Extensional Denotational Semantics of Higher-Order Probabilistic Programs, Beyond the Discrete Case

Guillaume Geoffroy

Extensional Denotational Semantics of Higher-Order Probabilistic Programs, Beyond the Discrete Case

Guillaume Geoffroy
Università di Bologna

***Abstract*—We describe a mathematical structure that can give extensional denotational semantics to higher-order probabilistic programs. It is not limited to discrete probabilities, and it is compatible with integration in a way the models that have been proposed before are not. It is organised as a model of propositional linear logic in which all the connectives have intuitive probabilistic interpretations. In addition, it has least fixed points for all maps, so it can interpret recursion.**

I. Introduction

Extensional denotational semantics of probabilistic programs have been around since the late 1970s [1], [2]. The idea is to represent first-order programs by measure transformers. For example, consider a program that takes as input a handle to a random generator of real numbers and outputs a randomly chosen real number: its denotation is a map that takes a probability measure on $\mathbb{R}$ (representing the distribution of the input) and returns a probability measure on $\mathbb{R}$ (representing the distribution of the output). If non-terminating programs are allowed, then instead, you get a map from sub-probability measures to sub-probability measures: a total measure strictly less than 1 denotes a non-zero probability of failing to produce a number (*e.g.* through non-termination). Beyond first order, "extensional" means that each type is interpreted as a set (in the case of the real numbers, the set $S(\mathbb{R})$ of sub-probability distributions on $\mathbb{R}$) with some additional structure, and programs are interpreted as structure-preserving maps, in such a way that the set of all structure-preserving maps can itself be equipped with the same structure. What structure should one use, though? This is a long-standing question: interaction between the "set of all sub-probability mesures" construction and the domain-theoretic tools traditionally used to represent function types has been notoriously troublesome [3]. As a result, for a while, more success was to be had from "intensional" approaches, such as games [4] and the geometry of interaction [5].

Some hints at how to answer this question can be found in Kozen's early extensional model [2]. This model can only represent first-order programs, and only those that are "linear", in the sense that they sample their input exactly once. Measure transformers that are *linear* and *effective*, in the sense that they actually represent one of these linear programs, have a particular property: they *commute with integrals*. Equivalently, they correspond to sub-probability kernels [6] (through the "bind" operation of the monad S of sub-probability measures [7]). Still equivalently, they are morphisms of algebras over this monad. This implies that, as noted by Kozen back then (though with different terminology), two linear effective functions that coincide on all Dirac distributions (*i.e.* on all deterministic inputs) are equal. This leaves out many maps; in particular, the map that takes a sub-probability measure on $\mathbb{R}$ and returns its continuous part is not linear effective.

If one extends Kozen's model to allow programs to sample their input any number of times, effective functions start to look like power series. Indeed, in this modified model, it can be checked that for all effective maps $f : S(\mathbb{R}) \to S(\mathbb{R})$, there exists a family $(\partial_n f : S(\mathbb{R}^n) \to S(\mathbb{R}))_{n\in\mathbb{N}}$ of *linear* effective maps (so morphisms of S-algebras) such that for all $\mu \in S(\mathbb{R})$, $f(\mu) = \sum_{n\in\mathbb{N}} \partial_n f(\mu^{\otimes n})$ (where $\mu^{\otimes n}$ denotes the product measure of n copies of μ). As a result, it is easy to prove that two effective maps that coincide on all finitely-supported measures are equal. A fortiori, the "continuous part" map defined above, which coincides with the zero map on all discrete measures, is not effective.

This suggests that, in order to get well-behaved extensional denotational semantics, types in general should be interpreted by S-algebras, linear programs by morphisms of S-algebras, and general programs by "power series" in the sense described above. Probabilistic coherence spaces [8] do precisely that. Among their many pleasant properties, they form a model of full propositional linear logic [9] in which each connective (or at least a complete set thereof) has an intuitive probabilistic interpretation. A considerable drawback is that they are designed to only work with countable data types, and therefore discrete probabilities. Indeed, the only reason why linear maps between probabilistic coherence spaces commute with integrals (*i.e.* are morphisms of S-algebras) is because in this context, integrals are just countable sums.

Several constructions have been proposed to overcome this limitation [10], [11], [12], [13]. However, they do so only partially. Indeed, none of them fits the above picture of S-algebras and power series, as can be seen by the fact that they all include the "continuous part" map mentioned above. This means that none of these models is compatible with integration (only with countable sums, at most), even though integration is a cornerstone of probability theory.

The contribution of this paper is to define such a model, which we call *convex quasi-Borel spaces*. This brings us one step closer to answering the long-standing question from the first paragraph. In addition to compatibility with integration, the construction we propose is a model of linear logic (with the same intuitions behind the connectives as in probabilistic coherence spaces), and all functions have least fixed points

(so the model interprets recursion). Our construction relies on two innovations with respect to previous models: we define integration axiomatically and simply ask that linear maps commute with integrals; and we do away with topology entirely – in particular we replace all limits and suprema with countable sums (which are just a particular kind of integrals). The idea behind the second point is that pointwise countable sums interact well with power series, whereas pointwise limits do not.

We begin this paper with a few reminders on *quasi-Borel spaces* [14] (hereafter QBSs), which are a generalisation of the traditional notion of measurable spaces. They form a category that contains the category of measurable spaces and measurable maps as a subcategory (and the category of standard Borel spaces as a full subcategory), supports a commutative "set of all probability measures" strong monad, and is cartesian closed. This means that, by themselves, QBSs can already be seen as a model of the simply typed lambda calculus that supports probabilistic constructions (however, this model pays no attention whatsoever to computability: it contains not just the "continuous part" map, but in fact any measurable map from $S(\mathbb{R})$ to $S(\mathbb{R})$). They can also be seen as an alternative theory of integration and measurability that supports function spaces, which is why our construction will be built upon them.

