Categories of relations as models of quantum theory

Chris Heunen* and Sean Tull†
{heunen,sean.tull}@cs.ox.ac.uk
University of Oxford, Department of Computer Science

Categories of relations over a regular category form a family of models of quantum theory. Using regular logic, many properties of relations over sets lift to these models, including the correspondence between Frobenius structures and internal groupoids. Over compact Hausdorff spaces, this lifting gives continuous symmetric encryption. Over a regular Mal'cev category, this correspondence gives a characterization of categories of completely positive maps, enabling the formulation of quantum features. These models are closer to Hilbert spaces than relations over sets in several respects: Heisenberg uncertainty, impossibility of broadcasting, and behavedness of rank one morphisms.

1 Introduction

Many features of quantum theory can be abstracted to arbitrary *compact dagger categories* [1]. Thus we can compare models of quantum theory in a unified setting, and look for features that distinguish the category **FHilb** of finite-dimensional Hilbert spaces that forms the traditional model. The category **Rel** of sets and *relations* is an alternative model. It exhibits many features considered typical of quantum theory [2], but also refutes presumed correspondences between them [15, 21]. However, apart from **Rel** and its subcategory corresponding to Spekkens' toy model [14], few alternative models have been studied in detail.

We consider a new family of models by generalizing to categories $\mathbf{Rel}(\mathbf{C})$ of relations over an arbitrary *regular category* $\mathbf{C}$, including any algebraic category like that of groups, any abelian category like that of vector spaces, and any topos like that of sets. Despite this generality, *internal logic* allows us to state and prove results as if working in **Rel**, as reviewed in Section 2. Just as **Rel** is of independent interest, also $\mathbf{Rel}(\mathbf{C})$ is not just a toy model: we shortly discuss *continuous symmetric encryption* by letting $\mathbf{C}$ consist of compact Hausdorff spaces. For another example see [7].

Section 5 shows that $\mathbf{Rel}(\mathbf{C})$ often has the unusual feature of lacking discernible measurement outcomes, but when $\mathbf{C}$ is a regular *Mal'cev category* it behaves more like **FHilb** than **Rel** in three ways: the *Heisenberg uncertainty* principle, the ability to *broadcast*, and behavedness of *rank one* morphisms. Thus this family of models is genuinely different, and leads to the following scale.

"least quantum"	$\leftrightarrow$	"most quantum"
Rel	$\mathbf{Rel}(\mathbf{C})$	**FHilb**

These properties are stated using the CP construction [16, 22], that makes the Frobenius structures in a category into the objects of a new one. The objects of $\mathbf{CP}(\mathbf{Rel})$ are *groupoids* [20], and Section 3 proves that this holds for $\mathbf{Rel}(\mathbf{C})$ too, for any regular $\mathbf{C}$. Our main result, discussed in Section 4, is that

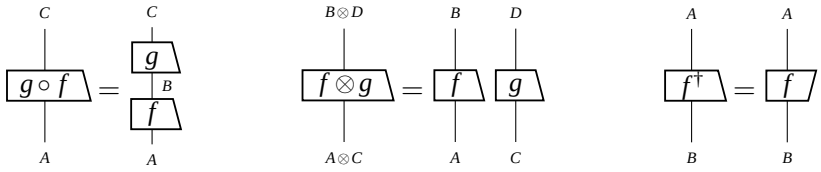
$$\mathbf{CP}(\mathbf{Rel}(\mathbf{C})) \simeq \mathbf{Rel}(\mathbf{Cat}(\mathbf{C})) \tag{1}$$

for regular Mal'cev categories $\mathbf{C}$, whose internal categories $\mathbf{Cat}(\mathbf{C})$ and groupoids are understood. Thus we link the CP passage, from state spaces to algebras of observables, to *categorification*.

*Supported by EPSRC Fellowship EP/L002388/1.
†Supported by EPSRC Studentship OUCL/2014/SET. We thank Bob Coecke and Aleks Kissinger for helpful discussions.

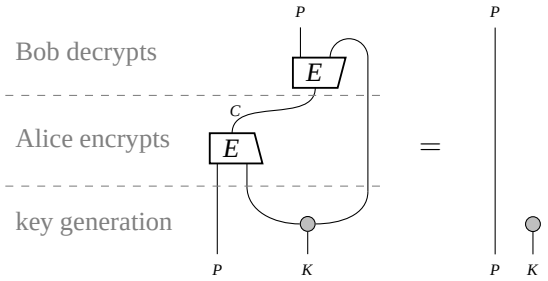
Submitted to:
QPL 2015

Notation We briefly recall the *graphical calculus* for monoidal dagger categories; for more detail, see [26]. Morphisms f are drawn as  ; composition, tensor product, and dagger, as:

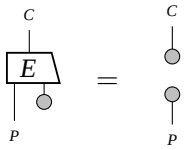


Distinguished morphisms are depicted with special diagrams: the identity $A \to A$ is just the line, $|$; the (identity on) the monoidal unit object I is the empty picture, and the swap map of symmetric monoidal categories becomes $\times$. In particular, we will draw  : $A \otimes A \to A$ and  : $I \to A$ for the multiplication and unit of *Frobenius structures*, made precise in Definition 3.1 below.

Continuous symmetric encryption We now illustrate the utility of $\mathbf{Rel}(\mathbf{C})$ in its own right, not as a toy model. The case $\mathbf{C} = \mathbf{Set}$ can model symmetric encryption [29], and the same techniques apply to any regular $\mathbf{C}$. A *symmetric encryption protocol* in $\mathbf{Rel}(\mathbf{C})$ is specified by an *encryption* morphism $E : M \times K \to E$ relating *plaintext P* and *key K* to *ciphertext C*, satisfying:



The Frobenius structure here is the canonical copying and deleting that is available in $\mathbf{Rel}(\mathbf{C})$ [11]. Equivalently, $(\forall p\colon P, k\colon K)(\exists c\colon C)E(p,k,c)$ and $E(p,k,c) \wedge E(p',k,c) \Rightarrow p = p'$. The protocol is *secure* when no information about plaintext can be deduced from ciphertext without the key:



For example, *one-time pad encryption* is the following secure encryption protocol in **Rel**: take P, K and C to be the set $\{f\colon [1,\ldots,n] \to G\}$ of messages in a given group G of length n, and take E to be the function $E(p,k)(t) = p(t)k(t)$ [29]. A *continuous* version can be described in the category $\mathbf{Rel}(\mathbf{KHaus})$ of relations over compact Hausdorff spaces. An analogue signal is a continuous function from an interval $[0,T] \subseteq \mathbb{R}$ to the unit circle $S^1 \subseteq \mathbb{C}$. Take P, K and C to be the space of such signals (under the product topology) and set $E(p,k)(t) = p(t)k(t)$. The latter protocol is useful when encrypting *e.g.* (continuous) speech rather than (discrete) strings of text, and was proven secure by Shannon himself [28]. [1]

[1] Caveat: the latter protocol requires arbitrary key signals. Practically, Alice could sample her signal at some points, and then transmit using (discrete) one-time pad encryption; Bob can then reconstruct an approximation of the signal. Shannon describes how to generate noise that, when sampled at a given frequency, provides a secure key. Thus the former protocol approximates the latter to any resolution.

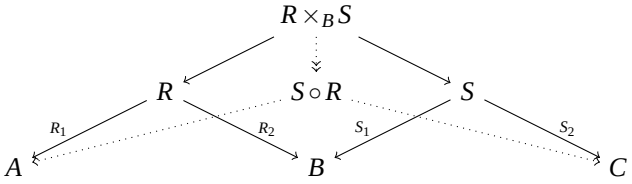
Future work This work is in its early stages, and opens many directions of investigation.

