has no global solution (corresponding to $\mathbb{S}[\mathcal{X}] = \emptyset$ in the sheaf-theoretic framework for contextuality [AB14] we have previously summarised), but where each equation admits a solution (i.e. we have $\mathbb{S}[C] \neq \emptyset$ for the measurement context C associated to each equation). In this Subsection we summarise the basic framework of All-vs-Nothing arguments from [ABK+15], taking the liberty of slightly generalising the definitions therein, from rings to modules over rings.

Let $\mathcal{R}$ be a commutative ring with unit: we will denote by $+$ the addition in the ring $\mathcal{R}$, and by $\oplus$ the addition in $\mathcal{R}$-modules. The ring $\mathcal{R}$ should not be confused with the semiring R over which the distributions are taken (i.e. the semiring of scalars of the R-probabilistic CPM category which the arguments take place in). If G is some $\mathcal{R}$-module, we will define an **$\mathcal{R}$-linear equation valued in** G to be a triple $\phi = (C, n, b)$ where:

(i) C is some finite set, and we define $\operatorname{index}(\phi) := C$;

(ii) $n : C \to \mathcal{R}$ is any function;

(iii) $b \in G$ is a given element of G.

If $\phi = (C, n, b)$ is an $\mathcal{R}$-linear equation valued in G, we will say that a function $s : C \to G$ (henceforth an **assignment**) **satisfies** ϕ, written $s \models \phi$, if and only if the following equation holds in G:

$$\bigoplus_{m \in C} n_m s_m = b \tag{4.85}$$

where we denoted $n_m := n(m)$ and $s_m := s(m)$. Any set W of assignments $C \to G$ can be associated a corresponding set $\mathbb{T}_{\mathcal{R}}(W)$ of satisfied equations, which is itself an $\mathcal{R}$-module[22]:

$$\mathbb{T}_{\mathcal{R}}(W) := \{\phi \mid s \models \phi \text{ for all } s \in W\} \tag{4.86}$$

Let $(\zeta_C)_{C \in \mathcal{M}}$ be a possibilistic empirical model for a measurement scenario $(\mathcal{E}, \mathcal{M})$, such that all measurements have the same $\mathcal{R}$-module G as their set of outcomes (for example we had $G = \mathbb{Z}_2$, a $\mathbb{Z}$-module, for Mermin's original argument). Let $\mathbb{S} \subseteq \mathcal{E}$ be the support subpresheaf for the empirical model and define its **R-linear theory**:

$$\mathbb{T}_{\mathcal{R}}(\mathbb{S}) := \bigcup_{C \in \mathcal{M}} \mathbb{T}_{\mathcal{R}}(\mathbb{S}[C]) \tag{4.87}$$

We say that a possibilistic empirical model is **All-vs-Nothing** with respect to ring $\mathcal{R}$ and $\mathcal{R}$-module G, written $\mathrm{AvN}_{\mathcal{R},G}$, iff the $\mathcal{R}$-linear theory admits no solution in G, i.e. iff there exists no global assignment $s : \mathcal{X} \to G$ such that:

$$s|_C \models \phi \text{ for all } C \in \mathcal{M} \text{ and all } \phi \in \mathbb{T}_{\mathcal{R}}(\mathbb{S}[C]) \tag{4.88}$$

To connect back with the notation in [ABK+15], we will simply write $\mathrm{AvN}_{\mathcal{R}}$ for $\mathrm{AvN}_{\mathcal{R},\mathcal{R}}$.

A straightforward generalisation (from rings to modules) of a result by [ABK+15] proves that any possibilistic empirical model which is $\mathrm{AvN}_{\mathcal{R},G}$ for some ring $\mathcal{R}$ and some $\mathcal{R}$-module G is strongly contextual: if the model weren't strongly contextual, then there would be some global section $s \in \mathbb{S}[\mathcal{X}]$, and this would imply $s|_C \in \mathbb{S}[C]$ for all $C \in \mathcal{M}$, which in turn would prove that global assignment s satisfies Equation 4.88 (by appealing to Equation 4.86).

A result by [AB14] shows that a probabilistic empirical model is strongly contextual if and only if it is maximally contextual, i.e. if and only if it lies on a face of the no-signalling polytope with no local vertices. As a consequence, showing that our generalised Mermin-type arguments are $\mathrm{AvN}_{\mathcal{R},G}$ is a particularly neat way of proving that they are maximally contextual, a highly desirable property for the device-independent security of the quantum-classical secret sharing protocol we will present in the next Subs.

Theorem 4.18 (**Mermin-type contextuality is AvN**).
Consider a R-probabilistic CPM category $\mathcal{C}$, and let $(\circ, \bullet, \mathcal{S}, \beta, N)$ be a generalised Mermin-type argument in it. If the associated empirical model is contextual, then it is $\mathrm{AvN}_{\mathbb{Z},K}$.

[22] This gives rise to some interesting results on affine closures, see [ABK+15].

Proof. The associated probabilistic empirical model is given by Equations 4.65 and 4.66: the only scalars appearing are 0 and the invertible $\frac{1}{|K(\bullet)|}$, which are (necessarily) sent to 0 and 1 respectively in the passage to the possibilistic empirical model. The possibilistic empirical model is as follows:

$$\mathbb{P}[(g_1, ..., g_N)|\text{control}] = \begin{cases} 1 & \text{if } g_1 \oplus ... \oplus g_N = 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.89}$$

$$\mathbb{P}[(g_1, ..., g_N)|k^{th} \text{ variation for } s] = \begin{cases} 1 & \text{if } g_1 \oplus ... \oplus g_N = a^s \\ 0 & \text{otherwise} \end{cases} \tag{4.90}$$

The possibilistic empirical model has the following support subpresheaf $\mathbb{S} \subseteq \mathcal{E}$:

$$\mathbb{S}[\text{control}] = \left\{ (c^i_{m^0_i})_{i=1}^N \in K^N \;\middle|\; \oplus_{i=1}^N c^i_{m^0_i} =_K 0 \right\} \tag{4.91}$$

$$\mathbb{S}[k^{th} \text{ variation for } s] = \left\{ (c^i_{m^s_{i+(k-1)}})_{i=1}^N \in K^N \;\middle|\; \oplus_{i=1}^N c^i_{m^s_{i+(k-1)}} =_K a^s \right\} \tag{4.92}$$

Amongst the (many) equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$ we can find the following $1 + N \cdot S$ equations:

$$\bigoplus_m s_m = 0, \text{ satisfied by all } s \in \mathbb{S}[\text{control}] \tag{4.93}$$

$$\bigoplus_m s_m = a^s, \text{ satisfied by all } s \in \mathbb{S}[k^{th} \text{ variation for } s] \tag{4.94}$$

Any global assignment satisfying all equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$ would in particular satisfy the $1 + N \cdot S$ equations above, and hence provide a solution in K to the system $\mathcal{S}$, as shown in the proof of Theorem 4.16. If the empirical model is contextual, then by Theorem 4.16 no such solution can exist: hence there can be no global assignment satisfying all equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$, proving that the model is in particular $\text{AvN}_{\mathbb{Z},K}$. □

Corollary 4.19. *The generalised Mermin-type arguments provide an infinite family of quantum realisable* $\text{AvN}_{\mathbb{Z},K}$ *empirical models, indexed by all finite abelian groups K and all finite consistent systems $\mathcal{S}$ of $\mathbb{Z}$-module equations valued in K which admit no solution in K. Furthermore, all* $\text{AvN}_{\mathbb{Z},K}$ *arguments for some fixed K are equivalently* $\text{AvN}_{\mathbb{Z}_n,K}$ *for any positive integer n divisible by the exponent of K: as a consequence, there are generalised Mermin-type arguments providing quantum realisable* $\text{AvN}_{\mathbb{Z}_n}$ *models for all positive integers $n \geq 2$.*

Proof. The first part is a straightforward consequence of Theorems 4.16, 4.17, 4.18 and 4.20 below. The second part is a consequence of the fact that any $\mathbb{Z}$-module equation valued in a finite abelian group K is equivalent to a $\mathbb{Z}_{\exp[K]}$-module equation (by taking remainders modulo $\exp[K]$ of all coefficients), and hence also to a $\mathbb{Z}_n$-module equation for any n divisible by the exponent $\exp[K]$ (by taking reminders modulo n of all coefficients). The last part is the special case where we consider the finite abelian group $K = \mathbb{Z}_n$ as a module over the ring $\mathcal{R} = \mathbb{Z}_n$. □

One open question about All-vs-Nothing arguments asks whether all quantum realisable $\mathrm{AvN}_{\mathbb{Z}}$ models are in fact $\mathrm{AvN}_{\mathbb{Z}_2}$. The following result answers the question negatively, showing that the infinite family of $\mathrm{AvN}_{\mathbb{Z}}$ models provided by the previous corollary form a non-collapsing hierarchy of $\mathrm{AvN}_{\mathbb{Z}_p}$ models for all $n \geq 2$.

Theorem 4.20 (Non-collapsing AvN hierarchy over finite fields).
For each $n \geq 2$, there is a quantum realisable $\mathrm{AvN}_{\mathbb{Z}_n}$ (and hence also $\mathrm{AvN}_{\mathbb{Z},\mathbb{Z}_n}$) empirical model which is not $\mathrm{AvN}_{\mathbb{Z}_m,K'}$ for any $m \geq 2$ coprime with n and any non-trivial abelian group K' with exponent dividing m; in particular, it is not $\mathrm{AvN}_{\mathbb{Z}_m}$.

Proof. The next Section fully works out the example of $K := \mathbb{Z}_n$ with the system $\mathcal{S}$ consisting of a single $\mathbb{Z}$-module equation $ty = 1$. If we pick a $t \in \{2, ..., n-1\}$ which divides n, the equation cannot be satisfied for $K = \mathbb{Z}_n$, giving rise to a model which is both $\mathrm{AvN}_{\mathbb{Z},\mathbb{Z}_n}$ and $\mathrm{AvN}_{\mathbb{Z}_n}$ (because the equation can be replaced by an equivalent $\mathbb{Z}_n$-module equation). Now consider some m coprime with n, and some abelian group K' with exponent dividing m. Then the equation has solutions in K', giving rise to a model which is not $\mathrm{AvN}_{\mathbb{Z},K'}$ nor $\mathrm{AvN}_{\mathbb{Z}_m,K'}$ (nor $\mathrm{AvN}_{\mathbb{Z}_m}$, in the case $K' := \mathbb{Z}_m$). Indeed, we must have $K' \cong \prod_{l=1}^{L} \mathbb{Z}_{p_l^{e_l}}$ for some primes p_l not dividing n and some exponents $e_l \geq 1$, and the equation has solutions in $\mathbb{Z}_{p_l^{e_l}}$ for all l (because t has the same prime factors of n, and hence no p_l can divide t). □

4.2.6 A fully worked-out example

In this Section, we fully work out a generalised Mermin-type argument, for the group $K := \mathbb{Z}_d$ and the system $\mathcal{S}$ consisting of a single $\mathbb{Z}$-module equation $ty = 1$ (i.e. we have $S = M = 1$), where $d \geq 2$ and $t \in \{1, ..., d-1\}$. This can equivalently be seen as a $\mathbb{Z}_d$-module equation $ty = 1 \pmod d$. We will go through the following stages: (i) we will present the measurement scenario and empirical model explicitly; (ii) we will characterise local hidden variable models; (iii) we will discuss the equations turning the model into an All-vs-Nothing argument; (iv) we will give a concrete realisation in terms of GHZ states and phase gates on qudits (i.e. d-dimensional quantum systems).