The remainder of the paper is mostly dedicated to the construction of the model itself. This construction follows the blueprint of linear logic [9]. First, we define convex QBSs, and as a canonical example, we define for all QBSs A the convex QBS $\underline{A}$ of random elements of A. Then we define the multiplicative constructions, notably *multilinear maps*, which represent probabilistic programs with multiple arguments that use each argument exactly once. In particular, we show that convex QBSs and linear maps form a closed symmetric monoidal category. Next come the additive constructions (the cartesian product and the coproduct), and then the exponential modalities. After that, we define *analytic maps*, which represent probabilistic programs in general, and we show that the category of convex QBSs and analytic maps is equivalent to the Kleisli category of the exponential comonad "!" – in particular, it is cartesian closed. Finally, we show that all analytic maps from a convex QBS to itself have a least fixed point, and that the operation that maps a map to its least fixed point is analytic. After building the model, we give an example of toy probabilistic language that can be interpreted in it.

Note that we use the expression "probabilistic program" in its narrow meaning of a program that can make random choices (as well as manipulate other programs that make their own random choices). The same expression is also used in the broader sense of a program that describes and manipulates statistical models [15], [16]. In that setting, compatibility with integration is all the more relevant, so it would be worth checking whether our approach can be generalised to it.

II. Preliminaries on quasi-Borel spaces

Getting a construction that is compatible with integration requires a theory of integration and measurability in the first place. Instead of the traditional theory of σ-algebras and measurable spaces, we use quasi-Borel spaces [14] (QBSs), because they are known to form a cartesian closed category.

The only cost of replacing measurable spaces with QBSs is that the "source of randomness" has to be a standard Borel space [6]. This is a reasonable assumption as far as computer science is concerned, since that includes the space $\{0,1\}^{\mathbb{N}}$ of all infinite sequences of bits[1].

In this section, we recall the definition of QBSs and define the monad S of *sub-probability measures*.

Definition 1 ([14])**.** A *quasi-Borel space* is the data of a set A and a set M_A of maps from $\mathbb{R}$ to A such that

- for all $\alpha \in M_A$ and all measurable maps $f : \mathbb{R} \to \mathbb{R}$ (where $\mathbb{R}$ is equipped with the Borel σ-algebra $\Sigma_{\mathbb{R}}$), $\alpha \circ f \in M_A$,
- for all constant maps $\alpha : \mathbb{R} \to A$, $\alpha \in M_A$,
- for all $(\alpha_n)_{n\in\mathbb{N}} \in M_A^{\mathbb{N}}$ and all partitions $(U_n)_{n\in\mathbb{N}}$ of $\mathbb{R}$ into Borel sets, M_A contains the case-split map that maps r to $\alpha_n(r)$ whenever $r \in U_n$.

Let A and B be QBSs. A *morphism of QBSs* from A to B is a map $f : A \to B$ such that for all $\alpha \in M_A$, $f \circ \alpha \in M_B$. QBSs and morphisms between them form a category, which we denote by Qbs.

Since this category is cartesian [14, Proposition 16] (and even cartesian closed), it induces a symmetric multicategory [17, Definitions 2.1.1 and 2.2.21], which we also denote by Qbs, with the set of n-ary maps $\mathrm{Qbs}(A_1, \ldots, A_n; B)$ defined as $\mathrm{Qbs}(A_1 \times \ldots \times A_n, B)$.

For all QBSs A and all sets $B \subseteq A$, we define the *subset QBS structure* on B by $M_B = \{\alpha \in M_A;\ \forall r \in \mathbb{R}, \alpha(r) \in B\}$.

Measurable spaces and measurable maps form a subcategory of Qbs: for all measurable spaces (A, Σ_A), we define a QBS (A, M_A) by letting M_A be the set of all measurable maps from $(\mathbb{R}, \Sigma_{\mathbb{R}})$ to (A, Σ_A). If (A, Σ_A) and (B, Σ_B) are measurable spaces, every measurable map from (A, Σ_A) to (B, Σ_B) is a morphism of QBSs from (A, M_A) to (B, M_B), though the converse is not necessarily true.

Recall [6, Introduction] that a *standard Borel space* (or simply *Borel space*) is a measurable space that is isomorphic to a Borel subset of $\mathbb{R}$. If (A, Σ_A) and (B, Σ_B) are standard Borel spaces, then a map $f : A \to B$ is measurable if and only if it is a morphism of QBSs [14, Proposition 15]. From now on, we will only consider QBSs and standard Borel spaces (seen as a particular case of QBSs), and never deal with general measurable spaces. As a result, we will refer to morphisms of QBSs simply as *measurable maps*: this will help convey the right intuitions, and it will never come in conflict with the usual notion of measurability.

[1] In fact, by standard results on Markov kernels, the probability measures that can be represented in QBSs are exactly those that can be obtained by pushing forward the usual "independent fair coins" measure on $\{0,1\}^{\mathbb{N}}$.

For all standard Borel spaces (A, Σ_A), we denote by $G(A)$ the set of all probability measures on A. We equip it with the smallest σ-algebra $\Sigma_{G(A)}$ such that for all $U \in \Sigma_A$, $\mu \mapsto \mu(U)$ is measurable. Recall [18] that $G(A)$ is itself a standard Borel space, and that a measurable map from A to $G(B)$ is the same thing as a Markov kernel from A to B. This construction has been successfully generalised to QBSs [14, Section V-D]. We describe an analogous construction for sub-probability measures, *i.e.* positive measures of total weight at most 1. With the exceptions of Facts 6 and 8, all the results we give here correspond to results that have already been established in the case of probability measures, so we omit their proofs, which are similar.

