A Diagrammatic Approach to Networks of Spans and Relations

Cole Comfort

New College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy in Computer Science

Michaelmas 2023

Acknowledgements

I would have not been able to write this thesis without the help and support of many people, both academics and nonacademics; especially due to the circumstances in the University of Oxford Department of Computer Science following the pandemic.

First, I thank my fellow students and postdocs in the quantum group at Oxford for their good company and research discussions: especially Alex, Amin, Antonin, James, John, Lia, Lukas, Matt, all three Nicks, Nihil, Sivert, Razin, Tein and Will. Also I can't forget Sander, who was a postdoc the year before when I visited during my masters degree. I am also thankful to Aleks for his advice and help in writing our paper as well as Bob for getting me funding and all the food and drink. I also am thankful to Paweł and the TallCat group in Estonia for welcoming me as a guest when I was at that time unwelcome in my own department. I also would like to thank the Programming Principles, Logic and Verification Group at UCL for allowing me to visit; especially Leo and Robin for fruitful discussions and Wojtek for his very welcoming company, and Martti for letting me sleep on his couch. I would also like to thank the group at Pisa for letting me visit; especially Alessandro and Filippo for discussions about research and Fabio for the good food and wine, and a second thanks to Alessandro for letting me sleep on his couch. I would also like to thank everyone at the Mathematically Structured Programming group in Glasgow. Also I am grateful to both Roberts in Edinburgh, especially to Robert Booth for letting me sleep on his floor for a week. Also thanks for the pints, Ross. I am also grateful to the Canadian category theory community, especially Amolak, Ben, Jon, Jeff and Robin. I am especially grateful to JS for his sage advice, encouragement and kindness; without which, I probably would have never done a Ph.D. Also thanks to all of my friends who regularly attend ACT and QPL, and the other category theorists who I bump into ever so often. I am also thankful for the helpful feedback on this thesis given to me by my assessors.

Finally, I am also grateful to my family and all my friends in Canada, Tallinn and Oxford who have not influenced my research but have made doing a Ph.D. more tolerable.

Statement of Originality

Chapters 2 and 3 are literature reviews. Chapter 4 contains work written solely by the author of this thesis with Sections 4.1-4.2 of Chapter 4 being adapted from conference proceedings [Com21]. Chapter 5 contains work adapted from a paper coauthored with my supervisor Aleks Kissinger (of which I was the primary contributor), published in conference proceedings [CK22]. The final part of Chapter 5 after and including Section 5.4 contains work solely by the author of this thesis.

Abstract

In this thesis we exhibit nondeterministic semantics for various classes of circuits. Motivated initially by quantum circuits, we also give nondeterministic semantics for circuits for classical mechanical systems and Boolean algebra. More formally, we interpret these classes of circuits in terms of categories of spans or relations: in less categorical terms these are equivalent to matrices over the natural numbers or the Boolean semiring. In the relational picture, we characterize circuits in terms of which inputs and outputs are jointly possible; and in the spans picture, how often inputs and outputs are jointly possible. Specifically, we first show that the class of circuits generated by the Toffoli gate as well the states $|0\rangle$, $|1\rangle$, $\sqrt{2}|+\rangle$ and their adjoints is characterized in terms of spans of finite sets. We also give a complete axiomatization for these circuits. With this semantics in mind, we discuss the connection to partial and reversible computation. Shifting to the phase-space picture we also characterize circuits in terms of how they relate abstract positions and momenta. We show how this gives a unifying relational semantics for certain classes circuits for classical mechanical systems, as well as for stabilizer quantum circuits.

Contents

Chapter 1

Introduction

The traditional paradigm for quantum computing decomposes a quantum computation into distinct stages. First, a quantum state is prepared in the lab; then, the quantum state is evolved by applying unitary operations; next, the quantum state is measured according to the Born rule. There are variations to this paradigm, for example, in measurement-based quantum computing one first prepares a quantum state, then evolves the state only by performing a series of conditioned partial measurements. However, these traditional approaches are quite rigid: the different stages of the process are modeled by different kinds of mathematical objects. Each of these stages interact with each other according to various rules: which are stitched together in order to interpret the full computation. As a consequence, the fundamental connections between these different paradigms are hard to see because their low-level descriptions introduce arbitrary book-keeping that must be painstakingly translated back and forth.

In this thesis, using categorical methods we reject these artificial distinctions and take a fundamentally different approach. The use of category theory in quantum mechanics is quite varied, and has been developed by many different people; however, we will largely follow the particular vein put forward by Abramsky and Coecke [AC04]. In this setting, quantum circuits are regarded as string diagrams for the †-compact closed category of finite dimensional Hilbert spaces and linear maps. One advantage of using this categorical structure to model circuits is that many of the ambient topological features of quantum circuits can be abstracted away into the †-compact closed structure: which is accompanied by an equally natural graphical calculus. This level of generality helps one abstract away from many of the irrelevant details. This can reveal the essential qualities of the problem at hand, freeing one from arbitrary conventions and notations.

For example, Abramsky and Coecke suggested studying the †-compact closed category of sets and relations as a toy model of quantum mechanics, as opposed to finite dimensional Hilbert spaces. Relations are subsets and are composed uniformly by tracing out the common elements in their intersection, rather than by function composition. In this thesis, we show that fragments of quantum mechanics can actually be *faithfully* reflected by sets and relations equipped with extra structure (and also by their close relatives sets and spans). Without starting from such an abstract perspective, these connections would be almost impossible to see. This relational approach yields a *nondeterministic semantics* for quantum circuits: which is much more flexible and symmetric than physicists' usual approach. The circuit is defined by the ensemble of all possible inputs that can be related to all possible outputs. To drive the point home, quantum processes are defined in terms of how they are related to other quantum processes: not just by how they act on inputs.

As we just mentioned, in this thesis we consider categories of relations and spans for our semantics: categories of spans keep track of the number of times that things are related, whereas categories of relations only keep track of the existence of a relation. The first class of subspaces which we consider is given by spans of finite sets. These are are regarded as configurations in the state space of certain classes of quantum systems. We show how that these form the classical fragment of quantum circuits. In this setting, one can regard maps between systems as solutions to sets of Boolean equations: where composition is given by unification.

The second class of circuits is given by affine coisotropic subspaces of symplectic vector spaces. Here, the systems correspond to the possible configurations of abstract positions and momenta. The subspaces between systems are the possible ways in which "particles" can flow between both systems. The relational composition of two of these subspaces corresponds to glueing together all of the possible flows. By changing the field with which we are forming our vector spaces, we get different interpretations of these systems. Over finite fields of odd prime-characteristic, we recapture odd-prime dimensional "quopit stabilizer circuits" and their tableaux; the novelty being that the relational composition of tableaux corresponds to the composition of the corresponding circuits. However, by shifting to fields of characteristic 0, we recapture classical mechanical systems. This level of generality allows us to make precise observations about the similarities between quantum and classical mechanics, and suggests new ways to model different kinds of of quantum systems.

Various themes reoccur throughout this thesis. First, because copying is not allowed in quantum mechanics, we use a more relaxed, relational notion of copying. This is formalized in terms of the "Cartesian bicategories of relations" of Carboni and Walters [CW87]. One very important example of which is that of "linear relations," ie. relations which have the structure of linear subspaces. This is studied in great detail, and given a complete axiomatization by Bonchi, Sobociński and Zanasi [BSZ17]. We will make heavy use of this, and take great inspiration from this work, as well as Zanasi's thesis on the same subject [Zan18]. We reveal that the mathematical objects studied in the work of Bonchi et al. have a deep structural connection with the quantum "ZX-calculus" introduced by Coecke and Duncan [CD11].

Another theme which comes up multiple times throughout this thesis is Selinger's CPM construction [Sel07]. Initially proposed as a categorical construction to add an abstract notion of quantum discarding to †-compact categories, we argue that it is much more fundamental and varied. For example, we show that in some cases, the symmetry between position and momentum can be encapsulated by inverting this construction.

1.1 Overview of structure of thesis

In Chapter 2 we review relevant notions in category theory. Not all subsections are needed to understand the whole thesis, some are only needed for specific parts. In Section 2.1 we review the theory of monoidal categories and string diagrams which allows us to regard circuits as abstract mathematical objects. In Subsection 2.1.1 we review †-categories, which give a categorical semantics for reversibility. In Subsection 2.1.2 we review how monoidal categories can be presented in terms of generators and relations and give examples. Reading all three of these sections is essential to understand this thesis. In Section 2.2 we review categories of spans and relations, which are the mathematical semantics for nondeterminism. This is somewhat more technical than the preceeding sections, but is not as essential to understand the thesis. The less interested readers can read the examples in this section, but skip the technical details. In section 2.3 we review internal category theory which is the mathematics needed to give more fine grained decompositional semantics of circuits. This section is only needed to understand Section 4.3.

In Chapter 3 we review categorical quantum mechanics which relates monoidal categories and †-categories to quantum computing. Importantly in Definition 3.2, we review the CPM construction, which is a categorical tool which gives a formal notion of doubling: this comes up multiple times throughout this thesis, as we study highly symmetrical mathematical objects. We also give overview of the families of languages for quantum circuits known as the ZX and ZH-calculi; as well as reviewing the mathematical machinery needed to model mixed states and measurement within this framework. We also review the stabilizer formalism.

In Chapter 4 we analyze the class of quantum circuits generated by the Toffoli gate as well the states $|0\rangle$, $|1\rangle$, $\sqrt{2}|+\rangle$ and their adjoints. In Proposition 4.13 we give a complete presentation for this category and interpret it in terms of spans of finite sets. In other words, this class of circuits is very close to a nondeterministic semantics, except where outcomes can happen multiple times. In Theorem 4.28, we show how this has a more elegant description in terms of interacting monoids which we call $\mathsf{ZX}\&$. The generators and relations of $\mathsf{ZX}\&$ are given in Definition 4.14. In Remark 4.29 we note $\mathsf{ZX}\&$ is the natural number labeled fragment of the qubit ZH-calculus. Consequently, in Corollary 4.30 we show how imposing an additional equation on $\mathsf{ZX}\&$, we depart from the interpretation into Hilbert spaces, and obtain a proper nondeterministic semantics in terms of relations between finite sets. We show in Corollary 4.31, that by adding two generators and equations to $\mathsf{ZX}\&$, we obtain the phase-free qubit ZH-calculus. We also decompose $\mathsf{ZX}\&$ into small fragments; recomposing these small building blocks incrementally via distributive law and pushout. We exhibit substructural features of these various decompositions and discuss how, by allowing only some of the generators, we obtain semantics which are partial, partially invertible and so on.

In Chapter 5 we analyze the structure of odd-prime dimensional/quopit stabilizer circuits. We expose the relational interpretation of these circuits, by adding generators at each point, obtaining different semantics for each classes of generators. We first recall that the phase-free fragment of the qupit ZX-calculus modulo scalars, for prime qudit dimension p, is isomorphic to the prop of linear relations over $\mathbb{F}_p$: i.e. where the maps are linear subspaces over $\mathbb{F}_p$. In Theorem 5.9 we give generators for the prop of Lagrangian relations over a field. In Corollary 5.12 show that doubling linear relations over $\mathbb{F}_p$ using the CPM construction, we obtain the prop of Lagrangian relations. In Corollary 5.24 we show that the prop of Lagrangian relations over odd prime fields is equivalent to quopit Weyl-free stabilizer circuits modulo scalars. The Weyl operators are introduced to this picture in Theorem 5.23 by adding affine shifts to obtain the prop of affine Lagrangian relations. To add quantum discarding, in Corollary 5.35 we show that one doesn't need to take the CPM construction again, but it suffices to add the discard *relation*: obtaining the prop of affine coisotropic relations. By splitting idempotents, in Theorem 5.39 we recover measurement; which has a succinct relational interpretation. Using this relational interpretation of mixed stabilizer circuits, in Section 5.5 we show how stabilizer error correction protocols can be implemented. Throughout this chapter, we compare the quantum semantics to the electrical circuits; highlighting the similarities and differences between both cases.

In Chapter 6 we discuss future work and the limitations of this thesis.

Chapter 2

Category theory

Although we formally state the various categorical constructions which are used throughout this thesis, in almost all cases the accompanying string diagrams also help give intuition to the reader. The exception to this rule is the somewhat more technical material on internal category theory and distributive laws of monoidal theories reviewed in Subsection 2.3 and used in Section 4.3. For this, we assume some basic understanding of bicategories.

As a matter of convention, call pairs of maps $f : X \to Y$ and $g : X \to Y$ with the same domain and codomain **parallel**. Similarly, call a pair of maps $f : X \to Y$ and $g : Y \to Z$ where the codomain of the first map is the domain of the second map **composable**. Given two composable maps $f : X \to Y$ and $g : Y \to Z$, we will denote their **diagrammatic composition** using a semicolon as follows $f; g : X \to Z$. This notation for composition will be preferred throughout this thesis; except when talking about quantum circuits. In this setting, to agree with the conventional notation we will denote their **contravariant composition** by concatenation as follows $gf : X \to Z$.

2.1 Monoidal categories and string diagrams

In this section we review the theory of monoidal categories as well as their string diagrams. The material for which a reference is not provided can be found in an introductory reference to category theory (eg [Lan78]). The reader uninterested in technical details is invited to skip the commutative diagrams and go straight to the pictures.

Definition 2.1. A **monoidal category** is a category $\mathbb{X}$ equipped with a functor $\mathbb{X} \times \mathbb{X} \to \mathbb{X}$ called the **tensor product**, equipped with a distinguished object I of $\mathbb{X}$ called the **tensor unit**; along with the following natural isomorphisms (given by components):

Left unitor: $u^L_X : I \otimes X \to X$

Right unitor: $$u_X^R : X \otimes I \to X$$

Associator: $$\alpha_{X,Y,Z} : (X \otimes Y) \otimes Z \to X \otimes (Y \otimes Z)$$

Satisfying the following coherence equations:

Mac Lane pentagon:

$$\begin{tikzcd}
((W \otimes X) \otimes Y) \otimes Z \arrow[rr, "\alpha_{W\otimes X,Y,Z}"] \arrow[d, "\alpha_{W,X,Y}\otimes 1_Z"'] & & (W \otimes X) \otimes (Y \otimes Z) \arrow[d, "\alpha_{W,X,Y\otimes Z}"] \\
(W \otimes (X \otimes Y)) \otimes Z \arrow[dr, "\alpha_{W,X\otimes Y,Z}"'] & & W \otimes (X \otimes (Y \otimes Z)) \\
& W \otimes ((X \otimes Y) \otimes Z) \arrow[ur, "1_W\otimes\alpha_{X,Y,Z}"'] &
\end{tikzcd}$$

Unit triangle:

$$\begin{tikzcd}
(X \otimes I) \otimes Y \arrow[rr, "\alpha_{X,I,Y}"] \arrow[dr, "u_X^R\otimes 1_Y"'] & & X \otimes (I \otimes Y) \arrow[dl, "1_X\otimes u_Y^L"] \\
& X \otimes Y &
\end{tikzcd}$$

We will call a map out of the tensor unit a **state**, a map into the tensor unit an **effect**, and an endomorphism on the tensor unit a **scalar**.

Example 2.2. Both the category FSet of finite sets and functions and the category Set of sets and functions are monoidal categories: both under the product (also called the Cartesian product) and coproduct (also called the disjoint union).

Given a field k, the category Vect_k of vector spaces over k and the category FVect_k of finite-dimensional vector spaces over k are monoidal categories: both under the bilinear tensor product and the direct sum.

The category Hilb of Hilbert spaces and the category FHilb of finite dimensional Hilbert spaces are both monoidal categories with respect to the bilinear tensor product and direct sum.

Definition 2.3. Given two monoidal categories $\mathbb{X}$ and $\mathbb{Y}$ a (strong) **monoidal functor** from $\mathbb{X}$ to $\mathbb{Y}$ is a functor $F : \mathbb{X} \to \mathbb{Y}$ together with an isomorphism $\varepsilon : I^{\mathbb{X}} \to F(I^{\mathbb{X}})$ and natural isomorphism with components $\mu_{X,Y} : F(X) \otimes^{\mathbb{Y}} F(Y) \to F(X \otimes^{\mathbb{X}} Y)$ such that the following coherence equations hold:

Interaction with associator:

$$\begin{tikzcd}
(F(X) \otimes^{\mathbb{Y}} F(Y)) \otimes^{\mathbb{Y}} F(Z) \arrow[r, "\alpha^{\mathbb{Y}}_{F(X),F(Y),F(Z)}"] \arrow[d, "\mu_{X,Y}\otimes^{\mathbb{Y}} F(Z)"'] & F(X) \otimes^{\mathbb{Y}} (F(Y) \otimes^{\mathbb{Y}} F(Z)) \arrow[d, "F(X)\otimes^{\mathbb{Y}}\mu_{Y,Z}"] \\
F(X \otimes^{\mathbb{X}} Y) \otimes^{\mathbb{Y}} F(Z) \arrow[d, "\mu_{X\otimes^{\mathbb{X}} Y,Z}"'] & F(X) \otimes^{\mathbb{Y}} F(Y \otimes^{\mathbb{X}} Z) \arrow[d, "\mu_{X,Y\otimes^{\mathbb{Y}} Z}"] \\
F((X \otimes^{\mathbb{X}} Y) \otimes^{\mathbb{X}} Z) \arrow[r, "F(\alpha^{\mathbb{Y}}_{X,Y,Z})"'] & F(X \otimes^{\mathbb{X}} (Y \otimes^{\mathbb{X}} Z))
\end{tikzcd}$$

Interaction with unitors:

$$\begin{tikzcd}
I^{\mathbb{Y}} \otimes^{\mathbb{Y}} F(X) \arrow[r, "\varepsilon \otimes^{\mathbb{Y}} F(X)"] \arrow[d, "(u^L)^{\mathbb{Y}}_{F(X)}"'] & F(I^{\mathbb{X}}) \otimes^{\mathbb{Y}} F(X) \arrow[d, "\mu_{1^{\mathbb{X}},X}"] \\
F(X) & F(I^{\mathbb{X}} \otimes^{\mathbb{X}} X) \arrow[l, "F((u^L)^{\mathbb{X}}_X)"]
\end{tikzcd}
\qquad
\begin{tikzcd}
F(X) \otimes^{\mathbb{Y}} I^{\mathbb{Y}} \arrow[r, "F(X) \otimes^{\mathbb{Y}} \varepsilon"] \arrow[d, "(u^R)^{\mathbb{Y}}_{F(X)}"'] & F(X) \otimes^{\mathbb{Y}} F(I^{\mathbb{X}}) \arrow[d, "\mu_{X,1^{\mathbb{X}}}"] \\
F(X) & F(X \otimes^{\mathbb{X}} I^{\mathbb{X}}) \arrow[l, "F((u^R)^{\mathbb{X}}_X)"]
\end{tikzcd}$$

A **monoidal natural transformation** between parallel monoidal functors $F, G : \mathbb{X} \to \mathbb{Y}$ is a natural transformation $\varphi : F \to G$ such that the following coherence equations hold:

$$\begin{tikzcd}
F(X) \otimes^{\mathbb{Y}} F(Y) \arrow[r, "\varphi_X \otimes^{\mathbb{Y}} \varphi_Y"] \arrow[d, "\mu^F_{X,Y}"'] & G(X) \otimes^{\mathbb{Y}} G(Y) \arrow[d, "\mu^G_{X,Y}"] \\
F(X \otimes^{\mathbb{X}} Y) \arrow[r, "\varphi_{X \otimes^{\mathbb{X}} Y}"'] & G(X \otimes^{\mathbb{X}} Y)
\end{tikzcd}
\qquad
\begin{tikzcd}
I^{\mathbb{Y}} \arrow[d, "\eta^F"'] \arrow[dr, "\eta^G"] & \\
F(I^{\mathbb{X}}) \arrow[r, "\varphi_{I^{\mathbb{X}}}"'] & G(I^{\mathbb{X}})
\end{tikzcd}$$

Monoidal categories, monoidal functors and monoidal natural transformations arrange themselves into the strict 2-category of monoidal categories.

If all of the components of the natural transformations are equalities, then the monoidal category is **strict**. Therefore, we can forget the bracketing when we tensor things, and regard the tensor product of multiple objects as a list. A **strict monoidal functor** is a monoidal functor where isomorphisms ε and μ are the identity. Likewise, strict monoidal categories, strict monoidal functors and monoidal natural transformations arrange themselves into the strict 2-category of strict monoidal categories.

Example 2.4. The category FinOrd of finite ordinals and functions is the category where:

Objects: The objects are the natural numbers.

Maps: For each natural number n, the finite ordinal $[n]$ is a distinguished n-element set with a chosen total order.

A map from $n \to m$ is a (not necessarily monotonic) function from $[n] \to [m]$.

The composition and identity is given by the composition and identity of sets and functions.

This is a strict monoidal category with respect to the disjoint union:

Tensor unit: The tensor unit is the natural number 0.

Monoidal product: On objects this acts as addition. On maps, $f : n \to m$ and $g : k \to \ell$, the map $f + g$ corresponds to the chosen disjoint union $f \sqcup g$ $[n + k] \to [m + \ell]$ respecting the chosen order.

Restricting FinOrd to functions which preserve the chosen order of the ordinals yields the strict monoidal category FinOrdMonot of finite ordinals and monotone functions.

The following example comes up quite a lot, so we spell it out it detail:

Example 2.5. Given a commutative semiring S, the category Mat_S, of matrices over S has:

Objects: Natural numbers.

Maps: A map from $n \to m$ is an $m \times n$ matrix. In other words, a matrix is an element $A = (a_{i,j})_{0 \leq i < m, 0 \leq j \leq n} \in S^{m \times n}$. Matrices are denoted as follows:

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{bmatrix}$$

Identity: Given by the dirac delta $I_n = (\delta_{i,j})_{0 \leq i,j < n}$

Composition: Given two matrices $n \xrightarrow{A} m \xrightarrow{B} \ell$ their composite BA has elements given my matrix multiplication:

$$(AB)_{i,j} = \sum_{k=0}^{m-1} a_{i,k} b_{k,j}$$

Mat_S is strict monoidal with respect to two monoidal structures. The first one is given by:

Monoidal product: Given by the direct sum, so that given any two matrices A, B:

$$A \oplus B := \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

Tensor unit: 0.

The second one is given by:

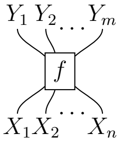
Monoidal product: Given by the Kronecker product so that given any two matrices A, B:

$$A \otimes B := \begin{bmatrix} a_{0,0}B & a_{0,1}B & \cdots & a_{0,n-1}B \\ a_{1,0}B & a_{1,1}B & \cdots & a_{1,n-1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0}B & a_{m-1,1}B & \cdots & a_{m-1,n-1}B \end{bmatrix}$$

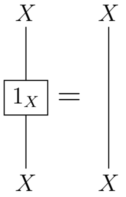
Where the notation $a_{i,j}B$ is the pointwise multiplication of B by $a_{i,j}$.

Tensor unit: 1.

Strict monoidal categories are very nice to work with because they have a particularly concise graphical calculus, called **string diagrams**. A map $f : X_1 \otimes \cdots \otimes X_n \to Y_1 \otimes \cdots \otimes Y_m$ is drawn as a box with n wires coming out of the bottom and m wires coming out of the top, all being labeled by their respective objects, as follows:



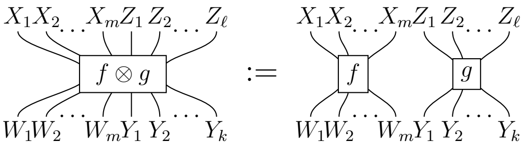
The identity on an object X is drawn as a line:



We often omit the object labels when it is clear from context. The tensor product of two maps

$$\frac{f : W_1 \otimes \cdots \otimes W_n \to X_1 \otimes \cdots \otimes X_m, \quad g : Y_1 \otimes \cdots \otimes Y_k \to Z_1 \otimes \cdots \otimes Z_\ell}{f \otimes g : W_1 \otimes \cdots \otimes W_n \otimes Y_1 \otimes \cdots \otimes Y_k \to X_1 \otimes \cdots \otimes X_m \otimes Z_1 \otimes \cdots \otimes Z_\ell}$$

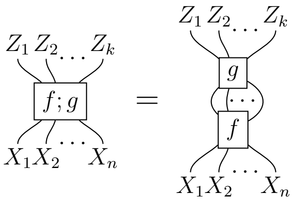
is drawn by pasting them side-by-side:



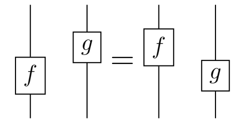
And the composite of two composable maps

$$\frac{f : X_1 \otimes \cdots \otimes X_n \to Y_1 \otimes \cdots \otimes Y_m, \quad g : Y_1 \otimes \cdots \otimes Y_m \to Z_1 \otimes \cdots \otimes Z_k}{f ; g : X_1 \otimes \cdots \otimes X_n \to Z_1 \otimes \cdots \otimes Z_k}$$

is drawn by connecting each of the Y_i wires together:



The axioms of a strict monoidal category are equivalent to planar isotopy of their string diagrams. In other words, the string diagrams can be continuously deformed as long as they don't cross over each other. For example, the functoriality of the tensor product allows one to exchange two disconnected maps:



We can always chose to work with strict monoidal categories if we want to:

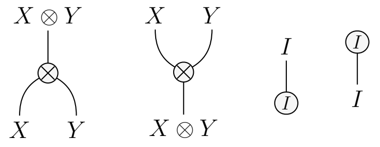
Theorem 2.6. *Every monoidal category is monoidally equivalent to a strict monoidal category.*

The strictification of a monoidal category has a particularly succinct presentation due to Wilson et al. [WGZ22], so that we can use string diagrams for strict monoidal categories to reason about nonstrict monoidal categories:

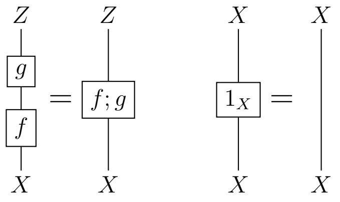
Definition 2.7. Given a monoidal category $(\mathbb{X}, \otimes, I, \alpha, u^L, u^R)$, there is a monoidally equivalent strict monoidal category $\overline{\mathbb{X}}$ with:

Objects: Finite lists of objects in $\mathbb{X}$, $\mathsf{List}(\mathsf{Ob}_{\mathbb{X}})$.

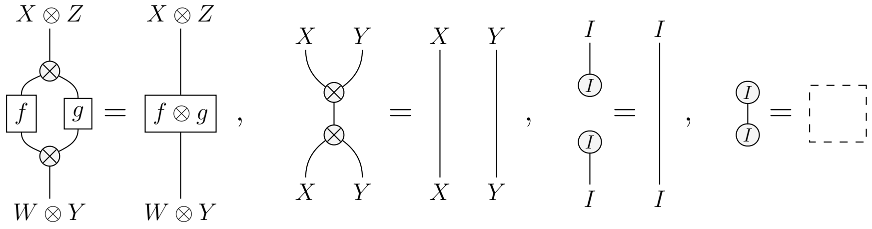
Maps: The maps are generated by a map $f : [X] \to [Y]$ for every map $f : X \to Y$ in $\mathbb{X}$ and the four following generators (referred to as tensor, cotensor, unit introduction and unit removal):

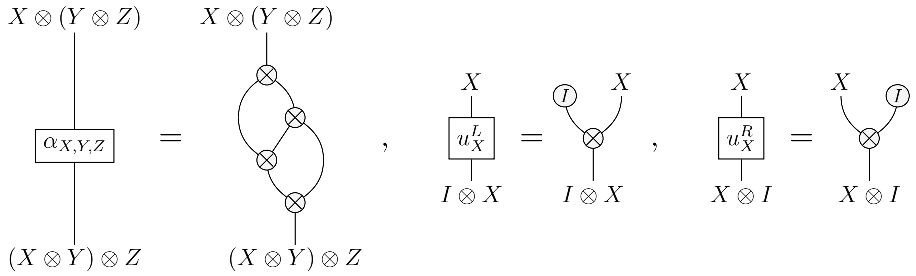


Modulo the equations: For all $f : X \to Y$ and $g : Y \to Z$ in $\mathbb{X}$:

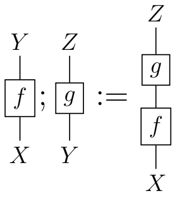


And for all $f : W \to X$ and $g : Y \to Z$ in $\mathbb{X}$:

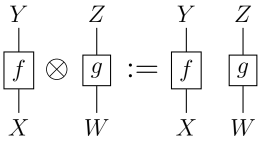




Composition: Vertical pasting:

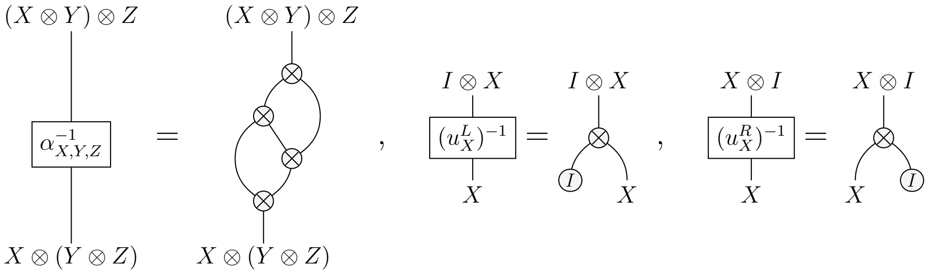


Tensor product: Horizontal pasting:



Tensor unit: The empty list [] (drawn as blank space).

By flipping around the diagrams for the unitors and associators we get their inverses:



Even in the case when we are already working in a strict monoidal category, it will still often be useful to use string diagrams for its strictification; for example, we can bundle up wires together so that we can make inductive arguments using pictures. Indeed, these string diagrams have been rediscovered by Carette et al. in the setting of quantum circuits, dubbed “the scalable ZX-calculus” for precisely this reason [CHP19]. They have not made use of the units and counits in this setting; nevertheless it has found rich applications [BR22, CDP21]. We will discuss this further in Chapter 3.

Aside 2.8. These string diagrams are closely related to proof nets for linearly-distributive categories; so much so, that this monoidal counterpart was considered folklore by some.

Some monoidal categories are monoidally equivalent to **skeletal**, strict monoidal categories, where the adjective skeletal means that every two isomorphic objects are equal. These are very nice to work with because if we want, we can forgo having to use the tensoring/untensoring and unit introduction and removal:

Example 2.9. FinOrd is a skeletal and strict monoidal under both tensor products. It is monoidally equivalent to FSet under both thensor products.

Given a commutative semiring R, Mat_R is a skeletal category and is strict monoidal. Moreover for a field k, by chosing a basis for each dimension, FVect_k is monoidally equivalent to Mat_k under the bilinear tensor product and the direct sum.

In particular, because $\mathsf{FVect}_\mathbb{C}$ and FHilb are monoidally equivalent under both the bilinear tensor product and the direct sum then FHilb is monoidally equivalent to the skeletal strict monoidal category $\mathsf{Mat}_\mathbb{C}$ under both tensor products.

The strictification of a monoidal category need not be skeletal, for example there is no skeletal strict monoidal category which is monoidally equivalent to Set. Indeed, the strictification which we described when applied to FSet is not skeletal and thus not FinOrd on the nose.

There is a more refined notion of monoidal category where one can pass wires through each other:

Definition 2.10. A **symmetric monoidal category** is a monoidal category equipped with an extra natural isomorphism called the symmetry

$$\sigma_{X,Y} : X \otimes Y \to Y \otimes X$$

satisfying the following coherence equations:

Interaction with unitors:

$$\begin{tikzcd}
I \otimes X \arrow[rr, "\sigma_{I,X}"] \arrow[dr, "u^L_X"'] & & X \otimes I \arrow[dl, "u^R_X"] \\
& X &
\end{tikzcd}$$

Interaction with associator:

$$\begin{tikzcd}
(X \otimes Y) \otimes Z \arrow[r, "\sigma_{X,Y} \otimes 1_Z"] \arrow[d, "\alpha_{X,Y,Z}"'] & (Y \otimes X) \otimes Z \arrow[d, "\alpha_{Y,X,Z}"] \\
X \otimes (Y \otimes Z) \arrow[d, "\sigma_{X,Y\otimes Z}"'] & Y \otimes (X \otimes Z) \arrow[d, "1_Y \otimes \sigma_{X,Z}"] \\
(Y \otimes Z) \otimes X \arrow[r, "\alpha_{Y,Z,X}"'] & Y \otimes (Z \otimes X)
\end{tikzcd}$$

Symmetry map is self-inverse:

$$\begin{tikzcd}
X \otimes Y \arrow[r, "\sigma_{X,Y}"] \arrow[dr, equal] & Y \otimes X \arrow[d, "\sigma_{Y,X}"] \\
& X \otimes Y
\end{tikzcd}$$

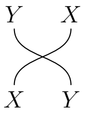
Example 2.11. Set, FSet, FinOrd, Mat_R, Vect_k, Hilb, FHilb are all symmetric monoidal categories with respect to the aforementioned monoidal structures; and the corresponding equivalences between these categories are also symmetric monoidal.

Definition 2.12. A (strong) **symmetric monoidal functor** between symmetric monoidal categories $\mathbb{X}$ and $\mathbb{Y}$ is a monoidal functor where the following coherence equation holds:

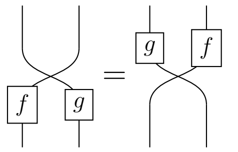
$$\begin{tikzcd}
F(X) \otimes^{\mathbb{Y}} F(Y) \arrow[r, "\sigma^{\mathbb{Y}}_{F(X),F(Y)}"] \arrow[d, "\mu_{X,Y}"'] & F(Y) \otimes^{\mathbb{Y}} F(X) \arrow[d, "\mu_{Y,X}"] \\
F(X \otimes^{\mathbb{X}} Y) \arrow[r, "F(\sigma^{\mathbb{X}}_{X,Y})"'] & F(Y \otimes^{\mathbb{X}} X)
\end{tikzcd}$$

A **symmetric monoidal natural transformation** is a monoidal natural transformation between symmetric monoidal functors. A **strict symmetric monoidal category** is a symmetric monoidal category, whose underlying monoidal category is strict. That is to say, all the coherence isomorphisms except for the symmetry maps are identities. A **strict symmetric monoidal functor** is a symmetric monoidal functor which is simultaneously a strict monoidal functor. Just as in the monoidal case, there are strict 2-categories of strict symmetric monoidal and symmetric monoidal categories.

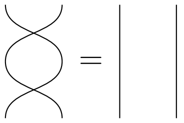
Strict monoidal categories also have a notion of string diagrams, except the symmetry allows wires to pass over each other:

$\sigma_{X,Y} =$ 

The naturality means that maps can be pulled through the symmetry:

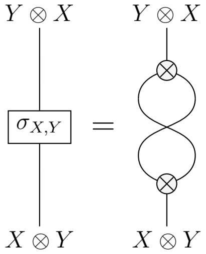


The interaction with the unitor and associator becomes completely absorbed into the graphical calculus. The self inverse of the symmetry map means that the wires untangle:



Theorem 2.13. *Every symmetric monoidal category is symmetric monoidally equivalent to a strict symmetric monoidal category.*

Non-strict symmetric monoidal categories have essentially the same notion of proof nets as non-strict monoidal categories, except where the symmetry map is internalized to untensoring, exchanging the wires and then tensoring:



This notion of string diagrams for (non-strict) symmetric monoidal categories is not contained in the paper of Wilson et al. [WGZ22]; however, it is folklore, in analogy to the case for symmetric linearly distributive categories [CS97].

Example 2.14. The category Mat_k is strict symmetric monoidal and symmetric monoidally equivalent to FVect_k under both aforementioned tensor products. The same with FinOrd and FSet.

Definition 2.15. A **compact closed category** is a symmetric monoidal category such that for every object X, there is a chosen object X^*, called the **dual** of X. For all objects X, there are maps called the **unit** and **counit**:

$$\eta_X : I \to X^* \otimes X \quad \text{and} \quad \varepsilon_X : X \otimes X^* \to I$$

satisfying the following coherence equations:

Zig-zag equations:

$$\begin{tikzcd}
(X \otimes X^*) \otimes X \arrow[r, "\alpha_{X,X^*,X}"] \arrow[d, "\varepsilon_X \otimes 1_X"'] & X \otimes (X^* \otimes X) & X^* \otimes (X \otimes X^*) \arrow[r, "\alpha_{X^*,X,X^*}"] \arrow[d, "1_{X^*} \otimes \varepsilon_X"'] & (X^* \otimes X) \otimes X^* \\
I \otimes X \arrow[r, "\sigma_{I,X}"'] & X \otimes I \arrow[u, "1_X \otimes \eta_X"'] & X^* \otimes I \arrow[r, "\sigma_{X^*,I}"'] & I \otimes X^* \arrow[u, "\eta_X \otimes 1_X X^*"']
\end{tikzcd}$$

Compatibility with the tensor product:

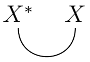
$$(X \otimes Y)^* = X^* \otimes Y^*$$

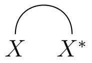
A strict compact closed category is a compact closed category where the underlying symmetric monoidal category is strict. A self-dual compact closed category is one where $X^* = X$ for all objects X. Strict symmetric monoidal functors and strong symmetric monoidal functors are the appropriate notion of map between strict/non-strict compact closed categories, as they preserve the duals strictly/strongly.

The following result follows immediately from the coherence theorem for symmetric monoidal categories because compact closed structure is preserved by symmetric monoidal functors:

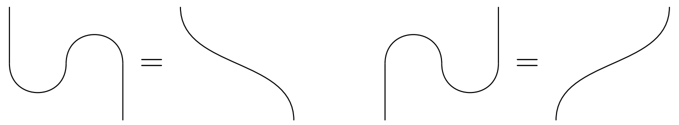
Theorem 2.16. *Every compact closed category is symmetric monoidally equivalent to a strict compact closed category.*

Compact closed categories axiomatize the kinds of processes where inputs can be turned into outputs, and vice-versa. In other words, they axiomatize a particular notion of feedback. This is illuminated by looking at the string diagrams. We will draw the unit and counit for the compact closed structure as follows in the strict case:

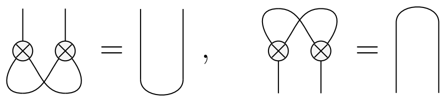
$\eta_X =$ 

and $\varepsilon_X =$ 

The zig-zag equations are drawn as follows;



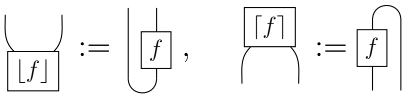
And the last two equations correspond to the requirement that:



This fixes the dualizing objects on tensor products $(X \otimes Y)^* = X^* \otimes Y^*$.

One thing that is nice about compact closed categories is that we can treat all maps as either states or effects:

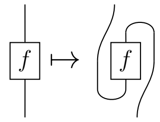
Definition 2.17. In a compact closed category, every map $f : X \to Y$ canonically induces a state $\lfloor f \rfloor : I \to X^* \otimes Y$ and an effect $\lceil f \rceil : X \otimes Y^* \to I$ given by bending the wires of f as follows:



This abstract wire-bending induces a functor:

Definition 2.18. If $\mathbb{X}$ is a compact closed category, there is a symmetric monoidal functor, $(-)^* : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$, called **the transpose**, which sends:

Objects $X \mapsto X^*$

Maps: 

Example 2.19. Out of all the examples we have discussed so far, only Mat_R, FVect_k and FHilb are compact closed when regarded as symmetric monoidal categories with respect to the bilinear tensor product. They are not compact closed with respect to the direct sum.

For FHilb and FVect_k, the compact closed structure is the same. The dual object is given by the internal hom into $\mathbb{C}/k$. Given an orthonormal basis $\{b_i\}_{i=0,\ldots,n-1}$ of a finite dimensional vector space X, with dual basis $\{b_i^*\}_{i=0,\ldots,n-1}$ of X^*, the unit and counit are given by the following linear maps:

$$\eta_X = 1 \mapsto \sum_{i=0}^{n-1} b_i^* \otimes b_i \qquad \varepsilon_X = b_i \otimes b_j^* \mapsto \begin{cases} 1 & \textit{If } i = j \\ 0 & \textit{Otherwise} \end{cases}$$

The situation for Mat_R is essentially the same. Because Mat_R is is skeletal, every object is equal to it's dual, so that $n^* = n$. The unit and counit are $\varepsilon_n = (1, \cdots, 1)$ and $\eta_n = \varepsilon_n^T$. In this case the transpose functor is exactly the transpose of matrices.

2.1.1 Dagger-monoidal categories

In this thesis, we will usually work with monoidal categories with extra structure called the dagger which allows one in some sense to "run maps in reverse" (see [Sel07, AC04]):

Definition 2.20. A **†-category** (*read dagger-category*) is a category $\mathbb{X}$ equipped with a functor $(-)^\dagger : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$ (*read the dagger*) that is:

Identity on objects: so that for all objects X of $\mathbb{X}$, $X^\dagger = X$.

Involutive: so that for all maps f of $\mathbb{X}$, $(f^\dagger)^\dagger = f$.

A map f in a dagger category is:

an isometry when $f^\dagger; f = 1$.

a coisometry when $f; f^\dagger = 1$.

unitary when $f^\dagger = f^{-1}$.

self-adjoint when $f^\dagger = f$.

a projector when $f; f = f$ and $f^\dagger = f$ (also known as a †-idempotent).

Example 2.21. $\mathsf{Mat}_\mathbb{C}$ is a †-category with respect to both the transpose and the complex conjugate transpose.

Example 2.22. The category Hilb of complex Hilbert spaces and bounded linear maps is a dagger category with respect to the Hermitian adjoint. The Hermitian adjoint of a map A is the unique map $A^\dagger$ satisfying the following equation:

$$\langle x; A|y\rangle = \langle x|A^\dagger; y\rangle$$

FHilb is also a †-category with respect to the Hermitian adjoint.

Lemma 2.23. *There is an equivalence of categories* FHilb $\cong \mathsf{Mat}_\mathbb{C}$ *preserving and reflecting the dagger structure. The Hermitian adjoint corresponds to the complex conjugate transpose along the equivalence* $\mathsf{Mat}_\mathbb{C} \cong$ FHilb.

This example is actually a bit tricky; while the dagger in $\mathsf{Mat}_{\mathbb{C}}$ is given by the complex conjugate transpose, the complex conjugate transpose in FHilb is *not* the Hermitian adjoint because A^* is only isomorphic to A.

There is a natural way to combine monoidal and dagger structure:

Definition 2.24. A **(strict) †-(symmetric) monoidal category** is a (strict) (symmetric) monoidal category equipped with a strict (symmetric) monoidal †-functor with respect to which all the components of the coherence isomorphisms of the (symmetric) monoidal category are unitary.

Example 2.25. The †-category and symmetric monoidal structures of FHilb, Hilb and $\mathsf{Mat}_{\mathbb{C}}$ are all compatible making them †-symmetric monoidal categories.

Moreover, FHilb and $\mathsf{Mat}_{\mathbb{C}}$ are equivalent as †-symmetric monoidal categories.

We capture more of monoidal category theory within the framework of dagger categories:

Definition 2.26. A (strict) †-compact closed category is a (strict) compact closed category which is (strict) †-symmetric monoidal and for all objects $\mathbb{X}$:

$$\begin{tikzcd} I \arrow[r, "\varepsilon_X^\dagger"] \arrow[dr, "\eta_X"'] & X \otimes X^* \arrow[d, "\sigma_{X,X^*}"] \\ & X^* \otimes X \end{tikzcd}$$

or equivalently

$$\begin{tikzcd} X \otimes X^* \arrow[r, "\sigma_{X,X_*}"] \arrow[dr, "\eta_X"'] & X^* \otimes X \arrow[d, "\varepsilon_X^\dagger"] \\ & I \end{tikzcd}$$

Example 2.27. The compact closed and †-symmetric monoidal structures of $\mathsf{Mat}_{\mathbb{C}}$ and FHilb are both compatible, making them †-compact closed.

2.1.2 Monoidal presentations

In this subsection, we review how monoidal categories can be presented in terms of generators and equations. A more detailed reference can be found in the Ph.D. thesis of Zanasi [Zan18].

Definition 2.28. A **monoidal theory** is a triple $T = (\mathsf{Ob}, \Sigma, E)$. Ob is the set of **colours**. The set The set of **signatures** Σ contains generators of the form $f : [X_1, \cdots, X_n] \to [Y_1, \cdots, Y_m]$, where the **arity** $[X_1, \cdots, X_n]$ and **coarity** $[Y_1, \cdots, Y_m]$ are in $\mathsf{List}(\mathsf{Ob})$ and the **name** is f indexed from some fixed set. For every object X, there is a distinguished generator $\mathsf{id}_X : X \to X$ called the **unit**. The set of (Ob, Σ)-**terms** is given by induction. For the base case, all generators are formal generators. For the first inductive case, given composable terms $f : X \to Y$ and $g : Y \to Z$, there is a formal composite $f; g : X \to Z$. Second, given two parallel terms $f : X \to Y$ and $g : Z \to W$ there is a formal tensor product $f \otimes g : [X, Z] \to [Y, W]$.

The set of **equations** E consists of pairs of parallel formal terms $f : X \to Y$ and $g : X \to Y$.

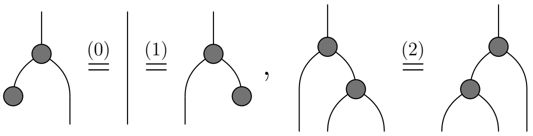
Every monoidal theory defines a strict monoidal category $\overline{T}$. This is the free strict monoidal category with objects in $\mathsf{List}(\mathsf{Ob})$ and maps formal composites of (Ob, Σ)-terms modulo the equations in E. $\overline{T}$ has the structure of a category as the identity on an object $[X_1, \cdots, X_n]$ is given by the formal composite $\mathsf{id}_{X_1} \otimes \cdots \otimes \mathsf{id}_{X_n}$ and the composition is given by formal composition. For the strict monoidal structure, the tensor unit is given by the empty list and the tensor product is given by the formal tensor product. Call such a monoidal category a **coloured pro**, or merely a **pro** when $|\mathsf{Ob}| = 1$. We will say that T is a **presentation** of a monoidal category $\mathbb{X}$ when $\overline{T}$ is monoidally equivalent to $\mathbb{X}$.

The coloured pro in a presentation is regarded as the *syntax*, and the monoidal category which it is equivalent to is regarded as the **semantics**. Throughout this thesis, the semantics will usually be concrete mathematical objects which are easy to define; whereas, finding the defining set of equations for the syntax is substantially harder. Therefore, even if both monoidal categories are equivalent, they feel much different.

Throughout this thesis, when we impose an equation between generators, if it comes up later then we will put a label above the axiom. Whenever the same axiom is imposed again we will refer to the first time it is referenced.

In practice, we won't explicitly regard a monoidal theory as a triple; rather, we will present coloured pros by drawing a list of generating equations between string diagrams. For example, the way in which string diagrams for nonstrict monoidal categories were constructed in Definition 2.7 is secretly a monoidal theory. For a more elementary example:

Example 2.29. Consider the monoidal theory m generated by a monoid on one object:

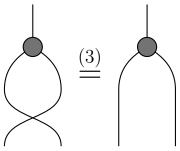


This is a presentation for the pro $\mathsf{FinOrdMonot}$, of finite ordinals and monotone maps [Laf95, Section 3.1].

Definition 2.30. A **symmetric monoidal theory** T consists of the same data as a monoidal theory except the equations are now defined by parallel maps generated by $\Sigma \sqcup C$, where $C = \{\sigma_X : [X, X] \to [X, X] \mid \forall X \in \mathsf{Ob}\}$ is the set of distinguished symmetry maps.

The corresponding strict symmetric monoidal category $\overline{T}$ is given by quotienting the symmetric monoidal category freely generated by the objects Ob and maps Σ by the equations in E. These symmetric monoidal categories are called **coloured props**, or merely **props** when $|\mathsf{Ob}| = 1$.

Example 2.31. Consider the symmetric monoidal theory cm generated by a monoid ●, which is also commutative:

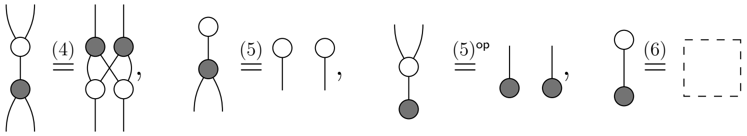


This is a presentation for the prop of finite ordinals and functions FinOrd under the disjoint union [Laf95, Section 3.3]. This is a formal way to talk about the graph of a function between finite sets.

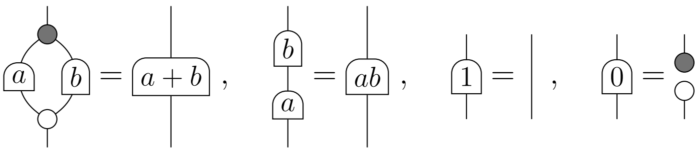
This elegant presentation of the symmetric monoidal category of finite sets motivates finding presentations for other well-known mathematical structures.

The following result has probably been known for quite some time. The earliest reference I could find is due to Lafont, where he considers only the Boolean semiring [Laf95, Figure 3]; in a subsequent paper, he proves the analogous result for arbitrary fields [Laf03, Figure 26]:

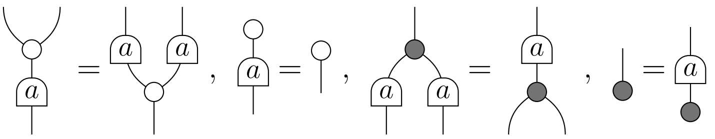
Example 2.32. Take a commutative semiring S. Consider the prop cb_S generated by a commutative monoid ● and comonoid ○ interacting to form a **bicommutative bialgebra**:



with generators for all elements $a, b \in S$ such that the structure of the commutative semiring S is reflected in the convolution of the bialgebra



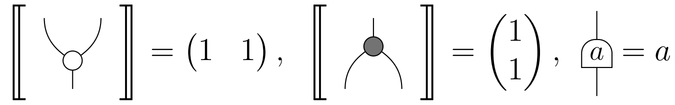
where the commutative monoid and cocommutative comonoid are both natural with respect to the scalars:



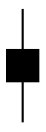
This monoidal theory is equivalent to the prop of matrices over S, Mat_S, under the direct sum. Recall that the direct sum of matrices R and S is given by the following block diagonal matrix:

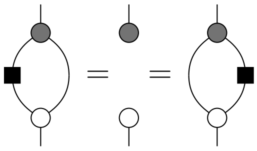
$$R \oplus S := \begin{bmatrix} R & 0 \\ 0 & S \end{bmatrix}$$

The generators of this presentation are interpreted in Mat_S as follows:

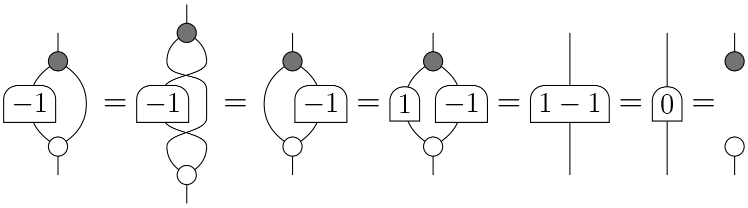


The unit and counit are interpreted as the unique matrices from $0 \to 1$ and $1 \to 0$, respectively. Because $\mathbb{N}$ is the initial commutative semiring, $\mathsf{Mat}_{\mathbb{N}}$ can be presented in terms of the prop for the free bicommutative bialgebra, where the generators and equations for scalars are derivable.

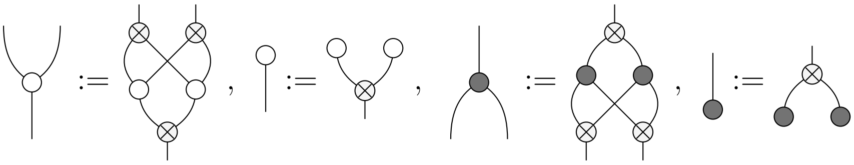
In particular, when S is a ring, then the bialgebra is promoted to a **Hopf algebra**, so that there exists an **antipode**  such that:



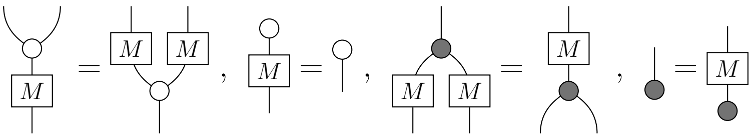
where the antipode of the Hopf algebra is given by the scalar -1:



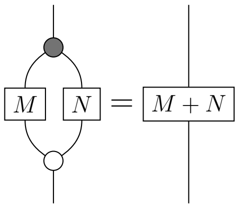
If we define monoids and comonoids on composite systems as follows:



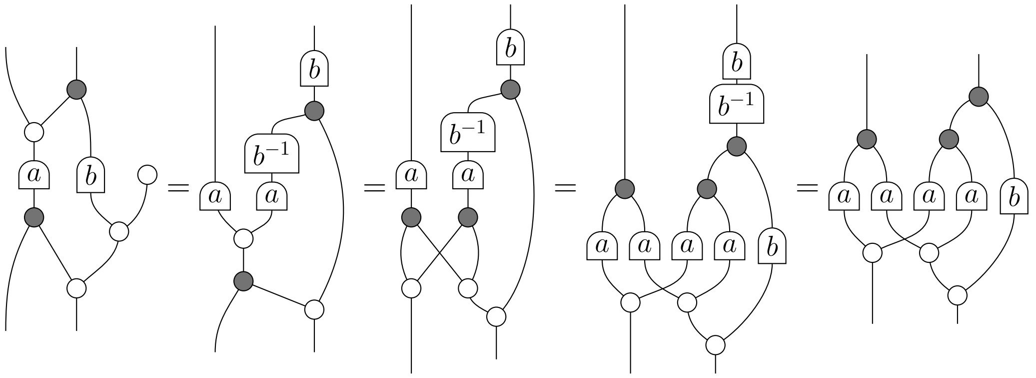
then arbitrary matrices $M : n \to m$ are natural with respect to these families of maps:



Therefore, given two parallel matrices M and N, their sum is given by convolution with the bialgebra:

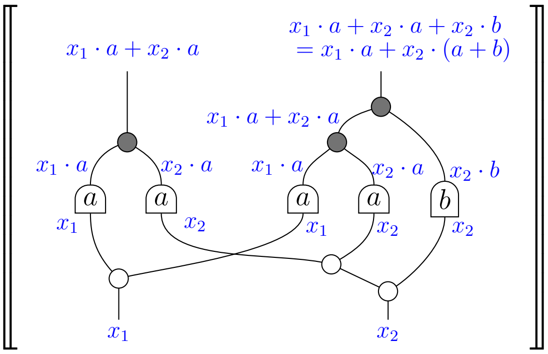


One can perform matrix multiplication by pulling all of the white generators to the bottom and grey generators to the top so that the elements of the commutative semiring live in the middle. Consider the following example:



This makes it clear how to interpret this as a matrix. Follow the wires from the bottom and chase their paths to the top, copying them when they meet white nodes, adding them when they meet grey ones, and multiplying them when they meet scalars:

Example 2.33.



$$= \begin{bmatrix} a & a \\ a & a+b \end{bmatrix}$$

Where

$$\begin{bmatrix} a & a \\ a & a+b \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot a + x_2 \cdot a \\ x_1 \cdot a + x_2 \cdot (a+b) \end{bmatrix}$$

Matrices can be generalized to have no fixed origin:

Definition 2.34. Given a commutative semiring R, the prop AffMat_R of affine matrices over R has:

Objects: Natural numbers.

Maps: A map $(M, a) : n \to m$ is a pair of a matrix $M : n \to m$ and a vector $1 \to m$.

Identity: The identity on an object n is the pair

$$(I_n, \mathbf{0} : 1 \to n)$$

where I_n is the identity matrix and $\mathbf{0}$ is the zero vector.

Composition

$$\frac{n \xrightarrow{(M,a)} m \ , \quad m \xrightarrow{(N,b)} k}{n \xrightarrow{(M,a);(N,b):=(NM,Na+b)} k}$$

Monoidal structure: The tensor product is given pointwise:

$$(M,a) \oplus (N,b) := (M \oplus n, a \oplus b)$$

The tensor unit is the identity on 0.

Note that Mat_R faithfully embeds into AffMat_R:

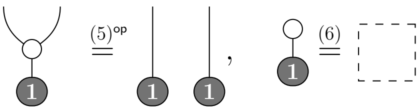
$$\left(n \xrightarrow{M} m\right) \mapsto \left(n \xrightarrow{(M,\mathbf{0})} m\right)$$

In the other direction, there is also a fathful embedding $\mathsf{AffMat}_R \to \mathsf{Mat}_R$ taking an affine matrix to its **augmented matrix**:

$$\left(n \xrightarrow{(M,a)} m\right) \mapsto \left(n+1 \xrightarrow[.]{\begin{bmatrix} M & a \\ \mathbf{0} & 1 \end{bmatrix}} m+1\right)$$

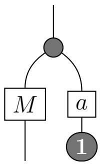
I can not find a reference for the following result, but it is is an immediate consequence of Bonchi et al.'s analysis of affine relations [BPSZ19]:

Example 2.35. Given a commutative semiring R, the prop acb_R is presented by adding the following generators and relations to cb_R:

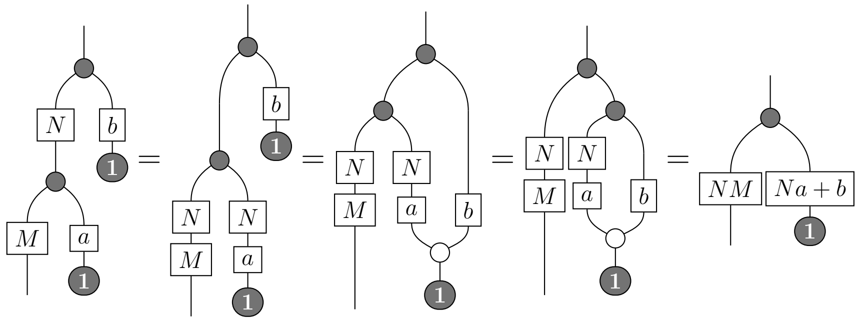


This is a presentation for the prop of affine matrices over S. This new generator is interpreted as the affine shift.

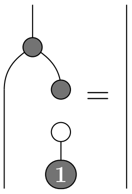
Then an affine matrix (M,a), it is represented by the following string diagram:



so that the composite of two affine matrices can be computed diagrammatically:

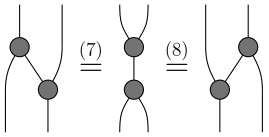


The other axiom is needed for the identity law:

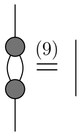


The following structure will show up quite a lot throughout this thesis:

Example 2.36. A **Frobenius** algebra is a monoid ● and comonoid ● interacting to satisfy the Frobenius laws:



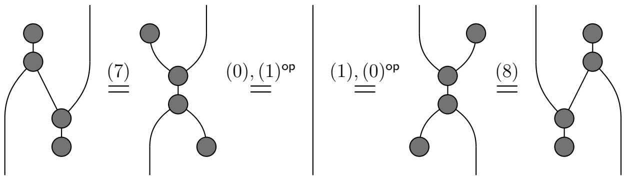
This is moreover a **special** Frobenius algebra when:



A commutative (special) Frobenius algebra is a (special) Frobenius algebra between a commutative monoid and a cocommutative comonoid.

Denote the pro generated by a Frobenius algebra by fa, and a special Frobenius algebra by sfa. Denote the prop generated by a commutative Frobenius algebra by cfa, and a special commutative Frobenius algebra by scfa.

Frobenius algebras make objects self dual:



So that symmetric monoidal categories equipped with a compatible supply of commutative (†-)Frobenius alegbras compatible with the monoidal structure is self dual (†-)compact closed.

2.2 Categories of spans and relations

Categories are defined in a manner which distinguishes the inputs and outputs of maps. †-categories are one approach to moving beyond this bias; however, they are "evil" in the sense that the †-structure is not always preserved/reflected by categorical equivalence.

Spans and relations provide a categorically well-behaved, flexible setting with which to interpret processes without elevating inputs over outputs. Whereas functions produce unique outputs from inputs, spans and relations nondeterministicaly associate several inputs with several outputs. To introduce these mathematical constructions, all of the category theory in this subsection which is not explicitly cited is standard and can be found, for example, in most introductions to category theory; for example in Mac Lane's canonical reference [Lan78]. We first need to recall some basic facts about limits.

Definition 2.37. The **product** of two objects X and Y (if it exists) in some category, is an object $X \times Y$ equipped with maps $\pi_0 : X \times Y \to X$ and $\pi_1 : X \times Y \to Y$ called the **projections**, such that for any object A and diagram $X \xleftarrow{f} A \xrightarrow{g} Y$ there exists a unique map $\langle f, g \rangle : A \to X \times Y$ called **the pairing map** making the following diagram commute:

$$\begin{tikzcd}
& A \arrow[ld, "f"'] \arrow[rd, "g"] \arrow[d, dashed, "{\langle f,g \rangle}"] & \\
X & X \times Y \arrow[l, "\pi_0"] \arrow[r, "\pi_1"'] & Y
\end{tikzcd}$$

Given two maps $f : W \to X$ and $G : Y \to Z$, their product is defined to be the universal map $f \times g : W \times Y \to X \times Z$:

$$\begin{tikzcd}
W \arrow[d, "f"'] & W \times Y \arrow[l, "\pi_0"'] \arrow[r, "\pi_1"] \arrow[d, dashed, "f \times g"] & Y \arrow[d, "g"] \\
X & Y \times Z \arrow[l, "\pi^0"'] \arrow[r, "\pi_1"'] & Z
\end{tikzcd}$$

The **diagonal map** at X is the pairing map on the identity $\Delta_X := \langle X, X \rangle$. A **terminal object** in a category (if it exists) is an object $\mathbb{1}$ equipped with a unique map $!_X : X \to \mathbb{1}$ for every object X called the **discard map** or the **terminal map**. A category is **Cartesian** when it has all finite products and a terminal object.

Let us spell out the dual notion in order to establish the dual notations. The **coproduct** in $\mathbb{X}$ is the product in $\mathbb{X}^{\mathsf{op}}$:

$$\begin{tikzcd}
& A & \\
X \arrow[ru, "f"] \arrow[r, "\iota_0"'] & X + Y \arrow[u, dashed, "{[f,g]}"'] & Y \arrow[lu, "g"'] \arrow[l, "\iota_1"]
\end{tikzcd}$$

Where $X + Y$ is the product object. An **initial object** in a category (if it exists) is an object $\emptyset$ equipped with a unique map $?_X : \emptyset \to X$ for each object X. A category is **coCartesian** when it has all finite coproducts and an initial object.

Example 2.38. Set and FSet are Cartesian with respect to the Cartesian product:

$$X \times Y := \{(x, y) \mid \forall x \in X, y \in Y\}$$

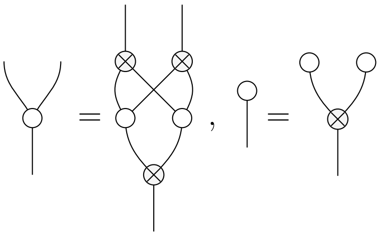
They are coCartesian with respect to the disjoint union

$$X + Y := \{(x, 1) \mid \forall x \in X\} \cup \{(y, 2) \mid \forall y \in Y\}$$

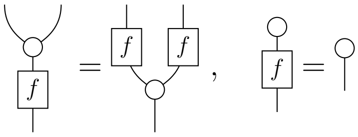
Similarly, FVect_k and Mat_S are Cartesian and coCartesian both with respect to the direct sum.