4.2.6.1 Measurement scenario.

Firstly, the exponent of $\mathbb{Z}_d$ is $k := d$, and we fix a number of parties $N = 1 \mod d$ (e.g. $N = d + 1$). Each party $i = 1, ..., N$ can make a measurement choice m_i in the set $\{0, 1\}$, and the measurement contexts take the following form. In the control, all parties make measurement choice 0, while the variations are N cyclic permutations, each one featuring $N - t$ contiguous parties making measurement choice 0 and t parties making measurement choice 1:

Party:	1	2	...	$N-t-1$	$N-t$	$N-t+1$	...	$N-1$	N
control	0	0	...	0	0	0	...	0	0
1^{st} variation	0	0	...	0	0	1	...	1	1
2^{nd} variation	0	0	...	0	1	1	...	1	0
3^{rd} variation	0	0	...	1	1	1	...	0	0
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
N^{th} variation	1	0	...	0	0	0	...	1	1

(4.95)

4.2.6.2 Empirical model.

The joint measurement outcomes $(g_1, ..., g_N)$ for the N parties are valued in $\mathbb{Z}_d^N$, and the generalised Mermin-type argument is associated with the following probabilistic empirical model:

	$g_1 \oplus ... \oplus g_N = 0$	$g_1 \oplus ... \oplus g_N = 1$	$g_1 \oplus ... \oplus g_N \neq 0, 1$
control	$\frac{1}{d^{N-1}}$	0	0
1^{st} variation	0	$\frac{1}{d^{N-1}}$	0
2^{nd} variation	0	$\frac{1}{d^{N-1}}$	0
3^{rd} variation	0	$\frac{1}{d^{N-1}}$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N^{th} variation	0	$\frac{1}{d^{N-1}}$	0

(4.96)

4.2.6.3 Local hidden variable models.

When t and d are coprime, the equation $ty = 1 \pmod{d}$ has a (unique) solution $y := t^{-1} \pmod{d}$, and a local hidden variable model for the empirical model 4.96 can be obtained as follows.

Consider the set Λ of all the $(g_1, ..., g_N) \in \mathbb{Z}_d^n$ such that $g_1 \oplus ... \oplus g_N = 0$, together with the uniform probability distribution $p : \Lambda \to \mathbb{R}^+$ on Λ (i.e. $p(g_1, ..., g_N) = \frac{1}{d^{N-1}}$). Also, consider deterministic local outcomes for each fixed value $\underline{g} \in \Lambda$ of the hidden variable such that, upon measurement choice m_i for party i, the measurement outcome is g_i whenever $m_i = 0$ and $g_i \oplus t^{-1}$ whenever $m_i = 1$.

In the control, all parties $i = 1, ..., N$ will choose $m_i = 0$, and the joint measurement outcome will be uniformly distributed over the subgroup $\Lambda \subset \mathbb{Z}_d^N$. In any variation, t parties will choose $m_i = 1$ and $N - t$ parties will choose $m_i = 0$, and the joint measurement outcome will be uniformly distributed over the coset $(1, 0, ..., 0) \oplus \Lambda \subset \mathbb{Z}_d^N$ (using the fact that $t \cdot t^{-1} = 1$ in $\mathbb{Z}_d$). Hence this really defines a local hidden variable model for the empirical model 4.96 associated with the generalised Mermin-type argument.

4.2.6.4 All-vs-Nothing arguments.

When t and d are not coprime, the equation $ty = 1 \pmod{d}$ cannot have solutions in $K = \mathbb{Z}_d$ (by a standard argument from number theory). The possibilistic empirical model associated with the argument has the following support subpresheaf $\mathbb{S} \subseteq \mathcal{E}$ (the control and the first three variations are shown here, to exemplify the pattern):

$$\begin{aligned} \mathbb{S}[\text{control}] = \ & \text{the set of all } (g_0^1, g_0^2, ..., g_0^{N-t-1}, g_0^{N-t}, g_0^{N-t+1}, ..., g_0^{N-1}, g_0^N) \in \mathbb{Z}_d^N \\ & \text{such that } \bigoplus_{i=1}^{N} g_0^i = 0 \end{aligned} \tag{4.97}$$

$$\begin{aligned} \mathbb{S}[1^{st} \text{ var'n}] = \ & \text{the set of all } (g_0^1, g_0^2, ..., g_0^{N-t-1}, g_0^{N-t}, g_1^{N-t+1}, ..., g_1^{N-1}, g_1^N) \in \mathbb{Z}_d^N \\ & \text{such that } \Big(\bigoplus_{i=1}^{N-t} g_0^i\Big) \oplus \Big(\bigoplus_{i=N-t+1}^{N} g_1^i\Big) = 1 \end{aligned} \tag{4.98}$$

$$\begin{aligned} \mathbb{S}[2^{nd} \text{ var'n}] = \ & \text{the set of all } (g_0^1, g_0^2, ..., g_0^{N-t-1}, g_1^{N-t}, g_1^{N-t+1}, ..., g_1^{N-1}, g_0^N) \in \mathbb{Z}_d^N \\ & \text{such that } \Big(g_0^N \oplus \bigoplus_{i=1}^{N-t-1} g_0^i\Big) \oplus \Big(\bigoplus_{i=N-t}^{N-1} g_1^i\Big) = 1 \end{aligned} \tag{4.99}$$

$$\begin{aligned} \mathbb{S}[3^{rd} \text{ var'n}] = \ & \text{the set of all } (g_0^1, g_0^2, ..., g_1^{N-t-1}, g_1^{N-t}, g_1^{N-t+1}, ..., g_0^{N-1}, g_0^N) \in \mathbb{Z}_d^N \\ & \text{such that } \Big(g_0^{N-1} \oplus g_0^N \oplus \bigoplus_{i=1}^{N-t-2} g_0^i\Big) \oplus \Big(\bigoplus_{i=N-t-1}^{N-2} g_1^i\Big) = 1 \end{aligned} \tag{4.100}$$

Amongst the (many) equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$ we can find the $N + 1$ equations equations above, one for the control (Equation 4.97) and N for the variations (Equations 4.98, 4.99 and 4.100, corresponding to the first three variations, exemplify the pattern), and any global assignment $(g_r^i)_{r=0,1}^{i=1,...,N}$ which satisfies all equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$ would in particular satisfy those $N + 1$ equations. However, adding up the N equations corresponding to the variations yields, after a bit of rearranging, the following equation (recall that $N = 1 \pmod{d}$):

$$(N-t)\Big(\bigoplus_{i=1}^{N} g_0^i\Big) \oplus t\Big(\bigoplus_{i=1}^{N} g_1^i\Big) = N \cdot 1 = 1 \tag{4.101}$$

Taking this together with the equation $\bigoplus_{i=1}^{N} g_0^i = 0$ associated with the control then results in the following equation:

$$t\Big(\bigoplus_{i=1}^{N} g_1^i\Big) = 1 \tag{4.102}$$

But this means that setting $y := \bigoplus_{i=1}^{N} g_1^i$ would yield a solution to the equation $ty = 1$ in $\mathbb{Z}_d$, which we assumed not to exist. Hence we cannot have any global assignment satisfying all equations in $\mathbb{T}_{\mathbb{Z}}(\mathbb{S})$, and the model is both $\mathrm{AvN}_{\mathbb{Z},\mathbb{Z}_n}$ and $\mathrm{AvN}_{\mathbb{Z}_n}$.

4.2.6.5 Quantum realisation

We now give a concrete realisation of this generalised Mermin-type argument in quantum-like theories of wavefunctions over commutative involutive semirings S, i.e. in R-probabilistic CP* categories CP*[S-Mat] (where R is the sub-semiring of positive elements in S). Let $(P, \cdot, 1) := \{x \in S \mid x^* x = 1\}$ be the multiplicative group of phases in S, and let ○ be the †-SCFA corresponding to the standard orthonormal basis $(|j\rangle)_{j \in \mathbb{Z}_d}$ of the quantum system $S^{\mathbb{Z}_d}$:

$$-\!\!\circ\!\!< \; := \sum_{j \in \mathbb{Z}_d} |j\rangle|j\rangle\langle j| \qquad\qquad -\!\!\circ \; := \sum_{j \in \mathbb{Z}_d} \langle j| \tag{4.103}$$

The ○-phase states take the form $|\alpha\rangle := \sum_{j \in \mathbb{Z}_d} \alpha_j |j\rangle$ for $\alpha_j \in P$, where without loss of generality we can set $\alpha_0 := 1$, and hence the group $(P(\circ), >\!\!\circ\!\!- , \circ\!\!-)$ of ○-phase gates is isomorphic to P^{d-1} (we will write its elements as $(\alpha_1, ..., \alpha_{d-1})$).

Assumption (i): the scalar $d := |\mathbb{Z}_d|$ is invertible in R. If $|\mathbb{Z}_d|$ is invertible in R, then the following defines a †-qSCFA on $S^{\mathbb{Z}_d}$:

$$>\!\!\bullet\!\!- \; := \sum_{i,j \in \mathbb{Z}_d} |i \oplus j\rangle\langle i|\langle j| \qquad\qquad \bullet\!\!- \; := |0\rangle \tag{4.104}$$

Then $(\circ, \bullet)$ form a strongly complementary pair, with $(K(\circ), >\!\!\bullet\!\!- , \bullet\!\!-) \cong \mathbb{Z}_d$.

Assumption (ii): the group P contains some element ζ of order d. If an element $\zeta \in P$ of order d exists, we can define the following group homomorphisms $\chi_k : \mathbb{Z}_d \to P$ for all $k \in \mathbb{Z}_d$:

$$\chi_k : j \mapsto \zeta^{jk} \tag{4.105}$$

Then these are exactly the S-valued multiplicative characters of $\mathbb{Z}_d$, and correspond to the ●-classical states $|\chi_k\rangle := \sum_{j\in} \zeta^{jk}|j\rangle$. There is a group isomorphism between the group of S-valued multiplicative characters and the group of complex multiplicative characters (e.g. given by $\zeta \leftrightarrow e^{i\frac{2\pi}{d}}$): as a consequence the S-valued multiplicative characters are enough to discriminate between elements of $\mathbb{Z}_d$, and thus the observable ● has enough classical states (and we can legitimately measure in it).

Assumption (iii): the group P contains some element ξ of order dt, and we picked $\zeta := \xi^t$ to satisfy Assumption (ii) above. The ○-classical states form the subgroup (K(●), ≻○– , ○–) $\cong \mathbb{Z}_d$ of the group of ○-phase gates, having elements in the form $\chi_k \equiv (\zeta^k, \zeta^{2k}, ..., \zeta^{(d-1)k})$. In this subgroup, the equation $ty = \chi_1 = (\zeta, \zeta^2, ..., \zeta^{d-1})$ does not admit any solution, because it doesn't in $\mathbb{Z}_d$. However, a solution $y := \beta$ exists in the larger group (P(○), ≻○– , ○–) of ○-phase states, in the form $\beta := (\xi, \xi^2, ..., \xi^{d-1})$. The corresponding ○-phase gate $P_\beta := \sum_{j\in\mathbb{Z}_d} \xi^j |j\rangle\langle j|$ can be then used to implement our generalised Mermin-type argument in CP*[S-Mat].

