Compactly accessible categories and quantum key distribution

COMPACTLY ACCESSIBLE CATEGORIES AND QUANTUM KEY DISTRIBUTION

CHRIS HEUNEN

Institute for Computing and Information Sciences, Radboud University, Nijmegen, the Netherlands

Abstract. Compact categories have lately seen renewed interest via applications to quantum physics. Being essentially finite-dimensional, they cannot accomodate (co)limit-based constructions. For example, they cannot capture protocols such as quantum key distribution, that rely on the law of large numbers. To overcome this limitation, we introduce the notion of a compactly accessible category, relying on the extra structure of a factorisation system. This notion allows for infinite dimension while retaining key properties of compact categories: the main technical result is that the choice-of-duals functor on the compact part extends canonically to the whole compactly accessible category. As an example, we model a quantum key distribution protocol and prove its correctness categorically.

1. Introduction

Compact categories were first introduced in 1972 as a class of examples in the context of the coherence problem [Kel72]. They were subsequently studied first categorically [Day77, KL80], and later in relation to linear logic [See89]. Interest has rejuvenated since the exhibition of another aspect: compact categories provide a semantics for quantum computation [AC04, Sel07]. The main virtue of compact categories as models of quantum computation is that from very few axioms, surprisingly many consequences ensue that were postulates explicitly in the traditional Hilbert space formalism, *e.g.* scalars [Abr05]. Moreover, the connection to linear logic provides quantum computation with a resource sensitive type theory of its own [Dun06].

Much of the structure of compact categories is due to a seemingly ingrained 'finite-dimensionality'. This feature is most apparent in the prime example, the category of vector spaces and linear maps. As we will see, the only compact objects in this category are the finite-dimensional vector spaces. This poses no problems when applied to quantum computation, where the amount of memory is physically bounded anyway. However, the employment of compact categories is sometimes optimistically publicised as providing 'a semantics for quantum protocols', or even 'axiomatics for quantum physics'. For these general purposes, a fixed finite dimension is a severe limitation since it rules out (co)limit constructions and arguments. In fact, the simplest possible physical situation, that of a

2000 ACM Subject Classification: F.3.2.

Key words and phrases: Compact categories, Accessible categories, Quantum key distribution.

LOGICAL METHODS IN COMPUTER SCIENCE DOI:10.2168/LMCS-???

single free-moving particle in three-dimensional space, is already modeled by the infinite-dimensional space $L^2(\mathbb{R}^3)$ of observables in traditional quantum physics [vN32]. Likewise, an important class of quantum protocols relies on the law of large numbers. They utilise the probabilistic nature of quantum physics to ensure that their goal is reached after sufficiently many tries. In fact, the two most-cited papers in quantum cryptography to date, describing quantum key distribution protocols, are of this kind [BB84, Eke91].

There have been earlier attempts to remedy the above limitation. Although he did not have the quantum setting in mind, Barr gave a construction to embed a category with certain minimal properties fully into a complete and cocomplete category that is *-autonomous, a notion closely related to compactness [Bar79]. However, as we will see, the important category of Hilbert spaces and bounded maps, that is the traditional model of quantum physics, is neither complete nor cocomplete.

Another proposal revolves around the use of nuclear ideals [ABP99, Blu06]. Analogous to ring theory, an ideal in this setting is a set of morphisms that is closed under composition with arbitrary morphisms. The adjective nuclear means that the key property that enables compact categories to model quantum protocols is postulated to hold for all morphisms in the ideal. This seems to be the right environment to study properties of morphisms in a quantum setting. For example, a very natural characterisation of trace-class morphisms emerges. However, it also forces one to consider two layers, the category and the nuclear ideal, and possible coherence with the ideal is a distraction when working with notions that are more naturally defined on the category. For example, any bounded map between Hilbert spaces has a dual map (in the opposite direction between the dual spaces), not just the Hilbert-Schmidt maps (that form a nuclear ideal).

The present work introduces the notion of a compactly accessible category in order to overcome the above limitation. It retains certain key properties of compact categories, and simultaneously allows for infinite dimension. The main idea is to relax the requirement that every object is compact to the requirement that every object is a directed colimit of compact ones, imitating the fact that every vector space is the directed colimit of its finite-dimensional subspaces. Categories in which every object is a directed colimit of finitely presentable ones are well-known as accessible categories, and a polished theory has developed around them [GU71, AR94]. We weaken the concept of finitely presentable object to that of a compactly presentable one, to ensure that the key properties of compact categories are inherited by compactly accessible categories. The central novel ingredient is the extra structure of a factorisation system. This approach provides a proper category in which to model quantum protocols, and hence is automatically compositional — as opposed to ideals that typically do not include all identity maps [BPP07]. Physically, directed colimits provide the intuition of 'time'. The main result, that justifies our definition of compactly accessible category, is Theorem 5.11. It shows that the choice-of-duals functor on the compact part extends canonically to the whole compactly accessible category. It is remarkable that this canonical extension of the choice-of-duals functor in the category of Hilbert spaces with its canonical factorisation system in fact provides an equivalence with the opposite category. This is another indication that the axiomatic structure of compactly accessible categories is on target. Moreover, Theorem 6.5 proves that if the choice-of-duals functor commutes with a dagger functor on the compact part, then so does its canonical extension. The latter is important for the modeling of quantum physics. As an example, we model a quantum key distribution protocol and prove its correctness categorically.

① Alice and Bob agree upon 3 measurements m_1, m_2, m_3.
② Alice secretly chooses $a_i \in \{1,2,3\}, i = 1,\ldots,3n$, randomly,
Bob secretly chooses $b_i \in \{1,2,3\}, i = 1,\ldots,3n$, randomly.
③ They share $3n$ *fresh qubit-pairs* prepared in the Bell-state $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$.
We denote them by $(q_i^a, q_i^b)_{i=1,\ldots,3n}$.
④ Alice measures q_i^a with m_{a_i} to get c_i, $i = 1,\ldots,3n$.
Bob measures q_i^b with m_{b_i} to get c'_i, $i = 1,\ldots,3n$.
⑤ Alice publicly announces a_i.
Bob publicly announces b_i.
Thus they determine $I = \{i \in \{1,\ldots,3n\} \mid a_i \neq b_i\}$.
With large probability $\#I \leq n$; *if not, go to step 2.*
⑥ Alice publicly announces c_i, $i \in I$.
Bob publicly announces c'_i, $i \in I$.
With large probability, c_i and c'_i are sufficiently correlated
by Bell's inequality for $i \in I$; *if not, go to step 2.*
⑦ Alice uses c_j, $j \in \{1,\ldots,3n\}\backslash I$ as her key bits.
Bob uses $1 - c'_j$, $j \in \{1,\ldots,3n\}\backslash I$ as his key bits.

Figure 1: A quantum protocol to obtain a $2n$-bits shared secret key [Eke91].

Section 2 first introduces the quantum key distribution protocol mentioned above. We recall the necessary details of compact categories in Section 3. Subsequently, Section 4 builds up to the notion of compactly presentable object, and Section 5 then defines compactly accessible categories and explores their structure. Dagger structure is added in Section 6, and Section 7 models and proves correct the protocol described in Section 2. Finally, Section 8 concludes.

2. Quantum key distribution

Quantum key distribution is the name for a collection of protocols that provide two parties using a quantum channel between them with a shared binary string, unknowable to anyone else. Moreover, such a scheme must be proven inherently secure by the laws of nature, *i.e.* not depending on any unsolved or computationally unfeasible mathematical problems. The most well-known protocol in this family is that of Bennett and Brassard [BB84], which essentially relies on Bell's inequality and the law of large numbers to provide secure keys.[1] There are several improvements upon this protocol. Especially Ekert [Eke91] developed a very nice simplification, which is outlined in Figure 1. As Bell's inequality provides a means to verify that two qubits are 'correlated enough', eavesdroppers can be detected with large probability. The law of large numbers thus ensures that this protocol works (up to a negligable probability that can be specified in advance). Notice that because of the possible jump back in steps ⑤ and ⑥, the number of fresh qubit-pairs needed is not known in advance.

The protocol in Figure 1 will be used in Section 7 as an example that can be modeled by compactly accessible categories. As such, we need to distinguish between correctness

[1]Such a protocol, like Diffie-Hellmann's [DH76], regulates key distribution, but gives no guarantee about authenticity of the two parties involved.

and security. A quantum key distribution protocol is correct if both parties end up with the same key in every run, *i.e.* when $c_j = 1 - c'_j$ for all $j \in \{1, \ldots, 3n\} \backslash I$ and every choice of m_i, a_i and b_i in Figure 1. It is secure when a potential eavesdropper cannot learn any of the key bits. In this instance, the security relies on Bell's inequality. Thus in this case one could say that correctness is a qualitative notion, and security a quantitative one. Because the entire purpose of the categorical approach is to abstract away from quantitative details like scalar factors, we will focus on correctness, and forget about the classical calculation in step ⑥. Since the centre of attention in this article is the elimination of finite-dimensionality, we will also not concern ourselves too much with the classical communication that is most noticable in step ⑤. The point is just to show that compactly accessible categories are able to model protocols that need an a priori unknown number of resources.

3. Compact objects and compact categories

This section recalls the concept of a compact category, by considering the required properties separately per object. It also reviews the key features of compact categories that are so important to model quantum protocols.

Definition 3.1. An object X of a symmetric monoidal category $\mathbf{C}$ is said to be *compact* when there are an object $Y \in \mathbf{C}$ and morphisms $\eta : I \to Y \otimes X$ and $\varepsilon : X \otimes Y \to I$ such that the following diagrams commute.

$$\begin{array}{ccccc} X & \overset{\cong}{\to} & X \otimes I & \xrightarrow{\mathrm{id}\otimes\eta} & X \otimes (Y \otimes X) \\ \| & & & & \downarrow \cong \\ X & \underset{\cong}{\leftarrow} & I \otimes X & \xleftarrow[\varepsilon\otimes\mathrm{id}]{} & (X \otimes Y) \otimes X \end{array} \qquad \begin{array}{ccccc} Y & \overset{\cong}{\to} & I \otimes Y & \xrightarrow{\eta\otimes\mathrm{id}} & (Y \otimes X) \otimes Y \\ \| & & & & \downarrow \cong \\ Y & \underset{\cong}{\leftarrow} & Y \otimes I & \xleftarrow[\mathrm{id}\otimes\eta]{} & Y \otimes (X \otimes Y) \end{array} \tag{3.1}$$

A symmetric monoidal category is called compact when all its objects are.

For a given compact object X, the object Y of the previous definition is called a *dual object* for X. Such dual objects are unique up to isomorphism [Dun06, Proposition 2.7]. A chosen dual object for X is usually denoted by X^*. Notice that I is a compact object in any strict symmetric monoidal category, with $I^* = I$. Also, if X is compact, then so is X^*. Moreover, any compact object X is isomorphic to its double dual X^{**} [Dun06, Proposition 2.13]. Let us see what the compact objects (and their dual objects) are in a few example categories.

