Relational semantics for quantum protocols

Cole Comfort

New College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy in Computer Science

????? 2023

Contents

Chapter 1

Introduction

Chapter 2

Background

2.1 Category theory

We assume that the reader has a basic understanding of monoidal bicategories. For reference, refer to ?????JAMIE AND CHRIS HEUNEN

Definition 2.1.1.

Definition 2.1.2.

Definition 2.1.3. *Given a category $\mathcal{V}$ with finite pullbacks $\mathcal{V}$, a category internal to $\mathcal{V}$ is a monad in* $\mathsf{Span}(\mathcal{V})$.

Internal categories are indeed categories. The collection of objects is given by the feet of the span, the set of morphisms by the apex, the domain and codomain by the left and right legs respectively. The components of the unit of the comonad give the identity morphisms and the multiplication of the monad gives the composition.

Lemma 2.1.4. *Monads internal to* Set *are in bijection with small categories.*

It is not the case that monad maps correspond to functors between internal categories. A canonical way to obtain such a notion requires the machinery of double categories, which is outside of the purview of this thesis. However, internal profunctors can be developed in the globular setting.

Definition 2.1.5.

Definition 2.1.6.

Definition 2.1.7.

Definition 2.1.8.

Definition 2.1.9.

Definition 2.1.10. *Given a category $\mathcal{V}$ with finite pullbacks, the 2-category of profunctors internal to $\mathcal{V}$, $\mathcal{V} - \mathsf{Prof}$ is $\mathsf{Mod}(\mathsf{Mnd}(\mathsf{Span}(\mathcal{V})))$.*

Bimodules allow us to consider distributive laws between two monads with shared structure, identified by the module actions. For example, a distributive law of monoidal categories should identify the action of permuting wires on both categories.

Definition 2.1.11.

Definition 2.1.12.

Definition 2.1.13.

Lemma 2.1.14.

Definition 2.1.15.

Definition 2.1.16.

Lemma 2.1.17.

Lemma 2.1.18.

2.2 Categorical quantum mechanics

Definition 2.2.1.

Definition 2.2.2.

Definition 2.2.3.

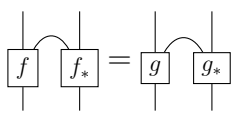
Definition 2.2.4.

Definition 2.2.5. *Given a †-compact closed category $\mathbb{X}$, there is a †-compact closed category $\mathsf{CPM}(\mathbb{X})$ has:*

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

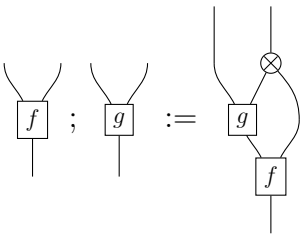
Maps: $$\frac{X \xrightarrow{f} Y \otimes S \in \mathbb{X}}{X \xrightarrow{(f,S)} Y \in \widetilde{\mathsf{CPM}}(\mathbb{X})}$$

Modulo the equivalence relation:

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

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

Or using proof net notation:

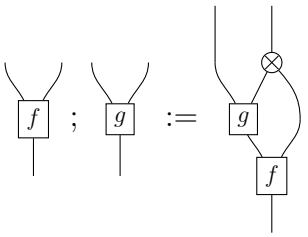


Identity: $\dfrac{1_X \in \widetilde{\mathsf{CPM}}(\mathbb{X})}{(u^R_A)^{-1} \in \mathbb{X}}$

Tensor product:

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

Or in proof net notation:



Dagger compact closed structure: *Inherited pointwise from* $\mathbb{X}$.

Chapter 3

The classical fragment of the ZH-calculus

3.1 Introduction

In this chapter a complete set of identities is provided for the fragment, $\mathsf{ZX}\mathscr{E}$, of the ZX-calculus, generated by black and white spiders, the not gate and the and gate. We show that this is a universal and complete presentation of "qubit multirelations," or equivalently $2^n \times 2^m$ dimensional matrices over $\mathbb{N}$. To prove completeness and universality requires much exposition. Along the way we show that the category of classical channels of a discrete inverse category is the Cartesian completion of that discrete inverse category. We then show that the corresponding environment structure is precisely the free counit completion of the chosen Frobenius structure. This allows us to present the Cartesian completion of, TOF, the category generated by the Toffoli gate, $|1\rangle$ and $\langle 1|$ by only adding the $|+\rangle$ state and the unitality equation. By freely adding both the unit and counit to TOF, corresponding to $\sqrt{2}|+\rangle$ and $\sqrt{2}\langle +|$, this yields an isomorphism with spans between ordinals 2^n, $n \in \mathbb{N}$, or equivalently, "qubit multirelations."

The identities which are given by this two way translation are *almost* the union of the complete identities for Boolean functions [48, Thm. 10] (functions of type $\mathbb{F}_2^n \to \mathbb{F}_2$) and the identities for $\mathsf{Span}^{\sim}(\mathsf{Mat}(\mathbb{F}_2))$ [13, Def. 5.1]. These classes of circuits, and these identities for that matter, are nothing new; however, we provide a completeness result, as well as a structural account of how the full classical qubit fragment of FHilb can be obtained from adding discarding and codiscarding to the full classically reversible Boolean fragment. In fact, some of these identities are presented in [44, Chap. 5], and they are used in the ZH-calculus [5, 61], as well as in some presentations of the ZX-calculus with the triangle generator as a primitive [49, 63]. This is particularity unsurprising for the latter, [63], where the author proves completeness of the ZX-calculus over arbitrary semirings, which subsumes the completeness result herein. Albeit, the presentation given here is substantially simpler. It worth mentioning that $\mathsf{ZX}\mathscr{E}$ is not a $\mathsf{ZX}*$-calculus in the sense of [17], because the and gate is not a spider. $\mathsf{ZX}\mathscr{E}$ should be instead though of as the "classical fragment" of the phase-free ZH-calculus: retaining the monoid for "and" without H-boxes. From this presentation only natural-number H-boxes can be derived.

We assume familiarity with the theory of monoidal categories and categorical quantum mechanics. Most of the paper will be devoted to reviewing the required categorical machinery of restriction and inverse categories, and developing it further, in order to prove the main result. With all of mathematics reviewed and developed in generality, the desired result follows from abstract nonsense after a mechanical calculation.

In Section 3.2, the theory of restriction categories and inverse categories is reviewed. In Section 3.3, we construct classical channels in the setting of discrete inverse categories, showing that the "environment structures" of the classical channels corresponds to adding counits to the base discrete inverse category. Finally, in Section 3.4, we actually compute the (co)unit completion of TOF. We show that this category has a much more canonical presentation, $\mathsf{ZX}\mathscr{E}$, in terms of interacting monoids/comonoids which very much resembles the ZH-calculus. We also show that this category is iso-

morphic to the category spans between ordinals 2^n.

3.2 Restriction and Inverse Categories

Restriction and inverse categories provide a categorical semantics for partial computing and reversible computing, respectively. We review how weakened products can be constructed in both settings; relating one to the other.

Definition 3.2.1. *[22, §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:[1]

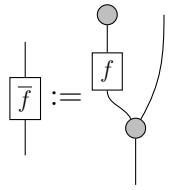
[R.1] $\overline{f}f = f$ **[R.2]** $\overline{f}\,\overline{g} = \overline{g}\,\overline{f}$ **[R.3]** $\overline{f}\,\overline{g} = \overline{\overline{f}\,g}$ **[R.4]** $f\overline{g} = \overline{fg}f$

Maps of the form $\overline{f}$ are called restriction idempotents. The canonical example of a restriction category is Par*, sets and partial maps. The restriction in this case, just restricts partial functions to their domain of definition.*

Restriction categories have a partial order on homsets given by $f \leq g \iff \overline{f}g = f$.

A map f in a restriction category is called a **partial isomorphism***, in case there exists a map g called the partial inverse of f so that $fg = \overline{f}$ and $gf = \overline{g}$. Similarly, a map f in a restriction category is* **total** *if $\overline{f} = 1$. Denote the subcategories of partial isomorphisms and total maps of a restriction category $\mathbb{X}$, respectively by* $\mathsf{ParIso}(\mathbb{X})$ *and* $\mathsf{Total}(\mathbb{X})$*.*

Example 3.2.2. *[53, p. 101] [20, §5] A* **counital copy category** *(or a p-category with a one element object) is a monoidal category with a family of commutative comonoids on every object compatible with the monoidal structure, with a natural comultiplication. This gives a restriction via copying and then discarding:*



Definition 3.2.3. *[22, §3.1] A* **stable system of monics** $\mathcal{M}$ *of $\mathbb{X}$ is a collection of monics in $\mathbb{X}$ containing all isomorphisms; where for any cospan $X \xrightarrow{f} Z \xleftarrow{m} Y$ in $\mathbb{X}$, where m' is in $\mathcal{M}$, the following pullback exists:*

$$\begin{array}{ccc} W & \xrightarrow{f'} & Y \\ {\scriptstyle m'}\downarrow & & \downarrow{\scriptstyle m} \\ X & \xrightarrow[f]{} & Z \end{array}$$

Where m' is in $\mathcal{M}$.

[1] Using diagrammatic composition.

Stable systems of monics allow one to represent the domains of definition of a partial functions as a subobjects:

Definition 3.2.4. *[22, §3.1] Given a stable system of monics $\mathcal{M}$ in a category $\mathbb{X}$, the* **partial map category** $\mathsf{Par}(\mathbb{X}, \mathcal{M})$ *is given by the same objects as in $\mathbb{X}$ where morphisms $X \to Y$, given by isomorphism classes of spans $X \xleftarrow{m} Z \xrightarrow{f} Y$ where f is a map in $\mathbb{X}$ and m is a map in $\mathcal{M}$. Composition is given by pullback and the identity is given by the trivial span.*

Partial map categories have a restriction structure given by: $(X \xleftarrow{m} Z \xrightarrow{f} Y) \mapsto (X \xleftarrow{m} Z \xrightarrow{m} X)$. Moreover, a partial isomorphism is a span $X \xleftarrow{e} Z \xrightarrow{m} Y$ where $e, m \in \mathcal{M}$; the partial inverse given by $Y \xleftarrow{m} Z \xrightarrow{e} X$.

Par is equivalently the partial map category $\mathsf{Par}(\mathsf{Set}, \mathcal{M})$ where $\mathcal{M}$ is all monics in Set.

Let $\mathsf{Span}^{\sim}(\mathbb{X})$ denote the category given by isomorphism classes of spans over $\mathbb{X}$. Given a stable system of monics $\mathcal{M}$ over $\mathbb{X}$, if $\mathbb{X}$ is finitely complete, then $\mathsf{Span}^{\sim}(\mathbb{X})$ exists, and thus, there is a faithful functor $\mathsf{Par}(\mathbb{X}, \mathcal{M}) \to \mathsf{Span}^{\sim}(\mathbb{X})$.

Definition 3.2.5. *[22, §2.3.2] An* **inverse category** *is a restriction category in which all maps are partial isomorphisms. The subcategory of partial isomorphisms of* Par *is called* Pinj.

Inverse categories can be presented with a dagger functor taking maps to their partial inverses:

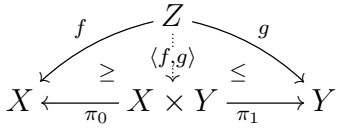
Theorem 3.2.6. *[22, Thm. 2.20] A restriction category $\mathbb{X}$ is an inverse category if and only if there is a dagger functor $(\_)^\circ : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$ such that for all $X \xleftarrow{f} Z \xrightarrow{g} Y$:*

$$f f^\circ f = f \quad f f^\circ g g^\circ = g g^\circ f f^\circ$$

Since restriction categories and inverse categories give a categorical semantics for partial computing and reversible computing, respectively, it is natural to ask when these categories have copying.

In the case of restriction categories, one must weaken the notion of the product to lax products using the partial order enrichment:

Definition 3.2.7. *[20] A restriction category has* **binary restriction products**, *when for all objects X, 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 $X \xleftarrow{f} Z \xrightarrow{g} Y$, the following diagram commutes there exists a unique $Z \xrightarrow{\langle f,g \rangle} X \times Y$ making the diagram commute:*



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** $\top$ *when for all objects* X*, there exists a unique total map* $!_X : X \to \top$ *such that* $f!_Y = \overline{f}!_X$*.*

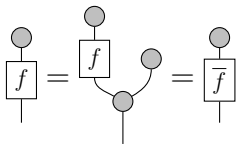
A restriction category with a restriction terminal object and binary restriction products is a **Cartesian restriction category***.*

An object A *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. Discrete Cartesian restriction categories are said to have restriction products.*

Theorem 3.2.8. *[20, Thm. 5.2] The structure of a counital copy category structure is precisely that of a Cartesian restriction category.*

In particular, the restriction operator is defined as follows, where the components of the restriction products are drawn in grey:

Remark 3.2.9.



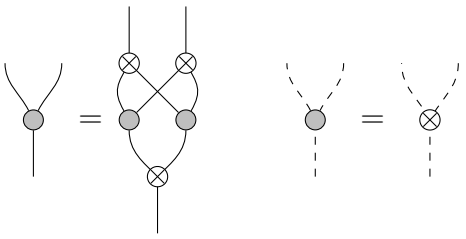
Proposition 3.2.10. *[20, §5.1]*

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

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.

The weakened notion of products in restriction categories is not satisfying for inverse categories because it does not impose enough equations governing the interaction between the diagonal map and its partial inverse.

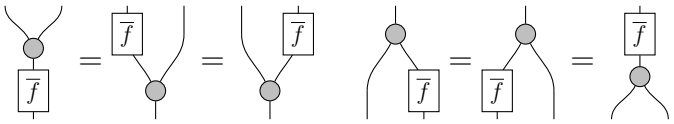
Definition 3.2.11. *[41, Def. 4.3.1] A symmetric monoidal inverse category* $\mathbb{X}$ *is a* **discrete inverse category** *when there is a natural, special commutative* †*-semi-Frobenius algebra*[2] *on every object (where the components of the semi-Frobenius algebra are drawn in grey) compatible with the tensor product:*



[2]The "semi" adjective on Frobenius just means that the a semigroup and cosemigroup are interacting instead of a monoid and comonoid.

Where the tensor product is also required to preserve restriction in both components.

In a discrete inverse category, restriction idempotents are prephases for the Frobenius algebra, so that:



Discrete inverse categories are the "right" notion of weakened products for monoidal inverse categories:

Theorem 3.2.12. *[41, Thm. 5.2.6] There is an equivalence of categories between the category of discrete inverse categories and the category of discrete Cartesian categories.*

To go from discrete Cartesian restriction categories to discrete inverse categories, one takes the subcategory of partial isomorphisms. The other direction is less trivial; in particular, this involves adding a restriction terminal object via the following construction which "adds a history" to a partial isomorphism:

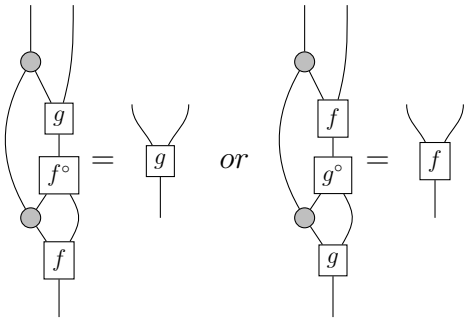
Definition 3.2.13. *[41, Def. 5.1.1] Given a discrete inverse category $\mathbb{X}$, define its* **Cartesian completion** *$\widetilde{\mathbb{X}}$ as the category with:*

Objects: *The same objects as $\mathbb{X}$.*

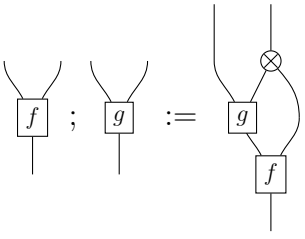
Maps:

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

Where two parallel maps $X \xrightarrow{(f,S),(g,T)} Y$ are equivalent when either (both conditions are equivalent):

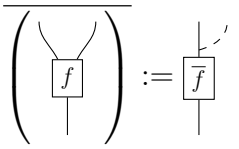


Composition:



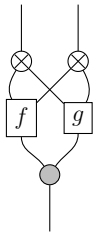
Identity:

Restriction:



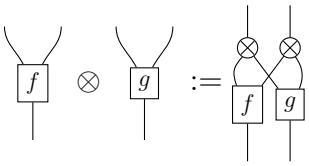
Restriction product:

$\langle f, g \rangle :=$



Restriction terminal map:

Tensor product:



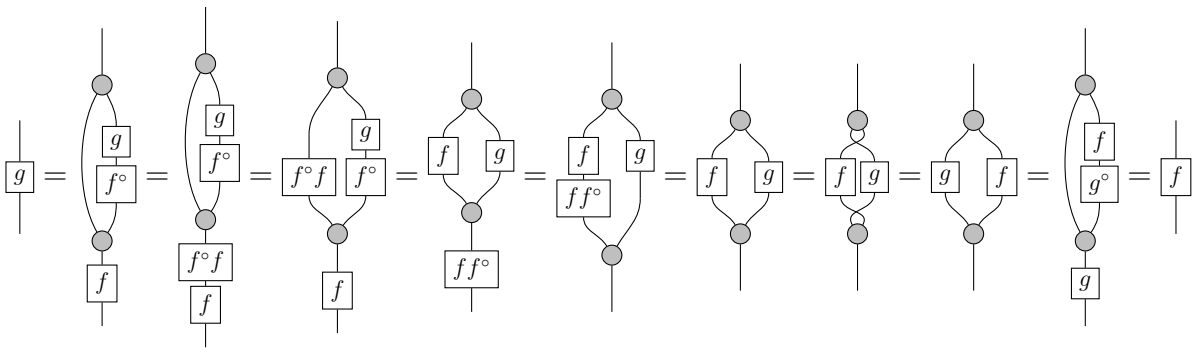
Tensor unit: *The same as in* $\mathbb{X}$.

Example 3.2.14. *[41, Ex. 5.3.3]* $\widetilde{\mathsf{Pinj}}$ *is* Par.

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

Lemma 3.2.15. *The canonical functor* $\iota : \mathbb{X} \to \widetilde{\mathbb{X}}$ *is faithful.*

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



□

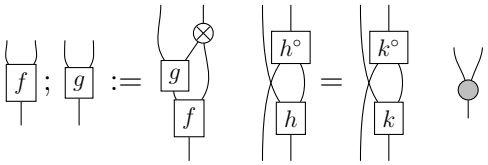
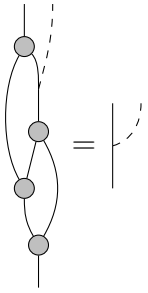


Figure 3.1: Composition of representatives $f; g$; equivalence relation $h \sim k$; decoherence map.

Lemma 3.2.16. *The induced Frobenius algebra structure in* $\widetilde{\mathbb{X}}$ *is counital.*

Proof. For all X, the map $X \to (X \otimes X) \otimes I$ in $\widetilde{\mathbb{X}}$ induced by the Frobenius algebra in $\mathbb{X}$ has a counit given by the unitor $X \to I \otimes X$ since, in $\mathbb{X}$:



□

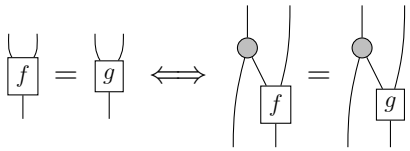
3.3 Categorical quantum mechanics and completely positive maps

The CPM construction gives a notion of quantum channels for any †-compact closed category [55]. The †-Frobenius algebras in the base category induce idempotents in CPM corresponding to decohering quantum channels. By considering the full subcategory of the Karoubi envelope whose objects are such idempotents one obtains the STOCH construction of [28]: yielding classical channels between finite dimensional C^*-algebras when applied to FHilb. However, the CPM construction can not be applied to Hilb in general because unlike FHilb, it is not compact closed. The CP^∞ construction [27] generalizes the CPM construction to (non compact closed) †-symmetric monoidal categories, by unbending the cups/caps and, identifying two super-maps when they act the same on all positive test maps: recovering the usual notion of purely quantum channels.

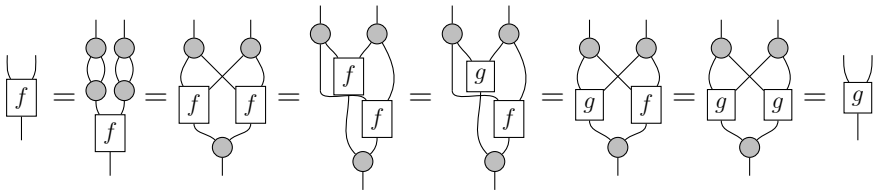
To generalize the STOCH construction to †-semi-Frobenius algebras, one must combine the STOCH and CP^∞ constructions, as the compact closed structure is no longer taken for granted. We show that the Cartesian completion is the same as first applying a modified version of the CP^∞ construction (without quantifying over all test maps, as seen in Figure 3.1) to a discrete inverse category and then taking the full

subcategory of the Karoubi envelope whose objects are the decoherence maps [3]. The following Lemma is needed to prove this fact:

Lemma 3.3.1. *Given two parallel maps $X \xrightarrow{f,g} Y \otimes Z$ in a discrete inverse category:*

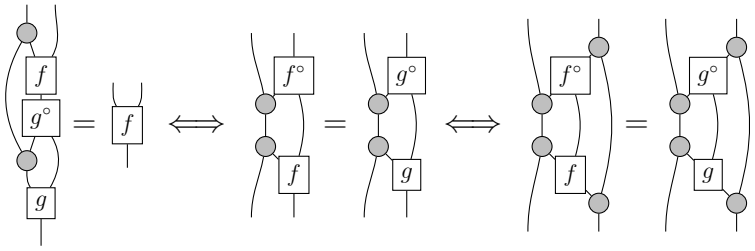


Proof. The one direction is trivial, for the other direction:

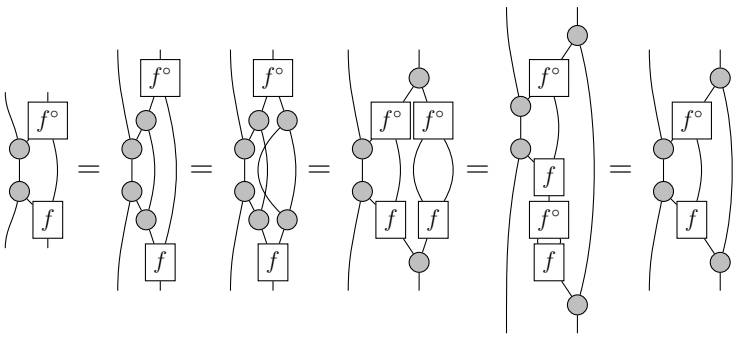


□

Lemma 3.3.2. *Given two maps $X \xrightarrow{f} Y \otimes S$ and $X \xrightarrow{g} Y \otimes T$, in a discrete inverse category:*

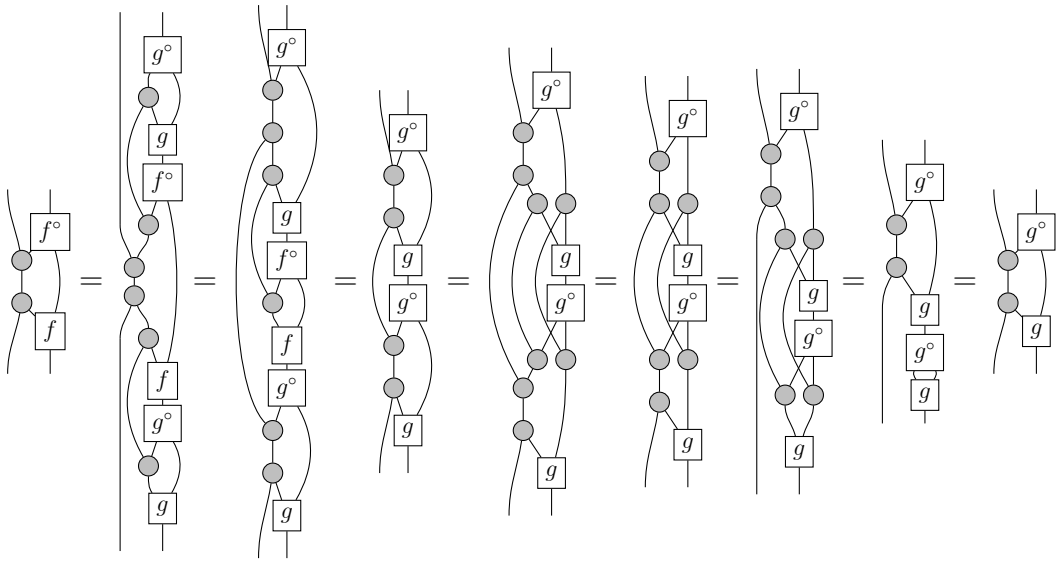


Proof. First note:

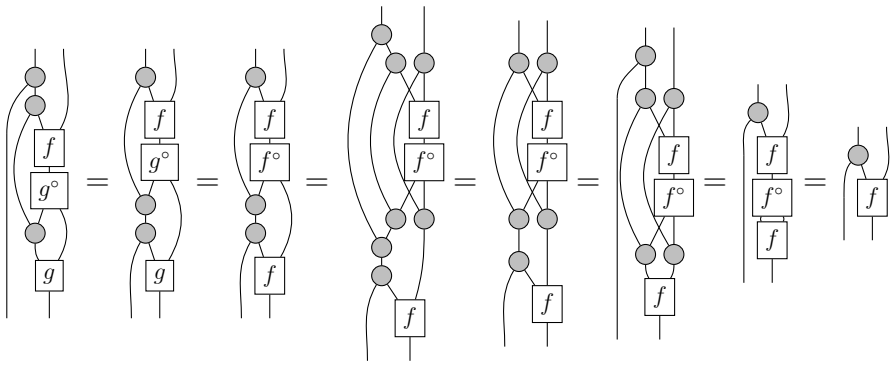


[3] Although, composition in this version of the CP^∞ construction, without universally quantifying over test maps, when applied to a discrete inverse category is not obviously well-defined unless the base category embeds in a compact closed category.

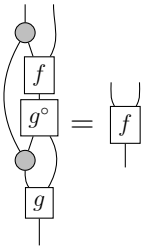
So that we only have to prove the first biconditional. Suppose that the left hand side holds, then:



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



Thus, by Lemma 3.3.1:



□

The natural question arises: can we characterize classical channels in this setting, algebraically in terms of a discarding morphism, without performing any doubling.

In other words, is there some notion of "environment structure" [31] for the *classical* channels of discrete inverse categories:

Definition 3.3.3. *Given a discrete inverse category $\mathbb{X}$, define the counital completion of $\mathbb{X}$, $c(\mathbb{X})$ to have the same objects and maps of $\mathbb{X}$, except with a freely adjoined counit $!_X : X \to I$ to the chosen semi-Frobenius algebra on X, for each object in $\mathbb{X}$ compatible with the monoidal structure.*

Lemma 3.3.4. *$c(\mathbb{X})$ is a discrete Cartesian restriction category.*

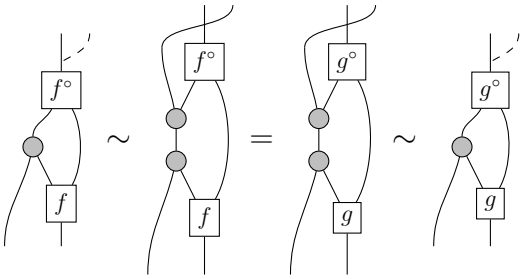
Proof. This is clearly a counital copy category, with a restriction terminal object given by the tensor unit. Moreover, because the Frobenius structure is special, it is also discrete. □

Lemma 3.3.5. *Given a discrete inverse category $\mathbb{X}$, $c(\mathbb{X})$ and $\widetilde{\mathbb{X}}$ are isomorphic as discrete Cartesian restriction categories.*

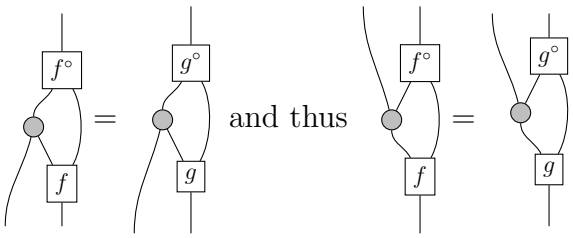
Proof. Define an identity on objects functor $F : c(\mathbb{X}) \to \widetilde{\mathbb{X}}$ in the obvious way, sending the counits to the ancillary space. Similarly, define an identity on objects functor from $G : \widetilde{\mathbb{X}} \to c(\mathbb{X})$ given by plugging counits into the ancillary space. These maps are clearly inverses to each other and preserve discrete Cartesian restriction structure; however, once again we mush show that they are actually functors.

To see that F is a functor, it suffices to observe that every object in $\widetilde{\mathbb{X}}$ is equipped with a counital Frobenius algebra, compatible with the monoidal structure, where the unit is in the image of the freely adjoined counit under F.