Definition 2. Let A be a QBS. The QBS of *sub-probability measures* on A, denoted by $S(A)$, is defined as the quotient [14, Proposition 25]

$$S(A) = \mathrm{Qbs}\left(\mathbb{R}, A \amalg \{*\}\right) \times G(\mathbb{R}) / \sim,$$

where $\mathrm{Qbs}(B_1, B_2)$ denotes the QBS of measurable maps from B_1 to B_2 [14, Proposition 18], $\amalg$ denotes the coproduct of QBSs [14, Proposition 17], $\{*\}$ denotes the one-element QBS, and $\sim$ denotes the following equivalence relation:

For all $(\alpha, \mu), (\beta, \nu)$, we let $(\alpha, \mu) \sim (\beta, \nu)$ if and only if for all measurable maps $f : A \to [0, +\infty]$,

$$\int_{r \in \alpha^{-1}(A)} f(\alpha(r))\, \mu(\mathrm{d}r) = \int_{s \in \beta^{-1}(A)} f(\beta(s))\, \nu(\mathrm{d}s).$$

We denote by $[\alpha, \mu]$ the equivalence class of (α, μ).

This approach of pushing forward by a partial map (or equivalently, a map that can take the "undefined" value $*$) in order to "shave" some of the original measure has already been used to define an analogue of the monad S in the context of ω-QBSs [11].

Definition 3. We make $S : \mathrm{Qbs} \to \mathrm{Qbs}$ into a functor by letting $S(f)\left([\alpha, \mu]\right) = [f \circ \alpha, \mu]$ for all $f : A \to B$ measurable and all $[\alpha, \mu] \in S(A)$.

For all QBSs A and B, it is clear that S defines a measurable map from $\mathrm{Qbs}\left(A, B\right)$ to $\mathrm{Qbs}\left(S(A), S(B)\right)$.

Definition 4 (Integration on QBSs)**.** Let A be a QBS. For all $\rho = [\alpha, \mu] \in S(A)$ and all $f \in \mathrm{Qbs}\left(A, [0, +\infty]\right)$, we let

$$\int_{x \in A} f(x)\, \rho(\mathrm{d}x) = \int_{r \in \alpha^{-1}(A)} f(\alpha(r))\, \mu(\mathrm{d}r) \in [0, +\infty].$$

One can check that this defines a measurable map from $S(A) \times \mathrm{Qbs}\left(A, [0, +\infty]\right)$ to $[0, +\infty]$.

Fact 5. *For all standard Borel spaces (A, Σ_A), the following map defines a bijection between the QBS $S(A, M_A)$ and the set of all sub-probability measures (in the traditional sense) on the standard Borel space (A, Σ_A):*

$$\left\{ \begin{array}{ccccc} S(A, M_A) & \to & \Sigma_A & \to & [0,1] \\ \rho & \mapsto & U & \mapsto & \int_{x \in A} \mathbf{1}_U(x)\, \rho(\mathrm{d}x), \end{array} \right.$$

where $\mathbf{1}_U$ denotes the indicator function of U. In addition, this bijection is natural in A, and integration as in Definition 4 corresponds to integration in the traditional sense through this bijection.

If we unfold Definition 2, we find that $M_{S(A)} = \{r \mapsto \left[s \mapsto \alpha(r, s), \mu_r\right] ;\ \alpha \in \mathrm{Qbs}\left(\mathbb{R} \times \mathbb{R}, A \amalg \{*\}\right), (r \mapsto \mu_r) \in \mathrm{Qbs}\left(\mathbb{R}, G\left(\mathbb{R}\right)\right)\}$. However, in order to define the monad multiplication, we will need the following characterisation[2].

Fact 6. *For all QBSs A, $M_{S(A)} = \{r \mapsto [\alpha, \mu_r] ;\ \alpha \in \mathrm{Qbs}\left(\mathbb{R}, A \amalg \{*\}\right), (r \mapsto \mu_r) \in \mathrm{Qbs}\left(\mathbb{R}, G(\mathbb{R})\right)\}$.*

Proof. Let $\alpha \in \mathrm{Qbs}\left(\mathbb{R} \times \mathbb{R}, A \amalg \{*\}\right)$ and $(r \mapsto \mu_r) \in \mathrm{Qbs}\left(\mathbb{R}, G(\mathbb{R})\right)$. The maps $r \mapsto \mu_r$ and $r \mapsto \delta_{\mathbb{R}}(r)$ are Markov kernels (where $\delta_{\mathbb{R}}(r)$ denotes the Dirac measure at r on $\mathbb{R}$), so $r \mapsto \delta_{\mathbb{R}}(r) \otimes \mu_r$ is a Markov kernel [6, Lemma 1.17, as a particular case of composition where the second kernel ignores its second argument] and therefore a measurable map from $\mathbb{R}$ to $G(\mathbb{R} \times \mathbb{R})$. Let φ be an isomorphism between the standard Borel spaces $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$. Then for all $r \in \mathbb{R}$, $\left[s \mapsto \alpha(r, s), \mu_r\right] = \left[\alpha \circ \varphi^{-1}, \varphi_\sharp\left(\delta_{\mathbb{R}}(r) \otimes \mu_r\right)\right]$, where $\varphi_\sharp\left(\delta_{\mathbb{R}}(r) \otimes \mu_r\right)$ denotes the pushforward measure of $\delta_{\mathbb{R}}(r) \otimes \mu_r$ by φ. □

In particular, for all $\rho \in S(S(A))$, there exists $\mu \in G(\mathbb{R})$, $U \in \Sigma_{\mathbb{R}}$, $(r \mapsto \nu_r) \in \mathrm{Qbs}\left(U, G\left(\mathbb{R}\right)\right)$ and $\alpha \in \mathrm{Qbs}\left(\mathbb{R}, A \amalg \{*\}\right)$ such that

$$\rho = \left[r \mapsto \left(\begin{array}{cc} [\alpha, \nu_r] & \text{if } r \in U \\ * & \text{otherwise} \end{array} \right), \mu\right].$$

Definition 7. We make S into a monad $(S, \delta, \mathbb{E})$ as follows[3]. For all QBSs A and all $x \in A$, $\delta_A(x) = [r \mapsto x, \mu] \in S(A)$, where μ is any probability measure on $\mathbb{R}$. For all

$$\rho = \left[r \mapsto \left(\begin{array}{cc} [\alpha, \nu_r] & \text{if } r \in U \\ * & \text{otherwise} \end{array} \right), \mu\right] \in S(S(A)),$$

$$\mathbb{E}_A(\rho) = \left[\alpha, V \mapsto \int_{r \in U} \nu_r(V)\, \mu(\mathrm{d}r)\right] \in S(A).$$

Alternatively, we write $\underline{x}$ for $\delta_A(x)$ and $\int_{\tau \in G(A)} \tau\, \rho(\mathrm{d}\tau)$ for $\mathbb{E}_A(\rho)$.

