Parametric Iteration in Resource Theories

Alessandro Di Giorgio
Tallinn University of Technology, Estonia

Pawel Sobocinski
Tallinn University of Technology, Estonia

Niels Voorneveld
Cybernetica AS, Tartu, Estonia

Abstract

Many algorithms are specified with respect to a fixed but unknown parameter. Examples of this are especially common in cryptography, where protocols often feature a security parameter such as the bit length of a secret key.

Our aim is to capture this phenomenon in a more abstract setting. We focus on resource theories – general calculi of processes with a string diagrammatic syntax – introducing a general parametric iteration construction. By instantiating this construction within the Markov category of probabilistic Boolean circuits and equipping it with a suitable metric, we are able to capture the notion of negligibility via asymptotic equivalence, in a compositional way. This allows us to use diagrammatic reasoning to prove simple cryptographic theorems – for instance, proving that guessing a randomly generated key has negligible success.

2012 ACM Subject Classification Theory of computation → Program semantics; Theory of computation → Logic and verification; Mathematics of computing → Probability and statistics

Keywords and phrases Markov categories, Cryptography, String diagrams, Asymptotic equivalence

Digital Object Identifier 10.4230/LIPIcs.CSL.2026.29

Funding Di Giorgio, Voorneveld and Sobocinski were supported by the European Union under Grant Agreement No. 101087529. Sobocinski was additionally supported by the Estonian Research Council via grants PRG1215 and TEM-TA5 and the Estonian Center of Excellence in Artificial Intelligence (EXAI).

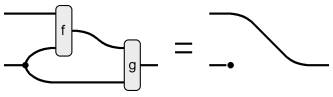
1 Introduction

Cryptographic protocols are designed to resist attacks by adversaries with bounded computational power. A fundamental feature is the use of a security parameter σ, which governs the time complexity of potential attacks. As σ increases, cryptographic schemes become more secure: for example, in public-key encryption, key lengths are chosen in relation to σ to ensure that brute-force attacks require time exponential in σ to succeed. More generally, security is often defined in asymptotic terms, stating that certain probabilities – such as the success rate of an adversary – become *negligible* as σ grows. This notion of negligibility from cryptography [14] also appears in other computational settings, such as approximation schemes in probabilistic algorithms. In both cases, reasoning about security or approximation guarantees requires a formal understanding of how computations depend on the parameter σ.

Traditionally, the definition of a cryptographic system follows a bottom-up approach: one chooses a model of computation, an algorithm and its notion of complexity, efficiency and security. This usually entails several technicalities that tend to hinder clarity and modularity. In particular, security proofs often become bogged down with low-level details of the computational model, making it difficult to generalise results, compare different cryptographic frameworks, or reason about their composition in a structured way.

This situation motivated the study of the subject at a higher level of abstraction, starting with the work of Canetti on Universal Composable Security [3] and followed by the work of Maurer and Renner on Abstract Cryptography [20, 19]. Motivated by similar intents, Broadbent and Karvonen [2] propose an abstract model of composable security definitions in terms of *resource theories*, formalised as symmetric monoidal categories.

The resource theoretic approach comes with the visual and intuitive language of string diagrams [13]. Consider the following example:

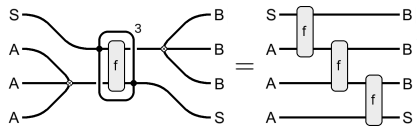


(1)

In the diagram above – read from left to right – we think of f and g as processes that transform the resources carried on the wires. The explicit splitting of wires via a *copier*, indicates that f and g share the second resource. If a resource is unused, as in the diagram on the right hand side, we simply *discard* it by closing the wire.

In cryptographic terms, we interpret the first input wire in (1) as carrying a message and the second as carrying a key. The processes f and g correspond to encryption and decryption, respectively. The equation postulates the correctness of the protocol: the original message – transformed into a cipher text by f – corresponds to the one decrypted by g. Equations between string diagrams such as these lead to proofs via *diagrammatic reasoning*, a powerful axiomatic technique that allows compositional reasoning about compound systems.

Our aim in this paper is to capture the notion of parametric algorithms within the abstract framework of resource theories. After a brief introduction to resource theories and their string diagrammatic language in Section 2, in Section 3 we define a notion of *iteration* bounded by an unspecified parameter, which we call $\star$-iteration. Perhaps unexpectedly, we do not study traces (as, e.g., in monoidal streams [9]) but instead define a functorial construction: given a morphism $f\colon S \otimes A \to B \otimes S$, we define $\tau^k_{S,(A),(B)}(f)\colon S \otimes A^k \to B^k \otimes S$ as its k-fold iteration. Below we give a diagrammatic representation of $\tau^k_{S,(A),(B)}(f)$, when $k = 3$.



Iterated morphism consumes and produces *lists* of resources of type A and B, respectively. The resource of type S can be thought of as a *state* carried over by the computation. A similar construction is found in probabilistic programming languages [11, 24], where iteration is usually bounded. Interestingly, useful results can be proved about iteration *without* instantiating the parameter. To this end, we introduce a technique we dub the *diagonal method* that allows us to prove useful, general results that add to the arsenal of diagrammatic reasoning about abstract resource theories with parametric iteration.

Parametric iteration is a feature that extends the expressivity of resource theories. Our main application in this paper is motivated by cryptography, and the notion of *negligibility* in particular. To do this, we work within a *probabilistic* resource theoretical context. This is the category $\mathsf{FinStoch}_{\{1,0\}}$ of Boolean stochastic maps. It is both a Markov category and one that possesses a *probabilistic choice structure*, which we introduce in Section 4. As a notable property, the probabilistic case structure ensures a unique (up to isomorphism) normal form for probabilistic Boolean functions. This, in turn, allows us to derive a completeness result (Theorem 11). While not essential to the main developments of the paper, it provides an interesting alternative proof to the one found in [21].

Formally, we first move from symmetric monoidal categories to metric-enriched ones, so that morphisms, i.e. processes, are equipped with a notion of *distance* between them (see e.g. [8, 17]).

We reconcile metric-enrichment with the parameterized iteration construction in Section 5, where we introduce a notion of *asymptotic equivalence* on morphisms. This captures negligibility – also referred to as *indistinguishability* – between processes. Intuitively, two processes f and g, potentially involving parametric iterations, are considered indistinguishable if their distance approaches 0 as the parameter σ tends to ∞. In related work [16], such notions of indistinguishability are studied in a bounded linear λ-calculus.

Guided by cryptographic intuitions, we conclude with some examples. Notably, we formally prove that a randomly generated key is unlikely to be any specific key (Lemma 21), and show we can asymptotically approximate fair choice with weighted choice with the iterated von Neumann trick (Lemma 22). We also discuss how we can perform arithmetic over the cyclic groups of sizes 2^σ and $2^\sigma - 1$, which is useful for instance in Diffie-Hellman key exchange and Zero knowledge proofs.

The paper presents two theoretical contributions. We define the parametrized iteration construction on symmetric monoidal categories, prove that it forms a category, preserves several categorical structures, and admits an endofuctor $\tau^\star$ for parametrized iteration. We moreover define the notion of asymptotic equivalence on the parametrized iteration over a metric-enriched symmetric monoidal category, and show that it defines a congruence and is preserved under the application of $\tau^\star$.

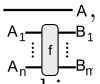
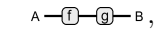
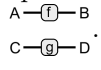
The paper includes appendices containing additional material and omitted proofs.

2 Symmetric Monoidal Categories as Resource Theories

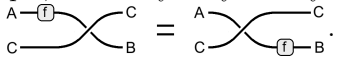
In this section we give a brief introduction to symmetric monoidal categories (SMCs) and their associated graphical calculus [13, 23, 22] in terms of resource theories, following [6].

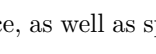
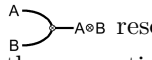
The basic data consists of objects $A, B, C, \ldots$ that we think of as types of resources, and morphisms $f\colon A \to B$, which we think of as transformations that convert a resource of type A into one of type B. Morphisms can be composed sequentially: given $f\colon A \to B$ and $g\colon B \to C$, their composite $f;g\colon A \to C$ represents performing f followed by g.

The monoidal product $\otimes$ lets us express having two resources at once – so $A \otimes C$ means having both A and C – and it extends to morphisms too: given $f\colon A \to B$ and $g\colon C \to D$, the morphism $f \otimes g\colon A \otimes C \to B \otimes D$ describes applying f and g in parallel. There is also a void resource I that acts neutrally under combination: $A \otimes I = A$.

These ideas are captured visually using the graphical calculus of string diagrams. A resource type A is drawn as a wire , and a transformation $f\colon A_1 \otimes \ldots \otimes A_n \to B_1 \otimes \ldots \otimes B_m$ is represented by a box  with n input wires on the left and m output wires on the right. Composition of morphisms is shown by connecting boxes in sequence  , while the monoidal product corresponds to placing them side-by-side  . The void resource I corresponds to no wires at all – i.e., the empty diagram.

Resources can also be swapped according to the symmetry $\chi_{A,B}\colon A \otimes B \to B \otimes A$, which is represented by a crossing of wires  .

Diagrams are subject to the axioms of symmetric monoidal categories (SMCs). However, note that equational reasoning in this setting amounts to deformation of diagrams without changing their topology. For example, naturality of symmetry amounts to sliding a box past a crossing of wires, illustrated as  .

In the next section, where we introduce the parametric iteration construction, it will be convenient to explicitly track both the combination of resources via the monoidal product and the void resource. Therefore, following [4], we extend the graphical calculus with operations that introduce  and discard the void resource, as well as split  and combine  resources. These operations are subject to the expected equations determined by the properties of the monoidal product.

Finally, note that all monoidal categories considered in this paper are taken to be strict, as justified by Mac Lane's strictification theorem [18].

3 Parametric Iteration

We define a category of parametric iterations over a symmetric monoidal category. We do this by introducing the concept of $\star$-iteration, which expresses the idea of iterating an operation a fixed yet unspecified number of times. We do not a priori choose how many times to iterate, the operations are *parametrized* over this yet to be specified choice of number of iterations.

We define parametric iteration over $\mathcal{C}$ in two stages. First we define the *free iteration construction* $\mathsf{FI}(\mathcal{C})$ which adds the relevant objects and operations which will be used to express iteration. We then quotient this category to create the *parametric iteration construction* $\mathsf{PI}(\mathcal{C})$ over $\mathcal{C}$, giving an interpretation to the added objects and operations.

We define the objects of $\mathsf{FI}(\mathcal{C})$ inductively as follows:

$$\frac{A \in \mathcal{C}}{(\!|A|\!) \in \mathsf{FI}(\mathcal{C})} \qquad \frac{A, B \in \mathsf{FI}(\mathcal{C})}{A \otimes B \in \mathsf{FI}(\mathcal{C})} \qquad \frac{A \in \mathsf{FI}(\mathcal{C})}{A^\star \in \mathsf{FI}(\mathcal{C})}$$

satisfying the equations $(\!|I|\!) \otimes A = A = A \otimes (\!|I|\!)$, $(\!|A|\!) \otimes (\!|B|\!) = (\!|A \otimes B|\!)$, and $(A \otimes B) \otimes C = A \otimes (B \otimes C)$. Here $A^\star$ represents a $\star$-tuple, that is a tuple of A's, with the exact number of elements bounded by an external parameter.

Given a tuple of objects $\mathbf{A} = (A_1, \ldots, A_n)$, we write $\mathbf{A} \cdot \star = A_1^\star \otimes \cdots \otimes A_n^\star$, and for each $k \in \mathbb{N}$, $\mathbf{A} \cdot k = A_1^k \otimes \cdots \otimes A_n^k$, following notation from [5], where A^k is the k-th power of A with respect to $\otimes$. In particular, $\mathbf{A} \cdot 1 = A_1 \otimes \cdots \otimes A_n$.