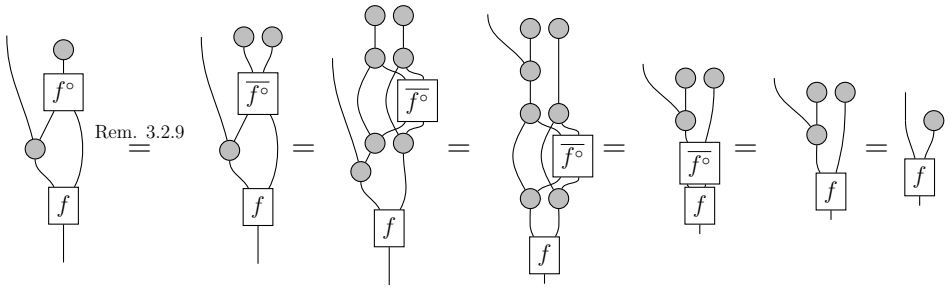
To prove that G is a functor, take some $(f, S) \sim (g, T)$ in $\widetilde{\mathbb{X}}$. Therefore, in $\widetilde{\mathbb{X}}$, since the Frobenius structure is counital:



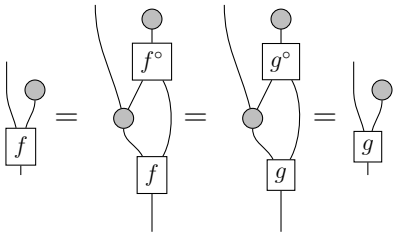
However, since the functor $\mathbb{X} \to \widetilde{\mathbb{X}}$ is faithful by Lemma 3.2.15, using the alternate equivalence relation of $\widetilde{\mathbb{X}}$ by Lemma 3.3.2, we have that in $\mathbb{X}$:



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



So that combining the previous two equations:



□

3.4 ZX&

In this section, we give a complete presentation, 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 adding a counit and unit to the semi-Frobenius algebra structure of the category TOF (described in [21]), and then performing a two way translation between this prop and ZX& which we prove is an isomorphism.

Definition 3.4.1. TOF *[21] is the PROP, generated by the 1 ancillary bits* $|1\rangle$ *and* $\langle 1|$ *as well as the Toffoli gate, satisfying the identities given in Figure 3.2.*

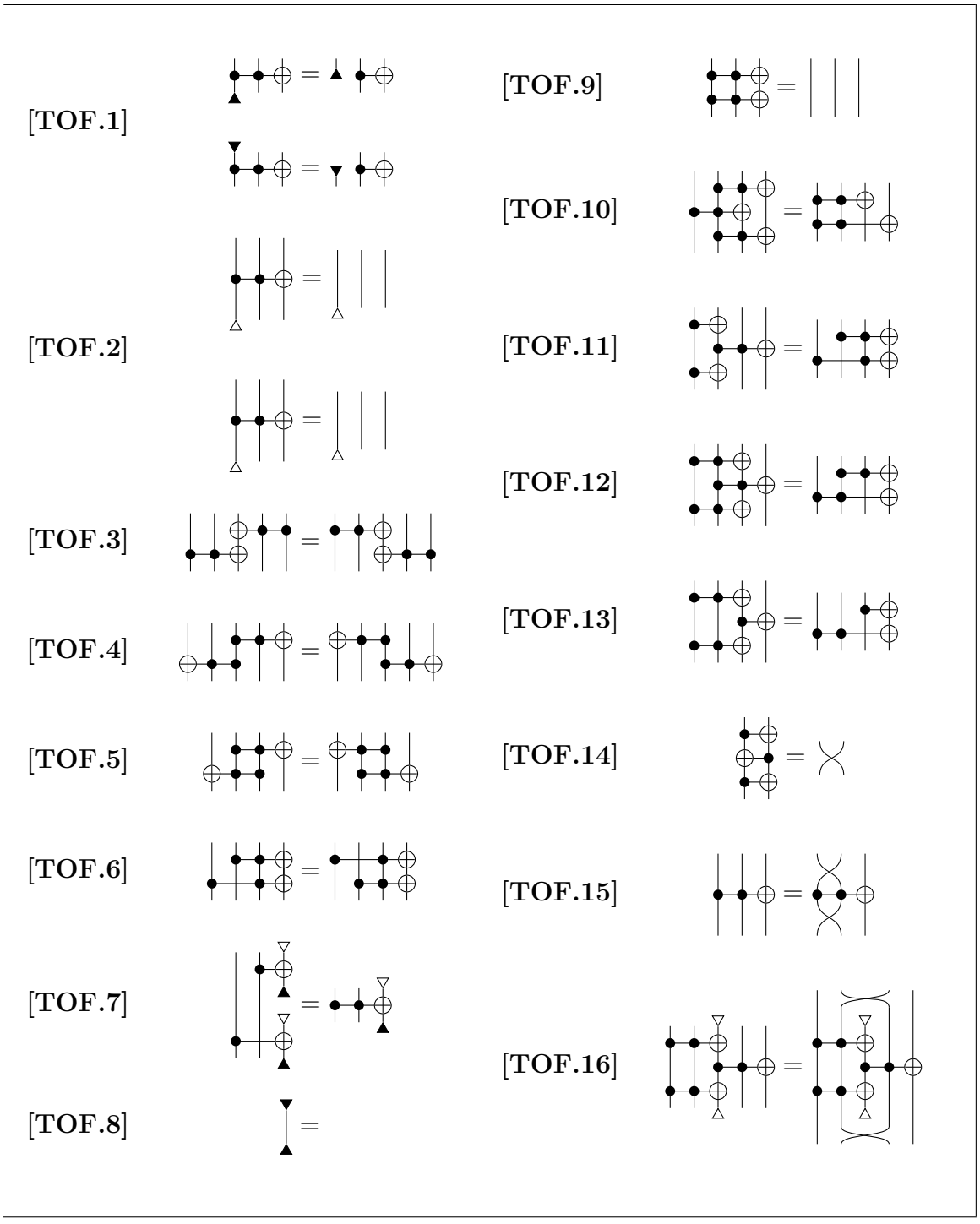
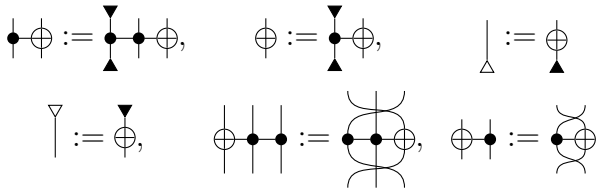


Figure 3.2: The identities of TOF

The Toffoli gate and the 1-ancillary bits allow cnot, not, $|0\rangle$, $\langle 0|$, *and flipped* tof *gate and flipped* cnot *gate can defined in this setting:*



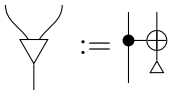
Theorem 3.4.2. *[21]* TOF *is isomorphic to the category of partial isomorphisms between ordinals* 2^n*,* $n \in \mathbb{N}$*.*

One can moreover construct generalized controlled not gates with arbitrarily many control wires in the obvious way. Let $[x, X]$ denote a generalized Toffoli gate acting on the xth wire, controlled on the wires indexed by a set X. Then we can partially commute generalized controlled-not gates:

Lemma 3.4.3. *[32, Lem. 7.2.6] Let* $[x, X]$ *and* $[y, Y]$ *be generalized controlled not gates in* TOF *where* $x \notin Y$*. We can perform the identities of Iwama et al. [46], to commute them past each other with a trailing generalized controlled not gate as a side effect:*

$$[y, X \cup Y][y, Y \sqcup \{x\}][x, X]$$

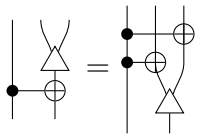
In TOF, one can define the diagonal map as follows:



Lemma 3.4.4. *[32, §5.3.2] The diagonal map is a natural special commutative †-symmetric monoidal nonunital Frobenius algebra.*

It is also natural on target qubits:

Lemma 3.4.5. *[32, Lem. B.0.2 (iii)]*



Adding a unit and counit to TOF

By adding a unit and counit, we obtain a full subcategory of spans of sets and finite ordinals:

Lemma 3.4.6. *The full subcategory of* $\mathsf{Span}^{\sim}(\mathsf{FinOrd})$ *generated by powers of 2 is presented by the pushout,* $\widehat{\mathsf{TOF}}$*, of the following diagram of props:*

$$c(\mathsf{TOF})^{\mathsf{op}} \leftarrow \mathsf{TOF} \rightarrow c(\mathsf{TOF})$$

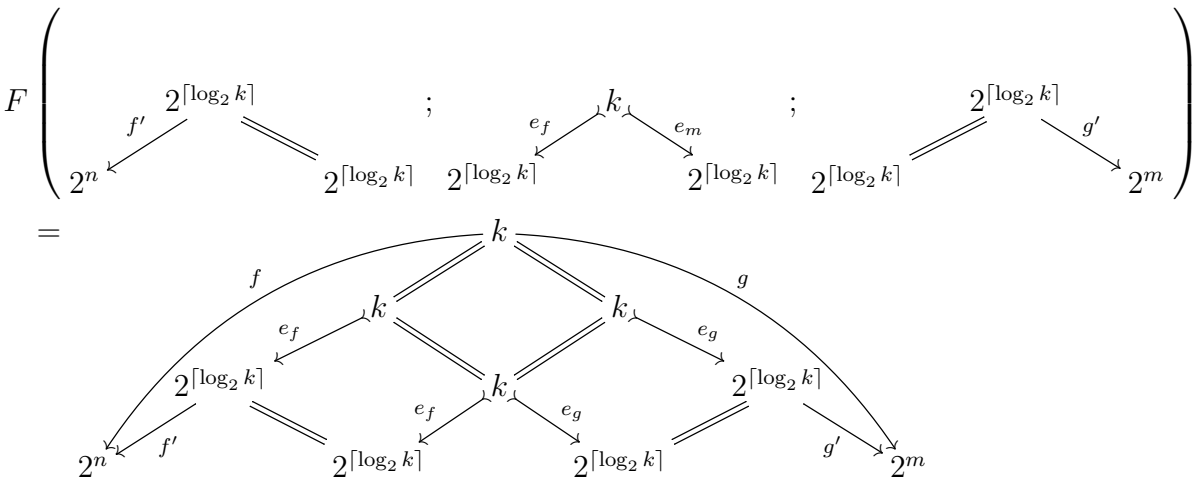
Proof. Recall that TOF is presented by the subcategory FPinj_2 of $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ with morphisms of the form $2^n \xleftarrow{e} k \xrightarrow{e'} 2^m$ for arbitrary natural numbers n, m, k and monics e and e'.

Similarly, $\widetilde{\mathsf{TOF}}$ is presented by the subcategory FPar_2 of $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ with morphisms of the form $2^\ell \xleftarrow{f} 2^n \xleftarrow{e} k \xrightarrow{e'} 2^m$ for arbitrary natural numbers ℓ, n, m, k and monics e and e' and function f. Let FSpan_2 denote the full subcategory of $(\mathsf{Span}^{\sim}(\mathsf{FinOrd}), \times)$ generated by powers of two. Consider the pushout $\mathbb{X}$ of the following diagram of props:

$$\mathsf{FPar}_2^{\mathsf{op}} \longleftarrow \mathsf{FPinj}_2 \longrightarrow \mathsf{FPar}_2$$

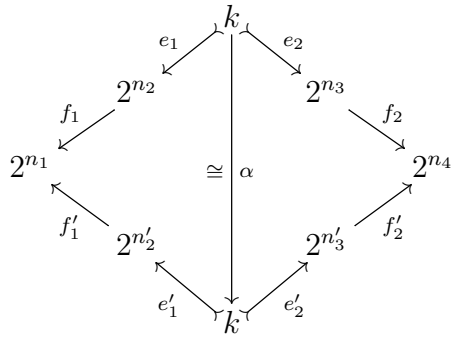
Consider the functor $F : \mathbb{X} \to \mathsf{FSpan}_2$ induced by the universal property of the pushout. We show that this functor is an isomorphism. This functor is clearly the identity on objects.

For fullness consider some span $2^n \xleftarrow{f} k \xrightarrow{g} 2^m$. 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 $f = ef'$. 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:

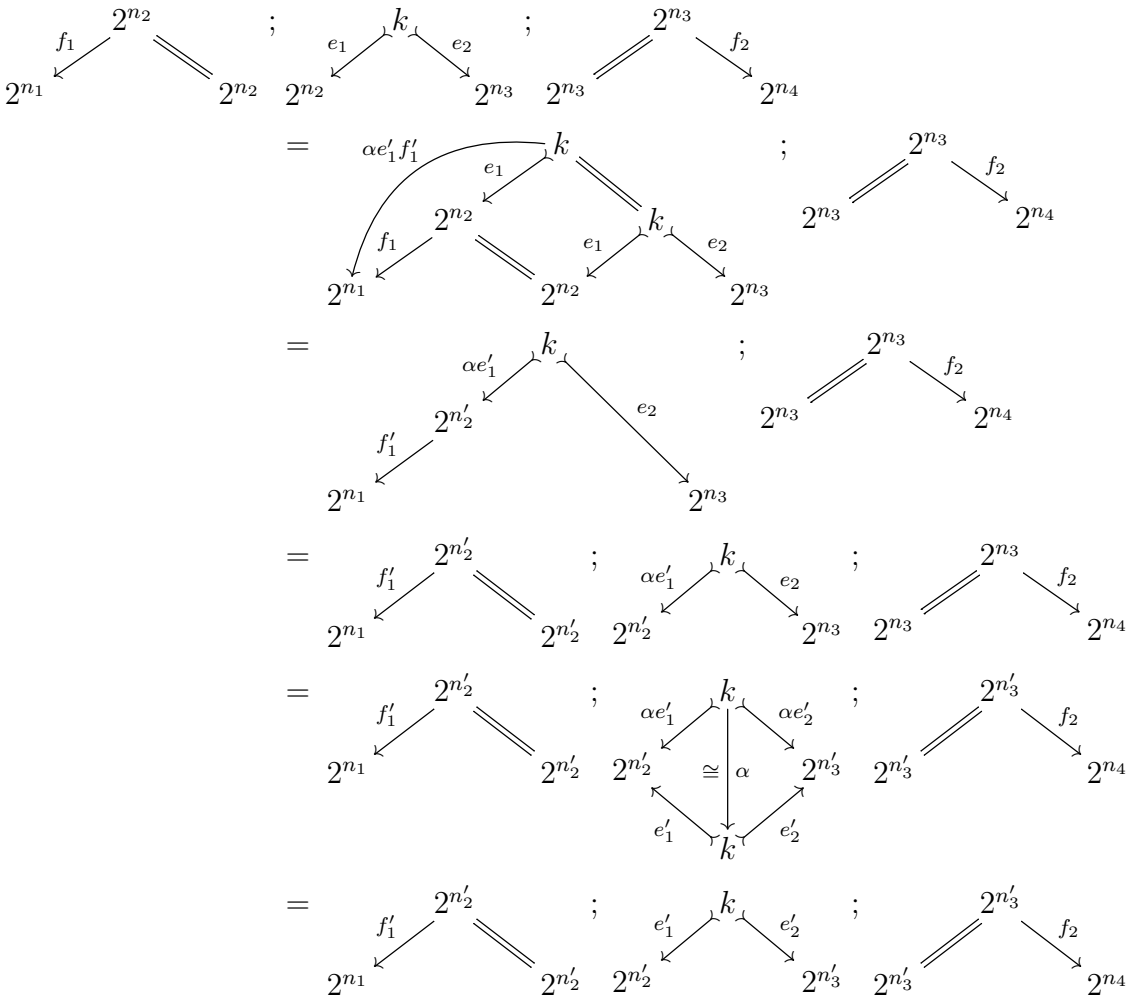


So F is full.

For faithfulness suppose we have any two isomorphic spans in $F(\mathbb{X})$:

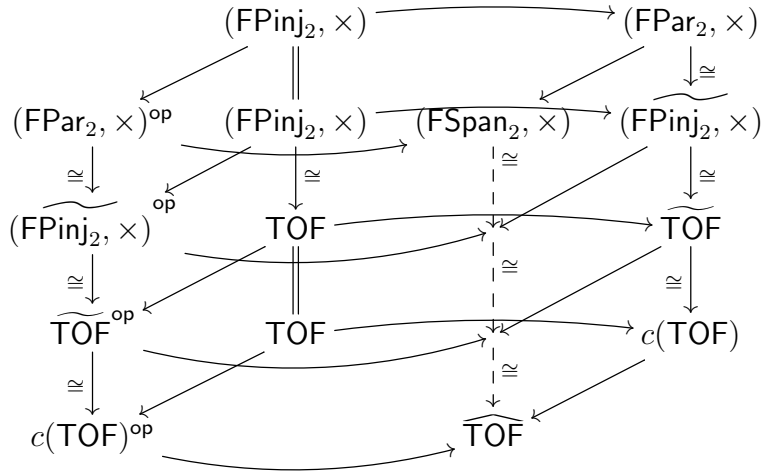


In $\mathbb{X}$, we have:



Therefore $\mathsf{FSpan}_2 \cong \mathbb{X}$.

Two show that $\widehat{\mathsf{TOF}} \cong \mathsf{FSpan}_2$, consider the following diagram where each horizontal face is a pushout:



All of the rear and left faces commute. Moreover, the vertical maps are isomorphisms, therefore the maps induced by universal property of the pushout are isomorphisms.

□

If f is a partial isomorphism between finite sets, then the white spiders correspond to the classical structure for the chosen computational basis. For the interpretation into FHilb via the ℓ_2 functor, this means that in the qubit case, the unit and counit correspond to $\sqrt{2}|+\rangle$ and $\sqrt{2}\langle+|$.

We give a more elegant presentation of this category in terms of interacting monoids and comonoids:

Definition 3.4.7. *Consider the self dual prop* $\mathsf{ZX}\&$ *generated by the addition spider with phases in* $\{0, \pi\}$*, the copy spider and the monoid for conjunction satisfying the identities given in Figure 3.3.*

One can interpret the generators as logical connectives and open wires as variables, similar to the regular logic [15], or the logic of a Cartesian bicategory [16], except we forget the 2-cells in $\mathsf{ZX}\&$. The decorated black spiders correspond to fixed variables and xor. White (co)multiplications (co)copy variables; the white unit is existential quantification and the counit is discarding. The relations are open Σ_1 Boolean formulas augmented with copying and discarding as well as duals; the open variables correspond to distinguished inputs and outputs.

The identities of $\mathsf{ZX}\&$ can also be interpreted by freely taking the coproduct of the free prop of commutative (co)monoids †-PROP 3×2 times, modulo various (undirected) distributive laws, and monoid maps. The distributive laws are summarized in Figure 3.4 (the duals under diagonal are omitted). Te spider rules implicitly identify the (co)units of the †-compact closed structure induced by Z and X; which is needed for completeness.

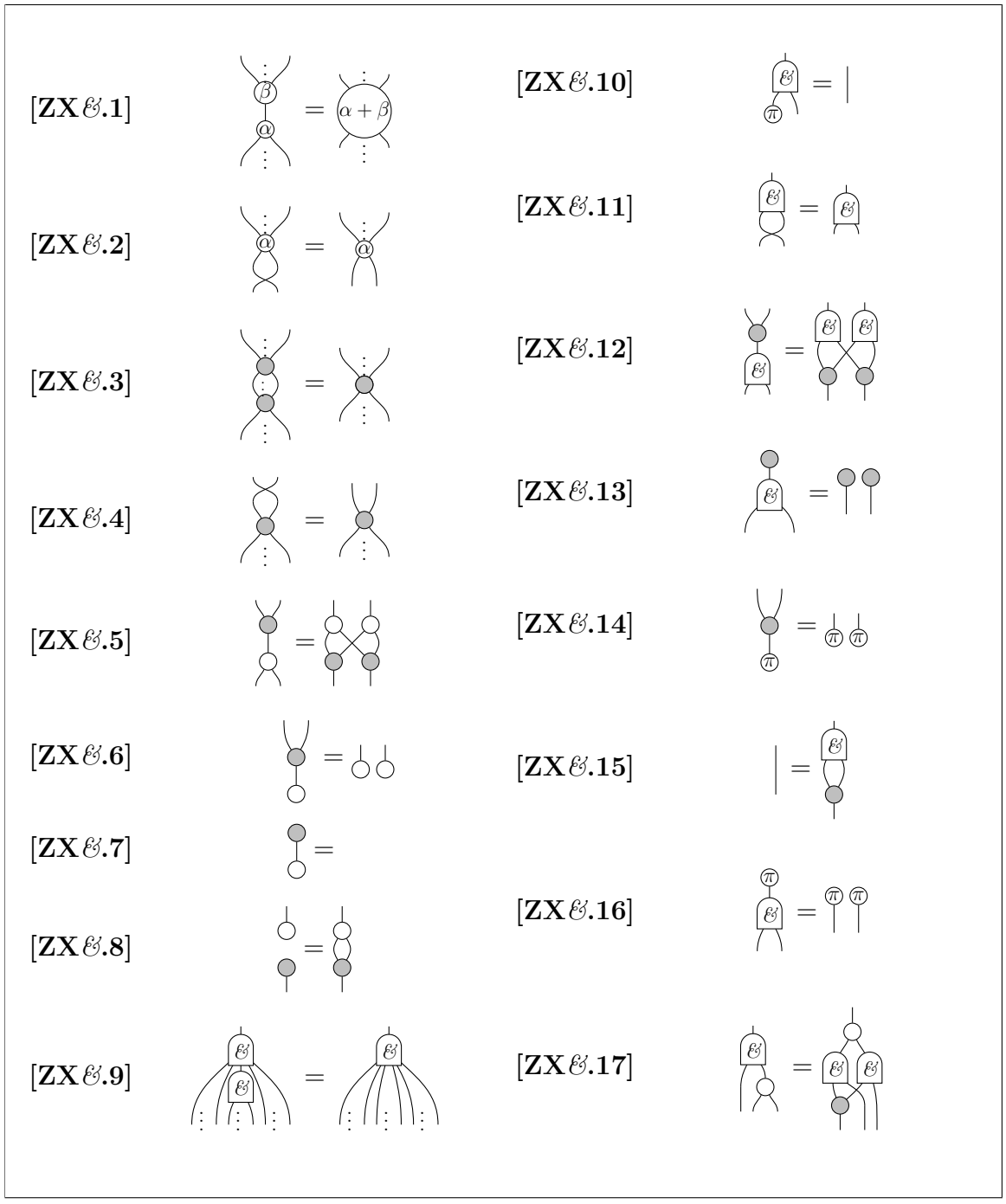


Figure 3.3: The identities of $\mathsf{ZX}\mathscr{G}$, where $\alpha, \beta \in \{0, \pi\}$ and a blank grey spider has angle 0.

λ	Z	X	$\&$	$Z^\dagger$	$X^\dagger$	$\&^\dagger$
Z	Comm. monoid			Extra special comm. †-Frobenius algebra	Hopf algebra with $s = 1$	Special bialgebra
X		Comm. monoid		Hopf algebra with $s = 1$	Comm. †-Frobenius algebra	
$\&$			Comm. monoid	Special bialgebra		
$Z^\dagger$				Cocomm. comonoid		
$X^\dagger$					Cocomm. comonoid	
$\&^\dagger$						Cocomm. comonoid

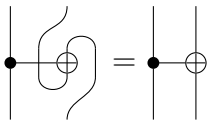
Figure 3.4: Generating distributive laws of $\mathsf{ZX}\&$.

Additionally, [**ZX&.16**] states that the counit of $\&^\dagger$ is copied by $\&$; ie. the counit is a monad map from $\&$ to the trivial monad. [**ZX&.17**] expreses the multiplication part of the distributive law of Lawvere theories between the props for multiplication and addition mod 2 (see [19] for distributive laws of Lawvere theories).

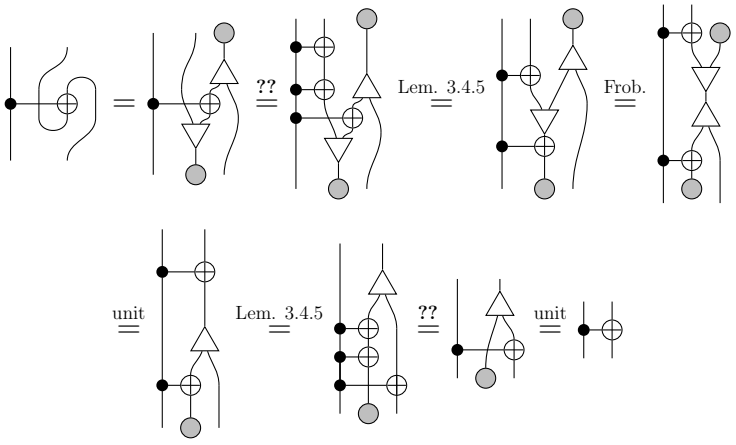
Before, we prove there is a functor from $\mathsf{ZX}\&$ to $\widehat{\mathsf{TOF}}$, we establish some basic properties of $\widehat{\mathsf{TOF}}$.

First, the cnot gate is its own mate on the second wire:

Lemma 3.4.8.



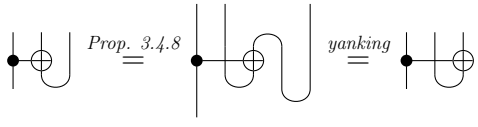
Proof.



□

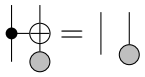
Therefore,

Lemma 3.4.9.

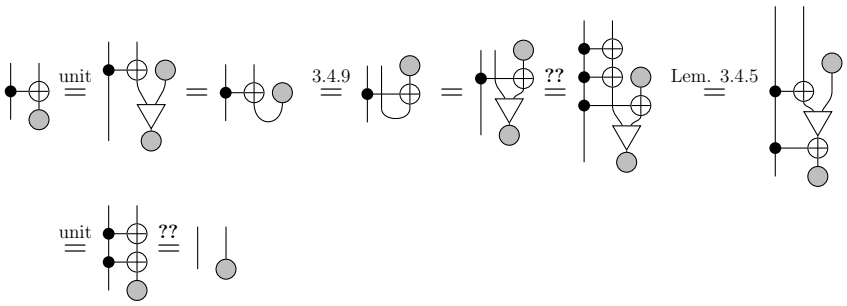


Thus

Lemma 3.4.10.

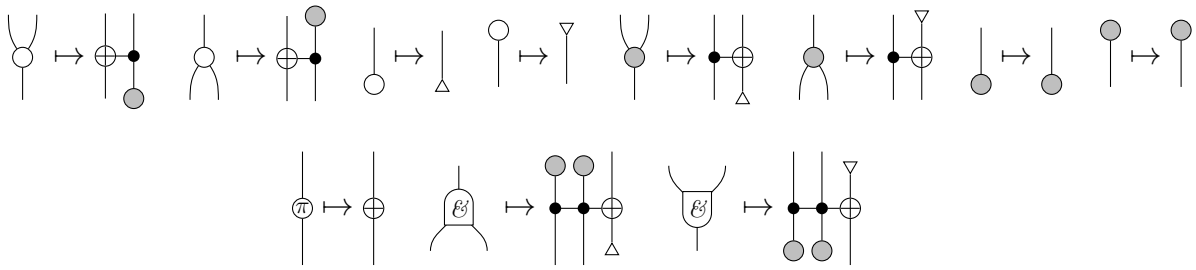


Proof.



□

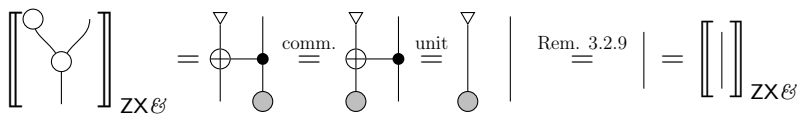
Proposition 3.4.11. *Consider the interpretation* $[\![\_]\!]_{\mathsf{ZX}\mathscr{E}} : \mathsf{ZX}\mathscr{E} \to \widehat{\mathsf{TOF}}$ *taking:*



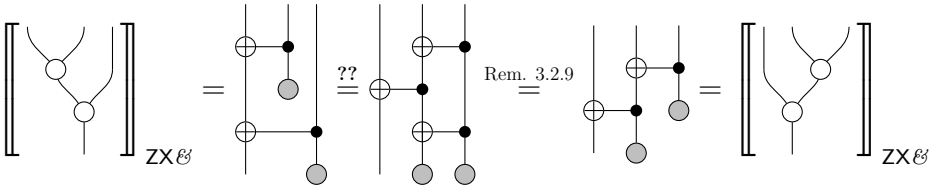
This interpretation is a strict symmetric †-monoidal functor.