Example 3.2. In a posetal symmetric monoidal category, diagrams (3.1) say that an object X is compact precisely when there is an object X^* such that $X^* \otimes X = I = X \otimes X^*$. Any ordered commutative monoid is such a category, where the order induces the morphisms, and the monoid multiplication and unit provide symmetric monoidal structure. Hence, the compact objects in an ordered commutative monoid, seen as a posetal category, are precisely its invertible elements. Thus any ordered Abelian group induces a compact category; an Abelian group is partially ordered if and only if it is torsion-free [MR77, Theorem 1.1.3]. This example has been studied more generally under the name 'Lambek pregroups' [Sad06].

Example 3.3. Denote by **Rel** the category with sets for objects, and relations $R \subseteq X \times Y$ for morphisms $X \to Y$. The composition of $X \xrightarrow{R} Y \xrightarrow{S} Z$ is the usual relational

composition

$$S \circ R = \{(x, z) \in X \times Z \mid \exists_{y \in Y}.(x, y) \in R \wedge (y, z) \in S\}.$$

This category is symmetric monoidal by the usual set-theoretic product, with the singleton set $\{*\}$ as its neutral element. Every object X in **Rel** is compact: by defining $X^* = X$ and

$$\eta_X = \{(*, (x, x)) : x \in X\},$$
$$\varepsilon_X = \{((x, x), *) : x \in X\},$$

one easily verifies that diagrams (3.1) commute. Hence **Rel** is a compact category.

This example can be generalized to the Kleisli category of the monad on **Set** given by $\mathcal{P}(M \times -)$ for an arbitrary commutative monoid M instead of the trivial monoid. It can also be generalized to the category of relations on an arbitrary regular category [CKS84]. In both generalized categories, every object is compact.

At first sight, one might expect that the category **Sup** of complete lattices and sup-preserving functions is compact, but it is not [Bar79, page 99]. Its largest compact subcategory is that of complete atomic boolean lattices and sup-preserving functions; this category is equivalent to **Rel**.

Example 3.4. Denote by **Vect** the category of complex vector spaces and linear maps. It is a symmetric monoidal category by the usual tensor product of vector spaces, with the complex field $\mathbb{C}$ as unit. Any finite-dimensional vector space X is a compact object in this category as follows. Let X^* be the dual vector space $\{f : X \to \mathbb{C} \mid f \text{ linear}\}$. If (e_i) is a basis for X, then the functionals $\overline{e}_i$ determined by $\overline{e}_i(e_j) = \delta_{ij}$ form a basis for X^*. Define η_X and ε_X by linear extension of

$$\eta_X(1) = \sum_{i=1}^{\dim(X)} \overline{e}_i \otimes e_i,$$
$$\varepsilon_X(e_i \otimes \overline{e}_j) = \overline{e}_j(e_i).$$

Diagrams (3.1) are readily seen to commute.

However, an infinite-dimensional vector space cannot be isomorphic to its double dual because of a well-known cardinality argument [Jac53, Theorem IX.2] that we sketch briefly. Let X be an infinite-dimensional vector space, and choose a basis B for it. Then $X \cong \coprod_B \mathbb{C}$, and so $X^* \cong \prod_B \mathbb{C}$ [AF74, Proposition 20.2]. So $\dim(X) \lneqq \dim(X^*) \lneqq \dim(X^{**})$, whence $X \ncong X^{**}$ and X is not a compact object in **Vect**.[2]

Hence the full subcategory **fdVect** of **Vect** containing only the finite-dimensional vector spaces is the largest compact subcategory of **Vect**.

This example can be generalized to the category of projective modules over a given semiring: the compact objects in that category are precisely the finitely generated ones.

Example 3.5. As an extension of the previous example, consider the category **Hilb** of Hilbert spaces. Its morphisms are the bounded linear maps, *i.e.* linear functions $f : X \to Y$ for which there is a constant $\|f\|$ such that $\|f(x)\| \leq \|f\|\|x\|$ for all $x \in X$. It is a symmetric monoidal category with the usual tensor product and the complex field $\mathbb{C}$ as unit. Any finite-dimensional Hilbert space X is a compact object in this category as follows. Let X^* be the conjugate of the dual space $\{f : X \to \mathbb{C} \mid f \text{ bounded linear}\}$, *i.e.* it has the same

[2]For completeness' sake, let us recall that even for a finite-dimensional vector space X, the isomorphism $X \cong X^*$ is not natural, although $X \cong X^{**}$ is [Mac86, Section VII.4].

additive group as the dual space, but conjugated scalar multiplication. Then $X^* \otimes X$ is isomorphic to the Hilbert space of all Hilbert-Schmidt maps $X \to X$ [KR83]. Define η_X by letting 1 correspond to the identity map under this isomorphism and extending linearly and continuously, and define ε_X as the adjoint of η_X. Then diagrams (3.1) commute. Since the identity map on X is a Hilbert-Schmidt map if and only if X is finite-dimensional, this recipe for obtaining compact structure on X only works for finite-dimensional X. In other words, **fdHilb** is a compact full subcategory of **Hilb**. Moreover, as Proposition 3.6(d) below shows, a compact full subcategory of **Hilb** is necessarily closed. Since only the Hilbert-Schmidt functions form a Hilbert space again [KR83], a compact full subcategory of **Hilb** must consist of objects between which all continuous linear functions are automatically Hilbert-Schmidt. That is, the largest compact full subcategory of **Hilb** is **fdHilb**.

This example can be generalized to the category of unitary representations of a given topological group: the compact objects in that category are precisely the representations with a finite-dimensional target space.[3]

Introducing the notation $\mathbf{C}_{\mathrm{cpt}}$ for the full subcategory of compact objects of $\mathbf{C}$, the previous examples thus show that $\mathbf{Rel}_{\mathrm{cpt}} = \mathbf{Rel}$, $\mathbf{Vect}_{\mathrm{cpt}} = \mathbf{fdVect}$, and $\mathbf{Hilb}_{\mathrm{cpt}} = \mathbf{fdHilb}$. This relates to order theory, in which 'finite element' and 'compact element' are used interchangeably [Joh82, AJ94]. On the one hand the name 'finite object' or 'finite-dimensional object' would also be apt in our case, but on the other hand it would be confusing since a compact object in **Rel** can be infinite as a set.

As an example of the properties of compact objects, we mention the following. They are standard results; here we formulate them for compact objects (instead of for compact categories).

Proposition 3.6. [Lin78] *Let* $\mathbf{C}$ *be a symmetric monoidal category.*

(a) *If* $X \in \mathbf{C}_{\mathrm{cpt}}$*, then* $\mathbf{C}(X,Y) \cong \mathbf{C}(I, X^* \otimes Y)$ *for all* $Y \in \mathbf{C}$*.*
(b) *If* $Y \in \mathbf{C}_{\mathrm{cpt}}$*, then* $\mathbf{C}(X,Y) \cong \mathbf{C}(X \otimes Y^*, I)$ *for all* $X \in \mathbf{C}$*.*
(c) *An object* $X \in \mathbf{C}$ *is compact if and only if there is an* $Y \in \mathbf{C}$ *such that* $\mathbf{C}(X \otimes Y, I) \cong \mathbf{C}(X,X) \cong \mathbf{C}(I, Y \otimes X)$*.*
(d) *An object* $X \in \mathbf{C}$ *is compact iff there is a* $Y \in \mathbf{C}$ *such that* $X \otimes (-)$ *is left adjoint to* $Y \otimes (-)$*. In that case,* $X \otimes (-)$ *is also right adjoint to* $Y \otimes (-)$*.*
(e) *If* $X \in \mathbf{C}_{\mathrm{cpt}}$*, then* $(-) \otimes X : \mathbf{C} \to \mathbf{C}$ *is both continuous and cocontinuous.* □

The crucial property of a compact category is that a choice of dual objects X^* extends functorially, as follows.

Proposition 3.7. [KL80] *For a morphism* $f : X \to Y$ *between compact objects* X, Y *in some category* $\mathbf{C}$*, define* $f^* : Y^* \to X^*$ *as the composite*

$$Y^* \cong Y^* \otimes I \xrightarrow{\mathrm{id} \otimes \eta_X} Y^* \otimes (X \otimes X^*) \xrightarrow{\mathrm{id} \otimes f \otimes \mathrm{id}} (Y^* \otimes Y) \otimes X^* \xrightarrow{\varepsilon_Y \otimes \mathrm{id}} I \otimes X^* \cong X^*.$$

This defines a functor $(-)^* : \mathbf{C}_{\mathrm{cpt}}^{\mathrm{op}} \to \mathbf{C}_{\mathrm{cpt}}$*.* □

[3] In fact, this is where the compactness terminology seems to have originated: the group G can be reconstructed from the described category $\mathbf{fdURep}(G)$ when it is compact [DR89, Müg06]. Hence the name transferred from the group to categories resembling $\mathbf{fdURep}(G)$. Alternatively, one could observe that being a Hausdorff space, a Hilbert space's unit ball is compact if and only if it is finite-dimensional. Finally, a Hilbert space is locally compact if and only if it is finite-dimensional [Hal82, Problem 10].

For future reference, let us mention that the correspondence in Proposition 3.6(a,b) of morphisms $f : X \to Y$ to their *names* $\ulcorner f \urcorner : I \to X^* \otimes Y$ and to their *conames* $\llcorner f \lrcorner : X \otimes Y^* \to I$ satisfies [Dun06, Lemma 2.18]:

$$(\mathrm{id} \otimes g) \circ \ulcorner f \urcorner = \ulcorner g \circ f \urcorner = (f^* \otimes \mathrm{id}) \circ \ulcorner g \urcorner. \tag{3.2}$$

Moreover, the choice-of-duals functor $(-)^*$ preserves limits and colimits. When $D : \mathbf{J} \to \mathbf{C}$ is any diagram in a compact category, we can speak of its dual diagram $D^* : \mathbf{J} \to \mathbf{C}^{\mathrm{op}}$ determined by $D^* = (-)^* \circ D$. This construction extends to *compact diagrams* in any category: we say a diagram in any category $\mathbf{C}$ is compact if it factors through $\mathbf{C}_{\mathrm{cpt}}$. We use the term *compact (co)limit* for a (co)limit of a compact diagram.

Proposition 3.8. *If* $\mathbf{C}$ *is a compact category,* $(-)^* : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ *preserves limits and colimits, i.e. for any diagram* $D : \mathbf{J} \to \mathbf{C}$*, we have* $(\lim(D))^* \cong \lim(D^*)$ *and* $(\mathrm{colim}(D))^* \cong \mathrm{colim}(D^*)$ *in* $\mathbf{C}^{\mathrm{op}}$*.*

Proof. If $\mathbf{C}$ is a compact category, the functor $(-)^* \colon \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ is an equivalence of categories [Dun06, Proposition 2.13]. □

4. Compactly presentable objects

The next section discusses a kind of category in which every object is a colimit of compact ones. However, taking colimits of just compact objects is not enough to retain a 'choice-of-duals-functor' as in Proposition 3.7. This section strengthens the notion of compact object as the constituent of the colimits accordingly, drawing inspiration from the notion of finitely presentable object. An extra ingredient is the structure of a factorisation system.