A Cartesian category is precisely a monoidal category which allows one to copy and delete things in a manner which is deterministic and total:

Lemma 2.39. *A category is Cartesian iff it has a symmetric monoidal structure equipped with a cocommutative comonoid* ○ *on every object (see Example 2.31) compatible with the monoidal structure, so that*



where the comultiplication and counit are also natural, so that for any map f:



The comonoid corresponds to the diagonal map and the counit corresponds to the discard map.

Therefore, when we gave presentations for FinOrd and Mat_S, the natural white commutative comonoid is precisely the one coming from the Cartesian structure. The naturality of the diagonal map corresponds to determinism, and the naturality of the discard corresponds to totality. We will come back to this shortly.

As we alluded to in the introduction of this subsection, the Cartesian notion of copying biases inputs over outputs, and the coCartesian notion of comparison biases outputs over inputs. We are interested in a more permissive (partial and nondeterministic), symmetric notion of copying, which is compatible with †-structure. The following construction allows us to develop such a structure, generalizing the product modulo shared structure:

Definition 2.40. The **pullback** of a diagram $X \xrightarrow{f} A \xleftarrow{g} Y$ (if it exists) is an object $X\ {}_f{\times}_g\ Y$ called the **apex** and maps $\pi_0 : X\ {}_f{\times}_g\ Y \to X$ and $\pi_1 : X\ {}_f{\times}_g\ Y \to Y$ called **the projections**, such that for any diagram $X \xleftarrow{p_0} P \xrightarrow{p_1} Y$ making the following diagram commute,

$$\begin{tikzcd}
& B \arrow[ld, "p_0"'] \arrow[rd, "p_1"] & \\
X \arrow[rd, "f"'] & & Y \arrow[ld, "g"] \\
& A &
\end{tikzcd}$$

there exists a unique map $u : P \to X\ {}_f\!\times_g Y$ making the following diagram commute:

$$\begin{tikzcd}
& P \arrow[d, dashed, "u"] \arrow[ddl, bend right, "p_0"'] \arrow[ddr, bend left, "p_1"] & \\
& X\ {}_f\!\times_g Y \arrow[dl, "\pi_0"'] \arrow[dr, "\pi_1"] \arrow[d, phantom, "\smile"] & \\
X \arrow[dr, "f"'] & {} & Y \arrow[dl, "g"] \\
& A &
\end{tikzcd}$$

A chevron is drawn under the apex of the span to denote that the square is a pullback. A category is **finitely complete** if it has a terminal object and all pullbacks exist. Notice that product $X \times Y$ is the pullback of the diagram $X \to 1 \leftarrow Y$. The dual notion of a pullback is a **pushout**; the pushout of a diagram $X \xrightarrow{f} A \xleftarrow{g} Y$ is denoted by $X\ {}_f\!+_g Y$. We draw a chevron on the apex of the cospan, to denote that a square is a pushout as follows:

$$\begin{tikzcd}
& P & \\
& X\ {}_f\!+_g Y \arrow[u, dashed] \arrow[d, phantom, "\smile"] & \\
X \arrow[uur, bend left, "i_0"] \arrow[ur, "\iota_0"] & {} & Y \arrow[uul, bend right, "i_1"'] \arrow[ul, "\iota_1"'] \\
& A \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Example 2.41. In Set the pullback of a cospan $X \xrightarrow{f} A \xleftarrow{g} Y$ is (up to unique isomorphism) the set:

$$\{(x, y) \in X \times Y : f(x) = g(y)\}$$

The pushout of a span $X \xleftarrow{f} A \xrightarrow{g} Y$ is the quotient of the set $X + Y$ by:

$$f(a) \sim g(a) \quad \text{for all } a \in A$$

The concrete pullback/pushout of matrices is essentially the same with the direct sum instead of the Cartesian product/disjoint union.

Spans form a bicategory under pullback:

Definition 2.42. Given a finitely complete category $\mathbb{X}$, the bicategory of spans $\mathsf{Span}(\mathbb{X})$ has:

0-cells: Objects of $\mathbb{X}$.

1-cells: 1-cells $(A, f, g) : X \to Y$ are spans in $\mathbb{X}$ from A:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X & & Y
\end{tikzcd}$$

Composition is induced by pullback:

$$\begin{tikzcd}[column sep=small]
& A \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X & & Y
\end{tikzcd}
\; ; \;
\begin{tikzcd}[column sep=small]
& B \arrow[dl, "h"'] \arrow[dr, "k"] & \\
Y & & Z
\end{tikzcd}
:=
\begin{tikzcd}[column sep=small]
& & A\,{}_g\!\times_k B \arrow[dl, "\pi_0"'] \arrow[dr, "\pi_1"] \arrow[d, phantom, "\smile"] & & \\
& A \arrow[dl, "f"'] \arrow[dr, "g"] & {} & B \arrow[dl, "h"'] \arrow[dr, "k"] & \\
X & & Y & & Z
\end{tikzcd}$$

The identity on X is given by the span:

$$\begin{tikzcd}
& X \arrow[dl, equal] \arrow[dr, equal] & \\
X & & X
\end{tikzcd}$$

2-cells: A 2-cell $\varphi : (A, f, g) \Rightarrow (B, h, k)$ between parallel spans is a map $\varphi : A \to B$ in $\mathbb{X}$ such that the following diagram commutes:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[dd, "\varphi"] & \\
X & & Y \\
& B \arrow[ul, "h"] \arrow[ur, "k"'] &
\end{tikzcd}$$

The composition and identity of 2-cells is given by the composition and identity in $\mathbb{X}$.

The composition of 1-cells is not strict, so that the associativity and unitality of composition hold up to coherent isomorphism. The coherence isomorphisms are the canonical 2-cells induced by the universal property of the pullback.

The ordinary category of spans of $\mathbb{X}$, $\mathsf{Span}^{\sim}(\mathbb{X})$, has maps being equivalence classes of isomorphic spans; so that,

$$(X \overset{f}{\leftarrow} A \overset{g}{\rightarrow} Y) \sim (X \overset{h}{\leftarrow} B \overset{k}{\rightarrow} Y)$$

if and only if there exists an isomorphism $A \overset{\varphi}{\rightarrow} B$ such that the following diagram commutes:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[dd, "\varphi", "\cong"'] & \\
X & & Y \\
& B \arrow[ul, "h"] \arrow[ur, "k"'] &
\end{tikzcd}$$

$\mathbb{X}$ embeds in $\mathsf{Span}^{\sim}(\mathbb{X})$ in two different ways: covariantly as the **graph** and contravariantly as the **cograph**:

$$\left(X \overset{f}{\rightarrow} Y\right) \mapsto \left(\begin{tikzcd} X \arrow[r, equal] & X \arrow[r, "f"] & Y \end{tikzcd}\right), \quad \left(X \overset{f}{\rightarrow} Y\right) \mapsto \left(\begin{tikzcd} Y & X \arrow[l, "f"'] \arrow[r, equal] & X \end{tikzcd}\right)$$

Regarded as a monoidal category under the Cartesian product, the two embeddings turn the diagonal maps and discard maps into commutative †-Frobenius algebras, making $\mathsf{Span}^{\sim}(\mathbb{X})$ self-dual †-compact closed, where the †-functor is given by the converse $(f, A, g) \mapsto (g, A, f)$.

For the interested reader, the monoidal structures (or lack thereof) of categories of cospans and spans of sets is elaborated on in great detail in the work of Bruni and Gadducci [BG03].

Categories of spans give mathematical semantics for nondeterministic processes where inputs are associated to possible outputs with multiplicity. A 2-cell between two processes thus describes a method to coherently transform one process into another. For example:

Example 2.43. $\mathsf{Span}^{\sim}(\mathsf{FSet})$ is †-symmetric monoidally equivalent to $\mathsf{Mat}_{\mathbb{N}}$ under both tensor products.

This example is quite useful for developing intuition. Take a span of finite sets $X \xleftarrow{f} M \xrightarrow{g} Y$, where X and Y have a chosen order. This determines an $|X| \times |Y|$ matrix, where the entry at $(x, y) \in X \times Y$ is given by the cardinality of the preimage $\langle f, g\rangle^{-1}(X \times Y)$. That is to say, the number of times x and y are related.

We seek, moreover, to quotient by multiplicity, to obtain a semantics for honest nondeterministic processes: where things can be related at most once. To do so, we need more assumptions about the category which we are working internal to:

Definition 2.44. A map $f : X \to Y$ is a **monomorphism** (monic) when for all maps $g, h : Z \to X$, $g; f = h; f$ implies $g = h$.

Dually, a map $f : X \to Y$ is an **epimorphism** (epic) when for all maps $g, h : Y \to Z$, $f; g = f; h$ implies $g = h$.

To add extra information to diagrams, we denote monomorphisms as arrows with tails $\rightarrowtail$ and epimorphisms as arrows with two heads $\twoheadrightarrow$.

Monomorphisms and epimorphisms are the categorically well-behaved analogues of injections and surjections; where a map is similarly an isomorphism when it is an epimorphism and a monomorphism. In all of the examples we care about in this thesis, the monomorphisms are exactly the injections and the epimorphisms are exactly the surjections. However, it is needed for a proper exposition of categories of relations.

There are special kinds of monomorphisms and epimorphisms which come up:

Definition 2.45. The **equalizer** of two parallel maps $f, g : X \to Y$, if it exists, is an object $E_{f,g}$ equipped with a map $m : E_{f,g} \to X$ such that for all objects F and maps $h : F \to E_{f,g}$, there exists a unique map $u : F \to X$ making the following diagram commute:

$$\begin{tikzcd}
F \arrow[d, "h"'] \arrow[rd, dashed, "u"] & & \\
E_{f,g} \arrow[r, tail, "m"'] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y
\end{tikzcd}$$

The maps m arising from equalizers are monomorphisms. Monomorphisms arising this way are called **regular monomorphisms**. The dual notion to an equalizer is a

coequalizer, and the epimorphisms arizing in this way are called **regular epimorphisms**.

We have already been using coequalizers throughout this thesis whenever we impose equations by taking quotients. Indeed:

Example 2.46. Sets and matrices both have equalizers and coequalizers. In sets, the equalizer of two functions $g, f : X \to Y$ is (up to unique isomorphism) the set

$$\{x \in X : f(x) = g(x)\} \subseteq X$$

The coequalizer is the quotient $Y/\sim$ of the set Y by the equivalence relation

$$f(x) \sim g(y)$$

The situation is essentially the same for matrices.

We use coequalizers to capture categories have good notions of images and kernels:

Definition 2.47. Take a finitely complete category. Construct the pullback of a map $f : X \to Y$ along itself:

$$\begin{tikzcd} X\ {}_f\!\times_f X \arrow[r, shift left, "\pi_0;f"] \arrow[r, shift right, "\pi_1;f"'] & Y \end{tikzcd}$$

Call this diagram a **kernel pair** at f, and call the object the **kernel** of f, denoted by $\mathsf{ker}(f) := X\ {}_f\!\times_f X$. If the kernel pair at f admits a coequalizer, call this object the **image** of f, denoted by $\mathsf{im}(f)$.

A **regular category** is a finitely complete category such that:

- Every kernel pair admits a coequalizer.
- Pullbacks of arbitrary maps along regular epimorphisms are regular epimorphisms.

Example 2.48. Set, FSet, FVect_k and Mat_k for k a field (or more generally a principal ideal domain) are all regular categories.

In these examples, kernels and images are the usual notions of kernels and images.

Lemma 2.49. *In a regular category, every map $f : X \to Y$ can be factorized into a regular epimorphism e_f followed by a monomorphism m_f up to unique isomorphism:*

$$\begin{tikzcd} X \arrow[r, two heads, "e_f"] \arrow[dr, "f"'] & X/\mathsf{ker} f =: \mathsf{coim}(f) \arrow[d, tail, "m_f"] \\ & Y \end{tikzcd}$$

Definition 2.50. Given a regular category $\mathbb{X}$, the strict 2-category of **relations** internal to $\mathbb{X}$, $\mathsf{Rel}(\mathbb{X})$ has:

0-cells: Objects of $\mathbb{X}$.

1-cells: 1-cells $(A, f, g) : X \to Y$ are jointly monic spans in $\mathbb{X}$ from A:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X & & Y
\end{tikzcd}$$

This span being **jointly monic** means that for any object B and maps $h, k : B \to A$ if $h; f = k; f$ and $h; g = k; g$, then $h = k$.

To compose jointly monic spans $(A, f, g) : X \to Y$ and $(B, h, k) : Y \to Z$, first compute the pullback:

$$\begin{tikzcd}
& & A \,{}_g\!\times_k B \arrow[dl, two heads, "\pi_0"'] \arrow[dr, two heads, "\pi_1"] \arrow[d, phantom, "\smile"] & & \\
& A \arrow[dl, "f"'] \arrow[dr, "g"] & {} & B \arrow[dl, "h"'] \arrow[dr, "k"] & \\
X & & Y & & Z
\end{tikzcd}$$

Composing with the pairing map we get a map $\langle \pi_0; f, \pi_1; k\rangle : A_g \times_k B \to X \times Z$. Because $\mathbb{X}$ is a regular category, there is a factorization of $\langle \pi_0; f, \pi_1; k\rangle$ into an regular epimorphism followed by monomorphism:

$$\begin{tikzcd}
A \,{}_g \times_k B \arrow[d, two heads, "e:=e_{\langle \pi_0;f,\pi_1;k\rangle}"'] \arrow[dr, "\langle \pi_0;f,\pi_1;k\rangle"] & \\
E := \mathsf{coim}(\langle \pi_0; f, \pi_1; k\rangle) \arrow[r, tail, "m:=m_{\langle \pi_0;f,\pi_1;k\rangle}"'] & X \times Z
\end{tikzcd}$$

which induces a jointly monic span, which we take to be the composite:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[dr, "g"] & & ; & & B \arrow[dl, "f"'] \arrow[dr, "g"] & & := & & E \arrow[dl, "m;\pi_0"'] \arrow[dr, "m;\pi_1"] & \\
X & & Y & & Y & & Z & & X & & Y
\end{tikzcd}$$

The identity for composition is the same as for spans.

2-cells: The 2-cells are the same as for spans.

Relations have the special property, unlike spans in general, that they are poset-enriched; that is to say, either there exists a single 2-cell between 1-cells or there is none. This makes things much simpler than the spans picture, because one never has to deal with coherence equations. This also justifies the interpretation of nondeterministic processes in this setting: possibility amounts to the mere existence of a 2-cell. Any two ways to arrive at the same result must be the same.

This is why, unlike for spans, we don't have to quotient to obtain an ordinary category of relations; we just need to forget about the 2-cells.

Just as for spans, relations are †-compact closed with respect to the Cartesian product where the †-functor is given by the converse. Consider the following concrete example:

Example 2.51. $\mathsf{Rel} := \mathsf{Rel}(\mathsf{Set})$ has:

0-cells: Natural numbers.

1-cells: A relation from $n \to m$ is a subset of $X \times Y$. The composition of relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ is given by:

$$R; S := \{(x, z) \in X \times Z : \exists y \in Y, (x, y) \in R \wedge (y, z) \in S\} \subseteq X \times Z$$

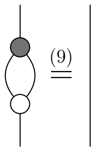
2-cells: A 2-cell $R \Rightarrow S$ is a subset $R \subseteq S$.

If we restrict ourselves to finite sets we have the following well known equivalence. The preservation and reflection of both monoidal structures is perhaps not so well-known; however, it is described in the infinite case in the work of Bruni and Gadducci [BG03, Section 3].

Lemma 2.52. $\mathsf{Rel}(\mathsf{FSet})$ *is symmetric monoidally equivalent to* $\mathsf{Mat}(\mathbb{B})$ *under both tensor products.*

This quotient $\mathsf{Span}^{\sim}(\mathsf{FSet}) \twoheadrightarrow \mathsf{Rel}(\mathsf{FSet})$ corresponds to applying the commutative semiring homorphism $\mathbb{N} \to \mathbb{B}$, where $\mathbb{B}$ is the Boolean semiring, making $2 = 1$.

Therefore the quotient from $\mathsf{cb}_{\mathbb{N}} \to \mathsf{cb}_{\mathbb{B}}$ can be stated as the following equation between string diagrams; meaning that we don't care which path we take, merely of the existence of a path:



The following category of relations is very important for this thesis:

Definition 2.53. Given a field k, the †-compact closed prop of **linear relations** over k, $\mathsf{LinRel}_{\mathsf{k}}$ is defined to be $\mathsf{Rel}(\mathsf{Mat}_k)$ with respect to the direct sum.

Explicitly, $\mathsf{LinRel}_{\mathsf{k}}$ has:

Objects: Natural numbers.

Maps: A linear relation $n \to m$ is a linear subspace of $k^n \oplus k^m$.

Composition: Given $R \subseteq k^n \oplus k^m$ and $S \subseteq k^m \oplus k^\ell$:

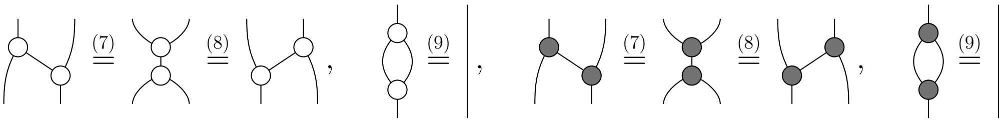
$$R; S := \{(x, z) \in k^n \oplus k^\ell : \exists y \in k^m, (x, y) \in R \wedge (y, z) \in S\} \subseteq k^n \oplus k^\ell$$

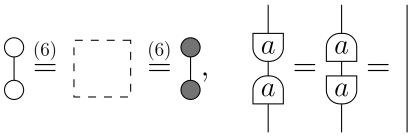
Tensor product: Given $R \subseteq k^n \oplus k^m$ and $S \subseteq k^\ell \oplus k^q$:

$$R \oplus S := \left\{ \left(\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} : \forall (a_1, b_1) \in R, (a_2, b_2) \in S \right) \right\} \subseteq k^{n+\ell} \oplus k^{m+q}$$

This prop has a presentation in terms of interacting Hopf algebras:

Definition 2.54. Given a field k, let ih_k be the quotient of the props $\mathsf{cb}_k + \mathsf{cb}_k^{\mathsf{op}}$, modulo the equations, for all $a \in k^*$ (where the generators of $\mathsf{cb}_k^{\mathsf{op}}$ are drawn as the vertically flipped generators of cb_k):

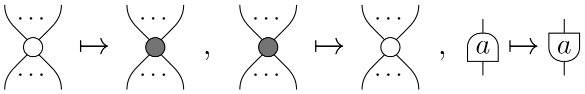




Lemma 2.55 ([Zan18, Section 3.4])**.** ih_k *is a presentation for* $\mathsf{LinRel_k}$*.*

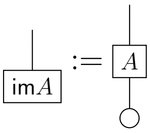
The colour-swapping dagger functor $(-)^T : \mathsf{ih}_k^{\mathsf{op}} \to \mathsf{ih}_k$ corresponds to the transpose of matrices; and the colour-preserving dagger functor $(-)^* : \mathsf{ih}_k^{\mathsf{op}} \to \mathsf{ih}_k$ corresponds to the transpose coming from the compact closed structure of ih_k. These should not be confused with each other: the latter is the relational converse. Combining these two daggers we have:

Lemma 2.56 ([Sob17])**.** *The orthogonal complement corresponds to the identity on objects involutive conjugation functor* $(-)^\perp : \mathsf{ih}_k \to \mathsf{ih}_k$;

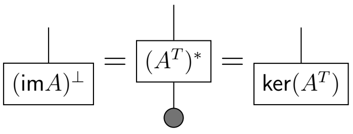


From this, there is a graphical proof of the rank-nullity theorem:

Lemma 2.57 ([Sob17])**.** *Given a matrix* $A : n \to m$ *in* $\mathsf{cb}_k \hookrightarrow \mathsf{ih}_k$*, then:*



Therefore



The previous two results are almost certainly contained in [Zan18] because of the importance of images and kernels in the proof that $\mathsf{ih}_k \cong \mathsf{LinRel_k}$, but they are hidden within calculations.

One might seek to find a similar presentation for relations internal to affine matrices. However, the category AffMat_k is not a regular category, it doesn't even have all pullbacks. The empty set can not be regarded as a vector space because it has no origin; however, because affine transformations are not required to preserve the origin, it is perfectly fine to ask for an affine transformation from an empty space.

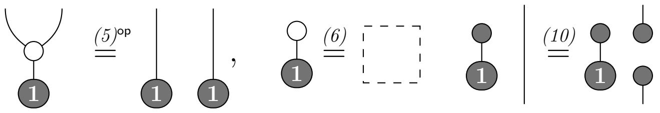
By shifting to the category AffMat_k+1 where one freely adds the empty set as the initial object, so that there is a unique map $\emptyset \xrightarrow{?_n} k^n$ for all n, we obtain an algebraic theory, and thus a regular category. Notice that AffMat_k is the full subcategory of $\mathsf{AffMat}_k + 1$ with nonempty objects. Therefore, we can take the category of internal relations:

Definition 2.58. The prop of **affine relations** over k, AffRel_k is the full subcategory of $\mathsf{Rel}(\mathsf{AffMat}_k + 1)$ of nonempty affine subspaces.

Concretely, this is constructed in the same way as $\mathsf{LinRel}_{\mathsf{k}}$, but maps $n \to m$ are now (possibly empty) affine subspaces $S \subseteq k^n \oplus k^m$. That is to say, S is a subset of $k^n \oplus k^m$ such that for any $a \in S$, the set $\{v + a \mid \forall v \in S\}$ is a linear subspace of $k^n \oplus k^m$. The empty set vacuously satisfies this condition.

We forget the empty set as an object and retain it merely as a subobject so that we can present it as a (single coloured) prop as follows:

Lemma 2.59 ([BPSZ19, Section A])**.** AffRel_k *is presented by the prop* aih_k *given by adding the following generators and equations to the presentation of* ih_k*:*

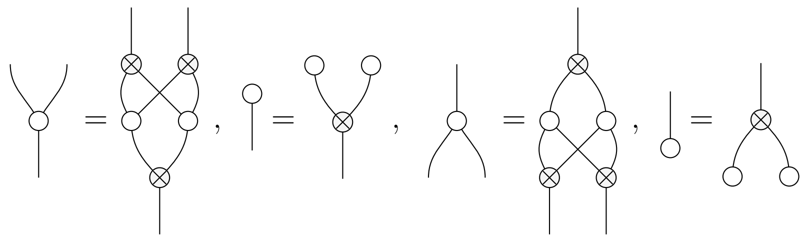


The first two equations come from the presentation of affine matrices, and the last equation enforces the initiality of the empty affine space as a subobject.

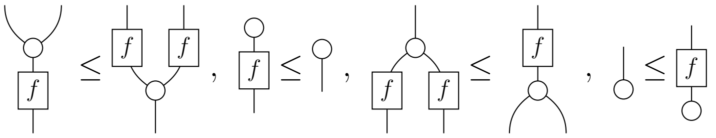
The original presentation of AffRel_k given by Bonci et al. was proven to be equivalent to the concrete category of affine relations [BPSZ19, Section A]; rather than the nonempty full subcategory of internal relations of possibly empty, finite dimensional affine spaces. However, as we have discussed, both perspectives are equivalent.

The essence of the Cartesian monoidal structure of categories of relations can be generalised to the following algebraic notion due to Carboni and Walters [CW87]:

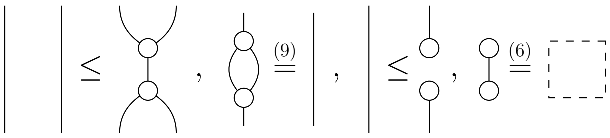
Definition 2.60. A **Cartesian bicategory of relations** is a symmetric monoidal category $\mathbb{X}$ enriched in posets, equipped with a commutative Frobenius algebra ○ on every object (see Example 2.36), compatible with the monoidal structure:



The (co)multiplications and (co)units are moreover required to be lax-natural so that for any map f:



And the multiplications and units are required to be right adjoint to the comultiplications and counits:



Therefore, now we can copy and delete things with the commutative comonoid structure in a partial, deterministic manner. Moreover the commutative monoid structure also allows us to compare and ask for the existence of things in a nondeterministic and partial manner.

Given a finitely complete category $\mathbb{X}$, $\mathsf{Span}(\mathbb{X})$ is not a Cartesian bicategory of relations because it is not poset enriched (there can be more than one 2-cell between 1-cells); however it is a *Cartesian bicategory* (see Carboni et al. [CKWW08]). All of the equations now only hold up to coherent isomorphism, however the story is essentially the same. This is much more difficult to work with because this notion requires coherence conditions so we will omit this more general definition for the sake of brevity.

Cartesian bicategories of relations subsume categories of internal relations:

Example 2.61. Given a regular category $\mathbb{X}$, $\mathsf{Rel}(\mathbb{X})$ is a Cartesian bicategory of relations under the Cartesian product and $\mathsf{Map}(\mathsf{Rel}(\mathbb{X})) = \mathbb{X}$, where $\mathsf{Map}(\mathbb{X})$ is the category of comonoid homorphisms in a Cartesian bicategory of relations $\mathbb{X}$.

We see that either the white and grey Frobenius algebras of the presentation ih_k of $\mathsf{LinRel}_\mathsf{k}$ can be regarded as the Frobenius algebra structure coming from viewing it as a bicategory of relations. Similarly, for the white Frobenius algebra of AffRel, but *not* the grey one because addition and copying are no longer dual to each other.

There are classes of categories in between Cartesian categories and Cartesian bicategories of relations which capture partially invertible and partial deterministic notions of copying. We review these notions and give examples which will serve to motivate their usage in quantum computing later in this thesis.

First, we review the categorical semantics of partiality:

Definition 2.62 ([CL02, Section 2.1.1])**.** A **restriction category** is a category along with a restriction operator $(A \xrightarrow{f} B) \mapsto (A \xrightarrow{\overline{f}} A)$ such that:

[R.1] $\overline{f};f = f$ **[R.2]** $\overline{f};\overline{g} = \overline{g};\overline{f}$ **[R.3]** $\overline{f};\overline{g} = \overline{\overline{f};g}$ **[R.4]** $f;\overline{g} = \overline{f;g};f$

Maps of the form $\overline{f}$ are called restriction idempotents. Restriction categories are poset enriched where $f \leq g \iff \overline{f};g = f$. A map f in a restriction category is **total** if $\overline{f} = 1$. Denote the subcategory of total maps of $\mathbb{X}$ by $\mathsf{Total}(\mathbb{X})$. A map f in a restriction category is called a **partial isomorphism**, in case there exists a **partial inverse** g of f so that $f;g = \overline{f}$ and $g;f = \overline{g}$. Denote the category of partial isomorphisms of $\mathbb{X}$ by $\mathsf{Inv}(\mathbb{X})$.

Example 2.63. The category Par of sets and partial functions is a restriction category. Given a partial map $f : X \to Y$, the restriction acts as the identity on the domain of definition:

$$\overline{f}(x) := \begin{cases} x & \text{if } f(x) \text{ is defined} \\ \text{undefined} & \text{otherwise} \end{cases}$$

To augment restriction categories with copying, one must relax the definition of a Cartesian category:

Definition 2.64 ([CL07])**.** A restriction category has **binary restriction products**, when for all objects X and Y, there exists an object $X \times Y$ and total maps $X \xleftarrow{\pi_0} X \times Y \xrightarrow{\pi_1} Y$, so that for all objects Z and all maps $X \xleftarrow{f} Z \xrightarrow{g} Y$, there exists a unique $Z \xrightarrow{\langle f,g\rangle} X \times Y$ making the diagram commute:

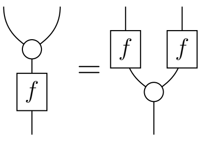
$$\begin{tikzcd}
& Z \arrow[ld, bend right, "f"'] \arrow[rd, bend left, "g"] \arrow[d, dashed, "{\langle f,g\rangle}"] & \\
X \arrow[r, phantom, "\geq", near end, shift left=3] & X \times Y \arrow[l, "\pi_0"] \arrow[r, "\pi_1"'] \arrow[r, phantom, "\leq", near start, shift left=3] & Y
\end{tikzcd}$$

so that $\overline{\langle f,g\rangle;\pi_0};f = \langle f,g\rangle;\pi_0$ and $\overline{\langle f,g\rangle;\pi_1};g = \langle f,g\rangle;\pi_1$ where additionally $\overline{\langle f,g\rangle} = \overline{f};\overline{g}$.

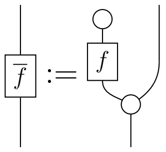
A restriction category has a **restriction terminal object** $\mathbb{1}$ when for all objects X, there exists a unique total map $!_X : X \to \mathbb{1}$ such that $f;!_Y = \overline{f};!_X$. A restriction category with a restriction terminal object and binary restriction products is a **Cartesian restriction category**. An object X in a restriction category with restriction products is **discrete** when the diagonal map $\Delta_X := \langle 1_X, 1_X\rangle$ is a partial isomorphism. A restriction category is discrete when all objects are discrete.

Example 2.65. Par is a canonical example of a discrete Cartesian restriction category; the restriction product is given by the Cartesian product on underlying sets and the terminal object is the singleton set.

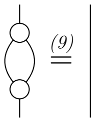
Theorem 2.66 ([CL07, Theorem 5.2])**.** *Cartesian restriction categories are in bijection with symmetric monoidal categories equipped with a supply of cocommutative comonoids* $\bigcirc$ *compatible with the tensor product, so that the multiplication is natural:*



The restriction is defined as follows:



This correspondence restricts to discrete Cartesian restriction categories when the multiplications have retracts ○:



which implies that these retracts are commutative semigroups, interacting with the multiplication to form non-unital Frobenius algebras.

We recall the following definition from Cockett and Lack, which was originally stated in the more general setting of categories with stable systems of monics, rather than finitely complete categories [CL02, Section 3]:

Definition 2.67. Given a finitely complete category $\mathbb{X}$, there is a discrete Cartesian restriction category, the **category of partial maps**, $\mathsf{Par}(\mathbb{X})$ is generated by spans (m, A, f), for m a monic and f and arbitrary map, i.e. spans of the form $X \overset{m}{\leftarrowtail} A \xrightarrow{f} Y$.

$\mathsf{Par}(\mathbb{X})$ is a discrete Cartesian restriction category where the natural monoid structure is given by spans of the form $X = X \overset{\Delta_X}{\rightarrowtail} X \times X$.

Its partial inverse is given by the span $X \times X \overset{\Delta_X}{\leftarrowtail} X = X$.

And the counit is given by $X = X \overset{!_X}{\twoheadrightarrow} \mathbb{1}$.

The basic idea is that the left leg picks out the domain of definition. Unrolling the definition, we see that a map $X \overset{m}{\leftarrowtail} A \xrightarrow{f} Y$ has a partial inverse precisely when f is a monomorphism; moreover, the restriction idempotents are spans where both legs are the same monomorphism: $X \overset{m}{\leftarrowtail} A \overset{m}{\rightarrowtail} Y$. This agrees with our running example of a restriction category:

Example 2.68. $\mathsf{Par} \cong \mathsf{Par}(\mathsf{Set})$

Full subcategories of Par are also restriction categories. Therefore, in such a setting the domain of definition need not be an actual object in the category of partial maps. In such a case the restriction idempotent $X \xrightarrow{e} X$ is regarded as a **subobject** of X. Despite not properly being an object, e is morally one. We discuss how subobjects can be promoted to objects in Definition 3.5.

Cartesian restriction categories are the partial version of Cartesian categories:

Lemma 2.69. *If $\mathbb{X}$ is a Cartesian restriction category, then $\mathsf{Total}(\mathbb{X})$ is Cartesian.*

Proof. By definition, the total maps in a Cartesian restriction category are those which are natural with respect to the counits. Moreover, all maps are already natural with respect to the diagonal maps. ☐

Similarly, discrete Cartesian restriction categories are a deterministic, yet partial version of relations:

Lemma 2.70. *The category of comultiplication homorphisms of a Cartesian bicategory of relations forms a discrete Cartesian restriction category.*

Let us refine the notion of a restriction category:

Definition 2.71 ([CL02, Section 2.3.2])**.** An **inverse category** is a restriction category in which all maps are partial isomorphisms.

Example 2.72. $\mathsf{Inv}(\mathsf{Par}) \cong \mathsf{Pinj}$

Inverse categories are particular kinds of †-categories:

Theorem 2.73 ([CL02, Theorem 2.20])**.** *A restriction category $\mathbb{X}$ is an inverse category if and only if there is a dagger functor $(-)^\circ : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$ such that for all $X \overset{f}{\leftarrow} Z \overset{g}{\rightarrow} Y$:*

[INV.1] $f; f^\circ; f = f$ **[INV.2]** $f; f^\circ; g; g^\circ = g; g^\circ; f; f^\circ$

The dagger functor takes maps to their partial inverse. In particular, the unitary maps in an inverse category are the total maps.

Sets and partial injections are intimately related to Hilbert spaces. The following functor was first discovered by Barr [Bar92]; later studied in much more detail by Heunen [Heu13]:

Definition 2.74. There is a †-symmetric monoidal embedding $\ell^2 : \mathsf{Pinj} \to \mathsf{Hilb}$:

Objects: Sets X are taken to the Hilbert space of square-summable functions on X:

$$\ell^2(X) := \left\{ \varphi : X \to \mathbb{C} \mid \sum_{x \in X} |\varphi(x)|^2 < \infty \right\}$$

Maps: Given a partial injection $f = X \overset{f_0}{\leftarrowtail} A \overset{f_1}{\rightarrowtail} Z$ and some $\varphi : X \to \mathbb{C}$ in $\ell^2(X)$:

$$(\ell^2(f)(\varphi))(y) = \sum_{x \in f_1^{-1}(y)} \varphi(f_0(x))$$

the partial inverse is mapped to the Hermitian adjoint.

In particular, $\ell^2(X)$ has a distinguished orthonormal basis given by

$$\{\delta_x : X \to \mathbb{C} \mid \forall x \in X\}$$

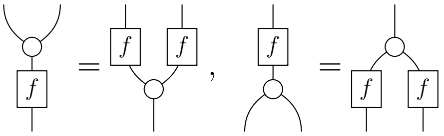
where δ_x is the Dirac delta at X:

$$\delta_x(y) \mapsto \begin{cases} 1 & \textit{if}\ \text{x=y} \\ 0 & \textit{otherwise} \end{cases}$$

The category of partial injections is unusual in the sense that it embeds into Hilb. This does not generalize to spans between sets, for example: the maps are no longer sent to bounded linear maps. However, if the domain is changed to the category of spans of *finite* sets this induces an embedding into FHilb. This is actually the version we will use throughout this thesis, but we give the general definition to highlight the importance of inverse categories in the categorical semantics of quantum mechanics.

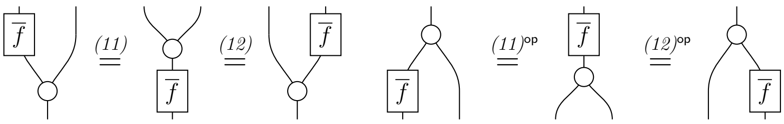
We also have a deterministic partially invertible notion of copying:

Definition 2.75 ([Gil14, Definition 4.3.1])**.** A symmetric monoidal inverse category $\mathbb{X}$ is a **discrete inverse category** when it is a dagger symmetric monoidal category, equipped with a commutative multiplication and cocommutative comultiplication ○ which are daggers of each other and interact via the special Frobenius laws which are natural so that:



Discrete inverse categories are inverse categories with respect to the dagger.

Lemma 2.76 ([Gil14, Lemma 4.3.5])**.** *The restriction idempotents are strengths for the multiplication and comultiplication so that:*



Lemma 2.77. *Given a finitely complete category* $\mathbb{X}$*, the category* $\mathsf{ParIso}(\mathbb{X}) := \mathsf{Inv}(\mathsf{Par}(\mathbb{X}))$ *of spans of monomorphisms in* $\mathbb{X}$ *is a discrete inverse category.*

These weaken the notion of copying even further:

Lemma 2.78 ([Gil14, Proposition 4.3.7])**.** *Given a discrete Cartesian restriction category* $\mathbb{X}$*,* $\mathsf{Inv}(\mathbb{X})$ *is a discrete inverse category.*

At least as far as the literature is concerned, the canonical way to obtain a discrete Cartesian restriction category from a discrete category is more difficult. We will first introduce the more general CoPara construction, which freely adds an effect to every object in a way that is compatible with the tensor product:

Definition 2.79. Given a symmetric monoidal category $\mathbb{X}$, the CoPara construction, $\mathsf{CoPara}(\mathbb{X})$ is the symmetric monoidal category obtained by freely adding maps $X \to I$ for every object X, compatible with the tensor unit:

Objects: Same as in $\mathbb{X}$.

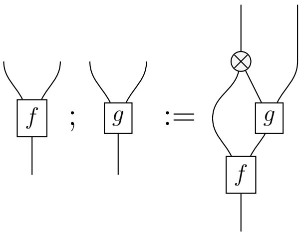
Maps:

$$\frac{X \xrightarrow{f} S \otimes Y \in \mathbb{X}}{X \xrightarrow{(f,S)} Y \in \mathsf{CoPara}(\mathbb{X})}$$

Composition:

$$\frac{X \xrightarrow{(f,S)} Y, \quad Y \xrightarrow{(g,T)} Z}{X \xrightarrow{(f,S);(g;T):=(f;(1_S\otimes g);\alpha^{-1}_{S,T,Z},S\otimes T)} Z}$$

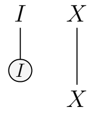
Or in string diagrams:



Identity:

$$\frac{1_X \in \mathsf{CoPara}(\mathbb{X})}{(u^L_X)^{-1} \in \mathbb{X}}$$

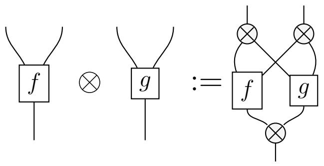
Or in string diagrams:



Tensor product:

$$\frac{X \xrightarrow{(f,S)} Y \;, \qquad Z \xrightarrow{(g,T)} W}{X \otimes Z \xrightarrow{(f,S)\otimes(g;T):=(f\otimes g);\alpha^{-1}_{S\otimes Y,T,W};\alpha_{S,Y,T}\otimes 1_W;(1_S\otimes\sigma_{Y,T})\otimes 1_W;\alpha^{-1}_{S,T,Y}\otimes 1_W;\alpha_{S\otimes T,Y,W}} Y \otimes W}$$

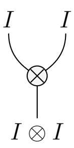
Or in string diagrams:



Tensor unit:

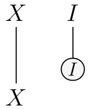
$$\frac{I \in \mathsf{CoPara}(\mathbb{X})}{1_{I\otimes I} \in \mathbb{X}}$$

Or in string diagrams:



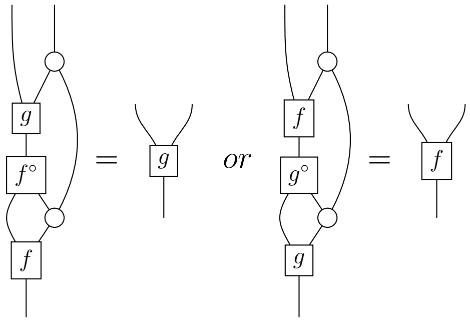
The coherence data for the monoidal structure is inherited in a straightforward way from $\mathbb{X}$. Moreover, if $\mathbb{X}$ is symmetric monoidal, then it is easy to see how $\mathsf{CoPara}(\mathbb{X})$

is as well. In other words $\mathsf{CoPara}(\mathbb{X})$ could have alternatively been presented by freely adding generators $d_X : X \to I$ to the monoidal theory of the strictification of $\mathbb{X}$, for every object in $\mathbb{X}$ compatible with the monoidal structure. In $\mathsf{CoPara}(\mathbb{X})$ the map d_X corresponds to the inverse left unitor $(u_X^L)^{-1}$:

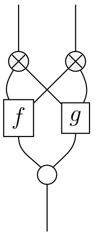
$d_X :=$ 

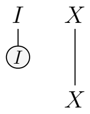
Variations on this theme will occur throughout this thesis, so we have promoted it to its own construction. For reference, the CoPara construction is dual to the Para construction which is interpreted as freely adding parameters to a monoidal category (see [FST19]). This allows us to define the following:

Definition 2.80 ([Gil14, Definition 5.1.1])**.** Given a discrete inverse category $\mathbb{X}$, its **Cartesian completion** $\widetilde{\mathbb{X}}$ is the quotient of $\mathsf{CoPara}(\mathbb{X})$ by either of the following equivalent symmetric monoidal congruence relations:

$(f, S) \sim (g, T) \iff$ 

$\widetilde{\mathbb{X}}$ has the structure of a discrete Cartesian restriction category with:

Restriction product: $\langle f, g \rangle :=$ 

Restriction terminal map: 

We give a simpler characterization of this construction terms of adding counits to the inverse products in Proposition 4.5.

Theorem 2.81 ([Gil14, Theorem 5.2.6])**.** *There is an equivalence of categories between the category of discrete inverse categories and the category of discrete Cartesian categories.*

This equivalence is witnessed on the one hand by the Cartesian completion and on the other by taking the wide subcategory of partial isomorphisms. As a corollary, we see that

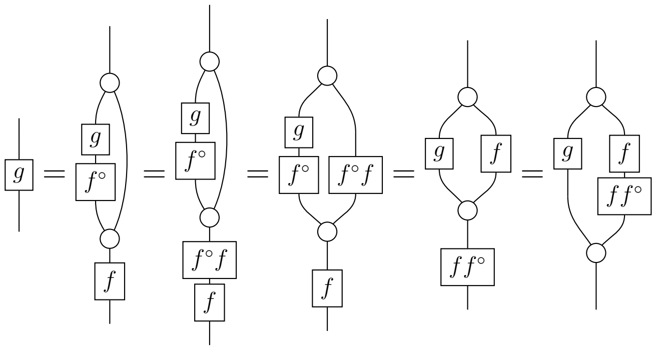
Example 2.82 ([Gil14, Example 5.3.3])**.** $\widetilde{\mathsf{Pinj}}$ is Par.

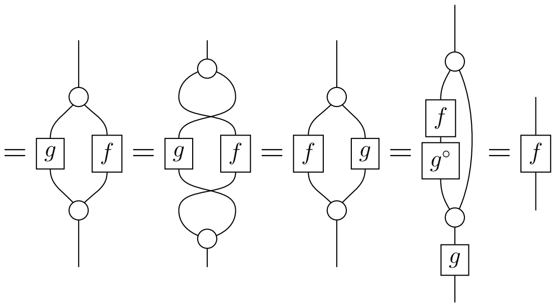
Proof. For a partial function $f : X \to Y$, $\{(x,(x,y))|(x,y) \in f\}/\sim$ is a partial isomorphism. ☐

The Cartesian completion is itself an embedding:

Lemma 2.83. *The canonical functor* $\iota : \mathbb{X} \to \widetilde{\mathbb{X}}$ *is faithful.*

Proof. Suppose that $\iota(f) \sim \iota(g)$, Then:





☐

Obtaining Cartesian bicategories of relations from discrete inverse categories is more difficult. We will discuss this later in Section 4.1. Let us summarize the various notions of weakenings of Cartesian bicategories of relations in a table:

	Δ	!	Δ^*	$!^*$
Discrete inverse category	nat		nat	
Discrete Cartesian restriction category	nat	lax	lax	
Cartesian category	nat	nat		
Cartesian bicategory of relations	lax	lax	lax	lax

2.3 (De)composing props

In this section we review some aspects of internal category theory so that we can compose props via distributive law. It is not necessary to read this section to understand most of this thesis, with the exception of Section 4.3.

One way to combine monoidal theories is via pushout. We generalize the analogous result of Zanasi to the coloured setting [Zan18, Proposition 2.51]:

Lemma 2.84. *Take three (symmetric) monoidal theories*

$$T_0 = (\mathsf{Ob}_0, \Sigma_0, E_0),\ T_1 = (\mathsf{Ob}_1, \Sigma_1, E_1),\ T_2 = (\mathsf{Ob}_2, \Sigma_2, E_2)$$

such that $\mathsf{Ob}_0 \subseteq \mathsf{Ob}_1, \mathsf{Ob}_2$*,* $\Sigma_0 \subseteq \Sigma_1, \Sigma_2$ *and* $E_0 \subseteq E_1, E_2$*. Then the pushout of the diagram* $\overline{T_1} \leftarrow \overline{T_0} \rightarrow \overline{T_2}$ *in the category of strict (symmetric) monoidal categories is presented by the (symmetric) monoidal theory:*

$$(\mathsf{Ob}_1 +_{\mathsf{Ob}_0} \mathsf{Ob}_2, \Sigma_1 +_{\Sigma_0} \Sigma_2, E_1 +_{E_0} E_2)$$

In practice, we usually won't be so explicit about the pushout of (symmetric) monoidal theories. Rather, we will present a set of generators and multiple equations between different subsets of generators. Indeed, we have done this many times up to this point when glueing (symmetric) monoidal theories together.

In the case when we want to identify the pushout of props with the pushout of their semantics we must be more careful. Take three coloured pro(p)s $\overline{T_0}, \overline{T_1}$ and $\overline{T_2}$ as above which are respectively presentations for (symmetric) monoidal categories $\mathbb{X}_0, \mathbb{X}_1$ and $\mathbb{X}_2$. In order for the pushout of the diagram of pro(p)s $\overline{T_1} +_{\overline{T_0}} \overline{T_2}$ as described above to be a presentation for the pushout of (symmetric) monoidal categories $\mathbb{X}_1 +_{\mathbb{X}_0} \mathbb{X}_2$, we must show that the universal map u induced by the pushout of the diagram $\mathbb{X}_1 \leftarrow \mathbb{X}_0 \rightarrow \mathbb{X}_2$ is inverse to the universal map v induced by the pushout of the diagram $\overline{T_1} +_{\overline{T_0}} \overline{T_2}$. That is to say, we ask for the following diagram of (symmetric) monoidal categories to commute:

$$\begin{tikzcd}
 & \overline{T_0} \arrow[rr] \arrow[dl] \arrow[dd, bend left] & & \overline{T_1} \arrow[dl] \arrow[dd, bend left] \\
\overline{T_2} \arrow[rr] \arrow[dd, bend left] & & \overline{T_1} +_{\overline{T_0}} \overline{T_2} \arrow[dd, bend left, "u"] & \\
 & \mathbb{X}_0 \arrow[rr] \arrow[dl] \arrow[uu, bend left] & & \mathbb{X}_1 \arrow[dl] \arrow[uu, bend left] \\
\mathbb{X}_2 \arrow[rr] \arrow[uu, bend left] & & \mathbb{X}_1 +_{\mathbb{X}_0} \mathbb{X}_2 \arrow[uu, bend left, "v"] &
\end{tikzcd}$$

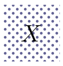
This method of pushout cubes is used extensively in Zanasi's thesis [Zan18]; and we will make heavy use of it in Section 4.3.

However, there is a more refined notion of composition of pro(p)s; to expose which, we first need to review a considerable amount of internal category theory.

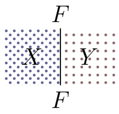
2.3.1 Internal categories and strict factorization systems

In this subsection we will make extensive use of bicategories. Just like monoidal categories, every bicategory is equivalent to a strict 2-category where the unitors and associators are identities. We have already been working with a strict 2-category throughout this thesis: the 2-category of categories, functors and natural transformations (as well as its various monoidal cousins). We have also already encountered a (nonstrict) bicategory, that of spans internal to a category.

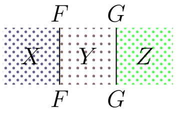
Strict 2-categories have a graphical calculus much like strict monoidal categories, except for the fact that the empty space between wires is now coloured by the 0-cells. For example a 0-cell X is drawn as a surface:



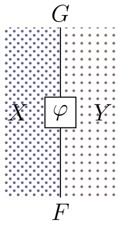
A 1-cell $F : X \to Y$ is drawn as a wire separating two surfaces:



The composition of two 1-cells $X \xrightarrow{F} Y \xrightarrow{G} Z$ is drawn as follows:



And a 2-cell $\varphi : F \Rightarrow G$ is drawn as a node between wires:



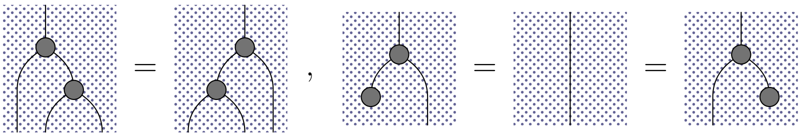
We1 won't go into full detail, but one can imagine how to compose things in both directions as in the monoidal setting. We will omit the labels when they are clear from context, as we have done for monoidal categories. For the rest of this section we will work exploit the coherence theorem and work in the setting of strict 2-categories. This notation shows how the following constructions are canonical:

Definition 2.85 ([Str72, Section 1]). Given a bicategory $\mathcal{B}$, there is a bicategory of monads in $\mathcal{B}$, $\mathsf{Mnd}(\mathcal{B})$ with:

0-cells: Monads are tuples (X, T, μ, η) in $\mathcal{B}$, where X is a 0-cell $T : X \to X$ is a 1-cell, and $\mu : T^2 \to T$ and $\eta : 1_X \to T$ are 2-cells satisfying the associativity and unit laws:

$$\begin{tikzcd}
T^3 \arrow[r, "T;\mu"] \arrow[d, "\mu;T"'] & T^2 \arrow[d, "\mu"] \\
T^2 \arrow[r, "\mu"'] & T
\end{tikzcd}
\qquad
\begin{tikzcd}
T \arrow[r, "\eta;T"] \arrow[d, "T;\eta"'] \arrow[dr, equal] & T^2 \arrow[d, "\mu"] \\
T^2 \arrow[r, "\mu"'] & T
\end{tikzcd}$$

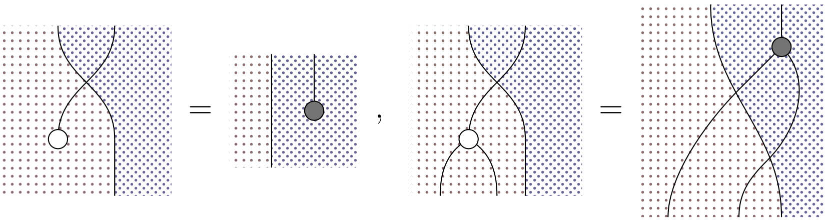
Graphically if we draw T as ●, then



1-cells: Monad maps $(F, \lambda) : (X, T, \mu^T, \eta^T) \to (Y, S, \mu^S, \eta^S)$, where $F : X \to Y$ is a 1-cell and $\lambda : S; F \to F; T$ is a 2-cell preserving the unit and multiplication as follows:

$$\begin{tikzcd}
F \arrow[r, "\eta^S;F"] \arrow[dr, "F;\eta^T"'] & S;F \arrow[d, "\lambda"] \\
& F;T
\end{tikzcd}
\qquad
\begin{tikzcd}
S^2;F \arrow[r, "S;\lambda"] \arrow[d, "\mu^S;F"'] & S;F;T \arrow[r, "\lambda;T"] & F;T^2 \arrow[d, "F;\mu^T"] \\
S;F \arrow[rr, "\lambda"'] & & F;T
\end{tikzcd}$$

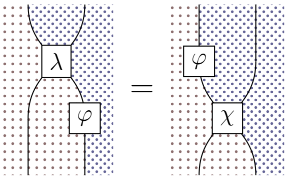
Graphically if we draw S as ○ and T as ● and λ as a crossing, then



2-cells: Intertwiners between monad maps $(F, \lambda) \to (G; \chi)$ are 2-cells $\varphi : F \to G$ such that:

$$\begin{tikzcd}
S;F \arrow[r, "S;\varphi"] \arrow[d, "\lambda"'] & S;G \arrow[d, "\chi"] \\
F;T \arrow[r, "\varphi;T"'] & G;T
\end{tikzcd}$$

Graphically:



Definition 2.86. Given a category $\mathcal{V}$ with finite pullbacks $\mathcal{V}$, a **$\mathcal{V}$-internal category** is a monad in $\mathsf{Span}(\mathcal{V})$.

Example 2.87. Monads internal to $\mathsf{Span}(\mathsf{Set})$ are in bijection with small categories.

Let us upack this a bit. A small category has a *set* Ob of objects, and a *set* Ar of maps. There is a map $\mathsf{dom} : \mathsf{Ar} \to \mathsf{Ob}$ which picks out the domain of maps and another map $\mathsf{codom} : \mathsf{Ar} \to \mathsf{Ob}$ picking out the codomain. That is to say, a span of sets:

$$S = \begin{tikzcd} & \mathsf{Ar} \arrow[dl, "\mathsf{dom}"'] \arrow[dr, "\mathsf{codom}"] & \\ \mathsf{Ob} & & \mathsf{Ob} \end{tikzcd}$$

Composition of maps is a function which takes maps $f : X \to Y$ and $g : Y \to Z$ to a new map $(f; g) : X \to Z$. This is asking for a 2-cell $\mu : S^2 \to S$ in $\mathsf{Span}(\mathsf{Set})$; the pullback picks out the composable maps and composes them. The associativity of composition corresponds to the associativity of μ as a semigroup. On the other hand, the unit of a small category is a function from Ob to S, picking out for every object X, a map 1_X with domain and codomain X, that is to say, a 2-cell $\mu : 1_{\mathsf{Ob}} \to S$. The unitality of composition is the unitality of the monad.

One should be careful to notice that the 1-cells in $\mathsf{Mnd}(\mathsf{Span}(\mathsf{Set}))$ do not correspond to functors between small categories. This structure naturally arizes by considering the analogous *double category*; however, this is out of scope for this thesis.

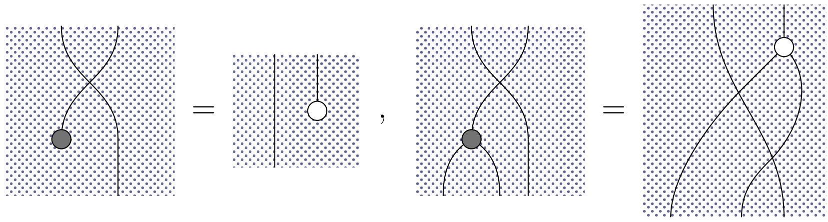
There is a canonical way to compose monads, and thus small categories:

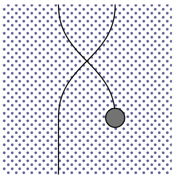
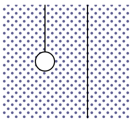
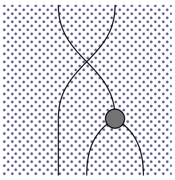
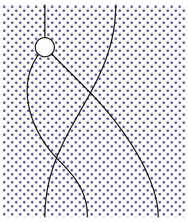
Definition 2.88. Given two monads $\mathbb{L} = (X, L, \mu^L, \eta^L)$ and $\mathbb{R} = (X, R, \mu^R, \eta^R)$ in a bicategory $\mathcal{B}$, a distributive law of R over L is a 2-cell $\lambda : R; L \to L; R$ in $\mathcal{B}$ satisfying the following coherence equations:

$$\begin{tikzcd} R \arrow[d, "\eta^L;R"'] \arrow[dr, "R;\eta^L"] & \\ L;R \arrow[r, "\lambda"'] & R;L \end{tikzcd} \qquad \begin{tikzcd} L^2;R \arrow[r, "L;\lambda"] \arrow[d, "\mu^L;R"'] & L;R;L \arrow[r, "\lambda;L"] & R;L;L \arrow[d, "R;\mu^L"] \\ L;R \arrow[rr, "\lambda"'] & & R;L \end{tikzcd}$$

$$\begin{tikzcd} R \arrow[d, "L;\eta^R"'] \arrow[dr, "\eta^R;L"] & \\ L;R \arrow[r, "\lambda"'] & R;L \end{tikzcd} \qquad \begin{tikzcd} L;R^2 \arrow[r, "\lambda;R"] \arrow[d, "L;\mu^R"'] & R;L;R \arrow[r, "R;\lambda"] & R;R;L \arrow[d, "\mu^R;L"] \\ L;R \arrow[rr, "\lambda"'] & & R;L \end{tikzcd}$$

Graphically where we draw λ as a crossing, R as ● and L as ○, we have




=

,

=


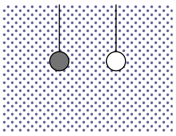
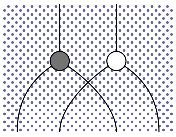
Distributive laws of monads induce composite monads:

Lemma 2.89. *Given a distributive law of monads $\lambda : R; L \to L; R$, the 1-cell $L; R$ has a monad structure with:*

unit: $\eta^{L;R} := 1_X \xrightarrow{\eta^L;\eta^R} L; R$

multiplication: $\mu^{L;R} := (L; R)^2 \xrightarrow{1_X;\lambda;1_X} L; L; R; R \xrightarrow{\mu^L;\mu^R} L; R$

Graphically:

$\eta^{L;R} =$

, $\mu^{L;R} =$


There is a concise way of viewing distributive laws:

Lemma 2.90 ([Str72, Section 6])**.** *Distributive laws of monads in a bicategory $\mathcal{B}$ are precisely monads in $\mathsf{Mnd}(\mathcal{B})$.*

The following notion allows one to factorize the maps in categories:

Definition 2.91 ([Gra00, Section 6.2])**.** A **strict factorization system** on a category $\mathbb{X}$ is a pair of subcategories $(\mathbb{L}, \mathbb{R})$ of $\mathbb{X}$ with the same objects as $\mathbb{X}$, such that every map in $\mathbb{X}$ can be uniquely factored into a map in $\mathbb{L}$ followed by a map in $\mathbb{R}$.

That is to say every map $f : X \to Y$ factorizes as follows

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\ell\in\mathbb{L}"'] & & Y \\ & A \arrow[ur, "r\in\mathbb{R}"'] & \end{tikzcd}$$

such that given another such factorization

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\ell'\in\mathbb{L}"'] & & Y \\ & A' \arrow[ur, "r'\in\mathbb{R}"'] & \end{tikzcd}$$

then the following diagram commutes:

$$\begin{tikzcd} X \arrow[r, "\ell"] \arrow[d, equal] & A \arrow[r, "r"] \arrow[d, equal] & Y \arrow[d, equal] \\ X \arrow[r, "\ell'"'] & A' \arrow[r, "r'"'] & Y \end{tikzcd}$$

Lemma 2.92 ([RW02, Theorem 3.8])**.** *Strict factorization systems of small categories* $(\mathbb{L}, \mathbb{R})$ *are precisely distributive laws of* $\mathbb{R}$ *over* $\mathbb{L}$ *regarded as monads in* $\mathsf{Span}(\mathsf{Set})$*.*

Therefore, a distributive law of small categories can be regarded as a way to uniquely factorize maps in $\mathbb{X}$ into two disjoint subcategories $\mathbb{L}; \mathbb{R}$; so that if a composite is out of order, there is a rule $\mathbb{L}; \mathbb{R} \to \mathbb{R}; \mathbb{L}$ to push them past each other uniquely.

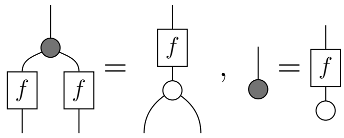
By changing Set to the category of monoids, Lack observed that one can recover the appropriate notion of a strict factorization system of pros [Lac04]. First recall the category of monoids:

Definition 2.93. Let Mon denote the category with set-monoids as objects and monoid homorphisms as morphisms. Recall:

A set monoid: is a monoid (X, m, e) in Set under the Cartesian product.

A monoid homorphism: $(X, m, e) \to (Y, m', e')$ is a function $f : X \to Y$ such that $f(m(x, y)) = m'(f(x), f(y))$ and $f(e) = e'$.

Drawing (X, m, e) as ○ and (Y, m', e') as ● that is:



Mon has finite pullbacks, so one can define categories within it. We already have introduced these categories in other terms:

Lemma 2.94 ([Lac04, Section 2.3])**.** *Monads in* $\mathsf{Span}(\mathsf{Mon})$ *are in bijection with small strict monoidal categories.*

There is an obvious analogue of strict factorizations for small strict monoidal categories, which we shall call monoidal strict factorization systems. In this setting $\mathbb{L}$ and $\mathbb{R}$ are small strict monoidal subcategories of $\mathbb{X}$. Therefore, reproducing Lemma 2.92 internal to Mon we have:

Lemma 2.95 ([Lac04, Theorem 3.8])**.** *Monoidal strict factorization systems of small categories* $(\mathbb{L}, \mathbb{R})$ *are precisely distributive laws of* $\mathbb{R}$ *over* $\mathbb{L}$*, viewed as monads in* $\mathsf{Span}(\mathsf{Mon})$*.*

Distributive laws of monoidal theories yield a monoidal theory for the composite internal monoidal category. The two theories are combined, plus rules to push the generators past each other. This follows immediately from the analysis of distributive laws of props of Lack [Lac04, Theorem 3.8], where a prop is a strict monoidal category regarded as a monad on $\mathbb{N}$ in $\mathsf{Span}(\mathsf{Mon})$.

Lemma 2.96. *Take two monoidal theories*

$$R = (\mathsf{Ob}, \Sigma_R, E_R),\ L = (\mathsf{Ob}, \Sigma_L, E_L)$$

with the same objects. Regard their corresponding pros $\overline{R}$ *and* $\overline{L}$ *as monads in* $\mathsf{Span}(\mathsf{Mon})$ *such that there is a distributive law* $\lambda : \overline{R};\overline{L} \Rightarrow \overline{L};\overline{R}$*, where* $\overline{L};\overline{R}$ *is a strict monoidal category and both* $\overline{L}$ *and* $\overline{R}$ *are strict monoidal subcategories of* $\overline{L};\overline{R}$

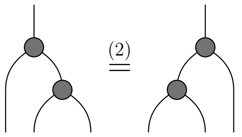
Then the monoidal theory for the composite pro $\overline{L};\overline{R}$ *is given by*

$$(\mathsf{Ob}, \Sigma_R \cup \Sigma_L, E_R \cup E_L \cup E_\lambda)$$

where λ *is the set of equations dictating the unique ways in which the generators in* R *can be pushed past those in* L*.*

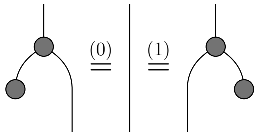
Example 2.97 ([Lac04, Example 3.13])**.** Let injmonot be the pro generated by a single generator $0 \to 1$ and no equations:

And let surjmonot denote the pro generated by a semigroup:



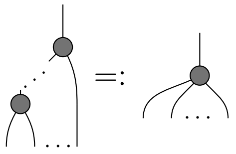
injmonot is a presentation for the monotone injections and surjmonot the monotone surjections in FinOrdMonot. The distributive law

injmonot; surjmonot;



is a presentation for FinOrdMonot. This corresponds to the strict factorization system coming from the epi-mono factorization of FinOrdMonot $\cong$ m (see Lemma 2.49).