This means that sub-probability distributions are stable under sub-convex combinations in a very broad sense, and that this "sub-convex combination" (or "expected value") operation is measurable. In addition, sub-probability distributions are stable under countable sums as long as the sum of the total weights is at most 1, and this "countable sum" operation is also measurable on its domain:

Fact 8. *Let A be a QBS. For all $(\rho_n)_{n \in \mathbb{N}} \in S(A)^{\mathbb{N}}$ such that $\sum_{n \in \mathbb{N}} \int_{x \in A} 1\, \rho_n(\mathrm{d}x) \leq 1$, there exists a unique*

[2] In fact, the original paper on QBSs goes the other way round. It defines the monad P of probability measures similarly to Fact 6, and then it lays out the arguments needed to prove a characterisation in the spirit of Definition 2 [14, proof of Lemma 27].

[3] δ stands for *Dirac*, and $\mathbb{E}$ stands for *expected value*.

$\left(\sum_{n\in\mathbb{N}}\rho_n\right) \in S(A)$ *such that for all measurable maps* $f : A \to [0,+\infty]$,

$$\int_{x\in A} f(x)\left(\sum_{n\in\mathbb{N}}\rho_n\right)(\mathrm{d}x) = \sum_{n\in\mathbb{N}}\int_{x\in A} f(x)\,\rho_n(\mathrm{d}x).$$

In addition, the map $(\rho_n)_{n\in\mathbb{N}} \mapsto \sum_{n\in\mathbb{N}}\rho_n$ *is measurable (when its domain is equipped with the subset QBS structure).*

Proof. Let $(r \mapsto \rho_{n,r})_{n\in\mathbb{N}} \in M_{S(A)}^{\mathbb{N}}$ such that $\sum_{n\in\mathbb{N}}\int_{x\in A} 1\,\rho_{n,r}(\mathrm{d}x) \leq 1$ for all $r \in \mathbb{R}$. We must prove that there exists a unique $(r \mapsto \tau_r) \in M_{S(A)}$ such that for all $f : A \to [0,+\infty]$ measurable and all $r \in \mathbb{R}$, $\int_{x\in A} f(x)\,\tau_r(\mathrm{d}x) = \sum_{n\in\mathbb{N}}\int_{x\in A} f(x)\,\rho_{n,r}(\mathrm{d}x)$.

For all n, let $\left(r \mapsto \left[\alpha_n, \mu_{n,r}\right]\right) = \left(r \mapsto \rho_{n,r}\right)$, and let φ_n be an isomorphism between the standard Borel spaces $\mathbb{R}$ and $(n, n+1]$. For all $n \in \mathbb{N}$ and all $r \in \mathbb{R}$, let $\nu_{n,r}$ be the measure on $\mathbb{R}$ defined by $\nu_{n,r}(U) = \mu_{n,r}\left(\varphi_n^{-1}(U) \cap \alpha_n^{-1}(A)\right)$. For all $r \in \mathbb{R}$, let $\nu_{*,r} = \left(1 - \sum_{n\in\mathbb{N}}\mu_{n,r}\left(\alpha_n^{-1}(A)\right)\right)\delta_{\mathbb{R}}(0)$. For all $r \in \mathbb{R}$, we let $\nu_{\infty,r} = \nu_{*,r} + \sum_{n\in\mathbb{N}}\nu_{n,r}$: $\left(r \mapsto \nu_{\infty,r}\right)$ is a measurable map from $\mathbb{R}$ to $G(\mathbb{R})$.

For all $s \in \mathbb{R}$, we let $\beta(s) = \alpha \circ \varphi_n^{-1}(s)$ if $s \in (n, n+1]$ and $\beta(s) = *$ if $s \leq 0$. Then $\tau_r = \left[\beta, \nu_{\infty,r}\right]$ satisfies the requirements. □

Spaces of the form $S(A)$ will serve as a model for convex QBSs. As a result, these two properties (the existence of a measurable "sub-convex combination" map and of a measurable "countable sum" partial map) will become the main axioms of convex QBSs.

III. Convex quasi-Borel spaces

The only thing one can do with a probabilistic program (or any program for that matter) is to place it in some context that has an observable outcome (such as producing a real value), and observe. What happens then constitutes the *behaviour* of the program. If programs can test values for equality with any constant, then it is sufficient to restrict the notion of observable outcome to just termination (= success) or non-termination (= failure).

The idea behind convex quasi-Borel spaces is to have a set of *random values* (representing programs) and a set of *linear tests* (representing contexts that use the program exactly once). For each linear test η and each random value x, the structure gives a *probability of success* $\eta x \in [0,1]$.