4.1. **Finitely presentable objects.** Intuitively, a finitely presentable object is one that can be described algebraically using a finite number of generators and finitely many equations [AR94]. Recall that a preorder is *directed* when every two elements have a common upper bound; a *directed colimit* is a colimit of a directed preorder considered as a diagram. Likewise, a preorder is codirected when its opposite is directed, and a codirected limit is a limit of a codirected preorder considered as a diagram.

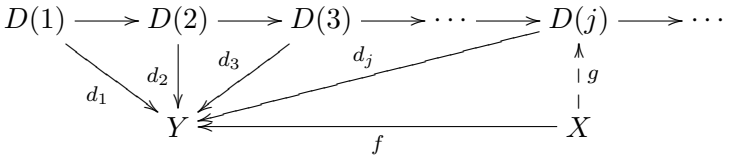
Definition 4.1. An object X in a category $\mathbf{C}$ is called *finitely presentable* when the hom-functor[4] $\mathbf{C}(X, -) : \mathbf{C} \to \mathbf{Set}$ preserves directed colimits.[5]

Writing this out, we see that X is finitely presentable when for any directed diagram $D : \mathbf{J} \to \mathbf{C}$, any colimit cocone $d_j : D(j) \to Y$ and any morphism $f : X \to Y$, there are $j \in \mathbf{J}$ and a morphism $g : X \to D(j)$ such that $f = d_j \circ g$. Moreover, this morphism g is

[4]If needed, one should replace **Set** by some suitably larger universe.

[5]This definition can be extended to λ-presentable, for a regular cardinal λ. Finite presentability then coincides with ω-presentability. Later notions, like finitely accessible category, can also be extended, but for the sake of clarity of presentation we do not do so in this article.

essentially unique, in the sense that if $f = d_j \circ g = d_j \circ g'$, then $D(j \to j') \circ g = D(j \to j') \circ g'$ for some $j' \in \mathbf{J}$.



The following example shows that finite presentability is certainly an interesting property in the context of compact objects in categories.

Example 4.2. In the posetal category induced by an ordered commutative monoid as in Example 3.2, an object X is finitely presentable precisely when in case X is smaller than a supremum of some directed set D, it is already smaller than some element of D. (This is closely related to a compact or finite element of a lattice in the order theoretical sense [Joh82, AJ94].)

The next example shows that in some categories, the finitely presentable objects are precisely the compact ones.

Example 4.3. An object in **Set** is finitely presentable if and only if it is a finite set. An object in **Vect** or **Hilb** is finitely presentable if and only if it is finite-dimensional.

However, the following example shows that **Rel** has only one finitely presentable object. This contrasts sharply with Example 3.3, that shows that every object in **Rel** is compact.

Example 4.4. The only finitely presentable object of **Rel** is the empty set.

Proof. Since $\emptyset$ is an initial object in **Rel**, any morphism $\emptyset \to \mathrm{colim}(D)$ is the empty relation, which factors uniquely through any $D(j)$.

Conversely, suppose that X has an element x. Consider the directed diagram $D : \mathbb{N} \to \mathbf{Rel}$, where $\mathbb{N}$ is a partial order seen as a category, determined by $D(n) = \{0, \ldots, n-1\}$ and $D(n \to m) = \{(i,i) \colon i = 0, \ldots, n-1\}$. Its colimit in **Rel** is $\mathbb{N}$, with colimit cocone $d_n = \{(i,i) \colon i = 0, \ldots, n-1\} \subseteq D(i) \times \mathbb{N}$. Define a relation $R \subseteq X \times \mathbb{N}$ by $R = \{(x,n) \colon n \in \mathbb{N}\}$. If this relation were to factor through any D_n then its image would have to be finite, which it is not. Hence X is not finitely presentable. □

It is interesting to note that, in a sense, the notion of compact object is stronger than that of finitely presentable object. By Proposition 3.6(d), the compact part $\mathbf{C}_{\mathrm{cpt}}$ of any category $\mathbf{C}$ is monoidal closed, and hence enriched over itself. Since the $\mathbf{C}$-functor $\mathbf{C}(X, -)$ is $\mathbf{C}$-cocontinuous for $X \in \mathbf{C}_{\mathrm{cpt}}$ [Lin78, Proposition 6], one might think that Proposition 3.6(e) implies that every compact object of a category is finitely presentable. However, there is a distinction between cocontinuity of $\mathbf{C}(X, -)$ in this enriched setting [Lin76] and 'ordinary' finite presentability. For example, sets and relations can be seen as an ordinary **Set**-category **Rel** with hom-sets $\mathcal{P}(X \times Y)$, but also as a **Rel**-category $\underline{\mathbf{Rel}}$ with hom-objects $X \times Y$. However, cocontinuity in **Rel** is different entirely from cocontinuity in $\underline{\mathbf{Rel}}$: the former just means that $X \times (-)$ preserves all colimits in **Rel**, whereas the latter means that $\mathbf{Rel}(X, -)$ preserves all colimits in **Rel**. In other words:

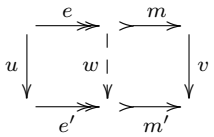
$$X \times \mathrm{colim}(D) \cong \mathrm{colim}\, X \times D(j), \text{ but}$$
$$\mathcal{P}(X \times \mathrm{colim}(D)) \ncong \mathrm{colim}\, \mathcal{P}(X \times D(j)), \text{ except for } X = \emptyset,$$

where $D : \mathbf{J} \to \mathbf{Rel}$ is a diagram, and the colimit is taken in **Rel**. This explains why **Rel** has only one finitely presentable object and every object is compact, but every object of $\underline{\mathbf{Rel}}$ is compact and finitely presentable.

4.2. **Factorisation systems.** To arrive at a suitable notion that is stronger than compactness of objects but retains the essential properties of finite presentability, we recall a concept that was popularised by Freyd and Kelly [FK72] but whose origins can be traced back to Mac Lane [Mac50] and Isbell [Isb57] (see also [BW84, Exercises 5.5] or [Bor94, Section 5.5]).

Definition 4.5. A *weak factorisation system* (E, M) for a category $\mathbf{C}$ consists of two classes of morphisms E and M of $\mathbf{C}$ such that

- E and M both contain all isomorphisms of $\mathbf{C}$, and are closed under composition;
- Every morphism f of $\mathbf{C}$ can be factored as $f = m \circ e$ for some $m \in M$ and $e \in E$; and
- The factorisation is functorial, in the sense that for morphisms u, v with $v \circ m \circ e = m' \circ e' \circ u$ for $m, m' \in M$ and $e, e' \in E$, there is a morphism w making the following diagram commute.



A weak factorisation system is called a *factorisation system* when the morphism w above is unique.

If no confusion about the (weak) factorisation system at hand can arise, we use the notation $\twoheadrightarrow$ for morphisms in E, and $\rightarrowtail$ for morphisms in M. Furthermore, we denote by $M(X, Y)$ the set of morphisms in M with domain X and codomain Y. Also, we denote by $M(X, -)$ the corresponding functor $\mathbf{C} \to \mathbf{Set}$.

Example 4.6. Any posetal category has a factorisation system where E consists of all identity morphisms, and M comprises all morphisms.

Example 4.7. An epimorphism in **Vect** is a surjective linear map, a monomorphism in **Vect** is an injective linear map. These provide a factorisation system for **Vect**.

Likewise, an epimorphism in **Hilb** is a continuous linear map with dense image, and a monomorphism in **Hilb** is an injective continuous linear map. These provide a factorisation system for **Hilb**.

Proof. Every epimorphism in **Vect** is regular since it is the coequaliser of its cokernel pair [Bor94, Example 4.3.10a]. Since the pullback of a surjective linear map is again a surjective linear map, the monomorphisms and (regular) epimorphisms form a factorisation system for **Vect** [BW84, Exercise 5.5.4]. The situation in **Hilb** is analogous, except that the image first needs to be closed to be a genuine Hilbert space. □

The fact that the bicategory of relations is defined as a subbicategory of the bicategory of spans [CKS84, FS90] inspires the following weak factorisation system for our other running example, **Rel**.

Example 4.8. Call a relation $R \subseteq X \times Y$ *functional* if $\forall_{x \in X} \exists!_{y \in Y} [(x,y) \in R]$, and *oppositely functional* if $\forall_{y \in Y} \exists!_{x \in X} [(x,y) \in R]$. Denote by M the collection of functional relations, and by E the collection of oppositely functional relations. Then (E, M) is a factorisation system for **Rel**.

Proof. First, isomorphisms in **Rel** are isomorphisms in **Set**, so that these are certainly in both E and M. Obviously, E and M are closed under composition.

Secondly, any morphism $R \subseteq X \times Y$ of **Rel** factors as $R = m \circ e$ for

$$e = \{(x,(x,y)) : x \in X, y \in Y \mid (x,y) \in R\} \subseteq X \times R,$$
$$m = \{((x,y),y) : x \in X, y \in Y \mid (x,y) \in R\} \subseteq R \times Y.$$

with $e \in E$ and $m \in M$.

Thirdly, we show that the factorisation is functorial. Assume

$$\begin{array}{ccccc} X & \xrightarrow{e} & R & \xrightarrow{m} & Y \\ {\scriptstyle U}\downarrow & & & & \downarrow{\scriptstyle V} \\ X' & \xrightarrow[e']{} & R' & \xrightarrow[m']{} & Y' \end{array}$$

for $e, e' \in E$ and $m, m' \in M$. Then

$$W = \{((x,y),(x',y')) \in R \times R' \mid (x,x') \in U, (y,y') \in V\}$$

is the unique relation between R and R' making both squares commute. □

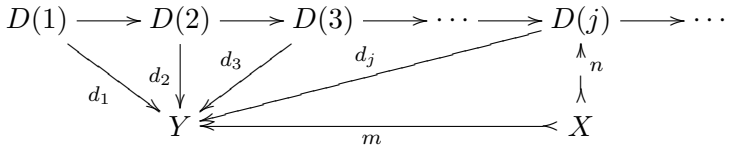
4.3. **Compactly presentable objects.** The following observation is a combination of the notions of compactness of objects and finite presentability that did not coincide in **Rel**. Since the 'monomorphisms' in Example 4.8 are functions, $M(X,-)$ preserves directed colimits in **Rel** if and only if X is a finite set by Example 4.3. This property that we name 'compact presentability' is now lifted to a definition, because it turns out to be exactly what we need in Section 5.

Definition 4.9. A compact object X in a symmetric monoidal category $\mathbf{C}$ is said to be *compactly presentable*[6] with respect to a weak factorisation system (E, M), when $M(X,-)$ preserves directed compact colimits.

Explicitly, a compact object X is compactly presentable (with respect to a weak factorisation system) when for any directed compact diagram $D : \mathbf{J} \to \mathbf{C}$, any colimit cocone $d_j : D(j) \to Y$ and any morphism $m : X \rightarrowtail Y$ in M, there are $j \in \mathbf{J}$ and a morphism

[6]The terminology is slightly unfortunate, because by the notation in the literature [AR94, GU71] it might suggest that $\mathbf{C}(X,-)$ preserves colimits of λ-directed diagrams for a 'compact cardinal' λ. Although Definition 4.9's *raison d'être* is to ensure the existence of the functor $(-)^*$ in Section 5, we refrain from a notational name like 'star-presentable object'. Likewise, 'locally compact object' has other connotations.