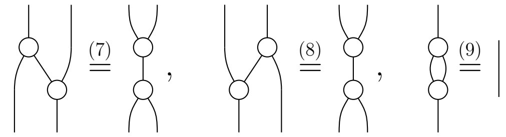
The strict factorization system gives us a unique normal form. We can therefore draw the unique connected components of the same arity as follows:



The prop sfa also arizes in terms of a distributive law of pros:

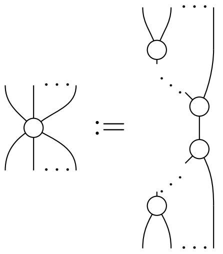
Example 2.98. Consider the distributive law of pros of a comonoid ○ over a monoid ○:

$\mathsf{m};\mathsf{m}^{\mathsf{op}};$

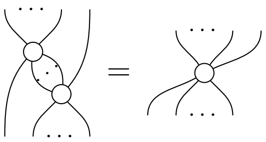


which we recall is the pro sfa for the free special Frobenius algebra. The unique normal form induced by this distributive will be widely used throughout this thesis:

Lemma 2.99 (Non-commutative special spider normal form)**.** *The circuits in* sfa *generated by the connected components of the Frobenius algebra have a unique normal form. We use the "spider notation" on the left to refer to these simply connected components:*

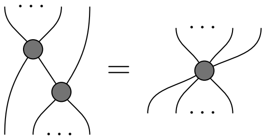


Because the connected circuits are reducible to each other, spiders connected by wires fuse:



We will also use the following related result:

Lemma 2.100 (Non-commutative spider normal form)**.** *In the case of the prop* fa *when the Frobenius algebra is not special, then the spider theorem only holds for simply connected circuits. For example, given a Frobenius algebra* ●*:*



This does not arise from a distributive law of pros, but it holds nevertheless.

2.3.2 Factorization systems over subcategories

We want to be able to take distributive laws of two categories which both share some structure. For example, what is the appropriate notion of distributive law of small strict symmetric monoidal categories where the symmetry maps of both categories are identified with each other? For this, we can regard the shared structure in the subcategory as actions on the larger categories; formally, this is a certain kind of bimodule:

Definition 2.101. Given a bicategory $\mathcal{B}$ with coequalizers, the bicategory of bimodules in $\mathcal{B}$, $\mathsf{Mod}(\mathcal{B})$ has:

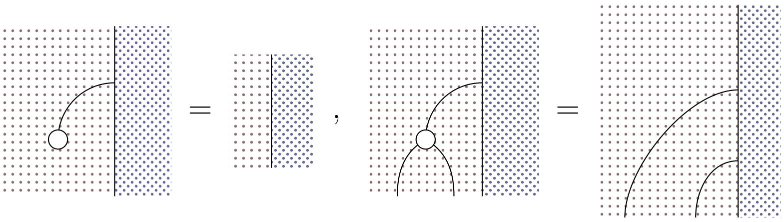
0-cells: Monads in $\mathcal{B}$.

1-cells: A 1-cell between monads $\mathbb{T} = (X, T, \mu^T, \eta^T) \to \mathbb{S} = (Y, S, \mu^S, \eta^S)$ is a $(\mathbb{T}, \mathbb{S})$-**bimodule**. That is a triple (F, τ, ρ) where $F : X \to Y$ is a 1-cell in $\mathcal{B}$ and $\tau : S; F \to F$ and $\rho : F; T \to F$ are 2-cells (the left and right **actions**, respectively) satisfying the following coherence equations:

(F, τ) **is a left $\mathbb{S}$-module:**

$$\begin{tikzcd} F \arrow[d, "\eta^S;F"'] \arrow[dr, equal] & \\ S;F \arrow[r, "\tau"'] & F \end{tikzcd} , \qquad \begin{tikzcd} S;S;F \arrow[r, "\mu^S;F"] \arrow[d, "S;\tau"'] & S;F \arrow[d, "\tau"] \\ S;F \arrow[r, "\tau"'] & F \end{tikzcd}$$

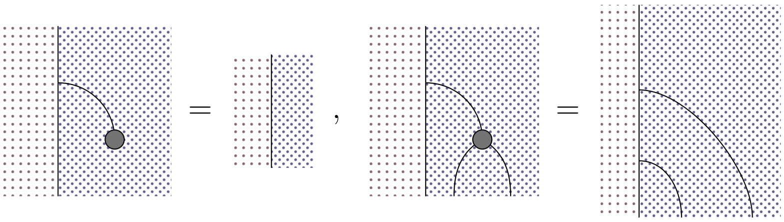
Graphically:



(F, ρ) **is a right $\mathbb{S}$-module:**

$$\begin{tikzcd} F \arrow[d, "F;\eta^T"'] \arrow[dr, equal] & \\ F;T \arrow[r, "\rho"'] & F \end{tikzcd} , \qquad \begin{tikzcd} F;T;T \arrow[r, "F;\mu^T"] \arrow[d, "\rho;T"'] & F;T \arrow[d, "\rho"] \\ F;T \arrow[r, "\rho"'] & F \end{tikzcd}$$

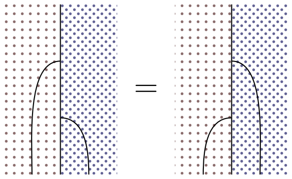
Graphically:



Module compatibility:

$$\begin{tikzcd} S;F;T \arrow[r, "S;\rho"] \arrow[d, "\tau;T"'] & S;F \arrow[d, "\tau"] \\ F;T \arrow[r, "\rho"'] & F \end{tikzcd}$$

Graphically:



Given a $(\mathbb{S},\mathbb{T})$-bimodule (F,τ,ρ) and a $(\mathbb{T},\mathbb{U})$-bimodule (G,τ',ρ'), the composite has 1-cell given by the coequalizer:

$$\begin{tikzcd}
F;T;G \arrow[r, shift left, "\tau';G"] \arrow[r, shift right, "F;\rho"'] & F;G \arrow[r, two heads] & F \otimes_T G
\end{tikzcd}$$

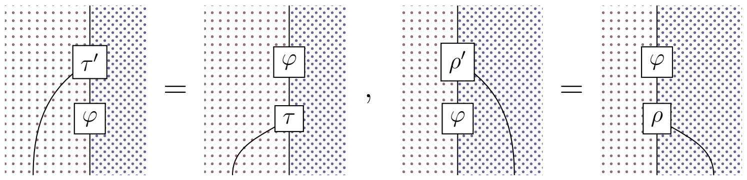
with left and right actions induced by τ and ρ'.

The identity 1-cell on a monad is the monad regarded as a bimodule over itself.

2-cells: A 2-cell between $(\mathbb{S},\mathbb{T})$-bimodules $(F,\tau,\rho) \to (G,\tau',\rho')$ is a 2-cell $\varphi : F \to G$ in $\mathcal{B}$ satisfying the following coherence conditions:

$$\begin{tikzcd}
S;F \arrow[r, "\tau"] \arrow[d, "S;\varphi"'] & F \arrow[d, "\varphi"] & F;T \arrow[r, "\rho"] \arrow[d, "\varphi;T"'] & F \arrow[d, "\varphi"] \\
S;G \arrow[r, "\tau'"'] & G & G;T \arrow[r, "\rho'"'] & G
\end{tikzcd}$$

Graphically:



Composition and identities are given pointwise in $\mathcal{B}$.

Now we can look at modules of internal categories:

Definition 2.102. Given a category $\mathcal{V}$ with finite pullbacks and coequalizers preserving them, let $\mathcal{V}$-$\mathsf{Prof} := \mathsf{Mod}(\mathsf{Span}(\mathcal{V}))^{\mathsf{op}}$ denote the bicategory of **$\mathcal{V}$-internal profunctors**. The 1-cells of $\mathcal{V}$-Prof are called (internal) **profunctors**. The tensor product of bimodules of internal categories is the (internal) **coend**.

We related distributive laws in internal categories to factorization systems. To do so we introduce the following notation:

Definition 2.103. Let $\mathsf{Iso}(\mathbb{X})$ denote the groupoid of all isomorphisms of $\mathbb{X}$.

There is a notion of factorization system where the factorization need only hold up to unique isomorphism:

Definition 2.104. An **orthogonal factorization system** on a category $\mathbb{X}$ is a pair of subcategories $(\mathbb{L},\mathbb{R})$ of $\mathbb{X}$ with the same objects as $\mathbb{X}$, where $\mathbb{L}$ and $\mathbb{R}$ contain all isomorphisms in $\mathbb{X}$, and moreover, where every map in $\mathbb{X}$ factors as a map in $\mathbb{L}$, followed by one in $\mathbb{R}$, up to unique isomorphism.

That is to say every map $f : X \to Y$ factorizes as follows

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\ell\in\mathbb{L}"'] & & Y \\
& A \arrow[ur, "r\in\mathbb{R}"'] &
\end{tikzcd}$$

such that given another such factorization

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\ell'\in\mathbb{L}"'] & & Y \\
& A' \arrow[ur, "r'\in\mathbb{R}"'] &
\end{tikzcd}$$

then there is a unique isomorphism $\varphi : A \to A'$ making the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "\ell"] \arrow[d, equal] & A \arrow[r, "r"] \arrow[d, dashed, "\varphi"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell'"'] & A' \arrow[r, "r'"'] & Y
\end{tikzcd}$$

This is the same as a distributive law of monads in $\mathsf{Set}\text{-}\mathsf{Prof}^{\mathsf{op}}$ over $\mathsf{Iso}(\mathbb{X})$:

Lemma 2.105 ([RW02, Theorem 5.9])**.** *An orthogonal factorization system* $(\mathbb{L},\mathbb{R})$ *on a small category* $\mathbb{X}$ *is precisely a distributive law of monads between* $\mathbb{L}$ *and* $\mathbb{R}$*, regarded as* $\mathsf{Iso}(\mathbb{X})$*-bimodules.*

We have already discussed two examples of orthogonal factorization systems in order to define categories of internal relations:

Example 2.106. Given a finitely complete category $\mathbb{X}$, the category $\mathsf{Span}^{\sim}(\mathbb{X})$ has an orthogonal factorization system where:

$$\mathbb{L} := \{\, Y \xleftarrow{f} X = X \;\mid \forall f \in \mathbb{X}(X,Y)\}\ ,\ \ \mathbb{R} := \{\, X = X \xrightarrow{f} Y \;\mid \forall f \in \mathbb{X}(X,Y)\}$$

Example 2.107. Regular categories have orthogonal factorization systems given by $\mathbb{L}$ the regular epimorphisms, and $\mathbb{R}$ the monomorphisms.

By asking that $\mathbb{X}$ is a small strict monoidal category and $\mathbb{L}$ and $\mathbb{R}$ are strict monoidal subcategories of $\mathbb{X}$, the notion of an orthogonal factorization system is adapted immediately to monoidal categories. And there is an analogous correspondence between $\mathbb{L}$ and $\mathbb{R}$, regarded as $\mathsf{Iso}(\mathbb{X})$-bimodules in $\mathsf{Span}(\mathsf{Mon})$. However, this is not satisfactory for our purposes.

In the most basic setting, the shared structure of small strict *symmetric* monoidal categories on the same set of objects is the permutations on the objects. Indeed, this is the basis of Lack's work on composing props [Lac04]. Factorizations up permutations are clearly not strict; and they are only an orthogonal factorization system when all isomorphisms are permutations. For our purposes, we will also need to consider cases when $\mathbb{J}$ is not even a groupoid! We will recall a considerably more general notion to this end:

Definition 2.108 ([Che20, Definition 4.10])**.** Let $\mathbb{X}$ be a category equipped with a subcategory $\mathbb{J}$ with the same objects. A **factorization system of $\mathbb{X}$ over $\mathbb{J}$** consists of a pair of subcategories $(\mathbb{L}, \mathbb{R})$ of $\mathbb{X}$ with the same objects as $\mathbb{X}$ such that $\mathbb{J}$ is a subcategory of both $\mathbb{L}$ and $\mathbb{R}$. And moreover, every map in $\mathbb{X}$ factorizes into maps in $\mathbb{L}$ followed by maps in $\mathbb{R}$ uniquely up to zig-zags in $\mathbb{J}$.

That is to say, given any map $f : X \to Y$ in $\mathbb{X}$, there is a factorization

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\ell \in \mathbb{L}"'] & & Y \\
& A \arrow[ur, "r \in \mathbb{R}"'] &
\end{tikzcd}$$

such that given another such factorization

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\ell' \in \mathbb{L}"'] & & Y \\
& A' \arrow[ur, "r' \in \mathbb{R}"'] &
\end{tikzcd}$$

then there exists factorizations:

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\ell_j \in \mathbb{L}"'] & & Y \\
& A_j \arrow[ur, "r_j \in \mathbb{R}"'] &
\end{tikzcd}$$

and maps in $\mathbb{J}$:

$$\begin{tikzcd}
A \arrow[r, "\varphi_0"] & A_0 & A_1 \arrow[l, "\varphi_1"'] \arrow[r, "\varphi_2"] & A_2 & A_3 \arrow[l, "\varphi_3"'] \arrow[r, "\varphi_4"] & \cdots & A_{n-1} \arrow[l, "\varphi_{n-1}"'] \arrow[r, "\varphi_n"] & A'
\end{tikzcd}$$

uniquely making following diagram commute:

$$\begin{tikzcd}
X \arrow[r, "\ell"] \arrow[d, equal] & A \arrow[r, "r"] \arrow[d, dashed, "\varphi_0"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell_0"] \arrow[d, equal] & A_0 \arrow[r, "r_0"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell_1"] \arrow[d, equal] & A_1 \arrow[r, "r_1"] \arrow[u, dashed, "\varphi_1"'] \arrow[d, dashed, "\varphi_2"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell_2"] \arrow[d, equal] & A_2 \arrow[r, "r_2"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell_3"] \arrow[d, equal] & A_3 \arrow[r, "r_3"] \arrow[u, dashed, "\varphi_3"'] \arrow[d, dashed, "\varphi_4"] & Y \arrow[d, equal] \\
\vdots \arrow[d, equal] & \vdots & \vdots \arrow[d, equal] \\
X \arrow[r, "\ell_{n-1}"] \arrow[d, equal] & A_{n-1} \arrow[r, "r_{n-1}"] \arrow[u, dashed, "\varphi_{n-1}"'] \arrow[d, dashed, "\varphi_n"] & Y \arrow[d, equal] \\
X \arrow[r, "\ell'"] & A' \arrow[r, "r'"] & Y
\end{tikzcd}$$

This specializes to strict factorization systems when $\mathbb{J}$ contains exactly the identities on all objects; and to orthogonal factorization systems when it contains all isomorphisms. Suppose that $\mathbb{J}$ is not a groupoid and we tried to replace the definition of an orthogonal factorization system $(\mathbb{L}, \mathbb{R})$ with one where the unique mediating map is merely a single map in $\mathbb{J}$. Now suppose we want to reduce a map in the composite

$$\mathbb{L} \otimes_{\mathbb{J}} \otimes \mathbb{R} \otimes_{\mathbb{J}} \cdots \otimes_{\mathbb{J}} \mathbb{L} \otimes_{\mathbb{J}} \mathbb{R}$$

to one in

$$\mathbb{L} \otimes_{\mathbb{J}} \mathbb{R}$$

Notice how $\mathbb{J}$ acts on $\mathbb{L}$ and $\mathbb{R}$ both on the left and and on the right. The one action is covariant and the other is contravariant. So there is a priori no unique way to slide all the maps in the various copies of $\mathbb{J}$ around and group them all together. This unique-zig-zag condition is asking precisely for this condition to hold. This is to be contrasted with the case when $\mathbb{J}$ is all isomorphisms; because a map $\varphi : X \to Y$ in $\mathbb{J}$ induces another map $\varphi^{-1} : Y \to X$ this zig-zag condition reduces to the unique factorization up to isomorphism of orthogonal factorization system. Indeed, when $\mathbb{J}$ only contains isomorphisms, this zig-zag condition reduces to a slight modification of the notion of an orthogonal factorization system.

This notion of factorization system over a subcategory is introduced by Cheng [Che20]; she establishes a correspondence between these factorization systems and distributive laws of monads in $\mathsf{Set\text{-}Prof}^{\mathsf{op}}$. The result is mentioned with distributive laws of Lawvere theories in mind, but it is a general fact:

Lemma 2.109. *A factorization system* $(\mathbb{L}, \mathbb{R})$ *of a small category* $\mathbb{X}$ *over a subcategory* $\mathbb{J}$ *is precisely a distributive law of monads* $\mathbb{R}$ *over* $\mathbb{L}$*, both regarded as* $\mathbb{J}$*-bimodules in* $\mathsf{Span}(\mathsf{Set})$*.*

By asking that $\mathbb{X}$ is a small strict monoidal category and $\mathbb{L}$, $\mathbb{R}$ and $\mathbb{J}$ are appropriately strict monoidal subcategories, the notion of a factorization system of $\mathbb{X}$ over $\mathbb{J}$ is adapted immediately to monoidal categories. And there is an analogous correspondence to distributive laws of $\mathbb{R}$ over $\mathbb{L}$, regarded as $\mathbb{J}$-bimodules in $\mathsf{Span}(\mathsf{Mon})$.

Lemma 2.110. *Take three symmetric monoidal theories*

$$R = (\mathsf{Ob}, \Sigma_R, E_R), \;\; L = (\mathsf{Ob}, \Sigma_L, E_L), \;\; J = (\mathsf{Ob}, \Sigma_J, E_J)$$

with the same objects, where $\overline{J}$ *embeds as a strict symmetric monoidal category within both* $\overline{L}$ *and* $\overline{R}$*. Regard both* $\overline{L}$ *and* $\overline{R}$ *as* $\overline{J}$*-bimodules, where the left and right actions are given by lifting the maps in* $\overline{J}$ *along this embedding.*

Suppose there is a distributive law of monads in the bicategory $\mathsf{Mon}\text{-}\mathsf{Prof}^{\mathsf{op}}$*:*

$$\lambda : \overline{R} \otimes_{\overline{J}} \overline{L} \Rightarrow \overline{L} \otimes_{\overline{J}} \overline{R}$$

where $\overline{L}$ *and* $\overline{R}$ *are canonically strict monoidal subcategories of* $\overline{L} \otimes_{\overline{J}} \overline{R}$*.*

Then the induced prop $\overline{L} \otimes_{\overline{J}} \overline{R}$ *is presented by a monoidal theory*

$$(\mathsf{Ob}, \Sigma_R \cup \Sigma_L, E_R \cup E_L \cup E_\lambda)$$

where E_λ *is the set of equations dictating the unique ways in which the generators of* Σ_R *can be pushed past those of* Σ_L *up to zig-zags in* $\overline{J}$*.*

This seems like a very complicated construction, but let us see some examples to understand the utility. As a general rule, because factorization systems are decompositional (so that we start with a category and decompose it into smaller parts), we will start first with a symmetric monoidal theory which we already know, and then decompose it into smaller constituent symmetric monoidal theories. For the most basic examples consider the free strict symmetric monoidal category on a set of objects:

Definition 2.111. Let p^X denote the free strict symmetric monoidal category with objects in X, where p is the free symmetric monoidal category with one object.

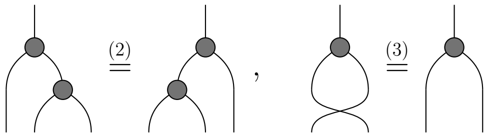
That is to say p^X is the category of permutations on X elements regarded as a strict monoidal category.

It is easy to see how every coloured prop with generating object set Ob is canonically a p^{Ob}-bimodule in $\mathsf{Span}(\mathsf{Mon})$ picking out the symmetry maps.

Consider the following distributive law of props, coming from the epi-mono factorization system of finite sets:

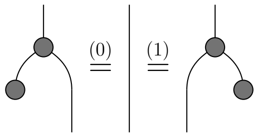
Example 2.112 ([Lac04, Example 5.1])**.** Let inj be the prop generated by a single generator $0 \to 1$ and no equations:

And let surj denote the prop generated by a commutative semigroup:



inj is a presentation for the injections and surj the surjections in FinOrd $\cong$ FSet under the coproduct. Moreover, distributive law:

$\mathsf{cm} = \mathsf{inj} \otimes_{\mathsf{p}} \mathsf{surj};$



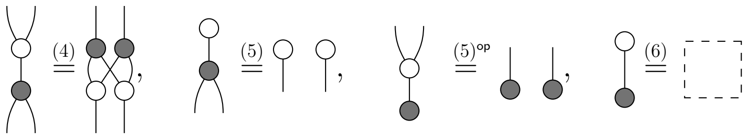
induces the prop for the commutative comonoid cm $\cong$ FinOrd $\cong$ FSet.

This distributive law corresponds to the epi-mono orthogonal factorization system of FinOrd. However, as opposed to the analagous story for FinOrdMonot, because the permutations are nontrivial isomorphisms, we had to take a distributive law of monads of bimodules over the permutations.

Bicommutative bialgebras also arise similarly:

Example 2.113. The prop cb for a bicommutative bialgebra, is presented by a distributive law between a monoid ● and comonoid ○:

$\mathsf{cm}^{\mathsf{op}} \otimes_{\mathsf{p}} \mathsf{cm};$



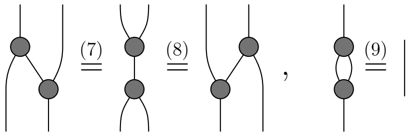
This is also is a symmetric monoidal orthogonal factorization system since it arizes from a category of spans:

Lemma 2.114 ([Lac04, Example 5.3])**.** cb *is a presentation for* $(\mathsf{Span}^{\sim}(\mathsf{FSet}), +)$.

Dually:

Example 2.115. The distributive law between a monoid ● and comonoid ●:

$\mathsf{cm} \otimes_{\mathsf{p}} \mathsf{cm}^{\mathsf{op}};$



This is the prop scfa for the free special commutative Frobenius algebra, which we discussed earlier.

This distributive law also arizes from a category of spans.

Lemma 2.116 ([Lac04, Example 5.4]). sfa *is a presentation for* $(\mathsf{Span}^{\sim}(\mathsf{FSet}^{\mathsf{op}}), +)$.

Remark 2.117. The spider normal form also holds for special commutative Frobenius algebras, where now components can be connected together using the symmetry maps.

In analogy to the noncommutative case, the spider normal form for non-special commutative Frobenius algebras also holds; although it does not arize from a distributive law of props. The original spider normal form was first proven for non-special symmetric Frobenius algebras, first published in the Ph.D. thesis of Abrams [Abr97]; wherein it was proved by topological methods rather than using the machinery of distributive laws.

Note that all of these examples of distributive laws of props are actually monoidal orthogonal factorization systems. Indeed, they are both special cases of the two examples of orthogonal factorization systems which we provided earlier: orthogonal factorization systems arizing from spans, and orthogonal factorization systems arizing from epi-mono factorization. We will see nontrivial examples of such distributive laws in Subsections 4.3.2 and 4.3.3.

Aside 2.118. There is another way to decompose props which we have not reviewed, because we will not make use of it. Since distributive laws are themselves monads, one can take distributive laws of distributive laws themselves.

In the case of distributive laws of categories, Cheng remarked that this is precisely a monad in $\mathsf{Mnd}(\mathsf{Mnd}(\mathsf{Span}(\mathsf{Set})))$ [Che11]. This corresponds to a "ternary strict factorization system" and can be iterated finitely many times to obtain n-ary strict factorization systems. The coherence conditions can be boiled down into asking that the appropriate distributive laws must interact to satisfy the Yang-Baxter equations.

There is nothing special about strict factorization systems of small categories. The way to decompose props in this setting would be in terms of monads in $\mathsf{Mnd}(\mathsf{Mnd}(\mathsf{Mod}(\mathsf{Span}(\mathsf{Mon}))))$. Indeed, this was used in Zansi's thesis multiple times [Zan18, Proposition 3.3., Example 2.34].

Chapter 3

Categorical quantum mechanics

String diagrams have been used in quantum theory for quite some time; in particular, as early as the work of Penrose [Pen71]. In such settings, string diagrams have been used as (often heuristic) tools for calculation. The more recent programme of "categorical quantum mechanics," following the seminal paper of Abramsky and Coecke [AC04] has endeavoured to reformulate finite dimensional quantum mechanics using category theory. In this setting, string diagrams are formal mathematical objects: allowing certain essential features to be abstracted away from the usual setting of finite dimensional Hilbert spaces.

In this section, we review this formalism as well as recent developments which are relevant to this thesis. A more in depth mathematical introduction can be found in the book of Heunen and Vicary [HV19], with a more broadly accessible and applied introduction being found in the book of Coecke and Kissinger [CK17]. For a more traditional approach to quantum computing see the book of Nielsen and Chuang [NC10].

To motivate this graphical treatment of finite dimensional quantum theory, we first establish some basic algebraic notations.

3.1 Quantum states and unitary evolution

Fix a finite dimensional Hilbert space $\mathcal{H}$ with dimension $d \geq 2$, which we will regard as our local state-space. An element of $\mathcal{H}$ is called a **qubit** when $d = 2$, a **qutrit** when $d = 3$, a **qupit** when d is prime, a **quopit** when d an odd prime and a **qudit** when there is no restriction on d.

The elements of an orthonormal basis of $\mathcal{H}$ indexed by a set $\mathcal{J}$ are drawn in "ket notation" by $|b_j\rangle$, for all $j \in \mathcal{J}$. The tensor product of these vectors is denoted as a list delimited by commas so that for example:

$$|b_x\rangle \otimes |b_y\rangle =: |b_x, b_y\rangle$$

Most of the time, we will not choose an arbitrary d-dimensional Hilbert space for the local state-space. Instead, we will work in the Hilbert space of square summable functions on $\mathbb{Z}/d\mathbb{Z}$, $\ell^2(\mathbb{Z}/d\mathbb{Z})$ (see Definition 2.74). Here, the elements of $\mathbb{Z}/d\mathbb{Z}$ induce a basis for $\ell^2(\mathbb{Z}/d\mathbb{Z})$ called the **standard basis** or Z-basis. We will denote the elements of the basis as $\{|0\rangle, \dots, |d-1\rangle\}$. The structure of a ring is therefore transported onto the standard basis elements (or a field when d is prime). These are regarded as the d-level quantum analogue of classical dits. Similarly, the n-qudit state space is regarded as the Hilbert space $\ell^2((\mathbb{Z}/d\mathbb{Z})^n)$, so that the n-standard basis elements have the structure of an n-dimensional $\mathbb{Z}/d\mathbb{Z}$-bimodule (or vector space, when d is prime).

Denote arbitrary vectors φ in $\mathcal{H}$ using this ket notation by $|\varphi\rangle$; where the adjoint of $|\varphi\rangle$ is denoted as a "bra" by $|\varphi\rangle^\dagger =: \langle\varphi|$.

Given two vectors $|\varphi\rangle$ and $|\psi\rangle$ on the same space, the inner product "bra-ket" is denoted by $\langle\varphi|\psi\rangle$ and the outer product by $|\varphi\rangle\langle\psi|$. This notation allows us to succinctly represent matrices. For example, a complex matrix from d^n to d^m regarded as an operator $A : \ell^2((\mathbb{Z}/d\mathbb{Z})^n) \to \ell^2((\mathbb{Z}/d\mathbb{Z})^m)$ with entries $a_{j,k}$ is denoted as follows:

$$A = \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} a_{j,k} |j\rangle\langle k|$$

Given another matrix $B : \ell^2((\mathbb{Z}/d\mathbb{Z})^m) \to \ell^2((\mathbb{Z}/d\mathbb{Z})^\ell)$ with entries $b_{k',j'}$:

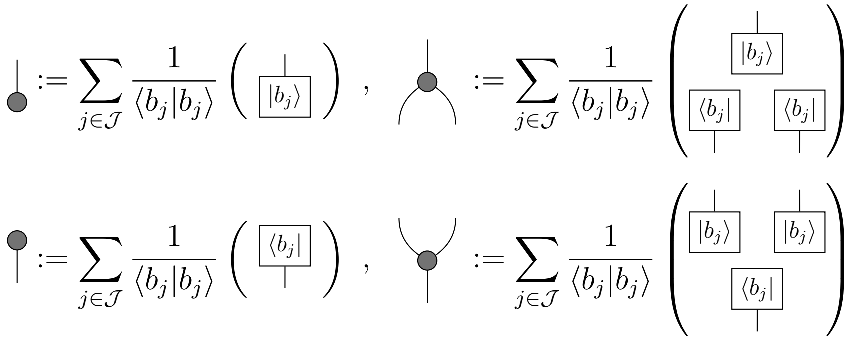
$$B = \sum_{j'=0}^{m-1} \sum_{k'=0}^{\ell-1} b_{k',j'} |k'\rangle\langle j'|$$

Their composite is computed by matrix multiplication:

$$\begin{aligned} BA &= \sum_{j'=0}^{m-1} \sum_{k'=0}^{\ell-1} b_{k',j'} |k'\rangle\langle j'| \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} a_{j,k} |j\rangle\langle k| = \sum_{k=0}^{n-1} \sum_{j,j'=0}^{m-1} \sum_{k'=0}^{\ell-1} b_{k',j'} a_{j,k} |k'\rangle\langle j'|j\rangle\langle k| \\ &= \sum_{k=0}^{n-1} \sum_{k'=0}^{\ell-1} \left(\sum_{j=0}^{m-1} b_{k',j} a_{j,k} \right) |k'\rangle\langle k| \end{aligned}$$

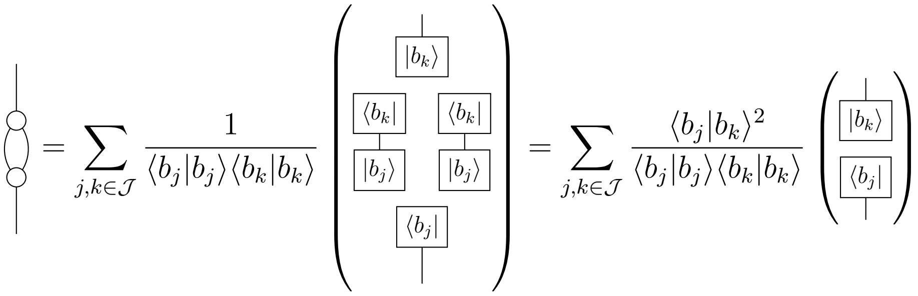
There is a graphical way to represent orthonormal bases:

Lemma 3.1 ([CPV13]). *Orthgonal bases $\{|b_j\rangle\}_{j\in\mathcal{J}}$ in* FHilb *are in bijection with commutative †-Frobenius algebras. The †-Frobenius algebras* ● *are of the form:*

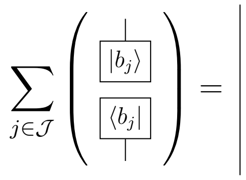


These are precisely the Frobenius algebras that (co)copy the basis elements. It is easy to see how the laws of a commutative †-Frobenius algebra hold; however, the proof of the converse direction is quite a bit trickier.

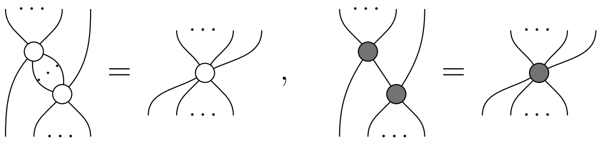
Notice how special *commutative †-Frobenius algebras* ○ *are in bijection with orthonormal bases, as:*



is equal to the identity if and only if the basis is orthonormal:



We will colour special commutative †-Frobenius algebras ○ and non-special commutative †-Frobenius algebras ●. Recall the two variations of the normal form for special and non-special commutative †-Frobenius algebras:

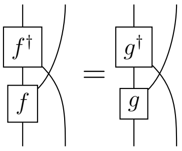


A **pure quantum state** is a vector $|\varphi\rangle$ with norm 1, so that $|\langle\varphi|\varphi\rangle|^2 = \langle\varphi|\varphi\rangle = 1$. Pure quantum states are interpreted as the possible physical states of a quantum system which has been unexposed to the classical world. The quantum evolution of pure quantum states is modeled by their postcomposition with unitary maps. Unitary maps are precisely the linear automorphisms which preserve the norm, and thus, preserve pure quantum states.

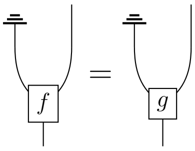
To actually do computations with quantum states, one has to measure things using a classical interface. Selinger gives a construction to produce categories of quantum channels from general †-compact closed categories [Sel07]. When applied to FHilb, this construction adds discarding behavior to quantum systems. This will provide the necessary machinery to model measurement.

We present this construction in terms of a quotient of the CoPara construction for the sake of uniformity of this thesis. This construction is *extremely important* for this thesis, so it is essential to understand.

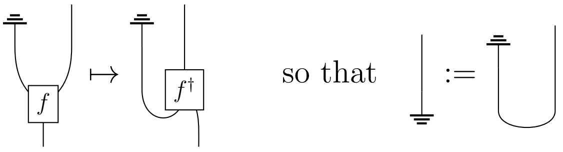
Definition 3.2 (CPM construction)**.** Given a compact closed †-symmetric monoidal category $\mathbb{X}$, then $\mathsf{CPM}(\mathbb{X}, (-)^\dagger)$ (which we will denote by $\mathsf{CPM}(\mathbb{X})$ when the dagger is clear from the context) is the quotient of $\mathsf{CoPara}(\mathbb{X})$ by the symmetric monoidal congruence relation, so that $\left(X \xrightarrow{(f,S)} Y\right) \sim \left(X \xrightarrow{(g,T)} Y\right)$ if and only if



Draw elements of this equivalence class using the following notation:

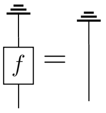


The dagger is defined as follows:



This makes $\mathsf{CPM}(\mathbb{X})$ into a †-symmetric monoidal category. The map $d_X = ((u_X^L)^{-1}, X)$ is called the **discarding map** on X:

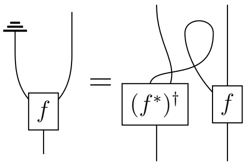
The canonical functor $\mathbb{X} \to \mathsf{CoPara}(\mathbb{X}) \to \mathsf{CPM}(\mathbb{X})$ taking $f \mapsto (f, I)$ is called **doubling**. The maps in the image of this functor are **pure**, and those which aren't are **mixed**. A map $f : X \to Y$ in $\mathsf{CPM}(\mathbb{X})$ is called **trace-preserving** when $f; d_Y = d_X$:



All maps can be obtained by composing pure maps with discard maps. Given a mixed map f in $\mathsf{CPM}(\mathbb{X})$ such a factorization into a pure map followed by a discard map is a **purification** of f.

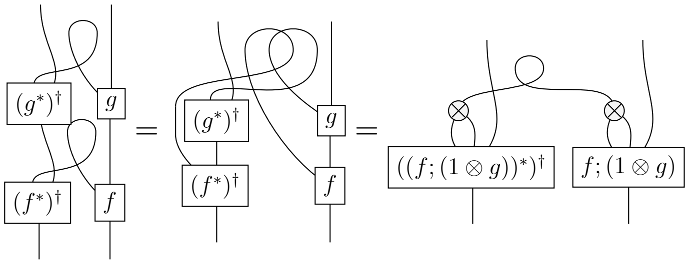
The compact closed structure of $\mathsf{CPM}(\mathbb{X})$ is inherited from the doubling of the compact closed structure of $\mathbb{X}$. If the †-symmetric monoidal structure of $\mathbb{X}$ is compatible with its compact closed structure, so that $\mathbb{X}$ is †-compact closed, then $\mathsf{CPM}(\mathbb{X})$ is †-compact closed as well.

Oftentimes, we will bend the "doubled picture" so that the inputs are on the bottom and the outputs are on the top:

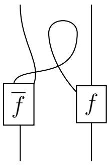


We could have chosen a different, equivalent congruence relation to quotient by to avoid the symmetry map on the cap, but this would be incompatible with notation for stabilizer tableaux which we use much later in this thesis.

In the doubled picture, the composition of equivalence classes is in $\mathsf{CPM}(\mathbb{X})$ is composition in $\mathbb{X}$:



This different perspective will prove useful for the purposes of calculation. Notice how we could have instead defined a †-monoidal structure in terms of the conjugation functor $\overline{(-)} := ((-)^*)^\dagger$, so that the equivalence classes look like:



Therefore, we shall invoke the CPM construction for both dagger structures and conjugation functors depending on which setting is most natural.

As mentioned before, the following example motivated this categorical construction:

Example 3.3. $\mathsf{CPM}(\mathsf{FHilb}, (-)^\dagger)$ is the dagger compact closed category of density matrices between finite dimensional Hilbert spaces. Density matrices are also called, "completely positive maps," hence the name CPM. This is dagger compact closed equivalent to the strict symmetric monoidal skeleton of density matrices $\mathsf{CPM}(\mathsf{Mat}_{\mathbb{C}}, \overline{(-)})$. In the nonstrict setting it is more convenient to work with the dagger, the Hermetian adjoint; however, in the skeletal case, we will use the complex conjugation functor.

Density matrices model mixed quantum circuits. The discarding map is interpreted as quantum discarding which exposes the quantum system to the classical world. The adjoint of the discard map is interpreted as the maximally-mixed state which injects classical noise into a system.

A (mixed) **quantum state** is a trace-preserving state in CPM(FHilb). Given a pure quantum state in FHilb, its doubled version is a quantum state in CPM(FHilb). Mixed quantum states are the states which can be obtained by discarding parts of pure quantum states, so that they can be regarded as the physical states of a quantum/classical system.

The trace-preserving maps in CPM(FHilb) model the mixed quantum-classical evolution of quantum states; as they are precisely the maps in CPM(FHilb) which preserve quantum states.

3.2 Quantum measurement

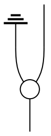
Given an orthonormal basis $B = \{|b_j\rangle\}_{j\in\mathcal{J}}$ of $\mathcal{H}$ and a quantum state state $|\varphi\rangle$ on $\mathcal{H}$ then:

$$\sum_{j\in\mathcal{J}} |\langle b_j|\psi\rangle|^2 = 1$$

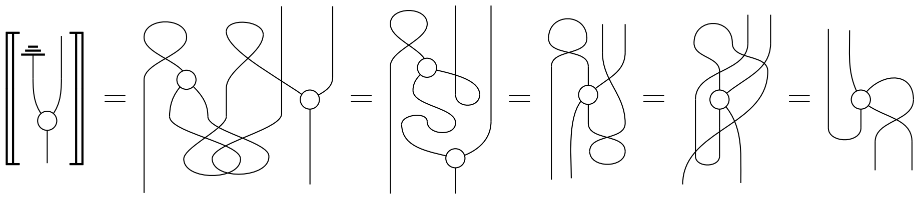
This gives a probability distribution over $\mathcal{J}$. The scalar $0 \leq |\langle b_j|\psi\rangle|^2 \leq 1$ is interpreted as the probability of measuring the basis element $|b_j\rangle$ on the state $|\psi\rangle$ with respect to the basis B. This basis dependent, probabilistic interpretation of quantum measurement is called the **Born rule**, although it is usually stated slightly differently.

The CPM construction and special commutative †-Frobenius algebras allow us to perform quantum measurement using only string diagrams. Some mathematical machinery is needed first:

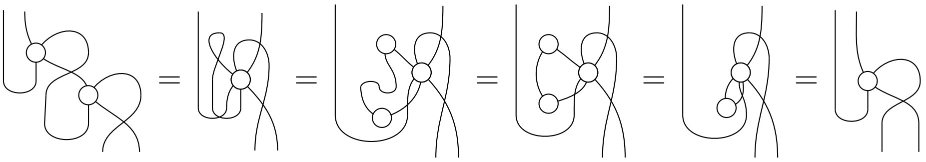
Definition 3.4. Given a special †-commutative Frobenius algebra B on a †-compact closed category $\mathbb{X}$, define the projector onto the B basis to be the following map in CPM($\mathbb{X}$):

$p_B :=$ 

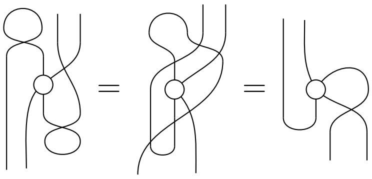
In the doubled picture, we untangle the quantum spaghetti:



Recall that a map e is a projector when it is idempotent (so that $e^2 = e$) and self-adjoint (so that $e^\dagger = e$). p_B is idempotent because:



And self-adjoint because:



Therefore it is actually a projector.

Given a quantum state $|\psi\rangle$ and an orthonormal basis B; $|\psi\rangle$ is said to **collapse** onto the basis B when it is postcomposed with p_B as follows $p_B|\psi\rangle$. This transforms a quantum state into a stochastic mixture of all of the basis elements of B. To promote these classical stochastic mixtures to their own systems, we need a way to turn subobjects into objects:

Definition 3.5. Given a category $\mathbb{X}$ and a class of idempotents $\mathcal{I}$, the **Karoubi envelope** $\mathsf{Split}_{\mathcal{I}}(\mathbb{X})$ of $\mathbb{X}$ at $\mathcal{I}$, is the category with:

Objects: Pairs (X, e) where X is an object of $\mathbb{X}$ and $e : X \to X$ is in $\mathcal{I}$.

Maps: A map $(e, f, m) : (X, e) \to (Y, m)$ is a map $f : X \to Y$ in $\mathbb{X}$ such that $e; f; m = f$.

Composition: $(e, f, m); (m, g, \ell) = (e, f; g, \ell)$.

Identities: $1_{(X,e)} = (1_X, e, 1_X)$.

In particular, when $\mathcal{I}$ contains all idempotents in $\mathbb{X}$, call $\mathsf{Split}(\mathbb{X}) := \mathsf{Split}_{\mathcal{I}}(\mathbb{X})$ the Karoubi envelope of $\mathbb{X}$. $\mathbb{X}$ fully and faithfully embeds into its Karoubi envelope via the functor:

$$\left(X \xrightarrow{f} Y\right) \mapsto \left((X, 1_X) \xrightarrow{(1_X, f, 1_Y)} (Y, 1_Y)\right)$$

$\mathbb{X}$ is **Cauchy-complete** when this embedding is an equivalence. Moreover, when $\mathbb{X}$ is monoidal, symmetric monoidal or compact closed, so is $\mathsf{Split}(\mathbb{X})$ with the embedding preserving this structure.

$\mathsf{Split}_{\mathcal{I} \cup \{1_X | X \in \mathbb{X}\}}(\mathbb{X})$ is said to be the category obtained by **splitting the idempotents in $\mathcal{I}$**. When one splits an idempotent $e : X \to X$, then (X, e) is the retract of $(X, 1_X)$:

$$\begin{tikzcd}
(X, e) \arrow[r, tail, "{(e,e,1_X)}"] \arrow[dr, equal, "{(1_X,e,1_X)}"'] & (X, 1_X) \arrow[d, two heads, "{(1_X,e,e)}"] \\
& (X, e)
\end{tikzcd}
\qquad
\begin{tikzcd}
(X, 1_X) \arrow[r, two heads, "{(1_X,e,e)}"] \arrow[dr, "{(e,e,e)}"'] & (X, e) \arrow[d, tail, "{(e,e,1_X)}"] \\
& (X, 1_X)
\end{tikzcd}$$

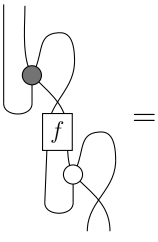
This specializes to †-compact closed categories, so that projectors get promoted to objects:

Definition 3.6 ([Sel08])**.** Given a †-category $\mathbb{X}$ and class of projectors $\mathcal{I}$ in $\mathbb{X}$, then $\mathsf{Split}_{\mathcal{I}}(\mathbb{X})$ is a † category. The map $(e, 1_X, 1_X) : (X, e) \to (X, 1_X)$ is an isometry with adjoint $(1_X, 1_X, e) : (X, 1_X) \to (X, e)$. In particular, when $\mathbb{X}$ is †-compact closed then so is $\mathsf{Split}^{\dagger}(\mathbb{X})$, with the embedding preserving this structure.

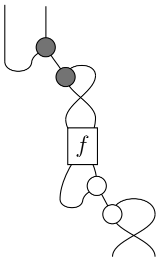
Selinger shows that splitting projectors in $\mathsf{CPM}(\mathsf{FHilb})$ yields a category where the the split projectors can be interpreted as classical types [Sel08]:

Remark 3.7. Given a basis $B = \{|b_j\rangle\}_{j\in\mathcal{J}}$ for $\mathcal{H}$, the isometry $(p_B, 1_{\mathcal{H}}, 1_{\mathcal{H}}) : (\mathcal{H}, p_B) \to (\mathcal{H}, 1_{\mathcal{H}})$ is regarded as the **state preparation map** and its adjoint $(1_{\mathcal{H}}, 1_{\mathcal{H}}, p_B) : (\mathcal{H}, 1_{\mathcal{H}}) \to (\mathcal{H}, p_B)$ a **destructive measurement** with respect to the basis B.

Let us unpack this a bit. Take an orthonormal basis B for $\mathcal{H}$ and B' for $\mathcal{H}'$ corresponding to a special commutative †-Frobenius algebras ○ and ●, respectively. Then maps $(\mathcal{H}, p_B) \to (\mathcal{H}', p_{B'})$ correspond to maps $p_B; f; p_{B'}$ for some $f : \mathcal{H} \to \mathcal{H}'$ in $\mathsf{CPM}(\mathsf{FHilb})$:

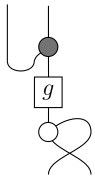


$=$

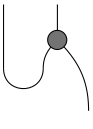
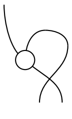


(3.1)

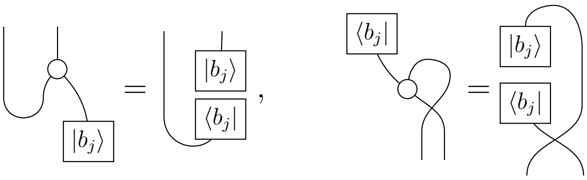
Therefore by inspecting the dimensions, every map $(\mathcal{H}, p_B) \to (\mathcal{H}', p_{B'})$ is of the following form, for some $g : \mathcal{H} \to \mathcal{H}'$ in FHilb:



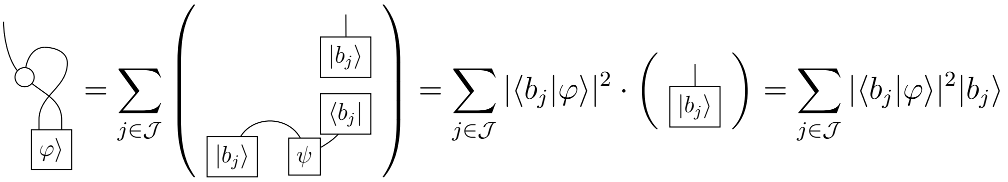
Because the equivalence classes of maps in $\mathsf{CPM}(\mathsf{FHilb})$ are defined in terms of the complex conjugation of maps in FHilb; the representative g in FHilb is unique up to a scalar factor $e^{2\pi\cdot i\cdot\theta}$ for some $\theta \in [0, 1)$. That is to say, these maps are unique **up to global phase**. Take $\mathcal{H} = \mathcal{H}'$. Up to global phase, the subobject $(\mathcal{H}, e_B)$ can be identified with the the Hilbert space $\mathcal{H}$; where state preparation with respect to ● and nondestructive measurement with respect to ○ correspond to the following maps:

$[\![(1_{\mathcal{H}}, 1_{\mathcal{H}}, p_{B'})]\!] =$  , $[\![(p_B, 1_{\mathcal{H}}, 1_{\mathcal{H}})]\!] =$ 

The state preparation map and measurement maps for ○ double the basis elements $|b_j\rangle$ and $\langle b_j|$ of B and B^*:

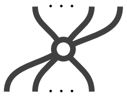


Given a quantum state $|\varphi\rangle$ on $\mathcal{H}$, measuring in the B-basis has the following effect:

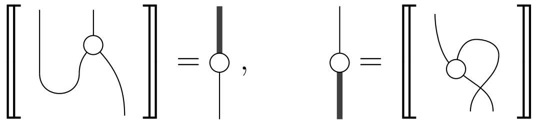


Therefore, measuring $|b_j\rangle$ yields the scalar $|\langle b_j|\varphi\rangle|^2$, which is the correct probability according to the Born rule.

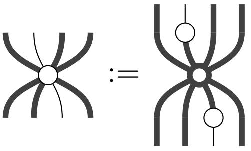
There is a graphical calculus for this two-coloured prop of classical and quantum types. The classical wires are drawn thin and the quantum wires are drawn thick. The pure spider we have have been working with so far is drawn with a thick border:



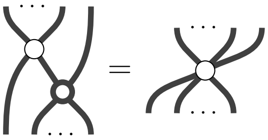
The state preparation and measurement are drawn as thin spiders interfacing between the quantum and classical systems:



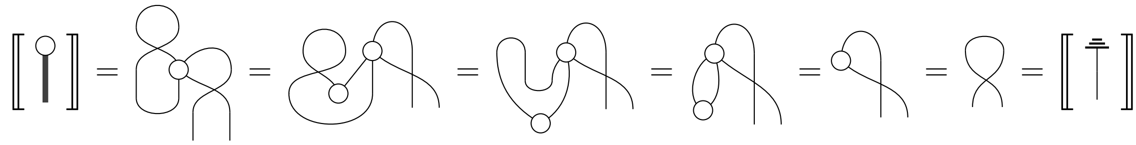
The conjugation of pure spiders by state preparation and measurement maps creates **thick-thin spiders** following Coecke and Kissinger [CK17] (which they call bastard spiders). Thick-thin spiders are drawn with a thin border to distinguish them from pure spiders, however, their legs can be either thick or thin. For example:



The thin border on ○ indicates that the state has been measured in the basis ○ and is a stochastic mixture of the basis element of B. When a pure spider is connected to a thick-thin spider they both fuse into a thick-thin spider:

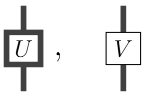


The discard map is classical spider with one thick wire:



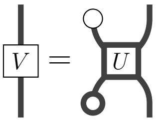
Notice that this way of describing the discard map is independent of the choice of orthonormal basis.

In general, we will draw thick borders around arbitrary pure maps U between quantum systems; and thin borders around mixed maps V between quantum systems:



All isometries and unitaries in $\mathsf{CPM}(\mathsf{FHilb})$ are pure so we always drawn them with a thick border. This notation allows us to succinctly state a special notion of purification in $\mathsf{CPM}(\mathsf{FHilb})$:

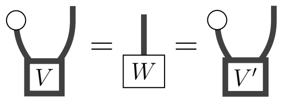
Proposition 3.8 (Stinespring dilation). *Given a trace preserving map V in $\mathsf{CPM}(\mathsf{FHilb})$, there exists a unitary U such that:*



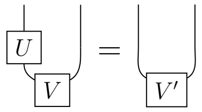
for all special commutative †-Frobenius algebras ○.

The proof is relatively involved so we will omit it. See Stinesprings paper for the original statement[Sti55], and Coecke and Kissinger's book for the graphical version which we use [CK17, Corollary 6.63]. Essentially, the significance of this result is that quantum processes can always be produced by first preparing a state, then applying quantum evolution and then discarding part of the state. There is another closely related result which we will make use of:

Proposition 3.9 (Essential uniqueness of purification). *Given two purifications $V : \mathcal{H}_1 \otimes \mathcal{H}_0$ and $V' : \mathcal{H}_1 \otimes \mathcal{H}_0$ of a mixed state $W : \mathcal{H}_0$ in $\mathsf{CPM}(\mathsf{FHilb})$:*



so that without loss generality $\dim \mathcal{H}_1 \leq \dim \mathcal{H}_2$*, then there exists an isometry $U : \mathcal{H}_1 \to \mathcal{H}_2$ such that:*

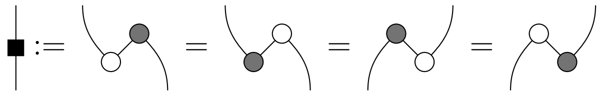


Moreover, U is unique up to a unique unitary.

3.3 The ZX-calculus

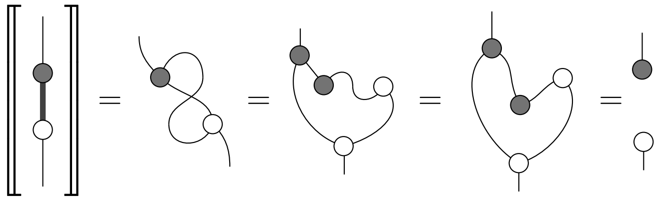
There is a very important relationship which bases can have to each other:

Definition 3.10. Take commutative †-Frobenius algebras ○ and ●. They are **strongly complementary** when they interact to form Hopf algebras (see Example 2.32) whose antipode is equivalently any of the following maps:



Strongly complementary bases have important information-theoretical properties:

Lemma 3.11. *Given two strongly complementary bases given by special commutative †-Frobenius alegbras ○ and ● preparing a state with respect to the basis ○ and measuring with respect to the basis ● preserves no information, as:*



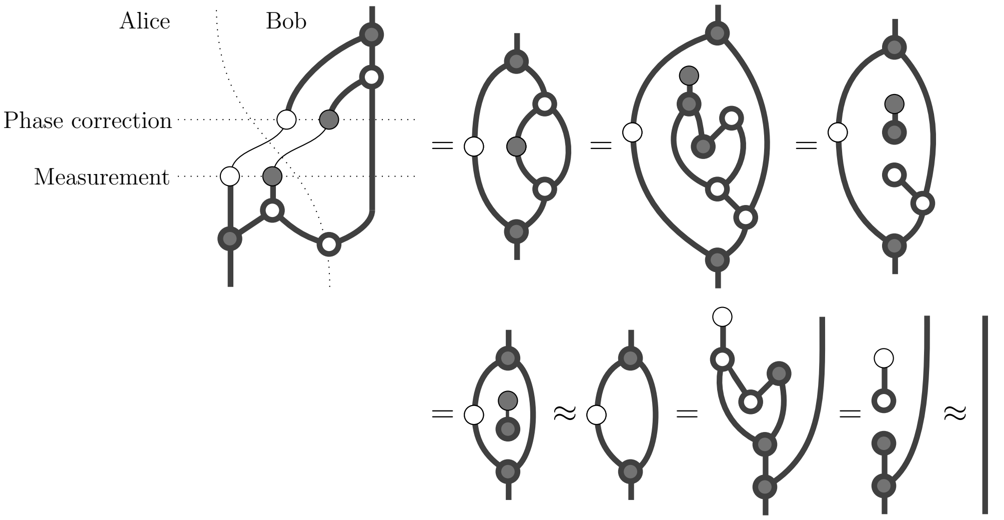
Even though we only used the Hopf law here, the bialgebra structure is indispensable for other reasons.

Given two strongly complementary observables, we can construct the quantum teleportation protocol (originally discovered for qubits by Bennett et al. [BBC^{+}93]). The abstract description of quantum teleportation in terms †-compact closed categories was first introduced by Abramsky and Coecke [AC04]; however, we present a qudit generalization of the one using thick-thin spiders found in Coecke and Kissinger's book [CK17, Page 706]:

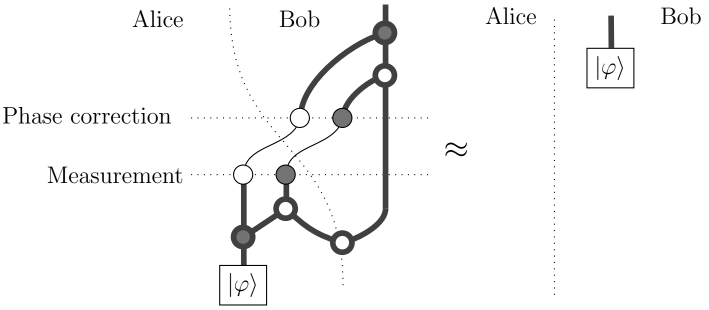
Protocol 3.12.

1. Alice and Bob first prepare a qudit Bell state together and establish a classical channel with which Alice is able to send two dits to Bob.
2. They are separated in space.
3. Alice applies a unitary operation in between her two qudits.
4. Alice measures both of the qudits in the complementary bases and then sends two classical dits to Bob.
5. Bob uses the two classical dits to perform phase-correction to his half of the Bell state in the complementary bases.

Graphically:

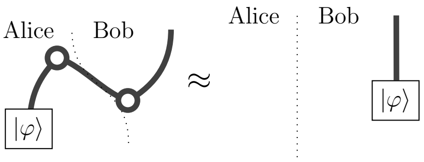


So that if Alice prepares a quantum state $|\varphi\rangle$, then Bob receives it:



Notice how all parts of this protocol are physically realizable operations. The Bell-state is a quantum state and unitary operations are quantum operations. As we discussed, measurement is realizable, and produces a classical outcome according to a probability distribution via the Born rule (in fact, in this case each possible outcome is equally likely). Finally, for Bob's phase correction operation, he receives the two measurement outcomes of Alice, and conditioned on these outcomes he applies quantum operations to the quantum channel.

This is in contrast to the naive way in which one might hope to teleport a qudit from Alice to Bob using the compact closed structure induced by ○:



The cap not a quantum operation, nor is it a measurement, or a classical operation, therefore it does not specify a physically realizable quantum protocol.

The reason we ask not only for the Hopf law but also for the bialgebra law is because the following two very important bases have this property:

Example 3.13. Given fixed dimension d, recall that the standard basis, or Z-basis, is denoted as follows:

$$\{|0\rangle, \dots, |d-1\rangle\}$$

The Fourier basis, or X-basis, is denoted as follows:

$$\{\sqrt{d}\mathcal{F}|0\rangle, \dots, \sqrt{d}\mathcal{F}|d-1\rangle\}$$

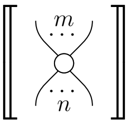
where the qudit quantum Fourier transform is the unitary map:

$$\mathcal{F} := \frac{1}{\sqrt{d}} \sum_{j,k=0}^{d-1} e^{2\pi \cdot i \cdot j \cdot k/d} |k\rangle\langle j|$$

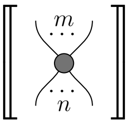
The Z and X bases are strongly complementary.

For qubits, the state $|+\rangle := \mathcal{F}|0\rangle$ is called the **plus state**; and $|-\rangle := \mathcal{F}|1\rangle$ is called the **minus state**. Notice how we multiply the X-basis elements by a factor of $\sqrt{d}$ so that these two Frobenius algebras interact to form a Hopf algebra on the nose (as opposed to up to scaling factors). This means that the Fourier basis we have chosen is only orthogonal, and thus the corresponding Frobenius algebra is not special. However, this isn't a problem, because it is special up to the invertible scalar $1/\sqrt{d}$.

This pair of complementary bases will occur throughout this thesis. As a matter of notation, as mentioned earlier we draw the "Z-spiders" for the standard basis in white, and "X-spiders" for the Fourier basis in grey as follows:



$$= \sum_{j=0}^{d-1} |j, \dots, j\rangle\langle j, \dots, j|$$

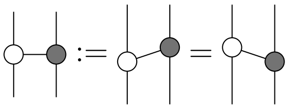


$$= \sqrt{d} \sum_{j=0}^{d-1} \mathcal{F}|j, \dots, j\rangle\langle j, \dots, j|\mathcal{F}^\dagger$$

The Z-spiders compare standard basis elements and the X-spiders compare their sums (which is why we ask for the Bialgebra law on top of the Hopf law):

$$\sqrt{d} \sum_{j=0}^{d-1} \mathcal{F}|j, \dots, j\rangle\langle j, \dots, j|\mathcal{F}^\dagger = \sum_{\forall x \in (\mathbb{Z}/d\mathbb{Z})^n, y \in (\mathbb{Z}/d\mathbb{Z})^m : \sum x_j = \sum y_k} |y_1, \dots, y_n\rangle\langle x_1, \dots, x_n|$$

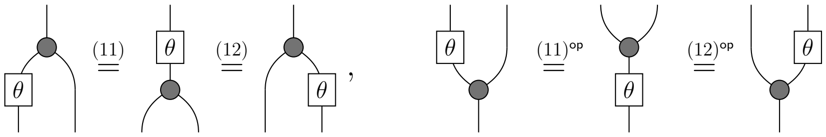
When $d = 2$, the antipode is the identity, therefore it doesn't matter if the wires are inputs or outputs of spiders. For example, we can draw the **controlled-not gate** by connecting together Z and X spiders, only having to worry about the connectivity:



In other terms, following Carette, the Z and X-spiders are **flexsymmetric** [Car21, Section 5].

We almost have all of the essential ingredients of categorical quantum mechanics; however, thick-thin spiders alone are not very expressive. The following bridges this gap:

Definition 3.14. Given a †-Frobenius algebra ● on an object X, a **phase** for the Frobenius algebra is a unitary endomorphism $\theta : X \to X$ which commutes with the multiplication and comultiplication, so that:



Phases for Frobenius algebras are closed under composition; and they form a group called the **phase group** for the Frobenius algebra. The phase group associated with a commutative Frobenius algebra is therefore Abelian.

The motivating example is again FHilb, which makes sense of the name:

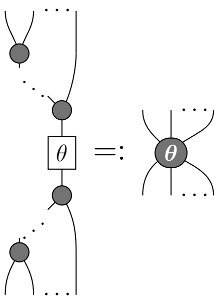
Example 3.15. Given an orthonormal basis $\{|b_j\rangle\}_{j\in\mathcal{J}}$ of $\mathcal{H}$, the phases are generated by the following unitaries, for all $\{\theta_j\} \in [0,1)^{\mathcal{J}}$:

$$\sum_{j\in\mathcal{J}} e^{2\pi\cdot i\cdot\theta_j/d}|b_j\rangle\langle b_j|$$

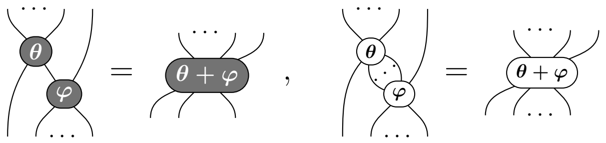
Recall that maps in CPM(FHilb) are unique up to global phase, therefore when the basis has a chosen order $\{|b_0\rangle, \cdots, |b_{d-1}\rangle\}$, as a matter of convention fix $\theta_0 = 0$. This means that the phases of that basis in CPM(FHilb) are uniquely parameterized by the group $[0,1)^{d-1}$. In the literature it is commonplace to index the phases over $[0,2\pi)^{d-1}$ rather than over $[0,1)^{d-1}$. We chose the latter because it is much more amenable to generalization away from quantum mechanics.

The normal form for spiders extends to spiders with phases:

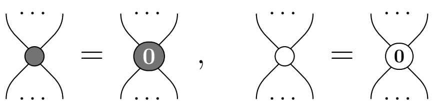
Lemma 3.16 (Phased spider normal form)**.** *The connected components of a commutative †-Frobenius algebra ● and its phase group can be factorized into the following form on the right. Call the notation on the left a phased-spider:*



The normal forms for commutative †-Frobenius algebras ● plus phases, as well as special special commutative †-Frobenius algebras ○ plus phases induce phased-spider fusion rules:



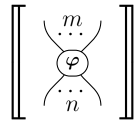
This notation is compatible with the non-phased spider notation, where a spider drawn with no phase corresponds to a phased spider whose phase is the identity:



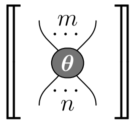
Definition 3.17. Given some fixed dimension d, a fragment of the qudit **ZX-calculus** is a prop generated by two strongly complementary spiders, each of which is parameterized by phase groups.

We also require that this comes equipped with a faithful †-symmetric monoidal functor into FHilb, sending the objects $n \mapsto \ell^2((\mathbb{Z}/d\mathbb{Z})^n)$ and sending the two phased spiders to the Z and X-phased spiders in a way that preserves the phase-group structure.