Morphisms of $\mathsf{FI}(\mathcal{C})$ are given inductively as follows:

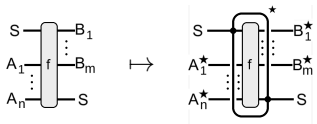
$$\frac{f : A \to B \in \mathcal{C}}{(\!|f|\!) : (\!|A|\!) \to (\!|B|\!)} \qquad \frac{A \in \mathsf{FI}(\mathcal{C})}{id_A : A \to A} \qquad \frac{f : A \to B \quad g : B \to C}{f ; g : A \to C} \qquad \frac{f : A \to B \quad g : C \to D}{f \otimes g : A \otimes C \to B \otimes D}$$

$$\frac{A, B \in \mathsf{FI}(\mathcal{C})}{\chi_{A,B} : A \otimes B \to B \otimes A} \qquad \frac{f : S \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes S}{\tau^\star_{S,\mathbf{A},\mathbf{B}}(f) : S \otimes \mathbf{A} \cdot \star \to \mathbf{B} \cdot \star \otimes S}$$

satisfying the relevant equations making $\mathsf{FI}(\mathcal{C})$ into a symmetric monoidal category, together with the equations $(\!|id_A|\!) = id_{(\!|A|\!)}$, $(\!|f ; g|\!) = (\!|f|\!) ; (\!|g|\!)$, $(\!|\chi_{A,B}|\!) = \chi_{(\!|A|\!),(\!|B|\!)}$, $(\!|f \otimes g|\!) = (\!|f|\!) \otimes (\!|g|\!)$. The latter equations make $(\!|-|\!) : \mathcal{C} \to \mathsf{FI}(\mathcal{C})$ sending A to $(\!|A|\!)$ and f to $(\!|f|\!)$ into a symmetric monoidal functor.

Here $\tau^\star$ is the operation which represents $\star$-iteration, transforming a list of $\star$-tuples $\mathbf{A} \cdot \star$ into a list of $\star$-tuples $\mathbf{B} \cdot \star$ by going through the elements one by one, carrying over the state S between iterations. We annotate $\tau^\star$ by lists telling us exactly how the input and output of f is divided into different tuples. For instance, if $f : S \otimes A^2 \to B \otimes S$, we could either create $\tau^\star_{S,(A^2),(B)}(f) : S \otimes (A^2)^\star \to B^\star \otimes S$ or $\tau^\star_{S,(A,A),(B)}(f) : S \otimes A^\star \otimes A^\star \to B^\star \otimes S$, where $(A^2)^\star$ is a $\star$-tuple of elements of A^2, and $A^\star \otimes A^\star$ are two $\star$-tuples of elements of A.

String diagrammatically, we denote $\tau^{\star}_{S,\mathbf{A},\mathbf{B}}(f)$ as follows:

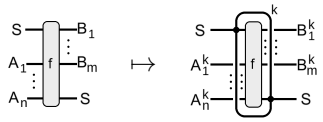


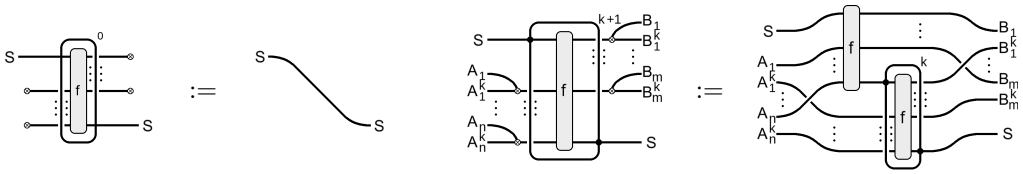
Here we mark *state wires* with a $\bullet$, and the $\star$-tuples with an interrupted wire. Each non-state wire is part of a different tuple. We may use multiple or no state wires as well.

We give an interpretation of iteration by defining τ^k as an operation on symmetric monoidal categories describing a constant number of k iterations. Given a symmetric monoidal category $\mathcal{C}$, we can inductively define operations $\mathsf{push}^k_{\mathbf{A}} : \mathbf{A}\cdot 1 \otimes \mathbf{A}\cdot k \to \mathbf{A}\cdot(k+1)$ and $\mathsf{pop}^k_{\mathbf{A}} : \mathbf{A}\cdot(k+1) \to \mathbf{A}\cdot 1 \otimes \mathbf{A}\cdot k$ which respectively pushes and pops the first element of each tuple of objects in $\mathbf{A}\cdot(k+1)$. For instance, if $\mathbf{A} = (X, Y)$, then $\mathsf{push}^3_{\mathbf{A}} : X \otimes Y \otimes X^2 \otimes Y^2 \to X^3 \otimes Y^3$ simply swaps the second and third element.

Given a morphism $f : S \otimes \mathbf{A}\cdot 1 \to \mathbf{B}\cdot 1 \otimes S$ in $\mathcal{C}$, we inductively define $\tau^k_{S,\mathbf{A},\mathbf{B}}(f) : S \otimes \mathbf{A}\cdot k \to \mathbf{B}\cdot k \otimes S$ for each $k \in \mathbb{N}$ as:

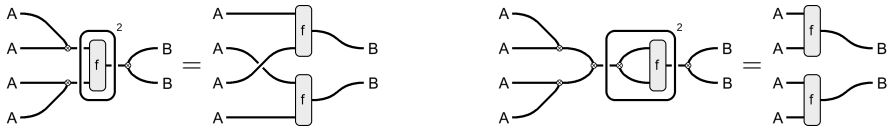
- $\tau^0_{S,\mathbf{A},\mathbf{B}}(f) = id_S$,
- $\tau^{k+1}_{S,\mathbf{A},\mathbf{B}}(f) = (id_S \otimes \mathsf{pop}^k_{\mathbf{A}}); (f \otimes id_{\mathbf{A}\cdot k}); (id_{\mathbf{B}\cdot 1} \otimes \tau^k_{S,\mathbf{A},\mathbf{B}}(f)); (\mathsf{push}^k_{\mathbf{B}} \otimes id_S)$.





Contrary to $\tau^{\star}$, the annotations for τ^k serve a further clarifying role, as they are also necessary for removing ambiguity even in those instances where the type of the produced morphism is known. Without this specification, the input may be wrongly distributed into separate tuples. For instance, a τ^3 iteration having A^6 as input, could consider this either as two triples of A, or one triple of A^2, which lead to different interpretations. In terms of string diagrams, we can keep the convention that each string represents a different tuple, which avoids the need for putting annotations in the string diagrams.

▶ **Example 1.** Suppose $f : A \otimes A \to B$, then $\tau^2_{1,(A,A),(B)}(f)$ and $\tau^2_{1,(A^2),(B)}(f)$ have the same type but yield two different results, represented respectively as string diagrams as follows:



For any $k \in \mathbb{N}$, we define a functor $S_k : \mathsf{FI}(\mathcal{C}) \to \mathcal{C}$ inductively as follows, first on objects:

- $S_k(\langle\!|A|\!\rangle) = A$,
- $S_k(A \otimes B) = S_k(A) \otimes S_k(B)$,
- $S_k(A^{\star}) = (S_k(A))^k$.

For $\mathbf{A} = (A_1, \ldots, A_n)$, then $S_k(\mathbf{A}) = (S_k(A_1), \ldots, S_k(A_n))$. S_k is defined on morphisms as:

- $S_k(id_A) = id_{S_k(A)}$,
- $S_k(\langle\!|f|\!\rangle) = f$,
- $S_k(f; g) = S_k(f); S_k(g)$,
- $S_k(f \otimes g) = S_k(f) \otimes S_k(g)$,
- $S_k(\chi_{A,B}) = \chi_{S_k(A),S_k(B)}$.

For $f : S \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes S$, then $S_k(\tau^\star_{S,\mathbf{A},\mathbf{B}}(f)) = \tau^k_{S,S_k(\mathbf{A}),S_k(\mathbf{B})}(S_k(f))$.

▶ **Definition 2.** *Two morphisms $f, g : A \to B$ in $\mathsf{FI}(\mathcal{C})$ are $\star$-equivalent if for any $k \in \mathbb{N}$, $S_k(f) = S_k(g)$. The parametric iteration category $\mathsf{PI}(\mathcal{C})$ of $\mathcal{C}$ is defined as $\mathsf{FI}(\mathcal{C})$ quotiented over this notion of $\star$-equivalence.*

We have a symmetric monoidal functor $\langle\!|-|\!\rangle : \mathcal{C} \to \mathsf{PI}(\mathcal{C})$ and for each $k \in \mathbb{N}$ a symmetric monoidal functor $S_k : \mathsf{PI}(\mathcal{C}) \to \mathcal{C}$. We consider the image of $\langle\!|-|\!\rangle$ in $\mathsf{PI}(\mathcal{C})$ as the constant fragment of $\mathsf{PI}(\mathcal{C})$. It holds that $S_k \circ \langle\!|-|\!\rangle$ is the identity functor on $\mathcal{C}$ for each $k \in \mathbb{N}$.

Before we continue on and prove results regarding $\star$-equivalence, we introduce a powerful proof technique we call the *diagonal method*. Consider $\mathsf{PI}(\mathsf{PI}(\mathcal{C}))$, which has two nested parametric iteration constructions, the second we label with $\star'$. We construct a symmetric monoidal functor $M : \mathsf{PI}(\mathsf{PI}(\mathcal{C})) \to \mathsf{PI}(\mathcal{C})$ that unifies the two iterations, i.e. it satisfies:

- $M(A^{\star'}) = M(A^\star) = (MA)^\star$,
- $M(\tau^{\star'}_{S,\mathbf{A},\mathbf{B}}(f)) = M(\tau^\star_{S,\mathbf{A},\mathbf{B}}(f)) = \tau^\star_{MS,M\mathbf{A},M\mathbf{B}}(Mf)$.

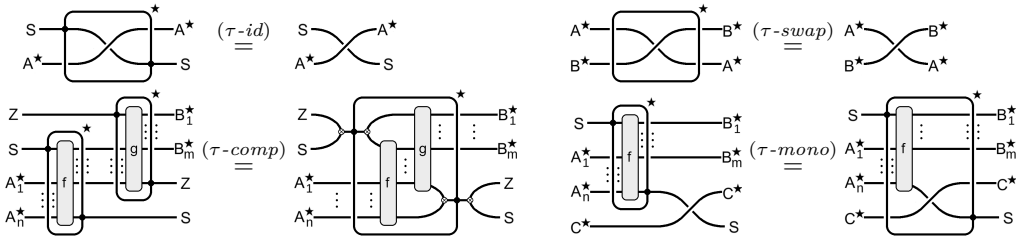
▶ **Lemma 3.** *There is a functor $M : \mathsf{PI}(\mathsf{PI}(\mathcal{C})) \to \mathsf{PI}(\mathcal{C})$ satisfying the properties above.*

Proof. Let us consider the obvious functor $M' : \mathsf{FI}(\mathsf{PI}(\mathcal{C})) \to \mathsf{PI}(\mathcal{C})$. We prove that M' preserves $\star$-equivalence. Let f and g be $\star$-equivalent morphisms in $\mathsf{FI}(\mathsf{PI}(\mathcal{C}))$, then for any $k \in \mathbb{N}$, $S_k(f) = S_k(g)$ in $\mathsf{PI}(C)$. So for any $r \in \mathbb{N}$, $S_r(S_k(f)) = S_r(S_k(g))$ in $\mathcal{C}$. Note that the S_k instantiates the $\star'$, and the S_r the $\star$.

Now, for any $k \in \mathbb{N}$, $S_k(M'f) = S_k(S_k(f)) = S_k(S_k(g)) = S_k(M'g)$, hence $M'f = M'g$. So M' preserves $\star$-equivalence and can be factored through $\mathsf{PI}(\mathsf{PI}(\mathcal{C}))$ creating M. ◀

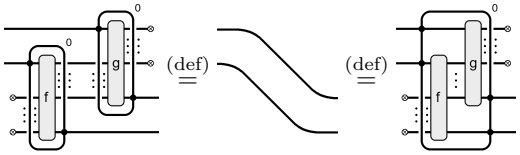
In practice, this allows us to prove $\star$-equivalence between morphisms by instantiating some of the iteration operations but not necessarily all. We can do this as long as we can find a separation into two iteration types, marking a choice of top level $\star$-iterations as $\star'$ in a way that type checks. We now have sufficient tools to prove some useful properties.