$n : X \rightarrowtail D(j)$ in M such that $m = d_j \circ n$. Moreover, this morphism n is essentially unique, in the sense that if $m = d_j \circ n = d_j \circ n'$, then $D(j \to j') \circ n = D(j \to j') \circ n'$ for some $j' \in \mathbf{J}$.



Notice that compact presentability is a strictly stronger notion than compactness of objects. This might be surprising because the former depends on the structure of a weak factorisation system whereas the latter does not. However, this is resolved by noting that the definition of compact presentability explicitly includes the clause that the object must be compact. Also, compact presentability is strictly weaker than finitely presentable and compact, because only composition with 'monomorphisms' is required to preserve certain colimits, instead of composition with all morphisms. This is clearly exhibited when we consider which objects are compactly presentable in our example categories.

Example 4.10. In a posetal category induced by an ordered commutative monoid as in Example 3.2, with the factorisation system of Example 4.6, an object X is compactly presentable when it is invertible and in case it is smaller than a supremum of some directed set D of invertible elements, it is already smaller than some element of D.

Proof. Since the 'monomorphisms' in the factorisation system of Example 4.6 are all morphisms, compactly presentable in this case coincides with compact and finitely presentable. The result thus follows by substituting Example 4.2 into Definition 4.9. □

Example 4.11. In **Rel**, with the factorisation system of Example 4.8, the compactly presentable objects are the finite sets.

Proof. Since the 'monomorphisms' in the factorisation system in **Rel** of Example 4.8 are functions, an object in **Rel** is compactly presentable precisely when it is finitely presentable in **Set**, which happens precisely when it is a finite set by Example 4.3. □

Example 4.12. In **Vect** and **Hilb**, with the factorisation system of Example 4.7 the compactly presentable objects are the finite-dimensional spaces.

Proof. Let X be a finite-dimensional vector space, $D : \mathbf{J} \to \mathbf{Vect}$ a directed compact diagram, and $f : X \to \mathrm{colim}(D)$ an injective linear map. Since we can choose a finite basis for X, also $\mathrm{Im}(f)$ is finite-dimensional. Hence, by induction, $\mathrm{Im}(f)$ can be written as the span of a finite number of basis vectors of $\mathrm{colim}(D)$, for any basis of $\mathrm{colim}(D)$. Since these basis vectors must be in some $D(j)$, so is their span, and thus f factors through $D(j)$, essentially uniquely.

Conversely, if f factors through a finite-dimensional space, X must be finite-dimensional, since $\mathrm{rank}(f) = \dim(X)$ because f is injective. The situation in **Hilb** is analogous. □

Example 4.10 shows that the object I is not necessarily compactly presentable: a counterexample is the category induced by $(\mathbb{Q}, +, \leq)$, since we have $0 \leq \sup_n(-\frac{1}{n})$, but of course $0 \not\leq -\frac{1}{n}$ for all n. Hence the compactly presentable objects do not form a monoidal subcategory in general. However, we can ensure that the tensor product of compactly presentable objects is again compactly presentable by the following assumptions on the (weak) factorisation system: $\eta_X \in M$ and $\varepsilon_X \in E$ for all $X \in \mathbf{C}_{\mathrm{cpt}}$, and M is closed under tensor products.

5. Compactly presentable categories and compactly accessible categories

The main idea of this article is very simple. To overcome the limitation of finite-dimensionality inherent in compact categories, we consider categories in which every object is a directed colimit of compact objects. Although directed colimits of monomorphisms between compact objects would suffice, the definitions turn out to be more concise in the general case.

In **Vect**, this is an extension of choosing a basis for every vector space: if (e_n) is a (well-ordered) basis for X, then X is the colimit of the totally ordered diagram

$$\mathrm{span}(e_1) \longrightarrow \mathrm{span}(e_1, e_2) \longrightarrow \mathrm{span}(e_1, e_2, e_3) \longrightarrow \cdots$$

where the morphisms are the obvious inclusions. Conversely, not every totally ordered diagram provides a basis for its colimit vector space, even if the constituent objects' dimension increases by one. However, every vector space is the directed colimit of its finite-dimensional subspaces, even if the dimension of the vector space is uncountable. For example, consider the free complex vector space $V = F(\mathbb{R})$ on the basis $\mathbb{R}$. Let $V_B = \{\varphi : \mathbb{R} \to \mathbb{C} \mid \varphi(x) \neq 0 \Rightarrow x \in B\}$ for $B \in \mathcal{P}_{\mathrm{fin}}(\mathbb{R})$ be the finite-dimensional subspaces. Then $V = F(\mathbb{R}) = F(\mathrm{colim}_B B) = \mathrm{colim}_B F(B) = \mathrm{colim}_B V_B$. Thus the slippery cardinality issue surrounding colimits of bases is defused by the information relating different subspaces encoded in the diagram of all finite-dimensional subspaces. Nevertheless, the choice of a basis is a good intuition for a directed colimit of compact objects.

Since we will ultimately consider such categories that moreover have an involution on the entire category (see Section 6), we might as well consider coherence of the choice-of-duals with colimits. For this, demanding colimits of compact objects is not enough — it turns out we need every object to be a directed colimit of compactly presentable objects to construct a choice-of-duals-functor on the entire category.

5.1. **(Directed) colimits.** Before we can postulate every object to be a (directed) colimit of some well-behaved kind of objects, a natural first requirement is that the category must have all (directed) colimits. Fortunately, our running example categories satisfy this.

In a posetal category, colimits correspond to suprema, and limits to infima. Hence the category of Example 3.2 has directed limits and codirected limits precisely when its partial order structure has directed infima and directed suprema. It is complete and cocomplete when it is a complete lattice ordered commutative monoid.

Lemma 5.1. ***Rel*** *has directed colimits and codirected limits, but is neither complete nor cocomplete.*

Proof. It suffices to show that **Rel** has colimits of totally ordered diagrams [AR94, Corollary 1.7]. Let $R_n \subseteq X_n \times X_{n+1}$ be such a chain. Put $X'_n = \{x \in X_n \mid \exists_{y \in X_{n+1}}.(x, y) \in R_n\}$, and $X = \coprod_n X'_n / \sim$, where $\sim$ is the smallest equivalence relation such that $x \sim y$ when $(x, y) \in R_n$. Then $S_n = \{(x, [x]) \in X'_n \times X \mid x \in X'_n\} \subseteq X_n \times X$ is a cocone. To show that it is universal, suppose that $T_n \subseteq X_n \times Y$ is another cocone. Then $T_n \subseteq X'_n \times Y$, for if some $(x, y) \in T_n$ with $x \notin X'_n$, then $(x, y) \notin T_{n+1} \circ R_n$ contradicts the fact that T_n forms a cocone. Define $T \subseteq X \times Y$ by $T = \{([x], y) \in X \times Y \mid x \in X'_n \mid (x, y) \in T_n\}$; this is

well-defined since T_n is a cocone. Moreover,

$$\begin{aligned} T \circ S_n &= \{(x,y) \in X_n \times Y \mid x \in X'_n \wedge ([x],y) \in T\} \\ &= \{(x,y) \in X_n \times Y \mid x \in X'_n \wedge (x,y) \in T_n\} \\ &= T_n, \end{aligned}$$

whence T is a mediating morphism. Finally, it is the unique such relation, since if also $T' \circ S_n = T_n$, then $([x],y) \in T'$ for $(x,y) \in X'_n \times Y$ iff $(x,y) \in T_n$, so $T' = T$. Hence X is a colimit and S_n a colimiting cocone.

However, **Rel** lacks equalizers. To see this, consider the sets $X = \{0,1\}$ and $Y = \{0\}$, and the parallel relations $R = X \times Y$ and $S = \{(0,0)\} \subseteq X \times Y$. Their equaliser must be contained in $T = \{(0,0)\} \subseteq \{0\} \times X$. Now $T' = \{0\} \times X$ also satisfies $R \circ T' = S \circ T'$, but does not factor through any subrelation of T.

The fact that **Rel** is a self-dual category establishes the statements about codirected limits and completeness. □

Lemma 5.2. ***Vect*** *is complete and cocomplete.*

Proof. The category **Vect** is algebraic, *i.e.* monadic over **Set**. Hence it is complete [BW84, Theorem 3.4.1] and cocomplete [BW84, Proposition 9.3.4]. This is also easily seen by directly constructing products, coproducts, kernels and cokernels [Mac98, Section V.2]. □

Lemma 5.3. ***Hilb*** *has directed colimits and codirected limits, but is neither complete nor cocomplete.*

Proof. It suffices to show that **Hilb** has colimits of totally ordered diagrams [AR94, Corollary 1.7]. Denote by $\mathbf{Hilb}_{\leq 1}$ the category of Hilbert spaces and contractions. Define a functor $F : \mathbf{Hilb} \to \mathbf{Hilb}_{\leq 1}$ by $F(H) = H$, acting on morphisms as $F(f) = \|f\|^{-1} \cdot f$ if $f \neq 0$ and $F(0) = 0$. One easily proves that F creates colimits of totally ordered diagrams. Since $\mathbf{Hilb}_{\leq 1}$ is known to have directed colimits [AR94, Example 2.3.9], so does **Hilb**.

To see that **Hilb** does not have all colimits, consider the following counterexample. Define an $\mathbb{N}$-indexed family $H_n = \mathbb{C}$ of objects of **Hilb**, and define $f_n : H_n \to \mathbb{C}$ by $f_n(z) = n \cdot z$. These are certainly bounded maps since $\|f_n\| = n$. Suppose the family (H_n) had a coproduct H. Then, for all $n \in \mathbb{N}$, the norm of the cotuple $f : H \to \mathbb{C}$ of (f_n) must satisfy

$$n = \|f_n\| = \|f \circ \kappa_n\| \leq \|f\| \cdot \|\kappa_n\| = \|f\|,$$

where κ_n denotes the coproduct injection, that may be assumed to have unit norm. This contradicts the boundedness of f, so **Hilb** is not cocomplete. Notice that diverging behaviour as in the above counterexample is excluded by directed diagrams.

The fact that **Hilb** is a self-dual category establishes the statements about codirected limits and completeness. □

5.2. **Finitely accessible categories.** For reference we now recall the kind of categories in which every object is a (directed) colimit of finitely presentable objects. The next subsection will imitate this construction with compactly presentable objects instead of finitely presentable ones.

Definition 5.4. A category is called *locally finitely presentable* when it is cocomplete and has a set[7] A of finitely presentable objects such that every object is a directed colimit of objects from A.

Definition 5.5. A category is called *finitely accessible* when it has directed colimits and there is a set A of finitely presentable objects such that every object is a directed colimit of objects from A.

Locally finitely presentable categories are precisely the free cocompletions of small categories [AR94, Theorem 1.46], and finitely accessible categories are precisely the free cocompletions of small categories with respect to directed colimits [AR94, Theorem 2.26]. This might suggest that it suffices to take the free cocompletion of a compact category with respect to directed colimits. However, then it is not clear how to extend the choice-of-duals-functor to the resulting accessible category (if it is possible at all).