That is to say, we have spiders decorated by phase groups G and H and group homomorphisms $g : G \to [0,1)^d$ and $h : H \to [0,1)^d$, respectively such that:



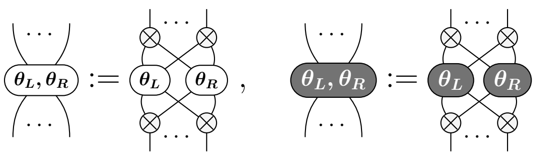
$$= \sum_{j=0}^{d-1} e^{2\cdot\pi\cdot i\cdot g_j(\varphi)/d} |j,\ldots,j\rangle\langle j,\ldots,j|$$



$$= \sqrt{d}\sum_{j=0}^{d-1} e^{2\cdot\pi\cdot i\cdot h_j(\theta)/d} \mathcal{F}|j,\ldots,j\rangle\langle j,\ldots,j|\mathcal{F}^\dagger$$

Take a fragment $[\![-]\!]$: ZX → Hilb of the ZX-calculus and a †-compact closed subcategory of $\mathbb{X} \hookrightarrow$ FHilb, such that this interpretation essentially-surjectively factors through $\mathbb{X}$ (so that $\mathbb{X}$ contains all the objects of $[\![\mathsf{ZX}]\!]$ up to isomorphism). The fragment is **universal** for $\mathbb{X}$ when the map ZX $\to \mathbb{X}$ is full and **complete** when it is faithful.

The **scalable ZX-calculus** (coined by Carette et al. [CHP19]) refers to string diagrams for the strictification of the ZX-calculus (ie, proof nets for the ZX-calculus). Frobenius algebras on wires of composite dimension are denoted as follows:



As we use string diagrams for nonstrict monoidal categories extensively throughout this thesis, we won't declare when we are using scalable ZX-notation; it will just be the default setting in which we work.

3.4 The stabilizer formalism

Consider the simplest fragment of the ZX-calculus:

Definition 3.18. The **phase-free** qudit ZX-calculus is the fragment of the ZX-calculus generated by the Z and X spiders with no phases.

This has a relational semantics; to expose which we need the following definition:

Definition 3.19. A unitary map $f : \mathcal{H} \to \mathcal{H}$ is a **stabilizer** of a state $|\varphi\rangle$ on $\mathcal{H}$ in case $|\varphi\rangle$ is a $+1$-eigenvector of g so that $g|\varphi\rangle = |\varphi\rangle$.

The qudit $\mathcal{X}$-gate (qubit not-gate) shifts the X-basis vectors by a mod d:

$$\mathcal{X} := \sum_{b=0}^{d-1} |b+1\rangle\langle b| \ , \quad \text{where} \quad \mathcal{X}^a = \sum_{b=0}^{d-1} |b+a\rangle\langle b|$$

Similarly, the qudit $\mathcal{Z}$-gate shifts the Z-basis vectors by a mod d:

$$\mathcal{Z} := \mathcal{F}\mathcal{X}\mathcal{F}^\dagger = \sum_{b=0}^{d-1} e^{2\cdot\pi\cdot b/d}|b\rangle\langle b| \ , \quad \text{where} \quad \mathcal{Z}^z = \mathcal{F}\mathcal{X}^z\mathcal{F}^\dagger = \sum_{b=0}^{d-1} e^{2\cdot\pi\cdot z\cdot b/d}|b\rangle\langle b|$$

An X-stabilizer of an n-qudit state φ is a stabilizer of the form:

$$\mathcal{X}^{a_0} \otimes \mathcal{X}^{a_1} \otimes \cdots \otimes \mathcal{X}^{a_{n-2}} \otimes \mathcal{X}^{a_{n-1}}$$

Similarly, a Z-stabilizer of an n-qudit state φ is a stabilizer of the form:

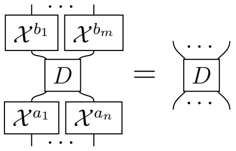
$$\mathcal{Z}^{a_0} \otimes \mathcal{Z}^{a_1} \otimes \cdots \otimes \mathcal{Z}^{a_{n-2}} \otimes \mathcal{Z}^{a_{n-1}}$$

The X stabilizers characterize the phase-free ZX-calculus: [1]

Lemma 3.20. *Given an odd prime p, $\mathsf{LinRel}_{\mathbb{F}_p}$ is isomorphic to the qupit phase-free ZX-calculus modulo invertible scalars.*

Proof. Given a phase-free ZX-diagram it is easy to see how the X-stabilizers form a linear subspace over $\mathbb{F}_p$ as follows:

$$[\![D]\!]_X := \left\{ \left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \right) \in \mathbb{F}_p^n \oplus \mathbb{F}_p^m \ : \right\}$$



---

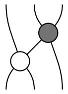
[1] This has been known for quite some time to both the categorical concurrency and quantum communities in the qubit case, see for example in the thesis of Zanasi [Zan18, Page 8].

Conversely, given an $\mathbb{F}_p$-linear subspace, take the projector onto the joint +1-eigenspace spanned by the corresponding X-stabilizers:

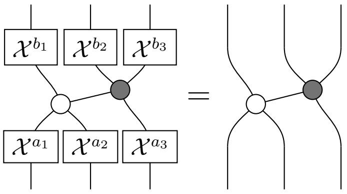
$$S \mapsto \frac{1}{|S|} \sum_{(x_1,\cdots,x_n)\in S} |x_1,\cdots x_n\rangle\langle x_1,\cdots,x_n|$$

Regarding this as a state on $\ell^2(\mathbb{F}_p^n)$ in $\mathsf{CPM(FHilb)}$, partition the codomain of the state into an input and output. Bending the input wires down yields an inverse to the previous mapping. ☐

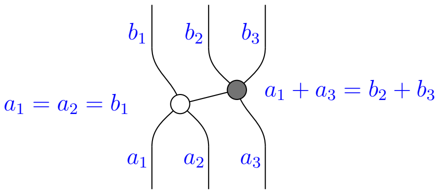
Example 3.21. Consider the following phase-free ZX-diagram:



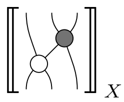
Its X-stabilizers are parameterized by all the $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_p$ such that:



By labeling the wires with linear equations over $\mathbb{F}_p$, we can calculate these stabilizers:



Which gives us a linear subspace of $\mathbb{F}_p^3 \oplus \mathbb{F}_p^3$:



$$\left[\!\left[\;\cdot\;\right]\!\right]_X = \left\{ \left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \right) : a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_p, a_1 = a_2 = b_1 \wedge a_1 + a_3 = b_2 + b_3 \right\}$$

Definition 3.22. The $\mathcal{X}$-gate fragment of the ZX-calculus is given by adjoining the $\mathcal{X}$-gate as a generator to the phase free ZX-calculus.

The qudit $\mathcal{X}$-gate is a phase for the X-spider as:

$$\mathcal{X} = \sum_{j=0}^{j-1} |j+1\rangle\langle j| = \sum_{j=0}^{d-1} e^{2\pi \cdot i \cdot j/d} \mathcal{F}|j\rangle\langle j|\mathcal{F}^\dagger$$

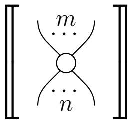
Therefore, natural number powers of the $\mathcal{X}$-gate are also phases for the X-spider as:

$$\mathcal{X}^n = \sum_{j=0}^{d-1} |j+n\rangle\langle j| = \sum_{j=0}^{d-1} e^{2\pi \cdot i \cdot n \cdot j/d} \mathcal{F}|j\rangle\langle j|\mathcal{F}^\dagger$$

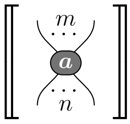
So one can ask if the fragment of the odd prime qudit ZX-calculus with these $\mathcal{X}$-gate phases has a similar relational semantics to the phase-free ZX-calculus. The answer is yes, and this result is not contained in the literature to the knowledge of the author:

Lemma 3.23. $\mathsf{AffRel}_{\mathbb{F}_p}$ *is isomorphic to the qupit fragment of the ZX-calculus with* $\mathcal{X}$*-gates as phases modulo invertible scalars.*

This is given by the interpretation:



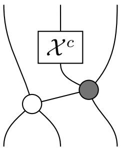
$$= \sum_{j=0}^{p-1} |j,\dots,j\rangle\langle j,\dots,j|$$



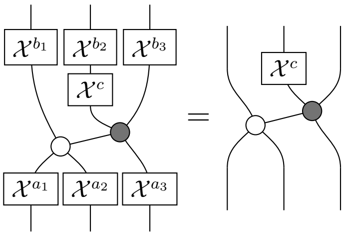
$$= \sum_{\sum x_i = \sum y_j + a \mod p} |y_1,\dots,y_n\rangle\langle x_1,\dots,x_n|$$

The proof is almost identical to that for linear relations and phase-free ZX-diagrams.

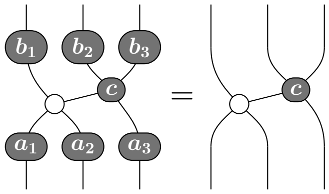
Example 3.24. Consider the following diagram in the $\mathcal{X}$-gate fragment of the qupit ZX-calculus:



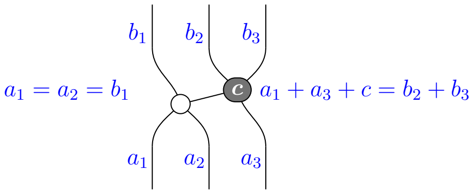
To compute the X stabilizers is to find the $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_p$ such that



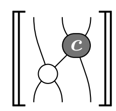
In $\mathsf{AffRel}_{\mathbb{F}_p}$, this equation looks like:



These $a_1, a_2, a_3, b_1, b_2, b_3$ are parameterized by the elements of the affine subspace:



So that:



$$= \left\{ \left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \right) : a_1 = a_2 = a_3 \wedge a_1 + a_3 + c = b_2 + b_3 \right\}$$

Because we can represent affine subspaces over $\mathbb{F}_p$ in the qupit ZX-calculus we can use the string diagrammatic notation for graphical linear and graphical affine algebra within the qupit ZX-calculus. In the literature, this representation of matrices over $\mathbb{F}_2$ has already been exploited [BR22, CDP21].

There is nothing particularly special about the $\mathcal{X}$-gate. By interpreting circuits in the $\mathcal{Z}$-gate fragment of the qupit ZX-calculus modulo scalars in terms of their Z-stabilizers, we would have similarly recovered the categories of linear/affine relations over $\mathbb{F}_p$.

The $\mathcal{Z}$ and $\mathcal{X}$ operators are very important in quantum computing:

Definition 3.25. Fix some local dimension d. A single qudit **Weyl operator** is an d-dimensional unitary of the form, $\mathcal{X}^x\mathcal{Z}^z$, for $x, z \in \mathbb{Z}/d\mathbb{Z}$.

An n-qudit Weyl operator is the n-fold tensor product of single qudit Weyl operators. The n-quopit Weyl operators form the **Heisenberg-Weyl group** $\mathcal{P}_d^n$ under matrix multiplication and the Hermitian adjoint. The n-qubit Heisenberg-Weyl group is generated by n-qubit Weyl operators in addition to the scalar i.

Note that the qubit Heisenberg-Weyl group is often called the Pauli group and its elements are called Pauli operators.

Weyl operators have the following property (see [NC10, Section 10.3.1]):

Lemma 3.26. *n-qupit Weyl operators are an orthonormal basis for the finite dimensional Hilbert space of operators*

$$\mathsf{FHilb}(\ell^2(\mathbb{F}_p^n), \ell^2(\mathbb{F}_p^n)) \cong \ell^2(\mathbb{F}_p^n)^* \otimes \ell^2(\mathbb{F}_p^n)$$

with respect to the scaled trace inner product:

$$\langle -, = \rangle := \frac{1}{p^n}\mathsf{Tr}((-)^\dagger, =)$$

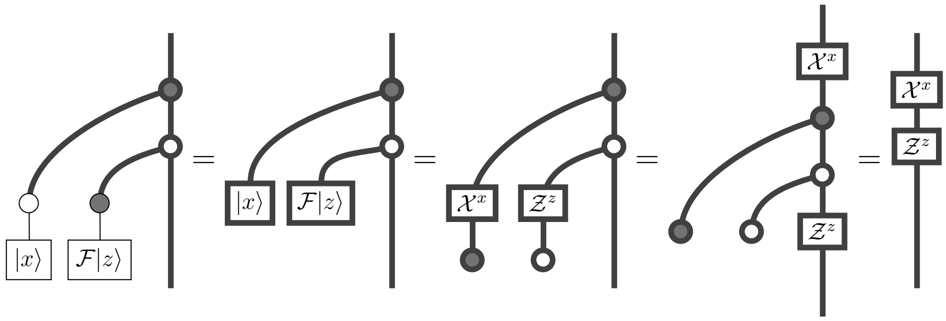
An obvious choice of operator basis would have been:

$$\{|a_0, \cdots, a_{n-1}\rangle\langle b_0, \cdots, b_{n-1}| \mid a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1} \in \mathbb{F}_p\}$$

However, these basis elements are not unitary, and therefore can not be used to correct for errors. On the other hand if at some point a known unitary error occurs, because Weyl operators form a unitary basis, the error can be undone by applying controlled Weyl operators. In fact, the quantum teleportation protocol relies on this fact. Let us reexamine the phase-correction step in this protocol in more detail. Notice how the Z-and X-bases are respectively:

$$\{\mathcal{X}^n|0\rangle\}_{n\in\mathbb{F}_p}\ ,\quad \{\mathcal{F}|n\rangle = \mathcal{F}\mathcal{X}^n|0\rangle = \mathcal{Z}^n\mathcal{F}|0\rangle\}_{n\in\mathbb{F}_p}$$

Therefore to correct for the error $\mathcal{Z}^{-z}\mathcal{X}^{-x}$ which was communicated to him by Alice in terms as the pair of classical dits (x, z), Bob applies the following classically controlled operation:



where the second last equation follows from the fact that $\mathcal{X}^x$ is a phase for ● and $\mathcal{Z}^z$ is a phase for ○.

The stabilizer formalism is a tractable tool used for correcting errors. Indeed, everything we have discussed so far, including quantum telportation is encompassed by this formalism. It was first introduced by Gottesman [Got97] and later generalized to qudits in various ways. We follow the qudit generalization of Gottesman [Got99]:

Definition 3.27. An n-qupit **Clifford operator** U is a unitary on $\ell^2(\mathbb{F}_p^n)$ that preserves the Heisenberg-Weyl group, so that $U\mathcal{P}_p^n U^\dagger = \mathcal{P}_p^n$. The n-qupit Clifford operators form the n-qupit **Clifford group** under matrix multiplication and the Hermitian adjoint. The qupit Clifford groupoid (or full qupit Clifford group) is the prop where the maps $n \to n$ are qupit Clifford operators.

An n-qupit (pure) **stabilizer state** is a state $U|0\rangle^{\otimes n}$ for an n-qudit Clifford U.

Given any n-qupit pure stabilizer state $|\psi\rangle$, the **stabilizer group** of $|\psi\rangle$ is the subgroup of $\mathcal{S}_{|\psi\rangle} \subset \mathcal{P}_p^n$ whose elements stabilize $|\psi\rangle$.

The reason why stabilizer states are so nice is because their representation in terms of stabilizer groups is very convenient, owing to the highly symmetric structure of the Heisenberg-Weyl group.

Lemma 3.28. *Up to global phase, stabilizer states are in bijective correspondence their stabilizer groups, and stabilizer groups are in bijection with maximal Abelian subgroups of* $\mathcal{P}_p^n$.

Definition 3.29. The prop of qupit **stabilizer circuits** is generated by qupit Clifford operators as well as the state $|0\rangle$ and effect $\langle 0|$.

There is a crucial difference between the qubit and quopit Heinsenberg-Weyl group:

Lemma 3.30. *All single quopit Weyl operators all can be factored into* $e^{2\pi\cdot i\cdot a/p}\mathcal{Z}^z\mathcal{X}^x$ *for* $a, z, x \in \mathbb{F}_p$. *Whereas all single qubit Weyl operators can be factored into* $i^a\mathcal{Z}^z\mathcal{X}^x$ *for* $z, x \in \mathbb{F}_2$ *and* $a \in \mathbb{Z}/4\mathbb{Z}$.

This difference between qubits and quopits is also reflected in the structure of the Clifford groupoid:

Lemma 3.31 ([Got99, Page 5])**.** *Up to nonzero scalars, the qupit Clifford groupoid is generated by the Fourier transform* $\mathcal{F}$, *the phase-shift gate* $\mathcal{S}$, *controlled-*$\mathcal{X}$ *gate* $\mathcal{C}_\mathcal{X}$, *and scaling gates* $\mathcal{M}_a$ *for every* $a \in \mathbb{F}_p^*$ *where:*

$$\mathcal{C}_\mathcal{X} := \sum_{j,k=0}^{p-1} |j, j+k\rangle\langle j, k| \qquad \mathcal{M}_a := \sum_{j=0}^{p-1} |j \cdot a\rangle\langle j|$$

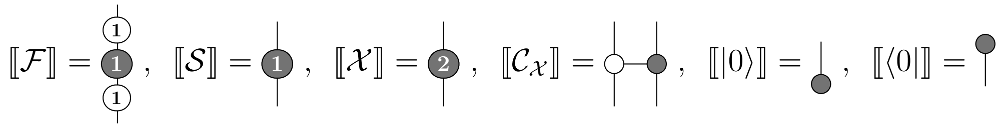
Such that for qubits, $\mathcal{S} := \sum_{j=0}^{1} i^j |j\rangle\langle j|$, *and for quopits,* $\mathcal{S} := \sum_{j=0}^{p-1} e^{\pi\cdot i\cdot j(j-1)/(2p)}|j\rangle\langle j|$

As we will discuss in much further detail in Chapter 5, the ZX-calculus is naturally suited for stabilizer circuits:

Definition 3.32. The **qubit stabilizer fragment of the ZX-calculus** is generated by two spiders with phases in the group $\mathbb{Z}/4\mathbb{Z}$ where:

$$\mathbb{Z}/4\mathbb{Z} \to [0,1)^2;\ n \mapsto (0, n/4)$$

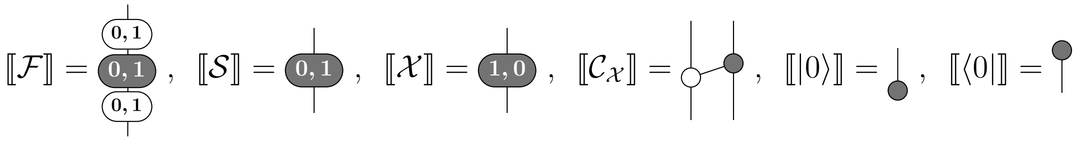
The generators of qubit stabilizer circuits are interpreted as follows:



The **quopit stabilizer fragment of the ZX-calculus** is generated by two spiders with phases in the group $(\mathbb{Z}/p\mathbb{Z})^2$ where:

$$(\mathbb{Z}/p\mathbb{Z})^2 \to [0,1)^p;\ (n,m) \mapsto \prod_{j=0}^{p-1}(nj + mj^2)/(2p) \mod 1$$

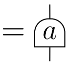
The generators of quopit stabilizer circuits are interpreted as follows:



The scaling gates (often called multiplication gates or multipliers) are derived in stabilizer circuits. They correspond to the multiplication by a scalar under the embedding:

$$(\mathsf{Mat}_{\mathbb{F}_p}, +) \to (\mathsf{LinRel}_{\mathbb{F}_p}, +) \to (\mathsf{FHilb}/\sim, \otimes)$$

That is using the notation for graphical linear/affine algebra within the qupit ZX-calculus:

$$[\![\mathcal{M}_a]\!] =$$ 

Even though the quopit and qubit stabilizer fragments of the ZX-calculus diverge, they coincide when the phases are restricted. We have already observed this during our analysis of the phase free, $\mathcal{X}$-gate and $\mathcal{Z}$-gate fragments of the ZX-calculus.

Definition 3.33. Given any prime p, the **biaffine** fragment of the qupit stabilizer ZX-calculus is generated by Z and X spiders with phases in the group $\mathbb{Z}/p\mathbb{Z}$ where:

$$\mathbb{Z}/p\mathbb{Z} \to [0,1)^p;\ n \mapsto \prod_{j=0}^{p-1}(nj)/(2p)$$

Concretely, the biaffine fragment of the qubit stabilizer ZX-calculus corresponds to the real fragment of qubit stabilizer circuits, where the stabilizers do not contain tensor factors of the form $\mathcal{Z}\mathcal{X}$.

Therefore, anytime we make a statement about quopit stabilizer circuits that doesn't refer to the Fourier transform or phase-shift gates, it also applies to biaffine qupit stabilizer circuits.

The qubit and qutrit stabilizer ZX-calculi both have complete presentations [Bac14, Bac15] and [Wan18]. However, during the process of writing this thesis, Booth and Carette gave a complete axiomatization for the quopit stabilizer ZX-calculus [BC22], followed shortly by an even simpler presentation by Poór et al. [PBC$^+$23]. Note that the interpretations of the generators in these papers differ from ours slightly for technical reasons: they designed their presentations to be flexsymmetric.

Despite being used being used extensively for error correction, as we will discuss in Section 5.5, unlike general quantum circuits, stabilizer circuits are not any more powerful than classical probabilistic computing:

Theorem 3.34 (Gottesman-Knill)**.** *Stabilizer circuits can be classically probabilistically simulated in polynomial time.*

The original proof for qudits is given by Gottesman, where he partially attributes it to Knill [Got98]; however, it follows immediately for qudits. Later on, we will effectively reprove the quopit Gottesman-Knill theorem when we give a relational characterization of quopit stabilizer circuits. In fact stabilizer circuits are the largest classically simulatable fragment containing the Clifford group:

Proposition 3.35 ([CAB12, Appendix D])**.** *Adding any non-Clifford unitary to stabilizer circuits is an approximately universal set of generators for qupit circuits.*

By approximately universal, this means that such a set of generators is dense in the appropriate sense. The qubit case seems to be folklore; Campbell et al.'s reference which we have cited only proves it for quopits. Surely this also holds for all dimensions, but the group theory becomes harder. It is dense in an efficient way, by the Solvay-Kiataev theorem. This is a technical result, first proved initially for qubits; the history again is kind of nuanced, it was first unofficially announced by Solvay, and published by Kitaev [Kit97]. This result was later generalized to all qudits by Dawson et Nielsen [DN06, Section 5].

Therefore, by adding any other phases to qupit stabilizer circuits is maximally expressive. Jeandel et al. constructed the first approximately universal axiomatization of the qubit ZX-calculus in this way [JPV18].

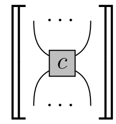
Later, two complete axiomatizations for the qubit ZX-calculus followed, where all phases are included. These two axiomatizations were proven independently. Ng and Wang gave one axiomatization and Jeandel et al. gave the other; almost at the same time [NW17, JPV20]. These presentations of the qubit ZX-calculus are universal on the nose, so that they both are presentations for the full subcategory of $\mathsf{Mat}_{\mathbb{C}}$ whose objects are powers of 2.

3.5 The ZH-calculus

Up until this point, we have discussed quantum circuits as being generated by spiders. Although spiders are good for copying and adding standard basis elements; it is hard to construct nonlinear behaviour using these generators.

To accommodate for this, H-**boxes** were devised in the qubit case by Backens and Kissinger [BK19]:

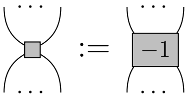
Definition 3.36. Given any $c \in \mathbb{C}$, the c-labelled qubit H-box with n inputs and m outputs is the operator $\ell^2(\mathbb{F}_2^n) \to \ell^2(\mathbb{F}_2^m)$:



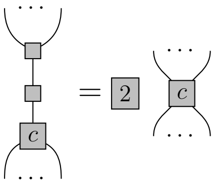
$$= \sum_{a_0,\ldots,a_{n-1},b_0,\ldots,b_{m-1}=0}^{1} c^{a_0\cdot\ldots\cdot a_{n-1}\cdot b_0\cdot\ldots\cdot b_{m-1}} |b_0,\ldots,b_{m-1}\rangle\langle a_0,\ldots,a_{n-1}|$$

Ie, the matrix where all entries are 1, except for the bottom-right entry which is c.

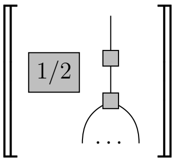
The H-box with label -1 and one input and one output is equal to $\sqrt{2}\mathcal{F}$. Because of this relationship with the Fourier transform, a "phase-free" H-box with no label corresponds to one with label -1:



This is the reason for the name "H-box," as the qubit Fourier transform is often called the "Hadamard gate." One should not confuse an H-box with one input and one output (drawn in grey) with the antipode for the Hopf algebra (drawn in black) for the Z and X-spiders. Although H-boxes do not correspond to Frobenius algebras, they do satisfy a sort of fusion rule:

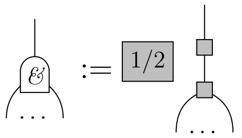


The following diagram multiplies standard basis elements:

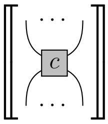


$$= \sum_{a_0,\ldots,a_{n-1}=0}^{1} |a_0 \cdot \ldots \cdot a_{n-1}\rangle\langle a_0, \cdots, a_{n-1}|$$

That is to say, H-boxes, allow us to construct and-gates, which we denote as follows:



In analogy to the ZX-calculus, a **fragment of the ZH-calculus** is presented by unphased Z and X spiders, in addition to H-boxes labelled by a semiring S and an interpretation into FHilb. The interpretation must send the Z and X spiders to the Z and X spiders in Hilb in the same way as for the phase-free ZX-calculus. We also ask that there is a semiring homomorphism $f : S \to \mathbb{C}$ such that



$$= \sum_{a_0,\ldots,a_{n-1},b_0,\ldots,b_{m-1}=0}^{1} (f(c))^{a_0\cdot\ldots\cdot a_{n-1}\cdot b_0\cdot\ldots\cdot b_{m-1}} |b_0, \ldots, b_{m-1}\rangle\langle a_0, \ldots, a_{n-1}|$$

The notions of completeness and universality are essentially the same as for the ZX-calculus. The full qubit ZH-calculus was proved to be complete and universal for all qubit complex matrices in the original paper of Backens and Kissinger [BK19].

Recall that an H-box with no label is the same as an H-box which is labelled by -1. Therefore an axiomatization for the phase-free ZH-calculus must be compatible with the semiring homomorphism $\mathbb{Z} \to \mathbb{C}$. Completeness for the phase-free ZH-calculus up to a scalar factor was proven by van de Wetering and Wolffs; giving a presentation for qubit matrices over $\mathbb{Z}[1/\sqrt{2}]$ [WW19]. In their paper, they also prove that the phase-free ZH-calculus is approximately universal for quantum circuits.

In the following chapter we prove completeness for the circuits generated by unphased Z and X-spiders as well as and gates and not-gates. We prove that this is essentially the natural-number labelled H-box fragment of the ZH-calculus, the only difference being that we carefully avoid having matrices with entries which are not natural numbers.

Recently, in a universal set of generators has been proposed for the qudit ZH-calculus in the Ms.C. thesis of Roy [Roy22], but no completeness theorem exists so far.

Chapter 4

Boolean circuits as spans of finite sets

In this chapter we provide a complete set of identities for quantum circuits generated by Z and X-spiders, the not gate and the and gate. We call this prop ZX&. We show that ZX& is a universal and complete presentation of $2^n \times 2^m$ dimensional matrices over $\mathbb{N}$; equivalently the subcategory of spans of finite sets where the objects are powers of two-element sets. We also show that this is the natural number labeled fragment of the ZH-calculus.

Conceptually, this is the category where the objects are natural numbers and a map from n to m is identified with the *multiset* of solutions to a set of Boolean equations in $n + m$ variables. In other words, in this chapter we give a presentation for the monoidal category whose maps are counting satisfiability problems.

For reference, a complexity theoretic analysis of counting satisfiability problems using the full fragment of the qubit ZH-calclus is performed in the following series of papers [BKM21, LMW23, LMW22]. However, markedly in our analysis, we restrict the ZH-calculus to the category where the maps are *exactly* such problems. We also provide a presentation for the prop of Boolean satisfiability problems, where we quotient by the multiplicty of solutions. [1]

---

[1] Our presentation ZX& solves the open question mentioned at the end of Laakkonen et al. which posits the existence of a prop whose maps correspond to instances of counting satisfiability problems [LMW22, Section 2.2]. However, our publication predates this question being posed [Com21]. The aforementioned article of Laakkonen et al. also mistakenly hints that the completeness result of Gu et al. solves the problem in the multiplicity-quotiented setting [GPZ23]. Moreover, Gu et al. encode Boolean satisfiability problems as *monotone* Boolean relations. This is too erestrictive to express fragments of the ZH-calculus, as the way that Gu et al. encode satisfiability problems is completely different.

Outline

To prove completeness of ZX&, we use the completeness result of Cockett et al. for the prop TOF generated by the Toffoli gate, the not gate and $|0\rangle$ and $\langle 0|$ [CC19]. TOF is complete for the full subcategory of partial isomorphisms between finite sets where the objects are powers of two. In some sense TOF is complete for the *subobjects* of ZX&, so that all Boolean formulae can be encoded in domain of definition of maps in TOF. Nevertheless, work is needed transport the completeness of TOF to the completeness of ZX&.

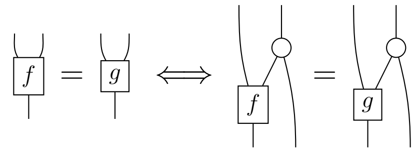
To this end, in Section 4.1 we first reformulate the Cartesian completion of a discrete inverse category. We show that this can be presented by freely adjoining counits to the inverse products of the base inverse category. In the Cartesian completion of TOF, this is interpreted as adjoining the generator $\sqrt{2}\langle +| = (1,1)^T$.

In Section 4.2, we take the pushout of the unit and counit completion of TOF, interpreted as adding the generators $\sqrt{2}|+\rangle$ and $\sqrt{2}\langle +|$ to TOF. This yields the completeness result as well as a presentation which can be regarded as a fragment of the ZH-calculus.

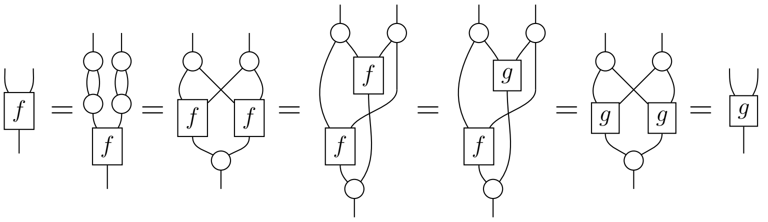
4.1 Cartesian completion as counit completion

In this section we prove that the Cartesian completion of a discrete inverse category can be presented in terms of freely adding a counit to the inverse products of the base monoidal category.

Lemma 4.1. *Given two parallel maps* $X \xrightarrow{f,g} S \otimes Y$ *in a discrete inverse category:*

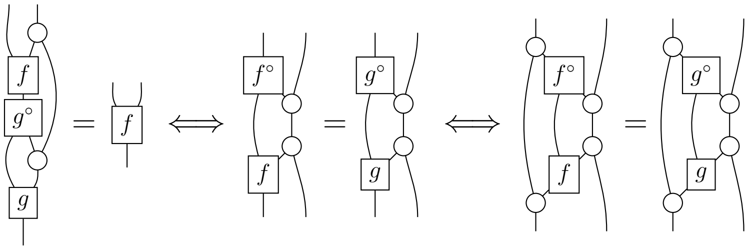


Proof. The forward direction is trivial. For the converse, assume the right hand side holds. Then:

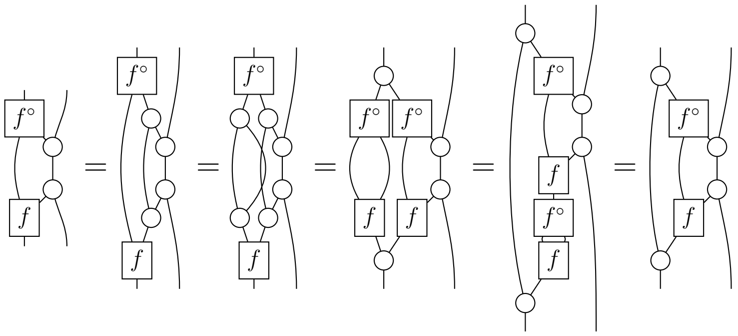


□

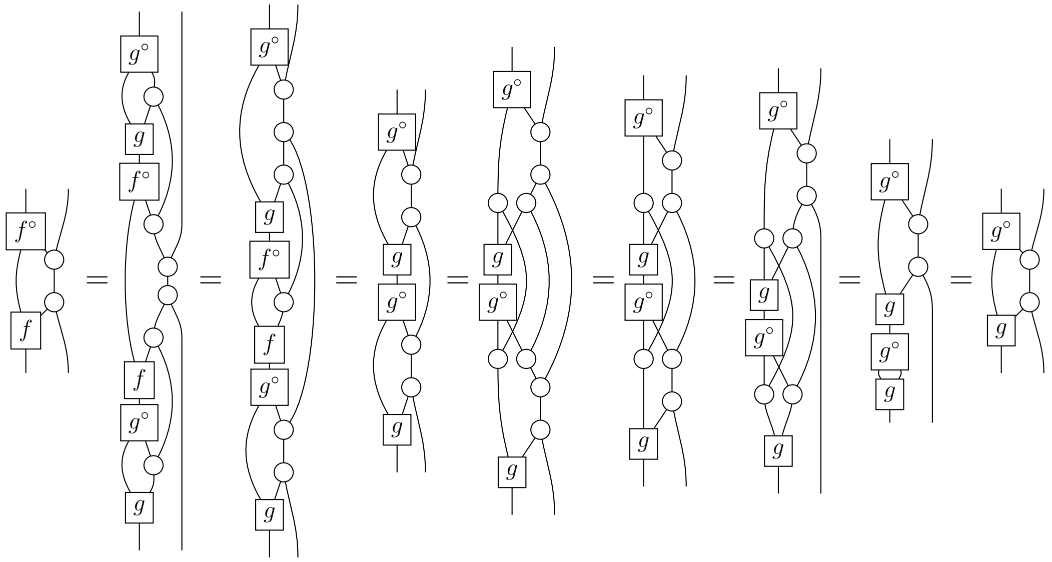
Lemma 4.2. *Given two maps $X \xrightarrow{f} S \otimes Y$ and $X \xrightarrow{g} T \otimes Y$, in a discrete inverse category:*



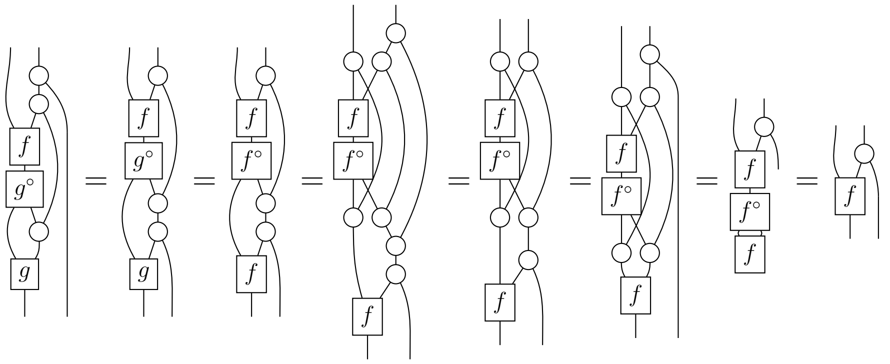
Proof. First note:



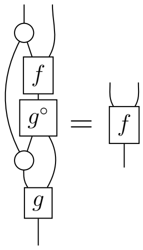
so that we only have to prove the first logical equivalence. Suppose that the left hand side holds, then:



Conversely, suppose that the right hand side holds. Then:



Thus, by Lemma 4.1:



□

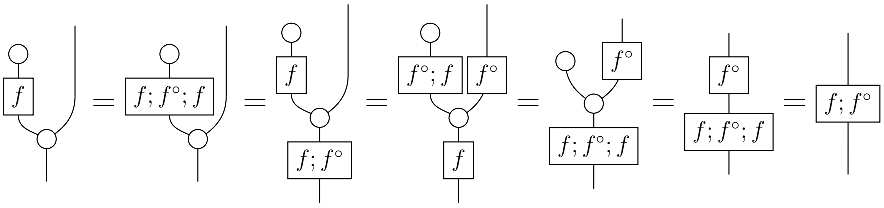
Definition 4.3. Given a discrete inverse category $\mathbb{X}$ define the counital completion of $\mathbb{X}$, $c(\mathbb{X})$, to be the quotient of $\mathsf{CoPara}(\mathbb{X})$ freely making the discard maps $((u_X^L)^{-1}, X)$ into the counit of the cosemigroup of the inverse product on $\mathbb{X}$.

Unrolling the definition, this construction just freely adds counits to the diagonal maps coming from the inverse products of $\mathbb{X}$. Therefore, we have immediately that:

Lemma 4.4. *$c(\mathbb{X})$ is a discrete Cartesian restriction category.*

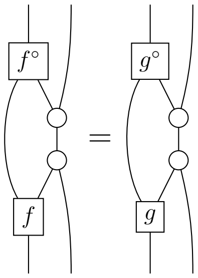
Proposition 4.5. *Given a discrete inverse category $\mathbb{X}$, its counital completion $c(\mathbb{X})$ and Cartesian completion $\widetilde{\mathbb{X}}$ are isomorphic as discrete Cartesian restriction categories.*

Proof. The restriction structure of $\widetilde{\mathbb{X}}$ and $c(\mathbb{X})$ both agree, as:

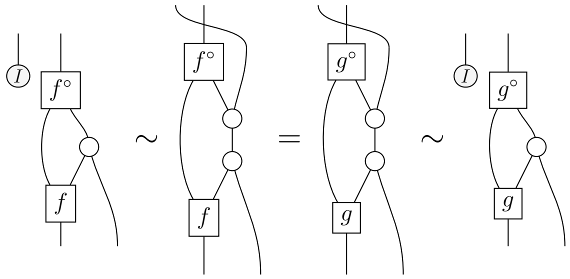


Since both $\widetilde{\mathbb{X}}$ and $c(\mathbb{X})$ are quotients of $\mathsf{CoPara}(\mathbb{X})$, there are identity on objects mappings $F : c(\mathbb{X}) \to \widetilde{\mathbb{X}}$ and $G : \widetilde{\mathbb{X}} \to c(\mathbb{X})$ which are inverse to each other. It remains to show that these are both well-defined functors. The functoriality of F is immediate because $\widetilde{\mathbb{X}}$ is a Cartesian restriction category and thus the diagonal maps all have counits.

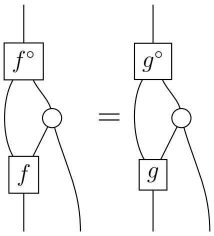
To prove that G is a functor, take some $(f, S) \sim (g, T)$ in $\widetilde{\mathbb{X}}$. By Lemma 4.2, this is asking precisely that the following condition holds in $\mathbb{X}$:



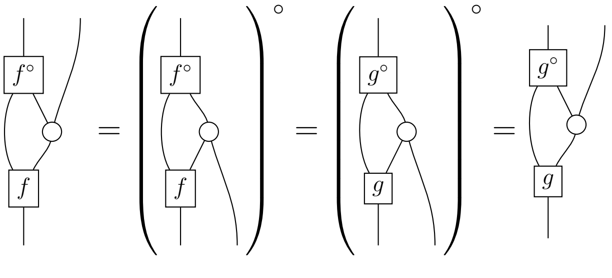
Moreover, since $\widetilde{\mathbb{X}}$ is a discrete Cartesian restriction category, the diagonal has counit; so that the following maps are equivalent:



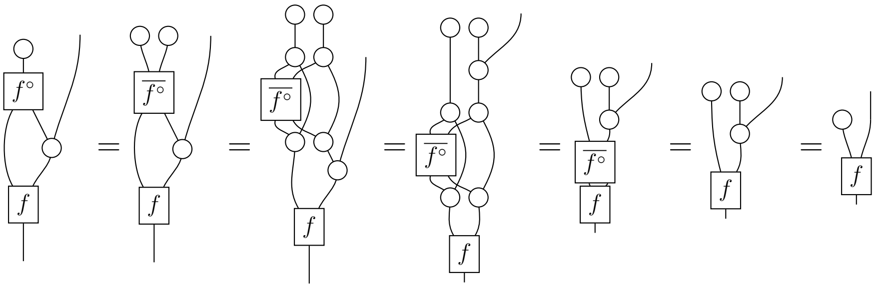
Since the functor $\mathbb{X} \to \widetilde{\mathbb{X}}$ is faithful by Lemma 2.83, we have that in $\mathbb{X}$:



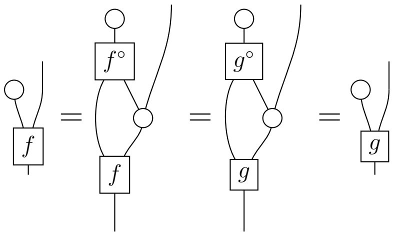
Therefore we can take the partial inverse in $\mathbb{X}$:



Therefore in $c(\mathbb{X})$:



Combining the previous two equations:



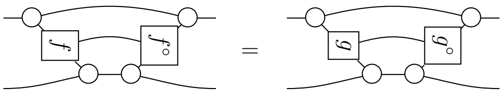
□

There is another equivalent way of viewing this construction, which follows immediately:

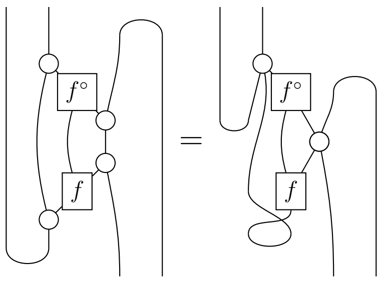
Corollary 4.6. $c(\mathbb{X})$ *is isomorphic to* $\mathsf{Split}_{\{(\Delta_X, X)\ |\ X \in \mathbb{X}_0\}}(\mathsf{CoPara}(\mathbb{X}))$.

Recalling the discussion of the Born rule in Remark 3.7, the Cartesian completion is very similar to the unnormalized stochastic channels in $\mathsf{CPM}(\mathsf{FHilb})$.

Upon further inspection, this resemblance is even more striking. Consider the alternative characterization of the Cartesian completion on the right hand side of Lemma 4.2. Rotating this diagram 90 degrees:



we see that this is essentially Equation 3.1. If the discrete inverse category embeds within a compact closed category then in this embedding we have that:



However, for arbitrary †-symmetric monoidal categories $\mathbb{X}$ (which do not embed in †-commpact closed categories), the quotient of $\mathsf{CoPara}(\mathbb{X})$ by the equivalence relation used to define $\mathsf{CPM}(\mathbb{X},(-)^\dagger)$ in Definition 3.2 is not a congruence with respect to composition (see [CH16, Remark 8]). The the knowledge of the author, it is not known if this is a congruence relation when $\mathbb{X}$ is an arbitrary discrete inverse category.

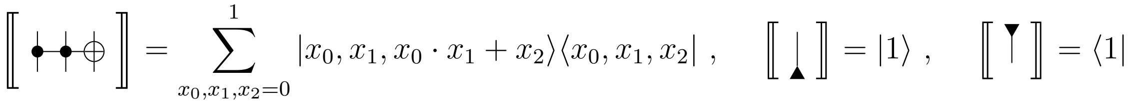
However, in the case that it is a congruence (for example, Pinj, because of the †-symmetric monoidal embedding into a †-compact closed category $\mathsf{Pinj} \hookrightarrow \mathsf{Rel}$) then the Cartesian completion is precisely $\mathsf{Split}_{\{(\Delta_X,X)\ \mid\ X\in\mathbb{X}_0\}}(\mathsf{CPM}(\mathbb{X},(-)^\circ))$.

This relationship between reversible computing and quantum computing still has much to be explored. For example, Heunen et al. relate the Cartesian completion of Par to Stinespring dilation [HK21]. Heunen et al. give a construction which when applied to the subcategory of unitary maps in FHilb yields completely positive maps in $\mathsf{CPM}(\mathsf{FHilb})$; and when applied to Pinj yields Par.

4.2 A graphical calculus for Boolean multirelations

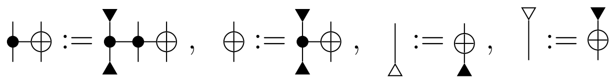
In this section, we give a complete presentation, $\mathsf{ZX}\&$, for the full monoidal subcategory of spans of finite sets where the objects are powers of the two element set. This is performed by freely adding a counit and unit to the semi-Frobenius algebra structure of the prop TOF, and then performing a two way translation between this prop and $\mathsf{ZX}\&$ which we prove is an isomorphism. First recall the prop TOF:

Definition 4.7 ([CC19, Section 4]). TOF is the prop, generated by the Toffoli gate tof, and the 1-ancillary bits $|1\rangle$ and $\langle 1|$ which are interpreted as follows:

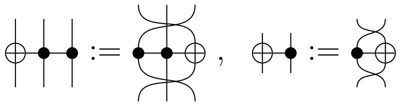


$$= \sum_{x_0,x_1,x_2=0}^{1} |x_0, x_1, x_0 \cdot x_1 + x_2\rangle\langle x_0, x_1, x_2| \ , \qquad = |1\rangle \ , \qquad = \langle 1|$$

where the cnot, not gates and 0-ancillary bits are derived:



and the flippped tof and cnot gates are also derived:



modulo the identities given in Figure 4.1.

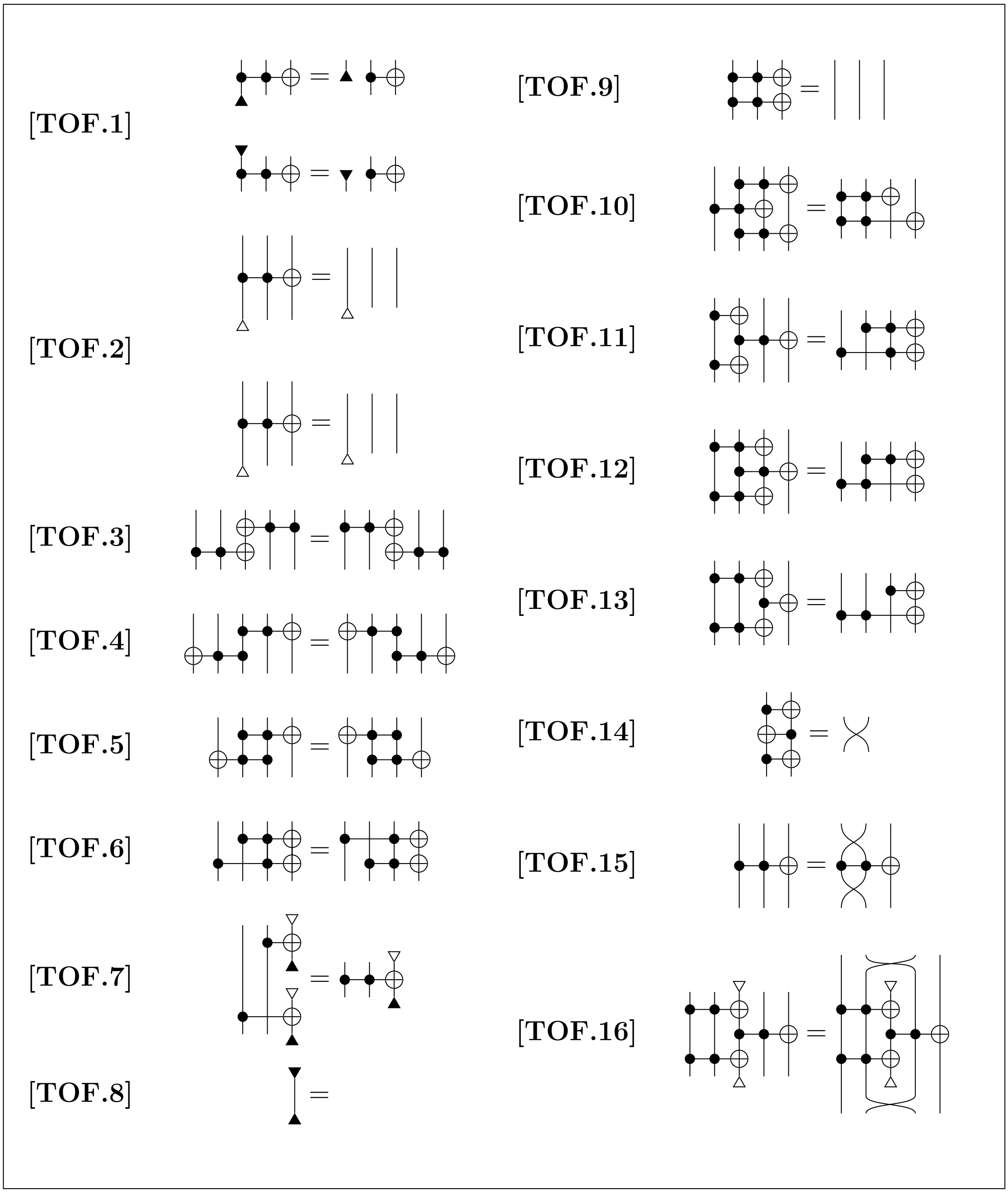
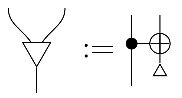


Figure 4.1: The identities of TOF

Lemma 4.8 ([CC19, Proposition 6.2])**.** TOF *is a discrete inverse category, where the partial inverse sends:*

$$\mathsf{tof} \mapsto \mathsf{tof}\ ,\ \ |0\rangle \mapsto \langle 0|\ ,\ \ \langle 0| \mapsto |0\rangle$$

The diagonal map on one wire is defined as follows:



Definition 4.9. Let FPinj_2, FPar_2 and FSpan_2 denote, respectively, the full subcategories of $\mathsf{ParIso}(\mathsf{Par}(\mathsf{FinOrd}))$, $\mathsf{Par}(\mathsf{FinOrd})$, $\mathsf{Span}^{\sim}(\mathsf{FinOrd})$ where the objects are powers of two.

Theorem 4.10 ([CC19, Theorem 10.6])**.** TOF *is isomorphic to* FPinj_2 *as a discrete inverse category.*

The interpretation of the generators we gave into $\mathsf{Mat}_{\mathbb{C}}$ can therefore be restated in terms of the ℓ^2 functor:

Corollary 4.11. TOF *embeds in* FHilb *via the* ℓ^2 *functor so that:*

$$\mathsf{TOF} \cong \mathsf{FPinj}_2 \hookrightarrow \mathsf{Pinj} \overset{\ell^2}{\rightarrowtail} \mathsf{FHilb}$$

4.2.1 Adding a unit and counit to TOF

Definition 4.12. Define $\widehat{\mathsf{TOF}}$ to be the pushout of the following diagram of props:

$$c(\mathsf{TOF})^{\mathsf{op}} \leftarrow \mathsf{TOF} \rightarrow c(\mathsf{TOF})$$

By adding a unit and counit, we obtain a full subcategory of spans of sets and finite ordinals:

Proposition 4.13. $\widehat{\mathsf{TOF}} \cong \mathsf{FSpan}_2$

Proof. Recall that TOF is presented by the subcategory FPinj_2 of $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ with morphisms of the form $2^n \overset{e}{\leftarrowtail} k \overset{e'}{\rightarrowtail} 2^m$ for arbitrary natural numbers n, m, k and monics e and e'.

Similarly, $\widetilde{\mathsf{TOF}}$ is presented by the subcategory FPar_2 of $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ with morphisms of the form $2^\ell \overset{f}{\leftarrow} 2^n \overset{e}{\leftarrowtail} k \overset{e'}{\rightarrowtail} 2^m$ for arbitrary natural numbers ℓ, n, m, k, monics e and e' and function f. Consider the pushout $\mathbb{X}$ of the following diagram of props:

$$\mathsf{FPar}_2^{\mathsf{op}} \leftarrowtail \mathsf{FPinj}_2 \rightarrowtail \mathsf{FPar}_2$$

Consider the functor $F : \mathbb{X} \to \mathsf{FSpan}_2$ induced by the universal property of the pushout. We show that this functor is an isomorphism. This functor is clearly the identity on objects. For fullness consider some span $2^n \overset{f}{\leftarrow} k \overset{g}{\rightarrow} 2^m$. We can construct a function $f' : 2^{\lceil \log_2 k \rceil} \to 2^n$ and monic $e_f : k \rightarrowtail 2^{\lceil \log_2 k \rceil}$ so that $f = e; f'$. Similarly, we can construct some $g' : 2^{\lceil \log_2 k \rceil} \to 2^n$ and monic $e_g : k \rightarrowtail 2^{\lceil \log_2 k \rceil}$ so that $g = e_g; g'$. Therefore:

$$F\left(\begin{tikzcd} & 2^{\lceil \log_2 k \rceil} \arrow[dl, "f'"'] \arrow[dr, equal] & \\ 2^n & & 2^{\lceil \log_2 k \rceil} \end{tikzcd} ; \begin{tikzcd} & k \arrow[dl, tail, "e_f"'] \arrow[dr, tail, "e_m"] & \\ 2^{\lceil \log_2 k \rceil} & & 2^{\lceil \log_2 k \rceil} \end{tikzcd} ; \begin{tikzcd} & 2^{\lceil \log_2 k \rceil} \arrow[dl, equal] \arrow[dr, "g'"] & \\ 2^{\lceil \log_2 k \rceil} & & 2^m \end{tikzcd} \right)$$

$$= \begin{tikzcd} & & & k \arrow[dl, equal] \arrow[dr, equal] \arrow[dll, phantom] \arrow[dd, phantom, "\smile"] \arrow[dddll, bend right, "f"'] \arrow[dddrr, bend left, "g"] & & & \\ & & k \arrow[dl, tail, "e_f"'] \arrow[dr, equal] \arrow[dd, phantom, "\smile"] & & k \arrow[dl, equal] \arrow[dr, tail, "e_g"] \arrow[dd, phantom, "\smile"] & & \\ & 2^{\lceil \log_2 k \rceil} \arrow[dl, "f'"] \arrow[dr, equal] & & k \arrow[dl, tail, "e_f"'] \arrow[dr, tail, "e_g"] & & 2^{\lceil \log_2 k \rceil} \arrow[dl, equal] \arrow[dr, "g'"'] & \\ 2^n & & 2^{\lceil \log_2 k \rceil} & & 2^{\lceil \log_2 k \rceil} & & 2^m \end{tikzcd}$$

So F is full. For faithfulness suppose we have two isomorphic spans in $F(\mathbb{X})$, which we can factorize as before:

$$\begin{tikzcd} & & k \arrow[dl, tail, "e_1"'] \arrow[dr, tail, "e_2"] \arrow[dddd, "\alpha", "\cong"'] & & \\ & 2^{n_2} \arrow[dl, "f_1"'] & & 2^{n_3} \arrow[dr, "f_2"] & \\ 2^{n_1} & & & & 2^{n_4} \\ & 2^{n'_2} \arrow[ul, "f'_1"] & & 2^{n'_3} \arrow[ur, "f'_2"'] & \\ & & k \arrow[ul, tail, "e'_1"] \arrow[ur, tail, "e'_2"'] & & \end{tikzcd}$$

In $\mathbb{X}$, we have:

$$\begin{tikzcd} & 2^{n_2} \arrow[dl, "f_1"'] \arrow[dr, equal] & \\ 2^{n_1} & & 2^{n_2} \end{tikzcd} ; \begin{tikzcd} & k \arrow[dl, tail, "e_1"'] \arrow[dr, tail, "e_2"] & \\ 2^{n_2} & & 2^{n_3} \end{tikzcd} ; \begin{tikzcd} & 2^{n_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n_3} & & 2^{n_4} \end{tikzcd}$$

$$= \begin{tikzcd} & & k \arrow[dl, tail, "e_1"'] \arrow[dr, equal] \arrow[dd, phantom, "\smile"] \arrow[ddll, bend right, "\alpha e'_1 f'_1"'] & & \\ & 2^{n_2} \arrow[dl, "f_1"'] \arrow[dr, equal] & & k \arrow[dl, tail, "e_1"'] \arrow[dr, tail, "e_2"] & \\ 2^{n_1} & & 2^{n_2} & & 2^{n_3} \end{tikzcd} ; \begin{tikzcd} & 2^{n_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n_3} & & 2^{n_4} \end{tikzcd}$$

$$= \begin{tikzcd} & & k \arrow[dl, tail, "\alpha e'_1"'] \arrow[ddrr, tail, "e_2"] & & \\ & 2^{n'_2} \arrow[dl, "f'_1"'] & & & \\ 2^{n_1} & & & & 2^{n_3} \end{tikzcd} ; \begin{tikzcd} & 2^{n_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n_3} & & 2^{n_4} \end{tikzcd}$$

$$= \begin{tikzcd} & 2^{n'_2} \arrow[dl, "f'_1"'] \arrow[dr, equal] & \\ 2^{n_1} & & 2^{n'_2} \end{tikzcd} ; \begin{tikzcd} & k \arrow[dl, tail, "\alpha e'_1"'] \arrow[dr, tail, "e_2"] & \\ 2^{n'_2} & & 2^{n_3} \end{tikzcd} ; \begin{tikzcd} & 2^{n_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n_3} & & 2^{n_4} \end{tikzcd}$$

$$= \begin{tikzcd} & 2^{n'_2} \arrow[dl, "f'_1"'] \arrow[dr, equal] & \\ 2^{n_1} & & 2^{n'_2} \end{tikzcd} ; \begin{tikzcd} & k \arrow[dl, tail, "\alpha e'_1"'] \arrow[dr, tail, "\alpha e'_2"] \arrow[dd, "\alpha", "\cong"'] & \\ 2^{n'_2} & & 2^{n'_3} \\ & k \arrow[ul, tail, "e'_1"] \arrow[ur, tail, "e'_2"'] & \end{tikzcd} ; \begin{tikzcd} & 2^{n'_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n'_3} & & 2^{n_4} \end{tikzcd}$$

$$= \begin{tikzcd} & 2^{n'_2} \arrow[dl, "f'_1"'] \arrow[dr, equal] & \\ 2^{n_1} & & 2^{n'_2} \end{tikzcd} ; \begin{tikzcd} & k \arrow[dl, tail, "e'_1"'] \arrow[dr, tail, "e'_2"] & \\ 2^{n'_2} & & 2^{n'_3} \end{tikzcd} ; \begin{tikzcd} & 2^{n'_3} \arrow[dl, equal] \arrow[dr, "f_2"] & \\ 2^{n'_3} & & 2^{n_4} \end{tikzcd}$$

Therefore $\mathsf{FSpan}_2 \cong \mathbb{X}$. To show that $\widehat{\mathsf{TOF}} \cong \mathsf{FSpan}_2$, consider the following diagram where each horizontal face is a pushout:

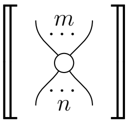
$$\begin{tikzcd}
 & (\mathsf{FPinj}_2, \times) \arrow[rr] \arrow[dl] \arrow[d, equal] & & (\mathsf{FPar}_2, \times) \arrow[d, "\cong"] \arrow[dl] \\
(\mathsf{FPar}_2, \times)^{\mathsf{op}} \arrow[rr, bend right] \arrow[d, "\cong"'] & (\mathsf{FPinj}_2, \times) \arrow[rr, bend left] \arrow[d, "\cong"] \arrow[dl] & (\mathsf{FSpan}_2, \times) \arrow[d, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \widetilde{(\mathsf{FPinj}_2, \times)} \arrow[d, "\cong"] \arrow[dl] \\
\widetilde{(\mathsf{FPinj}_2, \times)}^{\mathsf{op}} \arrow[rr, bend right] \arrow[d, "\cong"'] & \mathsf{TOF} \arrow[rr, bend left] \arrow[d, equal] \arrow[dl] & {} \arrow[d, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \widetilde{\mathsf{TOF}} \arrow[d, "\cong"'] \arrow[dl] \\
\widetilde{\mathsf{TOF}}^{\mathsf{op}} \arrow[rr, bend right] \arrow[d, "\cong"'] & \mathsf{TOF} \arrow[rr, bend left] \arrow[dl] & {} \arrow[d, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & c(\mathsf{TOF}) \arrow[dl] \\
c(\mathsf{TOF})^{\mathsf{op}} \arrow[rr, bend right] & & \widehat{\mathsf{TOF}} \arrow[ul, phantom, "\ulcorner", very near start] &
\end{tikzcd}$$

All of the rear and left faces commute. Moreover, the non-universal vertical maps are isomorphisms, therefore the maps induced by universal property of the pushout are isomorphisms. □

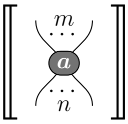
The pushout cube used in the preceeding proof is very similar in spirit to the pushout cubes previously used to construct categories of relations, for example in the Ph.D. thesis of Zanasi [Zan18] and the paper of Zanasi and Fong [FZ17]. However, our semantics is different, we construct a full subcategory of *spans*, not relations. It is not clear if there is a deeper connection which can be made.

We give a more elegant presentation of this category in terms of interacting monoids and comonoids:

Definition 4.14. The †-compact closed prop $\mathsf{ZX}\&$ is presented by phase-free Z-spiders, $\mathbb{Z}/2\mathbb{Z}$-phased X-spiders and the and-gate. These generators are interpreted in $\mathsf{Mat}_{\mathbb{C}}$ as follows:

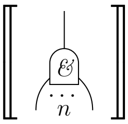


$$= \sum_{j=0}^{1} |j,\ldots,j\rangle\langle j,\ldots,j|$$



$$= \sqrt{2}\sum_{j=0}^{1} e^{2\cdot\pi\cdot i\cdot j\cdot a/2}\mathcal{F}|j,\ldots,j\rangle\langle j,\ldots,j|\mathcal{F}^{\dagger}$$

$$= \sum_{\sum x_i=\sum y_j+a \mod 2} |y_1,\ldots,y_n\rangle\langle x_1,\ldots,x_n|$$



$$= |a_0\cdot\ldots\cdot a_{n-1}\rangle\langle a_0,\cdots,a_{n-1}|$$

subject to the identities in Figure 4.2:

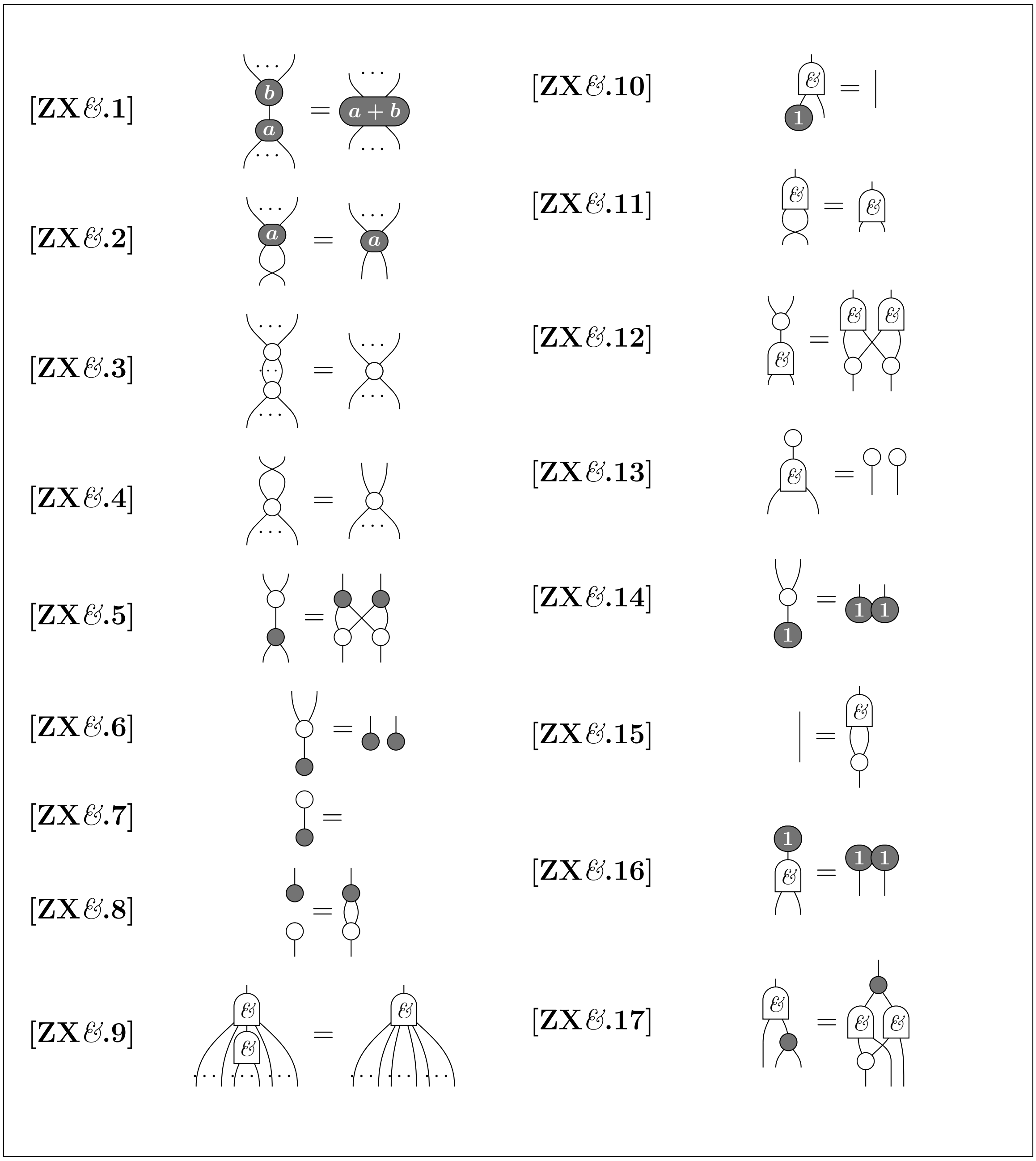
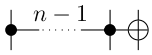


Figure 4.2: The identities of ZX&, for $a, b \in \mathbb{Z}/2\mathbb{Z}$

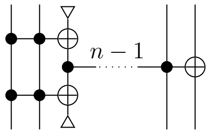
Before we prove there is a functor from ZX& to $\widehat{\mathsf{TOF}}$ we recall some basic properties of TOF. In TOF, one can construct controlled-not gates with arbitrarily many control wires using ladders of Toffoli gates:

Definition 4.15. A **generalized controlled-not gate** on n wires is denoted by

$\llparenthesis x, X \rrparenthesis$, where X indexes a subset of the n wires, and x is an index for precisely one wire such that $x \notin X$. Draw a generalized controlled-not gates $\llparenthesis x, X \rrparenthesis$ on n wires where x is the last wire and $|X| = n - 1$ as follows:



These gates are defined by induction on the number of wires. For the base case of $n = 1$ it is the `not` gate. For $n \geq 3$, then generalized controlled-not gate on $n + 1$ wires is defined as follows:



As a consequence, the generalized controlled-gate is `cnot` for $n = 2$ and `tof` for $n = 3$.