▶ **Lemma 4.** *The following equations hold:*

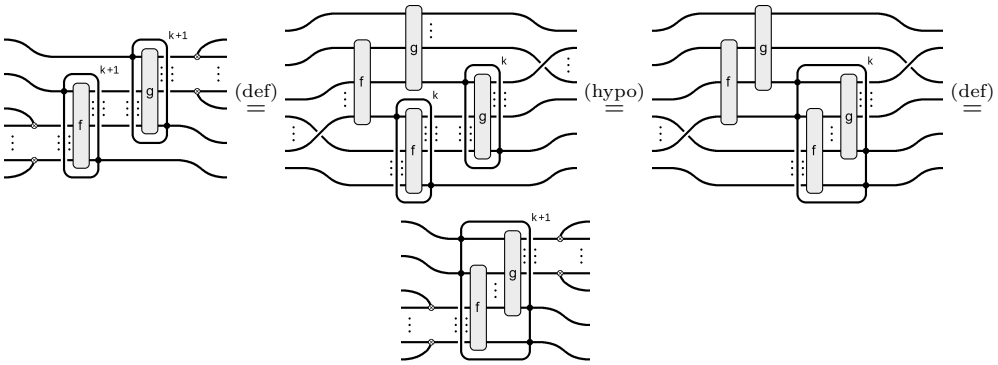


Proof. Let us prove (τ-comp), the other equations are shown in Appendix A. We use the diagonal method, instantiating only the outer iteration operations. We perform induction on those instantiations:

Induction basis:



Induction step:

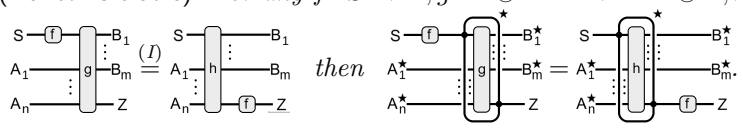


◀

▶ **Corollary 5.** *There is a symmetric monoidal endofunctor on $\mathsf{PI}(\mathcal{C})$ given by $A \mapsto A^\star$ and $f : A \to B \mapsto \tau^\star_{I,(A),(B)}(f)$.*

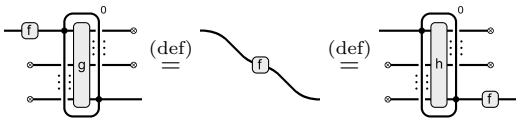
The following property is particularly useful in forthcoming examples:

▶ **Lemma 6** (Newton's cradle). *For any $f\colon S \to Z, g\colon Z \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes Z, h\colon S \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes S$, if*

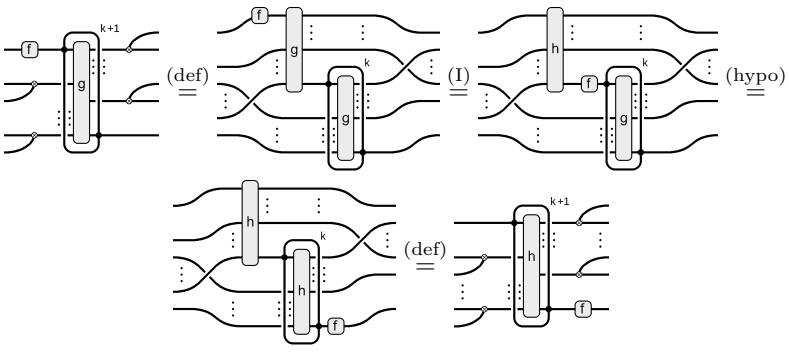


Proof. We use the diagonal method, and choose to instantiate only the top level iterations. We show by induction on $k \in \mathbb{N}$ that for each instantiation by k the equation holds.

Induction basis:



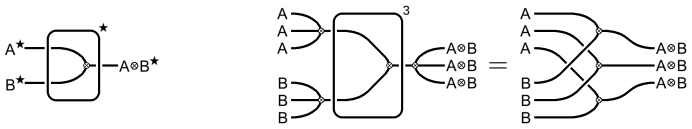
Induction step:



◀

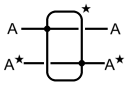
Let us look at two examples which occur in $\mathsf{PI}(\mathcal{C})$ for any symmetric monoidal category $\mathcal{C}$.

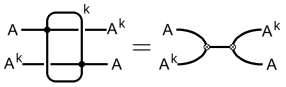
▶ **Example 7.** Consider *zipping* two $\star$-tuples using $\tau_{I,(A,B),(A\otimes B)}(id_{A\otimes B})$:



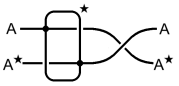
On the right we see an example instantiation performing three iterations. The zip operations gives one direction of an isomorphism between $A^\star \otimes B^\star$ and $(A \otimes B)^\star$.

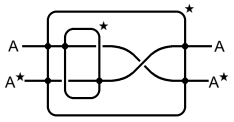
▶ **Example 8.** The morphism $\tau^\star_{A,(A),(A)}(id_{A^2}) : A^\star \otimes A \to A^\star \otimes A$ pushes a new element to the front of a $\star$-tuple, and pops the last element from the $\star$-tuple to make room.

$\tau^\star_{A,(A),(A)}(id_{A^2}) =$ 

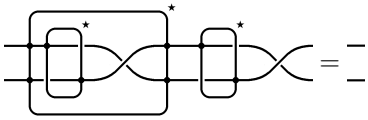
$\tau^k_{A,(A),(A)}(id_{A^2}) =$ 

We can use this to cycle forward and backward through the elements of a $\star$-tuple. We take $\mathsf{cycle}_A = \tau^\star_{A,(A),(A)}(id_{A^2}); \chi_{A^\star,A}$ and $\mathsf{cycle\text{-}back}_A = \tau^\star_{A\otimes A^\star,(),()}(\mathsf{cycle}_A)$,

$\mathsf{cycle}_A =$ 

$\mathsf{cycle\text{-}back}_A =$ 

Here we cycle back by cycling forward one less than what is needed to get back to where we started. Concretely, note that $S_k(\mathsf{cycle}_A) = \chi_{A^k,A}$, and for any $a, b \in \mathbb{N}$, $\chi_{A^{a+1},A^b}; \chi_{A^{a+b},A} = \chi_{A^b,A^{b+1}}$, so by induction, $S_k(\mathsf{cycle\text{-}back}_A) = (\chi_{A^k,A})^k = \chi_{A,A^k}$, so $S_k(\mathsf{cycle\text{-}back}_A; \mathsf{cycle}_A) = \chi_{A,A^k}; \chi_{A^k,A} = id_{A^{k+1}}$. We conclude that:



4 Reasoning with Probabilities and Distances

To model richer computational behaviors, we consider symmetric monoidal categories with additional properties and structure. In particular, for probabilistic computations, we focus on metric-enriched symmetric monoidal categories and Markov categories [10].

▶ **Definition 9.** *A* Markov category with probabilistic choice *is a symmetric monoidal category equipped with operations* $!_A \colon A \to I$, $\blacktriangleleft_A \colon A \to A \otimes A$, $\langle p \rangle \colon I \to \mathbb{B}$ *and* $\phi_A \colon A \otimes \mathbb{B} \otimes A \to A$, *represented in string diagrams, respectively, as*

where $p \in [0, 1]$, $\mathbb{B}$ *is a designated object and* A *is any object, and such that the axioms in Figure 1 hold. That is:*

- $(\blacktriangleleft_A, !_A)$ *is a cocommutative comonoid, that is* $\blacktriangleleft_A$ *is associative* ($\blacktriangleleft$-as), *cocommutative* ($\blacktriangleleft$-co) *and* $!_A$ *is the unit* ($\blacktriangleleft$-un),
- $\blacktriangleleft_A$ *and* $!_A$ *are coherent with the monoidal structure,*

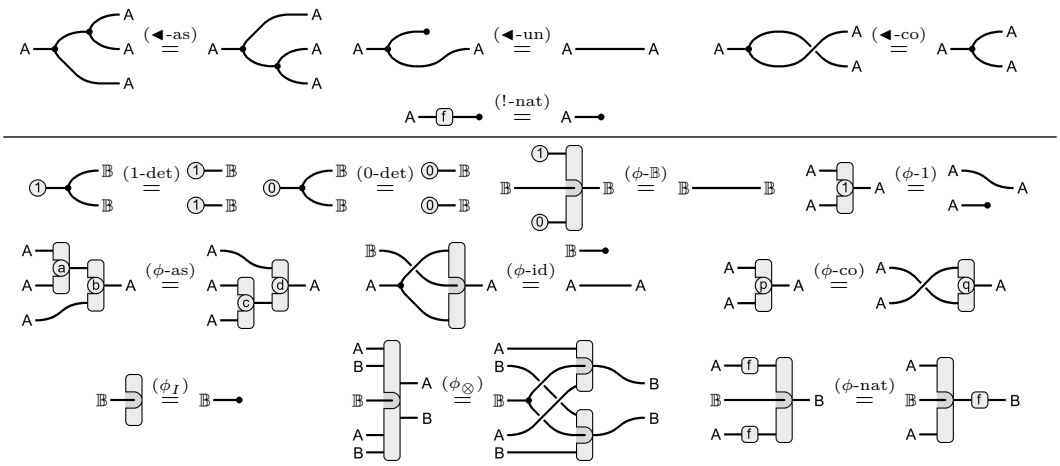


Figure 1 Axioms for Markov categories (top) and probabilistic choice (bottom). Here $f\colon A \to B$, $q = 1-p$, $c = \frac{(1-a)b}{1-ab}$ and $d = ab$.

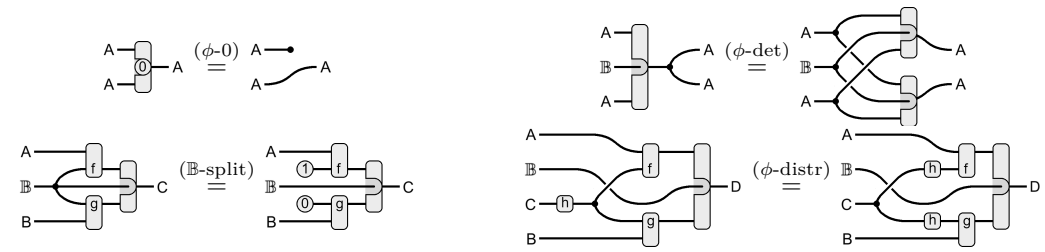
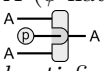
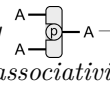


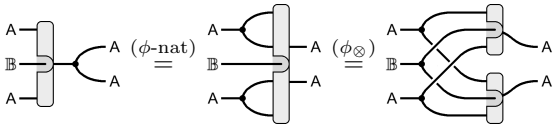
Figure 2 Derived laws for Markov categories with probabilistic choice.

- $!_A$ *is natural* (!-nat),
- $\langle 1\rangle$ *and* $\langle 0\rangle$ *are deterministic (*(1-det) *and* (0-det)*),*
- ϕ_A *is coherent with the monoidal structure (*(ϕ_I) *and* $(\phi_\otimes)$*),*
- ϕ_A *is natural in* A (ϕ-nat),
- ϕ^p_A*–where* ϕ^p_A *is*  *, often simply*  *–is a convex algebra, that is,* ϕ^p_A *is idempotent* (ϕ-id) *and satisfies parametric associativity* (ϕ-as) *and commutativity* (ϕ-co)*,*
- ϕ *and* $\langle 1\rangle$, $\langle 0\rangle$ *interact via* (ϕ-$\mathbb{B}$) *and* (ϕ-1)*.*

The $\mathbb{B}$ represents the type of two bit values, 1 and 0. $\langle p\rangle$ describes a weighted coin flip, which has a chance of p of producing 1, and a chance of $1-p$ of producing 0. The ϕ represents an *if-gate*, choosing between two results of the same type using a bit as an argument.