Proof. We prove that all of the axioms of $\mathsf{ZX}\mathscr{E}$ hold in $\widehat{\mathsf{TOF}}$:

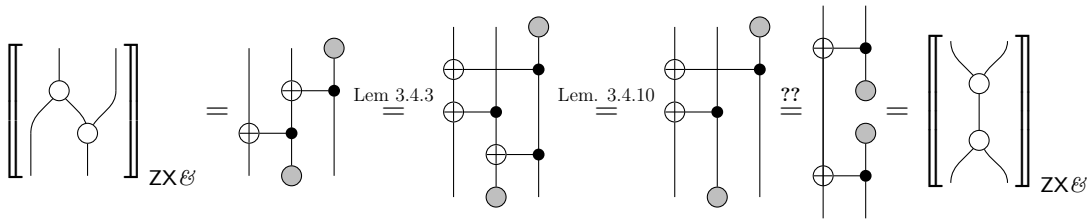
[**ZX$\mathscr{E}$.1**]: **Unitality:** By Lemma 3.4.10:



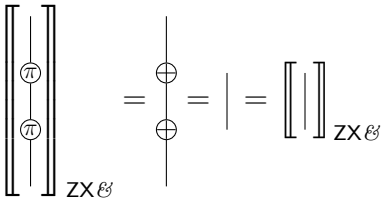
Associativity:



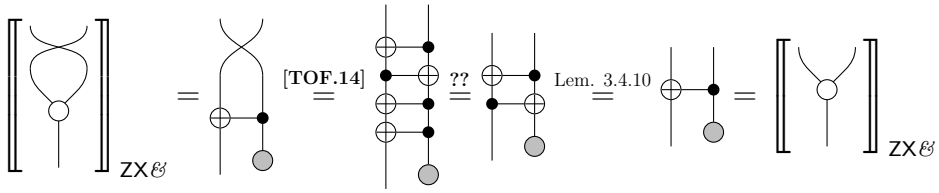
Frobenius:



Phase amalgamation:



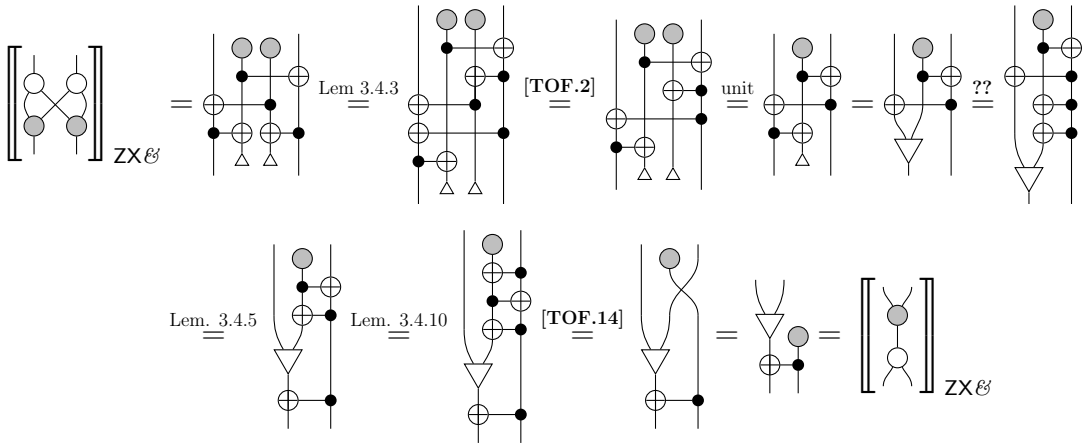
[**ZX&.2**]:



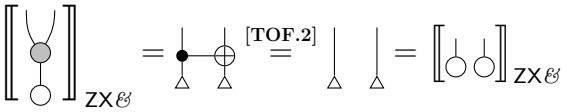
[**ZX&.3**]: This is immediate.

[**ZX&.4**]: This is immediate.

[**ZX&.5**]:

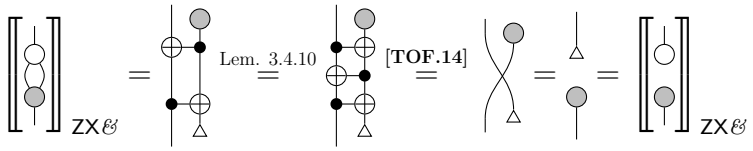


[**ZX&.6**]:

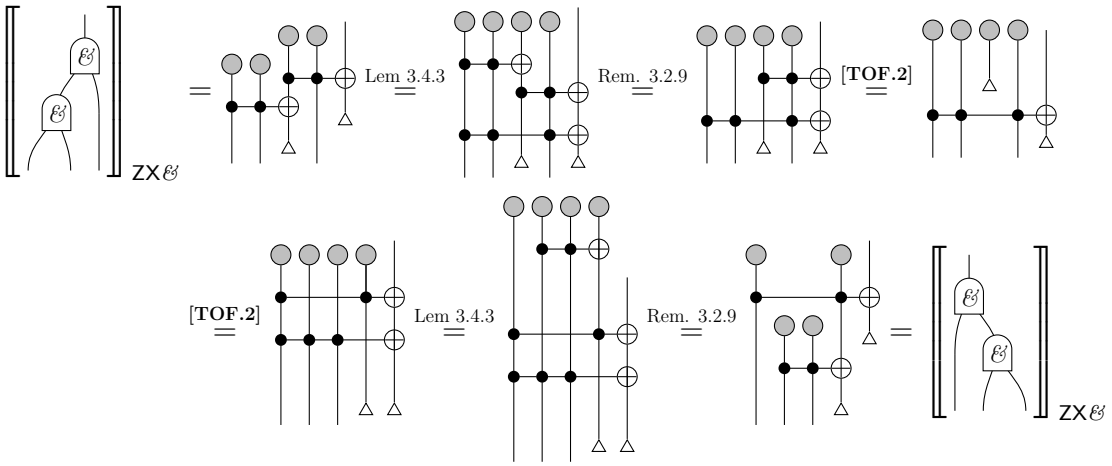


[**ZX&.7**]: This is immediate.

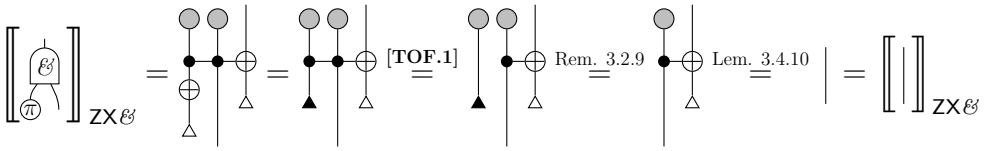
[**ZX&.8**]:



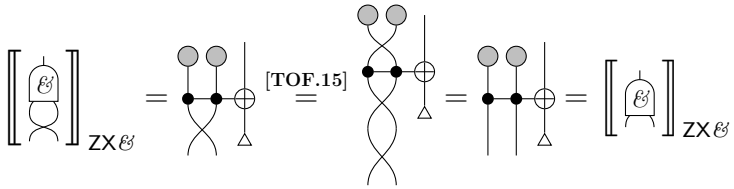
[**ZX&.9**]:



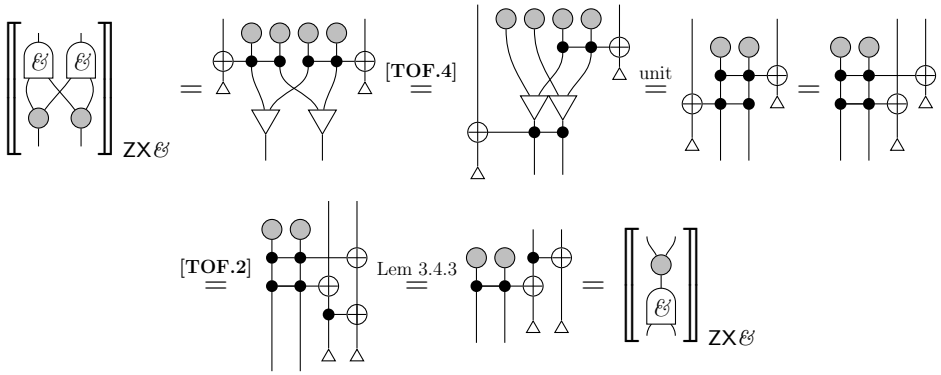
[**ZX&.10**]:



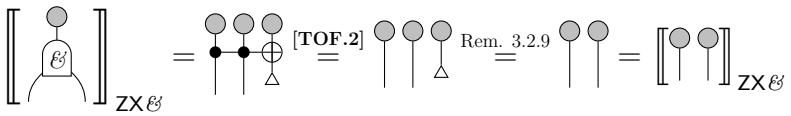
[**ZX&.11**]:



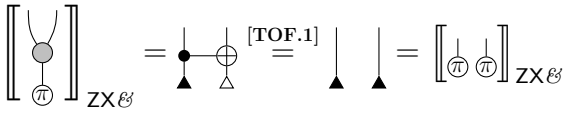
[**ZX&.12**]:



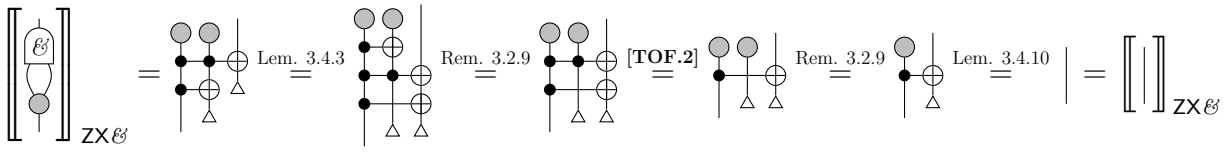
[**ZX&.13**]:



[**ZX&.14**]:

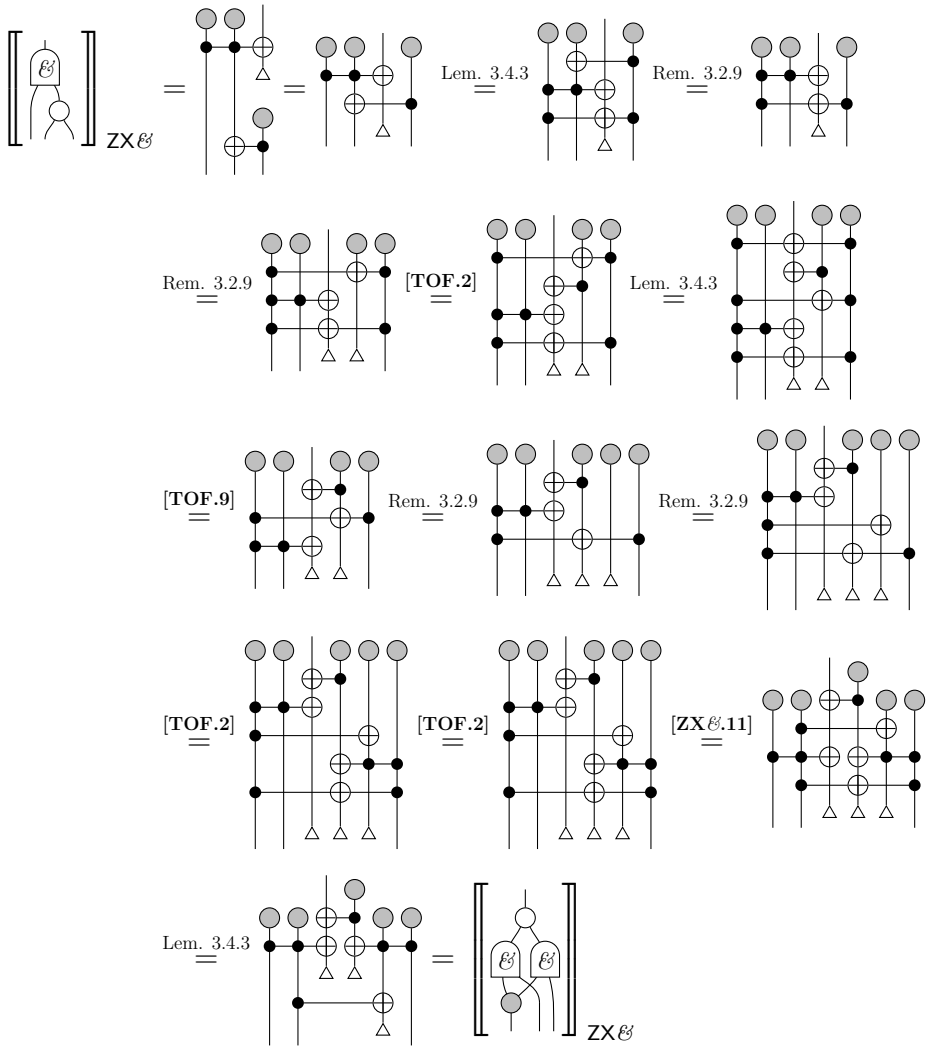


[**ZX&.15**]:



[**ZX&.16**]: This is precisely [**TOF.7**].

[**ZX&.17**]:

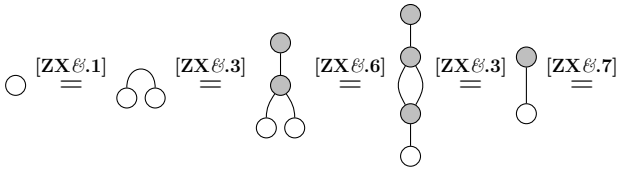


□

To prove functoriality in the other direction, we prove some basic properties of ZX&.

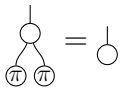
Lemma 3.4.12.

Proof.



□

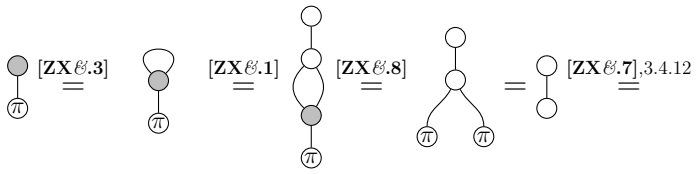
Lemma 3.4.13. *The phase fusion of the black spider in* $\mathsf{ZX}\mathscr{\&}$*,*



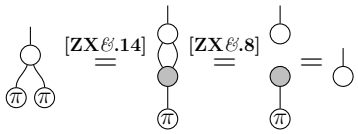
in the presence of the other axioms is equivalent to asserting:

Or in other terms, the phase fusion of the black spider is equivalent to the interaction of the unit for and and the counit for copying as a bialgebra.

Proof. For the one direction, suppose that phase fusion holds:

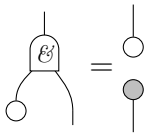


Conversely if the unit part of the bialgebra rule holds:

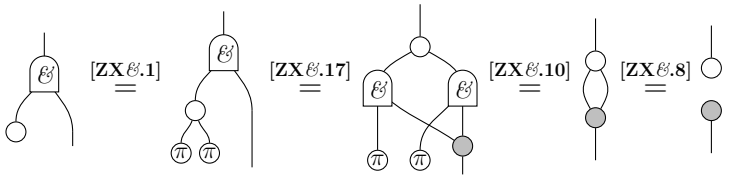


□

Lemma 3.4.14.

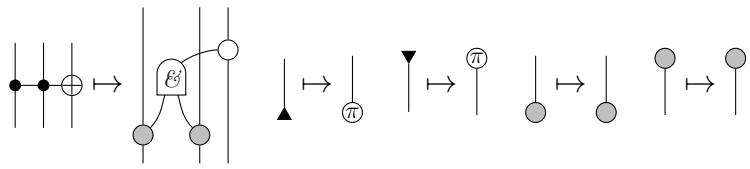


Proof.



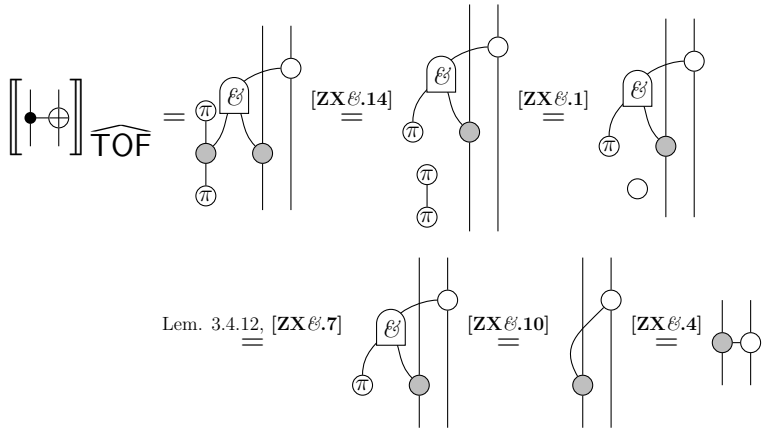
□

Proposition 3.4.15. *Consider the interpretation* $[\![\_]\!]_{\widehat{\mathsf{TOF}}} : \widehat{\mathsf{TOF}} \to \mathsf{ZX}\mathscr{\&}$ *taking:*

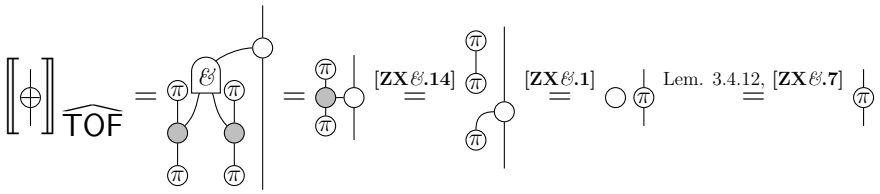


This interepretation is a strict symmetric †-monoidal functor.

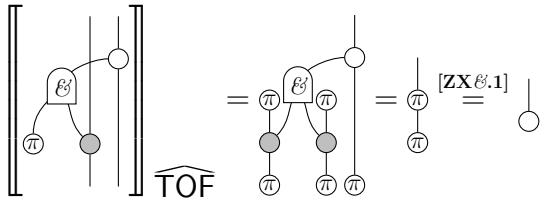
Proof. First, observe:



Thus:

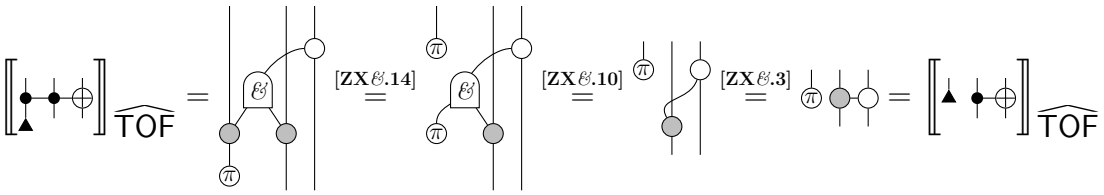


Thus:

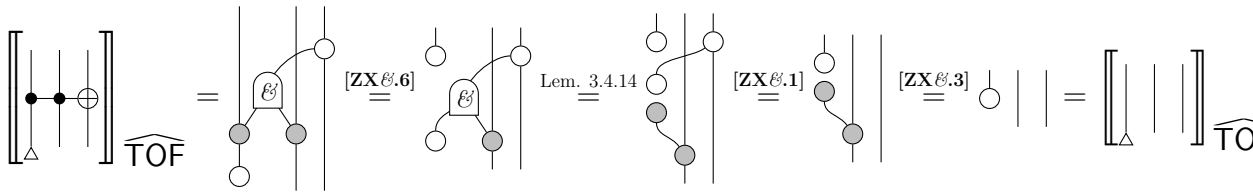


We prove that all of the axioms of $\widehat{\mathsf{TOF}}$ hold in $\mathsf{ZX}\&$:

[**TOF.1**]:



[**TOF.2**]:



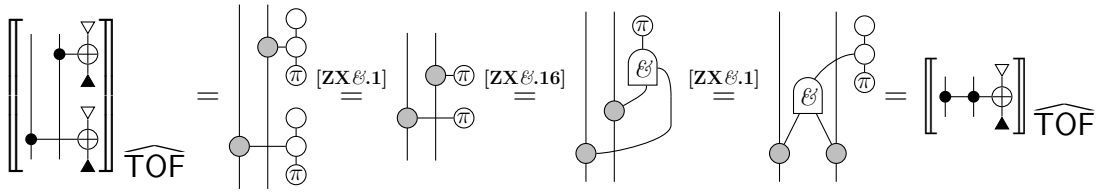
[**TOF.3**]: This follows from the spider law.

[**TOF.4**]: This follows from the spider law.

[**TOF.5**]: This follows from the spider law.

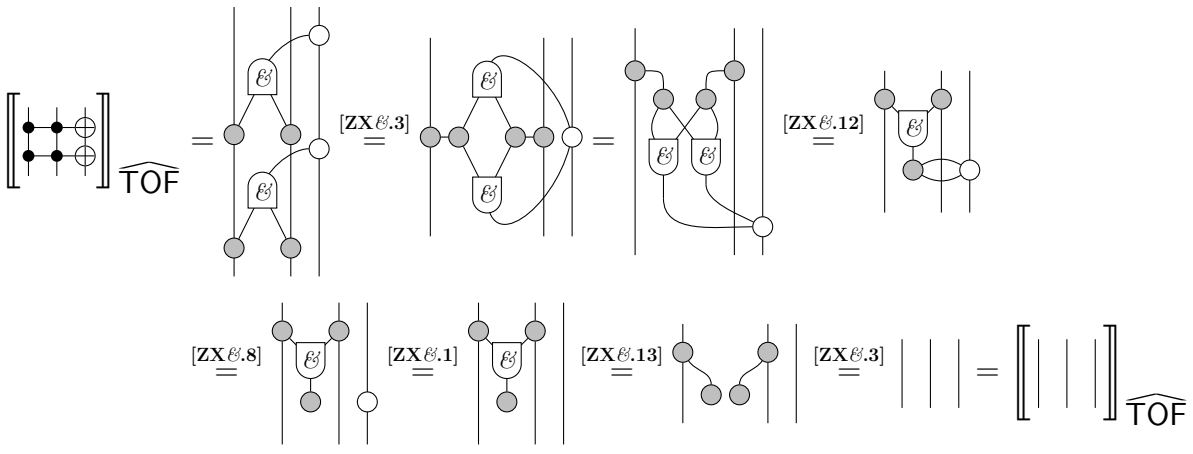
[**TOF.6**]: This follows from the spider law.

[**TOF.7**]:

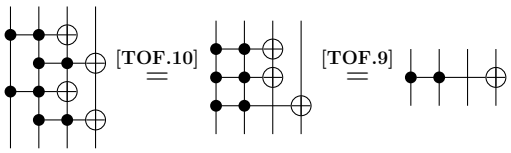


[**TOF.8**]: This follows immediately from Lemma 3.4.12 and [**ZX&.7**].

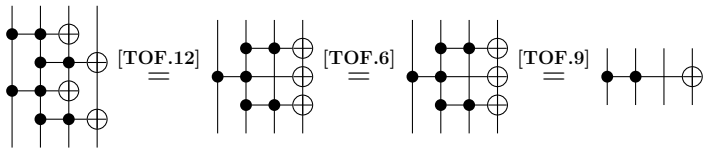
[**TOF.9**]:



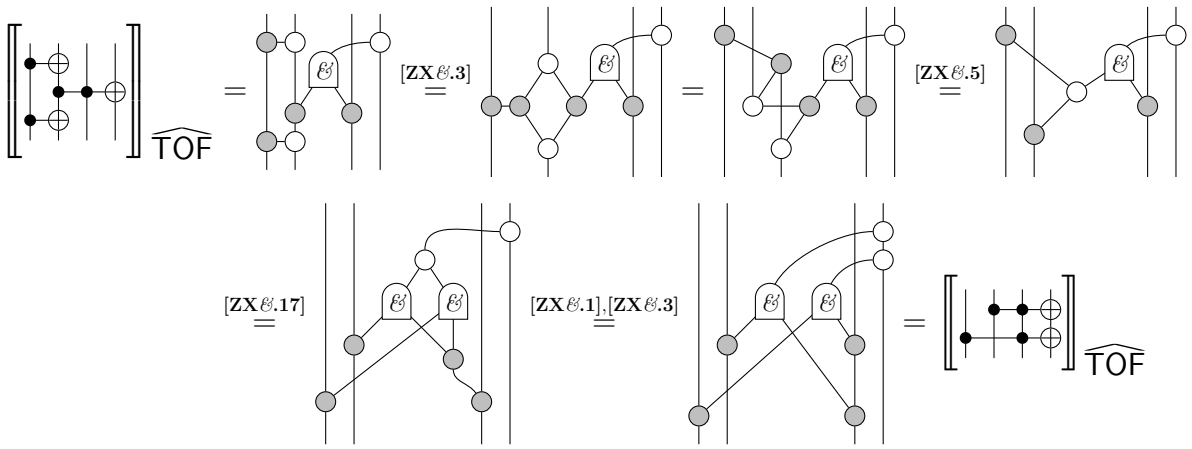
[**TOF.10**]: It is easier to prove that [**TOF.10**] is redundant. Given [**TOF.9**], [**TOF.6**] and [**TOF.12**], [**TOF.10**] is equivalent to the following:



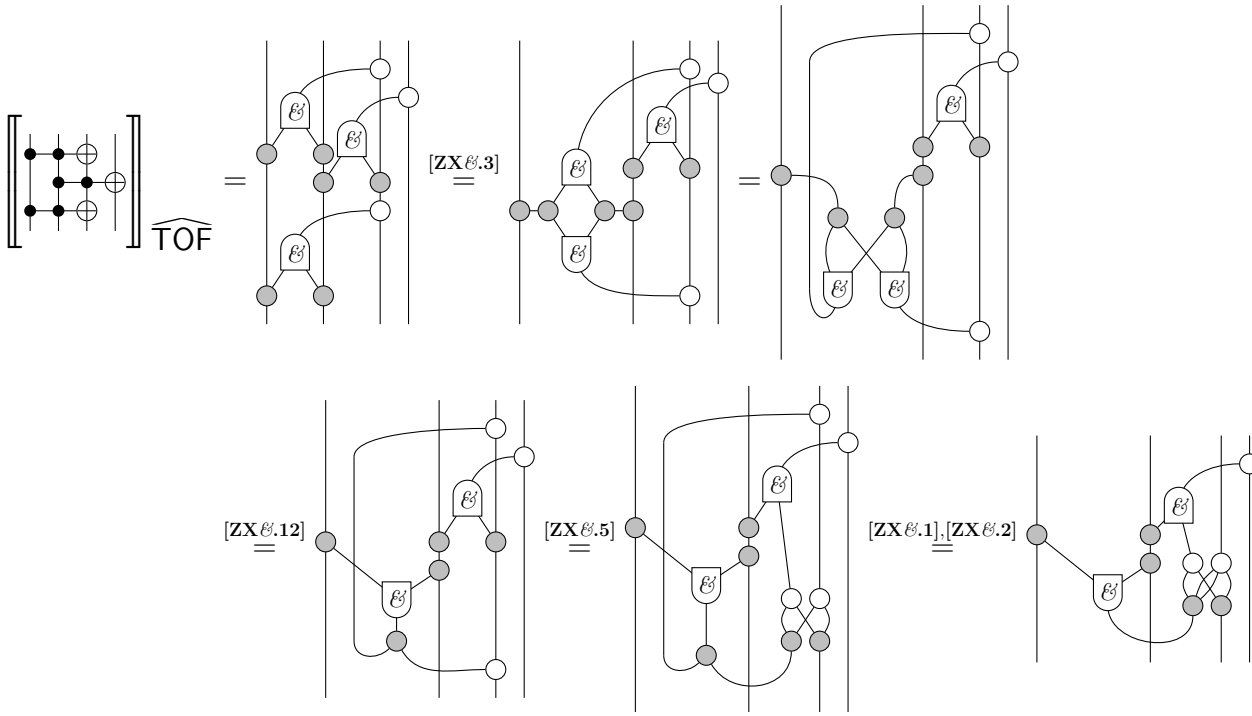
However

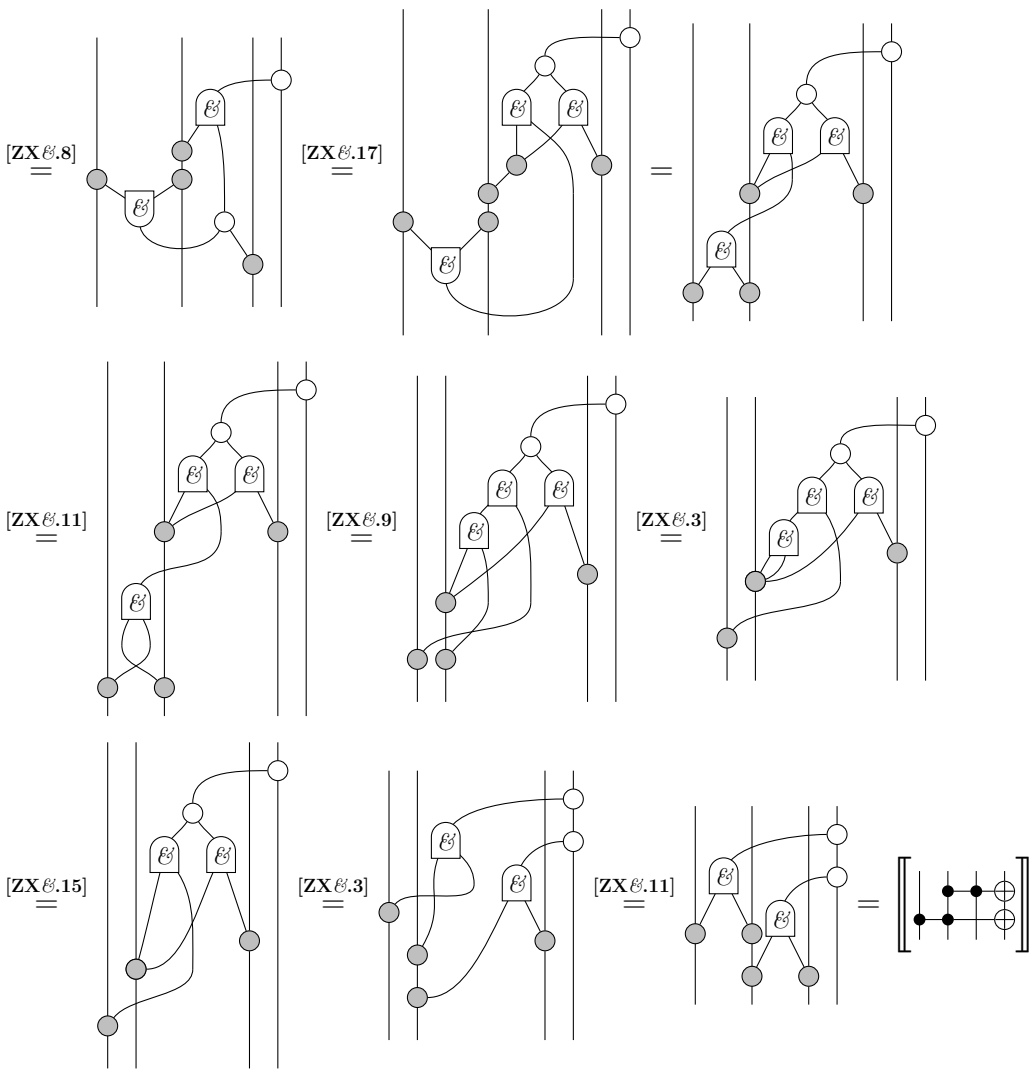


[**TOF.11**]:

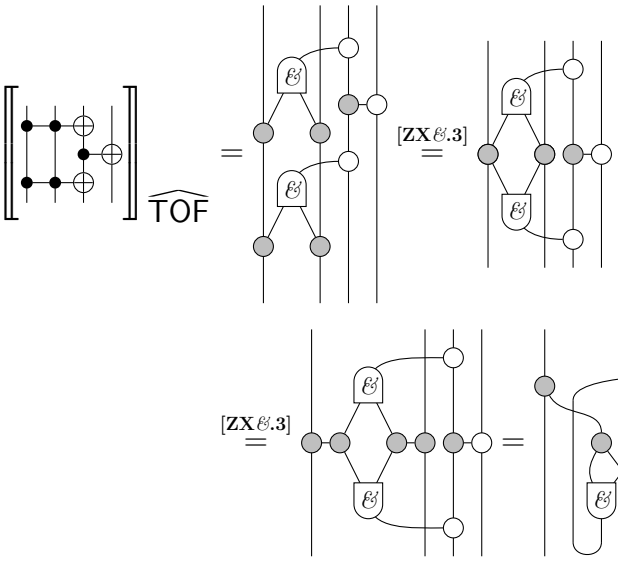


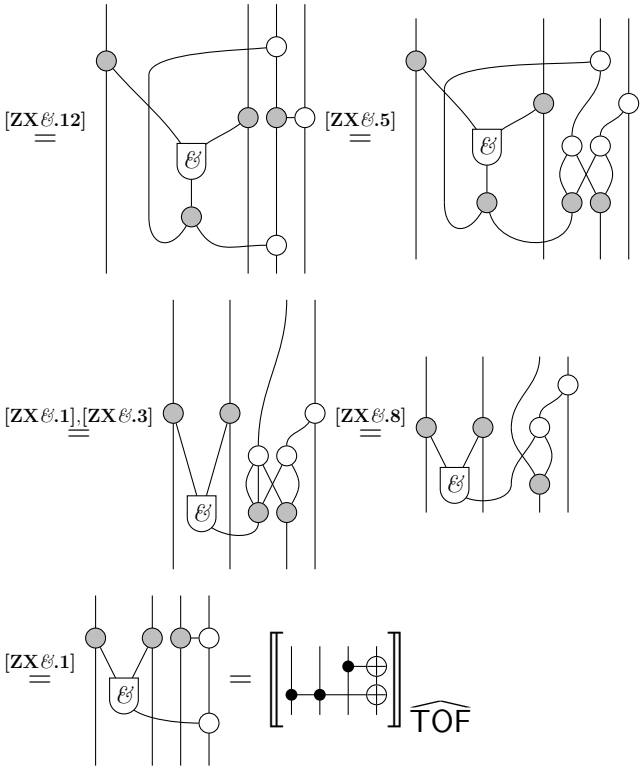
[**TOF.12**]:



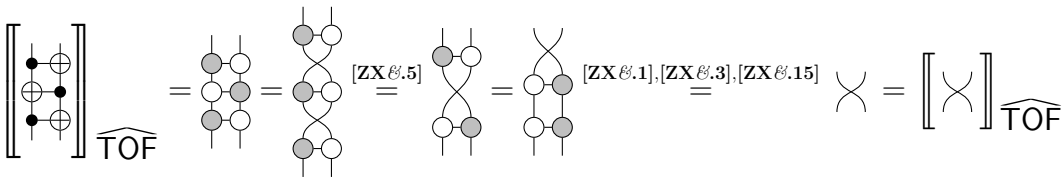


[**TOF.13**]:

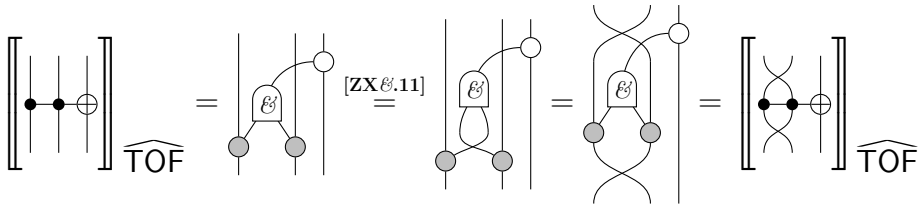




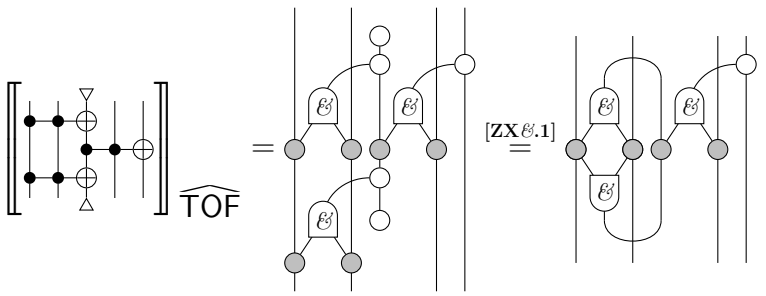
[**TOF.14**]:

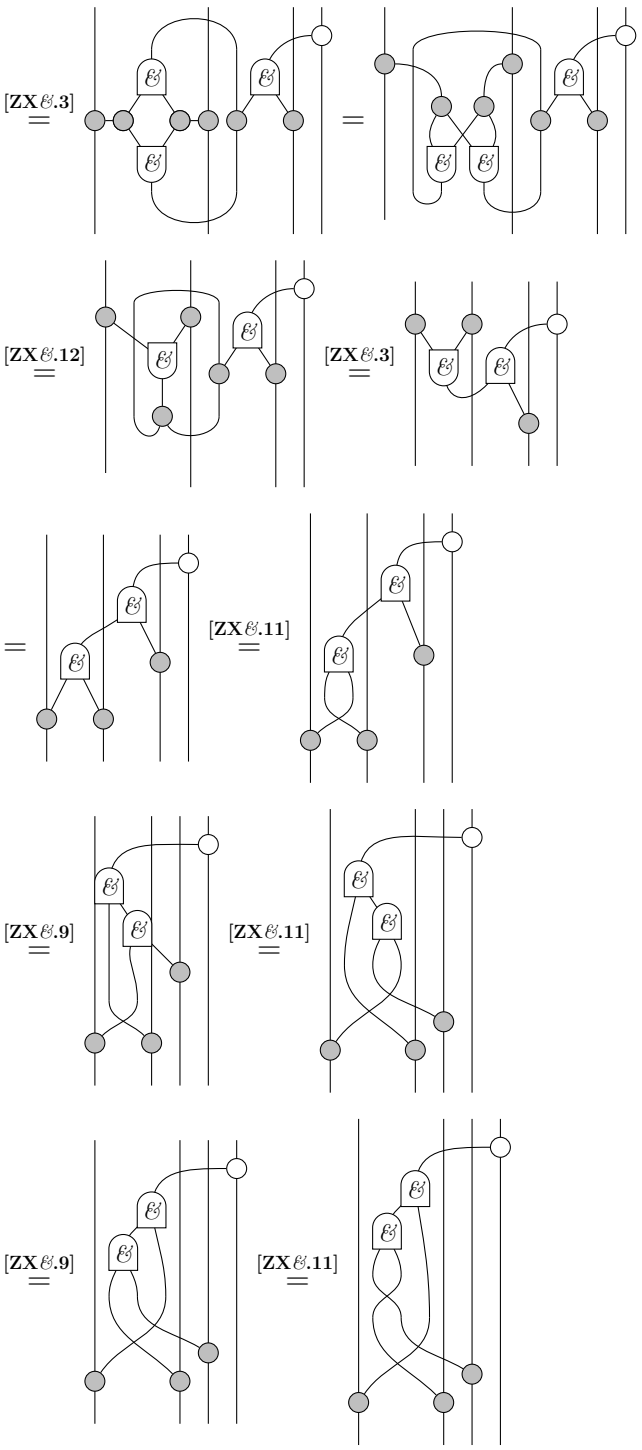


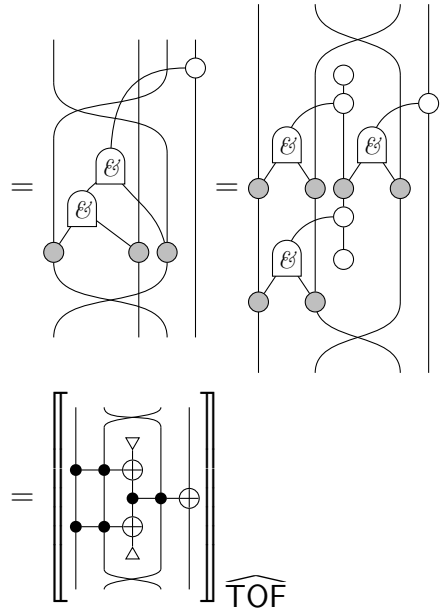
[**TOF.15**]:



[**TOF.16**]:




[ZX&.3]
=
=
[ZX&.12]
=
[ZX&.3]
=
=
[ZX&.11]
=
[ZX&.9]
=
[ZX&.11]
=
[ZX&.9]
=
[ZX&.11]
=



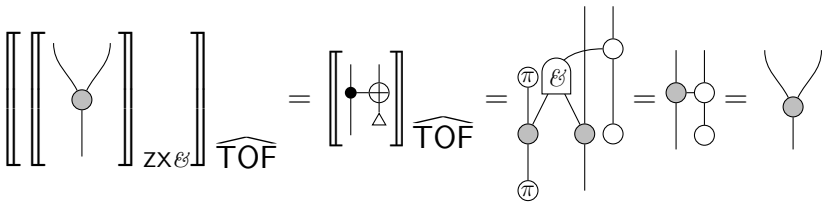
Where unitality and counitality follow from the fact that the white spiders are Frobenius algebras. Also, we must also note that both Frobenius algebras induce the same compact closed structure, as is implied by the spider law; this is immediate.

□

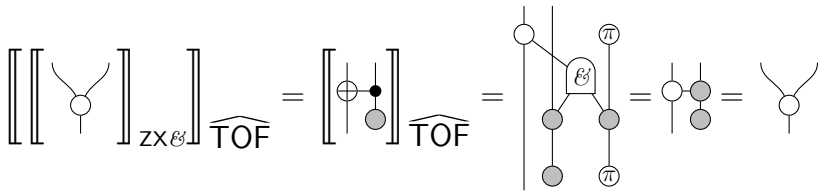
Theorem 3.4.16. *The interpretation functors* $[\![\_]\!]_{\mathsf{ZX}\mathscr{B}}$ *and* $[\![\_]\!]_{\widehat{\mathsf{TOF}}}$ *are inverses, so that* $\widehat{\mathsf{TOF}}$ *and* $\mathsf{ZX}\mathscr{B}$ *are isomorphic as strongly compact closed props.*

Proof. First we show that $[\![[\![\_]\!]_{\mathsf{ZX}\mathscr{B}}]\!]_{\widehat{\mathsf{TOF}}} = 1$:

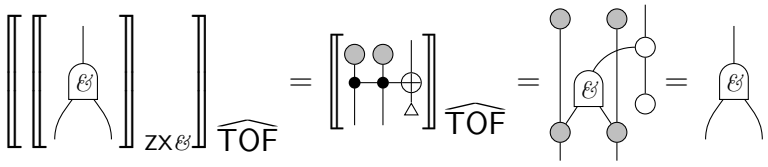
For the white spider: The case for the unit and counit is trivial. For the (co)multiplication we have:



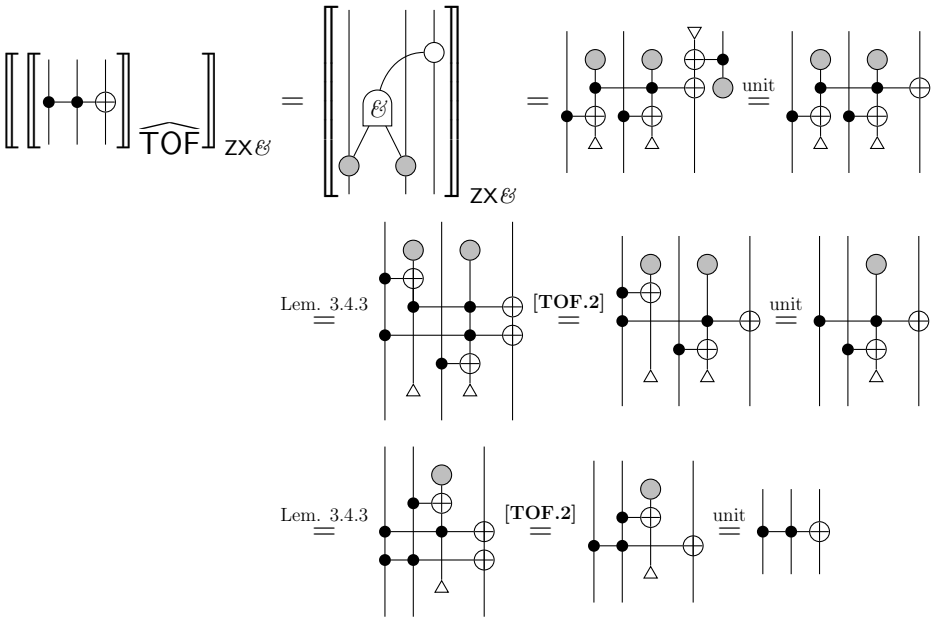
For the grey spider: The cases for the unit, counit and π phase are trivial. For the (co) multiplication we have:



For the and gate:



Next, we show that $[\![[\![\_]\!]_{\widehat{\mathsf{TOF}}}]\!]_{\mathsf{ZX}\mathscr{E}} = 1$: The ancillae are trivial. For the Toffoli gate:



□

Recall the following proposition:

Proposition 3.4.17. *[14, Prop. 2.6][4] The category* $\mathsf{Span}^{\sim}(\mathsf{FinOrd})$ *equipped with the Cartesian product is monoidally equivalent to the category of (finite) matrices over the natural numbers and the Kronecker product.*

Thus,

Corollary 3.4.18. $\mathsf{ZX}\mathscr{E}$ *is complete for the prop of* $2^n \times 2^m$ *matrices over the natural numbers.*

3.5 Conclusion

There are various other directions which could be pursued. One could also ask if there is a normal form for $\mathsf{ZX}\mathscr{E}$ induced by the presentation in terms of distributive

[4] In [14], they do not prove this equivalence is monoidal, but it is an obvious corollary. They also do not consider the finite case.

laws and monoid maps, using the correspondence between strict factorization systems and distributive laws in spans [54]. It would also be interesting to investigate the 2-categorical structure of ZX&; presenting the corresponding category of relations as a Frobenius theory [10] using the partial order enrichment of TOF.

Another immediate direction would be to add the white π phase to ZX& to obtain an approximately universal graphical calculus for quantum computing using only distributive laws and monoid maps. In such a fragment, one could construct the and gate for the X basis; perhaps expanding the table of distributive laws in Figure 3.4 to be complete for an approximately universal fragment of quantum computing, furthering the general programme of [13, 38] decomposing circuits using distributive laws. This approach is contrasted to considering H-boxes as primitives, as in the phase-free fragment of the ZH-calculus [61]—in ZX&+the white π phase, the unnormalized Hadamard gate is derived. Perhaps proving the minimality of the axioms using this presentation might be easier, although we do not prove minimality in this paper.

It would also be interesting to investigate the connection to the ZH-calculus and triangle fragments of the ZX-calculus; in particular, in regard to natural number labelled H-boxes, as in [37]. These gates can be represented in string diagrams. The diagram of the triangle can be interpreted as the assertion $x \wedge \neg y = \bot$ which is equivalent to the material implication $x \Rightarrow y$.

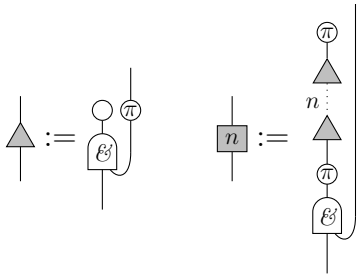
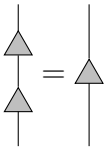


Figure 3.5: Triangles and H-boxes in ZX&, for $n \in \mathbb{N}$.

Therefore, to get a universal and complete graphical calculus for boolean relations, one must simply impose the following equation corresponding to the sequent $(x \Rightarrow y) \wedge (y \Rightarrow z) \vdash (x \Rightarrow z)$:



Chapter 4

Decomposing fragments of the ZX/ZH-calculus

We first review some basic theory involving the presentation of props. These results are mostly folklore, however, I will refer the reader to [65, §2] for a more comprehensive introduction.

Definition 4.0.1. *A* **pro** *is a strict monoidal category generated by one object under the tensor product, and a* **prop** *is a strict* symmetric *monoidal category generated by one object under the tensor product*

Definition 4.0.2. *A* **monoidal theory** *is a pair* (Σ, E) *of* **generators** Σ *and* **equations** E*. Each generator* $f \in \Sigma$ *has a chosen domain* $\mathsf{dom}(f) \in \mathbb{N}$ *and codomain* $\mathsf{cod}(f) \in \mathbb{N}$*, so that* f *can be seen as a map from* $\mathsf{dom}(f)$ *to* $\mathsf{cod}(f)$*.*

The free pro with signature Σ *has maps in* Σ^* *obtained by inductively tensoring all the generators and composing all appropriately typed generators in* Σ*, The equations in* E *are pairs of parallel maps in* Σ^**. Any monoidal theory* (Σ, E) *generates a pro* $\overline{(\Sigma, E)}$ *given by the free pro with signature* Σ *modulo the equations in* E*.*

A **symmetric monoidal theory** *is the symmetric version of a monoidal theory, which generates a prop. Here the set* Σ^* *is obtained by composing and tensoring maps with symmetries, and then quotienting by the axioms of a prop.*

Lemma 4.0.3. *Given two (symmetric) monoidal theories* (Σ_1, E_1) *and* (Σ_2, E_2) *the coproduct of pro(p)s* $\overline{(\Sigma_1, E_1)} + \overline{(\Sigma_2, E_2)}$ *is generated by the (symmetric) monoidal theory* $(\Sigma_1 + \Sigma_2, E_1 + E_2)$*.*

Lemma 4.0.4. *Given three (symmetric) monoidal theories* (Σ_1, E_1)*,* (Σ_2, E_2) *and* (Σ_3, E_3) *where* $\overline{(\Sigma_3, E_3)}$ *is a sub-pro(p) of both* $\overline{(\Sigma_1, E_1)}$ *and* $\overline{(\Sigma_2, E_2)}$*. The pushout of the diagram of pro(p)s*

$$\overline{(\Sigma_1, E_1)} \leftarrow \overline{(\Sigma_3, E_3)} \rightarrow \overline{(\Sigma_2, E_2)}$$

is generated by the (symmetric) monoidal theory $(\Sigma_1^* +_{\Sigma_3} \Sigma_2^*, E_1 + E_2)$*.*

We recall the novel way to compose pro(p), first described in [47]:

Definition 4.0.5. *Suppose there three (symmetric) monoidal theories* (Σ_1, E_1)*,* (Σ_2, E_2) *and* (Σ_3, E_3) *where* $\overline{(\Sigma_3, E_3)}$ *is a sub-pro(p) of both* $\overline{(\Sigma_1, E_1)}$ *and* $\overline{(\Sigma_2, E_2)}$*. A* **distributive law of pro(p)s** *is a distributive law* $\lambda : \overline{(\Sigma_2, E_2)} \otimes_{\overline{(\Sigma_3, E_3)}} \overline{(\Sigma_1, E_1)}$ *in* Mon-Prof*. Informally, this is a way to push all the maps in* Σ_1^* *past those of* Σ_2^* *modulo* Σ_3 *and the equations* $E_1 + E_2$ *and the axioms of a pro(p).*

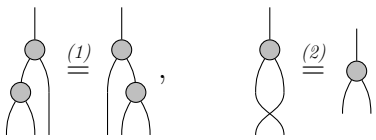
In [47] it is required that $\overline{(\Sigma_3, E_3)}$ is a groupoid; however, we must loosen this requirement (note that when this is not a groupoid, there is no correspondence to factorization systems as in [54]).

Lemma 4.0.6. *Suppose that we have three (symmetric) monoidal theories and a distribtuive law* $\lambda : \overline{(\Sigma_2, E_2)} \otimes_{\overline{(\Sigma_3, E_3)}} \overline{(\Sigma_1, E_1)}$ *as above.*

Then the induced pro(p) $\overline{(\Sigma_2, E_2)} \otimes_{\overline{(\Sigma_3, E_3)}} \overline{(\Sigma_1, E_1)}$ *is presented by the monoidal theory* $(\Sigma_1^* +_{\Sigma_3} \Sigma_2^*, E_1 + E_2 + E_\lambda)$*, where* E_λ *are all the equations needed to push elements of* Σ_1^* *past those of* Σ_2^* *up to* Σ_3^**, dictated by* λ*.*

There is a folklore result that the prop for the free commutative monoid is equivalent to the category of finite sets and functions under the direct sum. The string diagrams correspond to drawing the "graphs" of functions.

Definition 4.0.7. *Let* Inj *be the free prop with one generator of type* $0 \to 1$ *drawn as a black circle; and* Surj *be the prop generated by the free associative commutative binary operationm graphically generated by the following*[1]*:*



Definition 4.0.8. *Let* $\mathsf{Inj}(\mathbb{X})$ *and* $\mathsf{Surj}(\mathbb{X})$ *denote the subcategories of monomorphisms and epimorphisms of* $\mathbb{X}$*.*

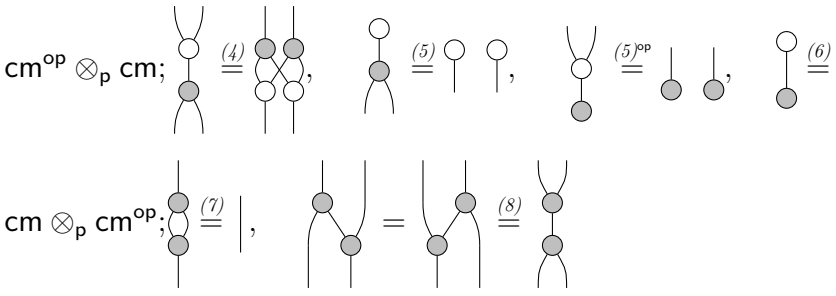
Lemma 4.0.9. *The category* $(\mathsf{Inj}(\mathsf{FinOrd}), +)$ *is presented by the prop* Inj *and* $(\mathsf{Surj}(\mathsf{FinOrd}), +)$ *by the prop* Surj*. Moreover,* $(\mathsf{FinOrd}, +)$ *is presented by the distributive law:*

Yielding the prop for the free commutative monoid, cm*.*

As observed in [12, Ex. 3.3 (a)], this distributive law corresponds to the epi-mono factorization of functions: one can always decompose a function into surjections following by injections by applying this equation multiple times.

Lack showed that the structure of special commutative Frobenius algebras and bicommutative bialgebras arise in terms of distributive laws corresponding to pushout and pullback in $(\mathsf{FinOrd}, +)$ [47, §5.3, 5.4]:

Definition 4.0.10. *Consider the following two distributive laws:*



The former yields, cb*, the prop for the free* **bicommutative bialgebra** *and the latter yields,* scfa*, the prop for the free* **special commutative Frobenius algebra**.

[1]Diagrams are read from bottom to top.

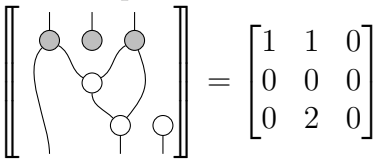
Lemma 4.0.11. *[47, §5.3, 5.4]* cb *is a presentation for* $(\mathsf{Span}(\mathsf{FinOrd}), +)$ *and* scfa *is a presentation for* $(\mathsf{Cospan}(\mathsf{FinOrd}), +)$.

The equations generating these distributive laws give us a recipe for how to generate all pushouts and pullbacks along epics and monics. This category of spans can be seen from a slightly different perspective:

Lemma 4.0.12. *There is an equivalence of props* $\mathsf{cb} \cong (\mathsf{Span}(\mathsf{FinOrd}), +) \cong (\mathsf{Mat}(\mathbb{N}), +)$.

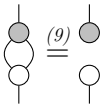
Although we are quite sure that the second equivalence is also folklore, a similar result is given in [14].

One way to see this is by interpreting the monoid as addition and 0 and the comonoid as copying/deleting. For example, consider the interpretation of the following diagram in $\mathsf{cm}^{\mathsf{op}} \otimes_{\mathsf{p}} \mathsf{cm}$ as a matrix:



$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

Definition 4.0.13. *Let* cb_2 *denote the quotient of* cb_2 *by the equation:*



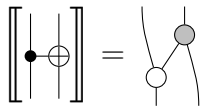
Lemma 4.0.14. cb_2 *is a presentation for the prop* $(\mathsf{Mat}(\mathbb{F}_2), +)$.

Proof. As an Abelian group $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$; which is generated by the equation $2 \equiv 0$, corresponding to this quotient of cb. □

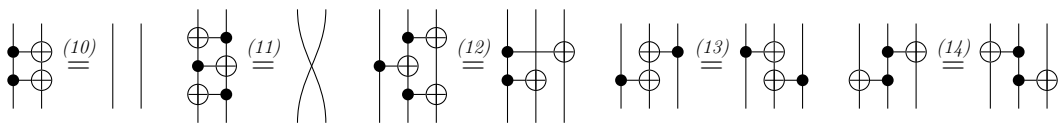
4.1 The phase-free fragment

In this section we build up to giving a presentation for $(\mathsf{Span}(\mathsf{Mat}(\mathbb{F}_2)), +)$ in a modular way. This category is shown to be the same as the phase-free Hadamard free fragment of the ZX-calculus. Although this presentation of linear spans has already been discussed in great detail for arbitrary PIDs [65], our particular method of exposition is necessary to motivate the affine and full cases.

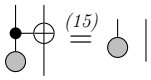
Definition 4.1.1. *Consider the prop* $\mathsf{lso}(\mathsf{cb}_2)$ *generated by the controlled not gate:*



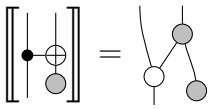
modulo the following relations:



Lemma 4.1.2. *[48, Thm. 6]* $\mathsf{lso}(\mathsf{cb}_2)$ *is a presentation for the prop* $(\mathsf{lso}(\mathsf{Mat}(\mathbb{F}_2), +))$

Definition 4.1.3. *Consider the prop* $\mathsf{Inj}(\mathsf{cb}_2)$ *generated by the coproduct of props* $\mathsf{Iso}(\mathsf{cb}_2) + \mathsf{Inj}$ *modulo the equation:* 

Lemma 4.1.4. *[48, Thm. 7]* $\mathsf{Inj}(\mathsf{cb}_2)$ *is a presentation for the prop* $(\mathsf{Inj}(\mathsf{Mat}(\mathbb{F}_2)), +)$

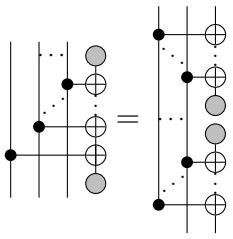
The white comultiplication can be derived in this fragment: 

As a matter of notation, given a category $\mathbb{X}$ with finite limits, we refer to the subcategory of $\mathsf{Span}(\mathbb{X})$ where the left leg is monic as $\mathsf{Par}(\mathbb{X})$, and the subcategory of spans where all legs are monic by $\mathsf{ParIso}(\mathbb{X})$. These two categories, respectively, give semantics for partial maps and partially invertible maps in $\mathbb{X}$ (see [22] for more details).