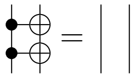
We can partially commute generalized controlled-not gates:

Lemma 4.16 ([IKY02, Section 3 (3)]). *Let $\llparenthesis x, X \rrparenthesis$ and $\llparenthesis y, Y \rrparenthesis$ be generalized controlled-not gates in* `TOF` *where $x \notin Y$. By completeness of* `TOF`*, we can commute them past each other with a trailing generalized controlled-not gate as a side effect:*

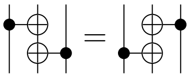
$$\llparenthesis x, X \rrparenthesis ; \llparenthesis y, \{x\} \sqcup Y \rrparenthesis = \llparenthesis y, X \cup Y \rrparenthesis ; \llparenthesis y, Y \sqcup \{x\} \rrparenthesis ; \llparenthesis x, X \rrparenthesis$$

The following equations hold in `TOF`:

Lemma 4.17 ([CCS18, Lemma 4.1]).

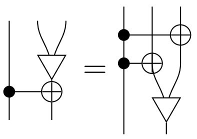


Lemma 4.18 ([CCS18, Lemma 4.1]).



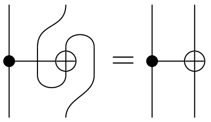
The diagonal map is natural on target qubits:

Lemma 4.19 ([Com19, Lemma B.0.2 (iii)]).

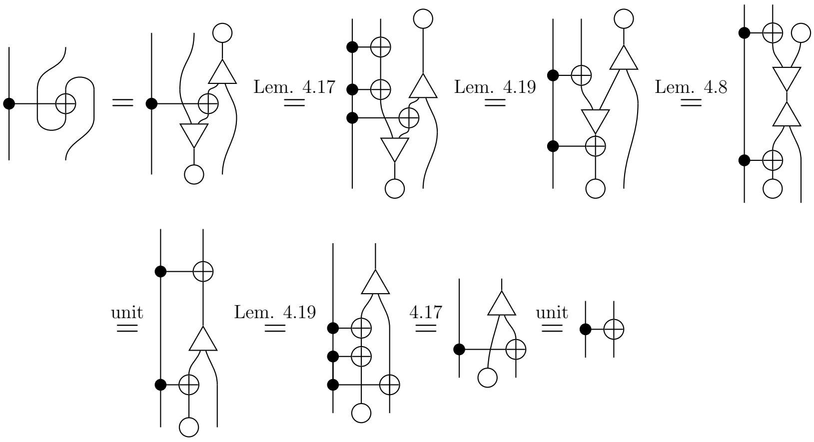


We also establish some basic properties of $\widehat{\mathsf{TOF}}$. First, the cnot gate is its own mate on the second wire:

Lemma 4.20.



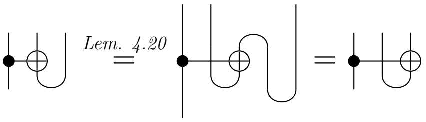
Proof.



□

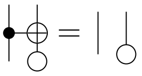
Therefore,

Lemma 4.21.

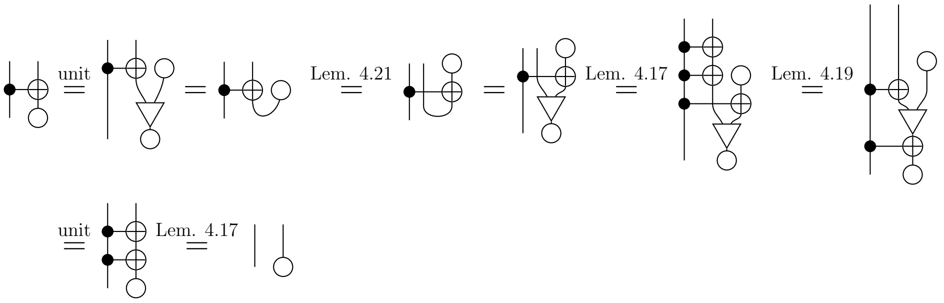


Thus

Lemma 4.22.

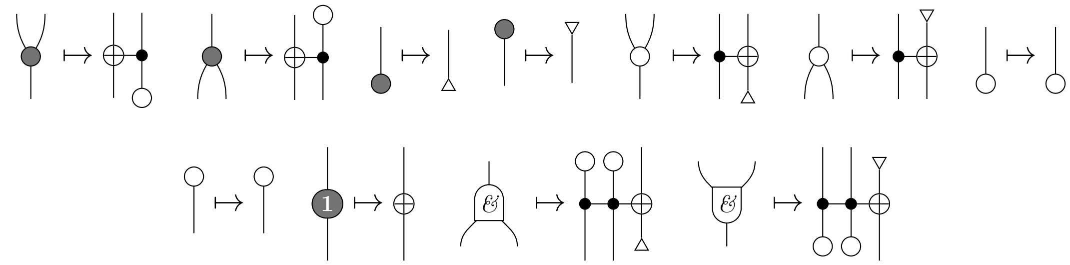


Proof.



□

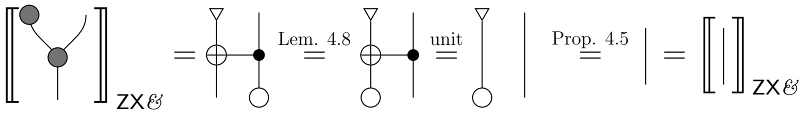
Proposition 4.23. *Consider the interpretation* $\llbracket \_ \rrbracket_{\mathsf{ZX}\&} : \mathsf{ZX}\& \to \widehat{\mathsf{TOF}}$ *taking:*



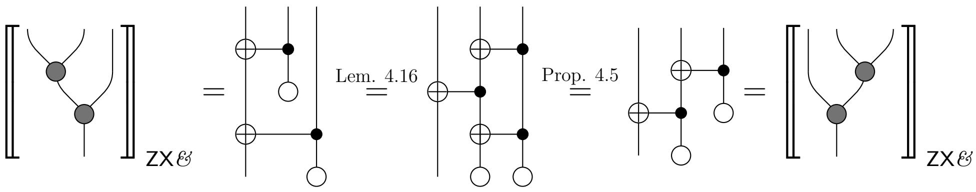
This interpretation is a strict symmetric †-monoidal functor.

Proof. We prove that all of the axioms of $\mathsf{ZX}\&$ hold in $\widehat{\mathsf{TOF}}$:

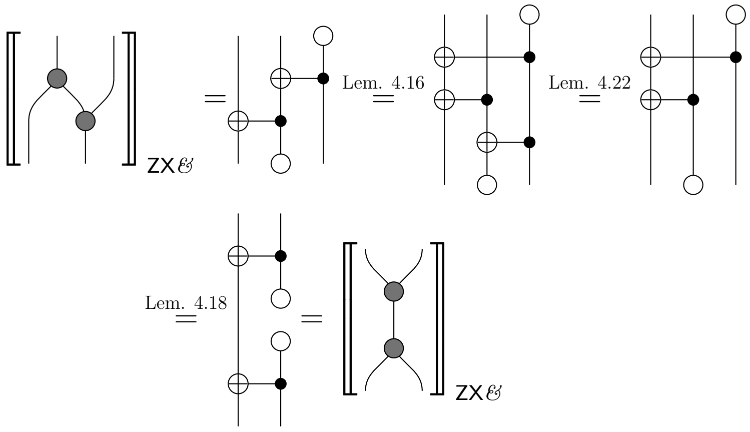
[ZX&.1]: **Unitality:** By Lemma 4.22:



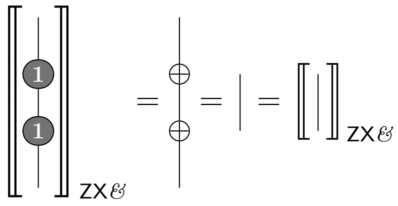
Associativity:



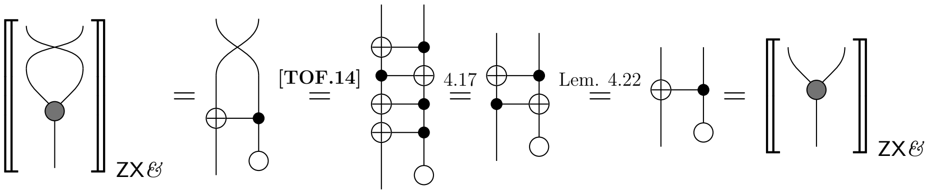
Frobenius:



Phase amalgamation:



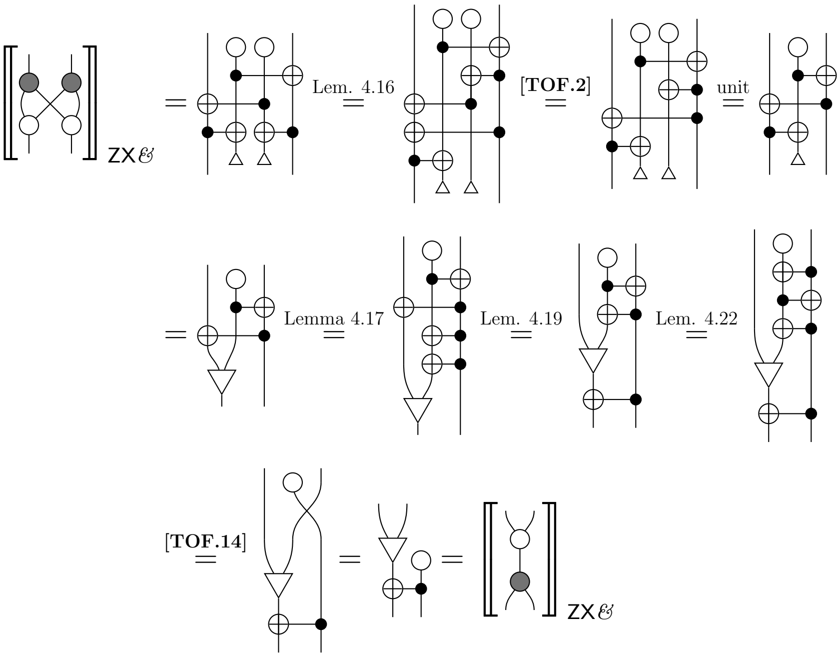
[ZX&.2]:



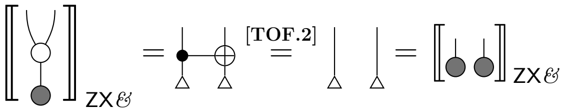
[ZX&.3]: This is immediate.

[ZX&.4]: This is immediate.

[ZX&.5]:

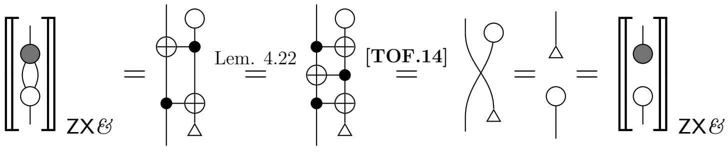


[ZX&.6]:

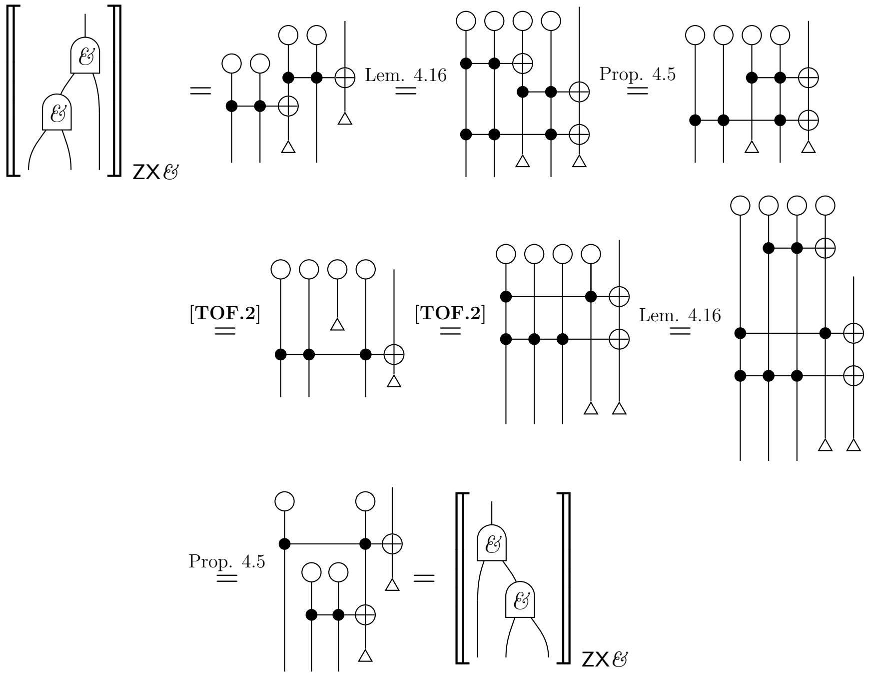


[ZX&.7]: This is immediate.

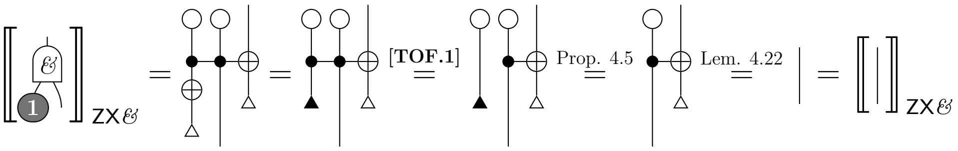
[ZX&.8]:



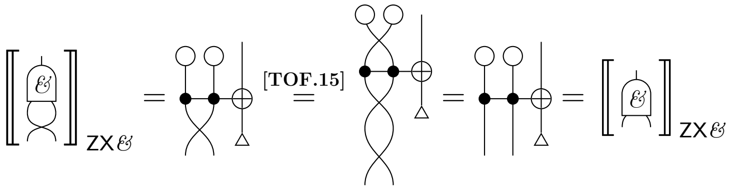
[ZX&.9]:



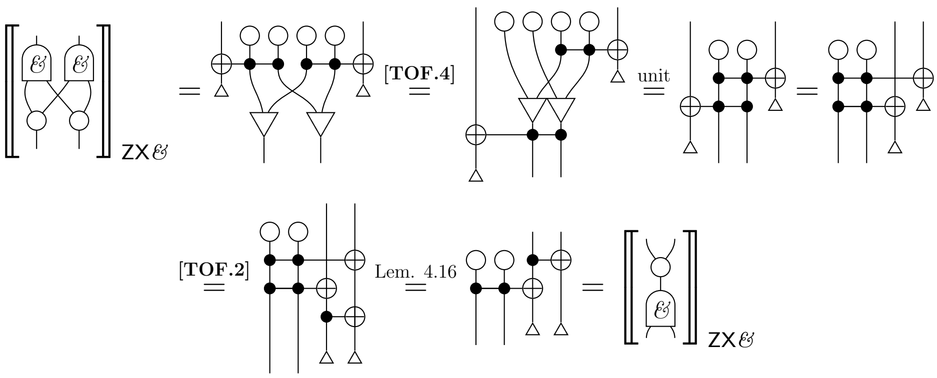
[ZX&.10]:



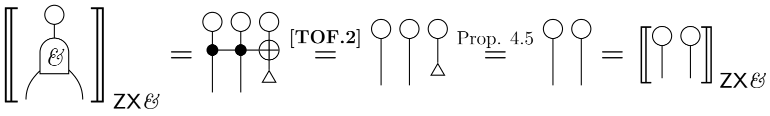
[ZX&.11]:



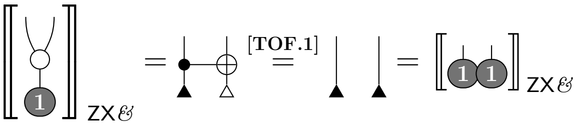
[ZX&.12]:



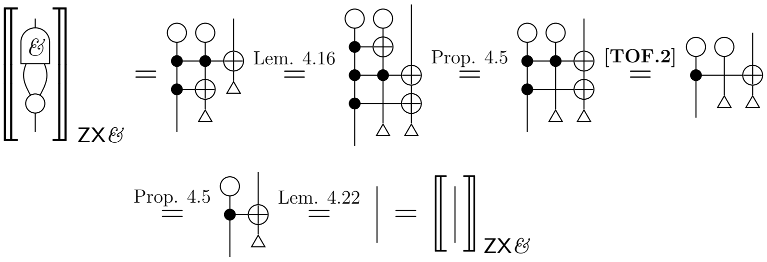
[ZX&.13]:



[ZX&.14]:

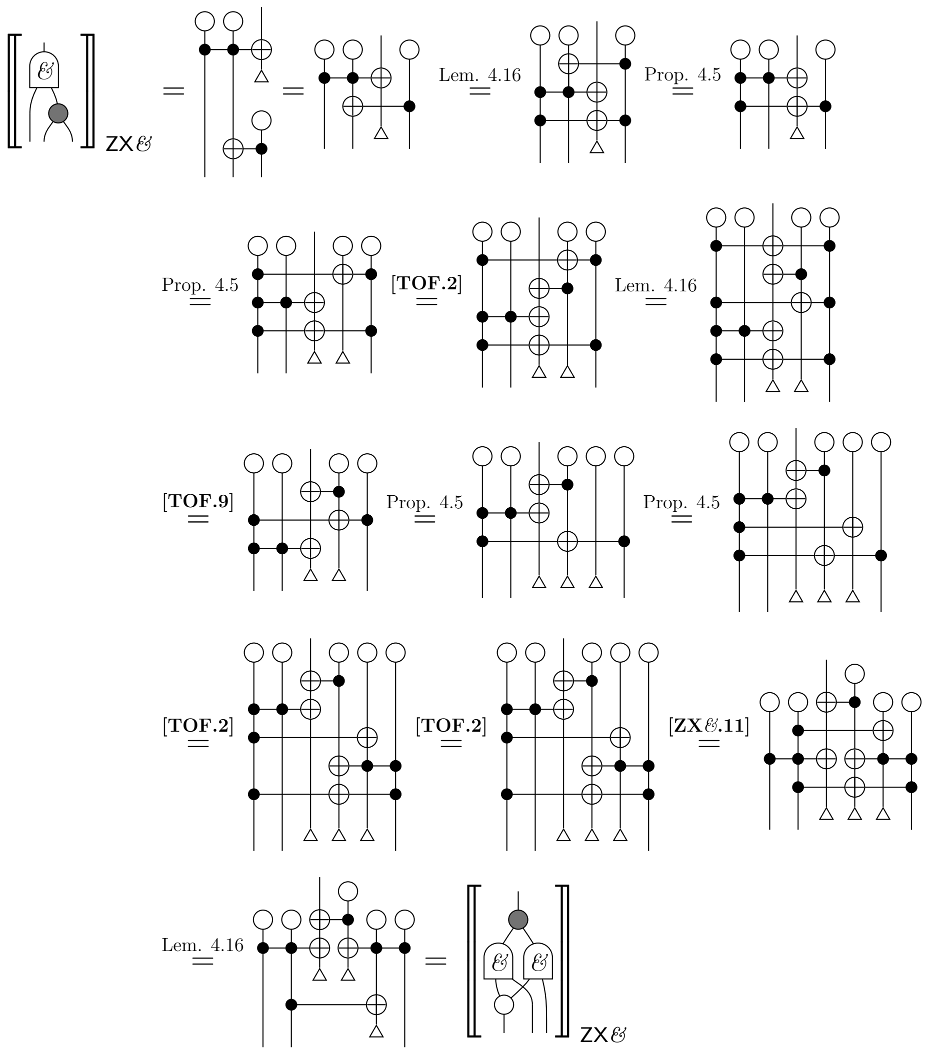


[ZX&.15]:



[ZX&.16]: This is precisely **[TOF.7]**.

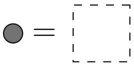
[ZX&.17]:



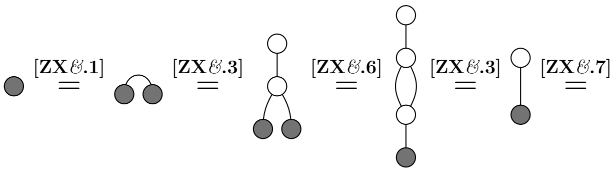
□

To prove functoriality in the other direction, we expose some basic properties of ZX&.

Lemma 4.24.

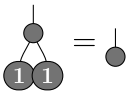


Proof.

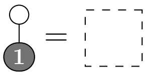


□

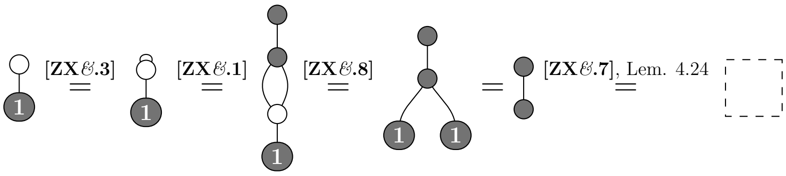
Lemma 4.25. *The phase fusion of the grey spider in* ZX&*,*



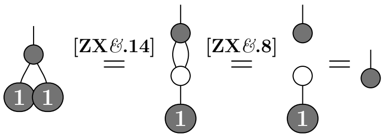
in the presence of the other axioms is equivalent to asserting:



Proof. For the one direction, suppose that phase fusion holds:

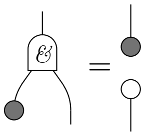


Conversely:

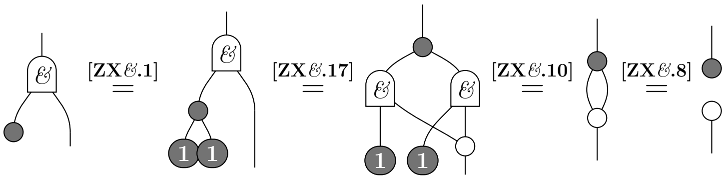


∎

Lemma 4.26.

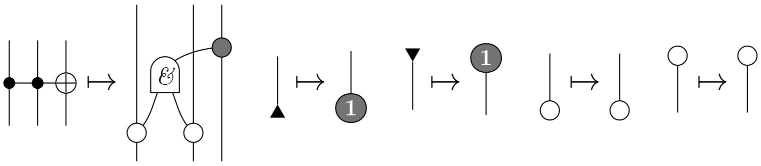


Proof.



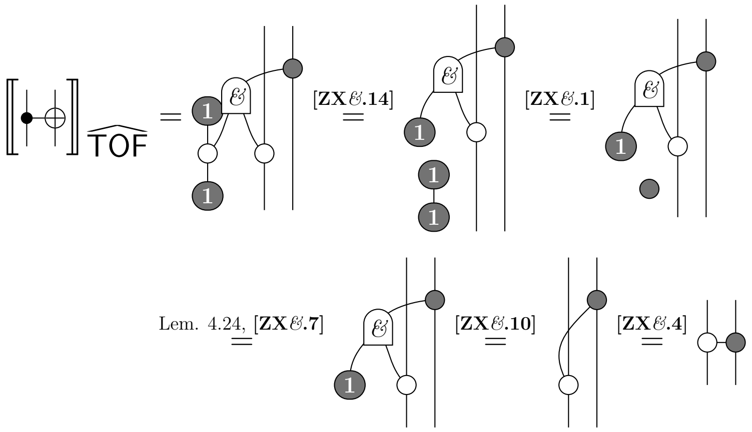
∎

Proposition 4.27. *Consider the interpretation* $[\![\_]\!]_{\widehat{\mathsf{TOF}}} : \widehat{\mathsf{TOF}} \to \mathsf{ZX}\&$ *taking:*

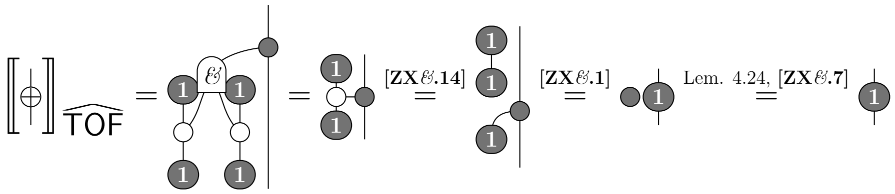


This interpretation is a strict symmetric †-monoidal functor.

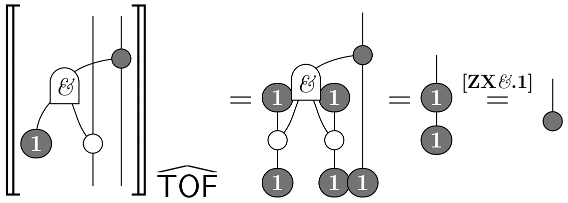
Proof. First, observe:



Thus:

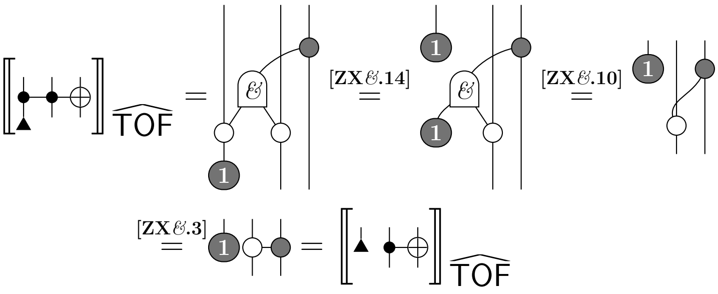


Thus:

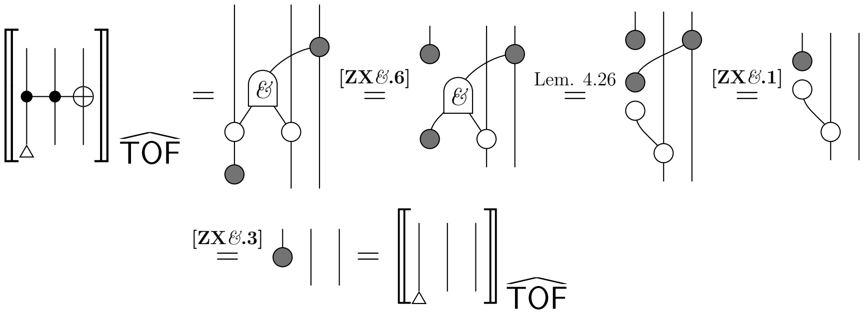


We prove that all of the axioms of $\widehat{\mathsf{TOF}}$ hold in ZX& :

[TOF.1]:

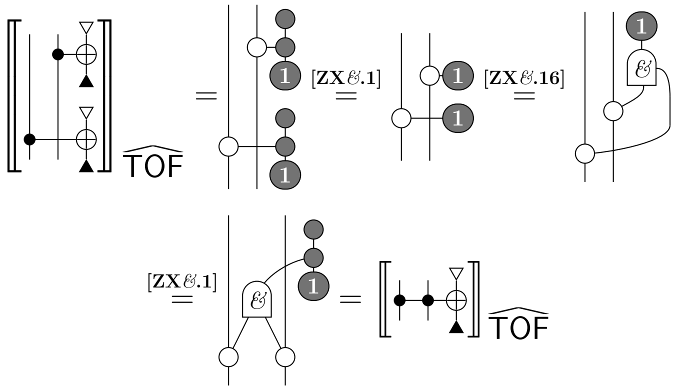


[TOF.2]:



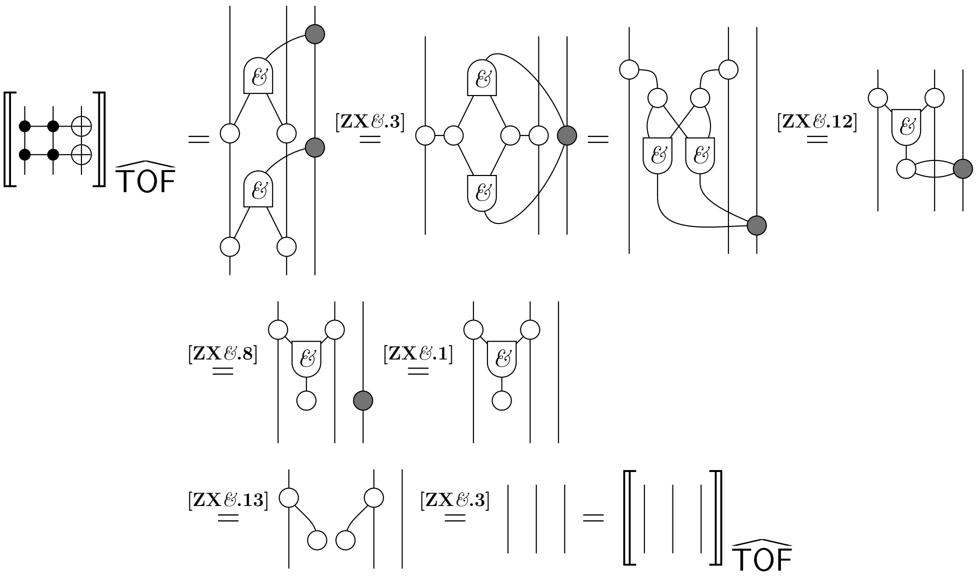
[TOF.3]-[TOF.6]: follow from the spider law.

[TOF.7]:

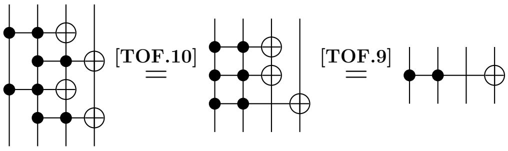


[TOF.8]: This follows immediately from Lemma 4.24 and **[ZX&.7]**.

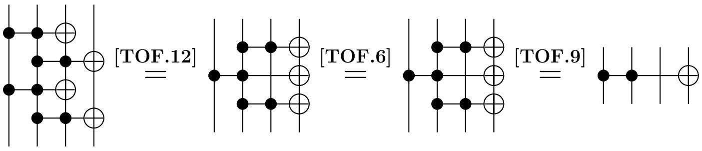
[TOF.9]:



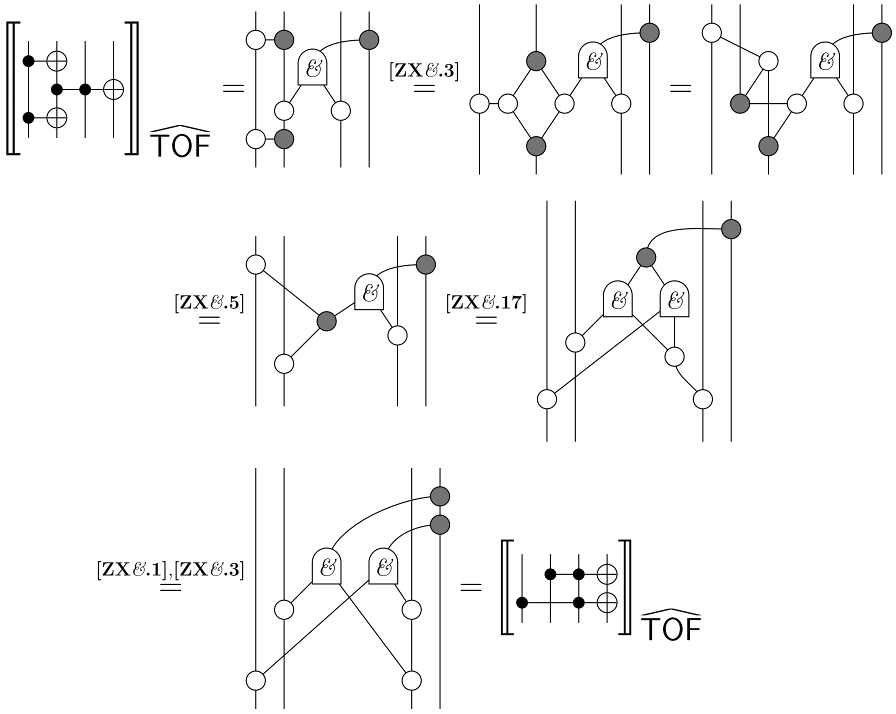
[TOF.10]: It is easier to prove that [**TOF.10**] is redundant. Given [**TOF.9**], [**TOF.6**] and [**TOF.12**], [**TOF.10**] is equivalent to the following:



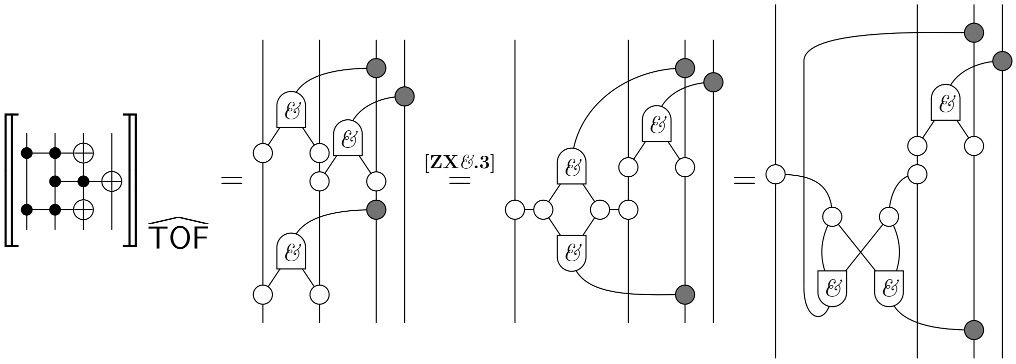
However

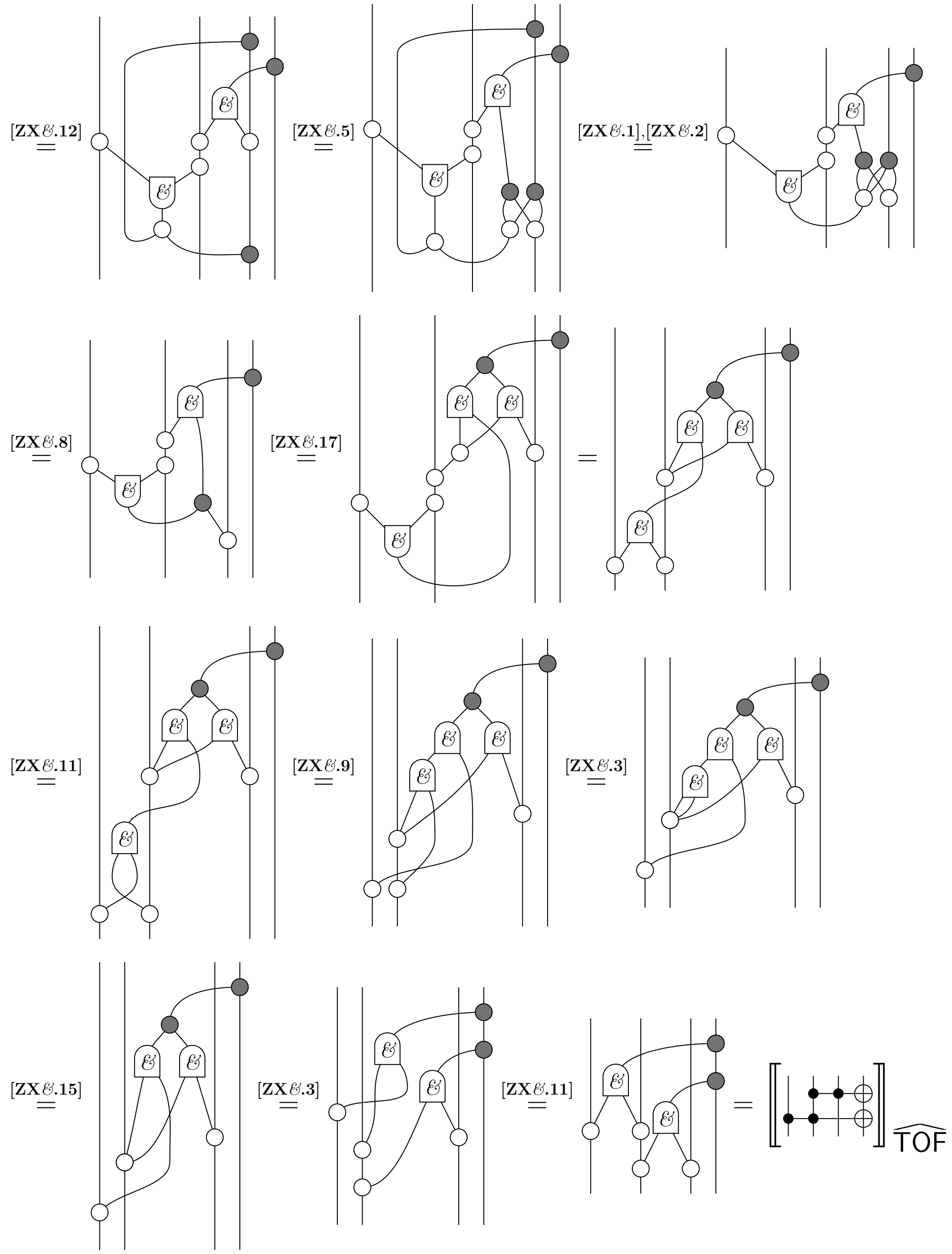


[TOF.11]:

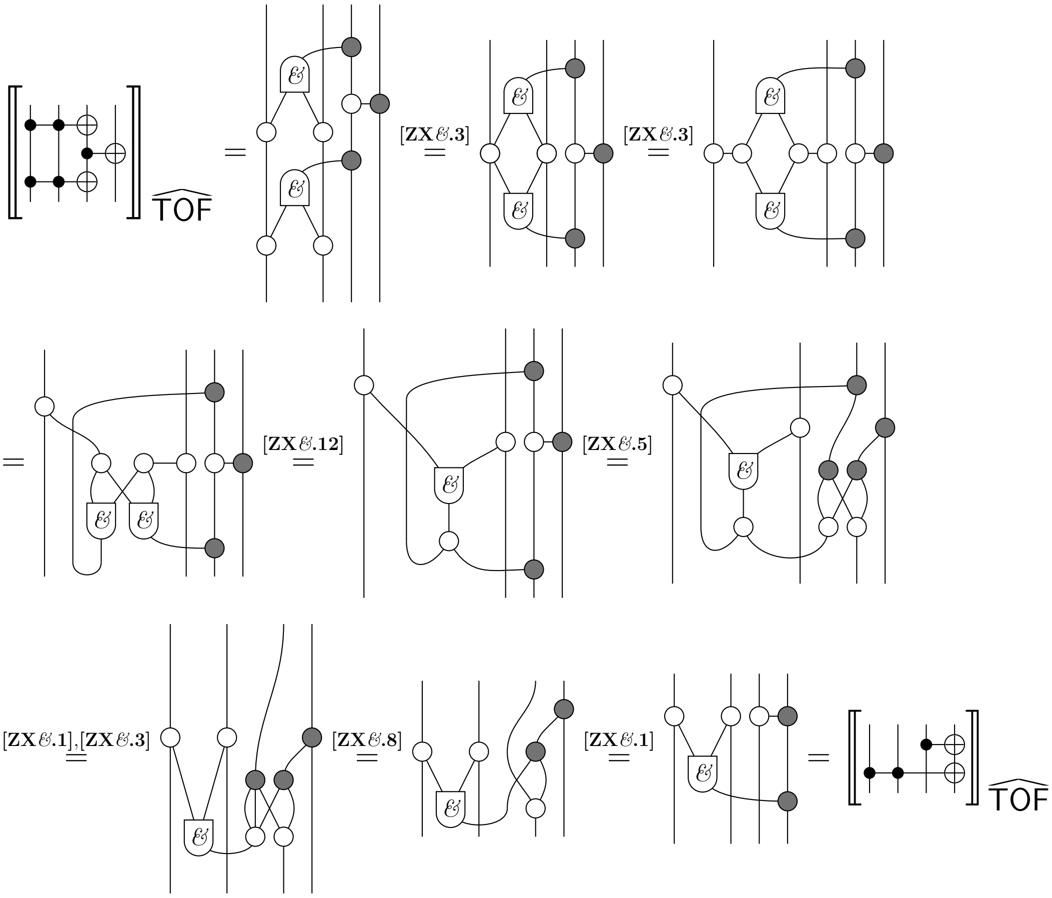


[TOF.12]:

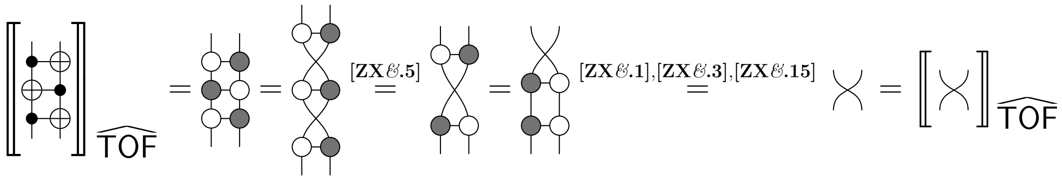



[ZX&.12] =
[ZX&.5] =
[ZX&.1],[ZX&.2] =
[ZX&.8] =
[ZX&.17] =
=
[ZX&.11] =
[ZX&.9] =
[ZX&.3] =
[ZX&.15] =
[ZX&.3] =
[ZX&.11] =
=
TOF

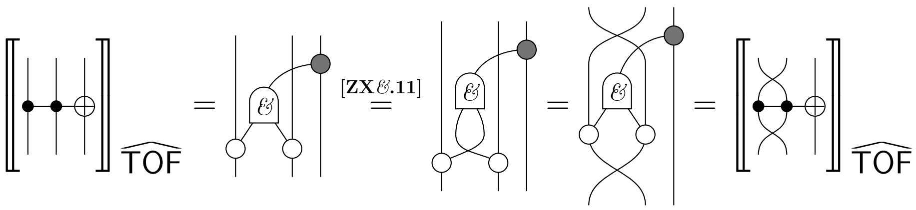
[TOF.13]:



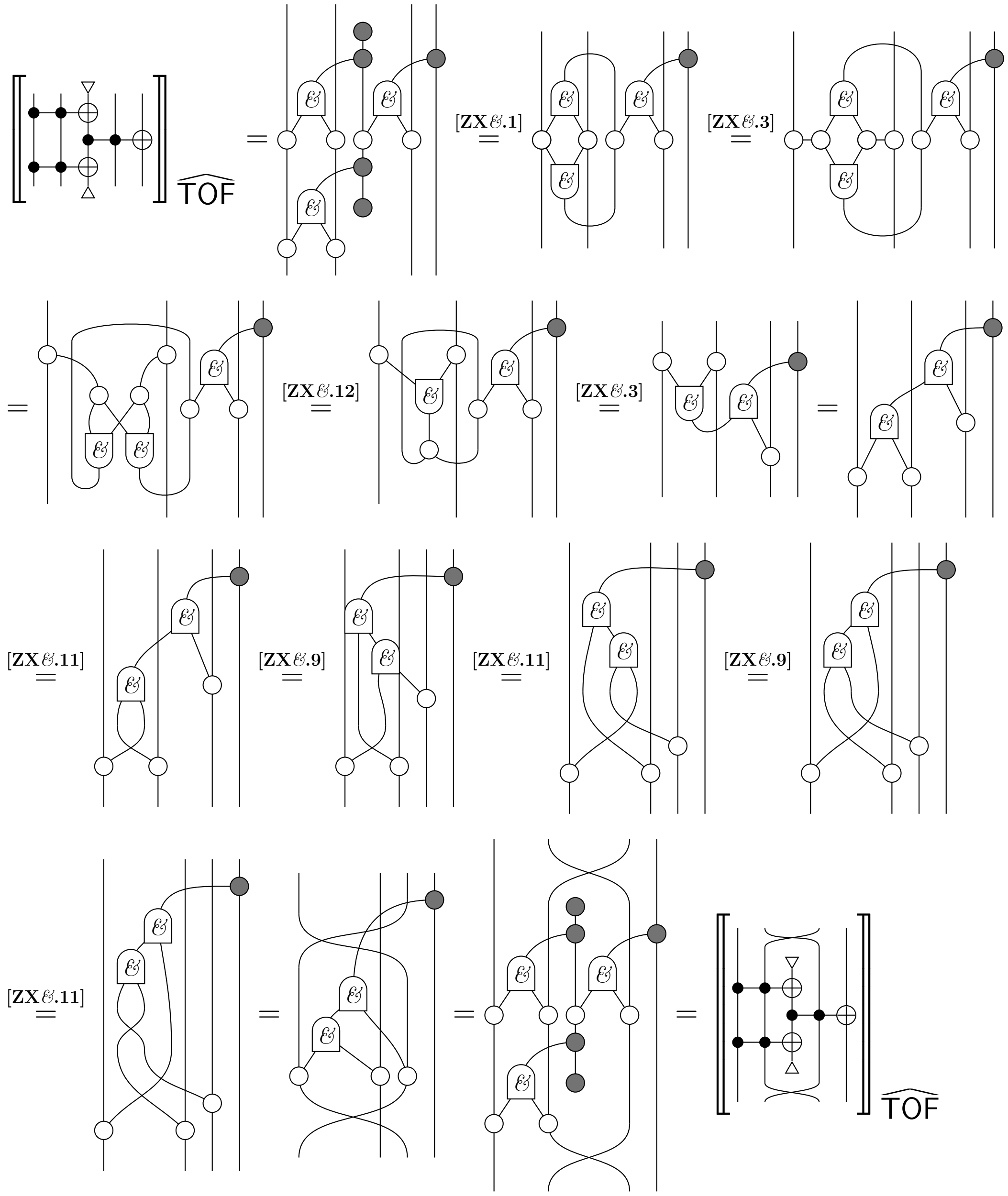
[TOF.14]:



[TOF.15]:



[TOF.16]:

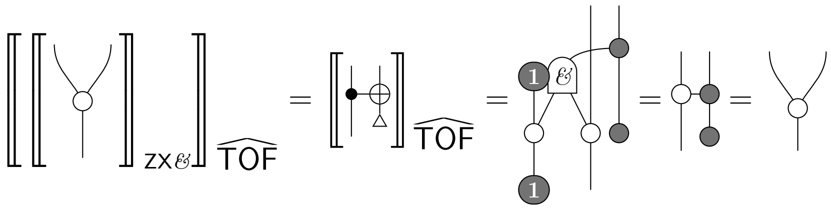


Unitality and counitality follow from the fact that the white spiders are Frobenius algebras. ☐

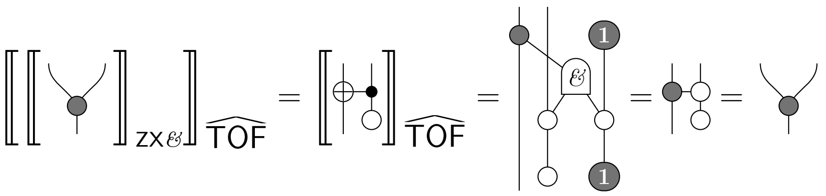
Theorem 4.28. *The interpretation functors* $[\![-]\!]_{\mathsf{ZX\&}}$ *and* $[\![-]\!]_{\widehat{\mathsf{TOF}}}$ *are inverses, so that* $\widehat{\mathsf{TOF}}$ *and* $\mathsf{ZX\&}$ *are isomorphic as †-compact closed props.*

Proof. First we show that $[\![[\![1]\!]_{\mathsf{ZX\&}}]\!]_{\widehat{\mathsf{TOF}}} = 1$:

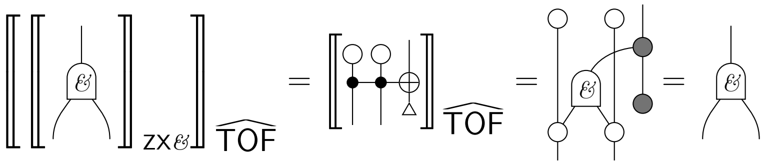
For the white spider: The case for the unit and counit is trivial. For the (co)multiplication we have:



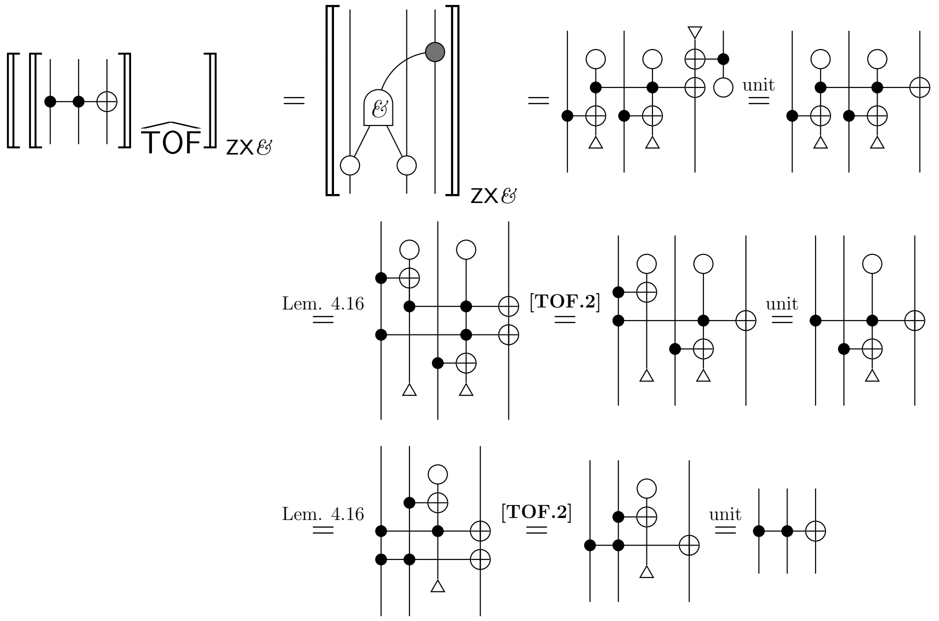
For the grey spider: The cases for the unit, counit and 1 phase are trivial. For the (co)multiplication we have:



For the and gate:



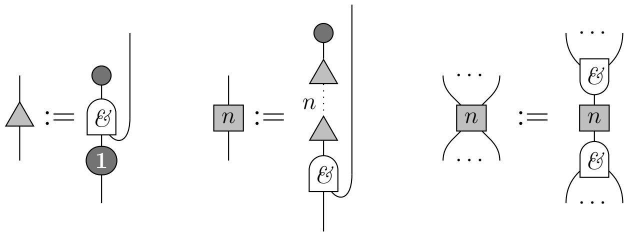
Next, we show that $[\![[\![-]\!]_{\widehat{\mathsf{TOF}}}]\!]_{\mathsf{ZX}\&} = 1$: The ancillae are trivial. For the Toffoli gate:



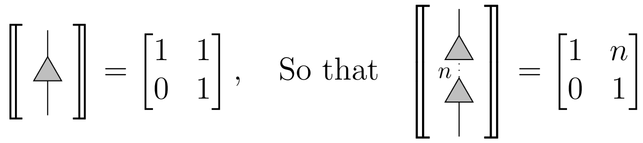
□

ZX& is the natural-number labelled fragment of the qubit ZH-calculus:

Remark 4.29. The triangle gate and H-boxes have the following interpretation in ZX&, for $n \in \mathbb{N}$:



where the triangle gate is interpreted as:

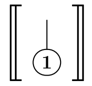


A presentation of “qubit relations [2] ” follows immediately from our characterization of ZX& in terms of the natural number-labeled fragment of the qubit ZH-calculus:

Corollary 4.30. *Consider the following 2-cells in* ZX&*:*

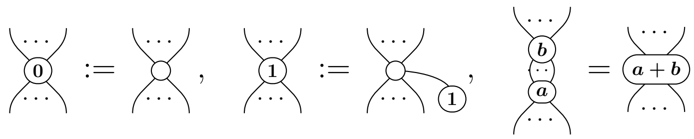
Quotienting by either of these two cells yields the prop ZX&/ ∼ *which is complete for the full subcategory relations between finite sets where the objects are powers of two, or equivalently the full subcategory of* $\mathsf{Mat}_{\mathbb{B}}$ *where the objects are powers of two. This is the posetal collapse of* ZX&*.*

If we could express the H-box labeled by -1 as well as the scalar $1/\sqrt{2}$, this would give us the phase-free ZH-calculus (which we recall from Definition 3.36). These obviously don't live in ZX&; however, if we add the unnormalized minus state to our semantics



$$= \sqrt{2}\mathcal{F}|1\rangle = |-\rangle = (1,-1)^T$$

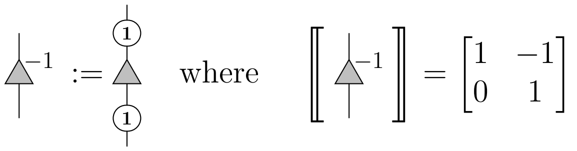
so that the Z-spiders are also phased by $a, b \in \mathbb{Z}/2\mathbb{Z}$:



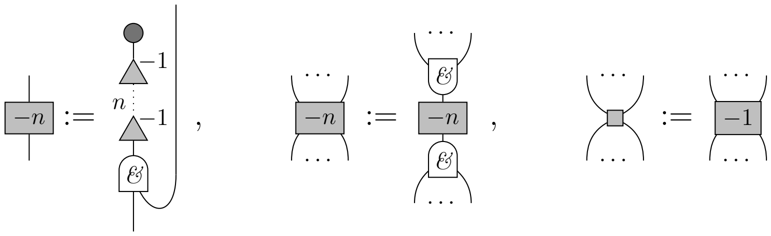
---

[2] I thank Robin Piedeleu for asking me if this can be done.

Then we can construct the inverse of the triangle gate by conjugation with $\mathcal{Z}$ gates:

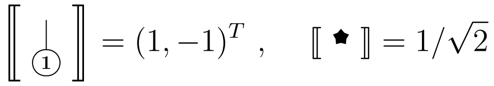


So that now for $n \in \mathbb{N}$:

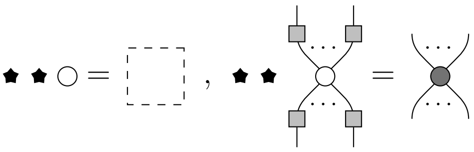


Therefore, by translating the presentation of the phase-free ZH-calculus of van de Wetering and Wolffs [WW19], we have immediately:

Corollary 4.31. *The prop presented by the generators and relations of* ZX& *in addition to the two extra generators interpreted in* $\mathsf{Mat}_{\mathbb{Z}[1/\sqrt{2}]}$ *as:*



modulo the equations:



is isomorphic to the phase-free ZH-calculus, where the integer-labeled H-boxes are derived generators.

This translation is trivial compared to the translation between ZX& and $\widehat{\mathsf{TOF}}$ because all of the axioms of the phase-free ZH-calculus are inspired by Boolean formulae; except for two. The first axiom we impose expresses the fact that $1/\sqrt{2}$ is invertible. The second relates addition and copying via Fourier transform. The phase-free ZH-calculus is already known to be approximately universal for qubits, so it is quite remarkable that our classical presentation of ZX& needs so little to be so quantum.

Because of the way we proved completeness for natural number qubit matrices, perhaps there is a more direct way to get around adding the scalar $1/\sqrt{2}$ to get a presentation for qubit matrices over $\mathbb{Z}$.

4.3 Decomposing Boolean circuits

In this section, we modularly build up to the prop $\mathsf{ZX}\&$ by taking distributive laws and pushouts of smaller symmetric monoidal theories. Along the way, we obtain various fragments of quantum circuits with partial, reversible and partially reversible semantics.

We use the machinery of distributive laws of monads in $\mathsf{Prof}(\mathsf{Mon})^{\mathsf{op}}$ discussed in Section 2.3. In the literature, props are usually decomposed according to orthogonal factorization systems, or more generally factorization systems over subgroupoids. However, we have to work in the more general setting of a factorization system over subcategories of subobjects. As discussed in Definition 2.108 and Lemma 2.108, the mathematical machinery already exists to do this. The original motivation of Cheng was to capture distributive laws of Lawvere theories and had nothing to do with subobjects [Che20].

We hope that the techniques used in this section can lead to presentations of other full subcategories of $\mathsf{Mat}_{\mathbb{N}}$ and $\mathsf{Mat}_{\mathbb{B}}$ which could eventually help prove the completeness of qudit fragments of the ZH-calculus.

Many of the fragments which we consider have already been given presentations by Lafont using more traditional methods [Laf03]. In these cases, we will try to present them in terms of distributive laws and give the appropriate citation to him.

Because we want to compose everything using distributive laws and pushouts, note that the counital completion of a discrete inverse prop $\mathbb{X}$ is the following pushout of props:

$$\mathbb{X} \leftarrow \mathsf{surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

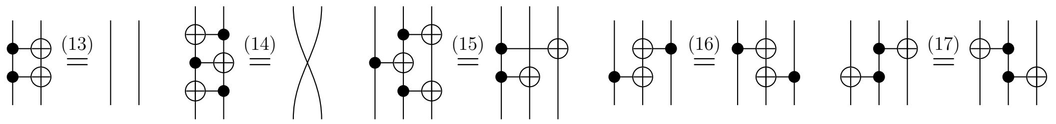
That is to say, it picks out the diagonal map of $\mathbb{X}$ and adds a counit. As a matter of notation, as we have been doing throughout this thesis, we will colour this comonoid and its components ○.

We recall some notation from all the way back in Section 2.2. $\mathsf{Inv}(\mathbb{X})$ denotes the subcategory of partial isomorphisms of a restriction category. $\mathsf{Iso}(\mathbb{X})$ denotes the category of isomorphisms in a category $\mathbb{X}$. $\mathsf{Par}(\mathbb{X})$ denotes the discrete Cartesian restriction category of partial maps $\mathbb{X}$. $\mathsf{ParIso}(\mathbb{X})$ denotes the discrete inverse category of spans of monorphisms in $\mathbb{X}$. Moreover, denote the category of monomorphisms in $\mathbb{X}$ by $\mathsf{Mono}(\mathbb{X})$.

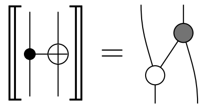
4.3.1 The phase-free fragment

hinery already exists to do th In this subsection we build up to giving a presentation for $(\mathsf{Span}^{\sim}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$ in a modular way. This category is shown to be the same as the phase-free of the ZX-calculus on the nose (not just up to invertible scalars). Note that a presentation for the full category of linear spans has already been discussed in great detail for arbitrary PIDs in Zanasi's Ph.D. thesis [Zan18]. First, we construct the linear isomorphisms:

Definition 4.32. Consider the prop $\mathsf{iscb}_{\mathbb{F}_2}$ generated by the controlled not gate modulo the following relations:

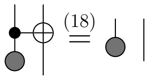


Lemma 4.33 ([Laf03, Theorem 6])**.** $\mathsf{iscb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Iso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$ *with respect to the interpretation:*



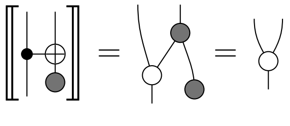
In fact, this result can be generalized to an arbitrary field [Laf03, Figure 37]. Adding the $|0\rangle$ state yields linear injections:

Definition 4.34. Consider the prop $\mathsf{incb}_{\mathbb{F}_2}$ generated by the coproduct of props $\mathsf{iscb}_{\mathbb{F}_2} + \mathsf{inj}$ modulo the equation:



Lemma 4.35 ([Laf03, Theorem 7])**.** $\mathsf{incb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Mono}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$

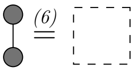
The white comultiplication can be derived in this fragment:



By adding the effect $\langle 0|$ we get linear partially reversible semantics:

Lemma 4.36. *There is a distributive law of props:*

$$\mathsf{piscb}_{\mathbb{F}_2} := \mathsf{incb}^{\mathsf{op}}_{\mathbb{F}_2} \otimes_{\mathsf{iscb}_{\mathbb{F}_2}} \mathsf{incb}_{\mathbb{F}_2};$$

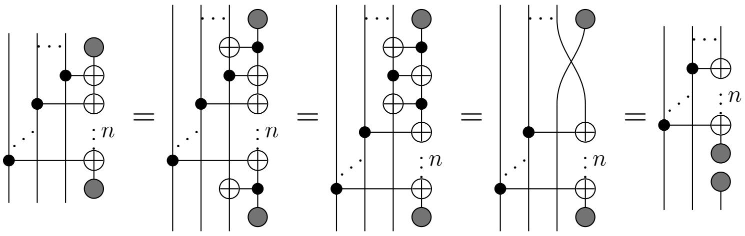


Proof. We can always slide things past each other, except for the critical pair when controlled not gates are sandwiched by a grey unit and counit on their target wires.

Take n to be the number of controlled not gates targeting the same wire, sandwiched by a grey unit and counit.

For the base case of $n = 0$, this follows from the Axiom (6) which we imposed.