▶ **Lemma 10.** *The laws in Figure 2 hold in any Markov category with probabilistic choice.*

Proof. We give a proof only for (ϕ-det), the rest can be found in Appendix C.



◀

Our leading example of Markov category with probabilistic choice is $\mathsf{FinStoch}$, the category of sets and stochastic maps. Objects are sets and morphisms $f\colon A \to B$ are functions $A \to \mathcal{D}B$ mapping each $a \in A$ to a finitely-supported discrete probability distribution over B. We represent a distribution as a function $v : A \to [0,1]$ with finite support $\mathsf{supp}(v) := \{a \in A \mid v(a) > 0\}$ and such that $\sum_{a\in A} v(a) = 1$, or, alternatively, as a formal sum $\sum_i p_i \,|a_i\rangle$, where the $|\cdot\rangle$ notation is used to separate the elements $a_i \in A$ from their associated probability $p_i \in [0,1]$.

We write $f(b|a)$ for $f(a)(b)$, representing the probability that f returns b, given a. For two stochastic maps $f\colon A \to B, g\colon B \to C$, their composition is defined by summing over the middle variable, i.e. $(f;g)(c \mid a) := \sum_{b\in B} g(c \mid b)f(b \mid a)$. Identities $id_A\colon A \to A$ map each $a \in A$ to the Dirac distribution at a, i.e. $id_A(a) := |a\rangle$.

Given two distributions $v \in \mathcal{D}A$ and $u \in \mathcal{D}B$, their product $v \otimes w \in \mathcal{D}(A \times B)$ is given by $v \otimes u(a,b) := v(a)u(b)$. This yields a symmetric monoidal structure, with the monoidal product $\otimes$ being the cartesian product of sets $\times$ on objects and with monoidal unit the singleton set $I := \{\bullet\}$. For arrows $f\colon A \to B$ and $g\colon C \to D$, $f \otimes g\colon A \otimes C \to B \otimes D$ is defined as $f \otimes g(b,d|a,c) := f(b|a)g(d|c)$, and symmetries $\chi_{A,B}\colon A \otimes B \to B \otimes A$ as $\chi_{A,B}(a,b) := |b\rangle \otimes |a\rangle$.

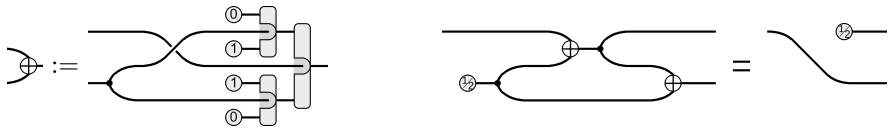
The comonoid structure is given by $\blacktriangleleft_A\,(a) := |a\rangle \otimes |a\rangle$ and $!_A(a) := |\bullet\rangle$, while for the probabilistic choice structure we take as choice object the set of Booleans $\{1,0\}$ and, for any $p \in [0,1]$, we define $\langle p\rangle\colon \{\bullet\} \to \{1,0\}$ as $\langle p\rangle(\bullet) := p\,|1\rangle + (1-p)\,|0\rangle$ and $\phi_A\colon A \otimes \{1,0\} \otimes A \to A$ as $\phi_A(a,1,b) := |a\rangle$ and $\phi_A(a,0,b) := |b\rangle$. Note that $\phi^p_A(a,b) = p\,|a\rangle + (1-p)\,|b\rangle$.

Throughout the rest of the paper we will work in $\mathsf{FinStoch}_{\{1,0\}}$, the subcategory of $\mathsf{FinStoch}$ consisting of stochastic maps between sets that are powers of the booleans. The structure of Markov category with probabilistic choice, introduced here, is novel and it offers an alternative presentation of $\mathsf{FinStoch}_{\{1,0\}}$ to the one in [21]. In particular:

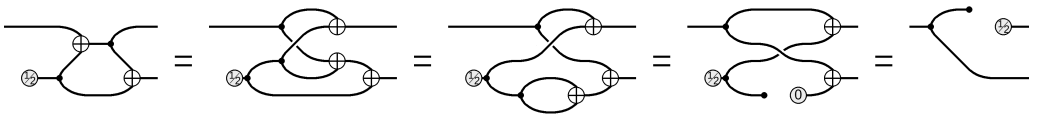
▶ **Theorem 11.** *the axioms in Figure 1 are* complete *for* $\mathsf{FinStoch}_{\{1,0\}}$.

The interested reader can find the details in Appendix B.

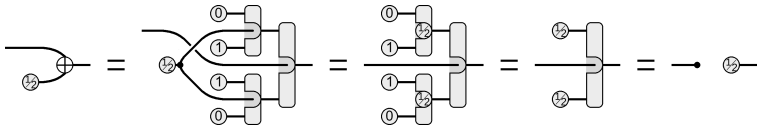
As an example of diagrammatic reasoning in $\mathsf{FinStoch}_{\{1,0\}}$ we look at the *one-time-pad* protocol on a single bit. We regard $\langle\frac{1}{2}\rangle\colon I \to \mathbb{B}$ as an operation that produces a randomly generated bit, and the xor $\oplus\colon \mathbb{B} \otimes \mathbb{B} \to \mathbb{B}$, defined below on the left, as an operation that encrypts and decrypts a bit.



The equation on the right expresses the correctness of the protocol: encoding and decoding with the same randomly generated bit gets the same result, and that to an adversary the encrypted message looks completely random. We prove correcteness by equational reasoning:



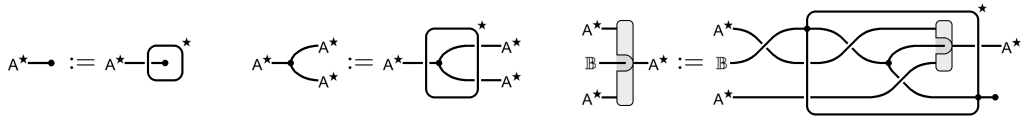
The equations use the fact that $\oplus$ is deterministic, associative, idempotent, unitary with respect to $\langle 0\rangle$ and nullary with respect to $\langle\frac{1}{2}\rangle$. All of these properties can be proved via the axioms of Markov categories with probabilistic choice. For example the fact that $\langle\frac{1}{2}\rangle$ is absorbing for $\oplus$ is proved using the laws in Figure 2 as follows:



Looking at $\mathsf{PI}(\mathsf{FinStoch}_{\{1,0\}})$, the above example can be extended to operations on $\mathbb{B}^\star$, encrypting and decrypting $\star$-tuples of bits. We now show that the parametric iteration construction preserves the structure of Markov categories with probabilistic choice.

▶ **Lemma 12.** *If $\mathcal{C}$ is a Markov category with probabilistic choice, then so is $\mathsf{PI}(\mathcal{C})$.*

Proof. For $\mathbb{B}$ we can take $(\!|\mathbb{B}|\!)$, and for $\langle p \rangle$ we take $(\!|\langle p \rangle|\!)$. We define discard $!_{A\star}$, copy $\blacktriangleleft_{A\star}$ and case $\phi_{A^\star}$ for $\mathsf{PI}(\mathcal{C})$ inductively on objects, with their definition on $A^\star$ being:



The relevant properties can be shown using the diagonal method, with the naturality equations in particular being instances of Newton's cradle. ◀

4.1 Quantitative Reasoning

The theory developed in the previous section allows for exact reasoning about boolean stochastic maps, enabling us to derive precise equalities between them.

However, in some cases – especially when parametric iteration is involved – we are interested in reasoning about approximate equivalence instead. To do so, we must move to metric-enriched symmetric monoidal categories. We begin by recalling some basic definitions.

▶ **Definition 13.** *A* metric space (A, d) *consists of a set A and a distance function $d : A \times A \to [0, \infty)$ such that for all $a, b, c \in A$:*

$$d(a,b) = 0 \Leftrightarrow a = b, \qquad d(a,b) = d(b,a), \qquad d(a,c) \leq d(a,b) + d(b,c). \tag{2}$$

A morphism between metric spaces $f : (A, d_A) \nrightarrow (B, d_B)$ *is given by a non-expansive function $f : A \to B$, that is a function satisfying $d_B(f(a), f(b)) \leq d_A(a, b)$ for all $a, b \in A$.*

▶ **Definition 14.** *The category $\mathbb{M}$ has metric spaces as objects and non-expansive functions as arrows. This is a monoidal category, with $\otimes$ defined on objects as the metric space $(A \otimes B, d_{A\otimes B})$, where $A \otimes B$ is the cartesian product of sets and $d_{A\otimes B}((a,b),(a',b')) := d_A(a,a') + d_B(b,b')$, and on arrows as $(f \otimes g)(a,c) := (f(a), g(c))$, for every $f\colon (A, d_A) \nrightarrow (B, d_B)$ and $g\colon (C, d_C) \nrightarrow (D, d_D)$.*

Our objects of study in this section are *metric enriched monoidal categories*, or categories enriched over $\mathbb{M}$. Unfolding the definition, a metric enriched monoidal category is a category whose homs are metric spaces, such that:

$$d_{A\to C}(f; g, f'; g') \leq d_{A\to B}(f, f') + d_{B\to C}(g, g') \tag{3}$$

and

$$d_{A\otimes C\to B\otimes D}(f \otimes g, f' \otimes g') \leq d_{A\to B}(f, f') + d_{C\to D}(g, g'). \tag{4}$$

▶ **Lemma 15.** $\mathsf{FinStoch}$ *is a metric enriched symmetric monoidal category.*

Proof. For each set A, we can define a metric tv_A on $\mathcal{D}A$ called the *total variation metric* (see e.g. [15]). We give two equivalent formulations of tv_A below, for any $v, w \in \mathcal{D}A$.

$$\mathsf{tv}_A(v,w) := \sum_{a \in \mathtt{supp}(v) \cup \mathtt{supp}(w)} \frac{|v(a) - w(a)|}{2} = 1 - \sum_{a \in \mathtt{supp}(v) \cap \mathtt{supp}(w)} \mathtt{min}(v(a), w(a))$$

We take as distance between arrows $d_{A \to B}(f,g) := \mathtt{max}_{a \in A} \mathsf{tv}_B(f(a), g(a))$, for every $f, g \colon A \to B$ in $\mathsf{FinStoch}$. This choice of distance makes $\mathsf{FinStoch}$ metric enriched (see Example 3.2.7 in [12]). ◀

Just as we approached exact reasoning equationally, we now aim to reason quantitatively in a similar style. To this end, we introduce a proof system that axiomatizes distances between morphisms of metric-enriched Markov categories with probabilistic choice.

$$\frac{}{f \equiv_0 f} \quad \frac{}{f \equiv_1 g} \quad \frac{f \equiv_\delta g}{g \equiv_\delta f} \quad \frac{f \equiv_\delta g \quad g \equiv_{\delta'} h}{f \equiv_{\delta + \delta'} h} \quad \frac{f \equiv_\delta g \quad \delta \leq \delta'}{f \equiv_{\delta'} g} \quad \frac{f \equiv_\delta f' \quad g \equiv_\delta g'}{(f \otimes id_{\mathbb{B}} \otimes g); \phi_X \equiv_\delta (f' \otimes id_{\mathbb{B}} \otimes g'); \phi_X}$$
$$\frac{f \equiv_\delta f'}{f;g \equiv_\delta f';g} \quad \frac{g \equiv_\delta g'}{f;g \equiv_\delta f;g'} \quad \frac{f \equiv_\delta f'}{f \otimes g \equiv_\delta f' \otimes g} \quad \frac{g \equiv_\delta g'}{f \otimes g \equiv_\delta f \otimes g'} \quad \frac{f \equiv_\delta f' \quad g \equiv_\gamma g'}{(f \otimes g); \phi^p_X \equiv_{p \cdot \delta + (1-p) \cdot \gamma} (f' \otimes g'); \phi^p_X} \tag{5}$$

We write $f \equiv_\delta g$ to say that f and g, of the same type, are provably at most δ away from each other. Moreover, we say that a proof system is *sound* if $f \equiv_\delta g$ implies $d(f,g) \leq \delta$, and is *complete* if $f \equiv_{d(f,g)} g$ for each pair of morphisms f, g of the same type.