- The *proof technique* of internal (regular) logic is very useful. We intend to develop a *graphical* version, where wires in string diagrams can be annotated with 'elements', and investigate its expressiveness [27].
- The correspondence (1) between groupoids and operator algebra remains to be understood, perhaps through so-called *groupoidification* [24]. If $\mathbf{C}$ is *exact* Mal'cev, so is $\mathbf{Cat}(\mathbf{C})$ [18, 3.2]. Hence $\mathbf{CP}(\mathbf{Rel}(\mathbf{Cat}^n(\mathbf{C}))) \simeq \mathbf{Rel}(\mathbf{Cat}^{n+1}(\mathbf{C}))$, leading to *higher categories*.
- Internal categories in the category of groups are *crossed modules* [8]. Tools from categorical quantum mechanics might shed light on crossed modules, or vice versa. In general, standard notions from categorical quantum mechanics should be investigated in $\mathbf{Rel}(\mathbf{C})$, such as (strong) *complementarity* of Frobenius structures [12].
- Relation-like categories have been axiomatized: as *allegories* by Freyd and Scedrov [17], and as *bicategories of relations* by Carboni and Walters [11]. We hope to extend our study to these more general settings.

2 Categories of relations and regular logic

This section describes regular categories, and their internal regular logic, by way of example; for more information, see [9]. We will be led by the construction of **Rel** from the category **Set** of sets and functions. Of course, both categories have the same objects. The issue is how to describe relations and their composition in terms of functions.

Observe that a relation $R \subseteq A \times B$ induces a pair of functions $R_1 \colon R \to A$ and $R_2 \colon R \to B$, namely $(a,b) \mapsto a$ and $(a,b) \mapsto b$. Moreover, the inclusion $R \hookrightarrow A \times B$ is monic. Equivalently, the two functions R_1, R_2 are *jointly monic*, and conversely, any two jointly monic functions $A \xleftarrow{R_1} R \xrightarrow{R_2} B$ determine a relation $R \subseteq A \times B$. Thus we can describe relations in terms of functions. Composition of relations is given in these terms by pullback:



(2)

The pullback itself is not good enough, as $R \times_B S \to A \times C$ might not be monic. To ensure this, we have to factor that function as a surjection followed by an injection, and consider its image $S \circ R$. Because pullbacks of surjections are surjections, the subobject $S \circ R$ is unique, giving a well-defined category **Rel**.

All in all, we have used the following properties of **Set**: it has products, pullbacks, a way to factorize morphisms as injections after surjections via their images, and stability of surjections under pullback. Generalizing surjections to regular epimorphisms leads to regular categories.

Definition 2.1. An epimorphism is *regular* when it is a coequalizer. The *kernel pair* of a morphism $f \colon A \to B$ is a pullback cone of $A \xrightarrow{f} B \xleftarrow{f} A$. A category is *regular* when it has finite limits, coequalizers of kernel pairs, and regular epimorphisms are stable under pullback.

Example 2.2. Examples of regular categories abound: any topos, such as **Set**; any algebraic variety, such as the categories **Gp** of groups, **Rng** of rings, or $\mathbf{Vect}_k$ of vector spaces; any category monadic over **Set**, such as **KHaus**; any abelian category, such as the category $\mathbf{Mod}_R$ of modules over a ring; any bounded meet-semilattice, considered as a category; any functor category $[\mathbf{C},\mathbf{D}]$ to regular $\mathbf{D}$.

There is another way to consider the construction (2), namely by *regular logic*. This is the fragment of first order logic whose formulae use only the connectives $\exists$ and $\wedge$ and equality. In **Set**, we can describe (2) using a regular formula as

$$S \circ R = \{(a,c) \in A \times C \mid (\exists b \in B)\, R(a,b) \wedge S(b,c)\}. \tag{3}$$

This makes sense in any regular category $\mathbf{C}$: any regular formula ϕ whose function symbols are morphisms in $\mathbf{C}$ and whose relation symbols are subobjects in $\mathbf{C}$ inductively defines a subobject $[\![(a_1,\ldots,a_n) \in A_1 \times \ldots \times A_n \mid \phi]\!] \rightarrowtail A_1 \times \cdots \times A_n$ as follows. Equality $[\![a \in A \mid f(a) = g(a)]\!]$ is interpreted as the equalizer of $f,g\colon A \to B$. Conjunction $[\![a \in A \mid R(a) \wedge S(a)]\!]$ is interpreted as the pullback of $R,S \rightarrowtail A$. Existential quantification $[\![a \in A \mid (\exists b \in B) R(a,b)]\!]$ is interpreted as the image of $R \rightarrowtail A \times B \xrightarrow{\pi_1} A$. This gives two equivalent ways to define our main object of study.

Definition 2.3. Let $\mathbf{C}$ be a regular category. Its category $\mathbf{Rel}(\mathbf{C})$ of relations has the same objects as $\mathbf{C}$, and subobjects $R \rightarrowtail A \times B$ as morphisms $A \to B$, with diagonal maps $A \to A \times A$ as identities, under composition (2), or equivalently $S \circ R = [\![(a,c) \in A \times C \mid (\exists b \in B) R(a,b) \wedge S(b,c)]\!]$.

We denote morphisms in $\mathbf{Rel}(\mathbf{C})$ as $R\colon A \nrightarrow B$, and the corresponding subobject in $\mathbf{C}$ as $R \rightarrowtail A \times B$. The category $\mathbf{Rel}(\mathbf{C})$ is a compact dagger category with the product $\times$ of $\mathbf{C}$ inducing $\otimes$ in $\mathbf{Rel}(\mathbf{C})$ (where it is no longer a cartesian product), and $R^\dagger(b,a) \Leftrightarrow R(a,b)$. Every object A is self-dual with canonical cup $[\![(a,b) \in A \times A \mid a = b]\!]$, and swap maps defined similarly.

Example 2.4. $\mathbf{Rel}(\mathbf{Set})$ is **Rel**, so this is a genuine generalization; $\mathbf{Rel}(\mathbf{Gp})$ has subgroups $R \leq G \times H$ as morphisms $G \to H$; $\mathbf{Rel}(\mathbf{Vect}_k)$ has subspaces $K \leq V \oplus W$ as morphisms $V \to W$ (*cf.* [7]).

Whenever one can derive an implication $\phi \Rightarrow \psi$ in regular logic, it follows that $[\![\phi]\!] \leq [\![\psi]\!]$ as subobjects. This allows us to state and prove (regular) theorems in $\mathbf{Rel}(\mathbf{C})$ as if reasoning in **Rel**. The following lemma works out an example of this technique; the rest of this paper will not be so painstakingly precise. As in **Set**, a relation $R\colon A \nrightarrow A$ is called *symmetric* when $R(a,b) \iff R(b,a)$, *reflexive* when $[\![a \in A \mid R(a,a)]\!] = A$, and *transitive* when $R(a,b) \wedge R(b,c) \Rightarrow R(a,c)$, equivalently $R \circ R \leq R$. A symmetric, reflexive and transitive relation is called an *equivalence relation*. As in any dagger category, a relation is called *positive* when it is of the form $S^\dagger \circ S$ for some relation S.

Lemma 2.5. Any positive relation $R\colon A \nrightarrow A$ in $\mathbf{C}$ regular is symmetric and satisfies $R(a,b) \Rightarrow R(a,a)$.