Suppose that the claim holds for some $n \in \mathbb{N}$. If $n+1$-cnot gates have their targets sandwiched between a grey unit and counit without loss of generality, we can assume they are controlled from different wires. This is because cnot gates are self-inverse, so that they can be slid together and cancel out. So given $n+1$ cnot gates controlled on different wires and targeting the final wire:



$\square$

Lemma 4.37. $\mathsf{piscb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$*.*

Proof. $\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2})$ is the category of spans of monorphisms in $\mathsf{Mat}_{\mathbb{F}_2}$. This equation is precisely the one needed to compute the pullback. $\square$

We can get partial linear maps by adding the effect $\sqrt{2}\langle +|$:

Definition 4.38. Let $\mathsf{prcb}_{\mathbb{F}_2}$ denote the pushout of the diagram of props:

$$\mathsf{piscb}_{\mathbb{F}_2} \leftarrow \mathsf{surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Adding a counit to the white comultiplication.

Lemma 4.39. $\mathsf{prcb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$*.*

Proof. We show that the following diagram commutes and that the vertical maps are isomorphisms:

$$\begin{tikzcd}
& \mathsf{surj}^{\mathsf{op}} \arrow[rr] \arrow[dl] \arrow[dd, equal] & & \mathsf{cm}^{\mathsf{op}} \arrow[dl] \arrow[dd, equal] \\
\mathsf{piscb}_{\mathbb{F}_2} \arrow[rr] \arrow[dd, "\cong"'] & & \mathsf{prcb}_{\mathbb{F}_2} \arrow[dd, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \\
& \mathsf{surj}^{\mathsf{op}} \arrow[rr] \arrow[dl] & & \mathsf{cm}^{\mathsf{op}} \arrow[dl] \arrow[ddl, bend left] \\
(\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) \arrow[rr] \arrow[drr, bend right] & & {} \arrow[d, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \\
& & (\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) &
\end{tikzcd}$$

Because $\mathsf{Mat}_{\mathbb{F}_2}$ is Cartesian, $\mathsf{piscb}_{\mathbb{F}_2} \cong \mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2})$ is a discrete inverse category. We know that the counital completion of a discrete inverse category is the same as its Cartesian completion from Proposition 4.5; moreover, the Cartesian completion of $\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2})$ is $\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2})$. So this diagram commutes as a consequence. $\square$

By adding the state $\sqrt{2}|+\rangle$ we obtain the prop of linear spans:

Definition 4.40. Let $\mathsf{spcb}_{\mathbb{F}_2}$ denote the pushout of the diagram of props:

$$\mathsf{prcb}_{\mathbb{F}_2}^{\mathsf{op}} \leftarrow \mathsf{piscb}_{\mathbb{F}_2} \rightarrow \mathsf{prcb}_{\mathbb{F}_2}$$

Lemma 4.41. $\mathsf{spcb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Span}^{\sim}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$.

Proof. We show that the following diagram commutes and that the vertical maps are isomorphisms:

$$\begin{tikzcd}
{} & & \mathsf{piscb}_{\mathbb{F}_2} \arrow[rrr] \arrow[dll] \arrow[dd, "\cong"] & & & \mathsf{prcb}_{\mathbb{F}_2} \arrow[dl] \arrow[dd, "\cong"] \\
\mathsf{prcb}_{\mathbb{F}_2}^{\mathsf{op}} \arrow[rrrr] \arrow[dd, "\cong"'] & & & & \mathsf{spcb}_{\mathbb{F}_2} \arrow[dd, dashed] & \\
& & (\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) \arrow[rrr] \arrow[dll] & & & (\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) \arrow[dl] \arrow[ddl, bend left] \\
(\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)^{\mathsf{op}} \arrow[rrrr] \arrow[drrrr, bend right] & & & & {} \arrow[d, dashed, "F"'] & \\
& & & & (\mathsf{Span}^{\sim}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) &
\end{tikzcd}$$

The cube easily commutes. What remains to be shown is that the universal map F is an isomorphism of props. It is clearly the identity on objects, so we just need to show it is full and faithful.

It is full because given any span $n \xleftarrow{f} k \xrightarrow{g} m$, we have:

$$F\left((n \xleftarrow{f} k = k); (k = k \xrightarrow{g} m)\right) = n \xleftarrow{f} k \xrightarrow{g} m$$

For faithfulness, given for any two isomorphic maps in $\mathsf{Span}(\mathsf{Mat}_{\mathbb{F}_2})$:

$$\begin{tikzcd}
& k \arrow[dl, "f'"'] \arrow[dr, "g'"] \arrow[dd, "h", "\cong"'] & \\
n & & m \\
& k \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Then in the domain of F:

$$\begin{tikzcd}
{} & k \arrow[dl, "f"'] \arrow[dr, equal] & & ; & & k \arrow[dl, equal] \arrow[dr, "g"] & & = & & k \arrow[dl, "f"'] \arrow[dr, equal] & & ; & & k \arrow[dl, equal] \arrow[dr, equal] & & ; & & k \arrow[dl, equal] \arrow[dr, "g"] & \\
n & & k & & k & & m & & n & & k & & k & & k & & k & & m \\
& & & & & & & & & & & & & k \arrow[ul, "h"] \arrow[ur, "h"'] \arrow[uu, "h"', "\cong"] & & & & &
\end{tikzcd}$$

$$\begin{tikzcd}
= & & k \arrow[dl, "f"'] \arrow[dr, equal] & & ; & & k \arrow[dl, "h"'] \arrow[dr, equal] & & ; & & k \arrow[dl, equal] \arrow[dr, "h"] & & ; & & k \arrow[dl, equal] \arrow[dr, "g"] & & = & & & k \arrow[dl, "h"'] \arrow[dr, equal] \arrow[ddll, bend right, "f'"'] & & & ; & & & k \arrow[dl, equal] \arrow[dr, "h"] \arrow[ddrr, bend left, "g'"] & & \\
{} & n & & k & & k & & k & & k & & k & & k & & m & & & k \arrow[dl, "f"] \arrow[dr, equal] & & k \arrow[dl, "h"'] \arrow[dr, equal] & & & & k \arrow[dl, equal] \arrow[dr, "h"'] & & k \arrow[dl, equal] \arrow[dr, "g"'] & \\
{} & & & & & & & & & & & & & & & & & n & & k & & k & & k & & k & & m
\end{tikzcd}$$

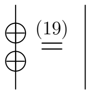
□

Given a PID k, the prop $(\mathsf{Span}^{\sim}(\mathsf{Mat}_k), \oplus)$ is already known to have a much nicer presentation given in terms of "interacting Hopf algebras" [Zan18, Definition 3.13].

4.3.2 Adding the not-gate

In this subsection we perform the same analysis for the affine fragment as we did in the previous subsection for the linear fragment. First, for the not gate:

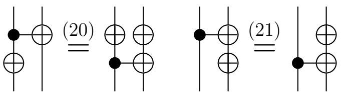
Definition 4.42. Let N_2 denote the prop generated by the not gate modulo the following equation:



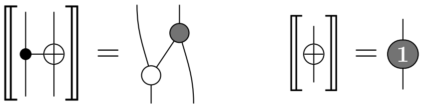
The not gate and cnot gate interact via a distributive law:

Definition 4.43. There is a distributive law of props:

$$\mathsf{isacb}_{\mathbb{F}_2} := \mathsf{iscb}_{\mathbb{F}_2} \otimes_{\mathsf{p}} \mathsf{N}_2;$$



Lemma 4.44 ([Laf03, Theorem 11])**.** $\mathsf{isacb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Iso}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus)$ *with respect to the interpretation:*



We get affine injections by adding the $|0\rangle$ state:

Definition 4.45. Let $\mathsf{inacb}_{\mathbb{F}_2}$ denote the pushout of the diagram of props:

$$\mathsf{incb}_{\mathbb{F}_2} \leftarrow \mathsf{iscb}_{\mathbb{F}_2} \rightarrow \mathsf{isacb}_{\mathbb{F}_2}$$

Lemma 4.46. $\mathsf{inacb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Mono}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus)$.

Proof. We show that the following diagram commutes and that the vertical maps are isomorphisms:

$$\begin{tikzcd}
 & \mathsf{iscb}_{\mathbb{F}_2} \arrow[dl] \arrow[rr] \arrow[dd, "\cong"] & & \mathsf{isacb}_{\mathbb{F}_2} \arrow[dl] \arrow[dd, "\cong"] \\
\mathsf{incb}_{\mathbb{F}_2} \arrow[rr] \arrow[dd, "\cong"'] & & \mathsf{inacb}_{\mathbb{F}_2} \arrow[dd, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \\
 & (\mathsf{Iso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) \arrow[dl] \arrow[rr] & & (\mathsf{Iso}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus) \arrow[dl] \arrow[ddl, bend left] \\
(\mathsf{Mono}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus) \arrow[rr] \arrow[dr, bend right] & & \cdot \arrow[d, dashed, "F"'] \arrow[ul, phantom, "\ulcorner", very near start] & \\
 & & (\mathsf{Mono}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus) &
\end{tikzcd}$$

The rear and left faces of the cube commute and their vertical maps are all isomorphisms. Therefore, the whole cube commutes via universal property of the pushout, with the upper universal map of the cube also being an isomorphism.

We seek to show that the lower universal map F is also an isomorphism. It is clearly the identity on objects, so we just have to show fullness and faithfulness.

For fullness, consider any map $n \overset{(A,x)}{\rightarrowtail} m$ in $(\mathsf{Mono}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus)$. Note that this can be factored into:

$$n \overset{(A,0)}{\rightarrowtail} m \underset{\cong}{\overset{(1,x)}{\to}} m$$

which lies in the image of F as $m \underset{\cong}{\overset{(1,x)}{\to}} m$ is an isomorphism.

For faithfulness, we show that there is a unique normal form for maps in

$$(\mathsf{Iso}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus) +_{(\mathsf{Iso}(\mathsf{Mat}_{\mathbb{F}_2}))} (\mathsf{Mono}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$$

There are two cases:

$$\left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,x)}{\to}} m\right) = \left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,0)}{\to}} m; m \underset{\cong}{\overset{(1,x)}{\to}} m\right) = \left(n \overset{A;B}{\rightarrowtail} m \underset{\cong}{\overset{(1,x)}{\to}} m\right)$$

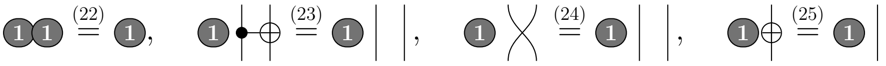
and

$$\left(n \overset{(A,x)}{\rightarrowtail} m; m \underset{\cong}{\overset{B}{\to}} m\right) = \left(n \overset{(A,0)}{\rightarrowtail} m; m \underset{\cong}{\overset{(1,x)}{\to}} m; m \underset{\cong}{\overset{B}{\to}} m\right) = \left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,B(x))}{\to}} m\right)$$
$$= \left(n \overset{A;B}{\rightarrowtail} m; m \underset{\cong}{\overset{(1,B(x))}{\to}} m\right)$$

□

To define partial isomorphisms, we add a generator to the constituent props corresponding to the zero subobject/zero scalar:

Definition 4.47. Let $\mathsf{isacb}_{\mathbb{F}_2}^{+1}$ denote the prop obtained by adjoining the following generator to $\mathsf{isacb}_{\mathbb{F}_2}$ ① modulo the equations:



Lemma 4.48. $\mathsf{isacb}_{\mathbb{F}_2}^{+1}$ *is a presentation for the subcategory of*

$$(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$$

generated by spans

$$\mathbb{F}_2^n = \mathbb{F}_2^n \underset{\cong}{\overset{f}{\to}} \mathbb{F}_2^n \quad \textit{and} \quad \mathbb{F}_2^n \overset{?}{\leftarrowtail} \emptyset \overset{?}{\rightarrowtail} \mathbb{F}_2^n$$

for all $n \in \mathbb{N}$ and isomorphisms f.

Proof. Identify the generator ① with the span $\mathbb{F}_2^0 \overset{?}{\leftarrowtail} \emptyset \overset{?}{\rightarrowtail} \mathbb{F}_2^0$. If there is a factor of ①, repeatedly apply these identities from left to right until the diagram corresponding to the identity tensored by ① is obtained, which is a normal form. □

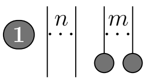
By adding the state $|0\rangle$ to our previous presentation, we get a presentation for injections which can also be zero:

Definition 4.49. Let $\mathsf{inacb}_{\mathbb{F}_2}^{+1}$ denote the pushout of the diagram of props:

$$\mathsf{inacb}_{\mathbb{F}_2} \leftarrow \mathsf{isacb}_{\mathbb{F}_2} \rightarrow \mathsf{isacb}_{\mathbb{F}_2}^{+1}$$

Lemma 4.50. $\mathsf{inacb}_{\mathbb{F}_2}^{+1}$ *is a presentation for the subcategory of* $(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$ *generated by spans* $\mathbb{F}_2^n = \mathbb{F}_2^n \xrightarrow{e} \mathbb{F}_2^m$ *and* $\mathbb{F}_2^n \xleftarrow{?} \emptyset \xrightarrow{?} \mathbb{F}_2^n$*, for all* $n, m \in \mathbb{N}$ *and monics* e*.*

The proof of this lemma is essentially the same for $\mathsf{isacb}_{\mathbb{F}_2}^{+1}$, although diagrams with a factor of ❶ are reduced to the following normal form:

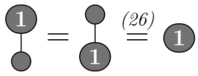


To get partial injections, we add the effect $\langle 0|$:

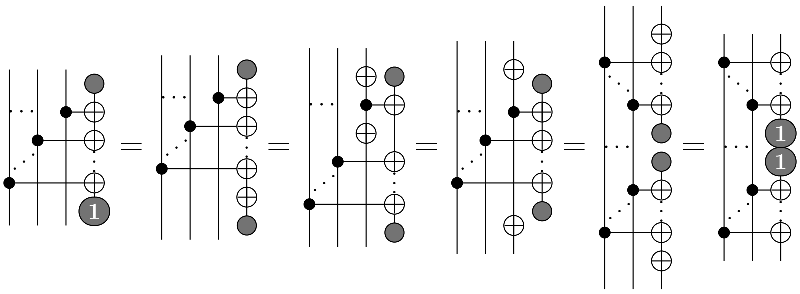
Lemma 4.51. *There is a distributive law of props:*

$$\mathsf{pisacb}_{\mathbb{F}_2} := (\mathsf{inacb}_{\mathbb{F}_2}^{+1})^{\mathsf{op}} \otimes_{\mathsf{isacb}_{\mathbb{F}_2}^{+1}} \mathsf{inacb}_{\mathbb{F}_2}^{+1}$$

Given by the equations of $\mathsf{piscb}_{\mathbb{F}_2}$ *as well as:*



Proof. The only nontrivial critical pair arises when controlled-not gates are sandwiched between grey, or grey 1 units/counits on their target wires. The case where there are no controlled not gates in between is resolved by Axiom (26). When there are more controlled-not gates, they can be pushed past each other as follows:

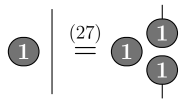


□

Lemma 4.52. $\mathsf{pisacb}_{\mathbb{F}_2}$ *is a presentation for the full subcategory* $(\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$ *of* $(\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$ *where the objects are nonempty affine vector spaces.*

Proof. The obvious functor $\mathsf{pisacb}_{\mathbb{F}_2} \to (\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$ is clearly full, as well as an isomorphism on ojects. It remains to show it is faihful. It is faithful on maps which are taken to spans with nonempty apex by the same argument as Lemma 4.37. For empty case, there is exactly one diagram of each type with a factor of 0; and similarly, there is exactly one span with an empty apex. $\square$

This is equivalent to the prop CNOT presented in the paper of Cockett et al. [CCS18]. Therefore the presentation we have given for $(\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$ can be simplified so that the identities given in Definition 4.47 can be replaced by the following equation:



In graphical affine algebra style, we could have equivalently asserted the equation (5).

To get to partial maps we add the effect $\sqrt{2}\langle +|$:

Definition 4.53. Let $\mathsf{pracb}_{\mathbb{F}_2}$ denote the pushout of the diagram of props:

$$\mathsf{pisacb}_{\mathbb{F}_2} \leftarrow \mathsf{surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Lemma 4.54. $\mathsf{pracb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Par}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$.

The proof is essentially the same as for Lemma 4.39. By adding the state $\sqrt{2}|+\rangle$ we get a presentation for affine spans:

Definition 4.55. Let $\mathsf{spacb}_{\mathbb{F}_2}$ denote the pushout of the diagram of props:

$$\mathsf{pracb}^{\mathsf{op}}_{\mathbb{F}_2} \leftarrow \mathsf{pisacb}_{\mathbb{F}_2} \rightarrow \mathsf{pracb}_{\mathbb{F}_2}$$

Lemma 4.56. $\mathsf{spacb}_{\mathbb{F}_2}$ *is a presentation for the prop* $(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$.

Proof. We show that the following diagram commutes and that the vertical maps are isomorphisms:

$$\begin{tikzcd}
& \mathsf{pisacb}_{\mathbb{F}_2} \arrow[ld] \arrow[rr] \arrow[d, "\cong"] & & \mathsf{pracb}_{\mathbb{F}_2} \arrow[ld] \arrow[dd, "\cong"] \\
\mathsf{pracb}^{\mathsf{op}}_{\mathbb{F}_2} \arrow[rr] \arrow[dd, "\cong"'] & (\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus) \arrow[ddl] \arrow[rrd] & \mathsf{spacb}_{\mathbb{F}_2} \arrow[dd, dashed] & \\
& & & (\mathsf{Par}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus) \arrow[ld] \arrow[ldd, bend left] \\
((\mathsf{Par}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*)^{\mathsf{op}}, \oplus) \arrow[rr] \arrow[rrd, bend right] & & {} \arrow[d, "F"'] & \\
& & (\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus) &
\end{tikzcd}$$

The rear and left faces of the cube commute and the vertical maps are all isomorphisms. Therefore, the whole cube commutes by the universal property of the pushout, with the upper universal map being an isomorphism. We seek to show that the lower universal map F is also an isomorphism. It is clearly the identity on objects, so we just have to show fullness and faithfulness. For fullness, let us first consider the nonempty case; that is a map $\mathbb{F}_2^n \xleftarrow{(A,x)} \mathbb{F}_2^k \xrightarrow{(B,y)} \mathbb{F}^m$ in $(\mathsf{Span}^{\sim}(\mathsf{AffMat}(\mathbb{F}_2) + 1)^*, \oplus)$. This is in the image of the following diagram under F:

$$(\mathbb{F}_2^n \xleftarrow{(A,x)} \mathbb{F}_2^k = \mathbb{F}_2^k); (\mathbb{F}_2^k = \mathbb{F}_2^k \xrightarrow{(B,y)} \mathbb{F}^m)$$

Otherwise, consider a map of the form $\mathbb{F}_2^n \xleftarrow{?} \emptyset \xrightarrow{?} \mathbb{F}^m$. This is in the image of the following diagram:

$$(\mathbb{F}_2^n \xleftarrow{?} \emptyset \xrightarrow{?} \mathbb{F}_2^0); (\mathbb{F}_2^0 \xleftarrow{?} \emptyset \xrightarrow{?} \mathbb{F}^m)$$

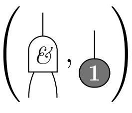
For faithfulness, again, we separate the proof into two cases. The functor is faithful on diagrams in $(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2}+1)^*, \oplus)$ with nonempty apex by the same argument as in Lemma 4.41. The case for spans with empty apex follows immediately as the only endomorphism on the empty set is the identity; thus, isomorphic spans must be equal on the nose. □

This gives a recipe for constructing the props of affine spans over arbitrary fields. To the knowledge of the authore there is no presentation for affine isomorphisms or affine monororphisms for arbitrary fields; however, one doesn't need to have presentations for all the intermediary categories in order to build a presentation for affine spans. In Zanasi's Ph.D. thesis, the category of linear spans over a principle ideal domain is constructed similarly without ever giving a presentation for the linear isomorphisms [Zan18, Section 3.3], so the situation should be completely analogous. We won't give the presentation here, because it doesn't bring much insight to this subject.

4.3.3 Adding the and-gate

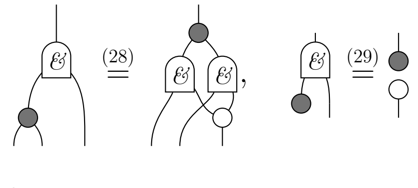
In this subsection we do the same thing as in the previous two subsections but in the nonlinear setting.

Definition 4.57. Consider the prop of bicommutative bialgebras $\mathsf{cb}_{\mathbb{B}}$, where the comonoid is drawn as ○ and the monoid is drawn as follows:



There is a distributive law of Lawvere theories:

$$\mathsf{f}_2 := \mathsf{cb}_{\mathbb{B}} \otimes_{\mathsf{cm}^{\mathsf{op}}} \mathsf{cb}_{\mathbb{F}_2};$$



where $\mathsf{cm}^{\mathsf{op}}$ picks out the comonoid ○ of $\mathsf{cb}_{\mathbb{B}}$ and $\mathsf{cb}_{\mathbb{F}_2}$.

The following result was not originally stated using distributive laws, and is due to Burroni [Bur]:

Lemma 4.58. f_2 *is a presentation for full subcategory of finite ordinals and functions whose objects are powers of 2,* $(\mathsf{FinOrd}_2, \times)$*, regarded as a prop with respect to the product.*

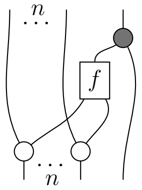
Note that this is equivalent to the prop of polynomial functions. I.e. where the maps $n \to m$ are elements of

$$(\mathbb{F}_2[x_1, \cdots, x_n]/\langle x_1^2 - x, \cdots, x_n^2 - x\rangle)^m$$

where composition is given pointwise by polynomial evaluation.

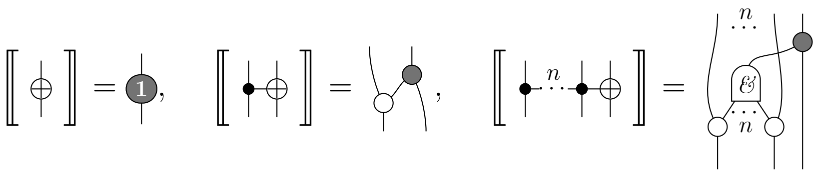
To find larger fragments, it will be useful to first identify the isomorphisms and the monics of f_2.

Definition 4.59. Given a map $f : n \to 1$ in f_2, the **oracle** $\mathcal{O}_f$ for f is defined as follows:



These are called oracles, because these correspond to the reversible implementations of Boolean functions which are queried by quantum circuits.

Lemma 4.60. *The oracles in f_2 are generated by the generalized controlled-not gates:*



Proof. Any Boolean function of n arguments can be represented by a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots x_n^2 - x_n\rangle$. Every polynomial in this quotient ring has a unique normal form given by sums of products. Each product corresponds to a generalized controlled-not gate, and the sum corresponds to composing these generalized controlled-not gates in sequence. $\square$

These generate all reversible Boolean circuits according to this classical result:

Lemma 4.61 ([Tof80, Theorem 5.1])**.** *The oracles in* f_2 *in addition to permutations generate all of* $\mathsf{Iso}(\mathsf{f}_2)$.

Recall the notation of a generalized controlled not gate controlled by wires indexed by X, operating on $x \notin X$ by $(\!|X, x|\!)$.

Iwama et al. originally gave a complete set of identities for circuits generated by generalized controlled not gates with one extra ancillary bit [IKY02]. It is worth mentioning that Shende et al. later used the commutator to generalize some of these identities [SPMH03, Corollary 26]. We conjecture that a very similar set of identities is complete for Boolean isomorphisms:

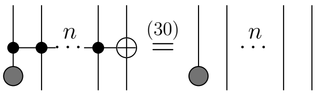
Conjecture 4.62. We conjecture that $(\mathsf{Iso}(\mathsf{FinOrd}_2), \times)$ is presented by the prop generated by all generalized controlled-not gates modulo the following identities:

- $\llparenthesis X, x \rrparenthesis ; \llparenthesis X, x \rrparenthesis = 1$.
- If $x \notin Y$ and $y \notin X$ then $\llparenthesis X, x \rrparenthesis ; \llparenthesis Y, y \rrparenthesis = \llparenthesis Y, y \rrparenthesis ; \llparenthesis X, x \rrparenthesis$.
- If $x \notin Y$, then $\llparenthesis X, x \rrparenthesis ; \llparenthesis \{x\} \sqcup Y, y \rrparenthesis = \llparenthesis X \cup Y, y \rrparenthesis ; \llparenthesis \{x\} \sqcup Y, y \rrparenthesis ; \llparenthesis X, x \rrparenthesis$.
- If $x \notin Y$, then $\llparenthesis \{x\} \sqcup Y, y \rrparenthesis ; \llparenthesis X, x \rrparenthesis = \llparenthesis X, x \rrparenthesis ; \llparenthesis \{x\} \sqcup Y, y \rrparenthesis ; \llparenthesis X \cup Y, y \rrparenthesis$.
- If $x \in Y$ and $y \in X$, then $\llparenthesis X, x \rrparenthesis ; \llparenthesis Y, y \rrparenthesis ; \llparenthesis X, x \rrparenthesis = \llparenthesis Y, y \rrparenthesis ; \llparenthesis X, x \rrparenthesis ; \llparenthesis Y, y \rrparenthesis$.

Despite this only being a conjecture, eventually once we add enough generators and identities, we get a finite, complete presentation: ZX&. Therefore take $\mathsf{Iso}(\mathsf{f}_2)$ to be the prop generated by the generalized controlled-not gates of which no complete set of equations is known.

Modulo a complete axiomatization of $\mathsf{Iso}(\mathsf{f}_2)$, by adding the state $|0\rangle$, we get a complete axiomatization of the monomorphisms in FinOrd_2.

Definition 4.63. Let inf_2 be the prop given by adjoining the grey unit to $\mathsf{Iso}(\mathsf{f}_2)$ modulo:



Lemma 4.64. inf_2 *is a presentation for the prop* $(\mathsf{Mono}(\mathsf{FinOrd}_2), \times)$.

The pullback of a diagram $2^n \rightarrowtail 2^k \leftarrowtail 2^m$ is not always a power of 2. Therefore, one should not expect to construct categories of partial isomorphisms via a distributive law $\mathsf{inf}_2 \otimes_{\mathsf{Iso}(\mathsf{f}_2)} \mathsf{inf}_2^{\mathsf{op}}$. Instead one must add all of the nontrivial subobjects to the constituent props forming the distributive law.

Definition 4.65. Consider the pro $\mathsf{sub}_{\mathbb{F}_2}$ whose maps $n \to n$ are generated by the elements of the ring of n-variable polynomial functions over $\mathbb{F}_2$:

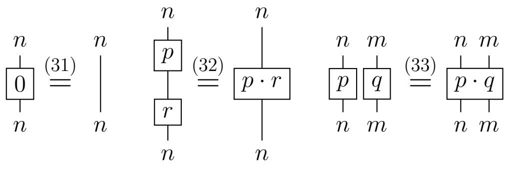
$$\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$$

So that $\forall n, m \in \mathbb{N}$ and

$$p, r \in \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$$

$$q \in \mathbb{F}_2[x_{n+1}, \ldots, x_{n+m}]/\langle x_{n+1}^2 - x_{n+1}, \ldots, x_{n+m}^2 - x_{n+m} \rangle$$

we quotient by the following equations:



Here the maps are polynomial functions; but composition is given by multiplication, not evaluation.

Lemma 4.66. $\mathsf{sub}_{\mathbb{F}_2}$ *is a presentation for the pro of subobects in* Span_2*; i.e. the symmetric spans of monomorphisms* $2^n \overset{e}{\leftarrowtail} k \overset{e}{\rightarrowtail} 2^n$.

Proof. Since $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n\rangle$ is the ring of polynomial functions in n-variables on $\mathbb{F}_2$ its elements are in bijection with functions $\mathsf{ev}_p : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by polynomial evaluation. Let $k = |\mathsf{ev}_p^{-1}(1)|$, then choose a map $f_p : k \rightarrowtail 2^n$ in f_2 picking out all the solutions to the polynomial equation $p(x_1, \cdots, x_n) = 0$. The functor from $\mathsf{sub}_{\mathbb{F}_2}$ to this subcategory of spans takes polynomials $p \mapsto (2^n \overset{f_p}{\leftarrowtail} k \overset{f_p}{\rightarrowtail} 2^n)$. Any two spans induced by the same polynomial are isomorphic, so this is well defined. It is clearly an isomorphism on objects, and it can easily be shown to be a monoidal functor.

The fullness is easy and the faithfulness comes from the fact that we can reduce every map to a polynomial and then reduce the polynomial to algebraic normal form. □

The axioms (32), (33) are reflected in **[ZX&.14]**; all of these axioms allow one to compose literals. This allows subobjects to be reduced to algebraic normal form.

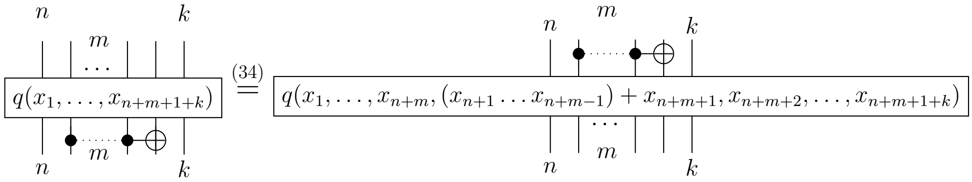
Now we compose these subobjects with the isomorphisms:

Definition 4.67. There is a distributive law of pros:

$$\mathsf{sisf}_2 := \mathsf{sub}_{\mathbb{F}_2}; \mathsf{Iso}(\mathsf{f}_2)$$

So that $\forall n, m, k \in \mathbb{N}$ and

$$q \in \mathbb{F}_2[x_1, \ldots, x_{n+m+1+k}]/\langle x_1^2 - x_1, \ldots, x_{n+m+1+k}^2 - x_{n+m+1+k}\rangle,$$

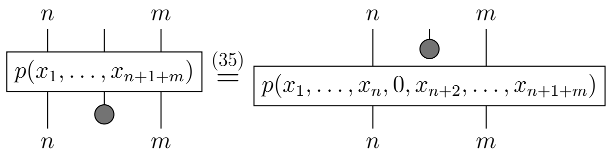


Lemma 4.68. sisf_2 *is a presentation for the subcategory of* $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ *generated by spans of the form* $2^n \overset{e}{\leftarrowtail} k \overset{e}{\rightarrowtail} 2^m \xrightarrow[\cong]{f} 2^m$, *for all* $n, m, k \in \mathbb{N}$ *and all isomorphisms* f *and monics* e.

Proof. The obvious functor is clearly monoidal. Moreover, it is full by construction. For the faithfulness, it suffices to observe that this is a strict factorization system. □

Definition 4.69. There is a distributive law of props:

$$\mathsf{sinf}_2 := \mathsf{sisf}_2 \otimes_{\mathsf{Iso}(\mathsf{f}_2)} \mathsf{inf}_2; \qquad \forall n, m \in \mathbb{N}, p \in \mathbb{F}_2[x_1, \ldots, x_{n+1+m}] :$$



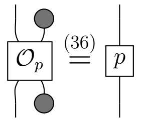
Lemma 4.70. sinf_2 *is a presentation for the subcategory of* $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}),\times)$ *generated by spans of the form* $2^n \overset{e}{\leftarrowtail} k \overset{e}{\rightarrowtail} 2^n \overset{e'}{\rightarrowtail} 2^m$ *for all* $n, m, k \in \mathbb{N}$ *and all monics* e, e'.

The proof is completely analogous to that of Lemma 4.68.

Any n variable polynomial function p can be interpreted as a span of monics via the oracle $\mathcal{O}_p$, where the the target wire is restricted to have the value 0. Each such polynomial function corresponds to a subobject, which complicates the matter further than in the affine case. Now we combine the subobjects with the isomorphisms:

Definition 4.71. There is a distributive law of props given by the following family of equations:

$$\mathsf{pisf}_2 := \mathsf{sinf}_2^{\mathsf{op}} \otimes_{\mathsf{sisf}_2} \mathsf{sinf}_2;$$



Note that this is actually a distributive law because the case where the target wire of an oracle is sandwiched between a grey unit and counit is the only critical pair needed to push $\mathsf{sinf}_2^{\mathsf{op}}$ past sinf_2 up to sisf_2.

Lemma 4.72. prif_2 *is a presentation for the full subcategory* $(\mathsf{FPinj}_2,\times)$ *of* $(\mathsf{ParIso}(\mathsf{FinOrd}),\times)$ *with objects powers of two.*

Proof. We have shown how to push all of the generators of sinf_2 past those of $\mathsf{sinf}_2^{\mathsf{op}}$ up to sisf_2.

The uniqueness up to zig-zags becomes trivial in this case. The invertible maps in $\mathsf{sinf}_2^{\mathsf{op}}$ act the same both on the left and on the right in analogy to the orthogonal factorization systems. Similarly, the non-invertible subobjects corresponding to spans $2^n \overset{e}{\leftarrowtail} k \overset{e}{\rightarrowtail} 2^n$ act the same both on the left and the right. □

This is equivalent to the prop TOF of Cockett et al. whose identities we have included in Figure 4.1 [CC19]. By adding the effect $\sqrt{2}\langle +|$ we get partial functions:

Definition 4.73. Consider the prop pf_2 given by the pushout of the following diagram of props, given by adding a counit to the diagonal map:

$$\mathsf{pisf}_2 \leftarrow \mathsf{surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Lemma 4.74. prf_2 *is a presentation for* $(\mathsf{FPar}_2,\times)$.

This is immediate because the pushout is precisely the Cartesian completion.

By adding the state $\sqrt{2}|+\rangle$ we get spans:

Definition 4.75. Let spf_2 denote the pushout of the diagram of props:

$$\mathsf{pf}_2^{\mathsf{op}} \leftarrow \mathsf{pif}_2 \rightarrow \mathsf{pf}_2$$

Lemma 4.76. spf_2 *is a presentation for* $(\mathsf{FSpan}_2, \times)$*.*

Since we know that $\mathsf{pis}_2 \cong \mathsf{TOF}$, adding a unit and counit to TOF yields $\mathsf{ZX}\&$, which we know is complete for $(\mathsf{FSpan}_2, \times)$.

We summarize the important fragments, as well as their semantics in Figure 4.3:

Linear Boolean circuits	Syntax	Semantics
Cartesian category	$\mathsf{cb}_{\mathbb{F}_2}$	$(\mathsf{Mat}_{\mathbb{F}_2}, \oplus)$
Isomorphisms	$\mathsf{iscb}_{\mathbb{F}_2}$	$(\mathsf{Iso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$
Monomorphisms	$\mathsf{incb}_{\mathbb{F}_2}$	$(\mathsf{Mono}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$
Partial isomorphisms	$\mathsf{piscb}_{\mathbb{F}_2}$	$(\mathsf{ParIso}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$
Partial maps	$\mathsf{prcb}_{\mathbb{F}_2}$	$(\mathsf{Par}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$
Spans	$\mathsf{spcb}_{\mathbb{F}_2}$	$(\mathsf{Span}^{\sim}(\mathsf{Mat}_{\mathbb{F}_2}), \oplus)$
Relations	$\mathsf{ih}_{\mathbb{F}_2}$	$(\mathsf{Rel}(\mathsf{Mat}(\mathbb{F}_2)), \oplus) \cong \mathsf{LinRel}_{\mathbb{F}_2}$

$$\hookdownarrow$$

Affine Boolean circuits	Syntax	Semantics	Full subcategory of
Cartesian category	$\mathsf{acb}_{\mathbb{F}_2}$	$(\mathsf{AffMat}_{\mathbb{F}_2}, \oplus)$	$(\mathsf{AffMat}_{\mathbb{F}_2} + 1, \oplus)$
Isomorphisms	$\mathsf{isacb}_{\mathbb{F}_2}$	$(\mathsf{Iso}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus)$	$(\mathsf{Iso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$
Monomorphisms	$\mathsf{inacb}_{\mathbb{F}_2}$	$(\mathsf{Mono}(\mathsf{AffMat}_{\mathbb{F}_2}), \oplus)$	$(\mathsf{Mono}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$
Partial isomorphisms	$\mathsf{pisacb}_{\mathbb{F}_2} \cong \mathsf{CNOT}$	$(\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$	$(\mathsf{ParIso}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$
Partial maps	$\mathsf{pracb}_{\mathbb{F}_2}$	$(\mathsf{Par}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$	$(\mathsf{Par}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$
Spans	$\mathsf{spacb}_{\mathbb{F}_2}$	$(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus)$	$(\mathsf{Span}^{\sim}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$
Relations	$\mathsf{aih}_{\mathbb{F}_2}$	$(\mathsf{Rel}(\mathsf{AffMat}_{\mathbb{F}_2} + 1)^*, \oplus) \cong \mathsf{AffRel}_{\mathbb{F}_2}$	$(\mathsf{Rel}(\mathsf{AffMat}_{\mathbb{F}_2} + 1), \oplus)$

$$\hookdownarrow$$

Multiplicative Boolean circuits	Syntax	Semantics	Full subcategory of
Cartesian category	f_2	$(\mathsf{FinOrd}_2, \times)$	$(\mathsf{FinOrd}, \times) \cong (\mathsf{FSet}, \times)$
Isomorphisms	oracles in f_2	$(\mathsf{Iso}(\mathsf{FinOrd}_2), \times)$	$(\mathsf{Iso}(\mathsf{FinOrd}), \times) \cong (\mathsf{Iso}(\mathsf{FSet}), \times)$
Monomorphisms	inf_2	$(\mathsf{Mono}(\mathsf{FinOrd}_2), \times)$	$(\mathsf{Mono}(\mathsf{FinOrd}), \times) \cong (\mathsf{Mono}(\mathsf{FSet}), \times)$
Partial isomorphisms	$\mathsf{pis}_2 \cong \mathsf{TOF}$	$(\mathsf{FPinj}_2, \times)$	$(\mathsf{ParIso}(\mathsf{FinOrd}), \times) \cong (\mathsf{FSet}, \times)$
Partial maps	pisf_2	$(\mathsf{FPar}_2, \times)$	$(\mathsf{Par}(\mathsf{FinOrd}), \times) \cong (\mathsf{Par}(\mathsf{FSet}, \times)$
Spans	$\mathsf{spf}_2 \cong \mathsf{ZX}\&$	$(\mathsf{FSpan}_2, \times)$	$(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times) \cong (\mathsf{Span}^{\sim}(\mathsf{FSet}), \times) \cong (\mathsf{Mat}(\mathbb{N}), \otimes)$
Relations	$\mathsf{ZX}\& / \sim$	$(\mathsf{FRel}_2, \times)$	$(\mathsf{Rel}(\mathsf{FinOrd}), \times) \cong (\mathsf{Rel}(\mathsf{FSet}), \times) \cong (\mathsf{Mat}(\mathbb{B}), \otimes)$

Figure 4.3: Periodic table of Boolean circuits. This table is a commutative diagram. Each subtable embeds into the one beneath it. Within each subtable, every row after "Cartesian category" embeds into the one beneath it, with the exception of "Spans" which quotients to "Relations."

4.4 Discussion

A natural next question would be to prove completeness for the natural number fragments of the qudit ZH-calculus/full subcategories d^n of $\mathsf{Mat}_{\mathbb{N}}$. There is a universal presentation of the qudit ZH-calculus given in Roy's M.Sc. thesis [Roy22]; however, completeness has not been proven. Perhaps this would be a first step towards proving completeness of the qudit ZH-calculus. The difficulty with generalizing our work is that finding normal forms for systems of Boolean equations is particularly easy. For example, the rule [**ZX&.13**] allows us to make the following deduction about Boolean formulae:

$$\frac{P(X) \cdot P(Y) = 1}{P(x) = 1, \qquad Q(y) = 1}$$

So that an n variable system of Boolean equations is equivalent to a single n-variable Boolean equation; which can be represented as a linear subspace over $\mathbb{F}_2^n$. Therefore [**ZX&.13**] allows us to reduce Boolean formulae to algebraic normal via Gaussian elimination.

In the qudit setting, the n-variable d-valued formulae have the structure of elements of the ring of polynomial functions $\mathbb{Z}/d\mathbb{Z}[x_1, \cdots, x_n]/\langle x_1^d - x_1, \cdots, x_n^d - x_n \rangle$; finding normal forms for the induced algebraic varieties is much trickier. However systems of polynomial equations over fields admit normal forms called Gröbner bases. Therefore, when the dimension d is prime one could potentially use Gröbner bases to find normal forms for these systems of polynomial equations over finite fields; rewriting circuits to Gröbner bases graphically modulo the ideals $\langle x_1^d - x_1, \cdots, x_n^d - x_n \rangle$.

Chapter 5

Stabilizer codes as affine cosiotropic relations

In this chapter we give a relational account of mixed stabilizer circuits using linear and affine symplectic geometry. As opposed to the previous chapter where we extended affine relations with the nonlinear `and` gate, in this chapter we add the linear phase shift gates instead. More conceptually unlike the previous chapter where we took the nonlinear state space approach such that that the objects were finite sets, here we take the linear/affine phase space approach where the the objects are symplectic vector spaces. Symplectic vector spaces capture the possible configurations of position and momentum: ie. the phase space. Symplectic vector spaces carry a symplectic form which measures the degree of commutation of points in the phase space. The morphisms between symplectic vector spaces which we study in this chapter are (affine) (co)isotropic relations: capturing the nondeterministic evolution of the mechanical system in a way that preserves the commutation between position and momentum.

Outline

In Section 5.1, we give an overview of linear symplectic geometry and linear Lagrangian relations using the language of graphical linear algebra. In Section 5.2, we give generators for Lagrangian relations; showing that for prime fields, Lagrangian relations can be generated by dubling linear relations. In Section 5.3 we show that only one more generator is needed to obtain the prop of affine Lagrangian relations. In the case of odd prime fields, we show in Theorem 5.23 that affine Lagrangian relations equivalent to quopit stabilizer circuits, modulo invertible scalars. This gives a graphical calculus which extends the previous work on Spekkens' qubit toy model by Backens et al. [BD16], and the qutrit stabilizer ZX-calculus by Wang [Wan18].

We also discuss the relation to electrical circuits. In Section 5.4 we show that quantum discard in quopit stabilizer circuits is equivalent to the discard *relation*. By splitting decoherence maps for the Z/X bases, we obtain a semantics for state preparation and measurement of stabilizer codes. We relate this to the affine relational semantics of electrical circuits with controlled voltage and current sources; and dually, ammeters and voltmeters. In Section 5.5, we discuss the connection to error correction.

5.1 Linear symplectic geometry

In this section, we give an brief overview of finite-dimensional linear symplectic geometry, as well as categories of linear coisotropic/isotropic and Lagrangian relations.

See the papers of Weinstein for generalizations of to the infinite-dimensional linear [Wei17] and the nonlinear settings [Wei82], respectively.

Definition 5.1. Given a field k and a finite-dimensional k-vector space V, a **symplectic form** on V is a bilinear map $\omega : V \times V \to k$ which is:

Alternating: $\forall v \in V$, $\omega(v, v) = 0$.

Non-degenerate: Given some $v \in V$, if $\omega(v, w) = 0$ for all $w \in V$, then $v = 0$.

A **symplectic vector space** is a vector space equipped with a symplectic form. A (linear) **symplectomorphism** is a linear isomorphism between symplectic vector spaces that preserves the symplectic form.

Lemma 5.2 (Linear Darboux's theorem)**.** *Every vector space k^{2n} with a chosen basis is equipped with a symplectic form given by the following block matrix:*

$$\Omega_n := \begin{bmatrix} 0_n & I_n \\ -I_n & 0_n \end{bmatrix}$$

so that $\omega_n(v, w) := v^T \Omega_n w$. Moreover, every finite dimensional symplectic vector space over k is symplectomorphic to one of the form k^{2n} with such a symplectic form.

Therefore, we can always chose a basis and work with the symplectic form ω_n by default, without having to specify which symplectic structure.

In linear mechanical systems, symplectic vector spaces are interpreted as the phase space: i.e. the space of configurations of position and momentum. The symplectomorphisms are regarded as the reversible Hamiltonian evolution of the phase-space.

Definition 5.3. Let $W \subseteq V$ be a linear subspace of a symplectic space V. The **symplectic complement** of the subspace W is the subspace of V on which the symplectic form vanishes on W:

$$W^\omega := \{v \in V : \forall w \in W, \omega(v, w) = 0\}$$

A linear subspace W of a symplectic vector space V is **isotropic** when $W^\omega \supseteq W$, **coisotropic** when $W^\omega \subseteq W$ and **Lagrangian** when $W^\omega = W$.

Notice that the symplectic complement reverses the order of inclusion, so that coisotropic subspaces are turned into isotropic subspaces and vice versa. In particular, we can see how this acts on the dimension of these subspaces, so that Lagrangian subspaces of k^{2n} have dimension n.

Take an isotropic subspace $W \subseteq k^{2n}$ of dimension $n - m$ with a chosen basis. As a matter of notation denote the basis as the rows of the matrix $[Z|X]$ where Z and X are $n - m \times n$ matrices. So that the image of this matrix is W.

The following categories of linear isotropic/coisotropic/Lagrangian relations generalizes symplectomorphisms in a way that allows nondeterministic Hamiltonian evolution:

Definition 5.4. Given a field k, the prop of (linear) **Lagrangian relations**, LagRel_k has morphisms $n \to m$ being Lagrangian subspaces of the symplectic vector space $k^{2n} \oplus k^{2m}$ with respect the symplectic form given by the block diagonal matrix:

$$\operatorname{diag}(-\Omega_n, \Omega_m)$$

Composition is given by relational composition. The tensor product is given by the direct sum, where the inputs and outputs are are grouped into separate gradings, within which the Z and X gradings are also grouped together. The props of (linear) **isotropic/coisotropic relations**, $\mathsf{IsotRel}_k$ and $\mathsf{CoIsotRel}_k$ are defined in the obvious analogous ways.

Note that we needed to insert a minus sign on $-\Omega_n$ so that these subspaces can be composed relationally. In other words states and effects must be isotropic with respect to the conjugate symplectic forms.

We see that these notions of subspaces generalize symplectomorphisms as follows:

Lemma 5.5. *Given a symplectomorphism f on (k^{2n}, ω_n) its graph*

$$\Gamma_f := \{(v, f(v)) \mid v \in k^{2n}\}$$

is a Lagrangian relation $n \to n$.

Lagrangian relations between symplectic vector spaces originally appeared in the literature in the paper of Guillemin et al. [GS79]; although in this paper, the authors discuss a private communication with Weinstein who developped a similar structure around the same time. Weinstein developed more general setting of Lagrangian submanifolds between symplectic manifolds, they are known also as canonical relations, or the symplectic "category" [Wei82]. The word category is in quotes because in this more general setting composition is not always defined.

There is an embedding of (co)istropic and Lagrangian relations into $\mathsf{LinRel}_\mathsf{k}$:

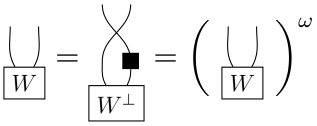
Lemma 5.6. *The forgetful functors fom Lagrangian/isotropic/cosisotropic relations to linear relations are faithful, strong symmetric monoidal.*

Due to the above lemma, we will regard LagRel_k, $\mathsf{IsotRel}_k$, $\mathsf{CoIsotRel}_k$ as (strong) symmetric monoidal subcategories of $\mathsf{LinRel_k}$. As such, we can ask what the generators of LagRel_k, $\mathsf{IsotRel}_k$ and $\mathsf{CoIsotRel}_k$ look like in terms of string diagrams of linear relations. We first describe what it means to be a Lagrangian relation in pictures. In Section 5.4, we will return to the question of (co)isotropic relations.

Concretely, the symplectic complement of a linear subspace $W \subseteq V$ is:

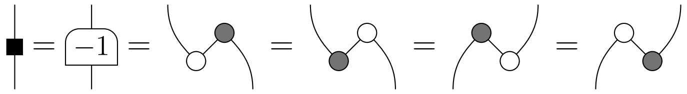
$$\begin{aligned} W^\omega := &\{(v_1, v_2) \in V : \forall (w_1, w_2) \in W, \omega((v_1, v_2), (w_1, w_2)) = 0\} \\ = &\{(v_1, v_2) \in V : \forall (w_1, w_2) \in W, \langle (v_2, -v_1), (w_1, w_2)\rangle = 0\} \\ = &\{(v_2, -v_1) \in V : \forall (w_1, w_2) \in W, \langle (v_1, v_2), (w_1, w_2)\rangle = 0\} \end{aligned}$$

Therefore, the condition asking that $W = W^\omega$ is graphically:

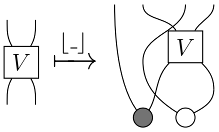


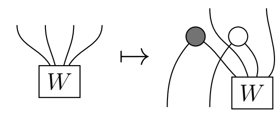
(5.1)

where recall that the antipode is given by:

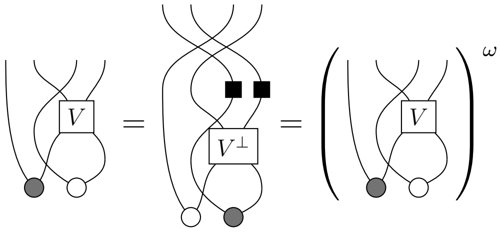


The category of Lagrangian relations is compact closed. Given a relation V between symplectic vector spaces, we can curry it into a state $\lfloor V \rfloor$; and similarily, we can uncurry a states back into processes:

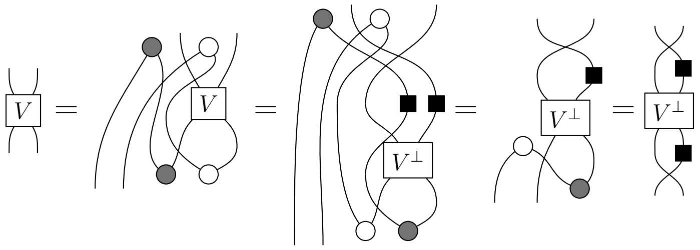




It is easy to see that these two constructions are inverse to each other. This allows us to derive a graphical criterion for arbitrary Lagrangian relations, generalizing Equation 5.1:

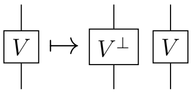


which holds if and only if

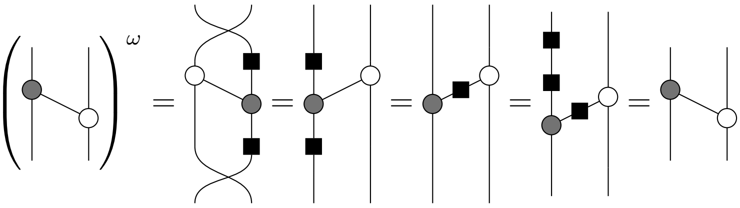


For this reason, we depict Lagrangian relations as processes where the input wires are on the bottom and output wires on on the top. There is a functor in the other direction, where recall from Lemma 2.56 that the orthogonal complement swaps colours and inverts scalars:

Lemma 5.7. *There is a faithful, strong symmetric monoidal functor* L : $\mathsf{LinRel_k} \to \mathsf{LagRel_k}$*, given by doubling with respect to the orthogonal complement:*

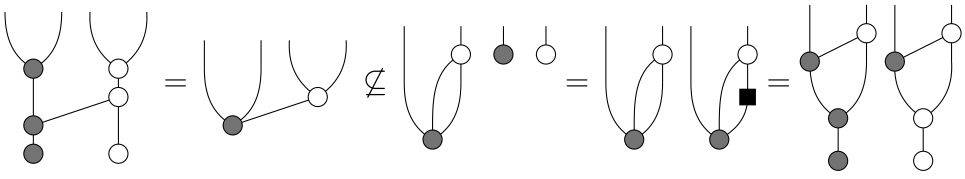


To check this is a functor, all we have to show is that it produces Lagrangian relations. This follows immediately from the naturality of the scalar -1. Indeed, because Lagrangian subspaces are isotropic and coisotropic, this extends to functors $\mathsf{LinRel_k} \to \mathsf{IsotRel_k}$ and $\mathsf{LinRel_k} \to \mathsf{CoIsotRel_k}$. This functor is a (strong) symmetric monoidal and faithful but not full, as for example, the following Lagrangian relation is not in the image of L:



Unlike $\mathsf{LinRel_k}$, these are no longer bicategories of relations:

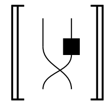
Remark 5.8. LagRel_k is not a bicategory of relations. No matter which Frobenius algebra we chose, it is not laxly natural with respect to both the phase shifts and the Fourier transform of the phase shifts:



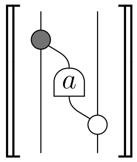
5.2 Generators for Lagrangian relations

In this section, we give a universal set of generators for LagRel_k; however, we do not directly give a complete set of identities. Instead we defer to the completeness of the monoidal presentation of $\mathsf{LinRel}_\mathsf{k}$.

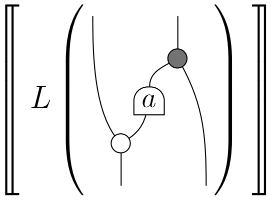
Consider the following symplectomorphisms: the symplectic Fourier transform F, the a-shift gate S_a and the controlled-a gate C_a:



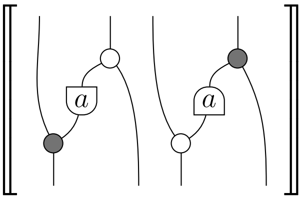
$$= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} =: F$$



$$= \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} =: S_a$$



$$=$$



$$= \begin{bmatrix} 1 & -a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & a & 1 \end{bmatrix} =: C_a$$

Use the notation $G^{(j)}$ to denote a gate G being applied to wire j; and the notation $C_a^{(i,j)}$ to denote the controlled-a gate controlling on wire i targeting wire j.

Note the right action of these gates in terms of matrix multiplication of Lagrangian subspaces for any nonzero $a \in k$ (as observed by Aaronson and Gottesman [AG04, page 4]):

- $F^{(i)}$ sets columns x_i to $-z_i$ and z_i to x_i.
- $S_a^{(i)}$ sets z_i to $z_i + a \cdot x_i$.
- $C_a^{(i,j)}$ sets x_j to $x_j - a \cdot x_i$ and z_i to $z_i + a \cdot z_j$.

Using these symplectomorphisms regarded as Lagrangian relations:

Theorem 5.9. *For any field k the maps in $L(\mathsf{LinRel}_\mathsf{k})$ as well as F and S_a for all $a \in k$ generate LagRel_k.*

Proof. The following proof is very similar to that of Aaronson and Gottesman [AG04, Lemma 6]. Consider a basis $[Z|X]$ of an arbitrary Lagrangian subspace over the field k. We show how one can reduce $[Z|X]$ to the block matrix $[I|0]$ by right multiplication with the aforementioned symplectomorphisms. To do so, we first reduce it to a matrix $[I|X']$. This involves repeatedly applying Gaussian elimination and then applying the Fourier transform to wires when the pivot is in the X block. We are guaranteed to obtain a matrix $[I|X']$ because the dimension of Lagrangian subspace of k^{2n} is n. Moreover, because $[I|X']$ spans a Lagrangian subspace, we have:

$$0 = \left[I|X'\right] \omega \left[I|X'\right]^T$$

which holds if and only if

$$0 = \left[I|X'\right]\left[X'|-I\right]^T = X'^T - X'$$

That is to say X' is symmetric, meaning that X' describes the adjacency matrix of a graph coloured by the elements of k. In the language of stabilizer circuits, this is called a *graph state.* In the case of prime fields, this observation was made by Gross [Gro06, Equation 18]. Graph states were originally discussed in the paper of Hein et al. [HDE$^+$06].

We prove that graph states can be reduced to the subspace $[I|0]$ by right multiplication of symplectomorphisms. The proof is by induction on the dimension of the subspace. This base case is trivial.

Suppose we have a $(n+1)$-dimensional Lagrangian subspaces described by a graph state, then:

$$\left[\begin{array}{ccccc|ccccc}
1 & 0 & 0 & \cdots & 0 & x_{1,1} & x_{1,2} & x_{1,3} & \cdots & x_{1,n} \\
0 & 1 & 0 & \cdots & 0 & x_{1,2} & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\
0 & 0 & 1 & \ddots & \vdots & x_{1,3} & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 1 & x_{1,n} & x_{2,n} & x_{3,n} & \cdots & x_{n,n}
\end{array}\right]$$

$$\xmapsto{(F^{(1)})^{-1}} \left[\begin{array}{ccccc|ccccc}
x_{1,1} & 0 & 0 & \cdots & 0 & -1 & x_{1,2} & x_{1,3} & \cdots & x_{1,n} \\
x_{1,2} & 1 & 0 & \cdots & 0 & 0 & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\
x_{1,3} & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_{1,n} & 0 & \cdots & 0 & 1 & 0 & x_{2,n} & x_{3,n} & \cdots & x_{n,n}
\end{array}\right]$$

$$\xmapsto{C^{(2,1)}_{x_{1,2}}} \left[\begin{array}{ccccc|ccccc}
x_{1,1} - 0 & 0 & 0 & \cdots & 0 & -1 & x_{1,2} - x_{1,2} & x_{1,3} & \cdots & x_{1,n} \\
x_{1,2} - x_{1,2} & 1 & 0 & \cdots & 0 & 0 & x_{2,2} - 0 & x_{2,3} & \cdots & x_{2,n} \\
x_{1,3} - 0 & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} - 0 & x_{3,3} & \cdots & x_{3,n} \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_{1,n} - 0 & 0 & \cdots & 0 & 1 & 0 & x_{2,n} - 0 & x_{3,n} & \cdots & x_{n,n}
\end{array}\right]$$

$$= \left[\begin{array}{ccccc|ccccc}
x_{1,1} & 0 & 0 & \cdots & 0 & -1 & 0 & x_{1,3} & \cdots & x_{1,n} \\
0 & 1 & 0 & \cdots & 0 & 0 & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\
x_{1,3} & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_{1,n} & 0 & \cdots & 0 & 1 & 0 & x_{2,n} & x_{3,n} & \cdots & x_{n,n}
\end{array}\right]$$

$$\xmapsto{\prod^n_{i>1} C^{(i,1)}_{x_{1,i}}} \left[\begin{array}{ccccc|ccccc}
x_{1,1} & 0 & 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\
0 & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 1 & 0 & x_{2,n} & x_{3,n} & \cdots & x_{n,n}
\end{array}\right]$$

$$\xmapsto{F^{(1)}} \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & x_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & x_{2,n} & x_{3,n} & \cdots & x_{n,n} \end{array}\right]$$

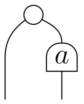
$$\xmapsto{S^{(1)}_{-x_{1,1}}} \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & x_{2,2} & x_{2,3} & \cdots & x_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & 0 & x_{2,3} & x_{3,3} & \cdots & x_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & x_{2,n} & x_{3,n} & \cdots & x_{n,n} \end{array}\right]$$

$$\xmapsto{\cdots} \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \end{array}\right]$$

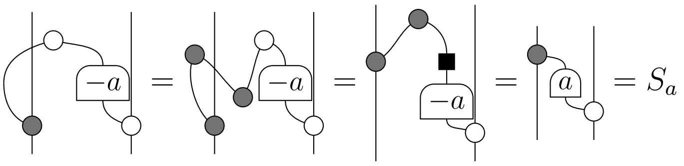
Therefore all Lagrangian relations can be reduced to the subspace $[I|0]$ by right multiplication by symplectomorphisms. In the n-dimensional case, this subspace is given by the circuit $L(\bullet^{\otimes n})$. □

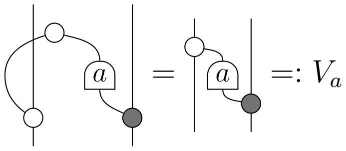
By decomposing the Fourier transform we obtain a more symmetric, equivalent set of generators:

Corollary 5.10. LagRel_k *is presented by* $L(\mathsf{LinRel_k})$ *as well as the following generators, for all* $a \in k^*$*:*

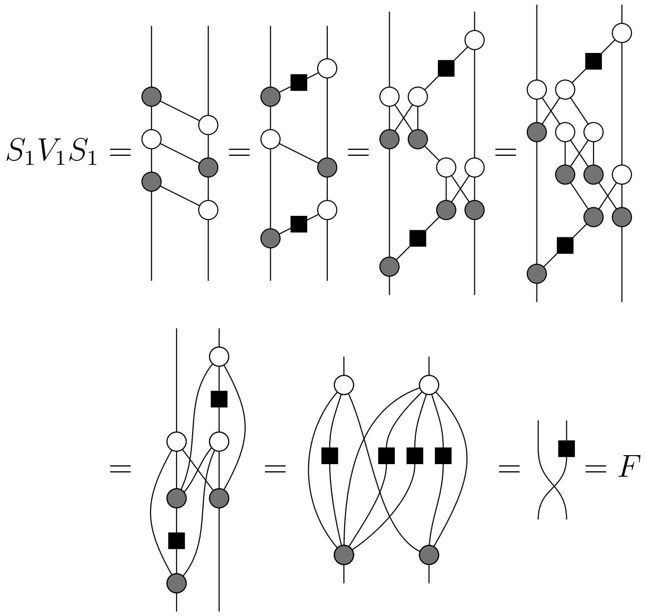
$d_a :=$  $: 1 \to 0$

Proof. We show that F and S_a can be constructed using these generators. The S_a gate and it's colour-reversed version V_a can be obtained by composing a pure morphism with d_{-a} and d_a, respectively:





We obtain F as $S_1V_1S_1$, which can be proven as a variation of the familiar "3 `cnot`" rule for quantum circuits (see e.g. [CD11, Section 3.2.1]):

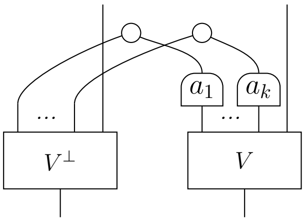


□

A variant of this decomposition is contained in the work of Baez et al. [BE15, page 6], although in the context of plain old linear relations instead of Lagrangian relations. Therefore the antipode is missing in their case, because they have no motivation to relate this decompostion to the symplectic Fourier transform. A similar observation was made by Ranchin [Ran14, Equation 34] in the "external setting" of qudit controlled-X gates.

From Corollary 5.10, we know that we can build any Lagrangian relation using "pure Lagrangian relations" in the image of the doubling functor as well as and "discard maps" d_a for all $a \in k^*$. Since the former is closed under composition and monoidal product:

Corollary 5.11 (Phase purification)**.** *Any linear Lagrangian relation can be written in the following form, for V a linear relation:*



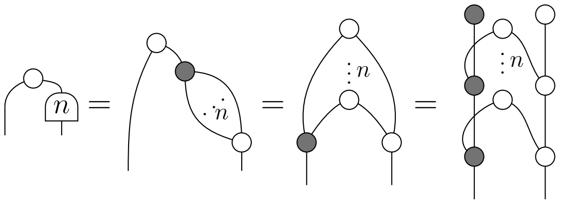
Recall from Definition 3.2: given a compact closed prop with an identity on objects monoidal conjugation functor, we can apply the CPM construction to obtain a compact closed prop (here we have a compact closed †-category rather than a †-compact closed category).

The phase-purification is so-called because of the similarity to the purification of maps in the CPM-construction. Indeed one might hope that LagRel_k is isomorphic to $\mathsf{CPM}(\mathsf{LinRel}_\mathsf{k}, (-)^\perp)$, however, in the example of phase-purification, we are tracing out both sides with respect to multiple compact closed structures: one for each $a_j \in k$. Prime fields are special:

Corollary 5.12. *F p prime:*

$$\mathsf{CPM}(\mathsf{LinRel}_{\mathbb{F}_\mathsf{p}}, (-)^\perp) \cong \mathsf{LagRel}_{\mathbb{F}_\mathsf{p}}$$

Proof.