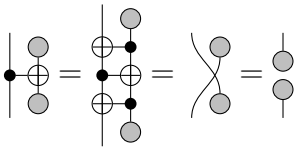
Definition 4.1.5. *Consider the prop* $\mathsf{ParIso}(\mathsf{cb}_2)$ *generated by the distributive law of props:*

$$\mathsf{Inj}(\mathsf{cb}_2)^{\mathsf{op}} \otimes_{\mathsf{Iso}(\mathsf{cb}_2)} \mathsf{Inj}(\mathsf{cb}_2);$$ 

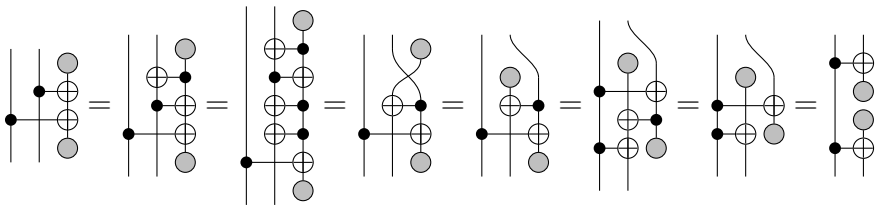
Remark 4.1.6. *This is actually a distributive law because the only only seemingly nontrivial situation arises when controlled not gates are sandwiched by black units/counits on their target wires. However the following identity holds by induction on the number of controlled not gates. For the base case of* $n = 0$*, this follows from the bone law which we added to the distributive law. For* $n > 1$*, we have the following situation:*



For $n = 1$*, that is:*



And for the base case for $n = 2$*:*



The inductive case is essentially the same as the base case for 2.

Lemma 4.1.7. $\mathsf{Parlso}(\mathsf{cb}_2)$ *is a presentation for the prop* $(\mathsf{Parlso}(\mathsf{Mat}(\mathbb{F}_2), +))$.

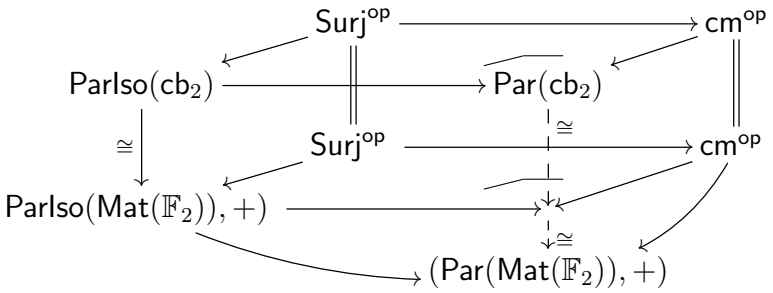
We can get partial maps by freely adding a counit to the nonunital, noncounital special commutative Frobenius algebra:

Definition 4.1.8. *Let* $\mathsf{Par}(\mathsf{cb}_2)$ *denote the pushout of the diagram of props:*

$$\mathsf{Parlso}(\mathsf{cb}_2) \leftarrow \mathsf{Surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Lemma 4.1.9. $\mathsf{Par}(\mathsf{cb}_2)$ *is a presentation for the prop* $(\mathsf{Par}(\mathsf{Mat}(\mathbb{F}_2), +))$.

Proof. One must show that the following diagram commutes:



It doesn't take to much work to show that $\mathsf{Parlso}(\mathsf{cb}_2) \cong \mathsf{Parlso}(\mathsf{Mat}(\mathbb{F}_2))$ is a discrete inverse category (defined in [41, §4.3]). We know that the counital completion of a discrete inverse category is the same as its Cartesian completion from [34, Lem. 3.5]; moreover, the Cartesian completion of $\mathsf{Parlso}(\mathsf{Mat}(\mathbb{F}_2))$ is $\mathsf{Par}(\mathsf{Mat}(\mathbb{F}_2))$. So this diagram commutes as a consequence.

□

This props has a particularly elegant presentation which is given in §**??**.

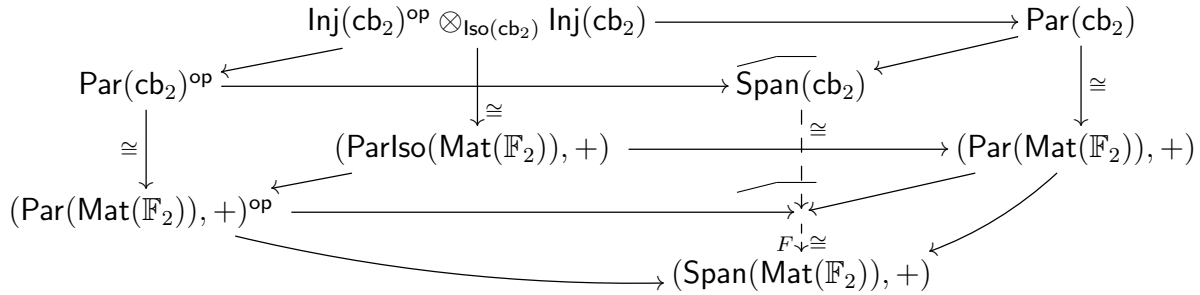
Definition 4.1.10. *Let* $\mathsf{Span}(\mathsf{cb}_2)$ *denote the pushout of the diagram of props:*

$$\mathsf{Par}(\mathsf{cb}_2)^{\mathsf{op}} \leftarrow \mathsf{Parlso}(\mathsf{cb}_2) \rightarrow \mathsf{Par}(\mathsf{cb}_2)$$

The following lemma holds because of [34, Lem. 4.3]:

Lemma 4.1.11. $\mathsf{Span}(\mathsf{cb}_2)$ *is a presentation for the prop* $(\mathsf{Span}(\mathsf{Mat}(\mathbb{F}_2)), +)$.

Proof.

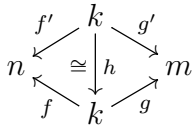


The cube easily commutes. What remains to be shown is that the universal map F is an isomorphism of props. It is clearly the identity on objects, so we just need to show it is full and faithful.

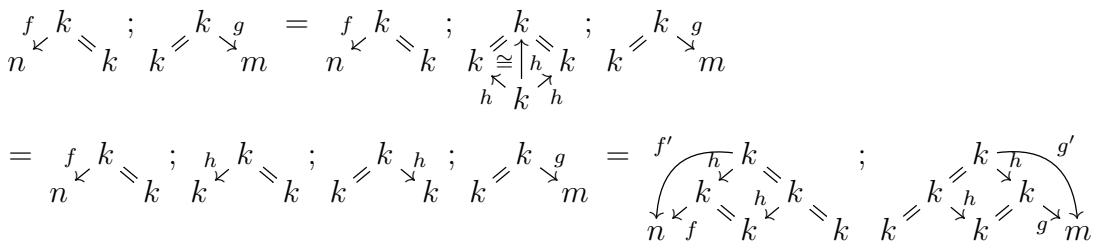
It is clearly full as any span $n \xleftarrow{f} k \xrightarrow{g} m$, we have:

$$F\left((n \xleftarrow{f} k = k); (k = k \xrightarrow{g} m)\right) = n \xleftarrow{f} k \xrightarrow{g} m$$

For faithfulness, we must observe given for any two isomorphic maps in $\mathsf{Span}(\mathsf{Mat}(\mathbb{F}_2))$:



Then in the domain of F, we have:



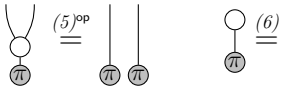
□

Given a PID k, the prop $(\mathsf{Span}(\mathsf{Mat}(k)), +)$ is already known to have a presentation given in terms of "interacting Hopf algebras" [65, Definition 3.13]. This is also the way in which the phase-free fragment of the ZX-calculus would be presented, in terms of two Frobenius algebras corresponding to the Z and X observables, interacting to form Hopf algebras in addition to a few more equations. We have included this presentation in §**??**.

4.2 Additive affine models

Definition 4.2.1. *Consider the prop* Affcb_2 *given by adjoining the following generator to* cb_2

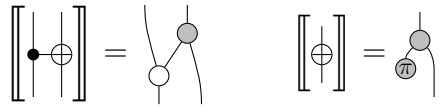
modulo the equations:



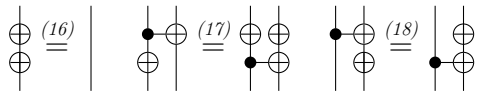
Lemma 4.2.2. *[48, §4]* Affcb_2 *is a presentation for the prop* $(\mathsf{AffMat}(\mathbb{F}_2), +)$.

Note that this assumes that affine matrices are non-empty, as this is a prop. This will become a problem later, when we wish to pull back affine spaces.

Definition 4.2.3. *Consider the prop* $\mathsf{Iso}(\mathsf{Affcb}_2)$ *generated by the controlled not gate, and the not gate (interpreted as matrices):*



Modulo the relations of $\mathsf{Iso}(\mathsf{cb}_2)$ *as well as the additional relations:*



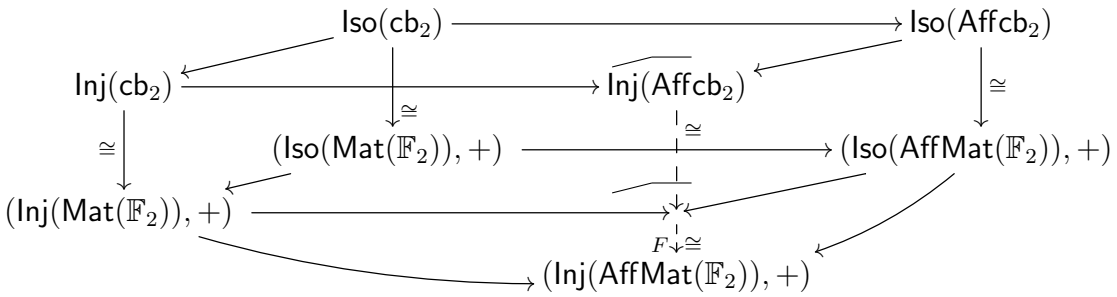
Lemma 4.2.4. *[48, Thm. 11]* $\mathsf{Iso}(\mathsf{Affcb}_2)$ *is a presentation for the prop* $(\mathsf{Iso}(\mathsf{AffMat}(\mathbb{F}_2), +))$.

Definition 4.2.5. *Let* $\mathsf{Inj}(\mathsf{Affcb}_2)$ *denote the pushout of the diagram of props:*

$$\mathsf{Inj}(\mathsf{cb}_2) \leftarrow \mathsf{Iso}(\mathsf{cb}_2) \rightarrow \mathsf{Iso}(\mathsf{Affcb}_2)$$

Lemma 4.2.6. $\mathsf{Inj}(\mathsf{Affcb}_2)$ *is a presentation for the prop* $(\mathsf{Inj}(\mathsf{AffMat}(\mathbb{F}_2)), +)$.

Proof. Consider the following diagram:



The rear and left faces of the cube commute and the vertical maps are all isomorphisms. Therefore, the whole cube commutes via 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, consider any map $n \overset{(A,x)}{\rightarrowtail} m$ in $(\mathsf{Inj}(\mathsf{AffMat}(\mathbb{F}_2)), +)$. Note that this can be factored into:

$$n \overset{(A,0)}{\rightarrowtail} m \underset{\cong}{\overset{(1,x)}{\rightarrow}} m$$

Which lies in the image of F as $m \underset{\cong}{\overset{(1,x)}{\rightarrow}} m$ is an isomorphism.

For faithfulness, we show that every map in $(\mathsf{Iso}(\mathsf{AffMat}(\mathbb{F}_2)), +) +_{(\mathsf{Iso}(\mathsf{Mat}(\mathbb{F}_2)),+)} (\mathsf{Inj}(\mathsf{Mat}(\mathbb{F}_2)), +)$ can be factored uniquely in this way. There are two cases:

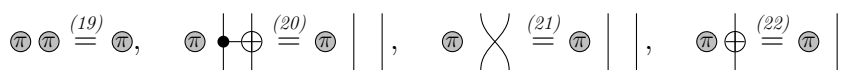
$$\left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,x)}{\rightarrow}} m\right) = \left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,0)}{\rightarrow}} m; m \underset{\cong}{\overset{(1,x)}{\rightarrow}} m\right) = \left(n \overset{A;B}{\rightarrowtail} m \underset{\cong}{\overset{(1,x)}{\rightarrow}} m\right)$$

$$\left(n \overset{(A,x)}{\rightarrowtail} m; m \underset{\cong}{\overset{B}{\to}} m\right) = \left(n \overset{(A,0)}{\rightarrowtail} m; m \underset{\cong}{\overset{(1,x)}{\to}} m; m \underset{\cong}{\overset{B}{\to}} m\right) = \left(n \overset{A}{\rightarrowtail} m; m \underset{\cong}{\overset{(B,B(x))}{\to}} m\right) = \left(n \overset{A;B}{\rightarrowtail} m; m \underset{\cong}{\overset{(1,B(x))}{\to}} m\right)$$

So every map in this pushout has the correct form, which is unique by construction. □

To define partial isomorphisms, we must add a point to the constituent props of the desired distributive law, because the empty set can arise as a subobject by pullback (where the empty set is not properly an object in the prop).

Definition 4.2.7. *Let* $\mathsf{Iso}(\mathsf{Affcb}_2)^{+1}$ *denote the prop obtained by adjoining the following generator to* $\mathsf{Iso}(\mathsf{Affcb}_2)$ $\textcircled{\pi}$ *modulo the equations:*



Lemma 4.2.8. $\mathsf{Iso}(\mathsf{Affcb}_2)^{+1}$ *is a presentation for the subcategory of* $(\mathsf{Span}(\mathsf{AffFdVect}(\mathbb{F}_2)), +)$ *generated by spans* $\mathbb{F}_2^n = \mathbb{F}_2^n \underset{\cong}{\overset{f}{\to}} \mathbb{F}_2^n$ *and* $\mathbb{F}_2^n \overset{?}{\leftarrowtail} \emptyset \overset{?}{\rightarrowtail} \mathbb{F}_2^n$*, for all* $n \in \mathbb{N}$ *and isomorphisms* f*.*

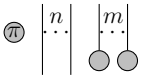
Proof. Identify this new generator with the span $\mathbb{F}_2^0 \leftarrow \emptyset \rightarrow \mathbb{F}_2^0$. If there is a factor of $\textcircled{\pi}$, repeatedly apply these identities from left to right until the diagram corresponding to the identity tensored by $\textcircled{\pi}$ is obtained, which is as a normal form. □

Definition 4.2.9. *Let* $\mathsf{Inj}(\mathsf{Affcb}_2)^{+1}$ *denote the pushout of the diagram of props:*

$$\mathsf{Inj}(\mathsf{Affcb}_2) \leftarrow \mathsf{Iso}(\mathsf{Affcb}_2) \rightarrow \mathsf{Iso}(\mathsf{Affcb}_2)^{+1}$$

Lemma 4.2.10. $\mathsf{Inj}(\mathsf{Affcb}_2)^{+1}$ *is a presentation for the subcategory of* $(\mathsf{Span}(\mathsf{AffFdVect}(\mathbb{F}_2)), +)$ *generated by spans* $\mathbb{F}_2^n = \mathbb{F}_2^n \overset{e}{\rightarrowtail} \mathbb{F}_2^m$ *and* $\mathbb{F}_2^n \overset{?}{\leftarrowtail} \emptyset \overset{?}{\rightarrowtail} \mathbb{F}_2^n$*, for all* $n, m \in \mathbb{N}$ *and monics* e*.*

The proof of this lemma is essentially the same for $\mathsf{Iso}(\mathsf{Affcb}_2)^{+1}$, although diagrams with a factor of $\textcircled{\pi}$ are reduced to the following normal form:

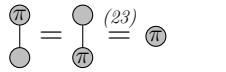


Unlike in the linear case, now we must consider a distributive law over a prop which is not a groupoid: we add a single idempotent corresponding to the empty set to the isomorphisms. To satisfy the requirement that this prop is a sub-prop of the left and right components of the distributive law, we also add this idempotent to the injections and the co-injections:

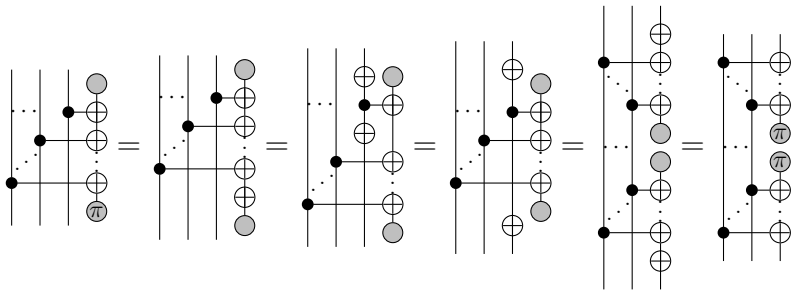
Definition 4.2.11. *Consider the prop* $\mathsf{piAffcb}_2$ *generated by the distributive law of props:*

$$(\mathsf{Inj}(\mathsf{Affcb}_2)^{+1})^{\mathsf{op}} \otimes_{\mathsf{Iso}(\mathsf{Affcb}_2)^{+1}} \mathsf{Inj}(\mathsf{Affcb}_2)^{+1}$$

Given by the equations of $\mathsf{piAffcb}_2$ *as well as:*

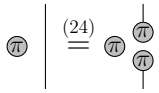


Remark 4.2.12. $(\mathsf{Inj}(\mathsf{Affcb}_2)^{+1})^{\mathsf{op}} \otimes_{\mathsf{Iso}(\mathsf{Affcb}_2)^{+1}} \mathsf{Inj}(\mathsf{Affcb}_2)^{+1}$ *is actually a distributive law because the only only nontrivial situation arises when controlled-not gates are sandwiched between black, or black* π *units/counits on their target wires. The case where there are no controlled not gates in between is resolved by the new axiom we have added. When there are more controlled-not gates, they can be pushed past each other as follows:*



Lemma 4.2.13. $\mathsf{ParIso}(\mathsf{Affcb}_2)$ *is a presentation for the full subcategory* $\mathsf{ParIso}(\mathsf{AffFdVect}(\mathbb{F}_2))^*$ *of* $\mathsf{ParIso}(\mathsf{AffFdVect}(\mathbb{F}_2))$ *where the objects are nonempty affine vector spaces.*

Proof. The obvious functor $\mathsf{ParIso}(\mathsf{Affcb}_2) \to \mathsf{ParIso}(\mathsf{AffFdVect}(\mathbb{F}_2))^*$ is clearly full, as well as an isomorphism on objects. 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 4.1.7. 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. □

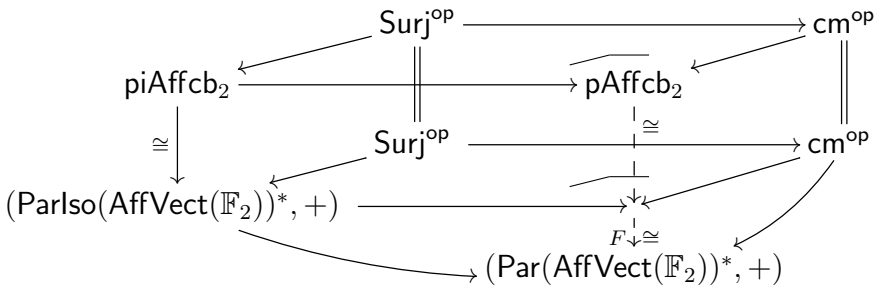
By [23] in this the identities of Definition 4.2.7 can be replaced by the following identity, while maintaining completeness: 

Definition 4.2.14. *Let* pAffcb_2 *denote the pushout of the diagram of props:*

$$\mathsf{piAffcb}_2 \leftarrow \mathsf{Surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Lemma 4.2.15. pAffcb_2 *is a presentation for the prop* $(\mathsf{Par}(\mathsf{AffFdVect}(\mathbb{F}_2))^*, +)$.

Proof.



We know that $\mathsf{piAffcb}_2 \cong \mathsf{ParIso}(\mathsf{AffVect}(\mathbb{F}_2))^*, +)$ is a discrete inverse category by [23, Prop. 3.4].

The cube commutes by the universal property of the pushout, as before.

We just have to show that the universal map F is an isomorphism. It is clearly the identity on objects, so we just have to show it is full and faithful. This follows from essentially the same argument as in the linear case.

□

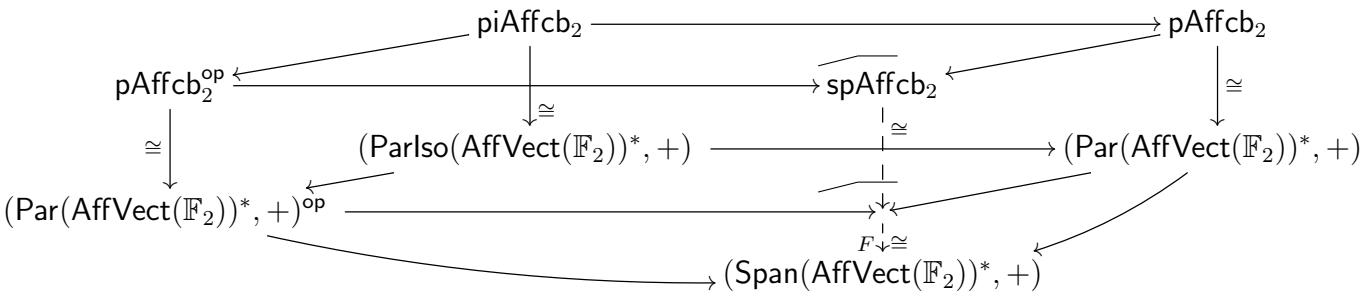
pAffcb_2 has a particularly elegant presentation given in §**??**, which is much more in the spirit of the ZX-calculus.

Definition 4.2.16. *Let* $\mathsf{spAffcb}_2$ *denote the pushout of the diagram of props:*

$$\mathsf{pAffcb}_2^{\mathsf{op}} \leftarrow \mathsf{piAffcb}_2 \rightarrow \mathsf{pAffcb}_2$$

Lemma 4.2.17. $\mathsf{spAffcb}_2$ *is a presentation for the prop* $(\mathsf{Span}(\mathsf{AffFdVect}(\mathbb{F}_2))^*, +)$.

Proof.



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 $(\mathsf{Span}(\mathsf{AffVect}(\mathbb{F}_2))^*, +)$. 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 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 $(\mathsf{Span}(\mathsf{AffVect}(\mathbb{F}_2))^*, +)$ with nonempty apex by the same argument as in Lemma 4.1.11. 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.

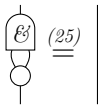
□

There is a particularly elegant equivalent presentation given in §??. This is almost equivalent to the presentation given in [11] which gives a presentation for the full subcategory of relations of finite dimensional affine vector spaces where the objects are given by the nonempty vector spaces, and is much more in the spirit of the ZX-calculus.

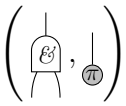
4.3 The and gate

Recall that unlike when the tensor product is the coproduct; when the tensor product is induced by the multiplication, to obtain a prop, one must consider the subcategory generated by tensoring a fixed object with itsef.

Definition 4.3.1. *Let $L_{\mathbb{F}_2^\times}$ be the prop generated by quotienting* cb *by the equation:*



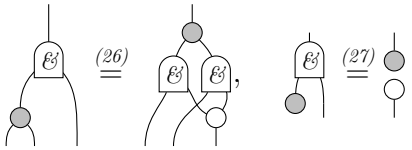
Where the components of the monoid are relabled as follows:



Lemma 4.3.2. *$L^\times_{\mathbb{F}_2}$ is a presentation for the Lawvere theory for the group of units of the field $\mathbb{F}_2$.*

Definition 4.3.3. *Consider the prop f_2, generated by the distributive law:*

$L_{\mathbb{F}_2^\times} \otimes_{\mathsf{cm}^{\mathsf{op}}} \mathsf{cb}_2;$

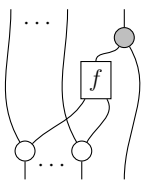


Lemma 4.3.4. *[48, Thm. 10] f_2 is a presentation for the prop $(\mathsf{FinOrd}_2, \times)$.*

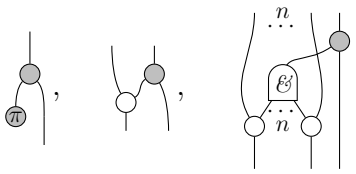
Therefore in some sense, we are justified in thinking of this prop $(\mathsf{FinOrd}_2, \times)$ as a sort of categorification of boolean polynomials.

To find larger fragments, it will be useful to first identify the isomorphisms and the monics of f_2.

Definition 4.3.5. *Given a map f in f_2, the* **oracle** *for f, $\mathcal{O}_f$ is defined as follows:*



Lemma 4.3.6. *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 $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots x_1^2 - x_1\rangle$. Every polynomial in this quotient ring has a unique normal form given by sums of products (which is not true for arbitrary finite fields). Each product corresponds to a generalized controlled-not gate, and the sum corresponds to composing these generalized controlled-not gates in sequence. □

In the quantum circuit notation the generalized controlled-not gates are drawn as follows (the first being the not gate, and the second being the controlled-not gate):

Lemma 4.3.7. *[60, Thm. 5.1] The prop generated by the oracles in* f_2 *generate* $\mathsf{Iso}(\mathsf{f}_2)$.

Denote a generalized controlled not gate controlled by wires indexed by X, operating on x by $\{X, x\}$

Iwama et al [46] originally gave a complete set of identities for circuits generated by generalized controlled not gates where the value of all-but-one output wires are fixed. It is worth mentioning that Shende et al. later used the commutator to generalize some of these identities [56, Cor. 26]. We conjecture that a very similar set of identities is complete for Boolean isomorphisms:

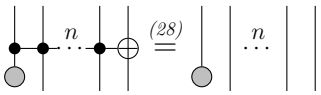
Conjecture 4.3.8. *Let* $\mathsf{Iso}(\mathsf{FinOrd}_2)$ *denote the prop generated by all generalized controlled-not gates modulo the following identities:*

- $\{X, x\}\{X, x\} = 1$
- *If* $x \notin Y$ *and* $y \notin X$ *then* $\{X, x\}\{Y, y\} = \{Y, y\}\{X, x\}$.
- *If* $x \notin Y$, *then* $\{X, x\}\{\{x\} \sqcup Y, y\} = \{X \cup Y, y\}\{\{x\} \sqcup Y, y\}\{X, x\}$.
- *If* $x \notin Y$, *then* $\{\{x\} \sqcup Y, y\}\{X, x\} = \{X, x\}\{\{x\} \sqcup Y, y\}\{X \cup Y, y\}$.
- *If* $x \in Y$ *and* $y \in X$, *then* $\{X, x\}\{Y, y\}\{X, x\} = \{Y, y\}\{X, x\}\{Y, y\}$.

Note that the symmetry is derived in this fragment by composing 3 controlled not gates, as in Definition . The axioms of a prop are derived, so we are justified in calling $\mathsf{Iso}(\mathsf{f}_2)$ a prop.

Although we aren't sure if these identities are complete, it doesn't matter in the end. With each generator we add, we add new enough identities to give a complete presentation, given that there is a complete presentation for $\mathsf{Iso}(\mathsf{f}_2)$. However, eventually once we add enough generators and identities, we get a finite, complete presentation.

Definition 4.3.9. *Let* $\mathsf{Inj}(\mathsf{f}_2)$ *be the prop given by adjoining the black unit to* $\mathsf{Iso}(\mathsf{f}_2)$ *modulo:*



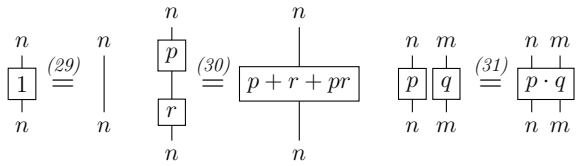
Lemma 4.3.10. $\mathsf{Inj}(\mathsf{f}_2)$ *is a presentation for the prop* $(\mathsf{Inj}(\mathsf{FinOrd}_2), \times)$.

The pushout of a diagram of sets and functions $2^n \hookleftarrow 2^k \hookrightarrow 2^m$ is not always a power of 2. Therefore, one should not expect to construct categories of partial isomorphisms via a distributive law of on $\mathsf{Inj}(\mathsf{f}_2) \otimes_{\mathsf{Iso}(\mathsf{f}_2)} \mathsf{Inj}(\mathsf{f}_2)^{\mathsf{op}}$. Instead one must add all of the nontrivial subobjects to the constituent props forming the distributive law; as opposed to the affine case, there are more than one such subobjects which arise in this way.

Definition 4.3.11. *Consider the pro* sub_2 *generated by endomorphisms such that for any* n, $\mathsf{sub}_2(n, n)$ *is the set described by all* n*-variable polynomials over* $\mathbb{F}_2$*. Denote such a generator by a box with* n *inputs and* n *outputs labelled by the corresponding polynomial.*

We require that the following equations hold so that

$$\forall n, m \in \mathbb{N}, p, r \in \mathbb{F}_2[x_1, \ldots, x_n], q \in \mathbb{F}_2[x_{n+1}, \ldots, x_{n+m}] :$$



As well as, for all n*, the equations of the quotient rings* $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$.