5.3. **Compactly accessible categories.** As mentioned above, this subsection mimicks Definitions 5.4 and 5.5 using compactly presentable objects. The reason for this adaptation will become clear in the next subsection: it ensures that the choice-of-duals-functor extends to the entire category. Since our main example, **Hilb**, is not cocomplete but has directed colimits by Lemma 5.3, we are mostly interested in (compactly) accessible categories, but for completeness we also consider locally (compactly) presentable categories.

However, first we need to require the weak factorisation system to cooperate with compactness. Compact presentability of objects already takes into account the 'monomorphisms', and the next definition fixes coherence with the 'epimorphisms'.

Definition 5.6. A (weak) factorisation sytem is called *compactly presentable* if quotients preserve compact presentability, that is, if $X \twoheadrightarrow Y$ and X is compactly presentable, then so is Y.

The (weak) factorisation systems for posetal categories, **Rel**, **Vect** and **Hilb** we met in Examples 4.7 and 4.8 are all easily seen to be compactly presentable. If X is a finite set and there is a surjection onto Y, then surely Y is finite. Likewise, if X is a finite-dimensional vector space and there is a surjection onto Y, then also Y must be finite-dimensional.

Definition 5.7. A category $\mathbf{C}$ is called *locally compactly presentable* if

- it is symmetric monoidal;
- it has compact limits and compact colimits;
- it is equipped with a compactly presentable weak factorisation system; and
- it has a set A of compactly presentable objects such that every object is a directed colimit of objects of A.

Definition 5.8. A category $\mathbf{C}$ is called *compactly accessible* if

- it is symmetric monoidal;
- it has directed compact colimits and codirected compact limits;
- it is equipped with a compactly presentable weak factorisation system; and
- it has a set A of compactly presentable objects such that every object is a directed colimit of objects of A.

[7] In fact, we allow a set A of finitely presentable objects, such that every object is a directed colimit of objects isomorphic to an object from A. That is, we only require the full subcategory of those objects to be *essentially small*, *i.e.* its skeleton must be small.

Since every set is a directed colimit (in **Rel**) of the diagram of its finite subsets (ordered by inclusion)[8], we see that **Rel**, equipped with the factorisation system of Example 4.11, is a compactly accessible category by collecting earlier results.

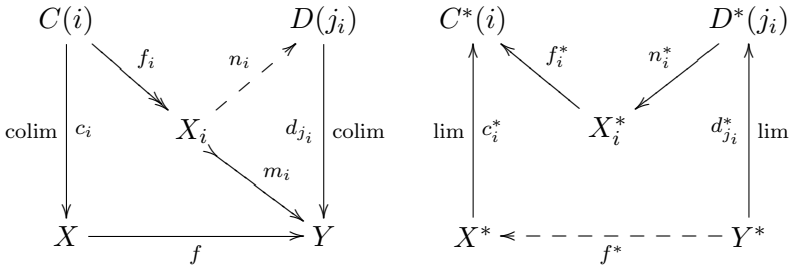
Of course, every compactly presentable category is a compactly accessible category. But also **Vect** and **Hilb** (and their generalisations indicated in Examples 3.4 and 3.5), equipped with their canonical factorisation systems (see Example 4.7), are examples of compactly accessible categories. Hence the previous definition at least succeeds in overcoming the limitation of finite-dimensionality.

We also see that the posetal category induced by an directed-complete ordered Abelian group of Example 3.2 is a compactly accessible category precisely if every element is a directed supremum of the compact elements below it, *i.e.* when the Abelian group is in fact ordered by an algebraic domain [AJ94].

5.4. **Properties of compactly accessible categories.** Compactly accessible categories inherit some of the pleasant properties from compact categories, and others only partly. The choice-of-duals-functor, that is arguably the most important feature of a compact category, extends canonically. We first define the construction on morphisms, and then prove it to be functorial.

Definition 5.9. Let $f : X \to Y$ be a morphism in a compactly accessible category $\mathbf{C}$. Pick directed compactly presentable diagrams $C : \mathbf{I} \to \mathbf{C}$ and $D : \mathbf{J} \to \mathbf{C}$ with colimit cocones $c_i : C(i) \to X$ and $d_j : D(j) \to Y$. Let limit cones $c_i^* : X^* \to C^*(i)$ and $d_j^* : Y^* \to D^*(j)$ be given. We define a morphism $f^* : X^* \to Y^*$ as follows.

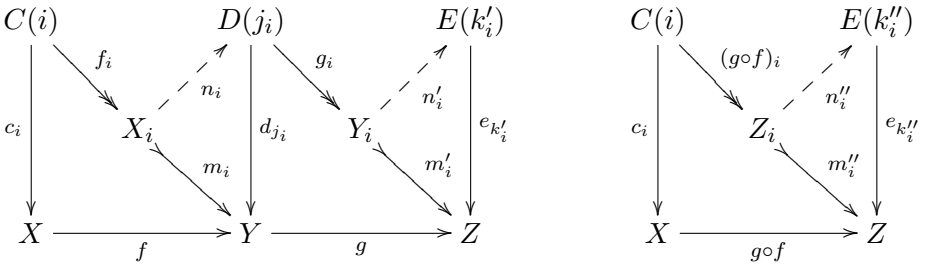
Every $f \circ c_i$ factors as $C(i) \xrightarrow{f_i} X_i \xrightarrowtail{m_i} Y$. Because $C(i)$ is compactly presentable, so is X_i, and hence there is a $j_i \in \mathbf{J}$ such that m_i factors as $X_i \xrightarrow{n_i} D(j_i) \xrightarrow{d_{j_i}} Y$. Because of the functorial property of the weak factorisation system and directedness of D, the morphisms $f_i^* \circ n_i^* \circ d_{j_i}^*$ form a cone from vertex Y^* to C^*. Define f^* to be the unique mediating morphism $Y^* \to X^*$.



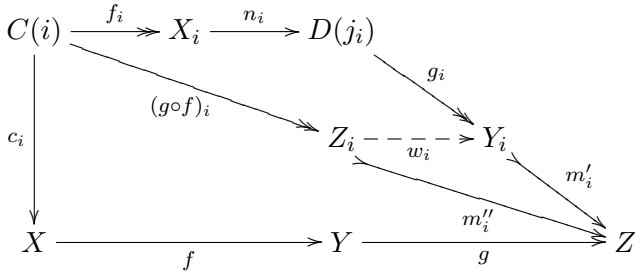
Lemma 5.10. *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$ be morphisms in a compactly accessible category $\mathbf{C}$. Pick directed compactly presentable diagrams $C : \mathbf{I} \to \mathbf{C}$, $D : \mathbf{J} \to \mathbf{C}$ and $E : \mathbf{K} \to \mathbf{C}$ with colimit cocones $c_i : C(i) \to X$, $d_j : D(j) \to Y$, and $e_k : E(k) \to Z$. Let limit cones $c_i^* : X^* \to C^*(i)$, $d_j^* : Y^* \to D^*(j)$ and $e_k^* : Z^* \to E^*(k)$ be given. Then $(g \circ f)^*$, as defined above, equals $f^* \circ g^*$.*

[8]Notice that, up-to-isomorphism, there is only a set of finite sets (namely $\mathbb{N}$).

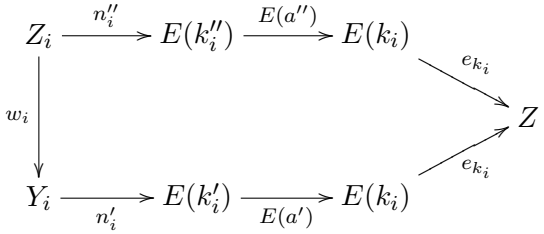
Proof. According to the construction in the previous definition, we get the following commuting diagrams.



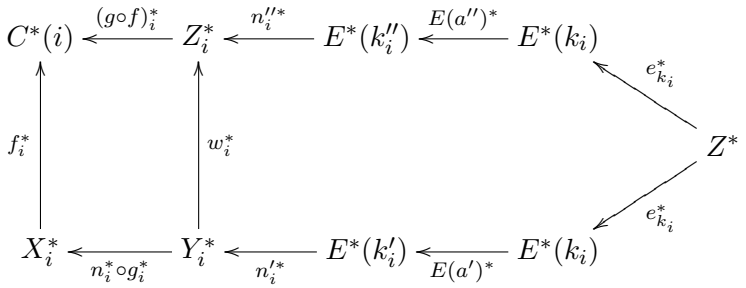
The functoriality of the weak factorisation system provides a morphism w_i making the following diagram commute.



Because E is a directed diagram, there exist $k_i \in \mathbf{K}$ and morphisms $a' : k'_i \to k_i$ and $a'' : k''_i \to k_i$ of $\mathbf{K}$. So the following diagram commutes.



Hence we get compatible cones $Z^* \to C^*$, as in the following diagram.



Thus by uniqueness of the mediating morphism, $(g \circ f)^* = f^* \circ g^*$. □

Theorem 5.11. *There is a canonical functor* $(-)^* : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ *on any compactly accessible category* $\mathbf{C}$*, extending that on* $\mathbf{C}_{\mathrm{cpt}}$*.*

Proof. An easy diagram chase shows directly that the construction in Definition 5.9 satisfies $\mathrm{id}^* = \mathrm{id}$. Combining this with Lemma 5.10, we see that $\mathrm{colim}(C) \cong \mathrm{colim}(D)$ for compactly presentable directed diagrams C and D implies that $\lim(C^*) \cong \lim(D^*)$. Hence picking one representative X^* of each isomorphism class $\lim(D^*)$ where $X \cong \mathrm{colim}(D)$ provides an action $(-)^* : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ on objects. Definition 5.9 subsequently gives an action on morphisms, and Lemma 5.10 shows that this is indeed functorial.

If we ensure that the choice of representatives X^*, Y^* coincides with the choice of duals for $X, Y \in \mathbf{C}_{\mathrm{cpt}}$, then the situation for a morphism $f : X \to Y$ collapses, so that the f^* of Definition 5.9 indeed coincides with the f^* of Proposition 3.7. After all, $C, D : \mathbf{1} \to \mathbf{C}$ with $C(*) = X$ and $D(*) = Y$ are compact directed diagrams. □

In **Vect**, equipped with its usual factorisation system (of Example 4.7), the functor $(-)^*$ of the previous theorem maps an object to its usual dual vector space (and a morphism to its usual dual). Hence, the dual-space functor of vector spaces is entirely determined when a choice of dual spaces of just the finite-dimensional vector spaces (and a factorisation system) has been fixed.

However, by allowing infinite-dimensionality in compactly accessible categories, we also partly lost some properties of compact categories. For example, the functor $(-)^*$ is no longer an equivalence.