Now we cover some specific quantum-like theories of interest:

(i) In the case of ordinary quantum theory, d is always invertible. We have that $P = S^1$, and we can always take $\xi := e^{i\frac{2\pi}{dt}}$ and $\zeta := e^{i\frac{2\pi}{d}}$.

(ii) In the case of real quantum theory, d is always invertible. However, we have that $P = \{\pm 1\}$, and hence the only argument allowed is the trivial one with $\mathbb{Z}_2$ and the equation $1 \cdot y = 1$ (which has solution $y := 1$ in $\mathbb{Z}_2$).

(iii) In the case of hyperbolic quantum theory, d is always invertible. However, we have $P = SO(1,1) \cong \mathbb{Z}_2 \times \mathbb{R}$, and again the only argument allowed is the trivial one with $\mathbb{Z}_2$ and the equation $1 \cdot y = 1$. Contrary to real quantum theory, non-trivial arguments would be allowed in hyperbolic quantum theory for infinite groups such as $\mathbb{Z}$; their implementation in the non-standard framework is left to future work.

(iv) In the case of finite-field quantum theory, the phase group takes the form $P \cong \mathbb{Z}_{p^n+1}$: an element ζ of order d exists if and only if $d|p^n+1$, and an element ξ of order dt exists if and only if $dt|p^n+1$. When this is the case, d is necessarily an invertible scalar (because d divides p^n+1, we cannot have that p divides d).

(v) In the case of relational quantum theory, parity quantum theory and tropical quantum theory we have $P = \{1\}$, and no value of d is admissible.

4.2.7 Quantum-classical Secret Sharing

In contrast to other information security protocols, classical secret sharing comes with the intrinsic assumption that some participants cannot, to some extent, be trusted. A *dealer* is interested in sharing some *secret* with a number of *players*, with the caveat that the secret be revealed to the players only when all players agree to cooperate[23]. Integrity and availability of communications is guaranteed by the existence of authenticated classical channels between dealer and players, and the protocol is only concerned with confidentiality, defined as the impossibility of recovering the secret unless all players cooperate.

The quantum-classical scheme of Hillery, Bužek and Berthiaume [HBB99] introduces a new layer of security to secret sharing, employing entangled states and non-commuting observables to detect eavesdropping. The HBB scheme is based on the same measurement contexts of Mermin's original parity argument: a dealer and $N-1$ players share N qubits in a GHZ state (with respect to the computational basis associated with the Pauli Z observable), and randomly choose to measure their qubit in either of the mutually unbiased Pauli X or Pauli Y observables. It can be shown [Zam12] that confidentiality is an immediate consequence of strong complementarity of the Pauli Z and X observables, while eavesdropping detection follows from mutual unbias of the Pauli X and Y observables.

We extend the HBB scheme from Mermin's original parity argument to our generalised Mermin-type arguments, and we use our result on contextuality to provide a number of device-independent security guarantees. For the remainder of this section, we will consider a generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$, on an object $\mathcal{H}$ of a R-probabilistic CP* category.

Consider a **dealer**, call her Alice, who wishes to share a **secret** with N' *players*, where $2 \leq N' < N$. As the owner of the secret, Alice is always a trusted party, the *only* trusted party in the protocol. The secret is assumed to take the form of a string of elements of $K(\bullet)$, the **plaintext** (at most one element of $K(\bullet)$, the **round plaintext**, transmitted for each round of the protocol). We wish to ensure that the plaintext can be decoded from the information Alice sends, the **cyphertext**, if and only if all players agree to cooperate (by which we mean that they all reveal their secret keys to some party in possession of the cyphertext). Alice and the players are given N devices (one per player, and $N - N'$ for Alice): at each round w, each device B_j is fed an **input** $m_j^w \in \{0, 1, ..., M\}$ and returns an **output** $g_j^w \in K(\bullet)$ (we also refer to the

[23] More in general, a minimum number of cooperating players can be specified.

outputs $g_1^w, ..., g_{N'}^w$ as the **secret keys** of the players for round w). We furthermore assume the following **security conditions** to hold.

(i) Alice and the players share an authenticated classical channel, ensuring integrity and availability of all classical communications involved in the protocol.

(iia) Alice and the players are in possession of N secure independent classical sources of randomness, to generate independent inputs at each round which are uniformly distributed in $\{0, 1, ..., M\}$.

(iib) Alice is in possession of a secure classical source of randomness, independent from all other, to decide which rounds will be **secret rounds** (with probability $(1 - \tau) > 0$) and which rounds will be **test rounds** (with probability $\tau > 0$).

(iii) During step 2 of the protocol below, no signalling is possible between distinct parties/devices[24].

(iv) We will assume that in step 3 Alice is communicated the measurement choices faithfully[25].

Because tampering can only be determined after the protocol has ended and the entirety (or an otherwise significant portion) of the plaintext has been transmitted, we distinguish between the **plaintext**, the data that can be decoded using the secret keys, and the actual **secret** that Alice wants the players to share. Before the protocol begins, Alice will obtain the plaintext by encrypting the secret with a secure symmetric encryption protocol[26], using a freshly generated ephemeral key which she will broadcast only if the protocol is successful. If the protocol fails, the random key will not be broadcast and the secret will be unrecoverable even if the plaintext is decoded.

The quantum-classical secret sharing protocol then proceeds as follows for each round $w = 1, ..., W$, until the entire secret has been transmitted. An individual round for a noiseless, trusted implementation is presented in Figure 4.1. Throughout the protocol, Alice keeps a count of occurrences of joint outputs $g_1, ..., g_N$ conditional to each joint input $m_1, ..., m_N$ that she observes in test rounds.

[24] This can be achieved, for example, by ensuring the devices are operated in conditions controlled by Alice (trusted laboratories, synchronized time-stamp servers, etc).

[25] This can be achieved by entrusting the laboratory setup with the communication of the random measurement choices to Alice, the player and the device.

[26] If the secret is in the form of a string of elements of $K(\bullet)$, the natural choice for this protocol, then the plaintext can be obtained by generating a string of uniformly random k^w elements of $K(\bullet)$, obtaining the round plaintext p^w from the corresponding "round secret" q^w as $p^w = q^w \oplus k^w$. Once the string of random elements is broadcast, upon successful completion of the protocol, the secret can be recovered from the decoded plaintext as $q^w = p^w \ominus k^w$.

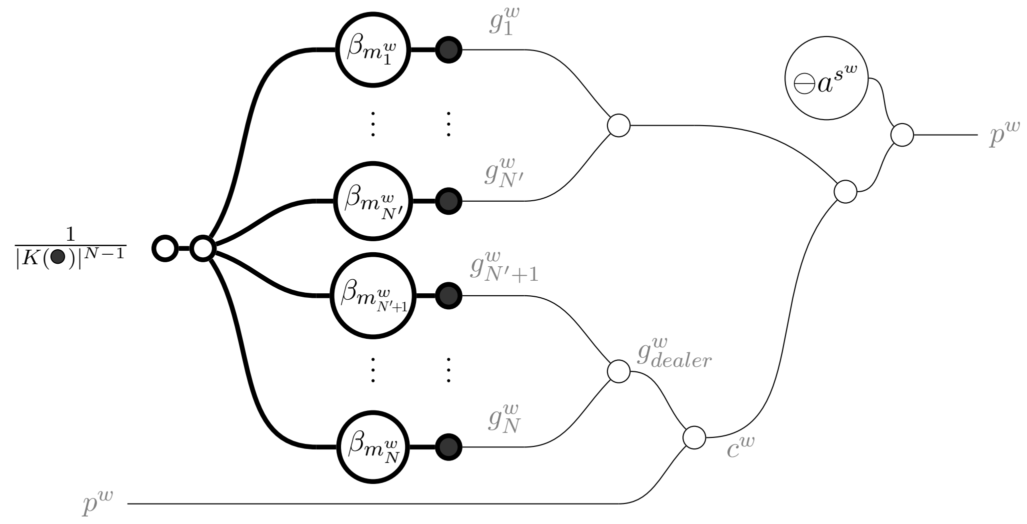


Figure 4.1: Graphical presentation of a noiseless, trusted implementation.

1. Alice and the players share N subsystems of a state ρ: each player has an individual subsystem and Alice keeps the remaining $N - N'$ subsystems. In a noiseless, trusted implementation, ρ is the N-partite $\circ$-GHZ state. For the purposes of a device-independent security analysis, ρ can be potentially any state (pure or mixed).

2. Alice and the players each sample their classical source of randomness and obtain inputs $m_1^w, ..., m_N^w$ which are passed to the devices $B_1, ..., B_N$ and result in outputs $g_1^w, ..., g_{N'}^w \in K(\bullet)$ for the players (the secret keys for the round) and $g_{N'+1}^w, ..., g_N^w \in K(\bullet)$ for Alice. In a noiseless, trusted implementation, B_j with input m_j^w applies the phase gate $P_{\beta_{m_j^w}}$ to the subsystem j and then measures it in the $\bullet$ observable.

3. The inputs for the players are communicated to Alice. She checks that $m_1^w, ..., m_N^w$ define a valid **measurement context** (either the control ($s = 0$) or a variation for some $s = 1, ..., S$).

4. Alice samples her source of randomness to decide whether the round will be a test round or a secret round.

4a. If the round is a test round, Alice requests all players to communicate their secret keys, and she increases the occurrence count for joint output $(g_1^w, ..., g_N^w)$ conditional to joint input $(m_1^w, ..., m_N^w)$.

4b. If the round is a secret round, Alice computes $g_{dealer}^w := \bigoplus_{j=N'+1}^{N} g_j^w$ and broadcasts the **round ciphertext** $c^w := p^w \oplus g_{dealer}^w$ to the players, where the **round**

plaintext p^w is the next element of the plaintext to be sent. She also broadcasts the relevant value $s^w \in \{0, 1, ..., S\}$ obtained from the joint inputs $m_1^w, ..., m_N^w$.

5. Anyone in possession of s^w, the round ciphertext c^w, and all secret keys $g_1^w, ..., g_{N'}^w$ can obtain the round plaintext p^w by computing $p^w = (c^w \oplus g_1^w \oplus ... \oplus g_{N'}^w) \ominus a^{s^w}$, where s^w is the value broadcast in Step 3.