Therefore, every map in $\mathsf{LagRel}_{\mathbb{F}_p}$ can be produced by tracing out a map in $L(\mathsf{LinRel}_{\mathbb{F}_\mathsf{p}})$. □

Note that LagRel_k is not †-compact closed with respect to $(-)^\dagger := ((-)^\perp)^*$. However, in Definition 5.27 we construct another †-functor with respect to which it is.

5.2.1 Passive linear electrical circuits as Lagrangian relations

Symplectic geometry was motivated by the goal to formalize Hamiltonian mechanics in a synthetic setting. Therefore, it is not a coincidence that in Baez et al. use linear Lagrangian relations to give a semantics for "passive linear circuits" [BF18]. These are an idealized class of electrical circuits with linear behaviour.

To each idealized wire with no resistance, Baez et al. associate the symplectic vector space $\mathbb{R}^2$. Given an element $(z, x) \in (\mathbb{R}^+)^2$, they interpret the z as the **current** flowing through the wire and x as the **potential**. The **voltage** around a node in a circuit is is the outgoing potential minus the incoming potential.

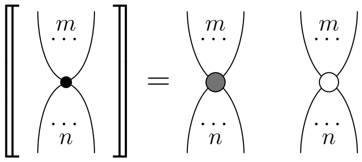
Baez et al. proceed to recall the following physical laws due to Ohm [Ohm27] followed by Kirchhoff [Kir45]:

Ohm's law: The voltage around the node in a circuit is equal to the current multiplied by the resistance.

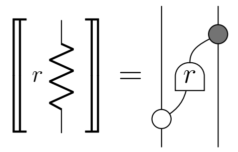
Kirchhoff's current law: The sum of currents flowing into a node is equal to the sum of currents flowing out of the node.

This allows an (ideal) junction with no resistance with n incoming wires and m outgoing wires to be modelled by a Lagrangian relation. By Kirchhoff's current law, the sum of the currents of the n incoming wires is equal to the sum of the currents of the m outgoing wires. Moreover, by Ohm's law, because resistance is zero, the n

incoming and m outgoing potentials are all made to be equal. That is to say that the junction is interpreted as the following Lagrangian relation:



This also allows us to capture (linear) resistors as Lagrangian relations. Given a linear resistor with resistance $r \in \mathbb{R}^+$, by Kirchhoff's current law the incoming current is equal to the outgoing current; and by By Ohm's law, the outgoing potential is equal to the current multiplied by r plus the incoming potential:



Baez et al. augment this semantics with time-dependent components [BF18], the exposition of which necessitates the following construction:

Definition 5.13. Given an integral domain R, the **field of fractions** of R has:

- Elements given by pairs $(a, b) \in R \times R^*$ modulo the equivalence relation $(a, b) \sim (c, d)$ whenever $ad = bc$. Denote the equivalence class of (a, b) by a/b.
- Addition is defined by $a/b + c/d = (ad + cb)/(bd)$. The unit for addition is $0/1$. The additive inverse of a/b is $(-a)/b$.
- Multiplication by $(a/b)(c/d) = (ac)/(b/d)$. The unit for multiplication is $1/1$. Given a nonzero element c/d, the inverse is d/c.

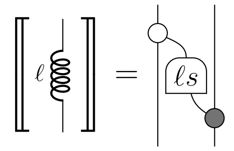
Because there is an obvious embedding of rings $a \mapsto (a/1)$, denote the equivalence class $a/1 = a$.

The **field of real rational functions** $\mathbb{R}(s)$ is the field of fractions of the polynomial ring $\mathbb{R}[s]$.

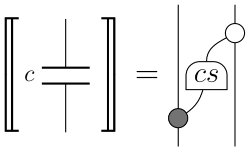
In a later paper of Baez et al., they interpret "linear constant-coefficient ordinary differential equations" relating n inputs to m outputs as $\mathbb{R}(s)$-linear relations from n to m [BE15]. The multiplication of the polynomial indeterminate s is regarded as differentiation, and multiplication by s^{-1} as integration. Regarding these differential equations as being dependent on time, in [BF18], Baez et al. interpret inductors and capacitors as Lagrangian relations over $\mathbb{R}(s)$. In some sense, the multiplication by the scalar s is interpreted as a discrete step forward in time, and by s^{-1} a discrete step backwards in time.

A (linear) inductor with inductance $\ell \in \mathbb{R}^+$ is a component with one input and one output such that the voltage is equal to the rate of change of the current multiplied by

ℓ. Applying Kirchhoff's current law Ohm's law we have that an inductor is interpreted as follows:



Dually, a (linear) capacitor with capacitance $c \in \mathbb{R}^+$ is a component with one input and one output where the current is equal to the rate of change of the voltage multiplied by c. The interpretation is given by:



Recently, the fragment of electrical circuits generated by these idealized junctions and resistors has been given a complete equational theory by Cockett et al. [CKS23]. A presentation of a more general class of circuits remains open, as we will discuss at the end of this chapter.

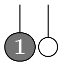
5.3 Affine Lagrangian relations

Affine Lagrangian relations are perhaps of more practical interest than linear Lagrangian relations. As we will discuss in this section, these give a semantics for quopit stabilizer circuits as well as well as passive electrical circuits plus current and voltage sources.

Definition 5.14. An **affine Lagrangian subspace** of a symplectic vector space k^{2n} is an affine subspace of $L + a \subseteq k^{2n}$ which is either empty or where L is a Lagrangian subspace. An affine relation $n \to m$ is an affine Lagrangian subspace of $k^{2n} \oplus k^{2m}$ with respect to the symplectic form given by the matrix $\text{diag}(\Omega_n, \Omega_m)$. Let $\mathsf{AffLagRel}_k$ denote the prop whose maps $n \to m$ are affine Lagrangian relations. The monoidal structure and composition is the same as for linear Lagrangian relations.

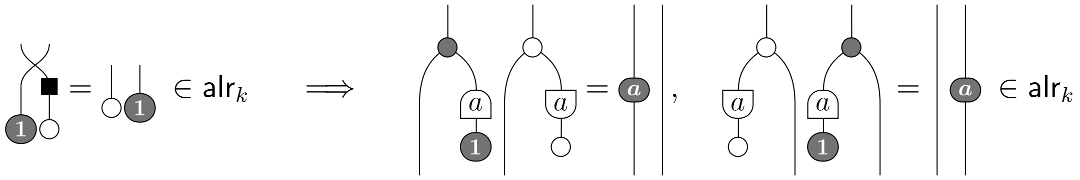
Because the tensor product is defined in the same way as in LagRel_k, as in Lemma 5.6, the forgetful functor $\mathsf{AffLagRel}_k \to \mathsf{AffRel}_k$ is faithful and strong monoidal.

Definition 5.15. Let alr_k denote the monoidal subcategory of aih_k with objects $2n$, generated by the morphisms in the image of $\mathsf{LagRel}_k \rightarrowtail \mathsf{LinRel_k} \cong \mathsf{ih_k} \hookrightarrow \mathsf{aih_k}$ as well as the following generator:



Lemma 5.16. alr_k *is a presentation of* $\mathsf{AffLagRel}_k$.

Proof. All the affine shifts can be produced from tensoring and composing these two maps on the right:



□

5.3.1 Stabilizer circuits and Spekkens' toy model

The connection between the stabilizer formalism and symplectic geometry has been known for quite a while, at least as early as the papers of Calderbank, Rains, Shor and Sloane in the qubit case [CRSS98, CRSS97]. This was further developed in great detail in the quopit case by Gross [Gro06]. However, its role in the stabilizer formalism is often underplayed, for example, it is not explicitly mentioned in Gottesman's highly influential Ph.D. thesis [Got97]. Perhaps a reason for this is that despite their dominance in the quantum computing literature, qubit stabilizer circuits do not conform so nicely to the symplectic geometric framework as do quopits.

In this subsection, we with build on the work of Gross and show that, when p is an odd prime, the prop of affine Lagrangian relations over $\mathbb{F}_p$ is isomorphic to quopit stabilizer circuits modulo invertible scalars.

To show this, we first recall two results of Gross, relating the stabilizer formalism to symplectic geometry. We reproduce the proofs here because of their importance. First we need the following convention to represent elements of the Heisenberg-Weyl group:

Definition 5.17. Given $a \in \mathbb{F}_p$ and $(z, x) \in \mathbb{F}_p^{2n}$, define the following operators:

$$\chi(a) = e^{2\pi \cdot i \cdot a/p}, \qquad \mathcal{W}(z, x) = \chi(-zx^T/2) \bigotimes_{j=0}^{n-1} \mathcal{Z}_{(j)}^{z_j} \mathcal{X}_{(j)}^{x_j}$$

This makes the following easier to prove:

Lemma 5.18 (Weil representation [Gro06, Theorem 3])**.** *For odd prime p, the group of affine symplectomorphisms over $\mathbb{F}_p^{2n}$ is isomorphic to the n quopit Clifford group modulo scalars.*

Proof. We know that the Clifford group is defined as the normalizer of the Heisenberg-Weyl group so that a Clifford operator is defined by its action on Weyl operators. Given an n quopit Clifford operator C and $(z, x) \in \mathbb{F}_p^{2n}$, there exists an isomorphism $C_L : \mathbb{F}_p^{2n} \to \mathbb{F}_p^{2n}$ and a vector $C_a \in \mathbb{F}_p^{2n}$ such that:

$$C\mathcal{W}(z, x)C^\dagger = \chi(C_a(z, x))\mathcal{W}(C_L(z, x))$$

We seek to show that C_L is the the symplectomorphism and C_a is the affine shift. C_L is clearly linear. To see that it is a symplectomorphism, first observe:

$$\mathcal{Z}\mathcal{X} = \chi(1)\mathcal{X}\mathcal{Z}$$

Therefore,

$$\begin{aligned}(\mathcal{Z}^{z_0}\mathcal{X}^{x_0})(\mathcal{Z}^{z_1}\mathcal{X}^{x_1}) &= \chi(-x_0z_1)\mathcal{Z}^{z_0}\mathcal{Z}^{z_1}\mathcal{X}^{x_0}\mathcal{X}^{x_1}\\ &= \chi(-x_0z_1)\mathcal{Z}^{z_1}\mathcal{Z}^{z_0}\mathcal{X}^{x_1}\mathcal{X}^{x_0}\\ &= \chi(z_0x_1 - x_0z_1)(\mathcal{Z}^{z_1}\mathcal{X}^{x_1})(\mathcal{Z}^{z_0}\mathcal{X}^{x_0})\\ &= \chi(\omega((z_0,x_0),(z_1,x_1)))(\mathcal{Z}^{z_1}\mathcal{X}^{x_1})(\mathcal{Z}^{z_0}\mathcal{X}^{x_0})\end{aligned}$$

So Weyl operators commute with each other up to the symplectic form:

$$\mathcal{W}(z,x)\mathcal{W}(z',x') = \chi(\omega(z,x),(z',x'))\mathcal{W}(z',x')\mathcal{W}(z,x)$$

Moreover, we can combine Weyl operators together as follows:

$$\mathcal{W}(z,x)\mathcal{W}(z',x') = \chi(\omega((z,x),(z',x'))/2)\mathcal{W}(z+z',x+x')$$

Therefore:

$$\begin{aligned}&C\mathcal{W}(z,x)\mathcal{W}(z',x')C^\dagger\\ &= C(\mathcal{W}(z,x)C^\dagger C\mathcal{W}(z',x'))C^\dagger\\ &= \chi(C_a(z,x) + C_a(z',x'))\mathcal{W}(C_L(z,x))\mathcal{W}(C_L(z',x'))\\ &= \chi(C_a(z,x) + C_a(z',x') + \omega(C_L(z,x)), C_L(z',x'))/2)\mathcal{W}(C_L(z,x) + C_L(z',x'))\end{aligned}$$

Similarly:

$$\begin{aligned}&C\mathcal{W}(z,x)\mathcal{W}(z',x')C^\dagger\\ &= \chi(\omega((z,x),(z',x'))/2)C\mathcal{W}(z+z',x+x')C^\dagger\\ &= \chi(\omega((z,x),(z',x'))/2 + C_a(z+z',x+x'))\mathcal{W}(C_L(z+z',x+x'))\\ &= \chi(\omega((z,x),(z',x'))/2 + C_a(z,x) + C_a(z',x'))\mathcal{W}(C_L(z,x) + C_L(z',x'))\end{aligned}$$

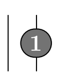
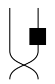
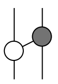
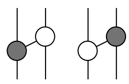
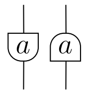
So $\omega(C_L(z,x), C_L(z',x')) = \omega((z,x),(z',x'))$; meaning that C_L is a symplectomorphism. Moreover for a Clifford operator D:

$$\begin{aligned}DC\mathcal{W}(z,x)C^\dagger D^\dagger &= D\chi(C_a(z,x))\mathcal{W}(C_L(z,x))D^\dagger\\ &= \chi(C_a(z,x) + D_a(C_L(z,x)))\mathcal{W}(D_L(C_L(z,x)))\end{aligned}$$

so C_L and C_a determine an affine transformation. $\square$

The reason this fails for qubits is because one can not represent all elements of the Heisenberg-Weyl group as $\chi(C_a(z,x))\mathcal{W}(z,x)$. For example, $\mathcal{X}\mathcal{Z} = i\mathcal{Z}\mathcal{X}$; however $i = e^{2\pi \cdot i/4}$, so there is no value of $a \in \mathbb{F}_2$ for which $\chi(a) = e^{2\pi \cdot i \cdot a/2} = e^{\pi \cdot ia} = i$.

Recall that, up to scalars, the n-qupit Clifford group is generated by the $\mathcal{X}$-gate, the $\mathcal{C}_{\mathcal{X}}$ gate, the Fourier transform $\mathcal{F}$ and the phase gate $\mathcal{S}$ and scaling gates $\mathcal{M}_a$ for all $a \in \mathbb{F}_p^*$. In the odd prime case, these correspond to the affine symplectormorphisms:

 $\leftrightarrow \mathcal{X}$,  $\leftrightarrow \mathcal{F}$,  $\leftrightarrow$ $\mathcal{S}$,  $\leftrightarrow \mathcal{C}_{\mathcal{X}}$,  $\leftrightarrow \mathcal{M}_a$

The following result gets us even closer to where we need to be:

Lemma 5.19 ([Gro06, Lemma 8]). *For every odd prime p and $n \in \mathbb{N}$, there is a bijection G between (nonempty) affine Lagrangian subspaces of $\mathbb{F}_p^{2n}$ and n-quopit stabilizer states modulo nonzero scalars.*

Proof. Given any affine Lagrangian subspace $L + a \subseteq \mathbb{F}_p^{2n}$; then up to global phase there is a stabilizer state $C|0\rangle^{\otimes n}$ determined by the rank 1 projector:

$$C|0\rangle^{\otimes n}\langle 0|^{\otimes n}C^\dagger := \frac{1}{p^n}\sum_{v\in L}\chi(\omega(a,v))\mathcal{W}(v)$$

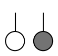
as for any $v' \in L$:

$$\begin{aligned}\chi(\omega(a,v'))\mathcal{W}(v')\frac{1}{p^n}&\sum_{v\in L}\chi(\omega(a,v))\mathcal{W}(v)\chi(-\omega(a,v'))\mathcal{W}(v')^\dagger\\ =&\frac{1}{p^n}\sum_{v\in L}\chi(\omega(a,v)+\omega(v,v'))\mathcal{W}(v)\mathcal{W}(v')\mathcal{W}(v')^\dagger\\ =&\frac{1}{p^n}\sum_{v\in L}\chi(\omega(a,v))\mathcal{W}(v)\mathcal{W}(v')\mathcal{W}(v')^\dagger\\ =&\frac{1}{p^n}\sum_{v\in L}\chi(\omega(a,v))\mathcal{W}(v)\end{aligned}$$

Moreover, every stabilizer state is of this form. Recall that stabilizer groups are Abelian. If two stabilizers $\chi(a)\mathcal{W}(u)$ and $\chi(b)\mathcal{W}(v)$ stabilize the same state, they must commute so $\omega(u,v) = 0$. A stabilizer state is stabilized by exactly p^n stabilizers, making the space of stabilizers into an affine Lagrangian subspace of $\mathbb{F}_p$. □

In other words, an augmented basis for the affine Lagrangian subspace over $\mathbb{F}_p$ corresponds to the **stabilizer tableau** for a pure quopit stabilizer state (i.e. a stabilizer tableau on n quopits with dimension n).

Explicitly, the state $|0\rangle$ is identified with the following Affine Lagrangian subspace:

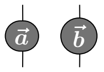
 $\leftrightarrow |0\rangle$

Definition 5.20. Let Stab_p denote the prop of quopit stabilizer circuits modulo nonzero scalars, regarded as a †-compact closed category.

We extend this isomorphism of states to an isomorphism of props using a symplectic notion of Heisenberg-Weyl groups and stabilizers:

Definition 5.21. Given a field k the n-fold symplectic Weyl operators are the symplectomorphisms of the following form, for $\vec{a}, \vec{b} \in k^{2n}$:

$$W(\vec{a}, \vec{b}) :=$$



The n-fold symplectic Weyl operators form the n-fold **symplectic Heisenberg-Weyl group**, P_k^n under composition. And altogether, they form a prop under tensor product and composition. Unlike the qudit Heisenberg-Weyl group, there is no phase-factor; as affine Lagragain relations only have scalars 0 and 1. Therefore the symplectic Heisenberg-Weyl group is merely a representation of the group additive group $k^{2n} \rightarrowtail \mathsf{AffLagRel}_k$.

Given some affine Lagrangian subspace f of $\mathbb{F}_k^{2n}$, the **symplectic stabilizer group** of f is the subgroup $S \subseteq P_k^n$ so for all $a \in S$, $f; a = f$.

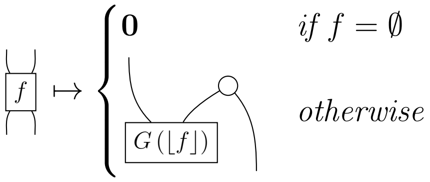
Lemma 5.22. *Two states in* $\mathsf{AffLagRel}_k$ *are equal if and only if they have the same symplectic stabilizer group.*

Proof. Take a state $f : 0 \to n$ in $\mathsf{AffLagRel}_k$. Then $W(z, x)$ is a stabilizer of f if and only if $(z, x) \in f$; therefore two subspaces are equal if and only if they have the same elements if and only if they have the same stabilizers. ☐

Theorem 5.23. *When p is an odd prime, there is a symmetric monoidal equivalence* $H : \mathsf{LagRel}_{\mathbb{F}_p} \to \mathsf{Stab}_p$ *defined:*

on objects by: $n \mapsto \ell^2(\mathbb{F}_p^n)$

on maps by:



where G is the bijection between affine Lagrangian subspaces and stabilizer states modulo scalars, and **0** *is the unique stabilizer circuit of appropriate dimension which is multiplied by the scalar 0.*

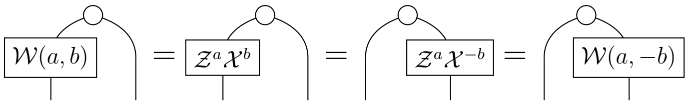
Proof. We already know that there is a bijection between the states of both of these props. Because these props are both compact closed, it only remains to show that this isomorphism is monoidal and functorial. It clearly is monoidal and preserves the identity; the nontrivial part is to show that it preserves composition.

Consider some composable pair in $\mathsf{AffLagRel}_{\mathbb{F}_p}$:

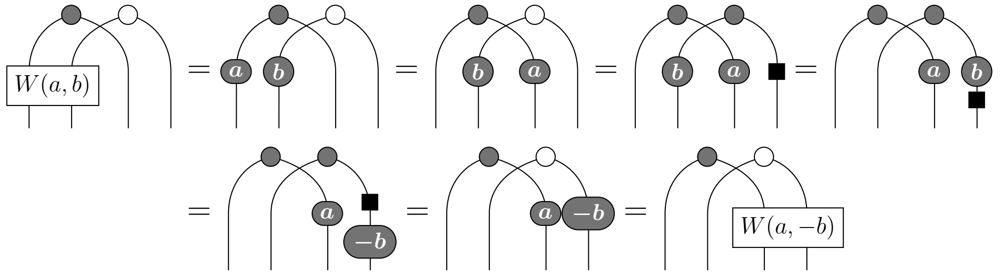
$$\mathbb{F}_p^n \xrightarrow{f} \mathbb{F}_p^m \xrightarrow{g} \mathbb{F}_p^\ell$$

If the composite is empty, then the result follows immediately. Suppose otherwise.

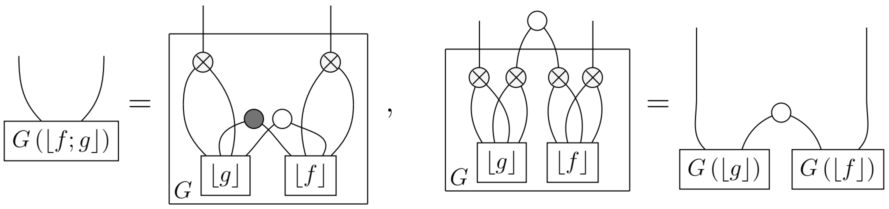
First, observe that in Stab_p:



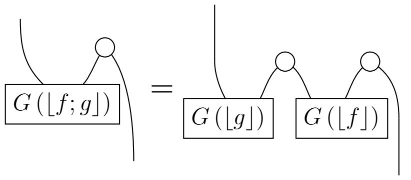
Moreover, in $\mathsf{AffLagRel}_{\mathbb{F}_p}$:



Therefore, the symplectic Weyl operators commute with the symplectic Z spider in $\mathsf{AffLagRel}_{\mathbb{F}_p}$ in the same way that the Weyl operators commute with the Z spiders in Stab_p. Therefore, the following two states in Stab_p have the same stabilizers



And thus they are equal. Therefore:



□

The novelty in interpreting stabilizer states in this categorical framework is that it reveals that the *relational composition* of tableaux is the composition of stabilizer circuits. If we drop the affine shifts, we get a smaller fragment of stabilizer circuits:

Corollary 5.24. *For odd prime p, $\mathsf{LagRel}_{\mathbb{F}_p}$ is a presentation for Weyl-free quopit stabilizer circuits.*

$\mathsf{AffLagRel}_{\mathbb{F}_2}$ has already been studied in other terms. Spekkens first introduced his toy model as a noncontextual, nonphysical hidden variable analogue to qubit stabilizer quantum mechanics, satisfying the so-called "knowledge-balance principle" [Spe07]. An epistemic and an ontic state are associated to every state in the the toy model. The epistemic state is interpreted as the knowledge which the observer has about the state, and the ontic state is interpreted as the physical/real properties of the state. When the observer gains knowledge about the state of the system, then the physical state looses degrees of freedom. This Galois connection between the epistemic and ontic state is given by the action of the symplectic complement. Therefore:

Corollary 5.25. $\mathsf{AffLagRel}_{\mathbb{F}_2}$ *is a presentation for the ZX-calculus for Spekkens' toy model of Backens et al. [BD16].*

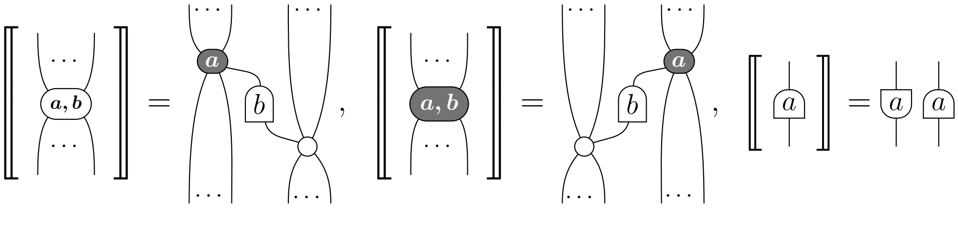
Later, this was formalized in terms of symplectic geometry by Spekkens [Spe16]. The general idea is that one interprets the Lagrangian subspace as the epistemic state of the position and momentum variables (ie, what the observer knows about the state); moreover, the symplectic complement of the Lagrangian subspace is interpreted as the ontic state (the physical or real, properties of the state). The Galois connection induced by the symplectic complement is interpreted as the knowledge balance principle. If the observer never measures anything so that the ontic state is equal to the epistemic state then:

We would have liked to use some modified form of the Weil representation for qubits, like that found in Heinrich's Ph.D. theis [Hei21, Section 3.3] or of the paper of de Beaudrap [Bea13]; however, because i has order 4 in the group $\mathbb{C}^*$, this would seemingly require some analogue of affine relations over the ring $\mathbb{Z}/4\mathbb{Z}$. Here the relational approach falls short to the functional approach, because $\mathbb{Z}/4\mathbb{Z}$ is not a principal ideal domain; and thus $\mathsf{Mat}_{\mathbb{Z}/4\mathbb{Z}}$ is not a regular category. Some other technique is needed to this end.

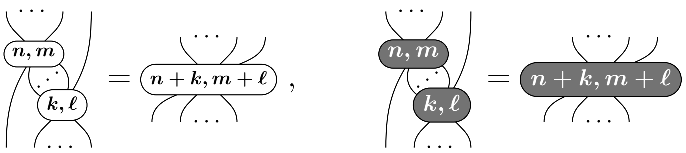
There is another way to present $\mathsf{AffLagRel}_k$ which makes it clear that $\mathsf{AffLagRel}_{\mathbb{F}_p}$ can be regarded as a fragment of the ZX-calculus:

Theorem 5.26 (The symplectic ZX-calculus)**.**

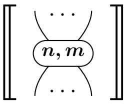
$\mathsf{AffLagRel}_k$ *is generated by two spiders both decorated by the additive group of k^2 as well as scaling gates when k is not a prime field:*



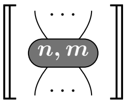
The spider fusion is pointwise:



Call the first component of the phase group the **affine phase** and the second component the **linear phase**. The white spider corresponds to the Z-basis and the grey spider corresponds to the X-basis. In Hilbert spaces, the spiders $\ell \to k$ are interpreted as follows:

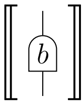


$$= \sum_{a=0}^{p-1} e^{\pi\cdot i/p(n\cdot a+m\cdot a^2)}|a,\dots,a\rangle\langle a,\dots,a|$$



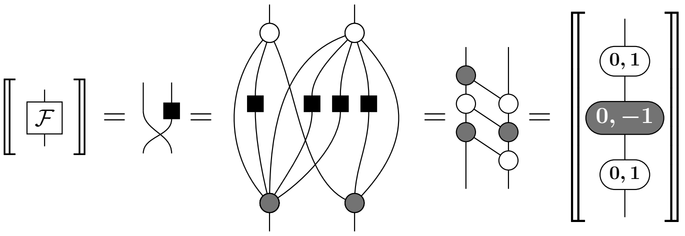
$$= \sum_{a=0}^{p-1} e^{\pi\cdot i/p(n\cdot a+m\cdot a^2)}\mathcal{F}^{\otimes k}|a,\dots,a\rangle\langle a,\dots,a|(\mathcal{F}^{\dagger})^{\otimes \ell}$$

The scaling gate, which is a derived generator in this setting is interpreted as:



$$= \sum_{a=0}^{p-1} |a\cdot b\rangle\langle a|$$

Recall that from Corollary 5.10 that the Fourier transform derived from the decomposition we discussed in the previous section:



In the ZX-calculus literature, this decomposition of the Fourier transform is *Euler decomposition*, coined by Duncan and Perdrix [DP09]. To my knowledge, this way in which Hopf algebras are used to derive the Euler decomposition was not previously known. Although in the quantum literature, as previously discussed, this same rule describes the "external" interaction of $\mathcal{C}_{\mathcal{X}}$ gates (as opposed to the "internal" interaction of phases).

This view of quopit stabilizer circuits in terms of the ZX-calculus means that the phase groups for the Z and X-spiders are the torus $(\mathbb{Z}/p\mathbb{Z})^2$ as noted by Ranchin [Ran16, Page 166]. This is in contrast to the qubit case where the phase groups are $\mathbb{Z}/4\mathbb{Z}$; which Coecke et al. point out as a crucial difference between Spekkens' toy model and qubit stabilizer theory [CES11]. However over $\mathbb{F}_2$ when the phases are restricted to the subgroup:

$$\mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z};\ a \mapsto 2a$$

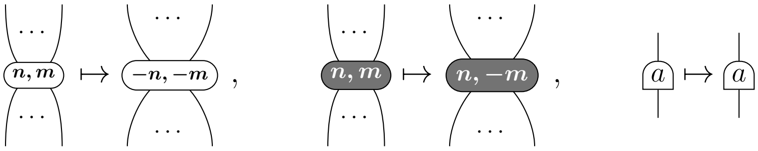
and for odd prime p, over $\mathbb{F}_p$ when the phases are restricted to the subgroup

$$\mathbb{Z}/p\mathbb{Z} \subseteq (\mathbb{Z}/p\mathbb{Z})^2;\ a \mapsto (a, 0)$$

these both uniformly pick out the qupit biaffine fragment of the ZX-calculus from Definition 3.33.

Up until now, we have also neglected to relate the symplectic picture to the †-structure of FHilb. This will be instrumental in the following section:

Definition 5.27. There is a monoidal conjugation functor $\overline{(-)} : \mathsf{AffLagRel}_k \to \mathsf{AffLagRel}_k$ given by:



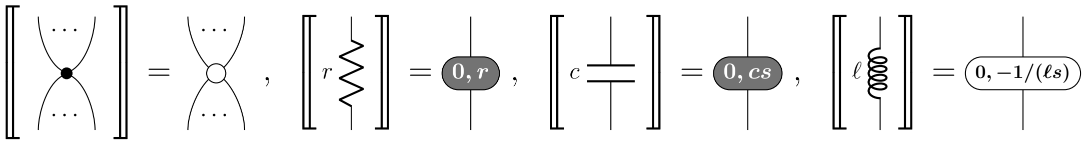
In the case of $k = \mathbb{F}_p$ for p an odd prime, this is transported to the complex conjugation along $\mathsf{AffLagRel}_{\mathbb{F}_p} \cong \mathsf{Stab}_p$:

Lemma 5.28. *For odd prime p, $\mathsf{AffLagRel}_{\mathbb{F}_p}$ and Stab_p are isomorphic as †-compact closed categories.*

Proof. We know that all stabilizer states are of the form $C|0\rangle^{\otimes n}$ for C Clifford operator. We already gave the generators for the qupit Clifford group and know that they are unitaries with respect to the Hermitian adjoint.

The affine symplectomorphisms corresponding to the generators of the Clifford group can be easily verified to be unitaries with respect to the dagger $(-)^\dagger := (\overline{(-)})^*$. Moreover, $|0\rangle$ is an isometry in Stab_p with the Hermitian adjoint just as ○● is an isometry with respect to $(-)^\dagger := (\overline{(-)})^*$. □

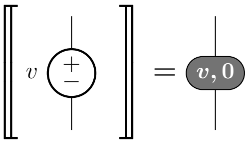
Remark 5.29. We restate the interpretation of passive electrical circuits in terms of phased spiders for affine Lagrangian relations. An idealized junction, a resistor with resistance r, a capacitor with capacitance c and an inductor with inductance ℓ are interpreted as:



In the work of Baez et al., the relational semantics of electrical circuits is broadened even further to capture current and voltage sources as affine Lagrangian relations over $\mathbb{R}(s)$ [BCR18]. A voltage source is a component with a fixed voltage v, imposes the affine Lagrangian relation:

$$\left\{ \left(\begin{bmatrix} z_0 \\ x_0 \end{bmatrix}, \begin{bmatrix} z_1 \\ x_1 \end{bmatrix} \right) \in \mathbb{R}(s)^{2(2)} \mid x_1 - x_0 = v, z_1 = z_0 \right\}$$

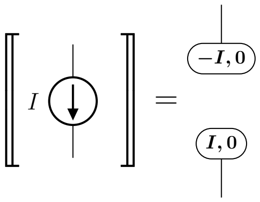
so that it is interpreted as the phased-spider:



Similarly a current source has a fixed current I, imposing the affine Lagrangian relation:

$$\left\{ \left(\begin{bmatrix} z_0 \\ x_0 \end{bmatrix}, \begin{bmatrix} z_1 \\ x_1 \end{bmatrix} \right) \in \mathbb{R}(s)^{2(2)} \mid z_0 = I = z_1 \right\}$$

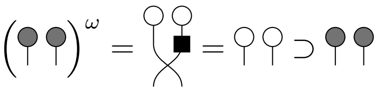
so that it is interpreted as the following diagram:



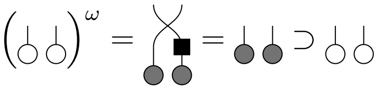
5.4 Affine coisotropic relations and mixed stabilizer circuits

In this section we show that by only requiring that the morphisms are affine *coisotropic* subspaces (subspaces V so that $V^\omega \subseteq V$) instead of affine Lagrangian subspaces (where $V^\omega = V$), we can capture the maximally mixed state/discarding; with which we can recover state preparation and measurement compositionally.

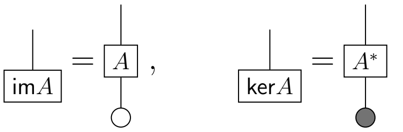
Remark 5.30. The cozero linear relation $2n \to 0$ is an isotropic subspace since:



And dually the discard linear relation $0 \to 2n$ is coisotropic since:



Recall from Lemma 2.57 that given a matrix $A : n \to m$ in cb_k:



Therefore, if we ask that A is a Lagrangian relation rather than matrix, we find that kernels of Lagrangian relations are isotropic subspaces and the images are coisotropic subspaces.

All (co)isotropic subspaces are generated in this way:

Theorem 5.31 (Symplectic Stinespring dilation)**.** *Every coisotropic subspace of* k^{2n} *of dimension* $n+m$ *is the image of a Lagrangian isometry* $m \to n$*.*

Proof. Suppose that we have a coisotropic subspace V^ω of k^{2n} with dimension $n+m$. Then V is an isotropic subspace of k^{2n} with dimension $n-m$. Applying Fourier transforms, we obtain a subspace symplectomorphic to V generated by a matrix whose pivots are all in the Z block. Therefore, we can row reduce this matrix to obtain one of the following form:

$$\left[\begin{array}{cc|cc} I_{n-m} & Z_B & X_A & X_B \end{array}\right]$$

By applying C_a gates from the first $n-m$ wires to the last m wires, we obtain an isotropic subspace V' generated by a matrix of the following form:

$$\left[\begin{array}{cc|cc} I_{n-m} & 0 & X'_A & X'_B \end{array}\right]$$

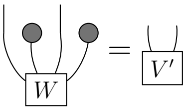
Therefore we have $V' = UV$ for a symplectomorphism U. Since all of the rows of the basis for V' are orthogonal with respect to the symplectic form, we have:

$$\begin{aligned} 0 &= \left[\begin{array}{cc|cc} I_{n-m} & 0 & X'_A & X'_B \end{array}\right] \omega \left[\begin{array}{cc|cc} I_{n-m} & 0 & X'_A & X'_B \end{array}\right]^T \\ &= \left[\begin{array}{cc|cc} I_{n-m} & 0 & X'_A & X'_B \end{array}\right] \left[\begin{array}{cc|cc} -X'_A & -X'_B & I_{n-m} & 0 \end{array}\right]^T \\ &= I_{n-m}(-X'_A)^T + 0(-X'_B)^T + X'_A I_{n-m} + X'_B 0 \\ &= (-X'_A)^T + X'_A \end{aligned}$$

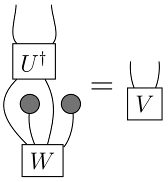
So that $X'_A = (X'_A)^T$ is a symmetric matrix. Therefore, the following matrix generates a graph state, and thus a Lagrangian subspace of $k^{2(n+m)}$:

$$\left[\begin{array}{ccc|ccc} I_{n-m} & 0 & 0 & X'_A & X'_B & 0 \\ 0 & I_m & 0 & (X'_B)^T & 0 & I_m \\ 0 & 0 & I_m & 0 & I_m & 0 \end{array}\right]$$

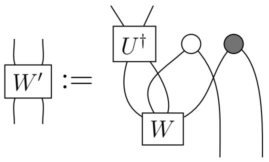
Let $W \subseteq k^{2(n+m)}$ be the Lagrangian subspace generated by this matrix. Then



And thus



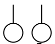
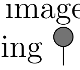
Therefore, V^ω is the image of the Lagrangian relation:

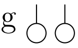
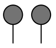


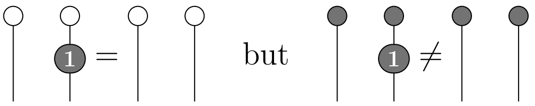
which is an isometry.

□

Corollary 5.32. *Every affine coisotropic subspace of k^{2n} of dimension $n+m$ is the image of a an affine Lagrangian isometry $m \to n$.*

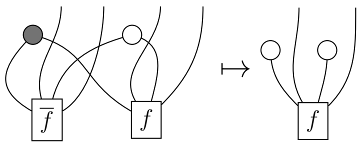
Remark 5.33. More concretely the prop is $\mathsf{CoIsotRel}_k$ is generated by adding  to the image of the embedding $\mathsf{LagRel}_k \hookrightarrow \mathsf{LinRel_k}$; and dually, $\mathsf{IsotRel}_k$ is generated by adding  to $\mathsf{LagRel}_k \hookrightarrow \mathsf{LinRel_k}$. So that the symplectic complement extends to an isomorphism of props $(-)^\omega : \mathsf{CoIsotRel}_k \cong \mathsf{IsotRel}_k$.

The props $\mathsf{AffCoIsotRel}_k$ and $\mathsf{AffIsotRel}_k$ are generated by respectively adding  and  to the images of the embeddings $\mathsf{AffCoIsotRel}_k, \mathsf{AffIsotRel}_k \hookrightarrow \mathsf{AffRel}_k$. However, in this case, they are not isomorphic as:



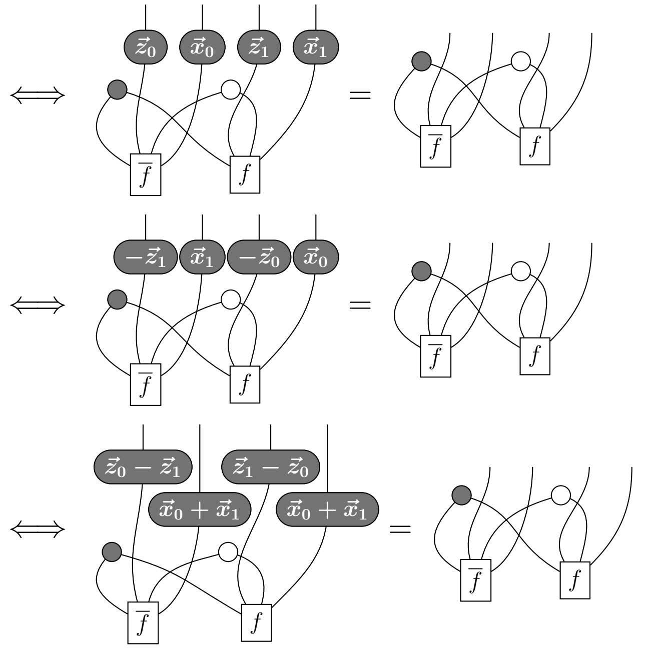
Theorem 5.34. $\mathsf{CPM}(\mathsf{AffLagRel}_k, \overline{(-)}) \cong \mathsf{AffCoIsotRel}_k$

Proof. Consider the identity on objects map $\mathsf{CPM}(\mathsf{AffLagRel}_k, \overline{(-)}) \to \mathsf{AffCoIsotRel}_k$, sending:



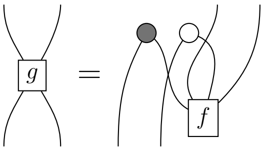
This is clearly bijective on objects. This is full by Corollary 5.32. So we just have to show that it is faithful and well defined. Take some $\widehat{f} \in \mathsf{CPM}(\mathsf{AffLagRel}_k, \overline{(-)})(0, n)$ with purification f. Then for $\vec{z}_0, \vec{x}_0, \vec{z}_1, \vec{x}_1 \in k^n$:

$$(\vec{z}_0, \vec{x}_0, \vec{z}_1, \vec{x}_1) \in \widehat{f} \iff$$

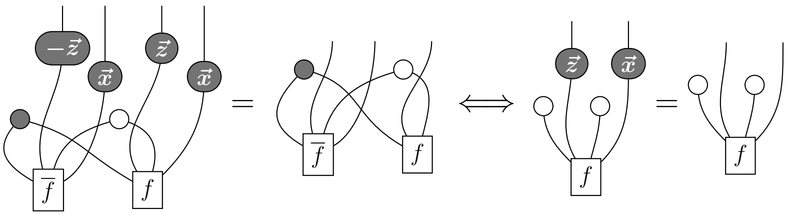


$$\iff (z_0 - \vec{z}_1, \vec{x}_0 + \vec{x}_1, z_1 - \vec{z}_0, \vec{x}_0 + \vec{x}_1) \in \widehat{f}$$

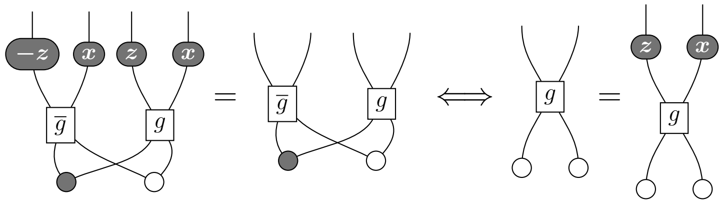
Therefore, maps in $\mathsf{CPM}(\mathsf{AffLagRel}_k, \overline{(-)})(0, n)$ are determined by their diagonal elements $(-z, x, z, x)$. Take:



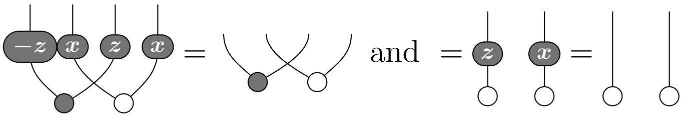
Therefore the following logical equivalence:



is equivalent to the following logical equivalence:



We prove the latter logical equivalence. If g is the identity, then for all $(z, x) \in k^{2n}$:



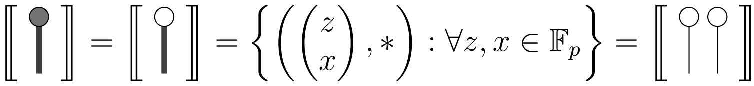
Given any map $g : m \to n$ in $\mathsf{AffLagRel}_k$, regarded as a state, we know that (z, x) is a stabilizer for g precisely when $(-z, x)$ is a stabilizer for $\overline{g}$. However, we know that the cup discards these diagonal stabilizers on the bottom of $\overline{g}$ and the codiscard map discards all Weyl operators.

□

Corollary 5.35. *For odd prime p:*

$$\mathsf{AffCoIsotRel}_{\mathbb{F}_p} \cong \mathsf{CPM}(\mathsf{AffLagRel}_{\mathbb{F}_p}) \cong \mathsf{CPM}(\mathsf{Stab}_p)$$

That is, adding the discard relation to $\mathsf{AffLagRel}_{\mathbb{F}_p}$ *gives a semantics for quopit* **mixed stabilizer circuits** *and mixed circuits in Spekkens' qubit toy model. Graphically:*



By mixed stabilizer circuits, we mean stabilizer circuits which can be obtained by discarding part of a pure stabilizer circuit, not an arbitrary convex combination of stabilizer circuits. Note that the terms "stabilizer mixed state/circuit" and "mixed stabilizer state/circuit" can interchangeably refer to either notion.

Mixed stabilizer states are also known as **stabilizer codes** for reasons that will become clear in Section 5.5. Mixed qubit biaffine stabilizer states are often called **CSS codes**, but there seems to be some ambiguity in the literature regarding wether to allow affine Z/X phases.

This is conceptually very close to the result of Huot and Staton where they show that the affine completion of isometries between finite dimensional Hilbert spaces, which freely adds a discard map, yields completely positive trace-preserving maps [HS19]. And even more similar, to the more refined result of Carette et al., where they show that various fragments of the ZX-calculus can be augmented with quantum discarding by freely adding a generator which discards isometries [CJPV21].

Although in our case the quantum discarding is interpreted as the literal *discard relation* of the corresponding stabilizers, therefore our semantics never departs from affine relations.

It was already known that stabilizer codes are in bijection with affine isotropic subspaces; for example, this was observed by Gross [Gro06, Section A]. Indeed affine coisotropic subspaces are in bijection with affine isotropic subspace by taking the symplectic complement of the linear component of the affine subspace; however, as noted in Remark 5.33, $\mathsf{AffIsotRel}_{\mathbb{F}_p} \not\cong \mathsf{AffCoIsotRel}_{\mathbb{F}_p}$, so their compositions as affine relations are different. The interpretation of the doubled cozero as the quantum discard map is not sound with respect to relational composition. This is closely related to the discrete Wigner function of Gross which we will comment further on in Remark 5.40.

This formalizes the relationship between mixed stabilizer circuits and stabilizer tableaux with not-necessarily-full rank in a compositional way. It is standard, and indeed very useful to interpret a stabilizer state in terms of its stabilizer tableau: which is an augmented basis $L + a$ of an affine isotropic subspace. In order to compose these tableaux, one must take the symplectic complement of the linear component of both spaces, and then compute their relational composition as affine coisotropic relations. Then the stabilizer tableau for this composite is obtained by taking the symplectic complement on the linear component once again.

Absolutely remarkably, and seemingly out of nowhere, the Weyl-free mixed quopit stabilizer circuits modulo invertible scalars can be expressed in terms of an iterated CPM construction[1] with respect to the orthogonal complement at the inner level, and the complex conjugation at the outer level:

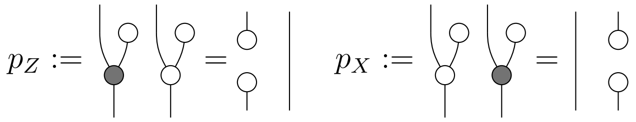
Corollary 5.36. *Given a prime p:*

$$\mathsf{IsotRel}_{\mathbb{F}_p} \cong \mathsf{CoIsotRel}_{\mathbb{F}_p} \cong \mathsf{CPM}(\mathsf{CPM}(\mathsf{LinRel}_{\mathbb{F}_p}, (-)^{\perp}), \overline{(-)})$$

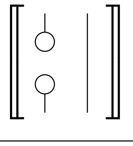
The middle isomorphism holds by fixing the affine shift to be 0. The astounding symmetry involved here raises the question if iterating the CPM construction more times; or with respect to different group representations. Perhaps the work of Gogioso can shed some light on this question [Gog19].

In order to add measurement and state preparation in the symplectic setting we inspect the structure of the Z and X projectors:

Definition 5.37. The Z and X projectors are defined as follows in $\mathsf{AffCoIsotRel}_k$:



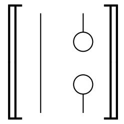
The Z projector discards and then codiscards the Z-gradient: cutting the Z gradient in two so that no information is preserved, while acting trivially on the X gradient. Dually for the X projector. Concretely, these are interpreted as the following relations:



$$= \left\{ \left(\begin{bmatrix} z \\ x \end{bmatrix}, \begin{bmatrix} z' \\ x \end{bmatrix} \right) \in k^{2+2} \mid \forall z, z', x \in k \right\}$$

---

[1] Recalling Definition 3.2.



$$= \left\{ \left(\begin{bmatrix} z \\ x \end{bmatrix}, \begin{bmatrix} z \\ x' \end{bmatrix} \right) \in k^{2+2} \mid \forall z, x, z' \in k \right\}$$

Recallling Definition 3.6 we split one of these projectors:

Definition 5.38. Denote the two-coloured prop generated by splitting p_Z in $\mathsf{AffCoIsotRel}_k$ by

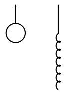
$$\mathsf{AffCoIsotRel}_k^M := \mathsf{Split}_{\{p_Z^{\otimes n}, 1_n | n \in \mathbb{N}\}}(\mathsf{AffCoIsotRel}_k)$$

Let $Q = (1_1, 1_1)$ denote the original object and $C = (1_1, p_Z)$ the object obtained by splitting p_Z. In the quantum setting, the object Q can be interpreted as a quantum channel and the object C as a classical channel.

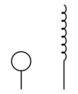
We could have instead split p_X, or split both p_X and p_Z; however, all three of these coloured props are equivalent. This equivalence is witnessed via the Fourier transform. Indeed this suffices to split all nonzero projectors up to isomorphism because all projectors of the same dimension are affine symplectomorphic. It is important to remark that the choice of projectors which are split effects the code-distance, because code-distance is basis dependent, and not invariant under equivalence.

This category has a succinct presentation; adding the affine relations to $\mathsf{AffCoIsotRel}_k$ obtained by cutting/splitting the Z projector in two:

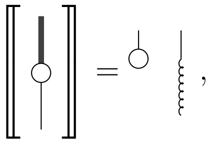
Theorem 5.39. *The full subcategory of* $\mathsf{AffCoIsotRel}_k^M$ *generated by tensor powers of* C *is isomorphic to* AffRel_k. *Therefore* $\mathsf{AffCoIsotRel}_k^M$ *is isomorphic to adding the following linear relations to the image of* $\mathsf{AffCoIsotRel}_k^M \to \mathsf{AffCoIsotRel}_k$ *in the way which makes this into a two-coloured prop:*

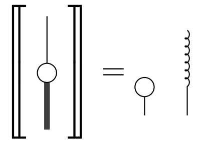


and

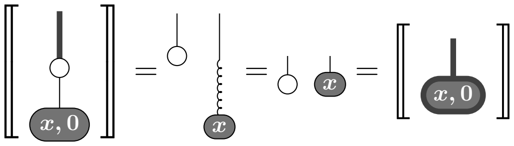


We draw the wire associated to C as a coil to indicate the type (although this is just syntactic sugar). In the quantum setting, the classical state "lives" on a single wire and the stabilizer state "lives" on the doubled wires. Because of this, the aforementioned circuits are interpreted in terms of state preparation and measurement in the Z-basis:

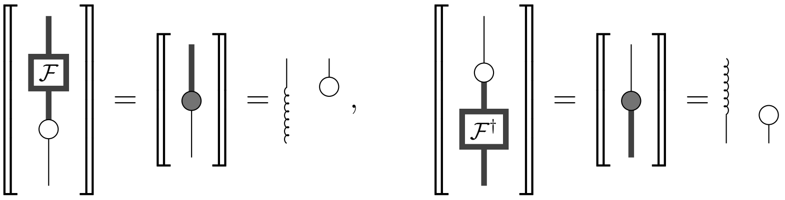




For example, given any classical dit $x \in \mathbb{F}_p$, to prepare the state $|x\rangle$ is to take the composite:



The state preparation and discarding in the X-basis are obtained by composition of these morphisms with the Fourier transform; yielding morphisms which discard the X wire instead of the Z wire:



Remark 5.40. Compare this relational semantics of measurement to the discrete Wigner function of Gross [Gro06]; which is the discrete version of the Wigner's quasi-probabilty distribution [Wig32]. Gross shows that on quopit stabilizer states, this is a probability distribution given by the indicator function of an affine Lagrangian subspace [Gro06, Lemma 9] (actually it works just as well for stabilizer codes/affine coistropic subspaces):

$$P_{G(L+a)} : \mathbb{F}_p^{2n} \to [0,1);\ (z,x) \mapsto 1/|L| \cdot \delta_{L+a}(z,x) = \begin{cases} 1/|L| & \text{if } (z,x) \in L+a \\ 0 & \text{otherwise} \end{cases}$$

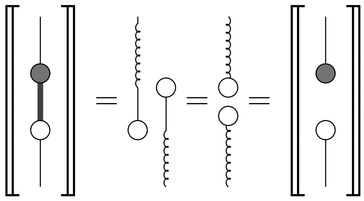
This probability distribution is uniform so that every outcome is equally likely. For example, the measurement of a stabilizer state $G(L+a)$ in the Z basis produces outcome $|x\rangle$ with probability:

$$\sum_{z \in \mathbb{F}_p} P_{G(L+a)}(z,x)$$

Moreover, this marginalization over z acts backwards on the state; so that in accordance with Spekkens toy model, the observer gains at most one pit of information by sampling x, but injects at most one pit of uncertainty back into the ontic state.

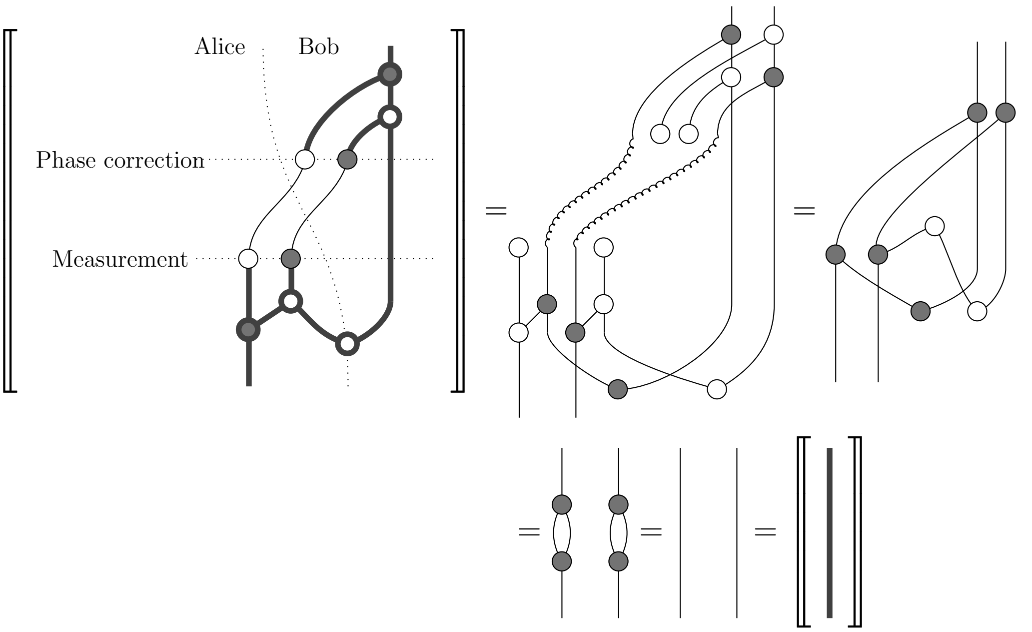
In the conventional, functional approaches to measurement of stabilizer states/states in Spekkens' toy model, for example Catani and Browne construct "measurement update rules" to compute this back action on the state [CB17]. This is essentially the same procedure performed to compute the effect of measuring a qubit stabilizer states, as described in the paper of Aaronson and Gottesman [AG04]. However, in the relational paradigm, the measurement outcome, the measurement update, the state preparation and the unitary evolution of the quantum state are all computed in the same way: by taking the relational composition.

Remark 5.41. Recall that in Lemma 3.11, we used the Hopf rule to show that preparing Z-basis and then measuring in the X-basis preserves no information. In the symplectic picture, this result becomes purely topological:



For this reason, we can prove the correctness of the qupit quantum teleportation algorithm discussed previously in Protocol 3.12 using only spider fusion:

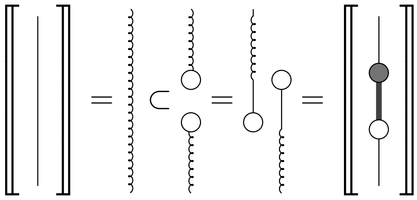
Example 5.42. Given any prime p, the following equations of string diagrams in $\mathsf{AffCoIsotRel}^{M}_{\mathbb{F}_p}$ proves the correctness of the quantum teleportation protocol where Alice on the left teleports a quopit to Bob, on the right. They share a Bell state (on the bottom of the diagram) and two classical dits (drawn as coiled wires).



Because $\mathsf{AffCoIsotRel}^{M}_{\mathbb{F}_p}$ is a subcategory of relations, composable maps are ordered by subspace inclusion (ie, it is poset-enriched). Moreover, since all possible outcomes are equally likely we can identify when the measurement statistics of one process arise from the marginalization of the measurement statistics of another process:

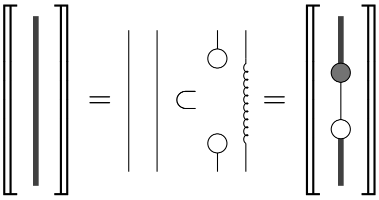
Definition 5.43. Take two quopit stabilizer circuits with state preparations and measurement f, g interpreted as parallel maps in $\mathsf{AffCoIsotRel}^{M}_{\mathbb{F}_p}$. Then f is a **coarse-graining** of g when $f \subset g$ is a (strict) affine subspace.

Example 5.44. For an extreme example, the circuit obtained by preparing in the Z-basis and measuring in the X-basis is a coarse-graining of the identity circuit on a classical wire:



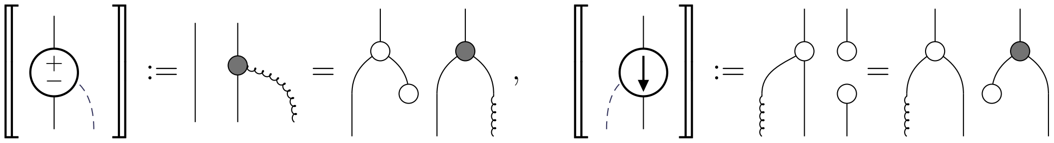
This follows from unit of the adjunction for the counit in the Cartesian bicategory of relations $\mathsf{AffRel}_{\mathbb{F}_p}$ (see Definition 2.60). Conceptually, this is because, given any input state, the circuit on the right hand side can produce any output state; however, the identity circuit forces the inputs to be the same as the outputs.

Example 5.45. Similarly, the decoherence map is a coarse-graining of the identity on a quantum wire :

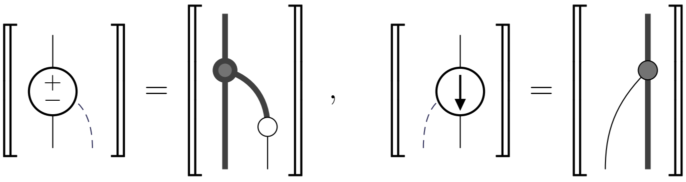


5.4.1 Electrical circuits with control and measurement

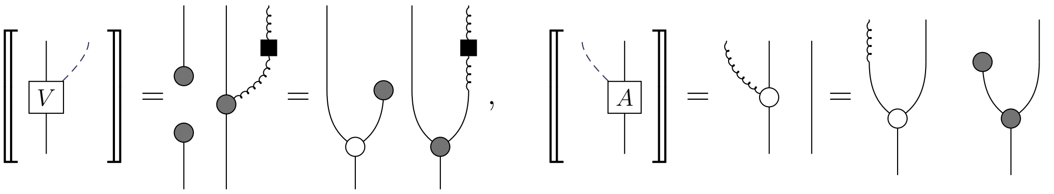
This coloured view of things recaptures Boisseau and Sobociński's relational semantics for controlled voltage and current sources as well as ammeters and voltmenters [BS22], but now in a symplectic setting. However the situation is more nuanced than for quantum circuits. $\mathsf{AffCoIsotRel}^{M}_{\mathbb{R}(x)}$ gives a semantics for all of the electrical circuit components we have discussed so far in addition to the controlled voltage and current sources:



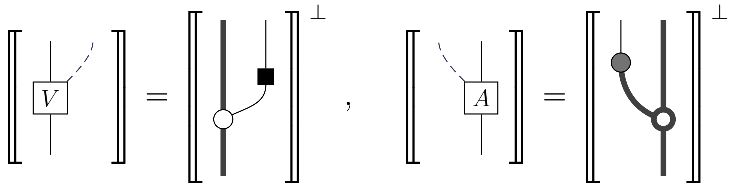
Or in thick-thin spider notation, the controlled voltage and current sources have the following form:



On the other hand the dual two-coloured prop $\mathsf{AffIsotRel}^{M}_{\mathbb{R}(x)}$ gives a semantics for all of the uncontrolled components we have discussed so far as well as voltmeters and ammeters:

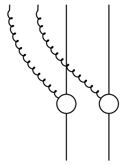


These are the orthogonal complement of the interpretation of stabilizer thick-thin spiders in terms of linear relations:



The controlled voltage source is the electrical circuit analogue of a X-phase correction in quantum circuits. Similarly, the controlled current source is the transpose of a measurement in the X-basis. However the voltmeters and ammeters have no quantum analogue.

Just as Spekkens' toy model can be interpreted as an epistemically restricted toy theory of quantum circuits; by dualizing things, we could also ask what properties of quantum mechanics hold in $\mathsf{AffIsotRel}_{\mathbb{F}_p}^{M}$. This is an "ontologically restricted" toy theory of quantum mechanics; or equivalently an epistemically "co-restricted" toy theory. In other words, where there is a *minimum* amount of knowledge the observer has about the ontic state so that discarding a state imposes extra equations on the epistemic state. We showed how affine isotropic relations are not compatible with discarding; however this view of measurement is not compatible with quantum theory for the following reason. If we added the quantum analogue of ammeters to our relational semantics of pure stabilizer circuits, we could compose the ammeter with another ammeter conjugated by the symplectic Fourier transform as follows:



This would allow us to simultaneously measure the Z and X observables which is not possible in quantum mechanics due to the uncertainty principle.

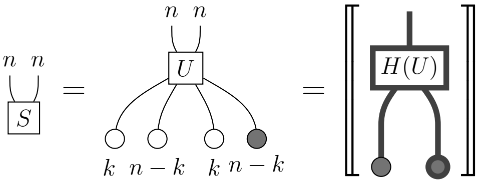
5.5 Error correction

In this section, we show how to implement quantum error correction protocols for stabilizer codes using the string diagrams we developed in the previous section. See the work of Gottesman [Got97] or Nielsen and Chuang [NC10] for reference on stabilizers codes and error correction. Nothing in this section is particularly novel from a technical point of view; however, it is conceptually different from the way that stabilizer codes are usually explained.

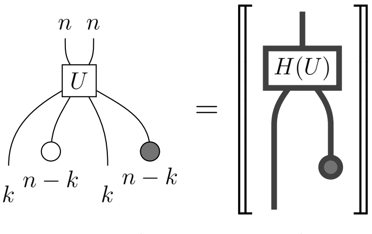
The graphical algebra approach to error correction which we employ in this section strictly generalizes that of Kissinger [Kis22], where CSS codes are interpreted in linear relations over $\mathbb{F}_2$.

Fix an odd prime local dimension p. Consider an affine coisotropic subspace $S = L + a \subseteq \mathbb{F}_p^{2n}$ where L has dimension $n+k$ (or for qubits take an affine coisotropic subspace $S = L + a \subseteq \mathbb{F}_p^{2n}$ without linear phase). Then the associated projector on n-quopits is called a $[n, k]$-stabilizer code, as it encodes k logical quopits into n physical quopits. The relationship between logical and physical quopits can be understood in terms of pictures. We will draw the doubled string diagrams for calculation accompanied by the quopit stabilizer thick-thin spider diagrams to give a less cluttered presentation.