Proposition 5.12. *The isomorphism* $X \cong X^{**}$ *holds for compact objects* X *in a compactly accessible category* $\mathbf{C}$*, but not for any object.*

Proof. For compact objects we have Proposition 3.8. As a counterexample for non-compact objects, we already saw in Example 3.4 that an infinite-dimensional vector space is not isomorphic to its double dual by a cardinality argument. □

Unfortunately this entails that the choice-of-duals-functor is no longer necessarily involutive up to isomorphism outside the compact part of the category. However, for the present purpose this is not a major issue, because the 'essence' of a quantum protocol resides in the compact part; the cocompletion aspect is only used because the dimension is not a priori bounded.

However, the canonical factorisation system in **Hilb** (see Example 4.7) provides a canonical extension of the choice-of-duals functor that *is* an equivalence. It is remarkable that such a functor can be derived from the axiomatic structure of compactly accessible categories.

Likewise, a compactly accessible category is no longer a tensored *-category [Müg06] in the sense that the tensor does not necessarily cooperate with the choice-of-duals-functor outside the compact part of the category.

Proposition 5.13. *If* X *or* Y *is compact, then* $(X \otimes Y)^* \cong X^* \otimes Y^*$*, but this isomorphism does not hold in general in a compactly accessible category.*

Proof. Without loss of generality, assume X to be compact. Let a directed compactly presentable diagram $D : \mathbf{J} \to \mathbf{C}$ with colimit Y be given. Since X^* is also compact, we

have by Proposition 3.6(e) that

$$\begin{aligned}(X \otimes Y)^* &= (X \otimes \operatorname*{colim}_j(D(j)))^* \\ &= (\operatorname*{colim}_j(X \otimes D(j)))^* \\ &= \lim_j(X^* \otimes D^*(j)) \\ &= X^* \otimes (\lim_j(D^*(j))) \\ &= X^* \otimes Y^*.\end{aligned}$$

However, for infinite-dimensional vector spaces X and Y it is not necessarily true that $(X \otimes Y)^* \cong X^* \otimes Y^*$. □

Again, it is interesting to remark that the previous proposition does hold for all Hilbert spaces X and Y, since every Hilbert space is naturally isomorphic to its dual (by the Riesz representation theorem).

6. Dagger compactly accessible categories

Although the choice-of-duals is arguably the most important feature, to model quantum protocols one needs a compact category to have a second involutive structure coherent with choice-of-duals [AC04, Sel07]. In the prime example category of finite-dimensional Hilbert spaces, this second structure provides complex conjugation, whereas the choice-of-duals accounts for transposition of matrices.

Definition 6.1. A *dagger category* is a category $\mathbf{C}$ equipped with an involutive, identity-on-objects functor $(-)^\dagger : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$.

All kinds of terminology transfers from **Hilb** to any dagger category. For example, a morphism f in a dagger category is called an *isometry* when $f^\dagger \circ f = \mathrm{id}$, and *unitary* when furthermore $f \circ f^\dagger = \mathrm{id}$.

Definition 6.2. A *dagger symmetric monoidal category* is a symmetric monoidal category $\mathbf{C}$ that is simultaneously a dagger category, such that

$$(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger,$$

and the associativity, left-unit, right-unit and symmetry monoidal structure isomorphisms are unitary.

Examples of dagger symmetric monoidal categories are **Rel** and **Hilb**. In **Rel**, the dagger structure is given on morphisms by $R^\dagger = \{(y, x) : (x, y) \in R\}$. The dagger structure in **Hilb** is provided by the Riesz representation theorem: for a morphism $f : X \to Y$ of **Hilb**, there is a unique morphism $f^\dagger : Y \to X$ satisfying $\langle f(x) \,|\, y\rangle = \langle x \,|\, f^\dagger(y)\rangle$ for all $x \in X$ and $y \in Y$ [KR83, Theorem 2.4.2].

We now adapt the definition of 'dagger compact category' slightly to encompass compactly accessible categories. First, the dagger structure should cooperate with the weak factorisation system.

Definition 6.3. A (weak) factorisation system (E, M) in a dagger category is called a *dagger (weak) factorisation system* when $e^\dagger$ is in M for each e in E, and $m^\dagger$ is in E for each m in M.[9]

The (weak) factorisation systems of **Rel** and **Hilb** of Examples 4.7 and 4.8 are obviously dagger (weak) factorisation systems with respect to the above dagger structure.

The next definition essentially states that a category $\mathbf{C}$ is dagger compactly accessible when it is a dagger category that is also compactly accessible, and $\mathbf{C}_{\text{cpt}}$ is dagger compact [Sel07].

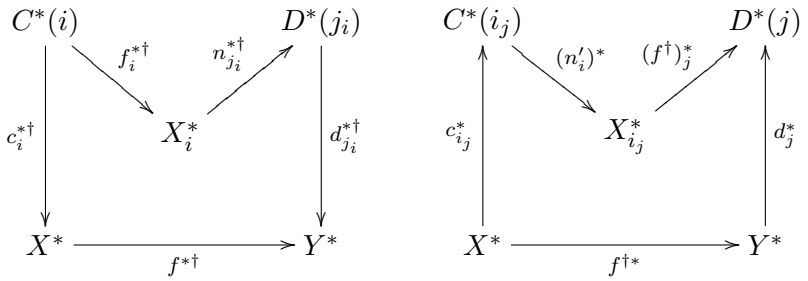
Definition 6.4. A *dagger compactly accessible category* is a compactly accessible category $\mathbf{C}$ that is also a dagger category, such that the weak factorisation system is a dagger weak factorisation system, and $\sigma \circ \varepsilon_X^\dagger = \eta_X : I \to X^* \otimes X$ for all $X \in \mathbf{C}_{\text{cpt}}$, where $\sigma : X \otimes X^* \to X^* \otimes X$ denotes the symmetry isomorphism.

Of course, our running example categories **Rel** and **Hilb** are both dagger compactly accessible categories, since $\mathbf{Rel}_{\text{cpt}}$ and $\mathbf{Hilb}_{\text{cpt}}$ are dagger compact categories.

The most important property of a dagger structure in relation to a compact category is that the dagger functor commutes with the choice-of-duals-functor. This provides 'complex conjugation'. This pleasant property is retained in full in dagger compactly accessible categories.

Theorem 6.5. *For every morphism $f : X \to Y$ in a dagger compactly accessible category $f^{\dagger *} = f^{*\dagger} : X^* \to Y^*$ holds.*

Proof. Since $(-)^\dagger$ is a strict involution, if $c_i : X \to C(i)$ is a limit cone, then $c_i^\dagger : C^\dagger(I) \to X$ is a colimit cocone, and vice versa. Moreover, since the weak factorisation system respects the dagger, if $f : X \to Z$ factors as $X \xrightarrow{e} Y \xrightarrow{m} Z$, then $f^\dagger : Z \to X$ factors as $Z \xrightarrow{m^\dagger} Y \xrightarrow{e^\dagger} X$. Hence in the defining diagrams of $f^{*\dagger}$ and $f^{\dagger *}$ below,



one has that $d_{j_i}^{*\dagger} \circ n_{j_i}^{*\dagger} \circ f_i^{*\dagger}$ and $d_j^{*\dagger} \circ (f^\dagger)_j^* \circ (n_i')^*$ form the same cocone. Since also $c_i^{*\dagger}$ and $c_{i_j}^{*\dagger}$ form the same cocone, the mediating morphisms $f^{*\dagger}$ and $f^{\dagger *}$ coincide. □

By the previous theorem, there is a covariant functor $(-)_* : \mathbf{C} \to \mathbf{C}$ determined by $X_* = X^*$ on objects and acting as $f_* = f^{*\dagger} = f^{\dagger *}$ on morphisms [Sel07, Definition 2.9]. In **Hilb** with its usual factorisation system (of Example 4.7), it maps a morphism to its complex conjugate.

[9] 'Factorisation' can be taken more literally by viewing M and E as subcategories of $\mathbf{C}$ and saying $\mathbf{C} = M \circ E$. A dagger factorisation system then resembles a square root, as $\mathbf{C} = E^\dagger \circ E$, or "$E = \sqrt{\mathbf{C}}$".

6.1. **Structure or property?** As a technical intermezzo, let us consider the status of compact accessibility: is it a structure or a property? A compactly accessible category requires a compactly presentable weak factorisation system. Initially it is not clear that this will uniquely exist. This makes compact accessibility into a structure, whereas compactness is a property.

First, notice that a compactly presentable factorisation system always exists. Any symmetric monoidal category has a compactly presentable factorisation system in which E is comprised of all isomorphisms and M consists of all morphisms.

This immediately shows that a compactly presentable factorisation system is not unique. A forteriori, this shows that the notion of compact presentability of objects is not independent of the chosen factorisation system: in **Rel** with the above factorisation system, every object is compactly presentable, whereas in **Rel** with the factorisation system of Example 4.8, only the finite sets are.

However, although these intermediate considerations might not be independent of the factorisation system used, the canonical extension of the choice-of-duals functor is, as soon as it is on objects. The following proposition states this rigorously.

Proposition 6.6. *Let (E, M) and (E', M') both be compactly presentable weak factorisation systems for a symmetric monoidal category $\mathbf{C}$. If objects X, Y are compactly presentable with respect to both factorisation systems, then X^*, Y^* are independent of the factorisation system used. Moreover, in that case f^* is independent of the factorisation system used for any morphism $f : X \to Y$.*

Proof. The claim on objects is just a reformulation of the hypothesis. Let us consider the claim on morphisms in the notation of Definition 5.9: suppose $c_i : C(i) \to X$ and $d_j : D(j) \to Y$ are colimit cones, and that $f \circ c_i$ factors as $m_i \circ e_i$ and $m'_i \circ e'_i$ in both factorisation systems, respectively. Then there are n_i and n'_i such that $m_i = d_{j_i} \circ n_i$ and $m'_i = d_{j'_i} \circ n'_i$. Since D is directed, there is a d_i with $d_i \circ n_i = m_i$ and $d_i \circ n'_i = m'_i$. So $d_i \circ n_i \circ e_i = f \circ c_i = d_i \circ n'_i \circ e'_i$, whence $e_i^* \circ n_i^* \circ d_i^*$ and $e_i'^* \circ n_i'^* \circ d_i^*$ form compatible cones, and both mediating morphisms f^* coincide. □

With the intuition of footnote 9, one might suspect that a factorisation system is unique in the presence of a dagger functor. In any factorisation system, each of the classes E and M is determined by the other via so-called orthogonality $E = M^\perp$ [Bor94, Proposition 5.5.3]. Thus, the larger E is, the smaller M can be. But compatibility with the dagger functor moreover requires $E = M^\dagger$, guaranteeing that E and M balance each other in size. However, here is an example of a dagger category with two different dagger compactly presentable factorisation systems. For any category $\mathbf{C}$, the cofree dagger category $\mathbf{C}_{\leftrightarrows}$ has the same objects; a morphism $X \to Y$ in $\mathbf{C}_{\leftrightarrows}$ consists of a pair of morphisms $f_\leftarrow : Y \to X$ and $f_\rightarrow : X \to Y$ of $\mathbf{C}$, with $(f_\leftarrow, f_\rightarrow)^\dagger = (f_\rightarrow, f_\leftarrow)$. All kinds of structures lift through this construction. If $\mathbf{C}$ is symmetric monoidal, so is $\mathbf{C}_{\leftrightarrows}$. An object in $\mathbf{C}$ is compact iff it is in $\mathbf{C}_{\leftrightarrows}$. An object in $\mathbf{C}$ is compactly presentable iff it is in $\mathbf{C}_{\leftrightarrows}$. A factorisation system for $\mathbf{C}$ lifts to a dagger factorisation system for $\mathbf{C}_{\leftrightarrows}$. Thus, a compactly presentable factorisation system for $\mathbf{C}$ lifts to a dagger compactly presentable factorisation system for $\mathbf{C}_{\leftrightarrows}$. Hence the above example in **Rel** provides an example of a dagger category $\mathbf{Rel}_{\leftrightarrows}$ with two different dagger compactly presentable factorisation systems.