Note that a sound proof system allows one to prove upper bounds to the actual distance between morphisms. As such, certain proofs give better bounds than others, allowing one to improve on a proof of distance by finding different routes. In particular, in order to prove security, one would like to prove that certain distances are below a level of allowed risk ε.

We now show that the proof system above is sound and complete for $\mathsf{FinStoch}_{\{1,0\}}$, equipped with the total variation distance.

This approach varies from the total variation treatment in [17], where the monoidal product combines different cases (disjunctive), whereas in our case the monoidal product combines resources (conjunctive).

▶ **Lemma 16.** *The proof system in* (5) *is sound and complete for* $\mathsf{FinStoch}_{\{1,0\}}$.

Proof. See Appendix C. ◀

5 Asymptotic Equivalence

For a metric enriched symmetric monoidal category $\mathcal{C}$, we can equip $\mathsf{PI}(\mathcal{C})$ with a notion of asymptotic equivalence. A nonnegative function $f \colon \mathbb{N} \to [0, \infty)$ *approaches zero*, written as $\lim_{k \to \infty} f(k) = 0$, if for any possible threshold $\varepsilon \in (0, \infty)$ there is some point $N \in \mathbb{N}$ after which the function is below ε. Symbolically: $\forall \varepsilon > 0. \, \exists N > 0. \, \forall k \geq N. \, f(k) < \varepsilon$.

From the perspective of cryptography, we consider ε the risk factor we are trying to beat, or the allowable failure rate of our algorithm. Then $N > 0$ is the minimum security parameter to guarantee that the actual probability of failure is below the allowable risk.

The following definition captures indistinguishability between morphisms in $\mathsf{PI}(\mathcal{C})$, given that they may be investigated a polynomial number of times by the distinguisher (e.g. adversary), and this distinguisher may choose a polynomial amount of inputs and study each probabilistically generated output.

▶ **Definition 17** (Asymptotic Equivalence)**.** *For a metric enriched symmetric monoidal category* C*, the asymptotic equivalence relation* $\equiv$ *on morphisms of* $\mathsf{PI}(\mathsf{C})$ *is defined as follows:*

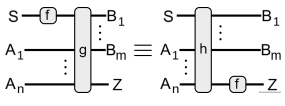
$$f \equiv g \iff \forall a \in \mathbb{N}. \lim_{k \to \infty} k^a \cdot d(S_k(f), S_k(g)) = 0 \qquad \text{for any } f, g \colon X \to Y \text{ in } \mathsf{PI}(\mathsf{C}).$$

▶ **Proposition 18.** $\equiv$ *is preserved under sequential composition and parallel composition.*

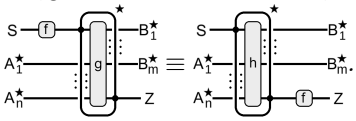
Proof. Suppose $f \equiv f'$ and $g \equiv g'$. Take $k \in \mathbb{N}$, and $\varepsilon > 0$, then by assumption on $\varepsilon/2$ there are N and M such that if $n \geq N$ and $n \geq M$, then respectively $n^k \cdot d(S_n(f), S_n(f')) < \varepsilon/2$ and $n^k \cdot d(S_n(g), S_n(g')) < \varepsilon/2$. Taking $K = \max(N, M)$, then for $n \geq K$ we get $n^k \cdot d(S_n(f;g), S_n(f';g')) = n^k \cdot d(S_n(f); S_n(g), S_n(f'); S_n(g')) \leq n^k \cdot (d(S_n(f), S_n(f')) + d(S_n(g), S_n(g'))) = n^k \cdot d(S_n(f), S_n(f')) + n^k \cdot d(S_n(g), S_n(g')) < \varepsilon/2 + \varepsilon/2 = \varepsilon$. The proof for parallel composition is analogous. ◀

We can show that the Newton's cradle equation from before also holds for asymptotic equivalence. We prove this using a method similar to the diagonal method. As a consequence, asymptotic equivalence is preserved under application of the $\star$-iteration operation $\tau^\star$.

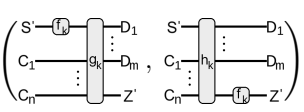
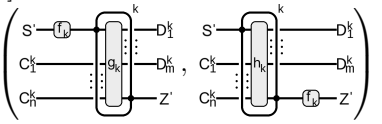
▶ **Lemma 19** (Newton's cradle, reprised). *For any* $f\colon S \to Z, g\colon Z \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes Z, h\colon S \otimes \mathbf{A} \cdot 1 \to \mathbf{B} \cdot 1 \otimes S$, *if*

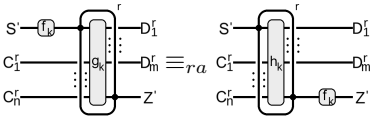


then

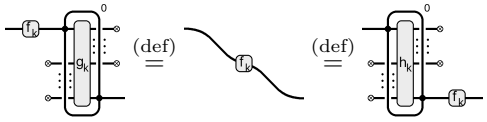


Proof. Let $k \in \mathbb{N}$, and take $S' = S_k(S)$, $Z' = S_k(Z)$, $\mathbf{C} = S_k(\mathbf{A})$, $\mathbf{D} = S_k(\mathbf{B})$, $f_k = S_k(f)$, $g_k = S_k(g)$, and $h_k = S_k(h)$. We shall define $a \in [0, 1]$ as:

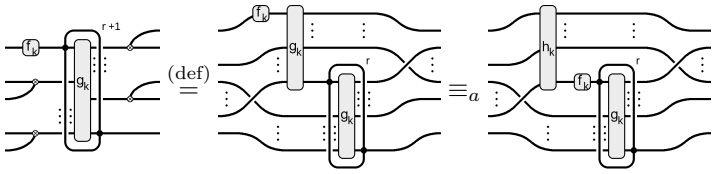
$a := d\Big($  $\Big)$ and prove that $d\Big($  $\Big) \leq ka$

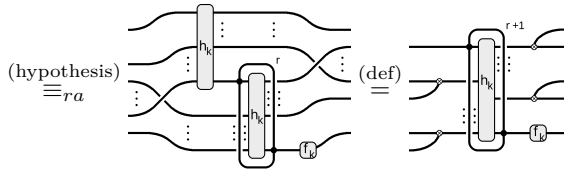
We prove this, by showing by induction on $r \in \mathbb{N}$ that:  $\equiv_{ra}$

Induction basis:



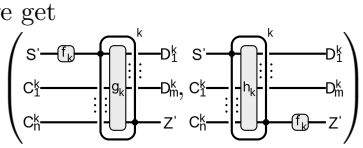
Induction step:





together getting an upper bound for the distance of $a + ra = (r + 1)a$, as required.

Taking $r = k$, we get a distance of ka between the two sides of the equation. Hence, given any $b \in \mathbb{N}$ we get

$\lim_{k\to\infty} k^b d\Big($  $\Big) = \lim_{k\to\infty} k^{b+1} d\Big($ $\Big) = 0$

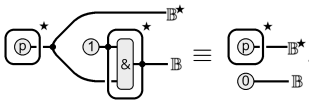
◀

5.1 Examples

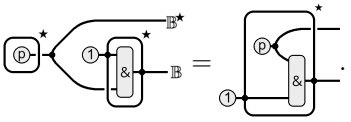
Asymptotic equivalence is used to reason whether it is possible to increase the security parameter to significantly minimize the risk of two programs being distinguished. This allows us to formally ignore undesirable situations if their probability of occurring is asymptotically insignificant, or in other words: *negligible*. Our first example shows that a randomly generated key of length σ is unlikely to be any specific key. This has three useful consequences:

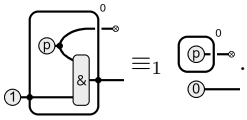
1. Two randomly generated keys of length σ are not equal (asymptotically).
2. If an adversary attempts to guess a key before that key is generated (or without any knowledge of the generated key), then this guess is wrong (asymptotically).
3. We can uniformly generate an element of $\mathbb{Z}_{2^\sigma-1}$ (asymptotically),

We first define $\mathsf{all\text{-}1} : \mathbb{B}^\star \to \mathbb{B}$ which checks if all elements of $\mathbb{B}^\star$ are equal to 1. Given an and-gate $\& : \mathbb{B}^2 \to \mathbb{B}$, we define $\mathsf{all\text{-}1} := (\langle 1 \rangle \otimes id_{\mathbb{B}^\star}); \tau^\star_{\mathbb{B},(\mathbb{B}),()}(\&)$.

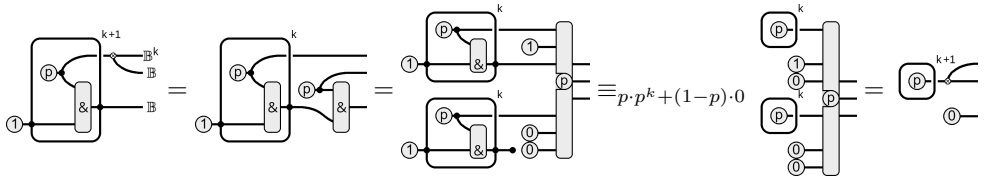
▶ **Lemma 20.** *If $p < 1$, then*  .

Proof. By induction on k, we can prove that the two diagrams as seen through S_k in the Lemma statement are at most p^k apart in the underlying metric-enriched category (to cover an edge-case we use $0^0 = 1$). Given that $p < 1$, we have that for any a, $\lim_{k\to\infty} k^a \cdot p^k = 0$.

First, observe that by (τ-comp) and (τ-mono),  .

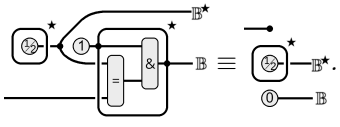
For $k = 0$, the required distance $\equiv_1$ is trivially true, i.e.  .

For $k' = k + 1$, we do the following steps.



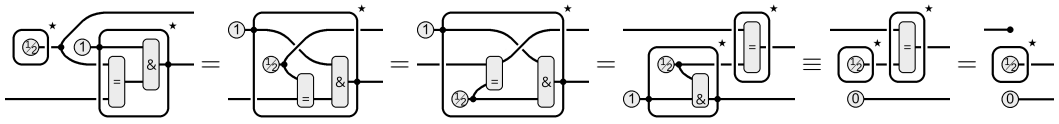
◀

In other words, no randomly generated key with weighted choice below 1 consists of only ones. Note in particular that this is the case even if the key is used in some other context. We define equality on bits using a negated xor gate $(=) : \mathbb{B}^2 \to \mathbb{B}$. Then equality on $\star$-tuples $(=)^\star : \mathbb{B}^\star \otimes \mathbb{B}^\star \to \mathbb{B}$ is done by iterating the equality and checking that all entries are one.

▶ **Lemma 21.** 

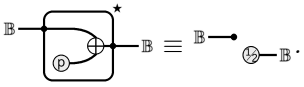
Proof. First, we merge the two iterations into one using (τ-comp) and (τ-mono). Then we can reorder $\langle 1/2 \rangle$ and $(=)$ operations in such a way that they still give the same probabilistic stochastic map. Thirdly, we can separate the iteration into two iterations, and apply

Lemma 20 to the first iteration. Lastly, merge the two remaining iterations again and note that equality to a random bit gives a random bit (similar to what we observed with xor before).



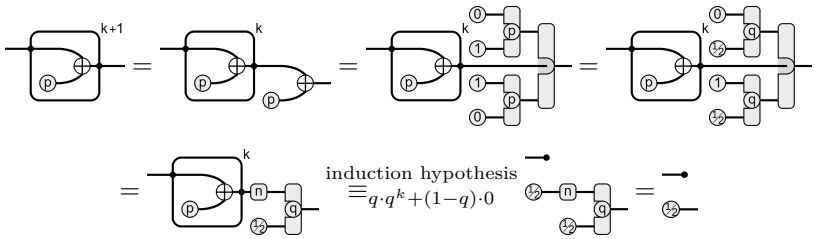
◀

We consider one final example, the iterated von Neumann's trick. This is a method for simulating a fair coin flip using a biased coin that lands on heads with probability $p \in (0, 1)$. The method involves flipping the biased coin twice and selecting the first outcome if both flips match; otherwise, the process is repeated. When a form of parametric iteration is available, the trick can be formalised as Example 11 in [24]. Here we give a categorical and diagrammatic representation as the diagram in the lemma.