The chosen generalised Mermin-type argument determines the following **promised conditional distribution** $\mathbb{P}_{promised}\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$, the one which Alice and the players expect to observe (asymptotically) in a trusted noiseless implementation (we use the more compact notation $\underline{g} := (g_1, ..., g_N)$ for the joint output and $\underline{m} := (m_1, ..., m_N)$ for the joint input):

$$\mathbb{P}_{promised}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] = \begin{cases} \frac{1}{|K(\bullet)|^{N-1}} & \text{if } g_1 \oplus ... \oplus g_N = \beta_{m_1} \oplus ... \oplus \beta_{m_N} \\ 0 & \text{otherwise} \end{cases} \tag{4.106}$$

At the end of the protocol, Alice normalises her joint output counts for each joint input to obtain the **observed conditional distribution** $\mathbb{P}_{observed}\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$ (which need not be no-signalling). She then computes the **noise parameter** ϵ as follows:

$$\epsilon := 1 - |K(\bullet)|^{N-1} \min \Big\{ \mathbb{P}_{observed}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] \Big| g_1 \oplus ... \oplus g_N = \beta_{m_1} \oplus ... \oplus \beta_{m_N} \Big\} \tag{4.107}$$

The error parameter as defined above is the smallest $\epsilon \in [0, 1]$ such that the observed conditional distribution can be decomposed as the following convex combination of promised conditional distribution and some **noise conditional distribution** $\mathbb{P}_{noise}\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$:

$$\mathbb{P}_{observed}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] = (1 - \epsilon)\, \mathbb{P}_{promised}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] + \epsilon\, \mathbb{P}_{noise}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] \tag{4.108}$$

Before a run of the protocol begins, Alice sets a maximum ϵ_{max} that she is going to accept for the noise parameter. Alice chooses as low an ϵ_{max} as possible compatibly with the specifications of the device provider (and any other beliefs she might have) on the amount of noise she should expect from the devices and states in the absence of any tampering from Eve. At the end of the protocol run, Alice compares the noise parameter ϵ she computed with the maximum ϵ_{max} she decided to accept: if $\epsilon \leq \epsilon_{max}$, she declares the protocol run a success and broadcasts the ephemeral key she used to encode the secret into the plaintext; if $\epsilon > \epsilon_{max}$, she declares the protocol run a failure and she destroys the ephemeral key, rendering the secret unrecoverable even if the plaintext is at some point obtained by the players or by Eve.

The HBB quantum-classical secret sharing protocol comes with two security guarantees: (i) ignorance about any one secret key for a round denies knowledge about the plaintext for that round; (ii) successful, undetected eavesdropping has low probability. It can be shown [Zam12] that in a noiseless and trusted implementation the first guarantee follows abstractly from strong complementarity of the Pauli Z and X observables, and the proof straightforwardly transfers to the strongly complementary pairs $(\circ, \bullet)$ appearing in our generalised protocol. Instead of treating eavesdropping directly, we will present a more general, device-independent proof of security, based solely on contextuality of the generalised Mermin-type argument used by the protocol.

Works on device-independent security (such as [BHK05, VV14] on quantum key distribution) usually posit Eve to be an adversary who can arbitrarily tamper with the shared state and measurement devices, and is only bound in her attempts by the physical theory under consideration[27] and by the security conditions explicitly enforced by the protocol (including no-signalling). Examples of things that the Eve can to do include:

(i) the measurement outcomes broadcast at a test round can reveal to Eve information about measurement outcomes in previous secret rounds;

(ii) Eve can keep a subsystem of the shared state to herself, which she can optimally measure, once all inputs and test round outputs have been broadcast, to obtain information about the secret keys.

Our choice of a device-independent setting comes from the more modest desire to show that the security guarantees follow from contextuality of the generalised Mermin-type argument, regardless of the specific implementation; as a consequence, we will be content with a more restricted model of attack. We assume that Alice and the players might be provided with noisy or imperfect states and devices, which might give Eve a variety of security loopholes to exploit. However, we assume that the device provider shows no malice:

(i) the devices are memoryless and operate independently at each round;

(ii) the states used at different rounds are independent and identical;

(iii) the states are not entangled with any additional system.

[27] Eve is often assumed to be bound by the laws of quantum theory, but sometimes super-quantum attackers are also considered, bound only by causality and no-signalling.

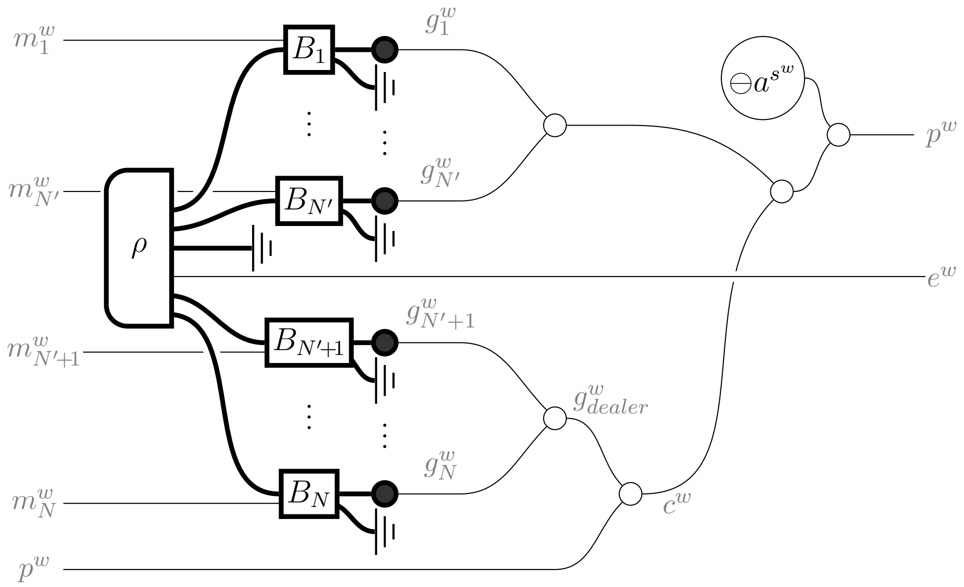


Figure 4.2: Graphical presentation of a generic, untrusted implementation at a single round of the protocol. Eve might have some classical information e^w about the states which Alice and the players don't know. The classical side of the protocol is entirely in the hands of Alice and the players, and proceeds as in the trusted noiseless case.

However, Eve might possess classical information about the states which is unavailable to the players (such as information leaked through noise or side channels, information acquired via eavesdropping, etc).

Although not fully general, this setup subsumes a variety of more specialised security scenarios that are of interest in classical and quantum cryptography:

(i) Real-world implementations are unavoidably noisy, and one should consider any noise as a potential source of cryptophthora[28]. Our setup allows for the possibility that both the shared state and the measurement devices be noisy, with no dependence on a specific model of noise; it also allows for the possibility that what looks like random noise to Alice and the players might actually carry side-channel information to Eve.

(ii) Eavesdropping detection is a typical desideratum in quantum cryptography, where Eve intercepts the local state of a player[29], measures it in some basis to obtain classical information, and forwards the resulting collapsed state to the player.

[28] Secret degradation, usually due to side-channel leakage.

[29] In our secret sharing protocol, a single player's secret key is all that Eve needs to break confidentiality, as we may freely assume that the remaining players are colluding with Eve.

> Our setup allows for the possibility of eavesdropping[30]: the classical information that Eve possesses about the state can be used to model the information she acquired by eavesdropping. Our security proof then has eavesdropping detection as a special case of protocol failure.

Figure 4.2 displays a single round w of the protocol in a generic, untrusted implementation. An N-partite state ρ is shared between Alice and the players at a given round of the protocol, with no additional subsystem accessible to Eve (who might however be in possession of classical information e^w about it). The measurement devices $B_1, ..., B_N$ operate independently at each round, with no memory or shared resource other than the state ρ. At each round w, device B_j takes measurement choice m_j^w as a classical input and returns measurement outcome g_j^w as a classical output. The rest of the protocol is entirely in the hands of Alice and the players, and proceeds as in the trusted noiseless case.

Our first result shows that lack of contextuality implies the existence of a scenario in which a perfect undetectable attack may take place. In fact, the scenario is not particularly remote: it might well happen happen that the device provider inadvertently chose phase states $\beta_1, ..., \beta_M$ which happen to be $\bullet$-classical states (maybe she did not notice, maybe she was tricked by Eve into choosing them), and that the GHZ state decoheres (spontaneously or with a malicious helping hand) in the $\bullet$ observable. In that case, Alice and the players will notice nothing wrong with their protocol, and Eve will obtain the entirety of the secret all by herself.

Theorem 4.21 (Perfect undetectable attack).
Consider a quantum-classical secret sharing protocol based on a generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$, in a R-probabilistic CP category with a positive semiring R of scalars. If the associated empirical model is non-contextual, then there is a shared state ρ and measurement devices $B_1, ..., B_N$ such that test rounds will succeed with certainty, and Eve will always know all the secret keys.*

Proof. By Theorem 4.16, if the empirical model is non-contextual then there exists a solution $(y_r := b_r)_{r=1}^M$ in $K(\bullet)$ to the system $\mathcal{S}$ (which we take to be in the form of System 4.56). For each round w, Eve samples a random variable uniformly distributed over the following set:

$$\left\{(h_1^w, ..., h_N^w) \in K(\bullet)^N \;\middle|\; h_1^w \oplus ... \oplus h_N^w = 0\right\} \tag{4.109}$$

[30] However, it does not cover a more advanced attack in which Eve sends through a subsystem of an entangled state, keeping the rest of the state to herself and measuring it in the future to obtain more information about the player's outcome.

Now assume that the separable pure state $|h_1^w\rangle \otimes ... \otimes |h_N^w\rangle$ is given in input to the measurement devices $B_1, ..., B_N$ at round w, and that the devices are designed so that B_j returns $g_j^w := h_j^w \oplus b_{m_j^w}$ upon measurement choice m_j^w (i.e. applies a phase $b_{m_j^w}$ which happens to be $\bullet$-classical). The state seen by Alice and the players is following round-independent mixed state ρ, but Eve at each round has additional information e^w which helps her identify which pure component of ρ will actually be sent to the parties at that specific round:

$$\rho := \sum_{h_1 \oplus ... \oplus h_N = 0} \frac{1}{|K(\bullet)|^{N-1}} |h_1\rangle\langle h_1| \otimes ... \otimes |h_N\rangle\langle h_1| \tag{4.110}$$

Once the measurement $(m_j^w)_{j=1}^{N'}$ choices for the players are broadcast, Eve can compute all the secret keys $(g_j^w)_{j=1}^{N'}$. Furthermore, since $(b_r)_{r=1}^{M}$ is a solution to $\mathcal{S}$, the measurement outcomes obtained from this setup will have the same distribution as the ones from a noiseless trusted implementation, and all test rounds will succeed with certainty. □

Our second result is restricted to probabilistic theories, i.e. distributively CMon-enriched CPM categories having $\mathbb{R}^+$ as their semiring of scalars. Consider the no-signalling polytope associated with the measurement scenario of a contextual generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$, and let F be the face of the polytope specified by the support of the empirical model (the one defined by Equation 4.106). For each vertex $v \in F$ of that face, corresponding to empirical model $\mathbb{P}_v\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$, let H_v be the average entropy across all measurement contexts:

$$H_v := \frac{1}{1 + N \cdot S} \sum_{\underline{m} \in \mathcal{M}} H\Big[\,\mathbb{P}_v\big[\,\_\,\big|\,\underline{m}\,\big]\,\Big] \tag{4.111}$$

Let $H_{promised}^{(min)} := \min_{v \in F} H_v$ be the minimum average entropy across all vertices of the face: because the generalised Mermin-type argument is strongly contextual, the face cannot contain any local vertices, and hence the minimum average entropy $H_{promised}^{(min)}$ is always strictly positive; a tighter estimation of this quantity is left to future work. Call $\eta := \Big(1 - \frac{H_{promised}^{(min)}}{|K(\bullet)|^{N-1}}\Big) \in [0, 1)$ the **information leakage fraction** for the face: it is the maximum fraction of plaintexts that Eve can expect to decipher when the empirical model she sees lies on face F.