Proof. Since R is positive we have that $R = S^\dagger \circ S$, for some relation $S : A \nrightarrow B$. Then R is symmetric since $R = S^\dagger \circ S = (S^\dagger \circ S)^\dagger = R^\dagger$. Further,

$$\begin{aligned} R = S^\dagger \circ S &= [\![(a,b) \in A \times A \mid (\exists c \in B)\, S(a,c) \wedge S(b,c)]\!] && \text{(definition of } \circ \text{ and } \dagger) \\ &\leq [\![(a,b) \in A \times A \mid (\exists c \in B)\, S(a,c)]\!] && (\exists \text{ preserves the order of subobjects}) \\ &= [\![(a,b) \in A \times A \mid R(a,a)]\!] \end{aligned}$$

demonstrating that $R(a,b) \Rightarrow R(a,a)$. ∎

3 Groupoids and completely positive maps

Frobenius structures play a central role in categorical quantum mechanics, representing C*-algebras in **FHilb** [30]. In **Rel**, they represent groupoids [20]. Theorem 3.4 below generalizes this to $\mathbf{Rel}(\mathbf{C})$ for any regular $\mathbf{C}$, by noting that the proof can be stated in regular logic.

Definition 3.1. A *special dagger Frobenius structure* in a dagger monoidal category is an object A with morphisms  : $A \otimes A \to A$ and : $I \to A$ satisfying *unitality*, *associativity*, *speciality*, and the *Frobenius law*:

It is *commutative* when  $\circ$  $=$  .

Definition 3.2. An *internal category* in a finitely complete category consists of objects C_0 (objects) and C_1 (morphisms), and morphisms s (source), t (target), u (identity), and m (composition):

$$C_0 \underset{\xleftarrow{s}}{\overset{\xleftarrow{t}}{\xrightarrow{u}}} C_1 \xleftarrow{m} C_1 \times_{C_0} C_1$$

Here $C_1 \times_{C_0} C_1$ is the pullback of s and t. These morphisms must satisfy familiar equations representing associativity of composition and usual behaviour of identities. An *internal functor* between internal categories is a pair of morphisms (f_0, f_1) commuting with the above structure. An *internal groupoid* additionally has an inversion morphism $i\colon C_1 \to C_1$ satisfying usual axioms. We write $\mathbf{Cat}(\mathbf{C})$ and $\mathbf{Gpd}(\mathbf{C})$ for the categories of internal categories and groupoids in $\mathbf{C}$.

Example 3.3. Internal categories or groupoids in **Set** are just (small) categories or groupoids. In $\mathbf{Vect}_k$, internal categories are the same as internal groupoids (see Section 4), and are also called *2-vector spaces* [3, Section 3]. Internal categories in **Gp** are studied under the names *strict 2-groups* [4] and *crossed modules* [25, Section 3.3].

Theorem 3.4. For any regular category $\mathbf{C}$, special dagger Frobenius structures in $\mathbf{Rel}(\mathbf{C})$ are the same as internal groupoids in $\mathbf{C}$. More precisely, a special dagger Frobenius structure $(A, \curlywedge, \circ)$ in $\mathbf{Rel}(\mathbf{C})$ defines an internal groupoid in $\mathbf{C}$ with composition $\curlywedge$ and identities given by $\circ$. Conversely, an internal groupoid $(C_0, C_1, m, s, t, u, i)$ in $\mathbf{C}$ defines a special dagger Frobenius structure $(A, \curlywedge, \circ)$ in $\mathbf{Rel}(\mathbf{C})$ with $A = C_1$, $\circ = (u\colon C_0 \rightarrowtail A)$ and $\curlywedge = (m\colon A \times A \nrightarrow A)$.

Proof. Observe that the proof for the case $\mathbf{C} = \mathbf{Set}$ (see [20, Theorems 7 and 12]) can be carried out entirely in regular logic. For details, see Appendix A. □

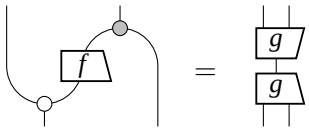
Example 3.5. For any object A of $\mathbf{Rel}(\mathbf{C})$, there is a canonical special dagger Frobenius structure $(A \times A, \curlywedge, \cup)$ which corresponds to the *indiscrete groupoid*

$$A \underset{\xleftarrow{\pi_1}}{\overset{\xleftarrow{\pi_2}}{\xrightarrow{\Delta}}} A \times A \overset{\circlearrowright \sigma}{\xleftarrow{\pi_{1,3}}} A \times A \times A$$

on A, having a unique morphism from a to b for each pair $(a,b) \in A \times A$. The identities are given by the diagonal $\Delta = \langle \mathrm{id}_A, \mathrm{id}_A \rangle\colon A \to A \times A$, while the inversion is the swap $\sigma = \langle \pi_2, \pi_1 \rangle\colon A \times A \to A \times A$.

Dagger Frobenius structures in **C** form the objects of a new category **CP**(**C**) [16, 22]. The key example is that **CP**(**FHilb**) is the category of finite-dimensional C*-algebras and completely positive maps. We briefly recall the relevant form of this *CP construction*; see Appendix B for a proof that this is indeed a well-defined category. Recall that *positive* (endo)morphisms in a dagger category are those the form $g^\dagger \circ g$ for some morphism g.

Definition 3.6. Let **C** be a compact dagger category. Then **CP**(**C**) is the category whose objects are special dagger Frobenius structures $(A, \curvearrowright)$ in **C**, and where morphisms $(A, \curvearrowright) \xrightarrow{f} (B, \curvearrowright)$ are morphisms $A \xrightarrow{f} B$ in **C** whose *Choi matrix* is positive:



for some $g\colon A \otimes B \to X$ in **C**. Such morphisms f are called *completely positive*.

To classify completely positive morphisms in **Rel**(**C**), we need to identify when a relation is positive, *i.e.* of the form $R = [\![(a,c) \in A \times A \mid (\exists b \in B)\, S(a,b) \wedge S(c,b)]\!]$ for some relation $S\colon A \nrightarrow B$. Lemma 2.5 showed that positive relations in any regular category satisfy

$$R(a,b) \Rightarrow R(a,a) \wedge R(b,a). \tag{4}$$

It follows that completely positive morphisms $R\colon (A, \curvearrowright, \circ) \to (B, \curvearrowright, \bullet)$ *respect inverses* [16, 7.2]:

$$R(a,b) \Rightarrow R(a^{-1}, b^{-1}) \wedge R(\mathrm{id}_{\mathrm{dom}(a)}, \mathrm{id}_{\mathrm{dom}(b)}), \tag{5}$$

where $(A, \curvearrowright, \circ)$ and $(B, \curvearrowright, \bullet)$ are regarded as internal groupoids in **C**. However, the converse of either statement need not hold.

Proposition 3.7. The following are equivalent for a regular category:

(a) every reflexive symmetric relation is positive;

(b) a relation is positive if and only if it satisfies (4);

(c) a relation between dagger Frobenius structures is completely positive iff it respects inverses.

Proof. For (a $\Rightarrow$ b), let $R : A \nrightarrow A$ be any relation satisfying (4), and define $U = [\![a \in A \mid R(a,a)]\!]$. Then R restricted to U is reflexive and symmetric, hence equal to $S^\dagger \circ S$ for some relation S. Then R is equal to $S'^\dagger S'$ where $S' = [\![(a,u) \in A \times U \mid (a = U(u)) \wedge S(a)]\!]$.

For (b $\Rightarrow$ c): the Choi matrix S of a relation R is given by $S((a,b),(a',b')) \iff R(a'^{-1} \circ a, b' \circ b^{-1})$, which can be seen to satsify (4) iff R itself respects inverses.

To see (c $\Rightarrow$ a), observe that a reflexive symmetric relation $R \rightarrowtail A \times A$ defines a state R' in **CP**(**Rel**(**C**)) of the special dagger Frobenius structure given by the indiscrete groupoid on A (Example 3.5). Positivity of the Choi matrix of R' in this case means that R is itself positive. □

A category satisfying the properties of the previous proposition is called *positively regular*. We can now generalize the known description of **CP**(**Rel**) of [16, Proposition 7.3].