▶ **Lemma 22.** 

Proof. The equation above states that the process of flipping a bit with probability p a total of k-times converges to a fair coin flip as k increases. We prove this by showing that for a constant number k of iterations, the two diagrams are $(2p-1)^k$ away if $p \geq 1/2$, and $(1-2p)^k$ away if $p \leq 1/2$. In both cases, the distance approaches zero exponentially.

We shall look at the case in which $p \geq 1/2$, the other case goes similarly. We prove the result by induction on k, as follows. The base case holds since everything is 1 away from everything else, which satisfies the condition. For the inductive step, let $k' = k + 1$ and observe that the following holds true, where we take $q = 2p - 1$ and $h = q^k$ the distance from the induction hypothesis. We write $n : \mathbb{B} \to \mathbb{B}$ for the not gate, then:



◀

6 Conclusions and Future Work

This work is a step towards an algebraic approach to cryptographic proofs completely parametric in security parameters. Such proofs normally entail showing that all protocols have polynomial time complexity with respect to the parameters, and require intricate probabilistic calculations. Binding the parameter helps avoid unsound proof pitfalls, such as accidentally using asymptotic rewriting while performing induction over number of iterations.

In order to incorporate further cryptographic protocols however, we need two further extensions. First, we need to allow for cryptographic primitives, which should be given as families of operations in $\mathcal{C}$ indexed over the security parameter, with accompanying assumptions regarding distances. This should be possible by extending $\mathcal{C}$ accordingly, and deriving further equations once one takes the parametric iteration over $\mathcal{C}$.

The second extension entails dealing with operations like *pseudorandom number generators*, as e.g. used in stream ciphers. In the current framework, we cannot generate more randomness from less. Concretely, we theoretically cannot have a morphism $f : \mathbb{B}^\star \to \mathbb{B}^\star \otimes \mathbb{B}$ such that $\tau^\star(\langle\frac{1}{2}\rangle); f \equiv \tau^\star(\langle\frac{1}{2}\rangle) \otimes \langle\frac{1}{2}\rangle$. The solution to this problem is to define a coarser relation, that of *contextual equivalence* relative to contexts of morphisms which can only investigate a finite amount of data, meaning whose input and output are constant (from $\mathcal{C}$). Our notion of asymptotic equivalence is (trivially) sound with respect to this notion of contextual equivalence, though further investigation of this relation is for future research.

On the topic of probabilistic computations, we use the fact that all our computations are total, which is reflected in the naturality property of our if-gate operation. Extending to partial probabilistic computations, we should generalize to partial Markov categories with a condition/equality operation. Our if-gate as well as the discard operation will only be natural over all total computations (those not involving conditioning). In order to more accurately model an if-statement as might be used in a programming language, we should either introduce a more structured functorial if operation, or move towards distributive monoidal categories and their associated languages of tape/sheet diagrams [1, 7].

References

1 Filippo Bonchi, Cipriano Junior Cioffo, Alessandro Di Giorgio, and Elena Di Lavore. Tape Diagrams for Monoidal Monads. In Corina Cîrstea and Alexander Knapp, editors, *11th Conference on Algebra and Coalgebra in Computer Science (CALCO 2025)*, volume 342 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:24, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CALCO.2025.11.

2 Anne Broadbent and Martti Karvonen. Categorical composable cryptography: extended version. *Logical Methods in Computer Science*, Volume 19, Issue 4, December 2023. doi:10.46298/lmcs-19(4:30)2023.

3 Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001. doi:10.1109/SFCS.2001.959888.

4 Titouan Carette, Dominic Horsman, and Simon Perdrix. Szx-calculus: Scalable graphical quantum reasoning. In *MFCS 2019-44th International Symposium on Mathematical Foundations of Computer Science*, volume 138, pages 55–1, 2019.

5 Apiwat Chantawibul and Pawel Sobocinski. Monoidal multiplexing. In B. Fischer and T. Uustalu, editors, *Theoretical Aspects of Computing ? ICTAC 2018*, volume 11187, pages 116–131. Springer, October 2018. doi:10.1007/978-3-030-02508-3_7.

6 Bob Coecke, Tobias Fritz, and Robert W Spekkens. A mathematical theory of resources. *Information and Computation*, 250:59–86, 2016. doi:10.1016/J.IC.2016.02.008.

7 Cole Comfort, Antonin Delpeuch, and Jules Hedges. Sheet diagrams for bimonoidal categories. *arXiv preprint arXiv:2010.13361*, 2020.

8 Ugo Dal Lago, Furio Honsell, Marina Lenisa, and Paolo Pistone. On Quantitative Algebraic Higher-Order Theories. In Amy P. Felty, editor, *7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)*, volume 228 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:18, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.FSCD.2022.4.

9 Elena Di Lavore, Giovanni de Felice, and Mario Román. Monoidal streams for dataflow programming. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '22, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3531130.3533365.

10 Tobias Fritz. A synthetic approach to Markov kernels, conditional independence and theorems on sufficient statistics. *Advances in Mathematics*, 370:107239, 2020. arXiv:1908.07021.

11 Steven Holtzen, Guy Van den Broeck, and Todd Millstein. Scaling exact inference for discrete probabilistic programs. *Proceedings of the ACM on Programming Languages*, 4(OOPSLA):1–31, 2020. doi:10.1145/3428208.

12 Nicholas Gauguin Houghton-Larsen. A mathematical framework for causally structured dilations and its relation to quantum self-testing. *arXiv preprint arXiv:2103.02302*, 2021. arXiv:2103.02302.

13 André Joyal and Ross Street. The geometry of tensor calculus, I. *Advances in Mathematics*, 88(1):55–112, July 1991. doi:10.1016/0001-8708(91)90003-P.

14 Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman & Hall/CRC, 2nd edition, 2014.

15 A.N. Kolmogorov and S.V. Fomin. *Introductory Real Analysis*. Selected Russian publications in the mathematical sciences. Prentice-Hall, 1970. URL: https://books.google.nl/books?id=914PAQAAMAAJ.

16 Ugo Dal Lago, Zeinab Galal, and Giulia Giusti. On computational indistinguishability and logical relations. In *Programming Languages and Systems: 22nd Asian Symposium, APLAS 2024, Kyoto, Japan, October 22-24, 2024, Proceedings*, pages 241–263, Berlin, Heidelberg, 2024. Springer-Verlag. doi:10.1007/978-981-97-8943-6_12.

17 Gabriele Lobbia, Wojciech Różowski, Ralph Sarkis, and Fabio Zanasi. Quantitative Monoidal Algebra: Axiomatising Distance with String Diagrams. In Paweł Gawrychowski, Filip Mazowiecki, and Michał Skrzypczak, editors, *50th International Symposium on Mathematical Foundations of Computer Science (MFCS 2025)*, volume 345 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 68:1–68:21, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2025.68.

18 Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 1998.

19 Ueli Maurer. Constructive cryptography–a new paradigm for security definitions and proofs. In *Joint Workshop on Theory of Security and Applications*, pages 33–56. Springer, 2011. doi:10.1007/978-3-642-27375-9_3.

20 Ueli Maurer and Renato Renner. Abstract cryptography. In Bernard Chazelle, editor, *Innovations in Computer Science - ICS 2011, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 1–21. Tsinghua University Press, 2011. URL: http://conference.iiis.tsinghua.edu.cn/ICS2011/content/papers/14.html.

21 Robin Piedeleu, Mateo Torres-Ruiz, Alexandra Silva, and Fabio Zanasi. A complete axiomatisation of equivalence for discrete probabilistic programming. In *Programming Languages and Systems: 34th European Symposium on Programming, ESOP 2025, Held as Part of the International Joint Conferences on Theory and Practice of Software, ETAPS 2025, Hamilton, ON, Canada, May 3–8, 2025, Proceedings, Part II*, pages 202–229, Berlin, Heidelberg, 2025. Springer-Verlag. doi:10.1007/978-3-031-91121-7_9.

22 Robin Piedeleu and Fabio Zanasi. *An Introduction to String Diagrams for Computer Scientists*. Elements in Applied Category Theory. Cambridge University Press, 2025.

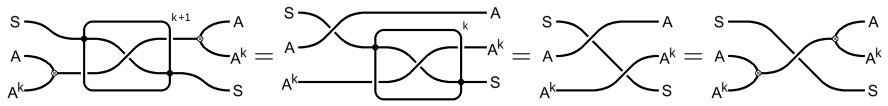
23 P. Selinger. *A Survey of Graphical Languages for Monoidal Categories*, volume 813 of *Lecture Notes in Physics*, pages 289–355. Springer, Berlin, Heidelberg, 2010. doi:10.1007/978-3-642-12821-9_4.

24 Mateo Torres-Ruiz, Robin Piedeleu, Alexandra Silva, and Fabio Zanasi. On iteration in discrete probabilistic programming. In *9th International Conference on Formal Structures for Computation and Deduction (FSCD 2024)*, volume 299 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:21. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.FSCD.2024.20.

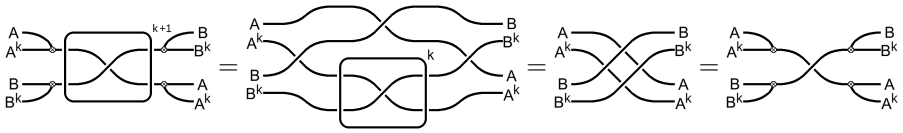
A Appendix to Section 3

Extended proof of Lemma 4. We prove each property using the diagonalisation method, instantiating the top level iterations by k. We prove the relevant equation by induction on k. The base case is relatively simple. We prove the induction steps below, unfolding once, then using the induction hypothesis, and finishing with an optional refolding.

Induction step for (τ-id):

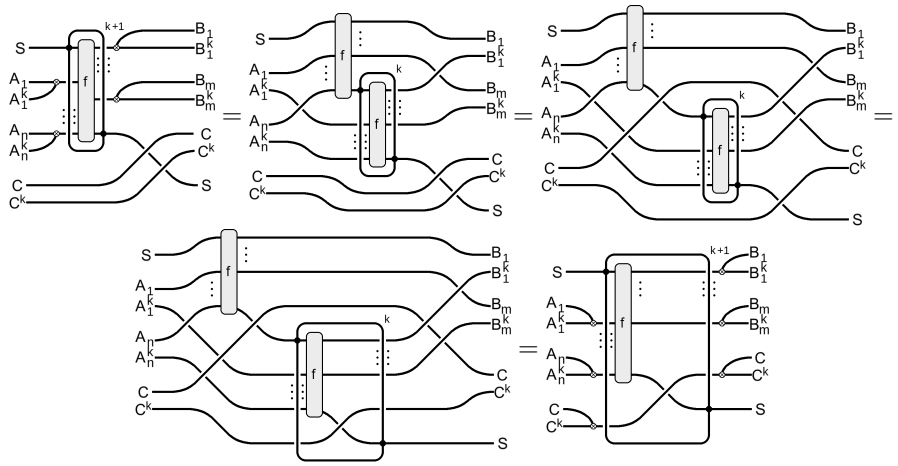


Induction step for (τ-swap):



Induction step for (τ-comp) is proved in Section 3.

Induction step for (τ-mono):



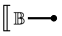
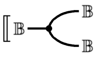
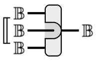
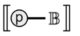
◀

B A Complete Equational Theory of Boolean Stochastic Maps

The structure of Markov categories with probabilistic choice, introduced in Section 4, is novel. Thus, it is interesting to study whether the axioms are *complete* with respect to the category $\mathsf{FinStoch}_{\{1,0\}}$. Here, completeness means that any equality between Boolean stochastic maps in $\mathsf{FinStoch}_{\{1,0\}}$ can also be derived syntactically using the axioms listed in Figure 1.