Lemma 4.3.12. sub_2 *is a presentation for the pro of symmetric spans of monic functions, ie spans of the following form* $2^n \xleftarrow{e} k \xrightarrow{e} 2^n$*, for all* $n, k \in \mathbb{N}$ *and monics* e*.*

Proof. Each polynomial $p \in \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$ corresponds to a function $\mathsf{ev}_p : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by evaluation. Let $k = |\mathsf{ev}^{-1}(1)|$, then there chose a function $f_p : k \rightarrowtail 2^n$ picking out all the solutions which evaluate to 1. The functor from sub_2 to this subcategory spans takes polynomials $p \mapsto (2^n \xleftarrow{f_p} k \xrightarrow{f_p} 2^n)$. Any two two spans induced by the same polynomial are isomorphic, so this is actually well defined. It is clearly an isomorphism on objects, and it can easily be shown to be a monoidal functor.

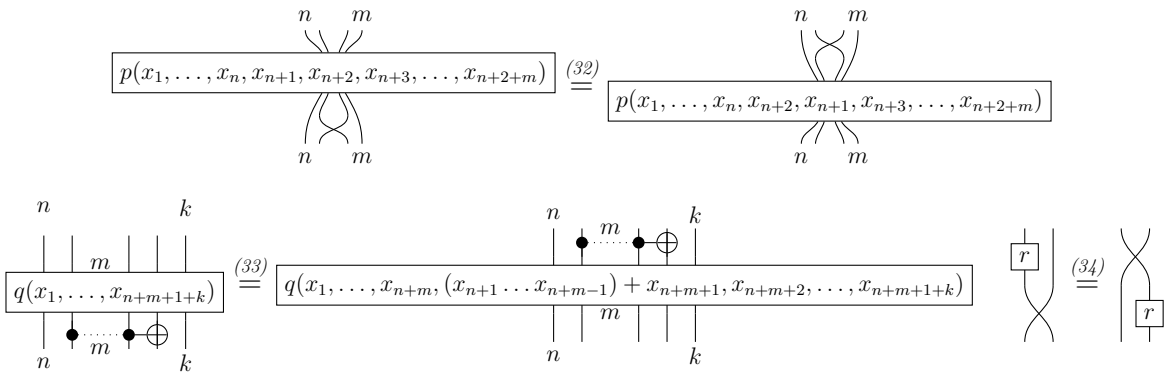
The fullness is easy and the faithfulness comes from the fact that we can reduce every map to a polynomial and then reduce the polynomial to algebraic normal form.

□

Definition 4.3.13. *Let* $\mathsf{sublsof}_2$ *be the prop generated by a distributive law of pros:*

$$\mathsf{sub}_2 \otimes \mathsf{Iso}(\mathsf{f}_2);$$

$$\forall n, m, k \in \mathbb{N}, \forall p \in \mathbb{F}_2[x_1, \ldots, x_{n+2+m}], q \in \mathbb{F}_2[x_1, \ldots, x_{n+m+1+k}], r \in \mathbb{F}_2[x_1, \ldots, x_n] :$$

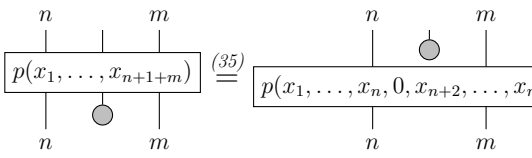


Lemma 4.3.14. $\mathsf{sublsof}_2$ *is a presentation for the subcategory of* $(\mathsf{Span}(\mathsf{FinOrd}), \times)$ *generated by spans of the form* $2^n \xleftarrow{e} k \xrightarrow{e} 2^m \xrightarrow[\cong]{f} 2^m$*, for all* $n, mk \in \mathbb{N}$ *and all isomorphisms* f *and monics* e*.*

Proof. The obvious functor is clearly monoidal. Moreover, it is full by construction. For the faithfulness, take two maps f and g in $\mathsf{sublsof}_2$. Then one can just push everything to the end and then use the decidability of equality on both factors of the distributive law to show that they are equal. □

Definition 4.3.15. *Consider the prop* $\mathsf{sublnjf}_2$ *generated by a distributive law of props:*

$\mathsf{sublsof}_2 \otimes_{\mathsf{Iso}(\mathsf{f}_2)} \mathsf{Inj}(\mathsf{f}_2); \forall n, m \in \mathbb{N}, p \in \mathbb{F}_2[x_1, \ldots, x_{n+1+m}] :$

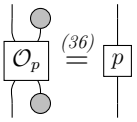


Lemma 4.3.16. $\mathsf{sublnjf}_2$ *is a presentation for the subcategory of* $(\mathsf{Span}(\mathsf{FinOrd}), \times)$ *generated by spans of the form* $2^n \xleftarrow{e} k \xrightarrow{e} 2^n \xrightarrow{e'} 2^m$ *for all* $n, m, k \in \mathbb{N}$ *and all monics* e, e'*.*

The proof is completely analogous to as in the case of subif_2.

Any n variable polynomial p can be interpreted as a span of monics via the oracle $\mathcal{O}_p$, where the value of the target wire is restricted to have the value 0. Each such polynomial corresponds to a subobject, which complicates the matter further than in the affine case.

Definition 4.3.17. *Consider the prop* pif_2 *given by the distributive law of props:*

$\mathsf{subInjf}_2^{\mathsf{op}} \otimes_{\mathsf{subIsof}_2} \mathsf{subInjf}_2;$  $\overset{(36)}{=}$

Lemma 4.3.18. pif_2 *is a presentation for the full subcategory* $(\mathsf{FPinj}_2, \times)$ *of* $(\mathsf{ParIso}(\mathsf{FinOrd}), \times)$ *with objects powers of two.*

Unlike the previous lemmas, this is not dependant on a complete presentation for the isomorphisms. The proof is a consequence of [32, Thm 7.6.14] where they give a finite, complete presentation for this category. The identities up to this point are equivalent to this finite presentation, whether or not the conjectured presentation for the isomorphisms is complete.

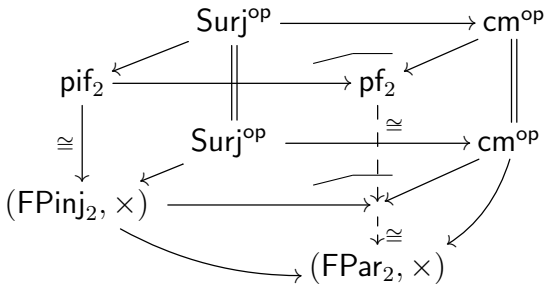
pif_2 can be presented in terms of finitely many generators and relations. The identities are contained in §**??**.

Definition 4.3.19. *Consider the prop* pf_2 *given by the pushout of the following diagram of props, given by adding a counit to the diagonal map:*

$$\mathsf{pif}_2 \leftarrow \mathsf{Surj}^{\mathsf{op}} \rightarrow \mathsf{cm}^{\mathsf{op}}$$

Lemma 4.3.20. pf_2 *is a presentation for the the full subcategory* $(\mathsf{FPar}_2, \times)$ *of* $(\mathsf{Par}(\mathsf{FinOrd}), \times)$ *with objects powers of two.*

Proof. One has to show that the following diagram commutes:



Again, the proof is essentially the same as for the linear and affine cases; the only difference being that the Cartesian completion of FPinj_2 is FPar_2.

□

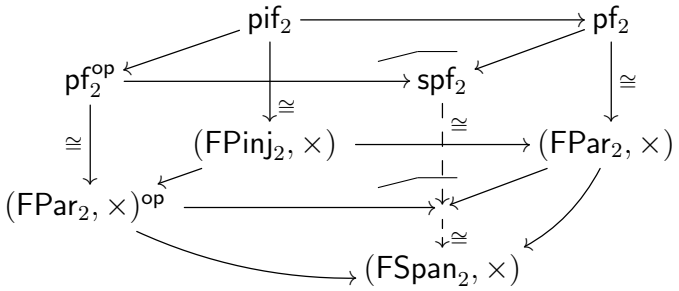
There is a particularly elegant finite presentation contained in §**??**, which is much more ZX-flavoured.

Definition 4.3.21. *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 4.3.22. *[34]* spf_2 *is a presentation for the full subcategory* $(\mathsf{FSpan}_2, \times)$ *of* $(\mathsf{Span}(\mathsf{FinOrd}), \times)$ *with objects powers of two.*

Proof. One has to show that the following diagram commutes:

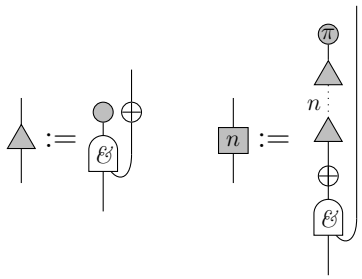


This follows from [34, Lem. 4.3].

□

There is a particularly elegant finite presentation contained in §**??**, which is much more ZX-flavoured, dubbed $\mathsf{ZX}\mathscr{C}$. Based on a similar observation to one made in [14], the author of [34] remarks that this category is equivalent as a prop to the full subcategory of natural number matrices where the objects are powers of 2.

As remarked in [34], this category is equivalent to the "natural number H-box fragment" of the ZH-calculus. That is to say, the prop generated by the Z and X spiders (coresponding to (co)copying and (co)addition) along with H-boxes which have values restricted to be natural numbers. The interpretation of these H-boxes is given in [34, Fig. 5], which we restate for reference:



Note that arbitrary arity H-boxes can be obtained by composition with and gates.

4.4 Conclusion and future work

In this paper, we have devised a method to give modular presentations for full subcategories of categories of spans; albeit, this method is proven to work in full generality. In all three cases we we have considered, there is a fully faithful symmetric monoidal functor $F : \mathbb{X} \to \mathbb{Y}$ between a prop $\mathbb{X}$ and a symmetric monoidal category $\mathbb{Y}$. And

the categories which we eventually build up to are the full subcategories of $\mathsf{Span}(\mathbb{Y})$ with objects in $F(\mathbb{X})$. In other words, these are structured span categories ${}_F\mathsf{Span}(\mathbb{Y})$, as considered in [6] (or structure cospan categories ${}_{F^{\mathsf{op}}}\mathsf{Cospan}(\mathbb{Y}^{\mathsf{op}})$). We build up to ${}_F\mathsf{Span}(\mathbb{Y})$ first by presenting the isos and monics in $\mathbb{Y}$ in terms of a symmetric monoidal theory. Then we consider the subcategory of ${}_F\mathsf{Span}(\mathbb{Y})$ generated by monic spans spans of the form $FX \xleftarrow{e} Y \xrightarrow{e} FX$, corresponding to the new subobjects created in pullback of maps in $F(\mathbb{X})$: presenting these as monoidal theories. Then we add these subobjects to the isos and monos by distributive law and again present these in terms of symmetric monoidal theories. After doing so, we are able to construct a distributive law between the monics and co-monics in ${}_F\mathsf{Span}(\mathbb{Y})$ up to isomorphisms with subobjects adjoined to all three props (this is a crucial step because in the non-linear case, not all pullbacks exist, so one can not construct a distributive law over the isomorphisms). We then observe that the prop generated by such a distributive law is a discrete inverse category (as defined in [41, Def. 4.3.1]), thus one can complete it to a discrete Cartesian restriction category by adding counits to the codiagonal map (as observed in [34, Lem. 3.5]). Finally, one can glue together the discrete inverse category to its opposite category up to the shared discrete inverse category to obtain ${}_F\mathsf{Span}(\mathbb{Y})$.

This method is quite generic, and it would be useful to establish some criteria for when it can be applied categories of structured spans. There are various ways in which this method could potentially be employed to give a modular presentation of such a category of structured spans. Possibly the easiest such class of examples would be that given by the functor $(\mathsf{AffMat}(k), +) \to (\mathsf{AffVect}(k), +)$, for an arbitrary field (or maybe even PID k). More difficult, would be the class of examples given by $\mathsf{FinOrd}_p \to (\mathsf{FinOrd}, \times)$, for arbitrary prime $p > 2$. As opposed to in the case of $p = 2$, the presentation for the prop of subobjects would be less simple; only in this case can systems of multivariate polynomials always be reduced to a single polynomial. To produce a normal form in the more general case, we expect that one would have to employ the use of Gröbner bases. Another model which one could pursue is that given by the functor from free, finitely generated commutative semigroups to additive monoids. A presentation is given for the corresponding category of relations in [50, §3.3]; however, it is not given a modular treatment. This would potentially be useful because of applications in concurrency theory.

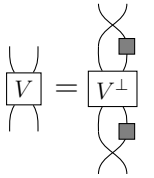
Other directions would be to try to add more phases in a modular fashion. Perhaps the work of [38] could help add more phases to this picture in a modular fashion.

Chapter 5

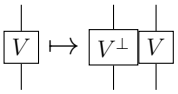
Relational semantics for stabilizer circuits

Linear Lagrangian relations, or more generally, affine Lagrangian relations provide a rich, compositional setting for modelling the evolutions of various physical systems. For example, certain classes of electrical circuits can be interpreted in terms of Lagrangian relations over the field of real rational functions [9, 11]. On a quite different note, the state preparation and quantum evolution of p-dimensional generalizations of Spekkens' toy theory [59] and (consequently) odd-prime-dimensional stabilizer quantum theory [42] have semantics in terms of affine Lagrangian relations over $\mathbb{F}_p$. Specifically, the state preparation corresponds to the affine Lagrangian relations from the tensor unit, and the evolution corresponds to affine symplectomorphisms. In this paper we extend this correspondance to the full category of Lagrangian relations, giving these circuits a proper categorical treatment.

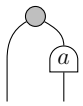
Formally, the category of Lagrangian relations is the symmetric monoidal subcategory of linear relations where the objects are symplectic vector spaces and the morphisms are linear relations satisfying an extra condition which can be captured graphically as the following, where $V^\perp$ denotes the orthogonal complement and the grey box denotes the *antipode* from the graphical theory of linear relations:



We show that any linear relation V determines a Lagrangian relation in terms of 'doubling', i.e. taking the tensor product of a linear relation with its complement:



By analogy to the CPM construction for the category of completely positive maps, we call these *pure* Lagrangian relations. In Theorem 5.3.2 we show that only one more class of 'discard' generators d_a for each a in the underlying field k is required to generate all Lagrangian relations.

$d_a :=$ 

From this, we immediately obtain a complete graphical calculus for Lagrangian relations over any field k, namely we can apply the complete calculus ih_k for linear relations [13] to diagrams built from pure morphisms and discard maps. This extends the doubled presentation of bond graphs, given in [35, 5.3], which are not universal for Lagrangian relations, and is instead only universal for a fragment of the pure morphisms. In Corollary 5.3.3, we also immediately get a *purification theorem* for Lagrangian relations, much like the purification (a.k.a. Stinespring dilation) of quantum channels which can be proven straightforwardly in the CPM construction over Hilbert spaces.

Furthermore, in the case of prime fields, i.e. finite fields $\mathbb{F}_p$ for p, we show in Corollary 5.3.4 that this is actually an instance of the original CPM construction, for a suitably defined dagger on the category of linear relations.

In Section 5.4 we show that only one more generator is needed to obtain *affine* Lagrangian relations. In the case of odd prime fields, we show in Theorem 5.4.16 that affine Lagrangian relations are prime-dimensional qudit stabilizer circuits, modulo invertible scalars. This give a graphical calculus extends to previous work on the qubit [4], and qutrit [62] cases. We also discuss the relation to electrical circuits.

Related work. It was previously shown that certain classes of electrical circuits have a semantics in terms of affine Lagrangian relations over the field of the real numbers and the real rational functions $\mathbb{R}[x, y]/\langle xy - 1\rangle$ [7, 9]. Similarly in [11, §VI], the authors give an interpretation of non-passive electrical circuits in terms of these 'doubled' string diagrams for affine relations over the real rational functions, however the authors did not give a full characterisation for the category of Lagrangian relations in terms of diagrammatic generators. We restate the interpretations of the electrical components given in [11, §VI] in terms of the graphical calculus for affine Lagrangian relations in Example 5.4.7.

A presentation of odd-prime stabilizer theory in terms of affine symplectomorphisms applied to Lagrangian subspaces appears in [42] and several follow-on works relating stabilizer theory to classical phase space via the discrete Wigner function. Our Theorem 5.4.16 is a categorical reformulation of the result of Spekkens' in which he shows that so called odd-prime-dimensional 'quadrature epistricted theories' are operationally equivalent to prime-dimensional qudit stabilizer circuits [59]; following earlier work in [58]. This operational equivalence has also been further explored in the non-prime case [18]. Note that operational equivalence is not the same as categorical equivalence. The notion of operational equivalence used in [59, 18] refers to the equivalence of protocols in which circuits are prepared, evolve and then are measured; whereas ours is more 'process-theoretic', i.e. we consider the category that contains states, effects, evolutions, and all possible compositions thereof. A complete presentation for Spekkens' qubit toy model in terms of a category of relations has also been given [4] following the categorical description by [25]. However, the authors do not explicitly establish that this is the category of affine Lagrangian relations over $\mathbb{F}_2$, but merely a subcategory of finite sets and relations. There is also a complete presentation for qutrit stabilizer theory [62] which, by Theorem 5.4.16, is equivalent to Spekkens' qutrit toy model, up to scalars; the connection to relations, in this case, being unexplored.

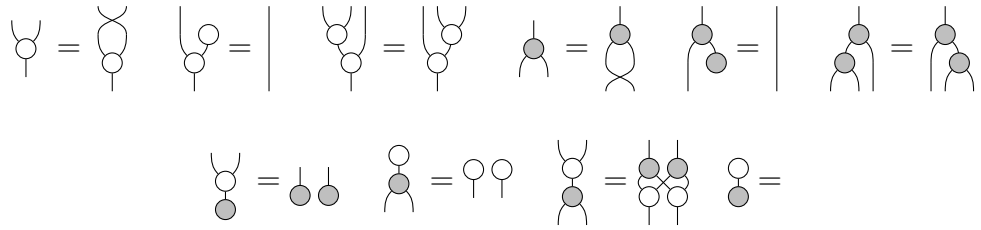
5.1 Linear relations

In order to decribe Lagrangian relations diagramatically, we must first recall the symmetric monoidal theory of linear relations. To do so, we first recall the symmetric

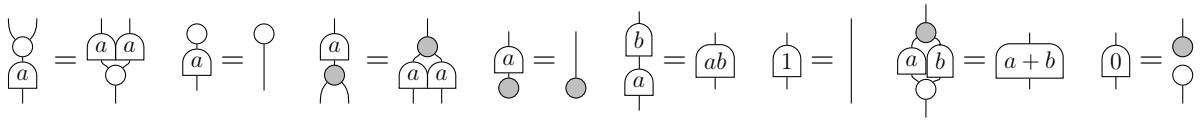
monoidal theory of matrices:

Definition 5.1.1. *[65, Defn. 3.4] Given a ring k, let cb_k denote the prop given by the generators*[1]*:*

modulo the equations of a bicommutative bialgebra:



and the additional equations:



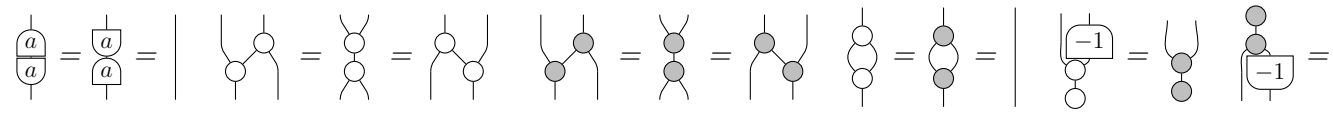
Proposition 5.1.2. *[65, Prop. 3.9] Given a ring k, cb_k is a presentation for the prop Mat_k, of matrices over k under the direct sum.*

One should interpret the grey monoid as addition and the white comonoid as copying.

Definition 5.1.3. *[65, Defn. 3.42] Given a field k, the prop of* **linear relations**, LinRel_k*, has morphisms $n \to m$ as linear subspaces of $k^n \oplus k^m$, under relational composition and the direct sum as the tensor product.*

It is only necessary for k to be a principle ideal domain for composition to be well defined, but a field will do for the purposes of this paper.

Definition 5.1.4. *[65, Defn. 3.44] Given a field k, let ih_k denote the prop given by the quotient of the coproduct of props $\mathsf{cb}_k^{\mathsf{op}} + \mathsf{cb}_k$ by the following equations, for all invertible $a \in k$ (where the generators of $\mathsf{cb}_k^{\mathsf{op}}$ are drawn by reflecting those of cb_k along the x-axis):*



Theorem 5.1.5. *[65, Thm. 3.49] ih_k is a presentation for LinRel_k.*

There is an interesting folklore result which was remarked in [33] [2]:

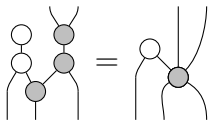
[1] We use the ZX-style colouring which is dual to that used in [65].

[2] One should note that the black box is the antipode, *not* the Fourier transform/Hadamard gate.

Lemma 5.1.6. *For a prime number p, $\mathsf{ih}_{\mathbb{F}_p}$ is a presentation for the phase-free, Fourier-free p-dimensional qudit ZX-calculus, modulo invertible scalars.*

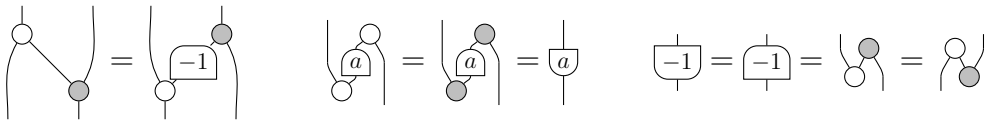
The following theorem will be useful for graphical manipulations:

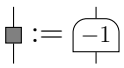
Theorem 5.1.7. *[2] (Spider Theorem) All connected components of special commutative Frobenius algebras with the same arity are equal.*

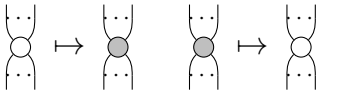
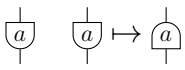
That is to say, we can unambiguously refer to these connected components by spiders. In ih_k, there are two spiders, so for example we can apply spider fusion to the following circuit: 

We shall use the following results:

Lemma 5.1.8. *[65, (D4)] [8, p. 4] [65, (D3)]*



Because of the symmetry of -1, we use the following (symmetric) notation for the antipode: 

Lemma 5.1.9. *[57] The functor $(\_)^\perp : \mathsf{ih}_k \to \mathsf{ih}_k$;*  

is the isomorphism which takes linear subspaces to their orthogonal complement, that is to say:

$$V \mapsto V^\perp := \{v \in V : \forall w \in V, \langle v, w\rangle = 0\}$$

Notice that the orthogonal complement is an involution so that $(V^\perp)^\perp = V$.

5.2 Lagrangian relations

Now that we have a graphical presentation of linear relations, we can now do same for (linear) Lagrangian relations. We first recall some of the basic theory of symplectic vector spaces. This is expounded upon in much greater generality in the not-necessarily-linear case in [64]. In this entire paper, we only care about the linear and affine cases; and things will assumed to be linear unless otherwise stated. As

previously mentioned, Lagrangian relations (and their affine counterpart) have previously been studied within the context of monoidal categories to model electrical circuits among other things [9, 7, 35]; although, to the knowledge of the authors, no proof of universality exists in the literature.

Definition 5.2.1. *Given a field k and a 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:** *if* $\exists v \in V \forall w \in V : \omega(v, w) = 0$, *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 5.2.2. *Every vector space k^{2n} is equipped with a bilinear form given by the following block matrix:*

$$\omega := \begin{bmatrix} 0_n & I_n \\ -I_n & 0_n \end{bmatrix}$$

so that $\omega(v, w) := v\omega w^T$. Moreover, every finite dimensional symplectic vector space over k is symplectomorphic to one of the form k^{2n} with such a symplectic form.

Definition 5.2.3. *Let $W \subseteq V$ be a linear subspace of a symplectic space V. The* **symplectic dual** *of the subspace W is defined to be $W^\omega := \{v \in V : \forall w \in W, \omega(v, w) = 0\}$. 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 $W^\omega = W$.*

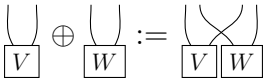
Lemma 5.2.4. *Every symplectomorphism $f : V \to V$ induces a Lagrangian relation $\Gamma_f := \{(fv, v) | v \in V\}$.*

These spaces have a natural grading into two distinct parts $V \oplus W \subseteq k^n \oplus k^n$. By analogy to the case of quantum stabilizer theory, we call the left part the *X-grading* and the right part the *Z-grading*.

As a matter of convention, we consider linear subspaces as being represented as the row space of a matrix. So in particular, a symplectic subspace of k^{2n} is represented by a matrix of the form $[X|Z]$ where X, Z are both $n \times n$-dimensional matrices. An isotropic subspace can equivalently be described as a matrix $[X|Z]$ so that $[X|Z]\omega[X|Z]^T = 0$. Moreover, a Lagrangian subspace can be described as a matrix as above which additionally has rank n.

Definition 5.2.5. *Given a field k, the prop of* **Lagrangian relations**, LagRel_k *has morphisms $k^{2n} \to k^{2m}$ as Lagrangian subspaces of the symplectic vector space $k^{n+m} \oplus k^{n+m}$ with symplectic form given above. Composition is given by relational composition and the tensor product is given by the direct sum.*

The direct sum of Lagrangian subspaces is graphically depicted as follows:



Where we are grouping the X gradings together on the left and the Z gradings together on the right. Note that this means the embedding of LagRel_k into $\mathsf{LinRel}_\mathsf{k}$ preserves the monoidal product only up to isomorphism. More precisely, we have the following fact.

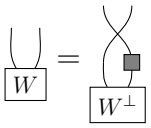
Lemma 5.2.6. *The forgetful functor $E : \mathsf{LagRel}_k \to \mathsf{LinRel}_\mathsf{k}$ is a faithful, strong symmetric monoidal.*

Proof. Functoriality and faithfulness is immediate. The strong monoidal structure is given by $E(I) = I$ and

$$E(A) \oplus E(B) := A \oplus A \oplus B \oplus B \xrightarrow{1\oplus\sigma\oplus 1} A \oplus B \oplus A \oplus B =: E(A \oplus B).$$

The symmetric monoidal structure on LagRel_k is chosen such that it is consistent with the monoidal structure above. □

Due to the above lemma, we will regard LagRel_k as a symmetric monoidal subcategory of $\mathsf{LinRel}_\mathsf{k}$. As such, we can ask what the generators of LagRel_k look like in terms of string diagrams of ih_k generators. We first describe what it means to be a Lagrangian relation in pictures, where the X block is the wire on the left and Z block is the wire on the right:

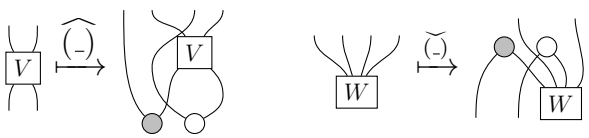


(5.1)

Algebraically, for W a subspace of V, the right hand side is interpreted as follows:

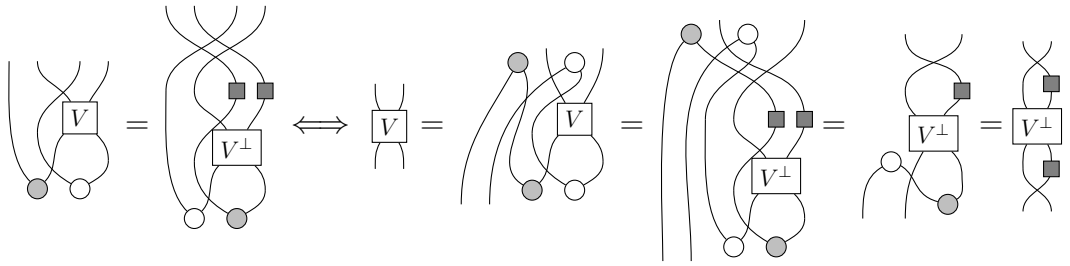
$$\begin{aligned} W^\omega :&= \{(v_1, v_2) \in V : \forall (w_1, w_2) \in W, \omega((v_1, v_2), (w_1, w_2)) = 0\} \\ &= \{(v_1, v_2) \in V : \forall (w_1, w_2) \in W, \langle (v_2, -v_1), (w_1, w_2)\rangle = 0\} \\ &= \{(v_2, -v_1) \in V : \forall (w_1, w_2) \in W, \langle (v_1, v_2), (w_1, w_2)\rangle = 0\} \end{aligned}$$

The category of Lagrangian relations is compact closed. Given a relation V between symplectic vector spaces, we can curry it into a state $\widehat{V}$; and similarily, we can uncurry a state W into a process $\widetilde{W}$,



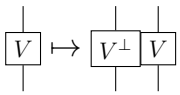
It is easy to see that these two constructions are inverse to each other. This allows us to derive a graphical criteria for abitrary Lagrangian relations, generalizing Equation

5.1:

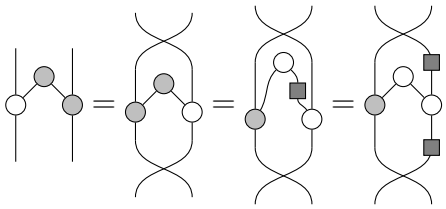


For this reason, we will depict Lagrangian relations as processes, where the input wires are on the bottom and output wires on on the top.