We will now show that protocols based on contextual generalised Mermin-type arguments always provide a certain amount of security: for observed noise parameter ϵ small enough, the maximum expected fraction of plaintexts that Eve can expect to decipher is sharply peaked somewhere between η and $c \cdot \epsilon$, where c is some constant depending on the geometry of the no-signalling polytope. In one extreme, we may have $\eta = 0$, i.e. all empirical model on the face carry the same maximal amount of entropy. In this case, Eve's chances of learning some parts of the secret rely entirely on the noise parameter ϵ: in her best case scenario, she observes a deterministic empirical model for some fraction ϵ of rounds, in which case she can gain complete knowledge about the round plaintext. In the other extreme, we have $\eta \gg \epsilon$, i.e. there are empirical models on the face F which might lead to more leakage of plaintext information than any number of deterministic model which might be lurking in the noise ϵ. In this case, Eve's best bet might just be to exploit the empirical models on the face F itself.

Theorem 4.22 (Device-independent security).
Consider a quantum-classical secret sharing protocol based on a generalised Mermin-type argument $(\circ, \bullet, \mathcal{S}, \beta, N)$*, in a probabilistic CP* category* $\mathrm{CP}^*[\mathcal{C}]$ *(with* $\mathbb{R}^+$ *as its positive semiring of scalars). Consider a run of the protocol with a large number* W *of rounds, of which* P *secret rounds and* T *test rounds (with* $P \rightarrow (1-\tau)W$ *and* $T \rightarrow \tau W$ *almost certainly as* $W \rightarrow \infty$*). Let* ϵ *be the noise parameter observed by Alice at the end (a random variable), and let* P_{Eve} *be maximum number of round plaintexts that Eve expects to successfully decipher (another random variable). Then the maximum fraction of plaintexts* P_{Eve}/P *that Eve expects to successfully decipher is sharply peaked around some value between* η *and* $O(\epsilon)$*, with variance bounded above by* $O(\frac{\tau(1-\tau)}{W})$ *almost certainly for* $W \rightarrow \infty$ *(where the big-O notation hides a constant depending on the geometry of the polytope alone).*

Proof. As part of this proof, a number of different conditional distributions will be considered:

(i) the no-signalling conditional distribution $\mathbb{P}_{true}(e)\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$ determined by ρ and the devices $B_1, ..., B_N$ conditional to Eve obtaining information e (this is the conditional distribution as seen from Eve's vantage point);

(ii) the no-signalling conditional distribution $\mathbb{P}_{true}\big[\, \underline{g} \,\big|\, \underline{m} \,\big] := \sum_e \mathbb{P}[e] \cdot \mathbb{P}_{true}(e)\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$ determined by ρ and the devices $B_1, ..., B_N$, averaged over Eve's information (this is the **true conditional distribution** as seen from Alice's vantage point, which her tests will estimate);

(iii) the no-signalling conditional distribution $\mathbb{P}_{promised}\big[\, \underline{g} \,\big|\, \underline{m} \,\big]$ derived from the generalised Mermin-type argument (this is what Alice would expect to estimate in the absence of any noise or tampering);

(iv) the conditional distribution $\mathbb{P}_{observed}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ estimated by Alice.

Alice's estimate of the true conditional distribution $\mathbb{P}_{true}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ can be modelled by considering the vector-valued random variables $\underline{X}^w := \big(X^w_{(\underline{g},\underline{m})}\big)$ for all test rounds w, where $X^w_{(\underline{g},\underline{m})}$ is the real-valued random variable defined as follows (note that $\underline{g}^w$ is a random element of $K(\bullet)^N$, and $\underline{m}^w$ is a uniformly random element of the set of $1 + NS$ measurement contexts):

$$X^w_{(\underline{g},\underline{m})} = \begin{cases} 1 & \text{if } \underline{g} = \underline{g}^w \text{ and } \underline{m} = \underline{m}^w \\ 0 & \text{otherwise} \end{cases} \tag{4.112}$$

The vector $\underline{X}^w$ takes the value 1 over the joint input/joint output pair recorded by Alice for round w, and 0 everywhere else: Alice's estimate of the true conditional distribution is then obtained from the average random variable $\frac{1}{T}\sum\limits_{w \text{ test}} \underline{X}^w$. By the central limit theorem, Alice's estimate $\mathbb{P}_{observed}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ will be normally distributed around the true conditional distribution, with variance $O(\frac{1}{T})$; because the noise parameter ϵ observed by Alice is obtained from this estimate, it will similarly be distributed around the true noise parameter ϵ_{true} defined below, with variance bounded above by $O(\frac{1}{T})$ (almost certainly for $T \to \infty$).

We define the **true noise parameter** ϵ_{true} to be obtained from the conditional distribution $\mathbb{P}_{true}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ in the same way that ϵ is obtained from the conditional distribution $\mathbb{P}_{observed}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$. This means ϵ_{true} is the largest such that $\mathbb{P}_{true}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ decomposes as follows, for some conditional distribution $\mathbb{P}_{true,noise}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$:

$$(1-\epsilon_{true})\,\mathbb{P}_{promised}\big[\,\underline{g}\,\big|\,\underline{m}\,\big] + (\epsilon_{true})\mathbb{P}_{true,noise}\big[\,\underline{g}\,\big|\,\underline{m}\,\big] \tag{4.113}$$

For each value $e \in E$ that Eve's information can take, we define the parameter $\xi(e) \in [0,1]$ to be the smallest possible such that the conditional distribution $\mathbb{P}_{true}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ decomposes as follows:

$$(1-\xi(e))\mathbb{P}_F(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big] + \xi(e)\mathbb{P}_{F,noise}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big] \tag{4.114}$$

for some distribution $\mathbb{P}_F(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ lying on the face F and some distribution $\mathbb{P}_{F,noise}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ lying outside of face F. To Eve, in possession of information e, the conditional distribution $\mathbb{P}_{true}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ looks like a biased coin deciding between the two following scenarios:

(a) with probability $(1-\xi(e))$, she observes a distribution $\mathbb{P}_F(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ lying on face F, which means that the fraction of the round plaintext that she expects to learn is bounded above by η;

(b) with probability $\xi(e)$, she observes some other distribution $\mathbb{P}_{F,noise}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$, which in the best case scenario could give her full knowledge of the round plaintext.

Because marginalising over Eve's knowledge[31] must result in the distribution $\mathbb{P}_{true}\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$, the geometry of the polytope implies that the convex combination $\sum_e \mathbb{P}[e]\xi(e)$ must go to zero as $O(\epsilon_{true})$ (i.e. there must be some constant $c > 0$ such that $\sum_e \mathbb{P}[e]\xi(e) \leq c \cdot \epsilon_{true}$).

It should be noted that the information e obtained by Eve is random to Eve herself: sometimes she will obtain information giving her better guessing probability, sometimes she will obtain information giving her worse guessing probability. When the distribution of e is taken into account, the fraction of round plaintexts that Eve can expect to decipher is bounded above by the following value, falling somewhere between η and $O(\epsilon_{true})$:

$$\sum_e \mathbb{P}[e] \Big((1-\xi(e))\eta + \xi(e)\Big) \tag{4.115}$$

Again by central limit theorem, the maximum fraction P_{Eve}/P of round plaintexts that Eve expects to successfully decipher is normally distributed around the value above, with variance $O(\frac{1}{P})$ (almost certainly for $P \to \infty$).

Finally, because P_{Eve}/P is sharply peaked around some value between η and $O(\epsilon_{true})$, with variance $O(\frac{1}{P})$, and because ϵ is sharply peaked around ϵ_{true}, with variance bounded above by $O(\frac{1}{T})$, we can conclude that P_{Eve}/P is sharply peaked around some value between η and $O(\epsilon)$, with variance bounded above by $O(\frac{1}{T} + \frac{1}{P})$ (which tends to $O(\frac{1}{\tau(1-\tau)W})$ almost certainly as $W \to \infty$). □

[31] I.e. taking the convex combination of the conditional distributions $\mathbb{P}_{true}(e)\big[\,\underline{g}\,\big|\,\underline{m}\,\big]$ with respect to the probability distribution $\mathbb{P}[e]$ of Eve's side-channel information.

Conclusions and future work

Categorical Quantum Dynamics

Throughout Chapter 3, we have seen how strong complementarity can be used to provide a compelling abstract description of the fundamental structural and operational features of quantum symmetries and dynamics.

We have started our journey from the familiar case of wavefunctions on periodic lattices, where we have identified the potential for strong complementarity to provide an abstract description of the relationship between the position and momentum observables. In line with our proposed coherent approach to group theory and quantum symmetries, we have defined a new notion of quantum group. Having proven a minimal set of result relating quantum groups to their classical counterparts, we have gone back to wavefunctions on periodic lattices, and we have embarked on a quest to prove that the strongly complementary observables of a quantum group truly model a sensible notion of position-momentum duality; we have shown that momentum eigenstates generate the translation symmetry, and dually that position eigenstates generate the boost symmetry; we have shown that the bialgebra law yields the Weyl form of the Canonical Commutation Relations; we have shown that putative position-momentum pair satisfies a suitably weak version of the uncertainty principle. Although narrated through the lens of periodic lattices, the results we obtained are fully general, and apply to all quantum groups.

Satisfied with our description of quantum groups as position-momentum pairs, we have shifted our attention towards more general symmetric systems. We have defined a notion of unitary representations for quantum groups, as the coherent counterparts of unitary symmetries for classical groups. Just like a classical group can be though of as a physical system exerting classical control over the symmetric system, a quantum group can be though of as a physical system exerting coherent control. We have characterised representations of quantum groups categorically as the algebras in the Eilenberg-Moore category for a certain monad, with equivariant maps as Eilenberg-

Moore morphisms. We have extended our results on symmetry-observable duality to unitary representations, and we have provided a suitable reformulation of Stone's Theorem to match them.

In order to treat the textbook case of 1-dimensional wavefunctions with periodic boundary conditions, we have introduced a new approach to infinite-dimensional separable Hilbert spaces based on non-standard analysis. Contrary to previous approaches, the category *Hilb of separable Hilbert spaces we introduced is compact closed, and has unital †-Frobenius algebras. We have then proceeded to construct a doubly well-pointed quantum group corresponding to the position-momentum pair for 1-dimensional wavefunctions with periodic boundary conditions. We have also remarked that our methods extend to all compact and discrete abelian groups.