Corollary 3.8. Let **C** be a positively regular category. Then **CP**(**Rel**(**C**)) is equivalent to the category of groupoids and relations in **C** that respect inverses. □

Example 3.9. Set is positively regular, since any relation R satisfying (4) is equal to $S^\dagger \circ S$ with $S = \{(a,a,b),(a,b,a) \mid R(a,b)\}$. More generally, any coherent category, such as **KHaus**, is positively regular and hence so is any topos. Section 4 will show that **Gp** and $\mathbf{Vect}_k$ are positively regular.

The category of semigroups satisfying $(\forall x,y)\, xyx = yxy$ is regular but not positively regular; positive relations satisfy $R(a,b) \wedge R(c,d) \Rightarrow R(acb, dbc)$, but relations satisfying (4) need not.

4 Mal'cev categories

This section studies a broad class of regular categories for which the CP construction takes a very natural form, allowing us to bypass the unusual notion of a relation respecting inverses.

Definition 4.1. A category $\mathbf{C}$ with finite limits is a *Mal'cev category* if every reflexive relation $R \rightarrowtail A \times A$ in $\mathbf{C}$ is an equivalence relation.

Proposition 4.2. The following are equivalent for a regular category:

(a) inverse-respecting subobjects $R \rightarrowtail A_1$ of internal groupoids are closed under composition;

(b) every relation $R \rightarrowtail A \times A$ is *difunctional*: $(\forall a,b,c,d \in A)\, R(a,b) \wedge R(c,b) \wedge R(c,d) \Rightarrow R(a,d)$;

(c) the category is Mal'cev.

Proof. For (a $\Rightarrow$ b), let $R \rightarrowtail A \times A$ be a relation. Define a new relation $S \rightarrowtail R \times R$ by setting $S((a,b),(c,d)) \Leftrightarrow R(a,d) \wedge R(c,b)$. Then S is reflexive, because it is defined on R, and symmetric. Thus S defines an inverse-respecting subobject of the indiscrete groupoid on R, and hence is closed under composition in $R \times R$. That is, S is transitive. Now suppose $R(a,b)$, $R(c,b)$, and $R(c,d)$. Then $S((a,b),(c,b))$ and $S((c,b),(c,d))$, hence $S((a,b),(c,d))$, and so $R(a,d)$.

To see (b $\Rightarrow$ a), consider an inverse-respecting subobject $R \rightarrowtail A_1$, and set $S = [\![(a,b) \in A_1 \times A_1 \mid (\mathrm{dom}(a) = \mathrm{cod}(b)) \wedge R(a,b)]\!]$. For composable a and b in A_1, let $x = \mathrm{dom}(a) = \mathrm{cod}(b)$. Since R is closed under $\mathrm{id}_{\mathrm{dom}(-)}$ and $\mathrm{id}_{\mathrm{cod}(-)}$, we have $S(\mathrm{id}_x, b)$, $S(a, \mathrm{id}_x)$, and $S(\mathrm{id}_x, \mathrm{id}_x)$. Now $S(a,b)$ by difunctionality, that is, $R(a \circ b)$, so R is closed under composition.

Finally, (b $\Leftrightarrow$ c) is well-known [10, Proposition 1.2]. □

Example 4.3. Mal'cev categories were first studied in the context of universal algebra. An algebraic variety is Mal'cev precisely when it contains an operation $p(x,y,z)$ with $p(x,y,y) = p(y,y,x) = x$. Hence the categories $\mathbf{Gp}$ and $\mathbf{Vect}_k$ are regular Mal'cev, as are the categories of Lie algebras, abelian groups, rings, commutative rings, associative algebras, quasi-groups and Heyting algebras. Any abelian category such as $\mathbf{Mod}_R$ is Mal'cev. The opposite category of any topos is regular Mal'cev.

In a Mal'cev category $\mathbf{C}$, the forgetful functor $\mathbf{Gpd}(\mathbf{C}) \to \mathbf{Cat}(\mathbf{C})$ is an isomorphism, that is, every internal category in $\mathbf{C}$ uniquely defines an internal groupoid [10, Theorem 2.2]. Moreover, $\mathbf{Gpd}(\mathbf{C})$ is regular when $\mathbf{C}$ is Mal'cev [18, Proposition 3.1 and Theorem 3.2]. In this case $\mathbf{Rel}(\mathbf{Gpd}(\mathbf{C}))$, which we now describe, makes sense. By contrast, $\mathbf{Rel}(\mathbf{Gpd}(\mathbf{Set}))$ is ill-defined.

Lemma 4.4. Let $\mathbf{C}$ be a regular category. Subobjects of (A_0, A_1) in $\mathbf{Gpd}(\mathbf{C})$ are subobjects $R \rightarrowtail A_1$ in $\mathbf{C}$ that are closed under $\mathrm{id}_{\mathrm{dom}(-)}$, inverses, and composition.

Proof. Morphisms $f = (f_0, f_1)\colon (C_0, C_1) \to (D_0, D_1)$ in $\mathbf{Gpd}(\mathbf{C})$ are determined by morphisms $f_1\colon C_1 \to D_1$ respecting the groupoid structure, since f_0 can be reconstructed as $c \mapsto \mathrm{dom}(f_1(\mathrm{id}_c))$ for $c \in C_0$. Now $K_1 = [\![(x,y) \in C_1 \times C_1 \mid\ f_1(x) = f_1(y)]\!]$ determines a subgroupoid $K \leq C \times C$, with $f \circ \pi_1 = f \circ \pi_2\colon K \to D$. If f is monic in $\mathbf{Gpd}(\mathbf{C})$, then $\pi_1 = \pi_2$ and so f_1 is monic in $\mathbf{C}$. □

Theorem 4.5. Regular Mal'cev categories are positively regular. Conversely, a positively regular category $\mathbf{C}$ is Mal'cev if and only if Corollary 3.8 provides equivalences

$$\mathbf{CP}(\mathbf{Rel}(\mathbf{C})) \simeq \mathbf{Rel}(\mathbf{Gpd}(\mathbf{C})) \simeq \mathbf{Rel}(\mathbf{Cat}(\mathbf{C})).$$

Note that $\mathbf{Rel}(\mathbf{Gpd}(\mathbf{C}))$ and $\mathbf{Rel}(\mathbf{Cat}(\mathbf{C}))$ are ill-defined for general positively regular $\mathbf{C}$.

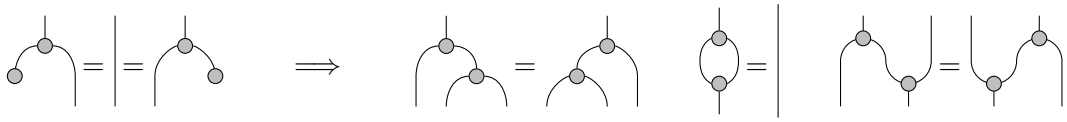
Proof. For the first statement, let R be any reflexive symmetric relation in a regular Mal'cev category. Then R is an equivalence relation and hence satisfies $R = R^\dagger \circ R$, making it positive.

Now let $\mathbf{C}$ be a positively regular category. By Corollary 3.8, $\mathbf{CP}(\mathbf{Rel}(\mathbf{C}))$ is equivalent to the category of groupoids and relations that respect inverses. By Lemma 4.4 and Proposition 4.2, the forgetful functor from $\mathbf{Rel}(\mathbf{Gpd}(\mathbf{C}))$ to this category is (well-defined and) an isomorphism if and only if $\mathbf{C}$ is Mal'cev, in which case $\mathbf{Gpd}(\mathbf{C})$ is isomorphic to $\mathbf{Cat}(\mathbf{C})$. □

Example 4.6. We may read the previous theorem as saying that the CP construction, usually taken to add mixed states and processes to pure quantum theory, can be regarded as a process of *categorification* in a broad class of categories of relations. The category $\mathbf{Cat}(\mathbf{Gp})$ of strict 2-groups is equivalent to the category $\mathbf{CrMod}$ of crossed modules, whence $\mathbf{CP}(\mathbf{Rel}(\mathbf{Gp})) \simeq \mathbf{Rel}(\mathbf{CrMod})$. Similarly, $\mathbf{CP}(\mathbf{Rel}(\mathbf{Vect}_k))$ is equivalent to the category of relations in 2-vector spaces.