Lemma 5.2.7. *There is a faithful, strong symmetric monoidal functor* $L : \mathsf{LinRel}_{\mathsf{k}} \to \mathsf{LagRel}_{\mathsf{k}}$ *given by the following action on the generators of* ih_k*; doubling, and then changing the colours of one of the copies:*



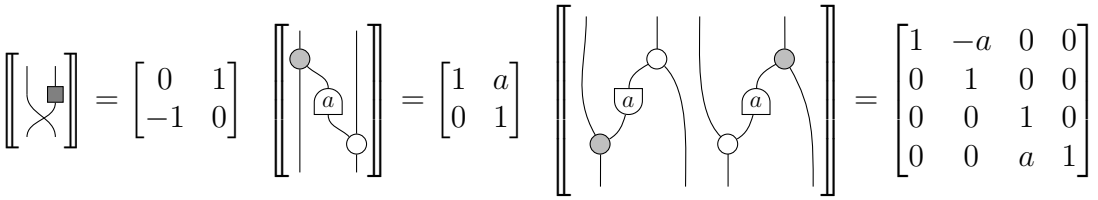
To check this is a functor, all we have to show is that it produces Lagrangian relations. This follows immediately from the naturality of -1. This functor is symmetric monoidal and faithful but not full, as for example, the following Lagrangian relation is not in the image of L:



5.3 Generators for Lagrangian relations

In this section, we shall give a universal set of generators for LagRel_k; although, we do not directly give a complete set of identities. Instead we defer to the completeness of the underlying category $\mathsf{ih}_k \cong \mathsf{LinRel}_{\mathsf{k}}$.

Consider the following symplectomorphisms; the discrete Fourier transform F, the a-shift gate S_a and the controlled-a gate 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 targetting wire j.

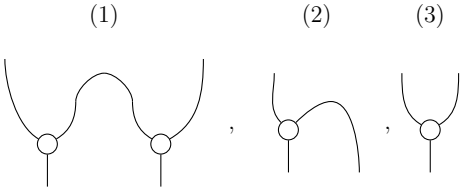
Note the right action of these gates in terms of matrix multiplication of Lagrangian subspaces for any nonzero $a \in k$ (as observed in [1, p. 4]):

- $F^{(i)}$ 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, we have:

Theorem 5.3.1. *For any field k the maps in $L(\mathsf{LinRel}_k)$ as well as F and S_a for all $a \in k$ generate LagRel_k.*

Proof. Consider the matrix $[X|Z]$ of an arbitrary Lagrangian relation over field k seen as a state. We show how one can reduce $[X|Z]$ to the block matrix $[I|0]$ by right multiplication with the aforementioned symplectomorphisms. To do so, we first reduce it to a matrix $[I|Z']$ by only applying row operations (keeping the subspace the same) as well as the Fourier transform. This involve repeatedly do Gaussian elimination and then applying the Fourier transform to wires when the pivot is in the Z block. We are guaranteed to obtain a matrix $[I|Z']$ because the dimension of Lagrangian subspace is n. A very similar observation was made in [1, Lem. 6].



As the Fourier transform is a symplectomorphism $[I|Z']$ is isotropic, so that:

$$0 = \begin{bmatrix} I|Z' \end{bmatrix} \omega \begin{bmatrix} I|Z' \end{bmatrix}^T$$

which holds if and only if

$$0 = \begin{bmatrix} I|Z' \end{bmatrix} \begin{bmatrix} Z'| - I \end{bmatrix}^T = {Z'}^T - Z'$$

That is to say Z' is symmetric, meaning that Z' 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 in [42, Eq. 18]. Graph states were originally discussed in [43].

We prove that graph states can be reduced to the subspace $[I|0]$ 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:

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & z_{1,1} & z_{1,2} & z_{1,3} & \cdots & z_{1,n} \\ 0 & 1 & 0 & \cdots & 0 & z_{1,2} & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & z_{1,3} & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & z_{1,n} & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right] \xmapsto{(F^{(1)})^{-1}} \left[\begin{array}{ccccc|ccccc} z_{1,1} & 0 & 0 & \cdots & 0 & -1 & z_{1,2} & z_{1,3} & \cdots & z_{1,n} \\ z_{1,2} & 1 & 0 & \cdots & 0 & 0 & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ z_{1,3} & 0 & 1 & \ddots & \vdots & 0 & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{1,n} & 0 & \cdots & 0 & 1 & 0 & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right]$$

$$\xmapsto{C^{(2,1)}_{z_{1,2}}}$$

$$\left[\begin{array}{ccccc|ccccc} z_{1,1}-0 & 0 & 0 & \cdots & 0 & -1 & z_{1,2}-z_{1,2} & z_{1,3} & \cdots & z_{1,n} \\ z_{1,2}-z_{1,2} & 1 & 0 & \cdots & 0 & 0 & z_{2,2}-0 & z_{2,3} & \cdots & z_{2,n} \\ z_{1,3}-0 & 0 & 1 & \ddots & \vdots & 0 & z_{2,3}-0 & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{1,n}-0 & 0 & \cdots & 0 & 1 & 0 & z_{2,n}-0 & z_{3,n} & \cdots & z_{n,n} \end{array}\right] = \left[\begin{array}{ccccc|ccccc} z_{1,1} & 0 & 0 & \cdots & 0 & -1 & 0 & z_{1,3} & \cdots & z_{1,n} \\ 0 & 1 & 0 & \cdots & 0 & 0 & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ z_{1,3} & 0 & 1 & \ddots & \vdots & 0 & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{1,n} & 0 & \cdots & 0 & 1 & 0 & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right]$$

$$\xmapsto{\prod_{i>1}^{n} C^{(i,1)}_{z_{1,i}}}$$

$$\left[\begin{array}{ccccc|ccccc} z_{1,1} & 0 & 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & 0 & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right] \xmapsto{F^{(1)}} \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & z_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & 0 & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right]$$

$$\xmapsto{S^{(1)}_{-z_{1,1}}}$$

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & z_{2,2} & z_{2,3} & \cdots & z_{2,n} \\ 0 & 0 & 1 & \ddots & \vdots & 0 & z_{2,3} & z_{3,3} & \cdots & z_{3,n} \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & z_{2,n} & z_{3,n} & \cdots & z_{n,n} \end{array}\right]$$

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 $L(\cup^{\otimes n})$.

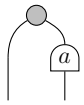
Thus, we have already described all the generators of Lagrangian relations. The gates F, C_a for all $a \in k$, along with the cup and cap and the zero state generate all Lagrangian relations. Note that C_a and the zero state are both in the image of the L.

□

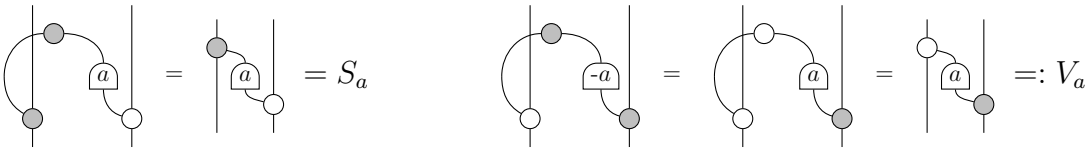
We can also give a presentation of this category which is very close to Selinger's CPM construction [55]. There are several equivalent ways to define the CPM construction. For our purposes, the most convenient one is the presentation used in both in [30, 29], which defines $\mathsf{CPM}[\mathbb{X}]$ as the subcategory of a dagger compact closed category $\mathbb{X}$ whose objects are of the form $A^* \otimes A$ for $A \in \mathbb{X}$ and whose morphisms are generated by (i) 'pure' morphisms, i.e. morphisms of the form $f_* \otimes f$ for $f \in \mathbb{X}$ and a covariant functor $(\_)_*$, and (ii) a 'discard' morphism d_A for every $A \in \mathbb{X}$ given by the counit $d_A := \varepsilon_A : A^* \otimes A \to I$ of the compact closed structure on A.

We nearly obtain such a presentation for LagRel_k using the covariant functor $(-)^\perp$ to define pure morphisms, with the only caveat being we need to consider a family of discard morphisms: each discard morphism being parametrised by a field element.

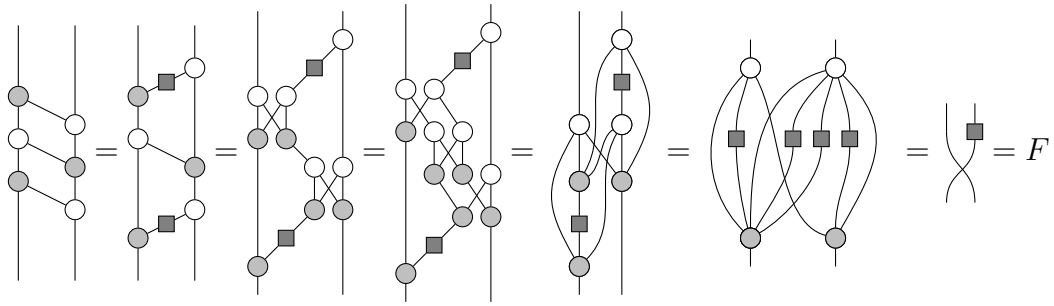
Theorem 5.3.2. LagRel_k *is the monoidal subcategory of* $\mathsf{LinRel}_\mathsf{k}$ *whose objects are of the form* $k^n \oplus k^n$*, for all natural numbers* n*, and whose morphisms are generated by pure morphisms of the form* $V^\perp \oplus V$ *for* $V \in \mathsf{LinRel}_\mathsf{k}$ *and for each* $a \in k$*, a 'discard' morphism:*

$d_a :=$ 

Proof. We just have to 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 can then obtain F as $S_1 \circ V_1 \circ S_1$, which can be proven as a variation of the familiar '3 CNOT' rule for quantum circuits (see e.g. [24, §3.2.1]):

$S_1 \circ V_1 \circ S_1 =$  $= F$

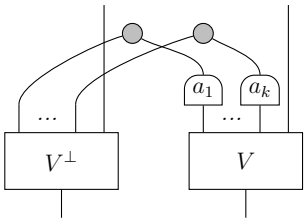
□

In the ZX-calculus literature, this decomposition of the Fourier transform is known as *Euler decomposition* [39]. A variant of this decomposition is given in [8, p.6]; although in the context of plain old linear relations instead of Lagrangian relations, so an antipode is missing in their case. A similar observation was made in [51, (34)] in terms of qudit controlled boost gates; however, the connection to phase-shift gates and Euler decomposition was not made.

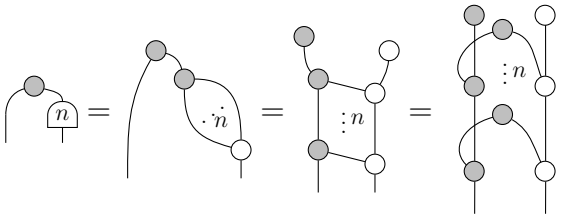
From Theorem 5.3.1, we know that we can build any Lagrangian relation using pure Lagrangian relations and discard maps. Since the former is closed under composition and monoidal product, the following can be shown immediately from string diagram deformation.

Corollary 5.3.3 (Phase purification)**.** *Any linear Lagrangian relation can be written*

in the following form, for V a linear relation:



In the case when we are working with prime fields, then Lagrangian relations are exactly an instance of the CPM construction. Namely, in the category of linear relations, $(-)^*$ is given by relational converse, so we can define a dagger functor $(-)^\dagger := ((-)^\perp)^*$ such that $(-)_* = (-)^\perp$. It only remains to show that all of the discarding maps arise from a single fixed cap. This can be done as follows, for $k = \mathbb{F}_p$:

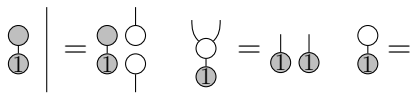


Corollary 5.3.4. *For p prime,* $\mathsf{LagRel}_{\mathbb{F}_p} \cong \mathsf{CPM}[\mathsf{LinRel}_{\mathbb{F}_p}]$.

5.4 Affine Lagrangian relations

Affine Lagrangian relations are perhaps of more practical interest than plain old Lagrangian relations. As we will discuss in this section, these give a semantics for qudit stabilizer circuits as well as certain electrical circuits. We use our universal set of generators for Lagrangian relations as well as the presentation for affine relations to get a universal set of generators for affine Lagrangian relations.

Definition 5.4.1. *[11, §A] Let* aih_k *denote the the prop presented by* ih_k *in addition to the generator* $\overset{|}{\textcircled{1}}$ *and three equations:*

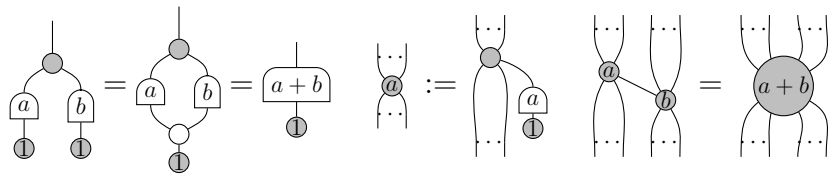


The following was stated slightly differently in the original paper:

Definition 5.4.2. *[11, Definition 5] Let* AffRel_k *denote prop, whose morphisms $n \to m$ are the (possibly empty) affine subspaces of $k^n \oplus k^m$; with composition given by relational composition and tensor product given by the direct sum.*

Theorem 5.4.3. *[11, Thm. 17]* aih_k *is a presentation of* AffRel_k.

Because the equation on the left holds, we can use the phased-spider notation (as in the ZX-calculus), so that for all $a, b \in \mathbb{F}_p$:



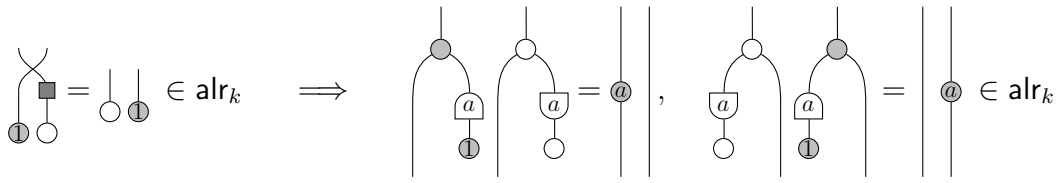
Definition 5.4.4. *Let* $\mathsf{AffLagRel}_k$ *denote the monoidal category whose objects are symplectic vector spaces, and whose morphisms are generated by the image of* $\mathsf{LagRel}_k \xrightarrow{E} \mathsf{LinRel_k} \to \mathsf{AffRel_k}$ *as well as all affine shifts and whose tensor product is the direct sum.*

Because the tensor product is defined in the same way as in LagRel_k, as in Lemma 5.2.6, the forgetful functor $\mathsf{AffLagRel}_k \to \mathsf{AffRel}_k$ is faithful, but only *strong* monoidal.

Definition 5.4.5. *Let* alr_k *denote the monoidal subcategory of* aih_k *with objects* $2n$*, generated by the morphisms in the image of* $\mathsf{LagRel}_k \xrightarrow{E} \mathsf{LinRel_k} \cong \mathsf{ih_k} \to \mathsf{aih_k}$ *as well as the following generator:*

Lemma 5.4.6. 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:

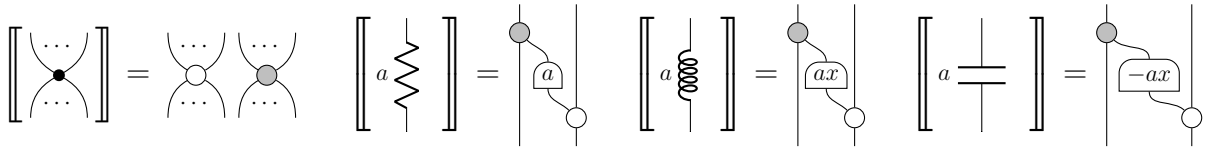


□

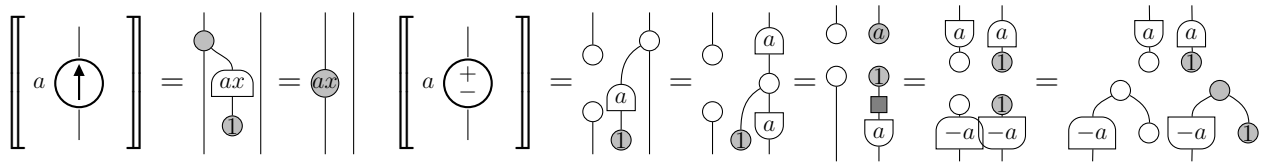
Therefore, we are justified in using string diagrams in alr_k to reason about morphisms in $\mathsf{AffLagRel}_k$.

We will restate the interpretations given in [11] of some components for electrical circuits in terms affine relations in terms of the generators for graphical calculus for Lagrangian relations. This interpretation is also explored in [9, 7]; albeit, not enjoying the graphical calculus for affine relations.

Example 5.4.7. *For any non-negative real* a*, wires,* a*-weighted resistors, inductors and capacitors have the following interpretations in* $\mathsf{AffLagRel}_{\mathbb{R}[x,y]/\langle xy-1\rangle}$*:*



Similarly for a-valued voltage and current sources (again, for a a non-negative real number):



Note that these generators do not generate the whole category of Lagrangian relations; for instance, the coefficients are required to be non-negative.

5.4.1 Stabilizer circuits and Spekkens' toy model

In this subsection, we show that, when p is an odd prime, the prop of affine Lagrangian relations over $\mathbb{F}_p$ is isomoprhic to p-dimensional qudit stabilizer circuits, modulo invertible scalars. We first consider an intermediary fragment between the Fourier-free, phase free fragments and stabilizer circuits.

Definition 5.4.8. *The qudit* **boost operator** *is the following unitary on d in* $\mathsf{Mat}(\mathbb{C})$*,* $\mathcal{X} := \sum_{a=0}^{d-1} |a+1\rangle\langle a|$.

In the qubit case, the boost operator is just the not gate. Adding the affine shift to $\mathsf{ih}_{\mathbb{F}_p}$, corresponds to adding the boost gate to the Fourier-free, phase-free ZX-calculus, extending Lemma 5.1.6. This is a qudit generalization of the observation made in [33]:

Lemma 5.4.9. *For p prime, $\mathsf{aih}_{\mathbb{F}_p}$ is isomorphic as a prop to the Fourier-free, p-dimensional qudit ZX-calculus with the boost operator modulo invertible scalars.*

We can go further with affine Lagrangian relations. Inspired by the work of Spekkens [58, 59]:

Definition 5.4.10. *When p is prime, let* **Spekkens' qudit toy model** *of dimension p denote the prop* $\mathsf{AffLagRel}_{\mathbb{F}_p}$.

We first give a short review of the qudit stabilizer formalism, before establishing the equivalence between Spekkens' toy model and stabilizer circuits in the odd prime qudit case. All of the material from Definition 5.4.11 to 5.4.13 are contained in [45].

Definition 5.4.11. *The qudit* **shift operator** *is the following unitary on d in* $\mathsf{Mat}(\mathbb{C})$*,* $\mathcal{Z} := \sum_{a=0}^{d-1} e^{2\pi i a/d} |a\rangle\langle a|$.

An n-qudit **Weyl operator** *an d^n-dimensional unitary generated by the shift, boost and identity operators as well as the scalar $e^{\pi i/d}$ under tensor product and matrix multiplication. /*

The n-qudit **Weyl group**,$\mathfrak{P}_d^n$, *is generated by the n-qudit Weyl operators under matrix multiplication.*

An n-qudit **Clifford operator** *U is an d^n-dimensional unitary so that $U\mathfrak{P}_d^n U^\dagger = \mathfrak{P}_d^n$.*

The n-qudit **Clifford group** *is formed by the n-qudit Clifford operators under matrix multiplication.*

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

Given any n-qudit stabilizer state $|\psi\rangle$, the **stabilizer group** *of $|\psi\rangle$ is the (Abelian) subgroup of $\mathfrak{S}_{|\psi\rangle} \subset \mathfrak{P}_d^n$ whose elements are the $U \in \mathfrak{P}_d^n$ for which $U|\psi\rangle = |\psi\rangle$.*

Lemma 5.4.12. *Two stabilizer states with the same stabilizer groups are the same, up to global phases.*

Lemma 5.4.13. *For natural numbers $n, d \geq 2$ the n-dimensional qudit stabilizer group modulo invertible scalars is generated under tensor and composition of I_d as well as the boost operator $\mathcal{X}$, the controlled-boost operator $\mathcal{C}$, the Fourier transform $\mathcal{F}$ and the phase-shift operator $\mathcal{S}$:*

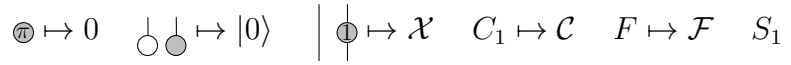
$$\mathcal{C} := \sum_{a,b=0}^{d-1} |a, a+b\rangle\langle a, b| \quad \mathcal{F} := \frac{1}{\sqrt{d}} \sum_{a,b=0}^{d-1} e^{2\pi i ab/d} |b\rangle\langle a| \quad \mathcal{S} := \sum_{a=0}^{d-1} e^{\pi i a(a+d)/d} |a\rangle\langle a|$$

Notice that the boost operator can be obtained by $\mathcal{Z} = \mathcal{F}\mathcal{X}\mathcal{F}^2$.

Definition 5.4.14. *Let Stab_p denote the subcategory of $\mathsf{Mat}(\mathbb{C})$ generated by the p-dimensional qudit Clifford group as well as the vectors $|0\rangle$, $\langle 0|$, quotiented by invertible scalars.*

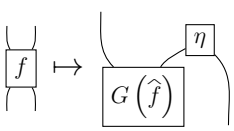
The following isomorphism is described in [42], when restricted to the nonempty case. This comes from the projective representation of the n qudit odd-prime-dimensional Clifford group in terms of the affine symplectomorphisms over $\mathbb{F}_p^n$. However, since there is only one empty relation and one zero matrix of every type, we get the following result immediately:

Lemma 5.4.15. *For every odd prime p, there is an isomorphism $G : \mathsf{AffLagRel}_{\mathbb{F}_p}(0, n) \to \mathsf{Stab}_p(0, n)$ determined by:*



We extend this isomorphim of states to an isomorphism of props:

Theorem 5.4.16. *When p is an odd prime, the mapping $H : \mathsf{AffLagRel}_{\mathbb{F}_p} \to \mathsf{Stab}_p$ defined by:*

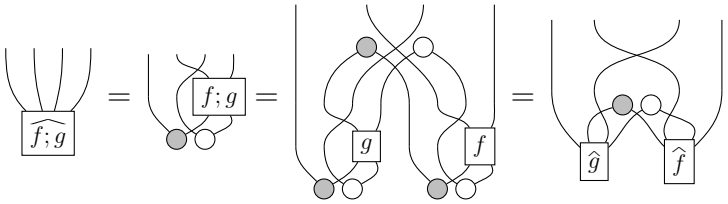


is a symmetric monoidal equivalence, where η is the cap of the compact closed structure induced by the Z observable.

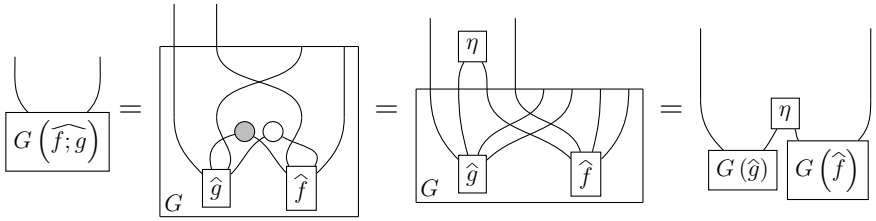
Proof. It preserves identities by the snake equations. Now we must show it preserves composition. Consider some composable pair in $\mathsf{AffLagRel}_{\mathbb{F}_p}$:

$$\mathbb{F}_p^n \xrightarrow{f} \mathbb{F}_p^m \xrightarrow{g} \mathbb{F}_p^\ell$$

If the composite is empty, then the result follows immediately. Suppose otherwise. We know that:

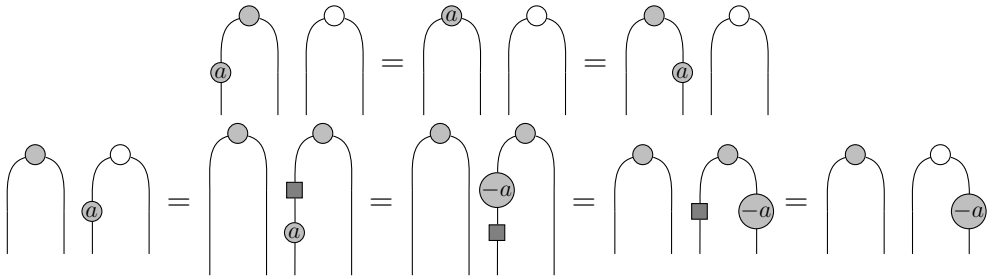


We have the following equality of diagrams in Stab_p, We draw the wires exiting G to be connected to the corresponding wires in the X block of the subspace.

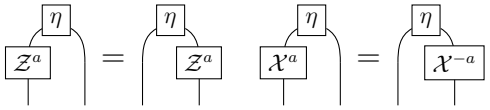


This second equality is the only nontrivial part. It follows by observing that both stabilizer states are stabilized by the same generalized Pauli operators, and thus they are the same. This is because the generalized Pauli operators can be pulled through G, by [42, Lemma 4], where they act the same on the caps of Lagrangian relations and in matrices.

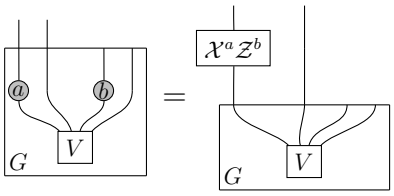
Explicity, the boost and shift operators commute with the cap as follows:



Which are analagous to the following commutations in stabilizer circuits:



Where moreover, for any Lagrangian relation V and $a, b \in \mathbb{F}_p$, we already know:



Therefore, functoriality follows by uncurrying the left and right hand sides of the previous equation. Fullness and faithfulness follow immediately from G being an isomorphism. □

Definition 5.4.17. *Define a conjugation functor* $\overline{(\_)} : \mathsf{AffLagRel}_k \to \mathsf{AffLagRel}_k$ *the identity on* $L(\mathsf{LinRel}_\mathsf{k})$ *and* X*, but taking* $F \mapsto F^{-1}$*,* $S_a \mapsto S_a^{-1}$ *and* $X \mapsto X$*.*

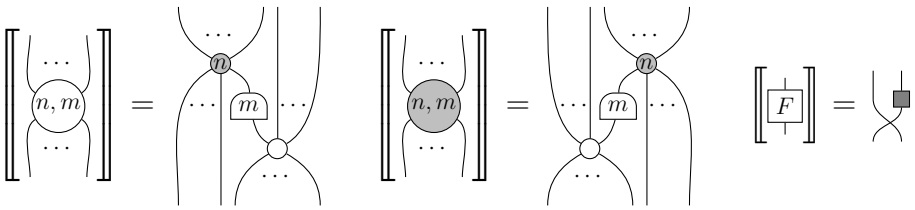
The following fact follows from a mechanical calculation:

Lemma 5.4.18. *For odd prime* p*, the conjugation functor* $\overline{(\_)} : \mathsf{AffLagRel}_{\mathbb{F}_p} \to \mathsf{AffLagRel}_{\mathbb{F}_p}$ *corresponds to complex conjugation in* Stab_p*.*

As we mentioned in the introduction, this is a categorical reformulation of the result of Spekkens' in which he shows that odd-prime-dimensional 'quadrature epistricted theories' are operationally equivalent to prime-dimensional qudit stabilizer circuits [59].

A complete presentation for Spekkens' qubit toy model in terms of a category of relations was given [4] in a style which mirrors that of the qubit ZX-calculus [24]. We now show how the generators of that presentation appear in our 'doubled' formulation.

Remark 5.4.19. *We can present Spekkens' p-dimensional qudit toy model in a manner similar to the ZX-calculus, in terms of being generated by spiders with phases labelled by the group* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$*,:*



The Fourier transform is redundant, as it can be obtained by Euler decomposition.

Notice that the phases of the Z and X observables are elements (n, m) of $\mathbb{F}_p \times \mathbb{F}_p$, and it is easy to see how the doubled spiders satisfy the phased spider fusion laws with respect to the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, as discussed in [52, p.166]. As discussed in [26] this is one of the central features which separates Spekkens' qubit model from qubit stabilizers, whose phase group is $\mathbb{Z}/4\mathbb{Z}$. This fact can be also observed graphically in

terms of the stabilizer fragment of the ZX-calculus (in contrast to the presentation of Spekkens' qubit toy model) which also enjoys a complete axiomatization [4].