Definition 9. A *convex quasi-Borel space* X is the data of

- two QBSs $|X|$ (random values) and $\left|X^\perp\right|$ (linear tests),
- a measurable map

$$\cdot_X : \left\{ \begin{array}{ccc} \left|X^\perp\right| \times |X| & \to & [0,1] \\ (\eta, x) & \mapsto & \eta x = \eta \cdot_X x \end{array} \right. ,$$

such that

- for all $x, y \in |X|$, if $\forall \eta \in \left|X^\perp\right|, \eta x = \eta y$, then $x = y$,
- there exists a (necessarily unique) measurable map $\mathbb{E}_X : S(|X|) \to |X|$ such that for all $\mu \in S(|X|)$ and all $\eta \in \left|X^\perp\right|$, $\eta(\mathbb{E}_X(\mu)) = \int_{x\in|X|}\eta x\,\mu(\mathrm{d}x)$,
- there exists a (necessarily unique) measurable map

$$\left\{ \begin{array}{c} \left\{ \begin{array}{c} (x_n)_{n\in\mathbb{N}} \in |X|^{\mathbb{N}}; \\ \forall \eta \in \left|X^\perp\right|, \sum_{n\in\mathbb{N}}\eta x_n \leq 1 \end{array} \right\} \\ (x_n)_{n\in\mathbb{N}} \end{array} \begin{array}{ccc} \to & & |X| \\ \mapsto & & \sum_{n\in\mathbb{N}} x_n \end{array} \right.$$

such that for all $(x_n)_{n\in\mathbb{N}}$ in its domain, $\eta\left(\sum_{n\in\mathbb{N}} x_n\right) = \sum_{n\in\mathbb{N}}\eta x_n$,

and such that, symmetrically,

- for all $\eta, \xi \in \left|X^\perp\right|$, if $\forall x \in |X|, \eta x = \xi x$, then $\eta = \xi$,
- there exists a (necessarily unique) measurable map $\mathbb{E}_{X^\perp} : S\left(\left|X^\perp\right|\right) \to \left|X^\perp\right|$ such that for all $\rho \in S\left(\left|X^\perp\right|\right)$ and all $x \in |X|$, $\left(\mathbb{E}_{X^\perp}(\rho)\right) x = \int_{\eta\in\left|X^\perp\right|}\eta x\,\rho(\mathrm{d}\eta)$,
- there exists a (necessarily unique) measurable map

$$\left\{ \begin{array}{c} \left\{ \begin{array}{c} (\eta_n)_{n\in\mathbb{N}} \in \left|X^\perp\right|^{\mathbb{N}}; \\ \forall x \in |X|, \sum_{n\in\mathbb{N}}\eta_n x \leq 1 \end{array} \right\} \\ (\eta_n)_{n\in\mathbb{N}} \end{array} \begin{array}{ccc} \to & & \left|X^\perp\right| \\ \mapsto & & \sum_{n\in\mathbb{N}}\eta_n \end{array} \right.$$

such that for all $(\eta_n)_{n\in\mathbb{N}}$ in its domain, $\left(\sum_{n\in\mathbb{N}}\eta_n\right) x = \sum_{n\in\mathbb{N}}\eta_n x$.

In particular, if X is a convex QBS, then one can easily check that $\left(|X|, \mathbb{E}_X\right)$ is an algebra over the monad S.

Remark 10. It would make sense to merge the two conditions (existence and measurability of integrals of sub-probability measures on one hand, and of countable sums on the other) and ask directly for the existence and measurability of integrals of s-finite measures [6]. The above definition even suggests how, in this context, to represent s-finite measures as a QBS (namely, as a quotient of $S(A)^{\mathbb{N}}$, with $(\mu_n)_{n\in\mathbb{N}}$ interpreted as "$\sum_{n\in\mathbb{N}}\mu_n$"). However, countable sums and sub-probability measures, taken separately, are simpler and, importantly, more widely known than s-finite measures: we made the choice of sacrificing some concision to gain in technical simplicity.

Since the above definition is symmetric, each convex QBS comes with a *dual*:

Definition 11. For all convex QBSs X, we define a convex QBS $X^\perp$ by letting

- $\left|X^{\perp\perp}\right| = |X|$,
- for all $x \in \left|X^{\perp\perp}\right|$ and all $\eta \in \left|X^\perp\right|$, $x \cdot_{X^\perp} \eta = \eta \cdot_X x$.

Notation 12 (Integration in convex QBSs)**.** For all QBSs A, all convex QBSs X, all measurable maps $f : A \to |X|$ and all $\mu \in S(A)$, we write $\int_{a\in A} f(a)\,\mu(\mathrm{d}a)$ for $\mathbb{E}(S(f)(\mu))$.

Here are the main, basic examples of convex QBSs (in fact, the first two can be seen as particular instances of the third).

Definition 13 (Multiplicative unit)**.** We define a convex QBS $\mathbb{W}$ (for *weights*) by:

- $|\mathbb{W}| = \left|\mathbb{W}^\perp\right| = [0,1]$,

- for all $\eta \in \left|\mathbb{W}^\perp\right|$ and all $x \in |\mathbb{W}|$, ηx is the product of η and x as elements of $\mathbb{R}$.

Definition 14 (Additive unit)**.** We define a convex QBS $\mathbb{0}$ by:

- $|\mathbb{0}| = \left|\mathbb{0}^\perp\right| = \{0\}$,
- for all $\eta \in \left|\mathbb{0}^\perp\right|$ and all $x \in |\mathbb{0}|$, $\eta x = 0$.

Definition 15 (Data types)**.** For all QBSs A, we define a convex QBS $\underline{A}$ by:

- $|\underline{A}| = S(A)$,
- $\left|\underline{A}^\perp\right| = \mathrm{Qbs}\left(A, [0,1]\right)$,
- for all $\eta \in \left|\underline{A}^\perp\right|$ and all $\mu \in |\underline{A}|$, $\eta\mu = \int_{x\in A} \eta(x)\mu(\mathrm{d}x)$.

Note that the existence and measurability of expected values and countable sums on $|\underline{A}|$ are given by Definition 7 and Fact 8, and that expected values and countable sums on $\left|\underline{A}^\perp\right|$ are computed pointwise.