In the final section of the Chapter, we have applied the tools developed in the remainder of the chapter to the coherent treatment of quantum dynamics. Armed with all the necessary results, we have quickly ploughed through quantum clocks and dynamical systems, we have identified a suitable coherent Hamiltonian, and we have shown that Schrödinger's Equation corresponds exactly to the defining equation for Eilenberg-Moore algebras. Using our previous results on symmetry-observable duality, we have provided simple diagrammatic proof for Stone's Theorem on 1-parameter unitary groups and von Neumann's Mean Ergodic Theorem, in the case of discrete periodic, discrete and continuous periodic dynamics. We have provided an abstract characterisation of the Feynman clock construction, and proven its validity in our framework (for arbitrary quantum groups). Finally, we have tackled the issue of synchronisation of dynamical systems, provided conditions for the existence of internal time observables, and proven sufficient conditions for the emergence of quantum clocks amongst synchronised systems.

Chapter 3 sure contains a lot of material, but a lot of work remains to be done. To begin with, we don't have a satisfactory characterisation of non-well-pointed quantum groups in fHilb, other than "they sort of look like other definitions of quantum groups". A structural theorem, akin to the one for well-pointed quantum groups, would make for a rounder picture, especially in connection with non-commutative geometry.

As far as the characterisation of quantum groups as position-momentum pairs is concerned, the desirable results are all there, with the possible exception of the uncertainty principle. While it is true that the full uncertainty principle is undesirably strong, the version we have proven might be seen as excessively weak, and a middle ground could perhaps be reached.

The state of symmetry-observable duality for general symmetric systems is also pretty satisfactory, but their categorical characterisation as Eilenberg-Moore algebras is open territory. Some additional results on the monadic approach to dynamics has been obtained in [Gog15a], but have not yet been adapted to the quantum group framework presented in this work.

Infinite-dimensional categorical quantum mechanics is perhaps the youngest addition here, and certainly requires more work and thought. While the techniques we exemplified extend straightforwardly to other compact and discrete abelian groups, it would greatly benefit the have a number of other examples of interest fully worked out. Extensions of the framework to locally compact symmetries and quantum field theory are currently in the making.

Finally, three main avenues of research are currently open in the applications to dynamics. Firstly, one would like to extend the results to the real-world case of continuous dynamics, governed by the symmetry group $(\mathbb{R}, +, 0)$. The main challenge, the derivation of a suitable coherent group, has already been solved in recent work, so this is mostly a matter of adapting the results where necessary, and reap the rewards. Secondly, our results on internal time observable have already answered some questions in the context of time observables in quantum theory, and we expect that techniques and ideas derived from them will provide a significant contribution to the debate in the near future. Thirdly, the very last results in the chapter point towards the possibility of formulating a toy model for emergent time in quantum theory based solely on hierarchies of mutually synchronised discrete periodic quantum clocks: a brief argument in favour of this construction has already been sketched, but the full development of such a model is left to future work.

Hidden Subgroup Problem

The abelian Hidden Subgroup Problem comprises many of the problems successfully tackled by quantum algorithms as special instances, but the traditional presentation of the quantum solution is too heavily algebraic to clearly show the key structures at work. In Chapter 4, we improved upon previous work by presenting the first fully graphical proof of correctness for the algorithm, proving that strong complementarity is the key algebraic feature behind the quantum advantage in the abelian HSP.

We have remarked that our diagrammatic treatment naturally extends to the non-abelian case, and that the known intractability of the problem is more a matter of classical post-processing than an issue with the quantum part itself. We have also remarked that our approach immediately transfers to other theories possessing the required algebraic structures, and as a corollary of our work we have shown that Simon's Problem can be efficiently solved in Real Quantum Theory.

A number of questions remain open. Firstly, the group theoretic nature of the Hidden Subgroup Problem begs the question of whether strong complementarity is somehow also a necessary condition for the implementation of a suitable quantum subroutine. Secondly, it would be interesting to look at concrete implementations of our results in other theories, such as Fermionic Quantum Theory or Spekkens' Toy Model. Finally, the relationship between strong complementarity and the quantum Fourier transform prompts further investigation of the role that these algebraic structures might be playing in a number of other quantum algorithms and protocols.

One might think that a similar physical setup, with position and momentum swapped, could be used to tackle the $G = T^N$ case. However, the annihilators $\mathrm{Ann}[H] \leq \mathbb{Z}^N$ are all infinite sub-lattices of $\mathbb{Z}^N$, and the classical post-processing is left with the daunting task of reconstructing one such lattice in polynomial time from polynomially many random samples. This seems to be sufficiently close to the Shortest Independent Vectors Problem—a known hard lattice problem [BS99], related to other quantum-resistant lattice problems [Reg04b, Reg04a]—to suggest that solving the HSP for compact Lie subgroups of $\mathbb{T}^N$ might be beyond current quantum approaches; however, a thorough investigation of this issue is left to future work.

Another research direction for the infinite abelian HSP using non-standard methods lies in its application to infinite-dimensional hyperbolic quantum theory, a non-standard model of which can be easily constructed on the same lines of *Hilb. We remarked that hyperbolic quantum theory does not have admit enough multiplicative characters for finite abelian groups other than $\mathbb{Z}_2^M$. However, it does admit enough multiplicative characters for the infinite abelian groups $\mathbb{Z}^N$, and this indicates that there could be a fully local toy model of infinite-dimensional (separable) quantum theory in which the HSP for $\mathbb{Z}^N$ can be efficiently solved without the requirement of non-locality. However, reasoning about non-locality in the infinite-dimensional setting is likely to be trickier than it might seem at first glance, and further pursuit of this observation is left to future work.

One might think that a physical setup similar to the one used for $G = \mathbb{Z}^N$, but with position and momentum swapped, could be used to tackle the $G = \mathbb{T}^N$ case. However, the annihilators $\mathrm{Ann}[H] \leq \mathbb{Z}^N$ are all infinite sub-lattices of $\mathbb{Z}^N$, and the classical post-processing is left with the daunting task of reconstructing one such lattice in polynomial time from polynomially many random samples. This seems to be sufficiently close to the Shortest Independent Vectors Problem—a known hard lattice problem [BS99], related to other quantum-resistant lattice problems [Reg04b, Reg04a]—to suggest that solving the HSP for compact Lie subgroups of $\mathbb{T}^N$ might be beyond current quantum approaches; however, a thorough investigation of this issue is left to future work.

Generalised Mermin-type non-locality

Using phase groups and strongly complementary observables, we have fully generalised Mermin-type non-locality arguments in Chapter 4, and we have provided the exact group-theoretic conditions required for non-locality to arise. Our results complete the line of enquiry on the connection between phase groups and non-locality started in [CES10, CDKW12]. We have furthermore shown that all our generalised arguments can be realised in quantum mechanics, using GHZ states and appropriate phase gates.

We have then proceeded to investigate the empirical models arising from our generalised arguments, using the sheaf-theoretic framework for non-locality and contextuality. We have shown the models to provide new instances of All-vs-Nothing arguments, and in particular to be strongly contextual. As a consequence, we have shown that the hierarchy of quantum-realisable All-vs-Nothing arguments over finite fields does not collapse.

Finally, our generalisations lead us to an extension of the quantum-classical secret sharing scheme of Hillery, Bužek and Berthiaume, which was originally based on Mermin's non-locality argument for qubit GHZ states. Using our results on strong contextuality, we have been able to provide device-independent security guarantees for our generalised protocol (and for the original HBB scheme as a special case).

A number of questions are left open to future investigation. Firstly, our generalised arguments are formulated for finite abelian groups, encoded by an orthonormal basis of unbiased states: an extension to arbitrary finite groups will be of interest, and more general subsets of the phase group could be considered.

Secondly, we have restricted ourselves to the case in which one structure is commutative and has enough points. Treatment of the more general case, where both structures are allowed to be possibly non-commutative, would extend our result from traditional groups to certain quantum groups.

Thirdly, we have shown that our generalised Mermin-type arguments are All-vs-Nothing, but the converse is not true in general. It would be interesting to investigate which modifications would be necessary to extend our techniques to other families of All-vs-Nothing arguments.

Finally, the model of attack we used to provide device-independent security guarantees is somewhat more restricted than the gold standard employed in device-independent quantum cryptography. A more complete proof of security should be a priority for future developments.

Acknowledgements

The writing of this Thesis was made possible by the loving, unconditional support of my wife Sukrita, my mum and dad, my little brother Niccolò and my best friend Nicolò. The content and presentation have greatly benefited from my many conversation with Bob Coecke, Aleks Kissinger, Dominic Horsman, Fabrizio Romano Genovese, Carlo Maria Scandolo, William Zeng, Ross Duncan, Chris Heunen, Dan Marsden, Amar Hadzihasanovic, David Reutter, Samson Abramsky and Paolo Perinotti. The very possibility of pursuing this line of research was entirely thanks to Bob Coecke—who took me in despite my loud, braggadocious Italian character—and to the generous funding provided by EPSRC and Trinity College's Williams Scholarship.

Bibliography

[Abr87] Samson Abramsky. Domain Theory and the Logic of Observable Properties. PhD thesis, Queen Mary College, University of London 1987.

[Abr13] Samson Abramsky. Relational Hidden Variables and Non-Locality. *Studia Logica*, 101(2):411–452, 2013.

[AB14] Samson Abramsky and Adam Brandenburger. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics*, 13, 2011.

[AB14] Samson Abramsky and Adam Brandenburger. An operational interpretation of negative probabilities and no-signalling models. In *Horizons of the Mind. A Tribute to Prakash Panangaden*, 59–75, 2014.

[ABK$^+$15] Samson Abramsky, Rui Soares Barbosa, Kohei Kishida, Raymond Lal, and Shane Mansfield. Contextuality, Cohomology and Paradox. In *24th EACSL Annual Conference on Computer Science Logic (CSL)*, 211–228, 2015.

[AB04] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*, 415–425, 2004.

[AB05] Samson Abramsky and Bob Coecke. Abstract physical traces. *Theory and Applications of Categories*, 14:111–124, 2005.

[AC09] Samson Abramsky and Bob Coecke. Categorical Quantum Mechanics. *Handbook of Quantum Logic and Quantum Structures*, 261–323, 2009.

[AH12a] Samson Abramsky and Chris Heunen. H*-algebras and nonunital Frobenius algebras: first steps in infinite-dimensional categorical quantum mechanics. *Mathematical Foundations of Information Flow*, 71:1–24, 2012.

[AH12b] Samson Abramsky and Chris Heunen. Operational theories and Categorical quantum mechanics. *Logic and Algebraic Structures in Quantum Computing*, 2012.

[AMB12] Samson Abramsky, Shane Mansfield, and Rui Soares Barbosa. The Cohomology of Non-Locality and Contextuality. *Electronic Proceedings in Theoretical Computer Science*, 95(Qpl 2011):1–14, 2012.

[AV93] Samson Abramsky and Steven Vickers. Quantales, observational logic and process semantics. *Mathematical structures in computer science*, 3:161–227, 1993.

[Amb45] Warren Ambrose. Structure theorems for a special class of Banach algebras. *Transactions of the American Mathematical Society*, 57(3):364–364, 1945.

[Ara80] Huzihiro Araki. On a characterization of the state space of quantum mechanics. *Communications in Mathematical Physics*, 75(1):1–24, 1980.

[Bac14] Miriam Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16(9), 2014.

[BD15] Miriam Backens and Ali Nabi Duman. A Complete Graphical Calculus for Spekkens' Toy Bit Theory. *Foundations of Physics*, 46(1):70–103, 2015.