Next we observe that, in any Mal'cev regular category, just as every internal category is in fact a groupoid, there is also redundancy in the definition of a dagger Frobenius structure.

Theorem 4.7. If $\mathbf{C}$ is a regular Mal'cev category, any pair of morphisms $\mu\colon A \otimes A \to A$, $\eta\colon I \to A$ in $\mathbf{Rel}(\mathbf{C})$ satisfying unitality form the composition and identities of an internal category in $\mathbf{C}$, or equivalently a dagger special Frobenius structure in $\mathbf{Rel}(\mathbf{C})$.



Proof. Since any internal category in $\mathbf{C}$ is a groupoid, the second statement follows from Theorem 3.4. Let $\mu = (M\colon A \times A \nrightarrow A)$ and $\eta = (U\colon I \nrightarrow A)$. Then unitality corresponds to the formulae

$$(\exists x \in U)\ M(x,a,a') \iff a = a' \tag{U1}$$

$$(\exists x \in U)\ M(a,x,a') \iff a = a' \tag{U2}$$

We will first show that M is single-valued as a relation. Suppose that both $M(a,b,c)$ and $M(a,b,d)$, then by (U1) $(\exists x \in U)\ M(c,x,c)$, and applying difunctionality we have $M(c,x,d)$ and so $c = d$. In any regular category, such a relation is represented by a subobject of the form $(A \times A \leftarrowtail B \xrightarrow{m} A)$ in $\mathbf{C}$, where $B = [\![(a,b) \in (A \times A) \mid (\exists c \in A)\ M(a,b,c)]\!]$; see [9, Lemma 2.8]. Write $(a,b)\!\downarrow$ for $B(a,b)$. Define the following relations in $\mathbf{C}$:

$$S = [\![(a,x) \in A \times U \mid (a,x)\!\downarrow]\!]\colon A \nrightarrow U \tag{6}$$

$$T = [\![(a,y) \in A \times U \mid (y,a)\!\downarrow]\!]\colon A \nrightarrow U \tag{7}$$

just as in [20, Definition 2]. Now S is total, by (U2), and single-valued since if $M(a,x,a)$ and $M(a,y,a)$ for x, y in U, then since unitality gives $M(x,x,x)$ we have $M(x,y,x)$ by difunctionality, and so $x = y$. The same holds for T, and so S, T correspond to morphisms s, t in $\mathbf{C}$ defining the data of an internal category

$$U \underset{s}{\overset{t}{\leftleftarrows\!\rightarrow}} A \xleftarrow{\ m\ } A \times_U A = B$$

where it remains to show that B is in fact a pullback of s and t, *i.e.* $(a,b)\!\downarrow$ if and only if $s(a) = t(b)$. Suppose that $(a,b)\!\downarrow$ and $s(a) = x$. Then we have $(a,b)\!\downarrow$, $(a,x)\!\downarrow$, $(x,x)\!\downarrow$ and hence $(x,b)\!\downarrow$ by difunctionality. Conversely, $(x,b)\!\downarrow$, $(a,x)\!\downarrow$, and $(x,x)\!\downarrow$ implies that $(a,b)\!\downarrow$. Finally, in [10, Theorem 2.2] it is shown that, in any Mal'cev category, all of the equations required of an internal category follow automatically whenever $m(a,s(a)) = a$, $m(t(a),a) = a$, and $s(x) = x = t(x)$ for all $a \in A$ and $x \in U$. □

Note that unitality is a property of  alone, since we must have  $= [\![a \in A \mid$ $(a,a,a)]\!]$.

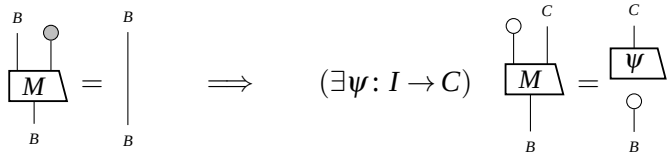
Example 4.8. Crossed modules are known to have numerous equivalent descriptions, as groups in **Cat** or **Gpd**, and as categories or groupoids in **Gp** [25, 3.1] [4]. We can now add that a crossed module is just a unital morphism in **Rel**(**Gp**). Similarly, a 2-vector space is simply a unital morphism in **Rel**($\mathbf{Vect}_{\mathbf{K}}$).

5 Quantum properties of Rel(C)

The category **Rel** of sets and relations is compact dagger, like **FHilb**, but fails to satisfy many properties that are seen as typical to quantum theory. This section presents three such properties of **FHilb** that fail in **Rel** but hold in **Rel**(**C**) whenever **C** is a regular Mal'cev category. In this sense **Rel**(**C**) is a 'more quantum' model than **Rel** for regular Mal'cev categories **C**. We conclude by countering this with some non-quantum features of our main **Rel**(**C**) examples not shared by **Rel**.

Heisenberg uncertainty The Heisenberg uncertainty principle states that no information can be obtained from a quantum system without disturbing its state [19, Section 5.2]. To model it categorically, we need an appropriate notion of quantum system. Following [16], we will take *quantum structures* to be special dagger Frobenius structure of the form $B = (A^* \otimes A, d \bigcirc, d^{-1} \cup)$, where the scalar $d\colon I \to I$ is invertible. In **FHilb**, these correspond to the C*-algebras $\mathbb{M}_n$ of n-by-n matrices. In **Rel**(**C**) for regular **C**, these correspond to indiscrete groupoids on A (see Example 3.5). We model the principle contrapositively as follows, abstracting the fact that POVMs on a Hilbert space A with n outcomes are precisely morphisms $B \to B \otimes C$ in $\mathbf{CP}^*[\mathbf{C}]$, where C is a commutative special dagger Frobenius structure on $\mathbb{C}^n$.

Definition 5.1. A compact dagger category satisfies the *Heisenberg uncertainty principle* when the following holds for any quantum structure $(B,$ $,$ $)$, any commutative special dagger Frobenius structure $(C,$ $,$ $)$, and any completely positive morphism $M\colon B \to B \otimes C$:



(8)

The category **FHilb** satisfies the Heisenberg uncertainty principle [23, Section 6.3].

Lemma 5.2. The category **Rel** does not satisfy the Heisenberg uncertainty principle.

Proof. Let A be the indiscrete groupoid on the two-element set $\{x,y\}$, and let B be the group $\mathbb{Z}_2 = \{0,1\}$, regarded as a groupoid. The inverse-respecting relation

$$M = \{(a,a,0)) \mid a \in A\} \cup \{((x,x),(x,x),1))\} \subseteq A \times (A \times B).$$

satisfies $M((x,x),(x,x),1)$ but not $M((y,y),(y,y),1)$. □

Proposition 5.3. Let **C** be a regular Mal'cev category. Then **Rel**(**C**) satisfies the Heisenberg uncertainty principle for any quantum structure $(B,$ $,$ $)$ and *any* special dagger Frobenius structure $(C,$ $,$ $)$.