In order to formally state completeness, we introduce the syntactic category PBCirc of probabilistic boolean circuits. This is the symmetric monoidal category of string diagrams freely generated by the single-sorted signature $(\mathbb{B}, \Sigma)$, where $\Sigma := \{\mathbb{B}\bullet, \mathbb{B}\curlyvee\mathbb{B}, \mathbb{B}\curlywedge\mathbb{B}, \mathbb{B}, \textcircled{p}\mathbb{B}\}$ and such that the morphisms are quotiented by the axioms in Figure 1.

Diagrams in PBCirc take semantics in $\mathsf{FinStoch}_{\{1,0\}}$ via the interpretation functor $[\![-]\!]$: PBCirc $\to$ $\mathsf{FinStoch}_{\{1,0\}}$, defined inductively as follows:

$[\![\mathbb{B}]\!] := \{1,0\}$ $[\![$  $]\!] :=!_{\{1,0\}}$ $[\![$  $]\!] :=◀_{\{1,0\}}$ $[\![$  $]\!] := \phi_{\{1,0\}}$ $[\![$  $]\!] := \langle p \rangle$

Then we say that the equational theory of PBCirc is complete for $\mathsf{FinStoch}_{\{1,0\}}$ if, for any two diagrams $c, d \in$ PBCirc of the same type, if $[\![c]\!] = [\![d]\!]$ then their equality can be derived using the axioms in Figure 1. We rephrase Theorem 11.

▶ **Theorem 23.** *The equational theory of* PBCirc *is* complete *for* $\mathsf{FinStoch}_{\{1,0\}}$.

Proof. The proof shows that each element of $\mathsf{FinStoch}_{\{1,0\}}$ has a unique normal form representation as a diagram in PBCirc, and each diagram in PBCirc is provably equal to a diagram in normal form.

We first equip each set $\mathbb{B}^n$ with a linear order. We then say that a formal sum $p_1 \cdot x_1 + \cdots + p_m \cdot x_m$ over $\mathbb{B}^n$ is in normal form if all $p_i > 0$ and the list $x_1, \ldots, x_m$ forms a sorted list of elements without repetition. As such, a formal sum in normal form is either of the form $1 \cdot x$, or $p \cdot x + (1-p) \cdot s$ with $p \in (0,1)$, and s a formal sum in normal form, containing values x' all higher than x according to the chosen order. Importantly, each distribution has a unique normal formal sum representation.

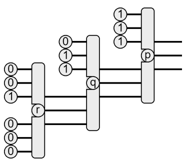
A weighted probabilistic tree over $\mathbb{B}^n$ is a diagram $I \to \mathbb{B}^n$ inductively defined as:

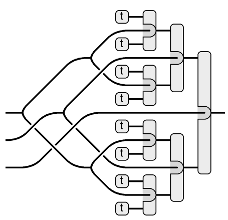
$$t, r \quad := \quad \langle b_1 \rangle \otimes \cdots \otimes \langle b_n \rangle \mid (t \otimes r); \phi^p_{\mathbb{B}^n}$$

where each $b_i \in \{0,1\}$. We represent a normal formal sum as a weighted probabilistic tree, by representing $1 \cdot (b_1, \ldots, b_n)$ as $\langle b_1 \rangle \otimes \cdots \otimes \langle b_n \rangle$, and $p \cdot (b_1, \ldots, b_n) + (1-p) \cdot s$ as $(\langle b_1 \rangle \otimes \cdots \otimes \langle b_n \rangle \otimes t); \phi^p_{\mathbb{B}^n}$, where t is the representation of the normal formal sum s. It can be shown that any weighted probabilistic tree over $\mathbb{B}^n$ is equal to the tree representation of a normal formal sum. This is done by using axioms (ϕ-1), (ϕ-co) and (ϕ-as) to get rid of zero-probability branches, sorting the order, and re-associating branches, as well as determinism of $\langle 1 \rangle$, $\langle 0 \rangle$ combined with (ϕ-id) to combine branches with the same result.

The normal forms of type $\mathbb{B}^0 \to \mathbb{B}^n$ are the tree representations of normal formal sums, which are unique for each distribution. We generalize to arbitrary $\mathbb{B}^k \to \mathbb{B}^n$ by doing a case distinction on inputs, where a normal form of type $\mathbb{B}^{k+1} \to \mathbb{B}^n$ is of the form: $(◀_{\mathbb{B}^k} \otimes id_{\mathbb{B}}); (id_{\mathbb{B}^k} \otimes \chi_{\mathbb{B}^k,\mathbb{B}}); (f_1 \otimes id_{\mathbb{B}} \otimes f_0); \phi_{\mathbb{B}^n}$, where f_1 and f_0 are normal forms of morphisms of type $\mathbb{B}^k \to \mathbb{B}^n$. Each morphism $f : \mathbb{B}^k \multimap \mathbb{B}^n$ of $\mathsf{FinStoch}_{\{1,0\}}$ has a unique normal form of this kind, with $f : \mathbb{B}^0 \to \mathbb{B}^n$ represented by the tree representation of the normal formal sum for the distribution given by $f(*)$, and $f : \mathbb{B}^{k+1} \to \mathbb{B}^n$ represented by taking f_1 and f_0 to be the normal form of the functions $(b_1, \ldots, b_k) \mapsto f(b_1, \ldots, b_k, 1)$ and $(b_1, \ldots, b_k) \mapsto f(b_1, \ldots, b_k, 0)$ respectively. This normal form is unique, as this specification is necessitated by the $[\![-]\!]$ functor.

See below examples of normal forms, with a normal form of a morphism of type $\mathbb{B}^0 \to \mathbb{B}^3$ on the left in the form of a sorted weighted tree (using lexicographic ordering on $\mathbb{B}^3$), and a normal form of a morphism of type $\mathbb{B}^3 \to \mathbb{B}^k$ with a weighted tree at each t (some liberties were taken regarding the order of swaps and copies).





We prove that each diagram is equivalent to one in normal form.

- First we show that the identity diagrams $id_{\mathbb{B}^n} : \mathbb{B}^n \to \mathbb{B}^n$ can be put in normal form. This can be shown by using the equations (ϕ-$\mathbb{B}$) and (ϕ-id) together with monoidal coherence and naturality of ϕ, given in equations (ϕ_I), ($\phi_\otimes$), and (ϕ-nat).
- Second, note that each morphism in a freely generated mono*id*al category can be described as a composition of morphisms of the form $(id_A \otimes s \otimes id_B)$, with s a generator, which in our case is of $\{\chi\} \cup \Sigma = \{\chi, \blacktriangleleft, !, \langle p \rangle, \phi\}$. Then show that $f; (id_A \otimes s \otimes id_B)$ can be reduced to a normal form, given that f is in normal form. This is done in three steps:
  1. Pull $(id_A \otimes s \otimes id_B)$ through each ϕ using naturality (ϕ-nat), both the if-gates used to distinguish between different inputs, as well as the if-gates used in the weighted probabilistic trees, until we get to leaves of the trees.
  2. Reduce each $(\langle b_1 \rangle \otimes \cdots \otimes \langle b_n \rangle); (id_A \otimes s \otimes id_B)$ to a weighted probabilistic tree.
  3. The result is f, but with different weighted probabilistic trees at each case in its case distinction. Put all those trees into normal form.

Hence we can normalize each $f : \mathbb{B}^k \to \mathbb{B}^n$ by first giving it a specification as composition of $(id_A \otimes s \otimes id_B)$ morphisms. Then normalize the identity function on $\mathbb{B}^k$ and inductively normalize by composing with each additional layer. ◀

▶ **Lemma 24.** PBCirc *is a metric enriched symmetric monoidal category.*

Proof of Lemma 24. We take as distance between arrows

$$d_{\mathbb{B}^n \to \mathbb{B}^m}(c, d) := d_{\{1,0\}^n \to \{1,0\}^m}([\![c]\!], [\![d]\!])$$

for every $c, d \colon \mathbb{B}^n \to \mathbb{B}^m$ in PBCirc.

First, we verify that $d_{\mathbb{B}^n \to \mathbb{B}^m}$ is indeed a distance – that is, it satisfies the conditions in (2). Most properties are straightforward to check; the only non-trivial one is $d_{\mathbb{B}^n \to \mathbb{B}^m}(c, d) = 0 \iff c = d$, which we prove below:

$$\begin{aligned}
d_{\mathbb{B}^n \to \mathbb{B}^m}(c, d) = 0 &\iff d_{\{1,0\}^n \to \{1,0\}^m}([\![c]\!], [\![d]\!]) = 0 && \text{(Definition of } d_{\mathbb{B}^n \to \mathbb{B}^m}\text{)} \\
&\iff [\![c]\!] = [\![d]\!] && \text{(Lemma 15)} \\
&\iff c = d && \text{(Theorem 11)}
\end{aligned}$$

To conclude that PBCirc is metric enriched, we need to verify also that ; and $\otimes$ are non-expansive, that is (3) and (4). We prove (3) below, the proof for the other is analogous.

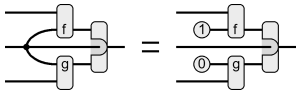
$$\begin{aligned}
d_{\mathbb{B}^n \to \mathbb{B}^m}(c; d, c'; d') &= d_{\{1,0\}^n \to \{1,0\}^m}([\![c; d]\!], [\![c'; d']\!]) && \text{(Definition of } d_{\mathbb{B}^n \to \mathbb{B}^m}\text{)} \\
&= d_{\{1,0\}^n \to \{1,0\}^m}([\![c]\!]; [\![d]\!], [\![c']\!]; [\![d']\!]) && \text{(}[\![-]\!] \text{ is a functor)} \\
&\leq d_{\{1,0\}^n \to \{1,0\}^l}([\![c]\!], [\![c']\!]) + d_{\{1,0\}^l \to \{1,0\}^m}([\![d]\!], [\![d']\!]) && \text{((3))} \\
&= d_{\mathbb{B}^n \to \mathbb{B}^l}(c, c') + d_{\mathbb{B}^l \to \mathbb{B}^m}(d, d') && \text{(Definition of } d_{\mathbb{B}^n \to \mathbb{B}^m}\text{)}
\end{aligned}$$

◀

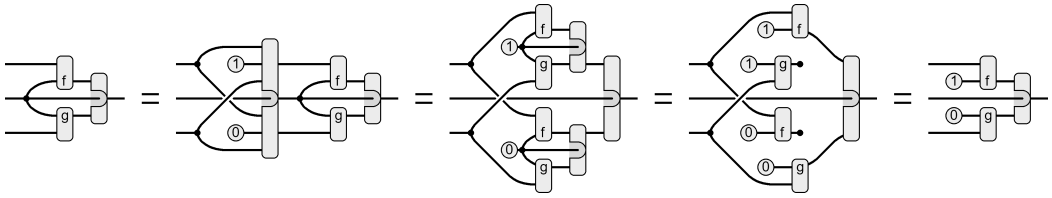
C Additional Proofs for Section 4

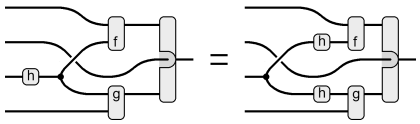
Proof of Lemma 10. (ϕ-0) is proven by using (ϕ-co) and (ϕ-1).

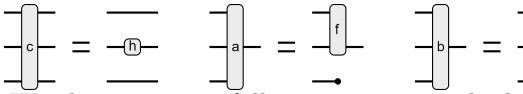
Now to prove (𝔹-split):

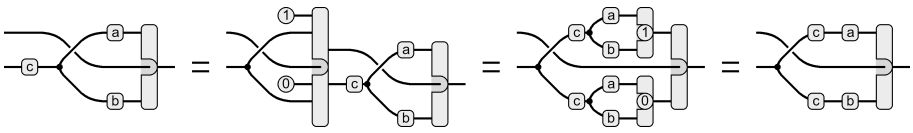


First we apply axiom (ϕ-id), (ϕ-$\mathbb{B}$), and (ϕ-id) to each of the incoming wires, and combining those with monoidal coherence ($\phi_\otimes$). Then we pull the main morphism through the ϕ-gate using naturality. As a third step, we use determinism of 1 and 0, as well as (ϕ-1) and (ϕ-0). Lastly, we use naturality of the discard operation to get the right result.