[Bae12] John C. Baez. Division Algebras and Quantum Theory. *Foundations of Physics*, 42(7):819–855, 2012.

[BD95] John C. Baez and James Dolan. Higher-dimensional Algebra and Topological Quantum Field Theory. *Journal of Mathematical Physics*, 36:6073–6105, 1995.

[BS10] John C. Baez and Mike Stay. *Physics, topology, logic and computation: a Rosetta Stone*. Springer, 2010.

[BV14] Krzysztof Bar and Jamie Vicary. Groupoid Semantics for Thermal Computing. *arXiv preprint*, 2014.

[Bar07] Jonathan Barrett. Information processing in generalized probabilistic theories. *Physical Review A - Atomic, Molecular, and Optical Physics*, 75(3):1–21, 2007.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):1–4, 2005.

[Bec75] William Beckner. Inequalities in Fourier Analysis. *Annals of Mathematics*, 102(2):159–182, 1975.

[BDP13] Alessio Belenchia, Giacomo Mauro D'Ariano, and Paolo Perinotti. Universality of Computation in Real Quantum Theory. *Europhysics Letters*, 104(2):20006, 2013.

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum Complexity Theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[BM75] Iwo Białynicki-Birula and Jerzy Mycielski. Uncertainty relations for information entropy in wave mechanics. *Communications in Mathematical Physics*, 44(2):129–132, 1975.

[BS99] Johannes Blömer and Jean-Pierre Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, 711–720, 1999.

[BH12] Sergio Boixo and Chris Heunen. Entangled and sequential quantum protocols with dephasing. *Physical Review Letters*, 108(12):1–5, 2012.

[Bos38] Raj Chandra Bose. On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Græco-Latin Squares. *Sankhya: The Indian Journal of Statistics (1933-1960)*, 3(4):323–338, 1938.

[But14] Jeremy Butterfield. On time in quantum physics. In Heather Dyke and Adrian Bardon, editors, *A Companion to the Philosophy of Time*. John Wiley & Sons Ltd, 2014.

[CB17] Lorenzo Catani and Dan E. Browne. Spekkens' toy model in all dimensions and its relationship with stabilizer quantum mechanics. *arXiv preprint*, 2017.

[CMP02] Nicolas J. Cerf, Serge Massar, and Stefano Pironio. Greenberger-Horne-Zeilinger Paradoxes for Many Qudits. *Physical Review Letters*, 89:080402, 2002.

[CDP10] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Physical Review A - Atomic, Molecular, and Optical Physics*, 81(6), 2010.

[CDP11] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Informational derivation of quantum theory. *Physical Review A - Atomic, Molecular, and Optical Physics*, 84(1):1–39, 2011.

[CS15] Giulio Chiribella and Carlo Maria Scandolo. Entanglement and thermodynamics in general probabilistic theories. *New Journal of Physics*, 17(10):103027, 2015.

[CY16] Giulio Chiribella and Xiao Yuan. Bridging the gap between general probabilistic theories and the device-independent framework for nonlocality and contextuality. *Information and Computation*, 2016.

[Coe08] Bob Coecke. Axiomatic description of mixed states from Selinger's CPM-construction. *Electronic Notes in Theoretical Computer Science* 210:3–13, 2008.

[Coe12] Bob Coecke. The logic of quantum mechanics - Take II. *Logic and Algebraic Structures in Quantum Computing*, 2012.

[Coe16] Bob Coecke. Terminality Implies No-signalling ... and Much More Than That. *New Generation Computing*, 34:69–85, 2016.

[CD11] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13, 2011.

[CDKW12] Bob Coecke, Ross Duncan, Aleks Kissinger, and Quanlong Wang. Strong complementarity and non-locality in categorical quantum mechanics. *Proceedings of the 2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012*, 245–254, 2012.

[CE12] Bob Coecke and Bill Edwards. Spekkens's toy theory as a category of processes. *Proceedings of Symposia in Applied Mathematics*, 71:28, 2012.

[CES10] Bob Coecke, Bill Edwards, and Robert W. Spekkens. Phase groups and the origin of non-locality for qubits. *Electronic Notes in Theoretical Computer Science*, 270(2):15–36, 2010.

[CH12] Bob Coecke and Chris Heunen. Pictures of complete positivity in arbitrary dimension. *Electronic Proceedings in Theoretical Computer Science*, 95:27–35, 2012.

[CHK14] Bob Coecke, Chris Heunen, and Aleks Kissinger. Categories of quantum and classical channels. *Quantum Information Processing*, 1–31, 2014.

[CK15] Bob Coecke and Aleks Kissinger. Categorical Quantum Mechanics I: Causal Quantum Processes. 2015.

[CK17] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes.* Cambridge University Press, 2017.

[CPP10] Bob Coecke, Eric Oliver Paquette, and Dusko Pavlovic. Classical and quantum structuralism. *Semantic Techniques in Quantum Computation*, 29–69, 2010.

[CP07] Bob Coecke and Dusko Pavlovic. Quantum measurements without sums. *Mathematics of Quantum Computation and Quantum Technology*, 2007.

[CPV13] Bob Coecke, Dusko Pavlovic, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 23(03), 2013.

[CP10] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. *Logical Methods in Computer Science*, 8(4:14):1–24, 2010.

[Cli71] William Clifford. Preliminary Sketch of Biquaternions. *Proceedings of the London Mathematical Society*, s1-4(1):381–395, 1871.

[Con94] Alain Connes. *Noncommutative Geometry.* 1994.

[CH15] Oscar Cunningham and Chris Heunen. Axiomatizing complete positivity. *Electronic Proceedings in Theoretical Computer Science*, (Qpl 2015):148–157, 2015.

[DeB14] Niel de Beaudrap. On computation with 'probabilities' modulo k. *arXiv preprint*, 2014.

[dWZ14] Christian Schröder de Witt and Vladimir Zamdzhiev. The ZX calculus is incomplete for quantum mechanics. *Electronic Proceedings in Theoretical Computer Science*, (Qpl 2014):8, 2014.

[DM16] Leonardo Disilvestro and Damian Markham. Quantum Protocols within Spekkens' Toy Model. *Quantum Physics and Logic*, 2016.

[DI08] Andreas Döring and Chris J. Isham. A topos foundation for theories of physics: I. Formal languages for physics. *Journal of Mathematical Physics*, 49(5), 2008.

[DR89] Sergio Doplicher and John E. Roberts. A new duality theory for compact groups. *Inventiones Mathematicae*, 98(1):157–218, 1989.

[Dri87] Vladimir Gershonovich Drinfel'd. Quantum groups. *Proceedings of the International Congress of Mathematicians*, 1(986):798–820, 1987.

[Dun15] Ross Duncan. A graphical approach to measurement-based quantum computing. In *Quantum Physics and Linguistics*. 2015.

[DD16] Ross Duncan and Kevin Dunne. Interacting Frobenius Algebras are Hopf. *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science - LICS '16*, 2016.

[EJ96] Artur Ekert and Richard Jozsa. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733–753, 1996.

[EDLP09] Julia Evans, Ross Duncan, Alex Lang, and Prakash Panangaden. Classifying all mutually unbiased bases in Rel. *arXiv preprint*, 2009.

[Far75] M. O. Farrukh. Application of nonstandard analysis to quantum mechanics. *Journal of Mathematical Physics*, 16(2):177, 1975.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.

[Fey86] Richard P. Feynman. Quantum Mechanical Computers. *Foundations of physics*, 66(6):507–531, 1986.

[FK97] Bob Flagg and Ralph Kopperman. Continuity spaces: reconciling domains and metric spaces. *Theoretical Computer Science*, 177:111–138, 1997.

[Flo62] Robert W. Floyd. Algorithm 97: shortest path.. *Communications of the ACM*, 5(6):345, 1962.

[Fuc15] László Fuchs. *Abelian groups.* Springer, 2015.

[Gog15a] Stefano Gogioso. Monadic Dynamics. *arXiv preprint*, 2015.

[Gog15b] Stefano Gogioso. Categorical Semantics for Schroödinger's Equation. *arXiv preprint*, 2015.

[Gog15c] Stefano Gogioso. A Bestiary of Sets and Relations. *Electronic Proceedings in Theoretical Computer Science*, (QPL 2015):208–227, 2015.

[Gog15d] Stefano Gogioso. Operational Mermin non-locality and All-vs-Nothing arguments. *arXiv preprint*, 2015.

[Gog17] Stefano Gogioso. Fantastic Quantum Theories and Where to Find Them. *arXiv preprint*, 2017.

[GG16] Stefano Gogioso and Fabrizio Genovese. Infinite-dimensional Categorical Quantum Mechanics. *Electronic Proceedings in Theoretical Computer Science* (QPL 2016), 236:51–69, 2016.

[GG17] Stefano Gogioso and Fabrizio Genovese. Towards Quantum Field Theory in Categorical Quantum Mechanics. *arXiv preprint*, 2017.

[GK17] Stefano Gogioso and Aleks Kissinger. Fully graphical treatment of the quantum algorithm for the Hidden Subgroup Problem. *arXiv preprint*, 2017.

[GS16] Stefano Gogioso and Carlo Maria Scandolo. Categorical Probabilistic Theories. *arXiv preprint*, 2017.

[GZ15a] Stefano Gogioso and William Zeng. Fourier transforms from strongly complementary observables. *arXiv preprint*, 2015.

[GZ15b] Stefano Gogioso and William Zeng. Mermin Non-Locality in Abstract Process Theories. *Electronic Proceedings in Theoretical Computer Science*, (QPL 2015):228–246, 2015.

[GZ17] Stefano Gogioso and William Zeng. Generalised Mermin-type non-locality arguments. *arXiv preprint*, 2017.

[Gol98] Robert Goldblatt. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis. Springer, 1998.

[Had15] Amar Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. *Proceedings - Symposium on Logic in Computer Science*, 2015:573–584, 2015.

[Hal13] Brian C. Hall. *Quantum theory for Mathematicians.* Springer, 2013.

[HRTS00] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. *Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing*, pages 627–635, 2000.

[HRS10] Sean Hallgren, Martin Roetteler, and Pranab Sen. Limitations of Quantum Coset States for Graph Isomorphism. *Journal of the ACM*, 57(6), 2010.

[Har01] Lucien Hardy. Quantum Theory From Five Reasonable Axioms. *arXiv preprint*, 2001.

[HK16] Chris Heunen and Aleks Kissinger. Can quantum theory be characterized in information-theoretic terms? *arXiv preprint*, apr 2016.

[HLS09] Chris Heunen, Nicolaas P. Landsman, and Bas Spitters. A topos for algebraic quantum theory. *Communications in Mathematical Physics*, 291(1):63–110, 2009.

[Hil98] David Hilbert. *The Theory of Algebraic Number Fields.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.

[HBB99] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, 1999.

[Hil05] Jan Hilgevoord. Time in quantum mechanics: a story of confusion. *Studies In History and Philosophy of Science Part B*, 36(1):29–60, 2005.

[Hor11] Clare Horsman. Quantum picturalism for topological cluster-state. *New Journal of Physics*, 133(9), 2011.

[JNW34] Pascual Jordan, John von Neumann, and Eugene Wigner. On an Algebraic Generalization of the Quantum Mechanical Formalism. *The Annals of Mathematics*, 35(1):29, 1934.