Proof. Regard M as a relation $M \rightarrowtail (A \times A) \times (A \times A) \times C$, where B is the indiscrete groupoid on A. Suppose M satisfies the left-hand side of (8), so that

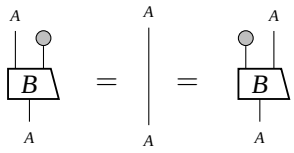
$$(\exists x \in C)\ M((a,a'),(b,b'),\mathrm{id}_{\mathrm{dom}(x)}) \iff (a,a') = (b,b'). \tag{9}$$

We wish to show $(\exists b \in A)\ M((a,a'),(b,b),x) \iff a = a' \wedge \psi(x)$ for some $\psi \rightarrowtail C$. Define the new relation $T = [\![(a,x) \in A \times C \mid M((a,a),(a,a),x)]\!]$. Then by (9) and closure of M under $\mathrm{id}_{\mathrm{dom}}$ and $\mathrm{id}_{\mathrm{cod}}$, we have $(\exists b \in A)\ M((a,a'),(b,b),x)$ if and only if $(a = a') \wedge T(a,x)$. It suffices to show that $T(a,x)$ holds precisely when $(\exists a' \in A)\ T(a',x)$, because we may then take $\psi = [\![x \in C \mid (\exists a \in A)\ T(a,x)]\!]$.

Once more using (9) and closure of M under $\mathrm{id}_{\mathrm{dom}}$ and $\mathrm{id}_{\mathrm{cod}}$, observe that $(\forall a,a' \in A)\ (\exists x \in C)$ such that $T(a,x) \wedge T(a',x)$. Hence if $T(a',x)$ holds then $(\exists y \in C)\ T(a,y) \wedge T(a',y) \wedge T(a',x)$ and so by difunctionality $T(a,x)$ holds, as desired. □

Broadcasting While statistical mechanics includes its own version of the no-cloning theorem, it has instead been argued that one of the unique features of classical systems is in their capacity to be *broadcast* [5]. We now capture this property categorically, following [16].

Definition 5.4. Let **C** be a compact dagger category. A *broadcasting map* for an object $(A, \curlywedge)$ of $\mathbf{CP}(\mathbf{C})$ is a morphism $A \xrightarrow{B} A \otimes A$ in $\mathbf{CP}(\mathbf{C})$ satisfying:



Any commutative dagger Frobenius structure in **C** has a broadcasting map $\curlyvee$, which can be shown to be completely positive. We say **C** satisfies the *no-broadcasting principle* if the converse holds.

The category **FHilb** satisfies the no-broadcasting principle [6].

Lemma 5.5. [21] The category **Rel** does not satisfy the no-broadcasting principle.

Proof. Let G be a nonabelian group, and regard it as a groupoid (G_0, G_1). Define a morphism $B\colon G_1 \times G_1 \to G_1$ in **Rel** by $B = \{(g, \mathrm{id}_{\mathrm{dom}(g)}, g) \mid g \in G_1\} \cup \{(g,g,\mathrm{id}_{\mathrm{dom}(g)}) \mid g \in G_1\}$. This relation respects inverses, so is a morphism of $\mathbf{CP}(\mathbf{Rel})$. It is also a broadcasting map since $(\exists x \in G_0)\ B(g, \mathrm{id}_x, h) \iff (\exists x \in G_0)\ B(g,h,\mathrm{id}_x) \iff g = h$ for $g,h \in G_1$. □

Proposition 5.6. For **C** regular Mal'cev, $\mathbf{Rel}(\mathbf{C})$ satisfies the no-broadcasting principle.

Proof. Suppose $B \rightarrowtail A \times A \times A$ in $\mathbf{CP}(\mathbf{Rel}(\mathbf{C}))$ is broadcasting. Then:

$$(\exists x \in A)\ B(a, \mathrm{id}_{\mathrm{dom}(x)}, a') \iff a = a' \iff (\exists x \in A)\ B(a, a', \mathrm{id}_{\mathrm{dom}(x)}) \tag{10}$$

Use closure of B under identities and inverses to show that, in any regular category **C**, (10) implies $(\forall a \in A)\ \mathrm{dom}(a) = \mathrm{cod}(a)$. Now, arguing in the internal logic of **C**, let $a, a' \in A$ be such that $\mathrm{dom}(a) = \mathrm{dom}(a')$, so that $B(a, \mathrm{id}_{\mathrm{dom}(a)}, a)$ and $B(a', a', \mathrm{id}_{\mathrm{dom(a)}})$. Since **C** is Mal'cev, B is closed under composition in A by Proposition 4.2, and so $B(a \circ a' \circ a^{-1}, a', \mathrm{id}_{\mathrm{dom}(a)})$. Hence $a \circ a' = a' \circ a$ by (10). □

Rank The third property we discuss concerns the linear structure of quantum theory. Due to this structure, morphisms in **FHilb** come with a notion of rank. Rays, morphisms of rank at most one, are reflected in the graphical calculus by disconnectedness.

Definition 5.7. We say a monoidal dagger category satisfies the *bottleneck principle* if morphisms R factor through I whenever $R^\dagger \circ R$ does so:

$$(\exists \psi, \phi \colon I \to A) \quad \begin{array}{c} A \\ | \\ R \\ | \\ R \\ | \\ A \end{array} \quad = \quad \begin{array}{c} A \\ | \\ \psi \\ | \\ \phi \\ | \\ A \end{array} \quad \Longrightarrow \quad (\exists \phi \colon I \to A, \psi \colon I \to B) \quad \begin{array}{c} B \\ | \\ R \\ | \\ A \end{array} \quad = \quad \begin{array}{c} B \\ | \\ \psi \\ | \\ \phi \\ | \\ A \end{array}$$

The category **FHilb** clearly satisfies the bottleneck principle, because $\operatorname{rank}(f^\dagger \circ f) = \operatorname{rank}(f)$.

Lemma 5.8. The category **Rel** does not satisfy the bottleneck principle.

Proof. Let $B = \{0,1\}$, and consider the relation $R \colon B \nrightarrow B$ given by $R = \{(0,0),(0,1),(1,1)\}$. Now $R^\dagger \circ R$ splits as the product relation $B \times B$, but R cannot be written as a product of subsets of B. □

The previous lemma leads to unusual behaviour from a quantum perspective in **Rel**. For example, taking the partial trace of an entangled state Ψ can result in a pure state:

$$\begin{array}{c} \Psi \quad \Psi \end{array} \quad = \quad \begin{array}{c} \psi \quad \psi \end{array}$$

which cannot occur for entangled states in **FHilb**.

Lemma 5.9. The category $\mathbf{Rel}(\mathbf{C})$ satisfies the bottleneck principle for regular Mal'cev categories $\mathbf{C}$.

Proof. A relation $R \colon A \nrightarrow B$ disconnecting in the above sense means $R(a,b) \wedge R(a',b') \Rightarrow R(a,b')$, in which case $R(a,b) \iff (\exists a' \in A) R(a',b) \wedge (\exists b' \in B) R(a,b')$. Suppose $R^\dagger \circ R$ splits as in the left-hand side of Definition 5.7, and assume $R(a,b)$ and $R(a',b')$; we will show that $R(a,b')$. It follows from $(R^\dagger \circ R)(a,a)$ and $(R^\dagger \circ R)(a',a')$ that $(R^\dagger \circ R)(a,a')$, that is, $(\exists e \in A)\ R(a,e) \wedge R(a',e)$. But then $R(a,e)$, $R(a',e)$ and $R(a',b')$, and so $R(a,b')$ holds by difunctionality. □

Projections To finish, we show that the models $\mathbf{Rel}(\mathbf{C})$ for regular Mal'cev $\mathbf{C}$, despite the above results, have some non-quantum features distinguishing them from **FHilb**. For example, by Proposition 4.2, any state $\psi \colon I \to (A, \curlywedge)$ in $\mathbf{CP}(\mathbf{Rel}(\mathbf{C}))$ is a *projection* [15, Definition 3.1]:

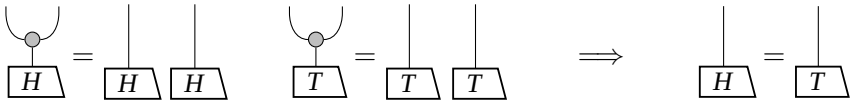
$$\begin{array}{c} A \\ \curlywedge \\ \psi \quad \psi \end{array} \quad = \quad \begin{array}{c} A \\ | \\ \psi \end{array} \quad = \quad \begin{array}{c} \psi \quad A \\ \curlyvee \end{array}$$

This is not the case in **FHilb**, where, up to scalar factors, the projections of a quantum structure are precisely projections in the usual sense, while states are arbitrary density matrices.