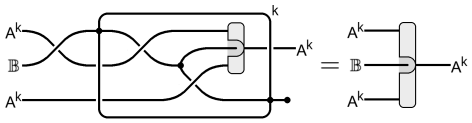
Lastly, proving (ϕ-distr): 

For simplicity, we define:  , and swap the first two wires of (ϕ-distr). We then prove as follows, starting with the equations (ϕ-$\mathbb{B}$), (ϕ-id), and ($\phi_\otimes$), then use (ϕ-nat), and finally simplifying using equations (ϕ-1) and (ϕ-0):



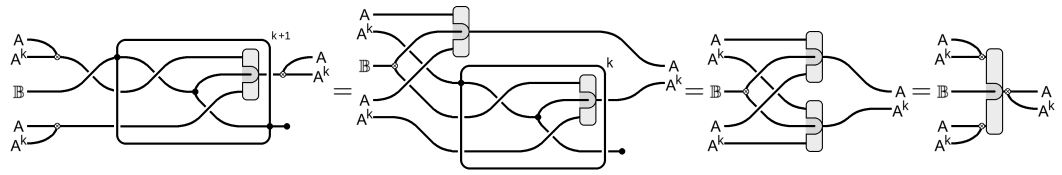
◀

Extended proof of Lemma 12. We define copy, discard and if-gate on objects as done in Section 4. We then show that in $\mathcal{C}$, $\tau^k_{1,(A),(A,A)}(\blacktriangleleft_A) = \blacktriangleleft_{A^k}$, $\tau^k_{1,(A),()}(!_A) = !_{A^k}$, and



Consequently, by induction on A in $\mathsf{PI}(\mathcal{C})$, we then reason that with the chosen definition, $S_k(\blacktriangleleft_A) = \blacktriangleleft_{S_k(A)}$, $S_k(!_A) = !_{S_k(A)}$, and $S_k(\phi_A) = \phi_{S_k(A)}$. This allows us to lift the equations for Markov categories and probabilistic choice to $\mathsf{PI}(\mathcal{C})$ via S_k.

We prove the relevant property for ϕ stated above by induction on k. The induction basis is simple. The induction step goes as follows:



Using the above property, we can show by induction on objects A that $S_k(\phi_A) = \phi_{S_k(A)}$. This allows us to prove the relevant equations by lifting them from $\mathcal{C}$. ◀

Proof of Lemma 16. For soundness we proceed by induction on the rules in (5). Observe that the laws which do not involve the probabilistic choice are trivially verified from the fact that $\mathsf{FinStoch}_{\{1,0\}}$ is metric-enriched.

For the top rightmost rule, given maps $c, c' \colon \{1,0\}^n \to \{1,0\}^m$ and $d, d' \colon \{1,0\}^l \to \{1,0\}^m$ such that $c \equiv_\delta c'$ and $d \equiv_\delta d'$, by inductive hypothesis we have that $d_{\{1,0\}^n \to \{1,0\}^m}(c, c') \leq \delta$ and $d_{\{1,0\}^l \to \{1,0\}^m}(d, d') \leq \delta$. Now let $h = (c \otimes id_{\mathbb{B}} \otimes d); \phi_{\{1,0\}^m}$ and $h' = (c' \otimes id_{\mathbb{B}} \otimes d'); \phi_{\{1,0\}^m}$ and observe that for any $a \in \{1,0\}^n, b \in \{1,0\}^l$, we have the following cases:

$$\begin{array}{ll} h(a,0,b) = (c \otimes !_{\{1,0\}^l})(a,b) = c(a) & h'(a,0,b) = (c' \otimes !_{\{1,0\}^l})(a,b) = c'(a) \\ h(a,1,b) = (!_{\{1,0\}^n} \otimes d)(a,b) = d(b) & h'(a,1,b) = (!_{\{1,0\}^n} \otimes d')(a,b) = d'(b) \end{array}$$

Thus, $d_{\{1,0\}^m}(h(a,0,b), h'(a,0,b)) = d_{\{1,0\}^m}(c(a), c'(a)) \leq \delta$ and $d_{\{1,0\}^m}(h(a,1,b), h'(a,1,b)) = d_{\{1,0\}^m}(d(b), d'(b)) \leq \delta$.

To conclude we have that

$$\begin{aligned} d_{\{1,0\}^{n+1+l} \to \{1,0\}^m}(h, h') &= \mathtt{max}_{(a,i,b) \in \{1,0\}^{n+i+l}} \mathsf{tv}_{\{1,0\}^m}(h(a,i,b), h'(a,i,b)) \\ &\leq \mathtt{max}_{(a,i,b) \in \{1,0\}^{n+i+l}} \delta = \delta. \end{aligned}$$

For the bottom rightmost rule, given maps $c, c' \colon \{1,0\}^n \to \{1,0\}^m$ and $d, d' \colon \{1,0\}^l \to \{1,0\}^m$ such that $c \equiv_\delta c'$ and $d \equiv_{\delta'} d'$, by inductive hypothesis: $d_{\{1,0\}^n \to \{1,0\}^m}(c, c') \leq \delta$ and $d_{\{1,0\}^l \to \{1,0\}^m}(d, d') \leq \gamma$. Now let $h = (c \otimes d); \phi^p_{\{1,0\}^m}$ and $h' = (c' \otimes d'); \phi^p_{\{1,0\}^m}$ and observe that for any $a \in \{1,0\}^n, b \in \{1,0\}^l$, we have that

$$h(a,b) = p \cdot c(a) + (1-p) \cdot d(b) \quad h'(a,b) = p \cdot c'(a) + (1-p) \cdot d'(b)$$

and thus,

$$\begin{aligned} & d_{\{1,0\}^{n+l} \to \{1,0\}^m}(h, h') = \mathtt{max}_{(a,b) \in \{1,0\}^{n+l}} \mathsf{tv}_{\{1,0\}^m}(h(a,b), h'(a,b)) \\ =& \mathtt{max}_{(a,b) \in \{1,0\}^{n+l}} \sum_x \frac{|h(a,b)(x) - h'(a,b)(x)|}{2} \\ =& \mathtt{max}_{(a,b) \in \{1,0\}^{n+l}} \sum_x \frac{|p \cdot (c(a)(x) - c'(a)(x)) + (1-p) \cdot (d(b)(x) - d'(b)(x))|}{2} \\ \leq& p \cdot \mathtt{max}_{a \in \{1,0\}^n} \sum_x \frac{|c(a)(x) - c'(a)(x)|}{2} + (1-p) \cdot \mathtt{max}_{b \in \{1,0\}^l} \sum_x \frac{|d(b)(x) - d'(b)(x)|}{2} \\ =& p \cdot d_{\{1,0\}^n \to \{1,0\}^m}(c, c') + (1-p) \cdot d_{\{1,0\}^l \to \{1,0\}^m}(d, d') \leq p \cdot \delta + (1-p) \cdot \gamma. \end{aligned}$$

For completeness, we rely on the normal form Theorem 11 and use the rules from (5). For morphisms $f, g \colon n \to m$ in normal form, we prove $f \equiv_{d(f,g)} g$ by induction on n and m.

- Base case: $n = m = 0$, then both morphisms are id_I. So $f \equiv_0 g$ and $d(f,g) = 0$.
- Suppose $n = 0$ and $m = m' + 1$. Then $f = (\langle 1 \rangle \otimes f_1 \otimes \langle 0 \rangle \otimes f_0); \phi^p$ and $g = (\langle 1 \rangle \otimes g_1 \otimes \langle 0 \rangle \otimes g_0); \phi^q$. Now, $d(f,g) = \min(p,q) \cdot d(f_1, g_1) + \min(1-p, 1-q) \cdot d(f_0, g_0) + (1 - \min(p,q) - \min(1-p, 1-q))$, since $d(\langle i \rangle \otimes f_i, \langle i \rangle \otimes g_i) = d(f_i, g_i)$, and $d(\langle i \rangle \otimes f_i, \langle 1-i \rangle \otimes g_{i-1}) = 1$. Assume w.l.o.g. that $p \leq q$, so $\min(p,q) = p$ and $\min(1-p, 1-q) = 1 - q$, and $d(f,g) = p \cdot d(f_1, g_1) + (1-q) \cdot d(f_0, g_0) + (q - p)$. Define $k = \frac{q-p}{1-p}$. We can then prove that $f = (\langle 0 \rangle \otimes f_0 \otimes \langle 0 \rangle \otimes f_0); (\langle 1 \rangle \otimes f_1 \otimes \phi^k); \phi^p$ using (ϕ-id), (ϕ-distr), and $g = (\langle 1 \rangle \otimes g_1 \otimes \langle 0 \rangle \otimes g_0); (\langle 1 \rangle \otimes g_1 \otimes \phi^k); \phi^p$ using the same rules and (ϕ-as). By induction hypothesis, $\langle 1 \rangle \otimes f_1 \equiv_{d(f_1,g_1)} \langle 1 \rangle \otimes g_1$ and $\langle 0 \rangle \otimes f_0 \equiv_{d(f_0,g_0)} \langle 0 \rangle \otimes g_0$, and trivially $\langle 0 \rangle \otimes f_0 \equiv_1 \langle 1 \rangle \otimes g_1$. Applying the second quantitative ϕ-rule twice, we get that $f \equiv_\alpha g$ for: $\alpha = p \cdot d(f_1, g_1) + (1-p) \cdot (k \cdot 1 + (1-k) \cdot d(f_0, g_0)) = p \cdot d(f_1, g_1) + (p - q) + (1-q) \cdot d(f_0, g_0)$.

- Suppose $n = k + 1$. Then $f = (\blacktriangleleft_{\mathbb{B}^k} \otimes id_{\mathbb{B}}); (id_{\mathbb{B}^k} \otimes \chi_{\mathbb{B},\mathbb{B}^k}); (f_1 \otimes id_{\mathbb{B}} \otimes f_0); \phi_{\mathbb{B}^m}$ and $g = (\blacktriangleleft_{\mathbb{B}^k} \otimes id_{\mathbb{B}}); (id_{\mathbb{B}^k} \otimes \chi_{\mathbb{B},\mathbb{B}^k}); (g_1 \otimes id_{\mathbb{B}} \otimes g_0); \phi_{\mathbb{B}^m}$. Note that

$$\begin{aligned} d(f,g) &= \mathtt{max}_{(x,i)\in\{1,0\}^n}(d(f(x,i),g(x,i))) = \mathtt{max}_{(x,i)\in\{1,0\}^n}(d(f_i(x),g_i(x))) \\ &= \mathtt{max}(\mathtt{max}_{x\in\{1,0\}^k}(d(f_1(x),g_1(x))), \mathtt{max}_{x\in\{1,0\}^k}(d(f_0(x),g_0(x)))) \\ &= \mathtt{max}(d(f_1,g_1),d(f_0,g_0)). \end{aligned}$$

  By induction hypothesis, $f_1 \equiv_{d(f_1,g_1)} g_1$ and $f_0 \equiv_{d(f_0,g_0)} g_0$. So since $d(f_i,g_i) \leq d(f,g)$ as proven above, $f_1 \equiv_{d(f,g)} g_1$ and $f_0 \equiv_{d(f,g)} g_0$. Applying the first quantitative ϕ-rule, we get: $(f_1 \otimes id_{\mathbb{B}} \otimes f_0); \phi_{\mathbb{B}^k} \equiv_{d(f,g)} (g_1 \otimes id_{\mathbb{B}} \otimes g_0); \phi_{\mathbb{B}^k}$, so with compositionality, $f \equiv_{d(f,g)} g$ as required. ◀