[JS91] André Joyal and Ross Street. The Geometry of Tensor Calculus I. *Advances in Mathematics*, 88:55–112, 1991.

[JSV96] André Joyal, Ross Street, and Dominic Verity. Traced Monoidal Categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 119(03):447–468, 1996.

[Joz97] Richard Jozsa. Quantum Algorithms and the Fourier Transform. *Proceedings of the Royal Sociey A*, 454(1969), 1998.

[Joz01] Richard Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science & Engineering*, 3(2):1–15, 2001.

[Kas95] Christian Kassel. *Quantum Groups.* Springer-Verlag, 1995.

[KZ02] Dagomir Kaszlikowski and Marek Zukowski. Greenberger-Horne-Zeilinger paradoxes for N N-dimensional systems. *Physical Review A*, 66:042107, 2002.

[KL80] Gregory Maxwell Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[Khr91] Andrei Khrennikov. padic quantum mechanics with p-adic valued functions. *Journal of Mathematical Physics*, 32(4):932–937, 1991.

[Khr93] Andrei Khrennikov. p-Adic probability theory and its applications. The principle of statistical stabilization of frequencies. *Theoretical and Mathematical Physics*, 97(3):1340–1348, 1993.

[Khr03] Andrei Khrennikov. Hyperbolic quantum mechanics. *Advances in Applied Clifford Algebras*, 13(1):1–9, 2003.

[Khr10] Andrei Khrennikov. Representation of Probabilistic Data by Quantum-Like Hyperbolic Amplitudes. *Advances in Applied Clifford Algebras*, 20(1):43–56, 2010.

[Kis12] Aleks Kissinger. *Pictures of Processes: Automated Graph Rewriting for Monoidal Categories and Applications to Quantum Computing.* PhD thesis, University of Oxford, 2012.

[KZ15] Aleks Kissinger and Vladimir Zamdzhiev. Quantomatic: A Proof Assistant for Diagrammatic Reasoning. *Automated Deduction - Cade-25*, 9195:326–336, 2015.

[Koc72] Anders Kock. Strong functors and monoidal monads. *Archiv der Mathematik*, 23(1):113–120, 1972.

[Kop88] Ralph Kopperman. All topologies come from generalised metrics. *The american mathematical monthly*, 95(2):89–97, 1988.

[LLK06] Jinhyoung Lee, Seung-Woo Lee, and Myungshik S. Kim. Greenberger-Horne-Zeilinger nonlocality in arbitrary even dimensions. *Physical Review A*, 73:032316, 2006.

[Maj00] Shahn Majid. *Foundations of quantum group theory.* Cambridge University Press, 2000.

[Mar] Daniel Marsden. A Graph Theoretic Perspective on CPM(Rel). *Electronic Proceedings in Theoretical Computer Science*, (QPL 2015), 2015.

[Mas87] Victor P. Maslov. On a new principle of superposition for optimization problems. *Russian Mathematical Surveys*, 42(3):43–54, 1987.

[MPAG13] Jarrod R. McClean, John A. Parkhill, and Alán Aspuru-Guzik. Feynman's clock, a new variational principle, and parallel-in-time quantum dynamics. *Proceedings of the National Academy of Sciences of the United States of America*, 110(41):E3901–9, 2013.

[Mer90] David Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58(8):731–734, 1990.

[Mik04] Grigory Mikhalkin. Amoebas of algebraic varieties and tropical geometry. In *Different faces of geometry*, 257–300, 2004.

[Mog91] Eugenio Moggi. Notions of computation and monads. *Information and Computation*, 93(1):55–92, 1991.

[MRS08] Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The Symmetric Group Defies Strong Fourier Sampling: Part I. *SIAM Journal on Computing*, 37(6):1842–1864, 2008.

[MV15] Benjamin Musto and Jamie Vicary. Quantum Latin squares and unitary error bases. *arXiv preprint*, 2015.

[Nym11] Peter Nyman. On the Consistency of the Quantum-Like Representation Algorithm for Hyperbolic Interference. *Advances in Applied Clifford Algebras*, 21(4):799–811, 2011.

[OO93] Izumi Ojima and Masanao Ozawa. Unitary representations of the hyperfinite Heisenberg group and the logical extension methods in physics. *Open Systems & Information Dynamics*, 2(1):107–128, apr 1993.

[Pal16a] Tim Palmer. Invariant Set Theory. *arXiv preprint*, 2016.

[Pal16b] Tim Palmer. p-adic Distance, Finite Precision and Emergent Superdeterminism: A Number-Theoretic Consistent-Histories Approach to Local Quantum Realism. *arXiv preprint*, 2016.

[Pas15] Tom Pashby. Time and quantum theory: A history and a prospectus. *Studies in History and Philosophy of Science Part B*, 52:24–38, 2015.

[Pav09] Dusko Pavlovic. Quantum and classical structures in nondeterminstic computation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5494:143–157, 2009.

[Pin98] Jean-Eric Pin. Tropical semirings. *Idempotency (Bristol 1994)*, Publ. Newton Inst, 11:50–69, 1998.

[RTHH16] Ravishankar Ramanathan, Jan Tuziemski, Michał Horodecki, and Paweł Horodecki. No Quantum Realization of Extremal No-Signaling Boxes. *Physical Review Letters*, 117(5):050401, 2016.

[Reg04a] Oded Regev. New lattice based cryptographic constructions. *Journal of the ACM*, 51(6):899–942, 2004.

[Reg04b] Oded Regev. Quantum Computation and Lattice Problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.

[Rob12] Bryan W. Roberts. *Time, symmetry and structure: a study in the foundations of quantum theory.* PhD thesis, 2012.

[Rob74] Abraham Robinson. *Non-standard analysis.* Princeton University Press, 1974.

[RTVW89] Ph. Ruelle, E. Thiran, D. Verstegen, and J. Weyers. Quantum mechanics on padic fields. *Journal of Mathematical Physics*, 30(12):2854–2874, 1989.

[RLZL13] Junghee Ryu, Changhyoup Lee, Marek Zukowski, and Jinhyoung Lee. Greenberger-Horne-Zeilinger theorem for N qudits. *Physical Review A*, 88:042101, 2013.

[SC16] John H. Selby and Bob Coecke. Process theoretic derivation of the Hermitian adjoint for quantum theory. *arXiv preprint*, 2016.

[Sel07] Peter Selinger. Dagger Compact Closed Categories and Completely Positive Maps. *Electronic Notes in Theoretical Computer Science*, 170:139–163, 2007.

[Sel09] Peter Selinger. A survey of graphical languages for monoidal categories. *Lecture Notes in Physics*, 813:289–355, 2009.

[Sel10] Peter Selinger. Autonomous categories in which A= A*. *7th workshop on Quantum Physics and Logic (QPL)*, 2010.

[Sho95] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. 1995.

[Shu12] Benjamin Schumacher and Michael D. Westmoreland. Modal quantum theory. *Foundations of Physics* 42(7):918–925, 2012.

[Shu16] Benjamin Schumacher and Michael D. Westmoreland. Almost quantum theory. In *Quantum Theory: Informational Foundations and Foils* 45–81, 2016.

[Sim97] Daniel R. Simon. On the Power of Quantum Computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[Sim88] Imre Simon. Recognizable sets with multiplicities in the tropical semiring. *Mathematical Foundations of Computer Science*, 107–120, 1988.

[Sim94] Imre Simon. On semigroups of matrices over the tropical semiring. *RAIRO - Theoretical Informatics and Applications*, 28(3-4):277–294, 1994.

[Spe07] Robert W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A*, 75(3):032110, 2007.

[SS07] David Speyer and Bernd Sturmfels. Tropical mathematics. *Mathematics Magazine*, 82(3):163–173, 2009.

[Sto30] Marshall H. Stone. Linear Transformations in Hilbert Space: III. Operational Methods and Group Theory. *Proceedings of the National Academy of Sciences*, 16(2):172–175, 1930.

[Sto32] Marshall H. Stone. On One-Parameter Unitary Groups in Hilbert Space. *Annals of Mathematics*, 33(3):643–648, 1932.

[Str07] Ross Street. *Quantum groups. A path to current algebra.* Cambridge University Press, 2007.

[Tul16] Sean Tull. Operational Theories of Physics as Categories. *arXiv preprint*, 2016.

[VV14] Umesh Vazirani and Thomas Vidick. Fully Device-Independent Quantum Key Distribution. *Physical Review Letters*, 113(14):140501, 2014.

[VV16] Dominic Verdon and Jamie Vicary. Tight reference frame-independent quantum teleportation. *arXiv preprint*, 2016.

[Vic11] Jamie Vicary. Categorical Formulation of Finite-Dimensional Quantum Algebras. *Communications in Mathematical Physics*, 304(3):765–796, 2011.

[Vic12a] Jamie Vicary. Higher Semantics for Quantum Protocols. In *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 606615, 2012.

[Vic12b] Jamie Vicary. Topological structure of quantum algorithms. In *Proceedings of the 2013 28th Annual ACM/IEEE Symposium on Logic in Computer Science*, 2012.

[Vit62] Andrew Viterbi. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *IEEE transactions on Information Theory*, 13(2):260–269, 1967.

[VV89] Vasilii S. Vladimirov and Igor V. Volovich. p-adic quantum mechanics. *Communications in Mathematical Physics*, 123(4):659–676, 1989.

[vN31] John von Neumann. Die Eindeutigkeit der Schrödingerschen Operatoren. *Mathematische Annalen*, 104(1):570–578, 1931.

[vN32a] John von Neumann. Uber Einen Satz Von Herrn M. H. Stone. *The Annals of Mathematics*, 33(3):567, 1932.

[vN32b] John von Neumann. Proof of the quasi-ergodic hypothesis. *Proceedings of the National Academy of Sciences*, 18(1):70–82, 1932.

[Wil16] Alexander Wilce. A Royal Road to Quantum Theory (or Thereabouts). *arXiv preprint*, 2016.

[Wor87] Stanislaw L. Woronowicz. Compact matrix pseudogroups. *Communications in Mathematical Physics*, 111(4):613–665, 1987.

[Wor98] Stanislaw L. Woronowicz. Compact quantum groups. *Symétries quantiques*, 845:884, 1998.

[Wot90] William K Wootters. Local accessibility of quantum states. *Complexity, entropy and the physics of information*, 8:39–46, 1990.

[Yet90] David N. Yetter. Quantales and (Noncommutative) Linear Logic. *The Journal of Symbolic Logic*, 55(1):41–64, 1990.

[Zam12] Vladimir Nikolaev Zamdzhiev. An Abstract Approach towards Quantum Secret Sharing. Technical report, 2012.

[Zen15] William Zeng. Models of Quantum Algorithms in Sets and Relations. *arXiv preprint*, 2015.

[ZV14] William Zeng and Jamie Vicary. Abstract structure of unitary oracles for quantum algorithms. *Electronic Proceedings in Theoretical Computer Science*, (Qpl 2014):13, 2014.

[ZK99] Marek Zukowski and Dagomir Kaszlikowski. Greenberger-Horne-Zeilinger paradoxes with symmetric multiport beam splitters. *Physical Review A*, 59:3200, 1999.