Unique measurement outcomes Another more striking difference from **FHilb** is that many of the categories **Rel**(**C**) lack distinct classical outcomes of experiments. These outcomes are represented categorically by states copied by the map $\curlyvee$ of a commutative Frobenius structure [13].

We call an object A of a regular category **C** *inhabited* if $[\![\exists a \in A]\!] = \mathrm{id}_1 : 1 \rightarrowtail 1$, and **C** *entirely inhabited* when this holds for all objects. Equivalently, any subobject of a terminal object 1 is isomorphic to 1.

Proposition 5.10. Let **C** be an entirely inhabited regular category. Then any two copyable states H, T of a special dagger Frobenius structure $(A, \curlyvee)$ in **Rel**(**C**) are equal.



Proof. Arguing just as in **Rel**(**Set**), any copyable state H of an internal groupoid $(A, \curlyvee)$ is easily seen to satisfy $\mathrm{dom}(a) = \mathrm{cod}(a')$ for all its members a, a', and $(\mathrm{dom}(a) = \mathrm{dom}(b)) \wedge H(b) \implies H(a)$ for any a, b in A. Now by assumption $H \wedge T$ is inhabited, meaning $(\exists b \in A)\ H(b) \wedge T(b)$. Hence $T(a)$ implies that $\mathrm{dom}(a) = \mathrm{dom}(b)$ with b in H, and so $H(a)$ holds also. □

Example 5.11. Any regular category with a zero object is entirely inhabited. This includes any abelian category, along with our main examples of Mal'cev categories **Gp** and $\mathbf{Vect}_k$. Hence these categories will be unable to model protocols which require distinct copyable states to represent classical bits. An 'ideal' choice of **C** for a toy model would be Mal'cev regular, while not being entirely inhabited: the category of quasi-groups provides such an example.

References

[1] S. Abramsky & B. Coecke (2004): *A categorical semantics of quantum protocols*. In: *Logic in Computer Science 19*, IEEE Computer Society, pp. 415–425, doi:10.1109/lics.2004.1319636.

[2] J.C. Baez (2006): *The structural foundations of quantum gravity*, chapter Quantum quandaries: a category-theoretic perspective, pp. 240–266. Oxford University Press, doi:10.1093/acprof:oso/9780199269693.003.0008.

[3] J.C. Baez & A.S. Crans (2004): *Higher-dimensional algebra VI: Lie 2-algebras*. *Theory and Applications of Categories [electronic only]* 12, pp. 492–538. Available at http://eudml.org/doc/124264.

[4] J.C. Baez & A.D. Lauda (2004): *Higher-dimensional algebra. V: 2-Groups. Theory and Applications of Categories [electronic only]* 12, pp. 423–491. Available at http://eudml.org/doc/124217.

[5] H. Barnum, J. Barrett, M. Leifer & A. Wilce (2007): *Generalized No-broadcasting theorem*. *Physical Review Letters* 99(24), pp. 1–4, doi:10.1103/PhysRevLett.99.240501.

[6] H. Barnum, C.M. Caves, C. a. Fuchs, R. Jozsa & B. Schumacher (1996): *Noncommuting Mixed States Cannot Be Broadcast*. *Phys. Rev. Lett.* 76(2818), doi:10.1103/PhysRevLett.76.2818.

[7] F. Bonchi, P. Sobociński & F. Zanasi (2014): *A Categorical Semantics of Signal Flow Graphs*. In: *CONCUR 2014, Lecture Notes in Computer Science* 8704, Springer, pp. 435–450, doi:10.1007/978-3-662-44584-6_30.

[8] R. Brown (1999): *Groupoids and crossed objects in algebraic topology*. *Homology, Homotopy and Applications* 1(1), pp. 1–78, doi:10.4310/hha.1999.v1.n1.a1.

[9] C. Butz (1998): *Regular Categories and Regular Logic*. *BRICS Lecture Series LS-98-2*, p. 46. Available at http://www.brics.dk/LS/98/2/BRICS-LS-98-2.pdf.

[10] A. Carboni, M.C. Pedicchio & N. Pirovano (1991): *Internal Graphs and Internal Groupoids in Mal'cev Categories*. *Category Theory 1991: Proceedings of an International Summer Category Theory*.

[11] A. Carboni & R.F.C. Walters (1987): *Cartesian bicategories I*. *Journal of Pure and Applied Algebra* 49, pp. 11–32, doi:10.1016/0022-4049(87)90121-6.

[12] B. Coecke & R. Duncan (2011): *Interacting Quantum Observables*. *New Journal of Physics* 13(4), p. 043016, doi:10.1007/978-3-540-70583-3_25.

[13] B. Coecke & R. Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. *New Journal of Physics* 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016.

[14] B. Coecke & B. Edwards (2011): *Toy quantum categories*. In: *Quantum Physics and Logic 2008, ENTCS*, 270, pp. 29–40, doi:10.1016/j.entcs.2011.01.004.

[15] B. Coecke, C. Heunen & A. Kissinger (2013): *Compositional Quantum Logic*. In B. Coecke, L. Ong & P. Panangaden, editors: *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky*, *Lecture Notes in Computer Science* 7860, Springer Berlin Heidelberg, pp. 21–36, doi:10.1007/978-3-642-38164-5_3.

[16] B. Coecke, C. Heunen & A. Kissinger (2014): *Categories of quantum and classical channels*. *Quantum Information Processing*, pp. 1–31, doi:10.1007/s11128-014-0837-4.

[17] P. Freyd & A. Scedrov (1990): *Categories, allegories*. 39, Elsevier, doi:10.5860/choice.29-2765.

[18] M. Gran (1999): *Internal categories in Malcev categories*. *Journal of Pure and Applied Algebra* 143(1-3), pp. 221–229, doi:10.1016/S0022-4049(98)00112-1.

[19] T. Heinosaari & M. Ziman (2012): *The mathematical language of quantum theory*. Cambridge University Press, doi:10.1017/cbo9781139031103.

[20] C. Heunen, I. Contreras & A. S. Cattaneo (2013): *Relative Frobenius algebras are groupoids*. *Journal of Pure and Applied Algebra* 217(1), pp. 114 – 124, doi:10.1016/j.jpaa.2012.04.002.

[21] C. Heunen & A. Kissinger (2015): *Can quantum theory be characterized by information-theoretic constraints? in preparation.*

[22] C. Heunen, A. Kissinger & J. Vicary (2015): *Faces of complete positivity*. *in preparation.*

[23] H. Maassen (2010): *Quantum Information, Computation and Cryptography*, chapter Quantum Probability and Quantum Information, pp. 65–108. *Lecture Notes in Physics* 808, Springer, doi:10.1007/978-3-642-11914-9_3.

[24] J. C. Morton (2011): *Two-vector spaces and groupoids*. *Applied Categorical Structures* 19(4), pp. 659–707, doi:10.1007/s10485-010-9225-0.

[25] B. Noohi (2007): *Notes on 2-groupoids, 2-groups and crossed modules*. *Homology, Homotopy and Applications* 9(1), pp. 75–106, doi:10.4310/HHA.2007.v9.n1.a3.

[26] P. Selinger (2009): *A survey of graphical languages for monoidal categories*. In: *New Structures for Physics*, Lecture Notes in Physics, Springer, pp. 289–355, doi:10.1007/978-3-642-12821-9_4.