Still, in all our example categories the dagger compactly presentable factorisation systems had a very canonical feel to them. All in all, dagger factorisation systems suggest themselves as a worthy subject of further study in their own right.

6.2. **Classical structures and measurements.** Finally, we need to model measurements in our semantics. These can be dealt with categorically [CP06] — the following definitions recall the necessary notions, adapted to the compactly accessible setting.

Definition 6.7. An object C in a dagger compactly accessible category $\mathbf{C}$ is said to be a *classical structure* when it is equipped with a commutative comonoid structure

$$C \otimes C \xleftarrow{\delta} C \xrightarrow{\epsilon} I$$

in which δ is an isometry, that moreover satisfies $\delta \circ \delta^\dagger = (\delta^\dagger \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \delta)$.

The precise meaning of the technical condition is not important here. The idea is that δ provides a 'copying' operation, and ϵ a 'deleting' operation. The definition thus counterfactually exploits the fact that quantum data cannot be cloned or forgotten. We remark that a classical structure (C, δ, ϵ) automatically satisfies Diagrams (3.1) with $C^* = C$, $\eta = \delta \circ \epsilon^\dagger$ and $\varepsilon = \epsilon \circ \delta^\dagger$. For more information we refer to [CP06].

We tentatively call an object in a dagger compactly accessible category that is not equipped with a fixed classical structure a *quantum object*. Any infinite-dimensional Hilbert space is a quantum object in **Hilb**, since it cannot carry any classical structure as that would entail finite-dimensionality [Koc03]. We refer to [CD08] for a way to select quantum objects representing qubits.

The type of a (demolition) measurement now is $X \to C$, for a classical structure C. As in the traditional Hilbert space formalism, we first define a basis, or projector-valued spectrum, in which to measure.

Definition 6.8. A *demolition projector-valued spectrum* on an object X in a dagger compactly accessible category $\mathbf{C}$ is a morphism $p : X \to C$, whose codomain C is a classical structure, that satisfies $p \circ p^\dagger = \mathrm{id}_C$.

In other words, a demolition projector-valued spectrum is the adjoint of an isometry, and hence the splitting of an idempotent [Sel06].

Now, a demolition measurement is nothing but a shell around a projector-valued spectrum that 'eliminates global phases' [CP06]. We ignore this and use measurement and projector-valued spectrum as synonyms.

7. Quantum key distribution, categorically

With dagger compactly accessible categories in place as a semantics, the stage is now set to model the quantum key distribution protocol in Figure 1. As mentioned before, as of yet we can only model the qualitative steps ①, ②, ③, ④ and ⑦ categorically. In fact, the entire purpose of a categorical semantics is to abstract away from the quantative details in steps ⑤ and ⑥. Though a categorical version of inequalities like Bell's would not be superfluous, it is outside of the scope of this article.

7.1. **The quantum channel.** The feature of the protocol in Figure 1 that cannot be accomodated in a dagger compact category is the possibly unbounded need for fresh qubit-pairs. Hence, as a preparation we set up an object from which to draw an a priori unknown number of qubit-pairs. Let $\mathbf{C}$ be a dagger compactly accessible category. Select a quantum

object X in $\mathbf{C}$, such that $X^* \otimes X$ is compactly presentable, to represent the qubit. Define a diagram $D : \mathbb{N} \to \mathbf{C}$ by

$$D(n) = (X^* \otimes X)^{\otimes n} = \underbrace{(X^* \otimes X) \otimes \cdots \otimes (X^* \otimes X)}_{n \text{ times}},$$

$$D(n \to n+1) : \ D(n) \xrightarrow[\cong]{} D(n) \otimes I \xrightarrow[\mathrm{id}\otimes\eta]{} D(n+1)$$

This is a directed compactly presentable diagram, and hence it has a colimit $Z = \mathrm{colim}(D)$. This object Z will function as a store of qubit-pairs that are guaranteed to be fresh; it models the quantum channel (and the index $\mathbb{N}$ of the colimit represents 'time'). Notice that this is not possible with X alone since that object is compact.[10]

One can now draw a fresh qubit-pair from the quantum channel Z as follows. Let $d_n : D(n) \to Z$ be a colimit cone. Then $\mathrm{id} \otimes d_{n-1} : D(n) \to (X^* \otimes X) \otimes Z$ forms another cone to Z, and hence there is a unique mediating morphism $d : Z \to (X^* \otimes X) \otimes Z$.

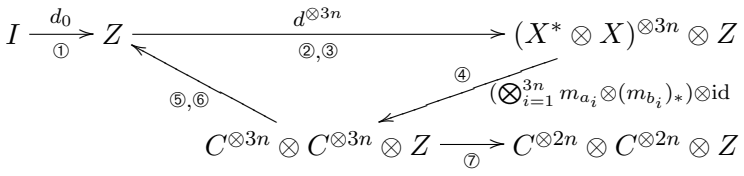
The following reasoning shows that $d : Z \to (X^* \otimes X) \otimes Z$ is in fact an isomorphism. Since $X^* \otimes X$ is a compact object, $(X^* \otimes X) \otimes (-)$ is cocontinuous by Proposition 3.6(e). Hence we have:

$$\begin{aligned}(X^* \otimes X) \otimes Z &= (X^* \otimes X) \otimes \operatorname*{colim}_n((X^* \otimes X)^{\otimes n}) \\ &\cong \operatorname*{colim}_n((X^* \otimes X)^{\otimes (n+1)}) \\ &\cong \operatorname*{colim}_n((X^* \otimes X)^{\otimes n}) = Z.\end{aligned}$$

Moreover, the diagram $I \xrightarrow{d_0} Z \xleftarrow{d^{-1}} (X^* \otimes X) \otimes Z$ is initial in the sense that for any given diagram $I \xrightarrow{f} A \xleftarrow{g} (X^* \otimes X) \otimes A$ there is a unique mediating morphism $Z \to A$. It is constructed via the colimit. We can understand Z as a list object with elements from $X^* \otimes X$: these objects are usually defined as initial algebras of the functor $1 + (X^* \otimes X) \otimes (-)$, but since our situation does not necessarily provide a coproduct we used cospans instead.[11]

Thus Z models the quantum channel, and $d : Z \to (X^* \otimes X) \otimes Z$ represents drawing one fresh qubit-pair prepared in Bell state.

7.2. **The categorical model of the protocol.** Having dealt with the qubit and the quantum channel, step ① now provides us with demolition measurements $m_i : X \to C$, where the classical structure C represents the bit. The protocol in Figure 1 can now be modelled as follows.



Since we chose to keep classical communication external, steps ②, ⑤, ⑥ and ⑦ depend on external events. Steps ⑤, ⑥ and ⑦ are modeled by forgetting the relevant information using ϵ, and step ② is fully external. Thus, the protocol is represented by a morphism $I \to C^{\otimes 2n} \otimes$

[10] There is a resemblance to type theory here: as X is a 'finite type', we need to have countably many copies of it to be able to draw countably many distinct variable letters.

[11] Naming the carrier of the initial diagram $(X^* \otimes X)^\star$ instead of Z would be apt but confusing.

$C^{\otimes 2n} \otimes Z$ with probability one: starting from nothing, Alice and Bob each end up having $2n$ bits, and there is still the possibility of obtaining fresh qubit-pairs on their shared quantum channel. The probabilistic branching, and in particular the (improbable) possibility of non-termination, could be dealt with more precisely using coalgebraic techniques [HJS06, BR97]. However, the above suffices as an illustration of the need for dagger compactly accessible categories.

We are now in a position to prove the correctness of the protocol categorically, *i.e.* to prove that Alice and Bob in fact end up with equal key bits, without assuming anything about the demolition measurements m_i or the external choices of a_i and b_i. It suffices to prove this for each individual key bit that arises from Alice and Bob using the same measurement, because step ⑦ discards the other bits. Hence the correctness of the protocol comes down to the following theorem.

Theorem 7.1. *The following diagram commutes for any demolition projector-valued spectrum $m : X \to C$.*

$$\begin{array}{ccccccccc}
Z & \xrightarrow{d} & X^* \otimes X \otimes Z & \xrightarrow{m_* \otimes m \otimes \mathrm{id}} & C^* \otimes C \otimes Z & \xrightarrow{\epsilon \otimes \mathrm{id} \otimes \mathrm{id}} & I \otimes C \otimes Z & \xrightarrow{\cong} & C \otimes Z \\
\| & & & & & & & & \| \\
Z & \xrightarrow[d]{} & X^* \otimes X \otimes Z & \xrightarrow[m_* \otimes m \otimes \mathrm{id}]{} & C^* \otimes C \otimes Z & \xrightarrow[\mathrm{id} \otimes \epsilon \otimes \mathrm{id}]{} & C \otimes I \otimes Z & \xrightarrow[\cong]{} & C \otimes Z
\end{array}$$

Proof. Because Z is only acted upon by the identity morphism, it suffices to prove commutativity of the following diagram.

$$\begin{array}{ccccccc}
I & \xrightarrow{\eta_X} & X^* \otimes X & \xrightarrow{m_* \otimes m} & C^* \otimes C & \xrightarrow{\epsilon \otimes \mathrm{id}} & I \otimes C & \xrightarrow{\cong} & C \\
\| & & & & & & & & \| \\
I & \xrightarrow[\eta_X]{} & X^* \otimes X & \xrightarrow[m_* \otimes m]{} & C^* \otimes C & \xrightarrow[\mathrm{id} \otimes \epsilon]{} & C^* \otimes I & \xrightarrow[\cong]{} & C
\end{array}$$

First, notice that

$$(m_* \otimes m) \circ \eta_X = (m_* \otimes m) \circ \ulcorner \mathrm{id}_X \urcorner \overset{(3.2)}{=} (m_* \otimes \mathrm{id}) \circ \ulcorner m \urcorner \overset{(3.2)}{=} \ulcorner m \circ m^\dagger \urcorner = \ulcorner \mathrm{id}_C \urcorner.$$

since $m \circ m^\dagger = \mathrm{id}$ by Definition 6.8. The commutativity of the above diagram is then established by the following calculation based on the properties of classical structures discussed after Definition 6.7.

$$\begin{aligned}
(\epsilon \otimes \mathrm{id}) \circ (m_* \otimes m) \circ \eta_X &= (\epsilon \otimes \mathrm{id}) \circ \ulcorner \mathrm{id}_C \urcorner \\
&= (\epsilon \otimes \mathrm{id}) \circ \delta \circ \epsilon^\dagger \\
&= (\mathrm{id} \otimes \epsilon) \circ \delta \circ \epsilon^\dagger \\
&= (\mathrm{id} \otimes \epsilon) \circ \ulcorner \mathrm{id}_C \urcorner \\
&= (\mathrm{id} \otimes \epsilon) \circ (m_* \otimes m) \circ \eta_X.
\end{aligned}$$

□

This protocol did not in fact use the choice-of-duals-functor on non-compact morphisms, because it only operates on compact parts of a non-compact object. However, it is entirely feasible that quantum protocols (or more general constructions in quantum physics) essentially rely on the choice-of-duals-functor on non-compact parts when modeled categorically.