Whenever we have two expressions Θ_1 and Θ_2 that are not necessarily defined (such as sums of elements of $|X|$ for some convex QBS X), we will write $\Theta_1 = \Theta_2$ for "Θ_1 is defined if and only if Θ_2 is, and in that case they are equal".

Notation 16. For all convex QBSs X, all $x, y \in |X|$ and all $r \in [0, +\infty)$, we write

- 0_X for the unique element of $|X|$ such that $\eta 0_X = 0$ for all $\eta \in \left|X^\perp\right|$,
- $x+y$ for the unique element of $|X|$ such that $\eta(x+y) = \eta x + \eta y$ for all $\eta \in \left|X^\perp\right|$, if it exists,
- rx for the unique element of $|X|$ such that $\eta(rx) = r\,\eta x$ for all $\eta \in \left|X^\perp\right|$, if it exists,
- $x \leq y$ if $\eta x \leq \eta y$ for all $\eta \in \left|X^\perp\right|$ (which defines a partial order on $|X|$),
- $\|x\|$ for $\sup_{\eta\in\left|X^\perp\right|} \eta x \in [0,1]$.

Note that the map $\|-\| : |X| \to [0,1]$ is not measurable in general, which limits its usefulness.

Fact 17. *The binary sum and scalar multiplication are measurable on their domains of definition (which are subsets of* $|X| \times |X|$ *and* $[0,+\infty) \times |X|$ *respectively).*

Proof. First, one can check that for all QBSs A, all $\mu \in S(A)$ and all $s \in [0,1]$, there exists a unique $s\mu \in S(A)$ such that for all $f \in \mathrm{Qbs}\left(A, [0,+\infty]\right)$, $\int_{a\in A} f(a)\,(s\mu)(\mathrm{d}a) = s\int_{a\in A} f(a)\,\mu(\mathrm{d}a)$. In addition, one can check that the operation $(s,\mu) \mapsto s\mu$ is measurable.

We have $x + y = \sum_{n\in\mathbb{N}} z_n$, where $z_0 = x$, $z_1 = y$, and $z_n = 0_X$ for $n > 1$, so the binary sum is measurable on its domain.

We have $rx = \sum_{n\in\mathbb{N}} \mathbb{E}_X\Big(r_n \delta_{|X|}(x)\Big)$, where r_n is 0 if $r < n$, $r - n$ if $n \leq r \leq n+1$, and 1 if $n+1 < r$. The map $r \mapsto (r_n)_{n\in\mathbb{N}}$ is measurable, as are $\delta_{|X|}$ and $\mathbb{E}_X$, so scalar multiplication is measurable on its domain. □

From the above proof, one also deduces that rx is always defined when $r \leq 1$.

When X is a convex QBS, we will generally write $x \in X$ for $x \in |X|$.

IV. Multilinear maps and multiplicative connectives

In this section, we define *multilinear maps* between convex QBSs, and we define a structure of convex QBS on spaces of multilinear maps. This construction generates all the multiplicative connectives. Intuitively, an *n-linear map* from $X_1, \ldots, X_n$ to Y represents a probabilistic program that takes n arguments of types $X_1, \ldots, X_n$, uses (*i.e.* samples) each one exactly once, and returns a result of type Y.

Given a convex QBS X, each linear test $\eta \in \left|X^\perp\right|$ can be seen as a map from $|X|$ to $[0,1] = |\mathbb{W}|$. Naturally, the set of (1-)*linear maps* from X to $\mathbb{W}$ will be defined as the set of all maps from $|X|$ to $|\mathbb{W}|$ that come from some $\eta \in \left|X^\perp\right|$. Multilinearity in general should be preserved by composition, so its definition should at least ensure that

- if a map $f : |X| \to |Y|$ is linear, then for all $\eta \in \left|Y^\perp\right|$, there exists $\xi \in \left|X^\perp\right|$ such that $\xi x = \eta f(x)$ for all x,
- if a map $f : |X_n| \times \ldots \times |X_n| \to |Y|$ is n-linear, then it is linear with respect to each argument.

It would be tempting to turn these two "if"s into "if and only if"s and use that as the definition of multilinearity. However, we must also add conditions of measurability:

Definition 18. Let n be a natural number and $X_1, \ldots, X_n, Y$ convex QBSs. An *n-linear map* from $X_1, \ldots, X_n$ to Y is a measurable map $f : |X_1| \times \ldots \times |X_n| \to |Y|$ such that for all $1 \leq k \leq n$, there exists a (necessarily unique) measurable map

$$f^{\perp k} : |X_1| \times \ldots \times |X_{k-1}| \times \left|Y^\perp\right| \times |X_{k+1}| \times \ldots \times |X_n| \to \left|X_k^\perp\right|$$

such that for all $x_1 \in |X_1|, \ldots, x_n \in |X_n|, \eta \in \left|Y^\perp\right|$,

$$\eta\, f(x_1, \ldots, x_n) = f^{\perp k}(x_1, \ldots, x_{k-1}, \eta, x_{k+1}, \ldots, x_n)\, x_k.$$

When $n = 1$, we say that f is *linear*, we write $f^\perp$ for $f^{\perp 1}$, and we write ηf for $f^\perp(\eta)$, so that the linearity condition reads $(\eta f)x = \eta(f(x))$.

If f is n-linear, then it is clear that $f^{\perp k}$ is n-linear for all $1 \leq k \leq n$.

One can easily check that multilinear maps commute with countable sums and expected values with respect to each argument. In particular, all linear maps are morphisms of S-algebras. We will see below (Fact 22) that in the case of data types, this necessary condition is also sufficient.

Fact 19. *Convex QBSs and multilinear maps between them form a symmetric multicategory (with composition and symmetries as in the symmetric multicategory* Set*), which we denote by* QbsConv.