[27] P. Selinger (2012): *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. *Logical Methods in Computer Science* 8(3), p. 6, doi:10.2168/lmcs-8(3:6)2012.

[28] C.E. Shannon (1943): *Analogue of the Vernam System for Continuous Time Series*. *Memorandum MM 43-110-44, Bell Laboraties*, doi:10.1109/9780470544242.ch3.

[29] M. Stay & J. Vicary (2013): *Bicategorical semantics for nondeterministic computation*. *Electronic Notes in Theoretical Computer Science* 298, pp. 367–382, doi:10.1016/j.entcs.2013.09.022.

[30] J. Vicary (2011): *Categorical formulation of finite-dimensional quantum algebras*. *Communications in Mathematical Physics* 304(3), pp. 765–796, doi:10.1007/s00220-010-1138-0.

A Proof of Theorem 3.4 for regular categories

Proof. Let $\mathbf{C}$ be regular and let $(A, \curlywedge, \bullet)$ be a special dagger Frobenius structure in $\mathbf{Rel}(\mathbf{C})$, with $\curlywedge = (M\colon A \times A \nrightarrow A)$, and $\bullet = (U \rightarrowtail A)$. We already saw how unitality is interpreted as the two regular formulae (U1), and (U2), while the other equations of Definition (3.1) translate into:

$$(\exists e \in A)\ M(a,b,e) \wedge M(e,c,d) \iff (\exists e \in A)\ M(a,e,d) \wedge M(b,c,e) \tag{A}$$

$$(\exists b \in A)(\exists c \in A)\ M(b,c,a) \wedge M(b,c,a') \iff a = a' \tag{S}$$

$$(\exists e \in A)\ M(a,e,c) \wedge M(e,d,b) \iff (\exists e \in A)\ M(c,e,a) \wedge M(e,b,d) \tag{F}$$

We follow the same proof strategy as in Theorem 4.7. It follows from (S) that M is single-valued as a relation and hence corresponds to a subobject of the form $(A \times A \leftarrowtail B \xrightarrow{m} A)$ in $\mathbf{C}$. Again, we write $(a,b)\!\downarrow$ for $B(a,b)$, so that $M(a,b,c)$ means that $(a,b)\!\downarrow$ and $m(a,b) = c$, and define relations $S : A \nrightarrow U$, $T : A \nrightarrow U$ by (6) and (7), as well as

$$I = [\![(a,b) \in A \times A \mid (\exists x \in U)(\exists y \in U)\ M(a,b,x) \wedge M(b,a,y)]\!] \colon A \nrightarrow A$$

It suffices to show these relations are total and single-valued, as they then correspond uniquely to morphisms s, t and i in $\mathbf{C}$ defining the data of an internal groupoid

$$U \underset{s}{\overset{t}{\leftleftarrows}} A \overset{i}{\circlearrowright},\quad A \xleftarrow{m} A \times_U A = B$$

where we must also show that B is in fact a pullback of s and t.

From the unit laws (U1), (U2) and associativity (A), deduce that elements of U only compose when they are equal, and then that if $(a,x)\!\downarrow$ and $(a,y)\!\downarrow$ we have $(x,y)\!\downarrow$ by associativity, and so $x = y$. Hence S is total and single-valued, as is T similarly. The special case of (F) in which $b = s(a)$, $c = t(a)$ and $d = a$ shows that I is total:

$$(\exists e \in A)\ M(a,e,s(a)) \wedge M(e,a,t(a)),$$

that is, 'every morphism has an inverse'. Uniqueness of inverses then follows as for any category, once we have shown that the composition m is associative. Writing a^{-1} for any inverse of a, associativity (A) gives $m(a^{-1},a) = s(a)$, and it follows that a and b are composable whenever $s(a) = t(b)$. Conversely, when a and b are composable, $m(a,b) = m(m(a,s(a)),b) = m(a,m(s(a),b))$ by (A) and so $s(a) = t(b)$. Hence B is indeed the pullback of s and t.

It remains to verify that these morphisms satisfy the equations defining an internal groupoid. Associativity of m only requires further that $(a,b)\!\downarrow$ and $(b,c)\!\downarrow$ imply $(m(a,b),c)\!\downarrow$. From (A) we find that $(m(a,b),s(b))\!\downarrow$ whenever a and b compose, and hence $s(m(a,b)) = s(b)$ as desired. Finally, that inverses behave as expected follows from the definition of I.

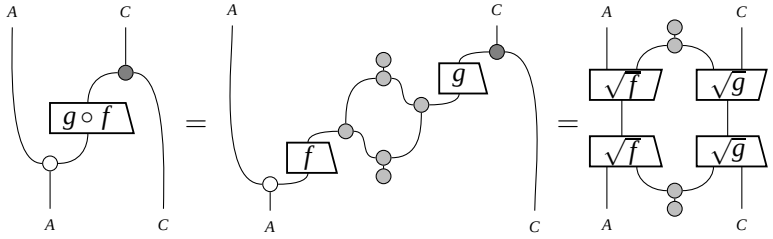
Thus any dagger special Frobenius structure in $\mathbf{Rel}(\mathbf{C})$ defines an internal groupoid in $\mathbf{C}$. Note also that this is the only possible choice of s, t and i compatible with M and U since any groupoid operations must satisfy the formulae defining S, T and I.

Conversely, given any internal groupoid $(C_0, C_1, m, s, t, u, i)$ in $\mathbf{C}$, we must show that $M = \curlywedge = (m\colon C_1 \times C_1 \nrightarrow C_1)$ and $U = \bullet = (u\colon C_0 \rightarrowtail C_1)$ satisfy the formulae (S), (A), (U1), (U2), and (F). Speciality (S) simply states that the relation $\curlywedge$ is single-valued and surjective, which holds since $m(a,s(a)) = a$ for any a in C_1. Equation (A) follows from associativity of composition m. Unitality (U1) and (U2) follows from the equations satisfied by u, s and t. Finally, the Frobenius law (F) simply amounts to the statement that $m(a^{-1},c) = m(b,d^{-1})$ if and only if $m(c^{-1},a) = m(d,b^{-1})$. □

B The category CP(C)

Proposition B.1. The category **CP**(**C**) is well-defined.

Proof. It inherits identities and composition from **C**. What we have to show is that composition is well-defined. Suppose that the Choi matrices of both morphisms $(A,\cup,\cdot) \xrightarrow{f} (B,\cup,\cdot) \xrightarrow{g} (C,\cup,\cdot)$ are positive, say with square roots $\sqrt{f}$ and $\sqrt{g}$. Then $g \circ f$ also has a positive Choi matrix:



□

A monoidal dagger category is *positively monoidal* when endomorphisms $f\colon A \to A$ are positive as soon as $f \otimes \mathrm{id}_A$ is positive. For such categories, one can prove Stinespring's theorem [16, Proposition 3.4], showing that the morphisms $f\colon A \to B$ are precisely those such that $f \otimes \mathrm{id}_E$ sends completely positive maps $I \to A \otimes E$ to completely positive maps $I \to B \otimes E$ for all special dagger Frobenius structures E. It follows that **CP**(**C**) is equivalent to **CP***(**C**) [16]. In particular, **CP**(**FHilb**) is the category of finite-dimensional C*-algebras and completely positive maps. However, this is irrelevant to this paper; for more details, see the forthcoming [22].

Proposition B.2. The category **Rel**(**C**) is positively monoidal for any regular category **C**.

Proof. If a relation $R\colon A \nrightarrow A$ satisfies $R \otimes \mathrm{id}_A = S^\dagger \circ S$ for some relation $S\colon A \times A \nrightarrow X$, then R is equal to $T^\dagger \circ T$ where $T = [\![(a,x) \in A \times X \mid (\exists c \in A)\ S(a,c,e)]\!]$ and hence is positive. □