8. Conclusion

With an eye towards applications in quantum theory, we developed the notion of a compactly accessible category using the structure of a factorisation system. It is a category that can contain objects that are not compact themselves, but are directed colimits of compact objects, thus allowing for infinite-dimensionality. Simultaneously, it has a functor that canonically extends the choice-of-duals on its compact part, and that commutes with a dagger structure if one is available. The need for such a category was illustrated by categorically modeling and proving correct a quantum key distribution protocol. The full structure of dagger compactly accessible categories was not needed for this specific example, in particular the extended choice-of-duals functor went unused. But in general an extended choice-of-duals functor is convenient and even arguably necessary. Moreover, in the presence of a dagger structure it hardly puts up more restrictions and hence is essentially for free.

Several connections to related research present themselves. First, a compact category has a canonical trace [Abr05]. Although the nuclear ideal setting [ABP99] seems ideal to study this phenomenon, perhaps the trace class morphisms can also be characterized by a colimit property, analogous to the passage from compact categories to compactly accessible ones. Secondly, compactly accessible categories can be seen as a 'technical implementation' of shape theory [Blu06], with the benefit of actually having concrete structure. One could look for the initial or terminal such implementation. Thirdly, the store of qubit-pairs in Section 7 strongly resembles Fock space [Vic07, BPS94], suggesting that compactly accessible categories might be naturally employed there. Lastly, one could develop a graphical calculus [Sel07] for (dagger) compactly accessible categories. However, for other purposes than aiding intuition, this seems a premature optimisation.

The presented material also indicates some directions for future research. First, a categorical version of the Bell inequalities would lend a definiteness to the categorical approach to quantum theory [AC04]. Secondly, the notion of complete positivity [Sel07] could be extended to compactly accessible categories. The usual formulation of a completely positive morphism in a dagger compact category relies essentially on the category being closed. As a dagger compactly accessible category is not necessarily closed (*e.g.* **Hilb**), a different characterization of complete positivity is in order. Thirdly, the connection to linear logic should be explored. Compact categories, as special cases of *-autonomous categories, model a large fragment of linear logic. It is also known that Barr's free construction of a *-autonomous category provides a model of full linear logic when one starts with an accessible category [Bar90]. Thus compactly presentable categories qualify as likely candidates to model linear logic, perhaps with unusual properties [Dun06]. Fourthly, locally presentable categories are known to be precisely the models of essentially algebraic theories. Likewise, accessible categories are precisely the axiomatisations by a basic theory in some many-sorted first-order logic [AR94]. One could look for similar results that characterise compactly presentable categories and compactly accessible categories as models of some algebraic theories. Lastly, extending a compact category to a compactly accessible one would be a valuable addition to the theory developed in this article, as we have motivated compactly accessible categories as an extension of compact ones, but gave only an axiomatic description. A conceivable starting point could be the fact that accessible categories are free cocompletions of small categories with respect to directed colimits [AR94, Theorem 2.26]. It would involve a completion of a factorisation system with directed colimits, which would likely involve a study of dagger factorisation systems in itself, as discussed in Section 6.1.

Acknowledgement

The author is most grateful to Bart Jacobs for his suggestions and encouraging feedback, and to Michael Barr, Bob Coecke, Jeff Egger and Isar Stubbe for helping to correct an erroneous example in previous presentations about this work. The anonymous referees made some detailed suggestions which improved the paper appreciably. Finally Rick Blute provided some helpful comments.

References

[ABP99] Samson Abramsky, Richard Blute, and Prakash Panangaden. Nuclear and trace ideals in tensored *-categories. *Journal of Pure and Applied Algebra*, 143:3–47, 1999.

[Abr05] Samson Abramsky. Abstract scalars, loops, and free traced and strongly compact closed categories. In *Proceedings of CALCO 2005*, volume 3629 of *Lecture Notes in Computer Science*, pages 1–31. Springer, 2005.

[AC04] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th IEEE conference on Logic in Computer Science*, pages 415–425. IEEE Computer Science Press, 2004.

[AF74] Frank Wylie Anderson and Kent R. Fuller. *Rings and categories of modules*. Springer, 1974.

[AJ94] Samson Abramsky and Achim Jung. Domain theory. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science Volume 3*, pages 1–168. Oxford University Press, 1994.

[AR94] Jiří Adámek and Jiří Rosicky. *Locally Presentable and Accessible Categories*. Cambridge University Press, 1994.

[Bar79] Michael Barr. **-autonomous categories*, volume 752 of *Lecture Notes in Mathematics*. Springer, 1979.

[Bar90] Michael Barr. Accessible categories and models of linear logic. *Journal of Pure and Applied Algebra*, 69:219–232, 1990.

[BB84] Charles H. Bennett and Giles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[Blu06] Richard Blute. Shape theory for nuclear ideals. *Theory and Application of Categories*, 2006. To appear.

[Bor94] Francis Borceux. *Handbook of Categorical Algebra*, volume 1. Cambridge University Press, 1994.

[BPP07] Richard Blute, Prakash Panangaden, and Dorette Pronk. Conformal field theory as a nuclear functor. In *Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin*, volume 172 of *Electronic Notes in Theoretical Computer Science*, pages 101–132. Elsevier, 2007.

[BPS94] Richard Blute, Prakash Panangaden, and Robert A. G. Seely. Holomorphic models of exponential types in linear logic. In *Proceedings of the 9th International Conference on Mathematical Foundations of Programming Semantics*, volume 802 of *Lecture Notes in Computer Science*, pages 474–512. Springer, 1994.

[BR97] Anna Bucalo and Giuseppe Rosolini. Lifting. In *Proceedings of the 7th International Conference on Category Theory and Computer Science*, volume 1290, pages 281–292. Springer, 1997.

[BW84] Michael Barr and Charles Wells. *Toposes, Triples and Theories*. Springer, 1984.

[CD08] Bob Coecke and Ross Duncan. Interacting quantum observables. In *ICALP (2)*, volume 5126 of *Lecture Notes in Computer Science*, pages 298–310. Springer, 2008.

[CKS84] Aurelio Carboni, Stefano Kasangian, and Ross Street. Bicategories of spans and relations. *Journal of Pure and Applied Algebra*, 33:259–267, 1984.

[CP06] Bob Coecke and Dusko Pavlovic. Quantum measurements without sums. In G. Chen, L. Kauffman, and S. Lamonaco, editors, *Mathematics of Quantum Computing and Technology*. Taylor and Francis, 2006.

[Day77] Brian J. Day. Note on compact closed categories. *Journal of the Australian Mathematical Society*, Series A 24(3):309–311, 1977.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[DR89] Sergio Doplicher and John E. Roberts. A new duality theory for compact groups. *Inventiones Mathematicae*, 98:157–218, 1989.
[Dun06] Ross Duncan. *Types for Quantum Computing*. PhD thesis, Oxford Computing Laboratory, 2006.
[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.
[FK72] Peter Freyd and Max Kelly. Categories of continuous functors I. *Journal of Pure and Applied Algebra*, 2, 1972.
[FS90] Peter Freyd and Andre Scedrov. *Categories, Allegories*. North-Holland, 1990.
[GU71] Peter Gabriel and Friedrich Ulmer. *Lokal präsentierbare Kategorien*. Number 221 in Lecture Notes in Mathematics. Springer, 1971.
[Hal82] Paul Halmos. *A Hilbert space problem book*. Springer, 2nd edition, 1982.
[HJS06] Ichiro Hasuo, Bart Jacobs, and Ana Sokolova. Generic trace theory. In *Proceedings of the 8th International Workshop on Coalgebraic Methods in Computer Science*, volume 164 of *Electronic Notes in Theoretical Computer Science*, pages 47–65. Springer, 2006.
[Isb57] John Isbell. Some remarks concerning categories and subspaces. *Canadian Journal of Mathematics*, 9:563–577, 1957.
[Jac53] Nathan Jacobson. *Lectures in Abstract Algebra, volume II: Linear Algebra*. Van Nostrand, Princeton, 1953.
[Joh82] Peter T. Johnstone. *Stone Spaces*. Cambridge University Press, 1982.
[Kel72] Max Kelly. *Many Variable Functorial Calculus I*, volume 281 of *Lectures Notes in Mathematics*, chapter Coherence in Categories, pages 66–106. Springer, 1972.
[KL80] Max Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.
[Koc03] Joachim Kock. *Frobenius algebras and 2-D Topological Quantum Field Theories*. Number 59 in London Mathematical Society Student Texts. Cambridge University Press, 2003.
[KR83] Richard V. Kadison and John R. Ringrose. *Fundamentals of the theory of operator algebras*. Academic Press, 1983.
[Lin76] Harald Lindner. *Monoidale und geschlossene Kategorien*. Habilitationsschrift, Universität Düsseldorf, 1976.
[Lin78] Harald Lindner. Adjunctions in monoidal categories. *Manuscripta Mathematica*, 26:123–139, 1978.
[Mac50] Saunders Mac Lane. Duality for groups. *Bulletin of the American Mathematical Society*, 56(6):485–516, 1950.
[Mac86] Saunders Mac Lane. *Mathematics, Form and Function*. Springer, 1986.
[Mac98] Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, 1998.
[MR77] Roberta B. Mura and Akbar Rhemtulla. *Orderable groups*, volume 27 of *Lecture Notes in Pure and Applied Mathematics*. New York: Marcel Dekker, 1977.
[Müg06] Michael Müger. Abstract duality for symmetric tensor *-categories. In *Handbook of the Philosophy of Physics*, pages 865–922. North Holland, 2006.
[Sad06] Mehrnoosh Sadrzadeh. High level quantum structures in linguistics and multi-agent systems. In P. Bruza, W. Lawless, and C. J. van Rijsbergen, editors, *AAAI Spring symposium on quantum interactions*, 2006.
[See89] Robert A. G. Seely. Linear logic, $*$-autonomous categories and cofree coalgebras. In John W. Gray and Andre Scedrov, editors, *Categories in Computer Science and Logic*, volume 92, pages 371–382. American Mathematical Society, 1989.
[Sel06] Peter Selinger. Idempotents in dagger categories. In *4th International Workshop in Quantum Programming Languages*, 2006.
[Sel07] Peter Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, 170:139–163, 2007.
[Vic07] Jamie Vicary. A categorical framework for the quantum harmonic oscillator. *International Journal of Theoretical Physics, to appear*, 2007.
[vN32] John von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer, 1932.