Proof. It is straightforward to check that composition preserves multilinearity. Since composition and the symmetries are inherited from the symmetric multicategory Set, they satisfy the coherence axioms of symmetric multicategories. □

In particular, convex QBSs and linear maps between them form a category, which we also denote by QbsConv. Note that $-^\perp$ is a functor from $\mathrm{QbsConv}^{\mathrm{op}}$ to QbsConv.

Definition 20. We make $\underline{-} : \mathrm{Qbs} \to \mathrm{QbsConv}$ into a map of symmetric multicategories [17, Definitions 2.1.9 and 2.2.21] by letting $\underline{f}(\mu_1, \dots, \mu_n) = \int_{x_1 \in A_1} \cdots \int_{x_n \in A_n} \underline{f(x_1, \dots, x_n)}\, \mu_n(\mathrm{d}x_n) \dots \mu_1(\mathrm{d}x_1) \in \underline{B}$ for all $f \in \mathrm{Qbs}(A_1, \dots, A_n; B)$ and all $\mu_1 \in \underline{A_1}, \dots, \mu_n \in \underline{A_n}$.

In particular, $\underline{-}$ is a functor from the category Qbs to the category QbsConv.

Definition 21. For all convex QBSs $X_1, \dots, X_n, Y$, we make the set $\mathrm{QbsConv}(X_1, \dots, X_n; Y)$ of all n-linear maps from $(X_1, \dots, X_n)$ to Y into a QBS as follows: for all maps $(r \mapsto f_r)$ from $\mathbb{R}$ to $\mathrm{QbsConv}(X_1, \dots, X_n; Y)$, $(r \mapsto f_r) \in M_{\mathrm{QbsConv}(X_1, \dots, X_n; Y)}$ if and only if

- $(r \mapsto f_r)$ is a measurable as a map from $\mathbb{R}$ to $\mathrm{Qbs}(|X_1| \times \dots \times |X_n|, |Y|)$,
- for all k, $(r \mapsto f_r^{\perp k})$ is measurable as a map from $\mathbb{R}$ to $\mathrm{Qbs}(|X_1| \times \dots \times |X_{k-1}| \times \left|Y^\perp\right| \times |X_{k+1}| \times \dots \times |X_n|, \left|X_k^\perp\right|)$.

Multilinear maps between data types correspond exactly to sub-probability kernels:

Fact 22. *For all QBSs $A_1, \dots, A_n, B$, the maps*

$$f \mapsto (\mu_1, \dots, \mu_n) \mapsto \iint_{x_1 \in A_1, \dots, x_n \in A_n} f(x_1, \dots, x_n)\, \mu_1(\mathrm{d}x_1) \dots \mu_n(\mathrm{d}x_n)$$

$$\text{and } g \mapsto (x_1, \dots, x_n) \mapsto g\big(\underline{x_1}, \dots, \underline{x_n}\big)$$

define inverse natural isomorphisms between the QBSs $\mathrm{Qbs}(A_1, \dots, A_n; S(B))$ *and* $\mathrm{QbsConv}\left(\underline{A_1}, \dots, \underline{A_n}; \underline{B}\right)$.

In particular, a map $f : |\underline{A}| \to |\underline{B}|$ is linear if and only if it is a morphism of S-algebras.

Now, we need to equip spaces of multilinear maps with a structure of convex QBS. In other words, we need to define *linear tests* on multilinear maps. Intuitively, to test a linear map means to apply it to a randomly chosen input and then test its output with a randomly chosen test:

Notation 23. Let $X_1, \dots, X_n, Y$ be convex QBSs. For all $\theta = (\mu_p)_{p \in \mathbb{N}}$ in $S\Big(|X_1| \times \dots \times |X_n| \times \left|Y^\perp\right|\Big)^{\mathbb{N}}$ and all $f \in \mathrm{QbsConv}(X_1, \dots, X_n; Y)$, we write $\mathrm{Test}(f, \theta)$ for

$$\sum_{p \in \mathbb{N}} \int_{|X_1| \times \dots \times |X_n| \times \left|Y^\perp\right|} \eta\, f(x_1, \dots, x_n)\, \mu_p(\mathrm{d}(x_1, \dots, x_n, \eta)).$$

We denote by $\mathrm{QbsConv}^\perp(X_1, \dots, X_n; Y)$ the quotient of the QBS

$$\left\{ \begin{array}{c} \theta \in S\left(|X_1| \times \dots \times |X_n| \times \left|Y^\perp\right|\right)^{\mathbb{N}}; \\ \forall f \in \mathrm{QbsConv}(X_1, \dots, X_n; Y), \mathrm{Test}(f, \theta) \leq 1 \end{array} \right\}$$

by the equivalence relation that identifies θ_1 and θ_2 if and only if $\mathrm{Test}(f, \theta_1) = \mathrm{Test}(f, \theta_2)$ for all $f \in \mathrm{QbsConv}(X_1, \dots, X_n; Y)$. We denote the equivalence class of θ by $[\theta]$.

Definition 24. Let $X_1, \dots, X_n, Y$ be convex QBSs. We define a convex QBS $(X_1, \dots, X_n) \multimap Y$ by

- $\left|(X_1, \dots, X_n) \multimap Y\right| = \mathrm{QbsConv}(X_1, \dots, X_n; Y)$,
- $\left|\big((X_1, \dots, X_n) \multimap Y\big)^\perp\right| = \mathrm{QbsConv}^\perp(X_1, \dots, X_n; Y)$,
- $[\theta] f = \mathrm{Test}(f, \theta)$.

We make $(-, \dots, -) \multimap -$ into a functor from $(\mathrm{QbsConv}^{\mathrm{op}})^n \times \mathrm{QbsConv}$ to QbsConv by letting $\big((\alpha_1, \dots, \alpha_n) \multimap \beta\big) f = (x_1, \dots, x_n) \mapsto \beta(f(\alpha_1(x_1), \dots, \alpha_n(x_n)))$.