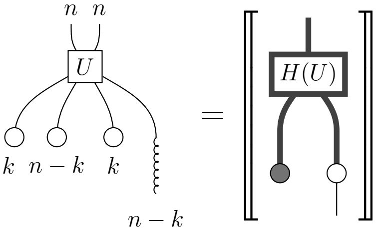
Recalling Corollary 5.32, fix a unitary dilation U of S:



The induced isometry, called the **encoder**, embeds k logical quopits into n physical quopits:

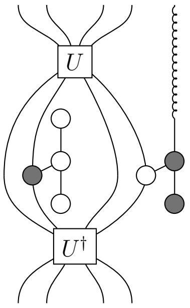


Splitting this projector fixes a basis $\{b_1, \ldots, b_{n-k}\}$ for L^ω which fixes the possible measurement outcomes:

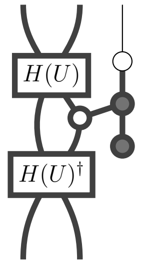


Suppose that Alice encodes a state on k logical qupits into n physical qupits using this isometry and then sends it to Bob on a noisy quantum channel. Recall from Lemma 3.26 that Weyl operators form a unitary operator basis. So that given any error on a quantum channel we can decompose it as a linear combination of Weyl operators $\mathcal{W}(e)$.

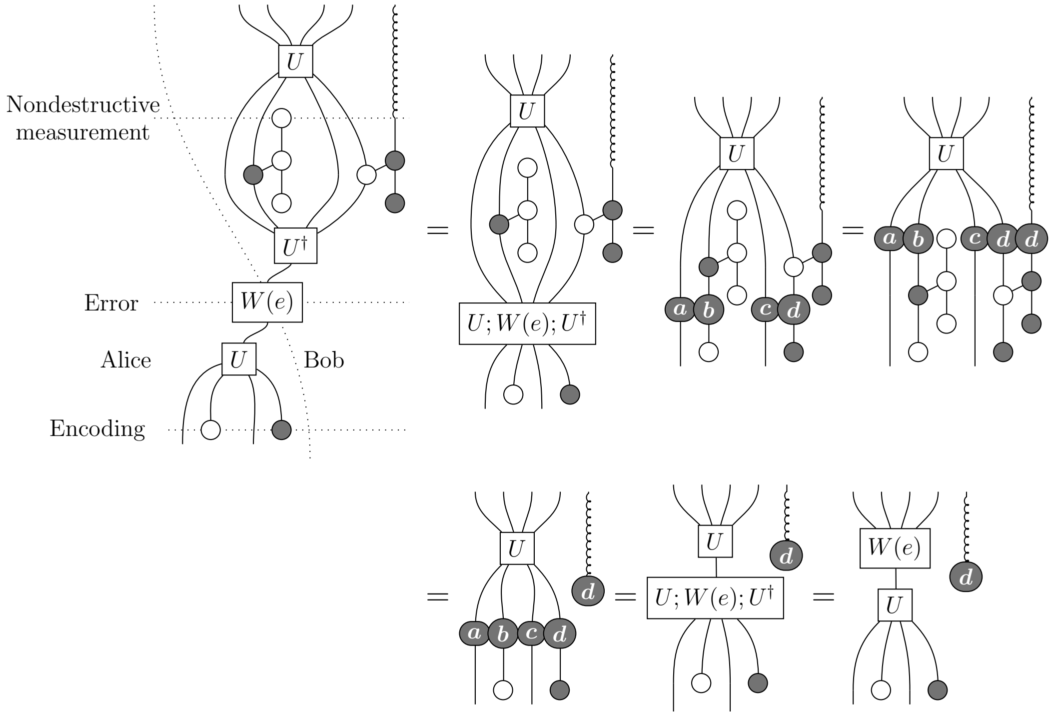
To detect the error, Bob applies the non-destructive measurement with respect to $H(U)(1_k \otimes \mathcal{Z}^{\otimes(n-k)})H(U)^\dagger$, which we draw in our calculus as follows:



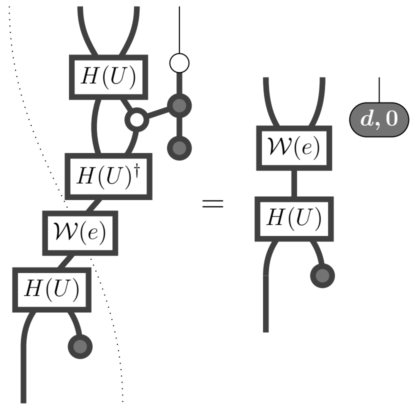
or in the thick-thin spider picture:



Because stabilizers preserve Weyl-operators under conjugation, in the symplectic picture, we have $W((a,b),(c,d)) = U; W(e); U^\dagger$. Therefore:



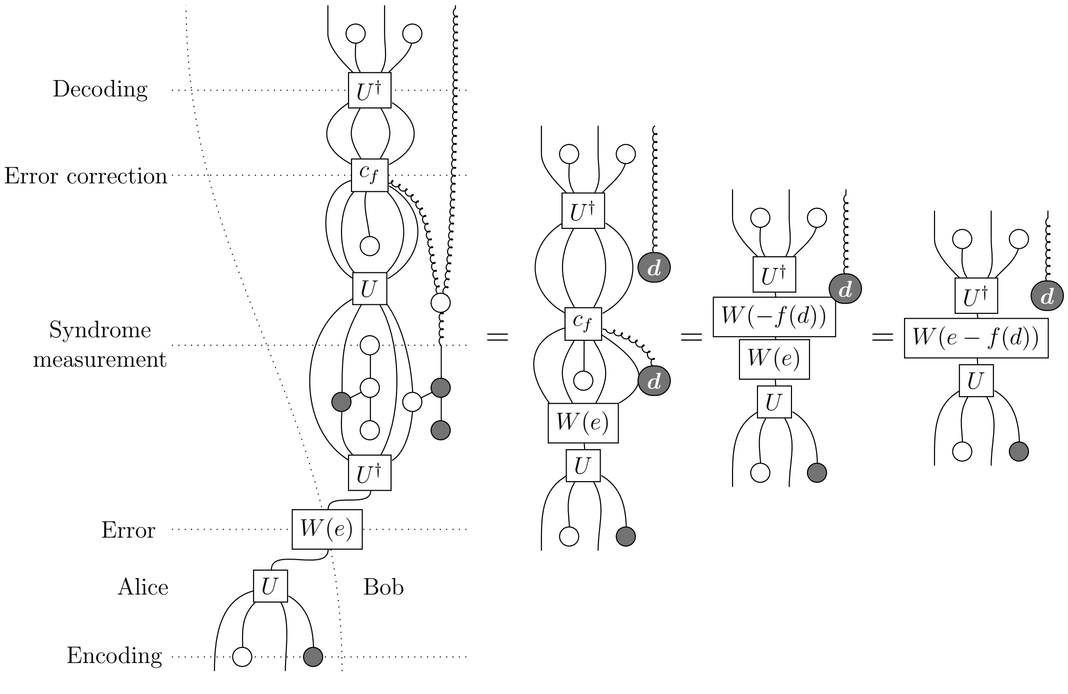
In the thick-thin spider picture, that is:



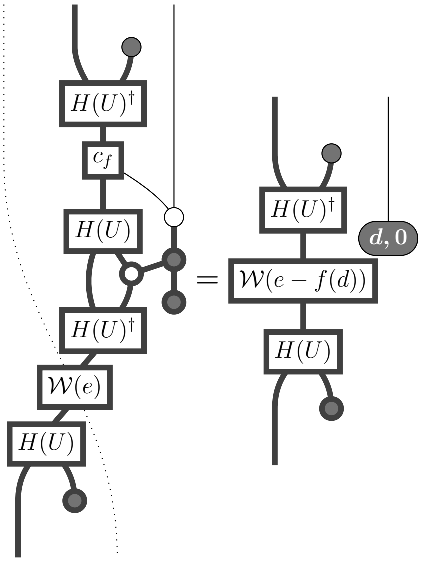
The tuple $d \in \mathbb{F}_p^{n-k}$ is called the **syndrome**. The syndrome measures the displacement of the basis elements b_i by errors. An error $W(e)$ is **undetectable** if and only if the syndrome is the zero vector; this is because e commutes with everything in $L + a$ meaning that $e \in L^\omega + a$. In particular, the trivial error is undetectable; so undetectable errors are indistinguishable from having no errors at all.

To correct for errors, given any nonzero syndrome measurement $d \in \mathbb{F}_p^{n-k}$, Bob picks an error $\mathcal{W}(e)$ which he wishes to correct. The choice of errors which Bob chooses to correct for determines a function $f : \mathbb{F}_p^{n-k} \to \mathbb{F}_p^{2n}$ sending $d \mapsto e$. Given syndrome d, Bob applies the operation $\mathcal{W}(-f(d))$ to his n quopits. Finally, Bob applies $U^\dagger$ to the quantum channel and then discards the last $n - k$ quopits.

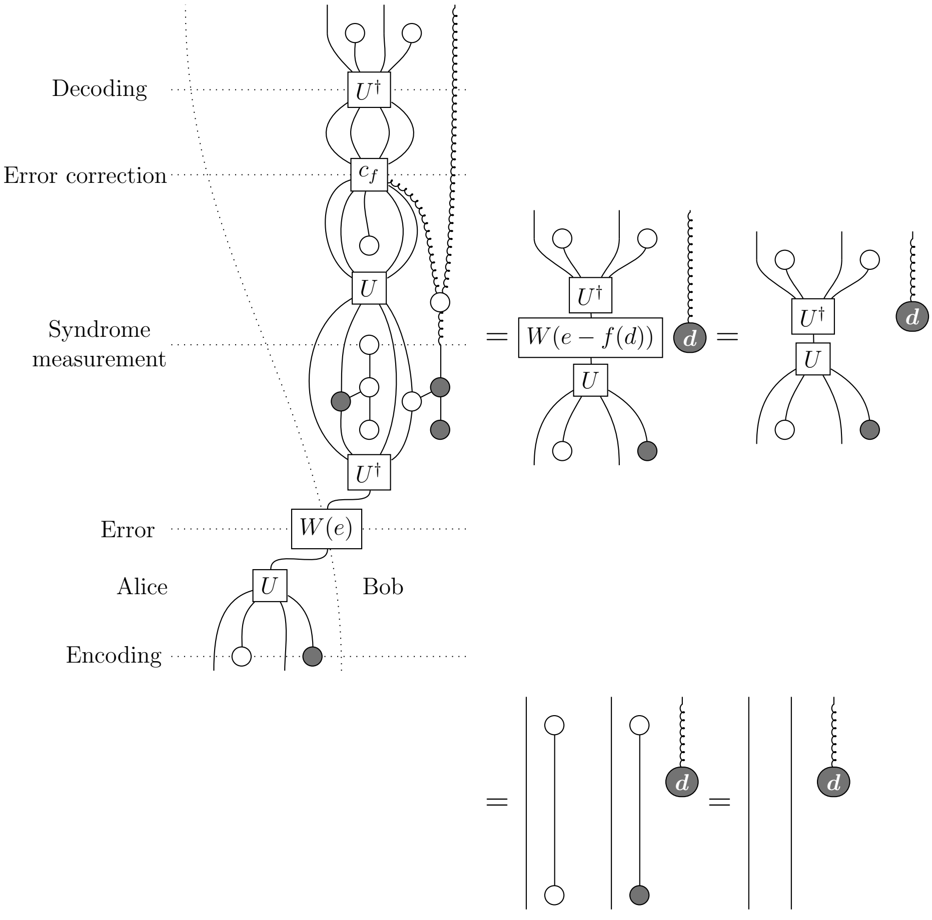
If f is an affine transformation, then there is a classically controlled operation $c_f : C^{\otimes(n-k)} \otimes Q^{\otimes n} \to Q^{\otimes n}$ which imeplements this controlled operation, so that:



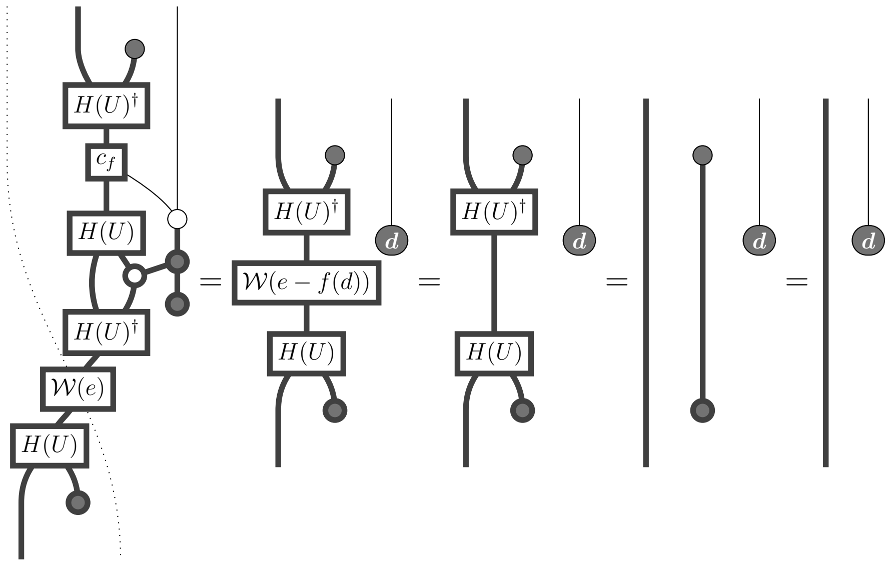
Or in the thick-thin spider picture:



So that if $e = f(d)$ then this reduces to the identity channel:



Or in the thick-thin spider picture:

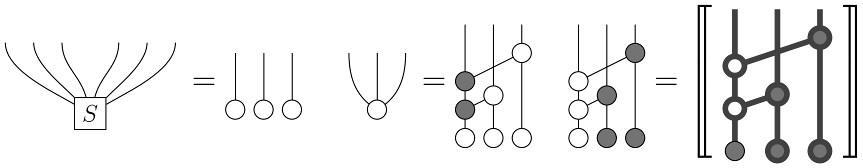


We use the threefold qubit repetition code (see [NC10, Section 10.1.1]) as an example (which is permissible within our calculus because it is a CSS code, that is, it has trivial linear phase):

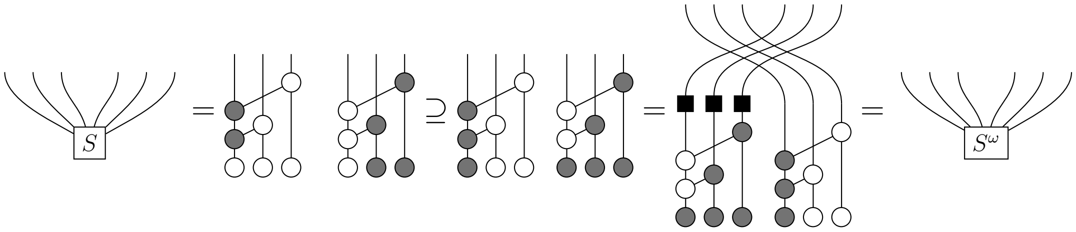
Example 5.46. Consider the Linear subspace:

$$S = \{((z_1, z_2, z_3), (x_1, x_2, x_3)) : x_1 = x_2 = x_3\} \subseteq \mathbb{F}_2^{2(3)}$$

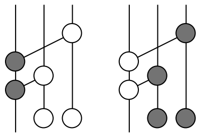
which can be written in the form of a circuit:



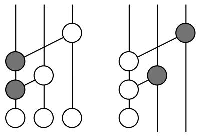
S is coisotropic because:



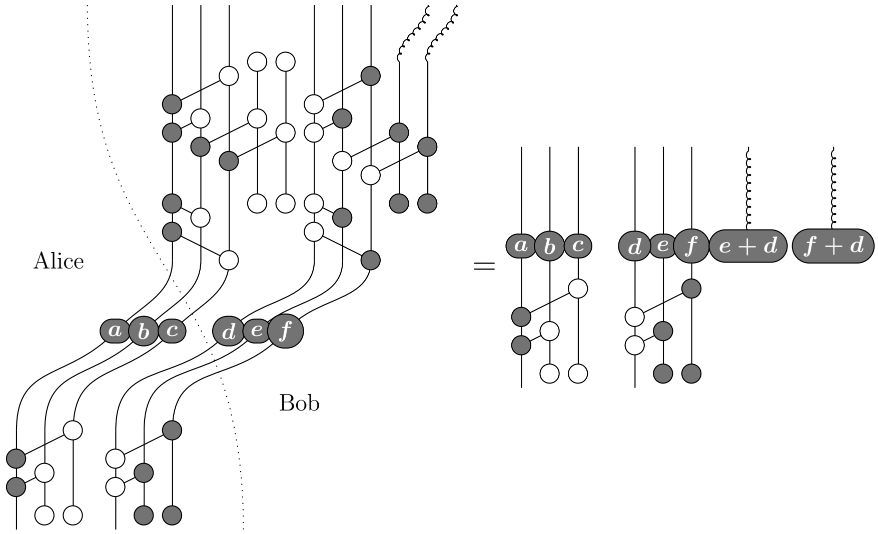
Chopping off the maximally mixed state gives us an encoding map:



Also, we will choose to measure in the Z-basis, so we split the projector:



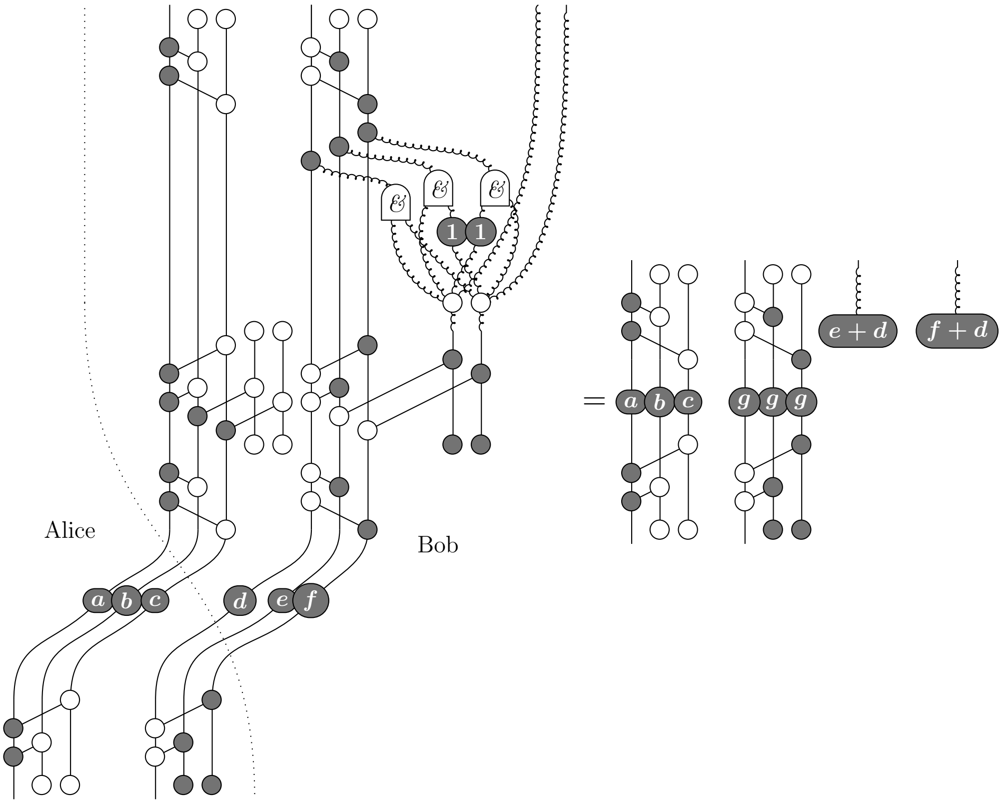
Suppose there is an error $W((a, b, c), (d, e, f))$, then we have the following error detection circuit:



Suppose we want to correct for single X errors, then we find that:

- An X error $(d, e, f) = (1, 0, 0)$ yields syndrome $(e + d, f + d) = (1, 1)$
- An X error $(d, e, f) = (0, 1, 0)$ yields syndrome $(e + d, f + d) = (1, 0)$
- An X error $(d, e, f) = (0, 0, 1)$ yields syndrome $(e + d, f + d) = (0, 1)$
- An X error $(d, e, f) = (0, 0, 0)$ yields syndrome $(e + d, f + d) = (0, 0)$

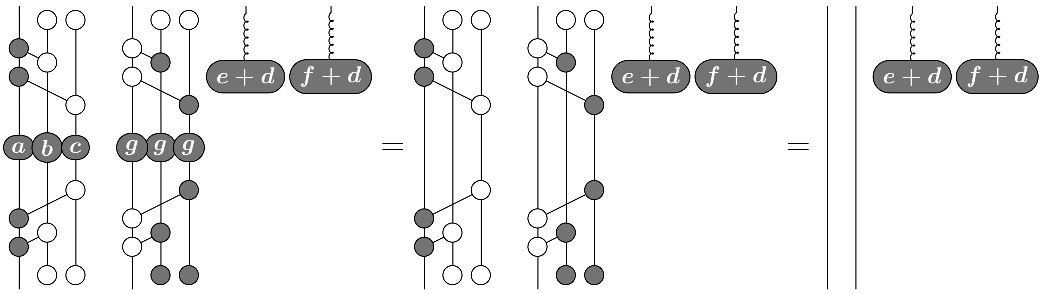
Therefore, we want to apply the correction $(s, t) \mapsto (st, s(t + 1), (s + 1)t)$. This is a nonlinear function, so we have to leave category $\mathsf{AffCoIsotRel}^{M}_{\mathbb{F}_p}$. The error correction protocol then has the following form:



where

$$g := d+(e+d)(f+d) = e+(e+d)(f+d+1) = f+(e+d+1)(f+d) = de+ef+fd \mod 2$$

If no more than one of d, e, f is 1 then $g = 0$. If furthermore $a = b = c = 0$, then:



Therefore this error correction protocol corrects for at most one X-error.

5.6 Discussion

It is important to note that the controlled operation we applied for the error correction step in the previous section requires nonlinear classical processing power, and therefore the diagram we drew doesn't "live" within the calculus $\mathsf{AffCoIsotRel}_{\mathbb{F}_p}^{M}$ we have constructed in this chapter.

Indeed, in this example, we have secretly been working in the pushout of the ffollowing diagram of coloured props:

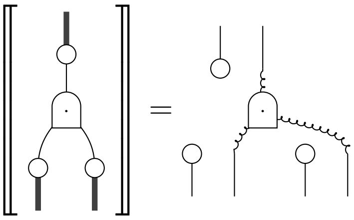
$$\mathsf{ZX\&}/\sim \leftarrow \mathsf{AffRel}_{\mathbb{F}_2} \rightarrow \mathsf{AffCoIsotRel}_{\mathbb{F}_2}^{M}$$

where $\mathsf{ZX\&}/\sim$ is the prop of qubit *relations* which we presented by taking a quotient of the prop $\mathsf{ZX\&}$. Moreover $\mathsf{AffRel}_{\mathbb{F}_2} \rightarrow \mathsf{ZX\&}/\sim$ sends linear subspaces to subsets; and $\mathsf{AffRel}_{\mathbb{F}_2} \rightarrow \mathsf{AffCoIsotRel}_{\mathbb{F}_2}^{M}$ sends

$$(n \xrightarrow{f} m) \mapsto (C^{\otimes n} \xrightarrow{(p_Z^{\otimes n}, f, p_Z^{\otimes m})} C^{\otimes n})$$

So we can regard the classical wires as being arbitrary subsets rather than affine subspaces. We can afford to do this because we gave $\mathsf{ZX\&}/\sim$ in the previous chapter; however, this is not very satisfying. We only have a presentation for the qubit version. This gives more motivation to actually work out a presentation for the quopit version of $\mathsf{ZX\&}/\sim$.

This raises the following question: what is the algebraic characterization of mixed stabilizer circuits/mixed CSS codes with nonlinear phase-correction. More concretely, what subcategory of affine relations is obtained by adding the decohered and gate:



Although we have given generators for $\mathsf{AffCoIsotRel}_k$, we have not given a complete set of relations. Note however, that there is an embedding $\mathsf{AffCoIsotRel}_k \hookrightarrow \mathsf{AffRel}_k$, and we already know that AffRel_k does admit a complete presentation. In the specific case for prime fields, our work combined with Booth et al.'s completeness result for the quopit stabilizer ZX-calculus [BC22] yields a complete presentation for $\mathsf{AffCoIsotRel}_{\mathbb{F}_p}$. The follow-up paper of Poór et al. which establishes a unique "AP-normal form" for quopit circuits greatly simplifies this presentation [PBC$^+$23] [2]. A completness result for arbitrary fields closely following their techniques is forthcoming [BCC24b].

Finding a presentation this fragment of the continuous variable ZX-calculus is closely related to the question of finding a graphical calculus for passive linear electrical circuits with current and voltage sources. Cockett et al. give a complete set of equations for the electrical circuits generated by ideal junctions and resistors [CKS23]. The normal form which they use involves a modified pivoting rule which

---

[2] A semantic version of this normal form also appeared in the paper of Cockett et al. [CKS23]; which is closely related to the "standard form" for qubit stabiliser codes of Cleve and Gottesman [CG97].

avoids rewriting the resistances to be negative. So finding a presentation for affine Lagrangian relations would be very close to adding current and voltage sources to the presentation of Cockett et al. [CKS23]. However, not every affine Lagrangian relation over $\mathbb{R}$ can be interpreted as an electrical circuit, so one would have to take extra care to answer this question. Perhaps the preceding paper of Cockett et al. [CKP22], motivated by connecting the relational semantics of electrical circuits and stabilizer circuits, could help answer this question. They give a normal form for circuits in LagRel_k, although not an explicit rewriting procedure.

The connection of the ZX-calculus to classical mechanical circuits is fascinating and leaves many questions open; however, once that the association is made with categories of affine Lagrangian/coisotropic relations, then this connection should not be surprising. Lagrangian relations were invented for classical quantization: the program of giving classical explanations for fragments of quantum mechanics [GS79]. Indeed, in a forthcoming paper we show how affine lagrangian relations over $\mathbb{R}$ can be extended... or affine Lagrangian relations over $\mathbb{C}$ can be restricted to give a semantics for Gaussian circuits with infinitely squeezed states [BCC24a]. Gaussian circuits are a tractable fragment of infinite dimensional quantum mechanics, analagous to how stabilizer circuits are a tractable fragment of finite dimensional quantum circuits (see Theorem 3.34). This approach suggests using categories of relations to give a compact closed semantics for infinite dimensional fragments of the ZX-calculus, as well as a concise way to deal with the problems involving dirac deltas. This is in contrast to the nonstandard analysis approach of Gogioso et al. which is significantly more powerful, yet complicated [GG17].

This connection also motivates finding generators and relations for classical mechanical systems. For the specific case of electrical circuits, there has already been some work in this direction [BS22, CKP22, CKS23]; however, the connection between the quantum ZX-calculus and these calculi for classical mechanical systems has not yet been exploited.

For example, using the technique developed by Baez et al. in [BE15] and applied to electrical circuits in the followup paper [BCR18], $\mathsf{AffCoIsotRel}_{\mathbb{F}_p(s)}$ apparently gives a notion of mixed stabilizer circuits with discrete-time evolution. What is the physical interpretation of this? Similarly, could the impedence boxes of Boisseau et al. [BS22] be used for quantum circuits?

Going in the other direction, there are already tools for rewriting ZX-diagrams [KZ15, KW20a, Vara, Varb]. ZX-diagram simplification has been used to optimize quantum circuits [DKPW20, KW20b]; however quantum computers are not currently useful. This motivates modifying the software and techniques for quantum circuit simplification to be used in the domain of classical mechanical systems. Such systems exist everywhere where there is a notion of Hamiltonian flow: for example, networks of roads through which traffic flows, computer networks through which information flows, factories through which goods flow, and so on. The potential industrial applications in control theory motivate further inquiry into this subject.

From a geometric viewpoint, this also motivates finding presentations for Lagrangian relations with respect to hyperbolic or parabolic form. In other words, mechanical systems where the phase space has uniformly positive or negative curvature: this would be presented by adding different generators to affine relations. The author suspects that, over odd prime fields, this may have applications in the theory of topological stabilizer codes.

Chapter 6

Conclusion

In this thesis, we have given nondeterministic semantics for two classes of circuits.

First, we gave a presentation $\mathsf{ZX}\&$ for the class of qubit circuits generated by the Toffoli gate, the not gate as well as the states $|0\rangle, \sqrt{2}|+\rangle$ and effects $\langle 0|, \langle +|\sqrt{2}$. We showed that this is isomorphic to the full subcategory of spans of finite sets (or equivalently matrices over the natural numbers) where the objects are powers of the 2 element set. We also imposed a quotient to give a presentation for the full subcategory of relations of finite sets (or equivalently matrices over the Boolean semiring) where the objects are powers of the 2 element set. In order to prove this, we gave a simpler characterization of the Cartesian completion of a discrete inverse category: which is one half of the equivalence between partially reversible and partial computing with copying. We restated this construction in terms of freely adding counits to the diagonal maps; and showed how this can be related to the construction of unnormalized stochastic systems from quantum systems. We analyzed the interaction of all of these generators and showed how larger and larger fragments of $\mathsf{ZX}\&$ can be constructed incrementally using pushouts and distributive laws; revealing the different nondeterministic/partial structures which occur along the way.

Secondly, we investigated the structure of stabilizer circuits; and showed how quopit stabilizer circuits are isomorphic to the prop of affine coisotropic relations over $\mathbb{F}_p$. To perform this, we studied the props of (affine) (co)isotropic and Lagrangian relations using graphical linear/affine algebra and the tools of categorical quantum mechanics. We gave generators for the each of these props and showed how over prime fields, Lagrangian relations can be presented as the CPM construction applied to linear relations with respect to the orthogonal complement. We showed that doubling the prop of (affine) Lagrangian relations again with respect to the symplectic generalization of complex conjugation, given any base field, yields the prop of (affine) coisotropic relations. We showed how by splitting the idempotents for the Z or X projectors one obtains a two-coloured prop where the state preparation and measurement maps have elegant relational interpretations. We showed how this gives a graphical semantics for mixed stabilizer circuits/stabilizer codes which are broadly used for quantum error correction. Also we related this semantics of mixed stabilizer circuits to relational semantics for electrical circuits.

In both of these two examples, these props are not only monoidal categories, but there are 2-cells between the maps themselves specifying when circuits with constrained behaviour can be coherently transformed into less constrained circuits. In the case of $\mathsf{ZX}\&$, this comes from the fact that it is a Cartesian bicategory. On the other hand, for qupit mixed stabilizer circuits, we showed how this embeds into the Cartesian bicategory of relations $\mathsf{AffRel}_{\mathbb{F}_p}$.

In this thesis, we have regarded circuits as subspaces respecting certain structures. By changing the structure which is respected, and thus the notion of subspace, one therefore yields different classes of circuits. This line of thinking leaves several threads open.

First, is to generalize $\mathsf{ZX}\&$ to qudits; providing semantics for other full subcategories of spans and relations of finite sets/matrices over the natural numbers and Booleans. In some sense, we have given the first model of "graphical algebraic geometry," to be compared with graphical linear algebra [BSZ17], graphical affine algebra [BPSZ19], graphical polyhedral algebra [BGS21], graphical piecewise-linear algebra [BP22]. Note that in some sense, our graphical analysis (affine) (co)isotropic relations is also the first step towards graphical symplectic algebra. Of course by splitting idempotents in $\mathsf{ZX}\&$ we would obtain presentations for the full categories matrices over the naturals and Booleans. The challenge is to find satisfying well-structured presentations of these categories, not an encoding of base n arithmetic in base 2. Doing so would potentially be the first step in proving completeness for qudit fragments of the ZH-calculus. We hinted at a potential way to solve this by computing Gröbner bases string-diagrammatically.

We also did not give a completely satisfying investigation into the connection between the two-sided (co)unital completion of the inverse products of a discrete inverse category and Cartesian bicategories (of the span-variety, not of relations). In general, it is natural to ask: when one takes the subcategory of partial isomorphisms of a Cartesian bicategory, when will the original Cartesian bicategory be recovered by adding units and counits to the inverse products. Is it enough to impose that the unit and counits be adjoint to each other, or will information about the original Cartesian bicategory be lost?

In terms of stabilizer circuits there are also many unanswered questions. First, is giving a presentation for affine coisotropic relations. This will not be too hard to do, given the recent developments on presenting quopit stabilizer circuits, as discussed in Section 5.6. This is a very important thing to work out, because of the close connection to Gaussian quantum mechanics. Even outside of the realm of quantum mechanics, giving a relational semantics thereof will possibly shed more light on the classical connection between Gaussian probability and nondeterminism as in the work of [SS22].

It would also be really interesting to augment our two-coloured semantics for stabilizer circuits and affine classical processing with stronger classical processing.

If the relational semantics for p-mode nonlinear classical nondeterministic circuits were combined with quopit stabilizer circuits, what sorts of quantum states could be constructed. Is this the convex hull of stabilizer states?

Also in our categorical analysis of stabilizer codes, we have not given a graphical/categorical account of code distance, which of great practical importance in quantum error correction.

For the interested reader, the author has also coauthored work which was not included in this thesis, all in some broad sense studying the connection between linear logic and quantum computing [CDH20, CCS21, CH23].

Bibliography

I have included URLs to publicly accessible versions of all cited works wherever possible. Therefore, as opposed to the DOIs, the URLs may not be the exact versions cited.

[Abr97] Lowell Abrams (1997): *Frobenius algebra structures in topological quantum field theory and quantum cohomology.* Ph.D. thesis, Johns Hopkins University. Available at `https://home.gwu.edu/~labrams/docs/thesis.pdf`.

[AC04] Samson Abramsky & Bob Coecke (2004): *A categorical semantics of quantum protocols.* In: *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, 2004.*, IEEE, pp. 415–425, doi:10.1109/LICS.2004.1319636. Available at `https://arxiv.org/pdf/quant-ph/0402130.pdf`.

[AG04] Scott Aaronson & Daniel Gottesman (2004): *Improved simulation of stabilizer circuits.* *Physical Review A* 70(5), p. 052328, doi:10.1103/PhysRevA.70.052328. Available at `https://arxiv.org/pdf/quant-ph/0406196.pdf`.

[Bac14] Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics.* *New Journal of Physics* 16(9), p. 093021, doi:10.1088/1367-2630/16/9/093021.

[Bac15] Miriam Backens (2015): *Making the stabilizer ZX-calculus complete for scalars.* *Electronic Proceedings in Theoretical Computer Science* 195, pp. 17–32, doi:10.4204/eptcs.195.2.

[Bar92] Michael Barr (1992): *Algebraically compact functors.* *Journal of Pure and Applied Algebra* 82(3), pp. 211–231, doi:10.1016/0022-4049(92)90169-g. Available at `https://www.math.mcgill.ca/barr/papers/algcmp.pdf`.

[BBC⁺93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres & William K. Wootters (1993): *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.* *Physical review letters* 70(13), p.

1895, doi:10.1103/PhysRevLett.70.1895. Available at `http://www.sabrizain.org/piccard/research/teleport.pdf`.

[BC22] Robert I. Booth & Titouan Carette (2022): *Complete ZX-Calculi for the Stabiliser Fragment in Odd Prime Dimensions.* doi:10.4230/LIPICS.MFCS.2022.24.

[BCC24a] Robert I. Booth, Titouan Carette & Cole Comfort (2024): *Complete equational theories for classical and quantum Gaussian relations.*

[BCC24b] Robert I. Booth, Titouan Carette & Cole Comfort (2024): *Graphical Symplectic Algebra.*

[BCR18] John C. Baez, Brandon Coya & Franciscus Rebro (2018): *Props in network theory.* *Theory and Applications of Categories* 33(25), pp. 727–783. Available at `http://www.tac.mta.ca/tac/volumes/33/25/33-25.pdf`.

[BD16] Miriam Backens & Ali Nabi Duman (2016): *A complete graphical calculus for Spekkens' toy bit theory.* *Foundations of Physics* 46(1), pp. 70–103, doi:10.1007/s10701-015-9957-7. Available at `https://arxiv.org/pdf/1411.1618.pdf`.

[BE15] John C. Baez & Jason Erbele (2015): *Categories in control.* *Theory and Applications of Categories* 30(24), pp. 836–881. Available at `http://www.tac.mta.ca/tac/volumes/30/24/30-24.pdf`.

[Bea13] Niel de Beaudrap (2013): *A Linearized Stabilizer Formalism for Systems of Finite Dimension.* *Quantum Info. Comput.* 13(1–2), p. 73–115, doi:10.26421/QIC13.1-2-6. Available at `https://arxiv.org/pdf/1102.3354.pdf`.

[BF18] John C. Baez & Brendan Fong (2018): *A compositional framework for passive linear networks.* *Theory and Applications of Categories* 33(38), pp. pp 1158–1222. Available at `http://www.tac.mta.ca/tac/volumes/33/38/33-38.pdf`.

[BG03] Roberto Bruni & Fabio Gadducci (2003): *Some algebraic laws for spans (and their connections with multirelations).* *Electronic Notes in Theoretical Computer Science* 44(3), pp. 175–193, doi:https://doi.org/10.1016/S1571-0661(04)80937-X. RelMiS 2001, Relational Methods in Software (a Satellite Event of ETAPS 2001).

[BGS21] Filippo Bonchi, Alessandro Di Giorgio & Pawel Sobocinski (2021): *Diagrammatic Polyhedral Algebra.* In Mikolaj Bojanczyk & Chandra Chekuri, editors: *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2021, December 15-17, 2021, Virtual Conference*, *LIPIcs* 213, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 40:1–40:18, doi:10.4230/LIPIcs.FSTTCS.2021.40.

[BK19] Miriam Backens & Aleks Kissinger (2019): *ZH: A Complete Graphical Calculus for Quantum Computations Involving Classical Non-linearity*. *Electronic Proceedings in Theoretical Computer Science* 287, pp. 23–42, doi:10.4204/eptcs.287.2.

[BKM21] Niel de Beaudrap, Aleks Kissinger & Konstantinos Meichanetzidis (2021): *Tensor Network Rewriting Strategies for Satisfiability and Counting*. *Electronic Proceedings in Theoretical Computer Science* 340, pp. 46–59, doi:10.4204/eptcs.340.3.

[BP22] Guillaume Boisseau & Robin Piedeleu (2022): *Graphical Piecewise-Linear Algebra*. In: *Lecture Notes in Computer Science*, 13242, Springer International Publishing, pp. 101–119, doi:10.1007/978-3-030-99253-8_6. Available at `https://arxiv.org/pdf/2111.03956.pdf`.

[BPSZ19] Filippo Bonchi, Robin Piedeleu, Paweł Sobociński & Fabio Zanasi (2019): *Graphical affine algebra*. In: *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE, pp. 1–12, doi:10.1109/LICS.2019.8785877. Available at `http://www.zanasi.com/fabio/files/paperLICS19.pdf`.

[BR22] Agustín Borgna & Rafael Romero (2022): *Encoding High-level Quantum Programs as SZX-diagrams*. Available at `https://arxiv.org/pdf/2206.09376.pdf`.

[BS22] Guillaume Boisseau & Paweł Sobociński (2022): *String Diagrammatic Electrical Circuit Theory*. *Electronic Proceedings in Theoretical Computer Science* 372, pp. 178–191, doi:10.4204/eptcs.372.13.

[BSZ17] Filippo Bonchi, Paweł Sobociński & Fabio Zanasi (2017): *Interacting Hopf algebras*. *Journal of Pure and Applied Algebra* 221(1), pp. 144–184, doi:10.1016/j.jpaa.2016.06.002. Available at `https://arxiv.org/pdf/1403.7048.pdf`.

[Bur] Albert Burroni: *Higher dimensional word problem*. In: *Category Theory and Computer Science*, Springer-Verlag, pp. 94–105, doi:10.1007/bfb0013459.

[CAB12] Earl T. Campbell, Hussain Anwar & Dan E. Browne (2012): *Magic-State Distillation in All Prime Dimensions Using Quantum Reed-Muller Codes*. *Physical Review X* 2(4), doi:10.1103/physrevx.2.041021. Available at `https://arxiv.org/pdf/1205.3104.pdf`.

[Car21] Titouan Carette (2021): *Wielding the ZX-calculus, Flexsymmetry, Mixed States, and Scalable Notations*. Theses, Université de Lorraine. Available at `https://hal.science/tel-03468027`.

[CB17] Lorenzo Catani & Dan Browne (2017): *Spekkens' toy model in all dimensions and its relationship with stabiliser quantum mechanics. New Journal of Physics* 19(7), p. 073035, doi:10.1088/1367-2630/aa781c. Available at `https://arxiv.org/pdf/1701.07801.pdf`.

[CC19] J.R.B. Cockett & Cole Comfort (2019): *The Category TOF. Electronic Proceedings in Theoretical Computer Science* 287, pp. 67–84, doi:10.4204/eptcs.287.4.

[CCS18] J.R.B. Cockett, Cole Comfort & Priyaa Srinivasan (2018): *The Category CNOT. Electronic Proceedings in Theoretical Computer Science* 266, pp. 258–293, doi:10.4204/eptcs.266.18.

[CCS21] J.R.B. Cockett, Cole Comfort & Priyaa Srinivasan (2021): *Dagger linear logic for categorical quantum mechanics. Logical Methods in Computer Science* Volume 17, Issue 4, doi:10.46298/lmcs-17(4:8)2021.

[CD11] Bob Coecke & Ross Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics. New Journal of Physics* 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016.

[CDH20] Cole Comfort, Antonin Delpeuch & Jules Hedges (2020): *Sheet diagrams for bimonoidal categories.* Available at `https://arxiv.org/pdf/2010.13361.pdf`.

[CDP21] Titouan Carette, Yohann D'Anello & Simon Perdrix (2021): *Quantum Algorithms and Oracles with the Scalable ZX-calculus. Electronic Proceedings in Theoretical Computer Science* 343, pp. 193–209, doi:10.4204/eptcs.343.10.

[CES11] Bob Coecke, Bill Edwards & Robert W. Spekkens (2011): *Phase groups and the origin of non-locality for qubits. Electronic Notes in Theoretical Computer Science* 270(2), pp. 15–36, doi:10.1016/j.entcs.2011.01.021. Available at `https://arxiv.org/pdf/1003.5005.pdf`.

[CG97] Richard Cleve & Daniel Gottesman (1997): *Efficient computations of encodings for quantum error correction. Physical Review A* 56(1), p. 76–82, doi:10.1103/physreva.56.76. Available at `https://arxiv.org/pdf/quant-ph/9607030.pdf`.

[CH16] Bob Coecke & Chris Heunen (2016): *Pictures of complete positivity in arbitrary dimension. Information and Computation* 250, pp. 50–58, doi:10.1016/j.ic.2016.02.007. Available at `https://arxiv.org/pdf/1110.3055.pdf`.

[CH23] Cole Comfort & James Hefford (2023): *Coend Optics for Quantum Combs. Electronic Proceedings in Theoretical Computer Science* 380, p. 63–76, doi:10.4204/eptcs.380.4.

[Che11] Eugenia Cheng (2011): *Iterated distributive laws. Mathematical Proceedings of the Cambridge Philosophical Society* 150(3), pp. 459–487, doi:10.1017/s0305004110000599. Available at `https://arxiv.org/pdf/0710.1120.pdf`.

[Che20] Eugenia Cheng (2020): *Distributive laws for Lawvere theories. Compositionality* 2, doi:10.32408/compositionality-2-1.

[CHP19] Titouan Carette, Dominic Horsman & Simon Perdrix (2019): *SZX-Calculus: Scalable Graphical Quantum Reasoning.* doi:10.4230/LIPICS.MFCS.2019.55.

[CJPV21] Titouan Carette, Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2021): *Completeness of Graphical Languages for Mixed State Quantum Mechanics. ACM Transactions on Quantum Computing* 2(4), doi:10.1145/3464693. Available at `https://arxiv.org/pdf/1902.07143.pdf`.

[CK17] Bob Coecke & Aleks Kissinger (2017): *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning.* Cambridge University Press, doi:10.1017/9781316219317. Available at `https://www.cs.ox.ac.uk/people/aleks.kissinger/PQP.pdf`.

[CK22] Cole Comfort & Aleks Kissinger (2022): *A Graphical Calculus for Lagrangian Relations.* 372, Open Publishing Association, pp. 338–351, doi:10.4204/eptcs.372.24.

[CKP22] J.R.B. Cockett, Amolak Ratan Kalra & Shiroman Prakash (2022): *Categories of Kirchhoff relations.* Available at `https://arxiv.org/pdf/2205.05870.pdf`.

[CKS23] J.R.B. Cockett, Amolak Ratan Kalra & Priyaa Varshinee Srinivasan (2023): *Normalizing Resistor Networks.* Available at `https://arxiv.org/pdf/2303.11839.pdf`.

[CKWW08] A. Carboni, G.M. Kelly, R.F.C. Walters & R.J. Wood (2008): *Cartesian bicategories II. Theory and Applications of Categories* 19(6), pp. 93–124. Available at `http://www.tac.mta.ca/tac/volumes/19/6/19-06.pdf`.

[CL02] J.R.B. Cockett & Steve Lack (2002): *Restriction categories I: categories of partial maps. Theoretical Computer Science* 270(1), pp. 223–259, doi:https://doi.org/10.1016/S0304-3975(00)00382-0.

[CL07] J.R.B. Cockett & Steve Lack (2007): *Restriction categories III: colimits, partial limits and extensivity. Mathematical Structures in Computer Science* 17(4), pp. 775–817, doi:10.1017/s0960129507006056. Available at `https://arxiv.org/pdf/math/0610500.pdf`.

[Com19] Cole Comfort (2019): *Classifying Reversible Logic Gates with Ancillary Bits.* Master's thesis, University of Calgary. Available at `http://pages.cpsc.ucalgary.ca/~robin/Theses/ucalgary_2019_comfort_cole.pdf`.

[Com21] Cole Comfort (2021): *The ZX&-calculus: A complete graphical calculus for classical circuits using spiders.* In Benoît Valiron, Shane Mansfield, Pablo Arrighi & Prakash Panangaden, editors: Proceedings 17th International Conference on *Quantum Physics and Logic,* Paris, France, June 2 - 6, 2020, *Electronic Proceedings in Theoretical Computer Science* 340, Open Publishing Association, pp. 60–90, doi:10.4204/EPTCS.340.4.

[CPV13] Bob Coecke, Dusko Pavlovic & Jamie Vicary (2013): *A new description of orthogonal bases. Mathematical structures in computer science* 23(3), pp. 555–567, doi:doi.org/10.1017/S0960129512000047. Available at `https://arxiv.org/pdf/0810.0812.pdf`.

[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor & N. J. A. Sloane (1997): *Quantum Error Correction and Orthogonal Geometry. Phys. Rev. Lett.* 78, pp. 405–408, doi:10.1103/PhysRevLett.78.405. Available at `https://arxiv.org/pdf/quant-ph/9605005.pdf`.

[CRSS98] A.R. Calderbank, E.M. Rains, P.M. Shor & N.J.A. Sloane (1998): *Quantum error correction via codes over GF(4). IEEE Transactions on Information Theory* 44(4), pp. 1369–1387, doi:10.1109/18.681315. Available at `https://arxiv.org/pdf/quant-ph/9608006.pdf`.

[CS97] J.R.B. Cockett & R.A.G. Seely (1997): *Weakly distributive categories. Journal of Pure and Applied Algebra* 114(2), pp. 133–173, doi:10.1016/0022-4049(95)00160-3. Available at `https://www.math.mcgill.ca/rags/linear/wdc-fix.pdf`.

[CW87] A. Carboni & R.F.C. Walters (1987): *Cartesian bicategories I. Journal of Pure and Applied Algebra* 49(1-2), pp. 11–32, doi:10.1016/0022-4049(87)90121-6.

[DKPW20] Ross Duncan, Aleks Kissinger, Simon Perdrix & John van de Wetering (2020): *Graph-theoretic Simplification of Quantum Circuits with the ZX-calculus. Quantum* 4, p. 279, doi:10.22331/q-2020-06-04-279. Available at `https://arxiv.org/pdf/1902.03178.pdf`.

[DN06] C.M. Dawson & M.A. Nielsen (2006): *The Solovay-Kitaev algorithm. Quantum Information and Computation* 6(1), pp. 81–95, doi:10.26421/qic6.1-6. Available at `https://arxiv.org/pdf/quant-ph/0505030.pdf`.

[DP09] Ross Duncan & Simon Perdrix (2009): *Graph states and the necessity of Euler decomposition.* In: *Conference on Computability in Europe,* Springer, pp. 167–177, doi:10.1007/978-3-642-03073-4_18. Available at `https://arxiv.org/pdf/0902.0500.pdf`.

[FST19] Brendan Fong, David Spivak & Rémy Tuyéras (2019): *Backprop as functor: A compositional perspective on supervised learning.* In: *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE, pp. 1–13, doi:doi:10.5555/3470152.3470163. Available at `https://arxiv.org/pdf/1711.10455.pdf`.

[FZ17] Brendan Fong & Fabio Zanasi (2017): *A Universal Construction for (Co)Relations.* doi:10.4230/LIPICS.CALCO.2017.12.

[GG17] Stefano Gogioso & Fabrizio Genovese (2017): *Infinite-dimensional Categorical Quantum Mechanics. Electronic Proceedings in Theoretical Computer Science* 236, pp. 51–69, doi:10.4204/eptcs.236.4.

[Gil14] Brett Giles (2014): *An investigation of some theoretical aspects of reversible computing.* Ph.D. thesis, University of Calgary, doi:10.11575/PRISM/24917.

[Gog19] Stefano Gogioso (2019): *Higher-order CPM Constructions. Electronic Proceedings in Theoretical Computer Science* 287, pp. 145–162, doi:10.4204/eptcs.287.8.

[Got97] Daniel Gottesman (1997): *Stabilizer Codes and Quantum Error Correction.* Ph.D. thesis, California Institute of Technology. Available at `https://arxiv.org/pdf/quant-ph/9705052.pdf`.

[Got98] Daniel Gottesman (1998): *The Heisenberg Representation of Quantum Computers.* In S. P. Corney, R. Delbourgo & P. D. Jarvis, editors: *Group 22 international colloquium on group theoretical methods in physics*, International Press of Boston, pp. 32–43. Available at `https://arxiv.org/pdf/quant-ph/9807006.pdf`.

[Got99] Daniel Gottesman (1999): *Fault-Tolerant Quantum Computation with Higher-Dimensional Systems.* In: *Quantum Computing and Quantum Communications*, Springer Berlin Heidelberg, pp. 302–313, doi:10.1007/3-540-49208-9_27. Available at `https://arxiv.org/pdf/quant-ph/9802007.pdf`.

[GPZ23] Tao Gu, Robin Piedeleu & Fabio Zanasi (2023): *A Complete Diagrammatic Calculus for Boolean Satisfiability. Electronic Notes in Theoretical Informatics and Computer Science* Volume 1 - Proceedings of..., doi:10.46298/entics.10481. Available at `https://arxiv.org/pdf/2211.12629.pdf`.

[Gra00] Marco Grandis (2000): *Weak subobjects and the epi-monic completion of a category. Journal of Pure and Applied Algebra* 154(1-3), pp. 193–212, doi:10.1016/s0022-4049(99)00191-7. Available at `https://core.ac.uk/download/pdf/82078126.pdf`.

[Gro06] David Gross (2006): *Hudson's theorem for finite-dimensional quantum systems. Journal of mathematical physics* 47(12), p. 122107, doi:10.1063/1.2393152. Available at `https://arxiv.org/pdf/quant-ph/0602001.pdf`.

[GS79] Victor Guillemin & Shlomo Sternberg (1979): *Some Problems in Integral Geometry and Some Related Problems in Micro-Local Analysis. American Journal of Mathematics* 101(4), p. 915, doi:10.2307/2373923.

[HDE$^+$06] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest & H.-J. Briegel (2006): *Entanglement in graph states and its applications. Proceedings of the International School of Physics* 162(Quantum Computers, Algorithms and Chaos), p. 115–218, doi:10.3254/978-1-61499-018-5-115. Available at `https://arxiv.org/pdf/quant-ph/0602096.pdf`.

[Hei21] Markus Heinrich (2021): *On stabiliser techniques and their application to simulation and certification of quantum devices.* Ph.D. thesis, Universität zu Köln. Available at `https://kups.ub.uni-koeln.de/50465/1/dissertation_heinrich.pdf`.

[Heu13] Chris Heunen (2013): *On the Functor ℓ2.* In: *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky*, Springer Berlin Heidelberg, pp. 107–121, doi:10.1007/978-3-642-38164-5_8. Available at `https://arxiv.org/pdf/1012.4526.pdf`.

[HK21] Chris Heunen & Robin Kaarsgaard (2021): *Bennett and Stinespring, Together at Last. Electronic Proceedings in Theoretical Computer Science* 343, pp. 102–118, doi:10.4204/eptcs.343.5.

[HS19] Mathieu Huot & Sam Staton (2019): *Quantum channels as a categorical completion.* In: *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE, doi:10.1109/lics.2019.8785700. Available at `https://arxiv.org/pdf/1904.09600.pdf`.

[HV19] Chris Heunen & Jamie Vicary (2019): *Categories for Quantum Theory: An Introduction.* Oxford University Press, doi:10.1093/oso/9780198739623.001.0001. Available at `https://www.cs.ox.ac.uk/people/jamie.vicary/IntroductionToCategoricalQuantumMechanics.pdf`.

[IKY02] K. Iwama, Y. Kambayashi & S. Yamashita (2002): *Transformation rules for designing CNOT-based quantum circuits.* In: *Proceedings 2002 Design Automation Conference (IEEE Cat. No.02CH37324)*, pp. 419–424, doi:10.1109/DAC.2002.1012662.

[JPV18] Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2018): *A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics.* In: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, ACM, doi:10.1145/3209108.3209131. Available at `https://arxiv.org/pdf/1705.11151.pdf`.

[JPV20] Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2020): *Completeness of the ZX-Calculus. Logical Methods in Computer Science* Volume 16, Issue 2, doi:10.23638/LMCS-16(2:11)2020.

[Kir45] Student of Kirchhoff (1845): *Ueber den Durchgang eines elektrischen Stromes durch eine Ebene, insbesondere durch eine kreisförmige. Annalen der Physik* 140(4), p. 497–514, doi:10.1002/andp.18451400402.

[Kis22] Aleks Kissinger (2022): *Phase-free ZX diagrams are CSS codes (...or how to graphically grok the surface code).* Available at `https://arxiv.org/pdf/2204.14038.pdf`.

[Kit97] A. Yu. Kitaev (1997): *Quantum computations: algorithms and error correction. Russian Mathematical Surveys* 52(6), pp. 1191–1249, doi:10.1070/rm1997v052n06abeh002155.

[KW20a] Aleks Kissinger & John van de Wetering (2020): *PyZX: Large Scale Automated Diagrammatic Reasoning.* In Bob Coecke & Matthew Leifer, editors: Proceedings 16th International Conference on *Quantum Physics and Logic,* Chapman University, Orange, CA, USA., 10-14 June 2019, *Electronic Proceedings in Theoretical Computer Science* 318, Open Publishing Association, pp. 229–241, doi:10.4204/EPTCS.318.14. Available at `https://github.com/Quantomatic/pyzx`.

[KW20b] Aleks Kissinger & John van de Wetering (2020): *Reducing the number of non-Clifford gates in quantum circuits. Physical Review A* 102(2), doi:10.1103/physreva.102.022406. Available at `https://arxiv.org/pdf/1903.10477.pdf`.

[KZ15] Aleks Kissinger & Vladimir Zamdzhiev (2015): *Quantomatic: A Proof Assistant for Diagrammatic Reasoning*, p. 326–336. Springer International Publishing, doi:10.1007/978-3-319-21401-6_22. Available at `https://quantomatic.github.io/`.

[Lac04] Steve Lack (2004): *Composing props. Theory and Applications of Categories* 13(9), pp. 147–163. Available at `http://www.tac.mta.ca/tac/volumes/13/9/13-09.pdf`.

[Laf95] Yves Lafont (1995): *Equational reasoning with 2-dimensional diagrams.* In: *Term Rewriting*, Springer Berlin Heidelberg, pp. 170–195, doi:10.1007/3-540-59340-3_13.

[Laf03] Yves Lafont (2003): *Towards an algebraic theory of Boolean circuits.* *Journal of Pure and Applied Algebra* 184(2), pp. 257–310, doi:https://doi.org/10.1016/S0022-4049(03)00069-0.

[Lan78] Saunders Mac Lane (1978): *Categories for the Working Mathematician.* Springer New York, doi:10.1007/978-1-4757-4721-8. Available at `http://www.mtm.ufsc.br/~ebatista/2016-2/maclanecat.pdf`.

[LMW22] Tuomas Laakkonen, Konstantinos Meichanetzidis & John van de Wetering (2022): *A Graphical #SAT Algorithm for Formulae with Small Clause Density.* Available at `https://arxiv.org/pdf/2212.08048.pdf`.

[LMW23] Tuomas Laakkonen, Konstantinos Meichanetzidis & John van de Wetering (2023): *Picturing Counting Reductions with the ZH-Calculus.* *Electronic Proceedings in Theoretical Computer Science* 384, pp. 89–113, doi:10.4204/eptcs.384.6.

[NC10] Michael A. Nielsen & Isaac L. Chuang (2010): *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, doi:10.1017/CBO9780511976667.

[NW17] Kang Feng Ng & Quanlong Wang (2017): *A universal completion of the ZX-calculus.* Available at `https://arxiv.org/pdf/1706.09877.pdf`.

[Ohm27] Georg Simon Ohm (1827): *Die galvanische Kette.* Bei T.H. Riemann, doi:10.5479/sil.354716.39088005838644.

[PBC+23] Boldizsár Poór, Robert I. Booth, Titouan Carette, John van de Wetering & Lia Yeh (2023): *The Qupit Stabiliser ZX-travaganza: Simplified Axioms, Normal Forms and Graph-Theoretic Simplification.* Available at `https://arxiv.org/pdf/2306.05204.pdf`.

[Pen71] Roger Penrose (1971): *Applications of negative dimensional tensors.* *Combinatorial mathematics and its applications* 1, pp. 221–244. Available at `https://ncatlab.org/nlab/files/PenroseNegativeDimensionalTensors.pdf`.

[Ran14] André Ranchin (2014): *Depicting qudit quantum mechanics and mutually unbiased qudit theories.* In Bob Coecke, Ichiro Hasuo & Prakash Panangaden, editors: Proceedings 14th International Conference on *Quantum Physics and Logic,* Kyoto University, Japan, 4-6 June 2017, *Electronic Proceedings in Theoretical Computer Science* 172, Open Publishing Association, pp. 68–91, doi:10.4204/eptcs.172.6.

[Ran16] André Ranchin (2016): *Alternative theories in quantum foundations.* Ph.D. thesis, Imperial College London, doi:10.25560/52462. Available at `https://spiral.imperial.ac.uk/bitstream/10044/1/52462/3/Ranchin-A-2017-PhD-Thesis.pdf`.

[Roy22] Patrick Roy (2022): *Qudit ZH-calculus*. Master's thesis, University of Oxford. Available at `https://www.cs.ox.ac.uk/people/aleks.kissinger/theses/roy-thesis.pdf`.

[RW02] Robert Rosebrugh & R.J. Wood (2002): *Distributive laws and factorization*. *Journal of Pure and Applied Algebra* 175(1-3), pp. 327–353, doi:10.1016/s0022-4049(02)00140-8. Available at `https://www.mta.ca/~rrosebru/articles/fac.pdf`.

[Sel07] Peter Selinger (2007): *Dagger compact closed categories and completely positive maps*. *Electronic Notes in Theoretical computer science* 170, pp. 139–163, doi:10.1016/j.entcs.2006.12.018. Available at `https://mathstat.dal.ca/~selinger/papers/dagger.pdf`.

[Sel08] Peter Selinger (2008): *Idempotents in Dagger Categories*. *Electronic Notes in Theoretical Computer Science* 210, pp. 107–122, doi:10.1016/j.entcs.2008.04.021. Available at `https://www.mathstat.dal.ca/~selinger/papers/idem-2up.pdf`.

[Sob17] Paweł Sobociński (2017): *Graphical Linear Algebra: Orthogonality and projections*. Available at `https://graphicallinearalgebra.net/2017/08/09/orthogonality-and-projections/`.

[Spe07] Robert W. Spekkens (2007): *Evidence for the epistemic view of quantum states: A toy theory*. *Physical Review A* 75(3), p. 032110, doi:10.1103/PhysRevA.75.032110. Available at `https://arxiv.org/pdf/quant-ph/0401052.pdf`.

[Spe16] Robert W. Spekkens (2016): *Quasi-quantization: classical statistical theories with an epistemic restriction*. In: *Quantum Theory: Informational Foundations and Foils*, Springer, pp. 83–135, doi:10.1007/978-94-017-7303-4. Available at `https://arxiv.org/pdf/1409.5041.pdf`.

[SPMH03] V.V. Shende, A.K. Prasad, I.L. Markov & J.P. Hayes (2003): *Synthesis of reversible logic circuits*. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 22(6), pp. 710–722, doi:10.1109/TCAD.2003.811448. Available at `https://arxiv.org/pdf/quant-ph/0207001.pdf`.

[SS22] Dario Stein & Richard Samuelson (2022): *A Category for unifying Gaussian Probability and Nondeterminism*. Available at `https://arxiv.org/pdf/2204.14024.pdf`.

[Sti55] W. Forrest Stinespring (1955): *Positive Functions on $C*$-Algebras*. *Proceedings of the American Mathematical Society* 6(2), p. 211, doi:10.2307/2032342.

[Str72] Ross Street (1972): *The formal theory of monads.* *Journal of Pure and Applied Algebra* 2(2), pp. 149–168, doi:10.1016/0022-4049(72)90019-9.

[Tof80] Tommaso Toffoli (1980): *Reversible computing.* In: *Automata, Languages and Programming*, Springer Berlin Heidelberg, pp. 632–644, doi:10.1007/3-540-10003-2_104.

[Vara] Various authors: *dizx.* Available at `https://github.com/jvdwetering/dizx`.

[Varb] Various authors: *zxlive.* Available at `https://github.com/Quantomatic/zxlive`.

[Wan18] Quanlong Wang (2018): *Qutrit ZX-calculus is Complete for Stabilizer Quantum Mechanics.* In Bob Coecke & Aleks Kissinger, editors: Proceedings 14th International Conference on *Quantum Physics and Logic,* Nijmegen, The Netherlands, 3-7 July 2017, *Electronic Proceedings in Theoretical Computer Science* 266, Open Publishing Association, pp. 58–70, doi:10.4204/EPTCS.266.3.

[Wei82] Alan Weinstein (1982): *The symplectic "category".* In: *Lecture Notes in Mathematics*, Springer Berlin Heidelberg, pp. 45–51, doi:10.1007/bfb0092426.

[Wei17] Alan Weinstein (2017): *Categories of (co)isotropic linear relations.* *Journal of Symplectic Geometry* 15(2), pp. 603–620, doi:10.4310/jsg.2017.v15.n2.a5. Available at `https://arxiv.org/pdf/1503.06240.pdf`.

[WGZ22] Paul Wilson, Dan Ghica & Fabio Zanasi (2022): *String diagrams for non-strict monoidal categories.* Available at `https://arxiv.org/pdf/2201.11738.pdf`.

[Wig32] E. Wigner (1932): *On the Quantum Correction For Thermodynamic Equilibrium.* *Physical Review* 40(5), pp. 749–759, doi:10.1103/physrev.40.749.

[WW19] John van de Wetering & Sal Wolffs (2019): *Completeness of the Phase-free ZH-calculus.* Available at `https://arxiv.org/abs/1904.07545`.

[Zan18] Fabio Zanasi (2018): *Interacting Hopf Algebras: the theory of linear systems.* Ph.D. thesis, Université de Lyon. Available at `https://discovery.ucl.ac.uk/id/eprint/10062538/1/thesis2015%20%281%29.pdf`.