By stating the interpretations of Spekkens' toy model in terms of the graphical calculus for Lagrangian relations alongside that of electrical circuits, we see the evident analogy between the phases in the ZX-calculus and the resistors, inductor, capacitors and voltage sources in electrical circuits.

5.5 Measurement and CoIsotropic relations

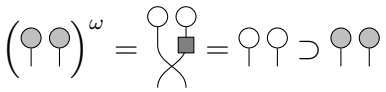
By allowing more morphisms than Lagrangian subspaces we can capture more behaviour. In this section, we show how the coisotropic generalization of Lagrangian relations gives a semantics for measurement in the symplectic setting.

Definition 5.5.1. *Given a field k, the prop* $\mathsf{IsotRel}_k$ *of* **isotropic relations** *has morphisms $n \to m$ as isotropic subspaces of the symplectic vector spaces $k^{n+m} \oplus k^{n+m}$. Dually, the prop* $\mathsf{CoIsotRel}_k$ *of* **coisotropic relations** *has morphisms are coisotropic subspaces. The composition, identity and tensor is that same as for Lagrangian relations. The* $\mathsf{AffIsotRel}_k$ *and* $\mathsf{AffCoIsotRel}_k$ *of* **affine (co)isotropic relations** *have morphisms are affine (co)isotropic subspaces of the direct sum of the domain and codomain.*

It is mechanical to verify that these are props.

Theorem 5.5.2. *The prop* $\mathsf{IsotRel}_k$ *is generated by adding the doubled zero relation to the image of the embedding* $\mathsf{LagRel}_k \to \mathsf{LinRel}_k$*, ie. the following generator in* ih_k*:*

Proof. First observe that this generator is an isotropic subspace of (k^{2n}, ω) since:



Suppose that we have an isotropic subspace V of (k^{2n}, ω) with dimension $n - m$.

By applying Fourier transforms, we obtain a symplectomorphic subspace generated by a matrix whose pivots are all in the X block. Therefore, we can row reduce this matrix to obtain one of the following form:

$$\left[\begin{array}{cc|cc} I_{n-m} & X_B & Z_A & Z_B \end{array}\right]$$

By applying controlled shift gates from the first $n - m$ wires to the last m wires we obtain an isotropic subspace generated by a matrix of the following form:

$$\left[\begin{array}{cc|cc} I_{n-m} & 0 & Z'_A & Z'_B \end{array}\right]$$

Since all of the rows of this subspace are orthogonal with respect to the symplectic form, we have:

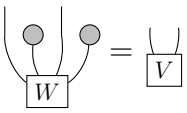
$$\begin{aligned}
0 &= \left[\begin{array}{cc|cc} I_{n-m} & 0 & Z'_A & Z'_B \end{array}\right] \omega \left[\begin{array}{cc|cc} I_{n-m} & 0 & Z'_A & Z'_B \end{array}\right]^T \\
&= \left[\begin{array}{cc|cc} I_{n-m} & 0 & Z'_A & Z'_B \end{array}\right] \left[\begin{array}{cc|cc} -Z'_A & -Z'_B & I_{n-m} & 0 \end{array}\right]^T \\
&= I_{n-m}(-Z'_A)^T + 0(-Z'_B)^T + Z'_A I_{n-m} + Z'_B 0 \\
&= (-Z'_A)^T + Z'_A
\end{aligned}$$

Which holds if and only if $Z'_A = (Z'_A)^T$ is symmetric.

Therefore, the following matrix generates a Lagrangian subspace of $k^{2(n+1)}$ because the X block is the identity and the Z block is symmetric:

$$\left[\begin{array}{ccc|ccc} I_{n-m} & 0 & 0 & Z'_A & Z'_B & 0 \\ 0 & I_m & 0 & (Z'_B)^T & 0 & v \\ 0 & 0 & 1 & 0 & v^T & 0 \end{array}\right]$$

Where v is the m-dimensional vector with only 1s. Let W be the Lagrangian subspace generated by this matrix. Then



This follows because composing W with the cozero maps on the last wire of the Z and X blocks picks out the columns where the last row of the X and Z blocks are both 0; that is, those of the generator matrix of V.

□

Since, the orthogonal complement reverses the order of inclusions, it extends to an isomorphism $\mathsf{CoIsotRel}_k \to \mathsf{IsotRel}_k$ so that:

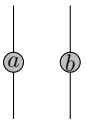
Corollary 5.5.3. *The prop* $\mathsf{CoIsotRel}_k$ *is generated by adding the doubled discard relation to the image of the embedding* $\mathsf{LagRel}_k \to \mathsf{LinRel}_\mathsf{k}$*, ie. the following generator in* ih_k*:* 

From the same argument that yields $\mathsf{AffLagRel}_k$ from LagRel_k:

Lemma 5.5.4. *The props* $\mathsf{AffIsotRel}_k$ *and* $\mathsf{AffCoIsotRel}_k$ *are generated by adding the generator* X *to the respective images of the embeddings* $\mathsf{IsotRel}_k \to \mathsf{LinRel}_\mathsf{k}$ *and* $\mathsf{CoIsotRel}_k \to \mathsf{LinRel}_\mathsf{k}$.

Notice that unlike in the linear case, these two props are not isomorphic, as the doubled discard and doubled cozero maps interact differently with the X gate. For example:

Definition 5.5.5. *Given a field k and natural number n, the* **generalized Pauli group** *on n wires, P_k^n is generated by the following affine Lagrangian relations under tensor product, for $a, b \in k$:*

$W(a,b) :=$ 

Just as in the quantum case, call elements of the generalized Pauli group **Weyl operators**. *Given a tuple $((a_1, \cdots, a_n), (b_1, \cdots, b_n)) \in (k^2)^n$ we can similarly define a Weyl operator $W(a_1, \cdots, a_n), (b_1, \cdots, b_n) = W(a_1, b_1) \oplus \cdots \oplus W(a_n, b_n)$.*

Definition 5.5.6. *Given some state $f : 0 \to n$ in $\mathsf{CPM}(\mathsf{AffLagRel}_k)$, the generalized* **stabilizer group** *of f is the subgroup of the generalized Pauli group generated by the Weyl operators $a \in P_k^n$ so that $U(f); (1_n \otimes a) = U(f)$, where $U : \mathsf{CPM}(\mathsf{AffLagRel}_k) \to \mathsf{AffLagRel}_k$ is the forgetful functor.*

Lemma 5.5.7. *Take an affine Lagrangian relation $f : 0 \to n + m$. Then a Weyl operator x in the stabilizer group of $\mathsf{CPM}(f); (1_n \oplus !_m)$ if and only if $x \oplus 1_m$ it is in the stabilizer group of f.*

Proof. Take some state f as above. If $\mathsf{CPM}(f); (1_n \oplus !_m)$ has no stabilizer group (because it is empty), then the claim follows vacuously. Take some $W(a,b) \in P_k^n$ in the stabilizer group of $\mathsf{CPM}(f); (1_n \oplus !_m)$. Then there exists some $W(c,d) \in P_k^m$ such that $f; (W(a,b) \oplus 1_m) = f; (1_n \oplus W(c,d))$.

Let d_i be the cozero relation on i wires.

Pick some element $((x_A, x_B), (z_A, z_B))$ in f so that $f; W((x_A, x_B), (z_A, z_B))); d_{n+m} = 1_0$.

Take $U : \mathsf{CPM}(\mathsf{AffLagRel}_k) \to \mathsf{AffLagRel}_k$ to be the forgetful functor. Then

$$
\begin{aligned}
1 &= U(\mathsf{CPM}(f); (1_n \oplus !_m); \mathsf{CPM}(W(x_A, z_A); d_n)) \\
&= U(\mathsf{CPM}(f); (1_n \oplus !_m); (1_n \oplus W(a,b)); \mathsf{CPM}(W(x_A, z_A); d_n)) \\
&= U(\mathsf{CPM}(f); (1_n \oplus !_m); (1_n \oplus W(a,b)); \mathsf{CPM}(W(x_A, z_A); d_n)) \\
&= (\overline{f} \oplus f); (1_n \oplus (1 \oplus W(c,d); \eta_m) \oplus 1_n); \overline{W(x_A, z_A)}; d_n \oplus W(x_A, z_A); d_n \\
&= d_m^T; W(x_B, -z_B) \oplus d_m^T; W(x_B, z_B); (1 \oplus W(c,d)); \eta_m \\
&= d_m^T; W(x_B, -z_B); W(c,d); W(-x_B, z_B); d_m \\
&= d_m^T; W(c,d); d_m
\end{aligned}
$$

Which is true if and only if $W(c,d) = 1$.

□

The following proposition is the symplectic version of the essential uniquess of dilation:

Proposition 5.5.8. *States in* $\mathsf{CPM}(\mathsf{AffLagRel}_k)$ *are uniquely determined by their stabilizer groups.*

Proof. By construction, the stabilizer group of a state is unique.

Pick two affine Lagrangian relations $f : 0 \to n+m$, $g : 0 \to n+\ell$ so that $\mathsf{CPM}(f);(1_n \oplus !_m)$ and $\mathsf{CPM}(g);(1_n \oplus !_\ell)$ have then same stabilizer group. Then from the previous lemma,

$$\begin{aligned} f;(x \oplus 1_m) = f &\iff U(\mathsf{CPM}(f);(1_n \oplus !_m));(1_n \oplus x) = U(\mathsf{CPM}(f);(1_n \oplus !_m)) \\ &\iff U(\mathsf{CPM}(g);(1_n \oplus !_\ell));(1_n \oplus x) = U(\mathsf{CPM}(g);(1_n \oplus !_\ell)) \\ &\iff g;(x \oplus 1_\ell) = g \end{aligned}$$

Without loss of generality take $m \geq \ell$. Then there are unitaries u, w on m, ℓ wires so that

$$f;(1_n \oplus u) = g;(1_n \oplus v \oplus 1_{m-\ell})$$

And thus an isometry $v : \ell \to m$ so that

$$f;(1_n \oplus u) = g;(1_n \oplus v)$$

Therefore,

$$\mathsf{CPM}(f);(1_n \oplus !_m) = \mathsf{CPM}(f;(1_n \oplus u));(1_n \oplus !_m) = \mathsf{CPM}(g;(1 \oplus v));(1_n \oplus !_m) = \mathsf{CPM}(g);(1_n \oplus !_\ell)$$

□

Theorem 5.5.9. $\mathsf{CPM}(\mathsf{AffLagRel}_k) \cong \mathsf{AffCoIsotRel}_k$

Proof. Because both categories are compact closed, it suffices to exhibit a bijection between the states of both categories.

We already know that affine coisotropic Lagrangian subspaces are determined by their stabilizers. Therefore it suffices to show that the stabilizers in $\mathsf{CPM}(\mathsf{AffLagRel}_k)$ and $\mathsf{AffCoIsotRel}_k$ agree; that is:

$$f;(x \oplus d_m) = f;(1_n \oplus d_m) \iff U(\mathsf{CPM}(f);(1_n \oplus !_m));(1_n \oplus x) = U(\mathsf{CPM}(f);(1_n \oplus !_m))$$

If f is empty, then the claim follows immediately. Suppose otherwise. The forward direction follows immediately from the fact that x is unitary. Conversely, we know there is some Weyl operator y such that $f;(x \oplus 1) = f;(1 \oplus y)$ but $f;(x \oplus d_m) = f;(1_n \oplus (y; d_m)) = f;(1_n \oplus d_m)$

□

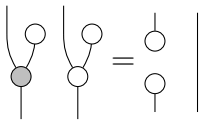
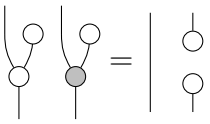
Corollary 5.5.10. *For odd prime p,* $\mathsf{AffCoIsotRel}_{\mathbb{F}_p} \cong \mathsf{CPM}(\mathsf{AffLagRel}_{\mathbb{F}_p}) \cong \mathsf{CPM}(\mathsf{Stab}_p)$*, that is, mixed stabilizer circuits modulo invertible scalars.*

Corollary 5.5.11. $\mathsf{AffCoIsotRel}_{\mathbb{F}_2} \cong \mathsf{CPM}(\mathsf{AffLagRel}_{\mathbb{F}_2}) \cong \mathsf{CPM}(\mathsf{Stab}_2)$*, that is, Spekkens' toy model with mixed states.*

Corollary 5.5.12. *For a prime number p,* $\mathsf{IsotRel}_{\mathbb{F}_p} \cong \mathsf{CoIsotRel}_{\mathbb{F}_p} \cong \mathsf{CPM}(\mathsf{CPM}(\mathsf{LinRel}_{\mathbb{F}_p}))$.

In the quantum setting, by connecting the discard map to a spider, one obtains a circuit which decoheres the state into a basis. In stabilizer circuits, discarding a white spider decoheres in the X basis, and discarding in the black spider decoheres in the Z basis. We use this intuition two define to maps in the general coisotropic setting:

Definition 5.5.13. *The X and Z decoherence maps are defined as follows in* $\mathsf{AffCoIsotRel}_{\mathbb{F}_p}$*:*

$p_X :=$  $p_Z :=$ 

Definition 5.5.14. *Let* $\mathsf{AffCoIsotRel}_k^M$ *denote the two coloured prop generated by splitting p_Z in* $\mathsf{AffCoIsotRel}_k$*. Let Q denote the original generating object and C the object obtained by splitting p_Z.*

We could have instead split p_X, or split both p_Z and p_Z; however, all three of these multicoloured props are equivalent. This equivalence is witnessed via the Fourier transform.

The idea here is that in the quantum setting, the object Q is interpreted as a quantum channel and the object C as a classical channel.

Lemma 5.5.15. *The full subcategory of* $\mathsf{AffCoIsotRel}_k^M$ *generated by tensor powers of C is isomorphic to* AffRel_k*.*

We can see this category more concretely in terms of being generated by certain linear relations:

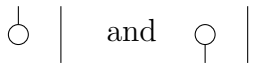
Theorem 5.5.16. $\mathsf{AffCoIsotRel}_k^M$ *is isomorphic to adding the following linear relations to the image of* $\mathsf{AffCoIsotRel}_k$ *in the way which makes this into a two-coloured prop:*

 *and*

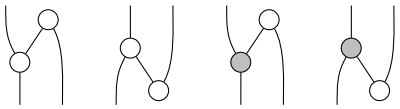
Proof. Suppose we have a morphism $C^{\oplus n} \to Q^{\oplus m}$ witnessed by two maps f, g □

This is somewhat counterintutitive, because we do not actually need to double wires to accomodate for classical and quantum information at the same time; rather, we need to halve it.

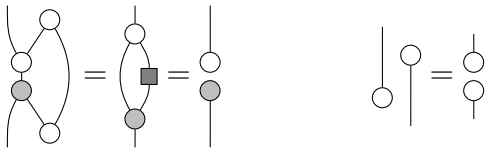
These morphisms are interpreted in terms of state preparation and measurement in the X basis. The state preparation and discarding in the Z basis are obtained by composition of these morphisms with the Fourier transform; yielding morphisms which dicard the X wire instead of the Z wire:



Remark 5.5.17. *In* FHilb*, the state preparation and measurement in the X and Z bases are given by the following ZX calculus diagrams:*

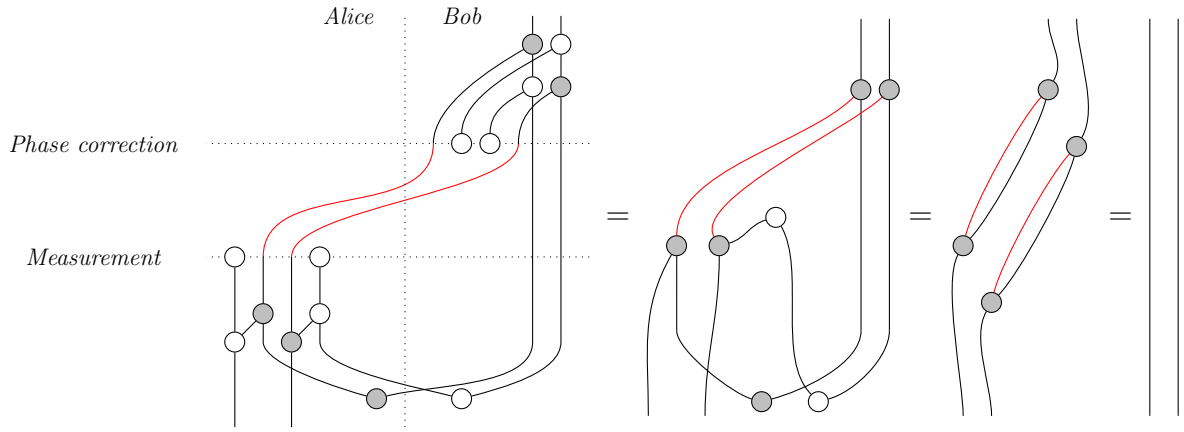


The strong complementarity of the X and Z variables in this setting follows from the fact that their corresponding Frobenius algebras interact to form a hopf algebra. However, in the symplectic picture, this result is purely topological:



For this reason, we can prove the correctness of the quantum teleportation algorithm using only spider fusion:

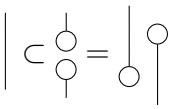
Example 5.5.18. *The following circuit in* $\mathsf{AffColsotRel}_{\mathbb{F}_p}^{M}$ *depicts a quantum teleportation protocol where Alice on the left teleports a qudit to Bob, on the right. They share an EPR pair (on the bottom of the diagram) and two classical dits (drawn in red).*



Because $\mathsf{AffCoIsotRel}_{\mathbb{F}_p}^M$ is a subcategory of relations, we can interpret the structure of the 2-cells in terms of quantum information theory.

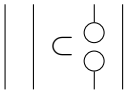
Remark 5.5.19. *Take two odd-prime dimensional qudit stabilizer circuits f, g interpreted as parallel maps in $\mathsf{AffCoIsotRel}_{\mathbb{F}_p}^M$. Then f is a coarse-graining of g when $f \subset g$.*

For an extreme example, the identity circuit on a classical wire is contained within the circuit obtained by preparing in the Z basis and measuring in the X:



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 outputs.

Similarly, the identity on a quantum wire is a coarse graining of the decoherence map:



5.6 Further work

There are several directions in which the work in this paper could be further explored. Since linear relations are can be defined over a principle ideal domain over a field, it is natural to ask if the work can be generalized to this setting. Also, we have not given a completeness result entirely in terms of the generators of LagRel_k. The proof of such would almost certainly involve mimicking the universality proofs of the qubit stabilizer/qutrit stabilizer/Spekkens' toy model [3, 4, 62] involving local equivalency/local complementation of graph states. If this were generalized to affine

Lagrangian relations this would yield a proper completeness result for the odd-prime-dimensional qudit stabilizer ZX calculus as a corollary. One could also potentially adapt this approach to characterize Lagrangian spans as described in [40, p. 187], where the scalars are not all quotiented out. Perhaps this would give a semantics for odd-prime-dimensional qudit stabilizer circuits on the nose.

This paper illuminates the deep connection between stabilizer circuits and electrical circuits. Perhaps, this can be taken further by adding nonlinear generators such as diodes.

Chapter 6

Quantum combs

Chapter 7

Categorical semantics for the scalable ZX-calculus

Chapter 8

Conclusion

Bibliography

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.

[2] Lowell Abrams. *Frobenius algebra structures in topological quantum field theory and quantum cohomology*. PhD thesis, Johns Hopkins University, 1997.

[3] Miriam Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16(9):093021, 2014.

[4] Miriam Backens and Ali Nabi Duman. A complete graphical calculus for Spekkens' toy bit theory. *Foundations of Physics*, 46(1):70–103, 2016.

[5] Miriam Backens and Aleks Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. *Electronic Proceedings in Theoretical Computer Science*, 287:23–42, January 2019.

[6] John C. Baez and Kenny Courser. Structured cospans. *Theory and Applications of Categories*, 35(48):1771–1822, 2020.

[7] John C. Baez, Brandon Coya, and Franciscus Rebro. Props in network theory. *Theory and Applications of Categories*, 33(25):727–783, 2018.

[8] John C. Baez and Jason Erbele. Categories in control. *Theory and Applications of Categories*, 30(24):836–881, 2015.

[9] John C. Baez and Brendan Fong. A compositional framework for passive linear networks. *Theory and Applications of Categories*, 33(38):pp 1158–1222, 2018.

[10] Filippo Bonchi, Dusko Pavlovic, and PawełSobociński. Functorial semantics for relational theories. *arXiv preprint arXiv:1711.08699*, 2017.

[11] Filippo Bonchi, Robin Piedeleu, Paweł Sobociński, and Fabio Zanasi. Graphical affine algebra. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12. IEEE, 2019.

[12] Filippo Bonchi, Paweł Sobociński, and Fabio Zanasi. Lawvere categories as composed PROPs. In *Coalgebraic Methods in Computer Science*, pages 11–32. Springer International Publishing, 2016.

[13] Filippo Bonchi, Paweł Sobociński, and Fabio Zanasi. Interacting Hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144–184, 2017.

[14] Roberto Bruni and Fabio Gadducci. Some algebraic laws for spans (and their connections with multirelations). *Electronic Notes in Theoretical Computer Science*, 44(3):175–193, 2003. RelMiS 2001, Relational Methods in Software (a Satellite Event of ETAPS 2001).

[15] Carsten Butz. Regular categories and regular logic, oct 1998.

[16] A. Carboni and R.F.C. Walters. Cartesian bicategories i. *Journal of Pure and Applied Algebra*, 49(1-2):11–32, November 1987.

[17] Titouan Carette and Emmanuel Jeandel. A recipe for quantum graphical languages. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 118:1–118:17, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[18] Lorenzo Catani and Dan Browne. Spekkens' toy model in all dimensions and its relationship with stabiliser quantum mechanics. *New Journal of Physics*, 19(7):073035, 2017.

[19] Eugenia Cheng. Distributive laws for Lawvere theories. *Compositionality*, 2, May 2020.

[20] Robin Cocket and Steve Lack. Restriction categories III: colimits, partial limits and extensivity. *Mathematical Structures in Computer Science*, 17(4):775–817, August 2007.

[21] J.R.B. Cockett and Cole Comfort. The category TOF. *Electronic Proceedings in Theoretical Computer Science*, 287:67–84, January 2019.

[22] J.R.B. Cockett and Steve Lack. Restriction categories i: categories of partial maps. *Theoretical Computer Science*, 270(1):223–259, 2002.

[23] Robin Cockett, Cole Comfort, and Priyaa Srinivasan. The category CNOT. *Electron. Proc. Theor. Comput. Sci.*, 266:258–293, February 2018.

[24] Bob Coecke and Ross Duncan. Interacting quantum observables. In *International Colloquium on Automata, Languages, and Programming*, pages 298–310. Springer, 2008.

[25] Bob Coecke and Bill Edwards. Spekkens's toy theory as a category of processes. In *Proceedings of Symposia in Applied Mathematics*, volume 71, pages 61–88, 2012.

[26] Bob Coecke, Bill Edwards, and Robert W. Spekkens. Phase groups and the origin of non-locality for qubits. *Electronic Notes in Theoretical Computer Science*, 270(2):15–36, 2011.

[27] Bob Coecke and Chris Heunen. Pictures of complete positivity in arbitrary dimension. *Information and Computation*, 250:50–58, October 2016.

[28] Bob Coecke, Chris Heunen, and Aleks Kissinger. Categories of quantum and classical channels. *Quantum Information Processing*, 15(12):5179–5209, oct 2014.

[29] Bob Coecke and Aleks Kissinger. *Categorical Quantum Mechanics I: Causal Quantum Processes*. Oxford University Press, 11 2017.

[30] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.

[31] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In *Computer Science Logic*, pages 230–244. Springer Berlin Heidelberg, 2010.

[32] Cole Comfort. Classifying reversible logic gates with ancillary bits. Master's thesis, University of Calgary, 2019.

[33] Cole Comfort. Distributive laws, spans and the ZX-calculus. *arXiv preprint*, 2021.

[34] Cole Comfort. The zx&-calculus: A complete graphical calculus for classical circuits using spiders. 340:60–90, 2021.

[35] Brandon Coya. *Circuits, bond graphs, and signal-flow diagrams: A categorical perspective*. PhD thesis, University of California Riverside, 2018.

[36] Niel De Beaudrap. A linearized stabilizer formalism for systems of finite dimension. *Quantum Info. Comput.*, 13(1–2):73–115, January 2013.

[37] Niel de Beaudrap, Aleks Kissinger, and Konstantinos Meichanetzidis. Tensor network rewriting strategies for satisfiability and counting. *Electronic Proceedings in Theoretical Computer Science*, 340:46–59, September 2021.

[38] Ross Duncan and Kevin Dunne. Interacting frobenius algebras are hopf. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '16, page 535–544, New York, NY, USA, 2016. Association for Computing Machinery.

[39] Ross Duncan and Simon Perdrix. Graph states and the necessity of euler decomposition. In *Conference on Computability in Europe*, pages 167–177. Springer, 2009.

[40] Brendan Fong. *The algebra of open and interconnected systems.* PhD thesis, University of Oxford, 2016.

[41] Brett Giles. *An investigation of some theoretical aspects of reversible computing.* PhD thesis, University of Calgary, 2014.

[42] David Gross. Hudson's theorem for finite-dimensional quantum systems. *Journal of mathematical physics*, 47(12):122107, 2006.

[43] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, M Nest, and H-J Briegel. Entanglement in graph states and its applications. *Proceedings of the International School of Physics*, 162(Quantum Computers, Algorithms and Chaos):115–218, 2006.

[44] Michael Herrmann. Models of multipartite entanglement. Master's thesis, University of Oxford, 2010.

[45] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. *Physical Review A*, 71(4):042315, 2005.

[46] K. Iwama, Y. Kambayashi, and S. Yamashita. Transformation rules for designing cnot-based quantum circuits. In *Proceedings 2002 Design Automation Conference (IEEE Cat. No.02CH37324)*, pages 419–424, 2002.

[47] Steve Lack. Composing props. *Theory and Applications of Categories*, 13(9):147–163, 2004.

[48] Yves Lafont. Towards an algebraic theory of boolean circuits. *Journal of Pure and Applied Algebra*, 184(2):257–310, 2003.

[49] Anthony Munson, Bob Coecke, and Quanlong Wang. AND-gates in ZX-calculus: Spider nest identities and QBC-completeness. *Electronic Proceedings in Theoretical Computer Science*, 340:230–255, September 2021.

[50] Robin Piedeleu. *Picturing resources in concurrency.* PhD thesis, University of Oxford, 2018.

[51] André Ranchin. Depicting qudit quantum mechanics and mutually unbiased qudit theories. In Bob Coecke, Hasuo Ichiro, and Prakash Panangaden, editors, Proceedings 14th International Conference on *Quantum Physics and Logic,* Kyoto University, Japan, 4-6 June 2017, volume 172 of *Electronic Proceedings in Theoretical Computer Science*, pages 68–91. Open Publishing Association, December 2014.

[52] André Ranchin. *Alternative theories in quantum foundations.* PhD thesis, Imperial College London, 2016.

[53] Edmund Robinson and Giuseppe Rosolini. Categories of partial maps. *Information and Computation*, 79(2):95–130, 1988.

[54] Robert Rosebrugh and R.J. Wood. Distributive laws and factorization. *Journal of Pure and Applied Algebra*, 175(1-3):327–353, November 2002.

[55] Peter Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical computer science*, 170:139–163, 2007.

[56] V.V. Shende, A.K. Prasad, I.L. Markov, and J.P. Hayes. Synthesis of reversible logic circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 22(6):710–722, 2003.

[57] Paweł Sobociński. Graphical linear algebra: Orthogonality and projections, 2017.

[58] Robert W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A*, 75(3):032110, 2007.

[59] Robert W. Spekkens. Quasi-quantization: classical statistical theories with an epistemic restriction. In *Quantum Theory: Informational Foundations and Foils*, pages 83–135. Springer, 2016.

[60] Tommaso Toffoli. Reversible computing. In *Automata, Languages and Programming*, pages 632–644. Springer Berlin Heidelberg, 1980.

[61] John van de Wetering and Sal Wolffs. Completeness of the phase-free zh-calculus, 2019.

[62] Quanlong Wang. Qutrit ZX-calculus is complete for stabilizer quantum mechanics. In Bob Coecke and Aleks Kissinger, editors, Proceedings 14th International Conference on *Quantum Physics and Logic,* Nijmegen, The Netherlands, 3-7 July 2017, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 58–70. Open Publishing Association, 2018.

[63] Quanlong Wang. Completeness of algebraic zx-calculus over arbitrary commutative rings and semirings, 2019.

[64] Alan Weinstein. Symplectic groupoids and Poisson manifolds. *Bulletin of the American mathematical Society*, 16(1):101–104, 1987.

[65] Fabio Zanasi. *Interacting Hopf Algebras: the theory of linear systems.* PhD thesis, Université de Lyon, 2018.