For all convex QBSs $X_1, \dots, X_n, Y$, all permutations σ of $[n] = \{1, \dots, n\}$ and all $f : (X_{\sigma(1)}, \dots, X_{\sigma(n)}) \multimap Y$, we denote by $\sigma^* f$ the linear map $(x_1, \dots, x_n) \mapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. This defines a natural isomorphism σ^* between $(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \multimap Y$ and $(X_1, \dots, X_n) \multimap Y$. We write σ_* for $(\sigma^*)^\perp$.

The convex QBS $\mathbb{W}$ is both neutral and dualising:

Fact 25. *For all convex QBSs $X_1, \dots, X_n, Y$, the map*

$$f \mapsto (x_1, \dots, x_n, r) \mapsto r\, f(x_1, \dots, x_n)$$

defines a natural isomorphism between $(X_1, \dots, X_n) \multimap Y$ and $(X_1, \dots, X_n, \mathbb{W}) \multimap Y$, and the map $\eta \mapsto y \mapsto \eta y$ defines a natural isomorphism between $Y^\perp$ and $Y \multimap \mathbb{W}$.

The symmetric multicategory QbsConv is closed in the following sense:

Proposition 26. *For all convex QBSs $X_1, \dots, X_m$, $Y_1, \dots, Y_n, Z$, the maps*

$$f \mapsto (x_1, \dots, x_m) \mapsto (y_1, \dots, y_n) \mapsto f(x_1, \dots, x_m, y_1, \dots, y_n)$$

$$F \mapsto (x_1, \dots, x_m, y_1, \dots, y_n) \mapsto F(x_1, \dots, x_m)(y_1, \dots, y_m)$$

define inverse natural isomorphisms between $(X_1, \dots, X_m, Y_1, \dots, Y_n) \multimap Z$ and $(X_1, \dots, X_m) \multimap (Y_1, \dots, Y_n) \multimap Z$.

Proof. For simplicity, we assume $m = n = 1$, and we drop the corresponding indices. The general proof is similar.

First, we check that the first map, which we will denote by φ, is well-defined. Let $f \in (X, Y) \multimap Z$. For all $x \in X$, $\varphi(f)(x)$ is linear, with $\varphi(f)(x)^\perp = (\zeta \mapsto f^{\perp 2}(x, \zeta))$. In addition, $\varphi(f)$ is linear, with $\varphi(f)^\perp = ([\theta] \mapsto (x \mapsto \mathrm{Test}(\varphi(f)(x), \theta)))$ (identifying $X^\perp$ with $X \multimap \mathbb{W}$): indeed, for all $(y, \zeta) \in |Y| \times \left|Z^\perp\right|$ and all $x \in |X|$, $\mathrm{Test}\left(\varphi(f)(x), \underline{(y, \zeta)}\right) = \zeta\, f(x, y) = f^{\perp 1}(\zeta, y)(x)$.

Now, we check that φ is linear. For all $f \in (X, Y) \multimap Z$, all $x \in X$ and all $[\theta_2] \in (Y \multimap Z)^\perp$, $\mathrm{Test}\left(\varphi(f), \underline{(x, [\theta_2])}\right) = \mathrm{Test}\left(f, \int \underline{(x, y, \zeta)}\, \theta_2(\mathrm{d}(y, \zeta))\right)$, so φ is linear, with $\varphi^\perp = [\theta_1] \mapsto f \mapsto \mathrm{Test}((x, [\theta_2]) \mapsto \mathrm{Test}((y, \zeta) \mapsto \zeta f(x, y), \theta_2), \theta_1)$.

The proof of linearity for the inverse map is similar. □

We saw that whenever f is n-linear, $f^{\perp k}$ is also n-linear for all k. In fact, there is a stronger result:

Fact 27. *For all convex QBSs $X_1, \dots, X_n, Y$ and all $k \leq n$, the map $f \mapsto f^{\perp k}$ defines a natural isomorphism between $(X_1, \dots, X_n) \multimap Y$ and $(X_1, \dots, X_{k-1}, Y^\perp, X_{k+1}, \dots, X_n) \multimap X_k^\perp$.*

For all convex QBSs X, Y, we let $X \otimes Y = \big((X, Y) \multimap \mathbb{W}\big)^\perp$. For all $x \in X$ and $y \in Y$, we denote by $x \otimes y$ the unique element of $|X \otimes Y|$ such that $f(x \otimes y) = f(x, y)$ for all $f \in \big|(X, Y) \multimap \mathbb{W}\big| = \big|(X \otimes Y)^\perp\big|$. It follows from the above discussion that the map

$$f \mapsto (w_1, \dots, w_n, x, y) \mapsto f(w_1, \dots, w_n, x \otimes y)$$

defines a natural isomorphism between $(W_1, \dots, W_n, X \otimes Y) \multimap Z$ and $(W_1, \dots, W_n, X, Y) \multimap Z$, and therefore that $(\mathrm{QbsConv}, \mathbb{W}, \otimes, \multimap)$ is a closed symmetric monoidal category. For all maps $f : (X, Y) \multimap Z$, we will denote by $x \otimes y \mapsto f(x, y)$ the corresponding map in $X \otimes Y \multimap Z$.

As in probabilistic coherence spaces, the intuition behind the tensor product $\otimes$ is that a random value of type $X \otimes Y$ is a random pair of values of types X and Y, that is to say, two random values of types X and Y that have to be sampled jointly. This intuition is supported by how the tensor product behaves on data types:

Fact 28. *For all QBSs A and B, the map*

$$\rho \mapsto \int_{(x,y) \in A \times B} \underline{x} \otimes \underline{y}\, \rho(\mathrm{d}(x, y))$$

defines a natural isomorphism between $\underline{A \times B}$ and $\underline{A} \otimes \underline{B}$.

Proof. Consequence of Fact 22. □

V. Additive connectives

Definition 29. Let $(X_i)_{i \in I}$ be a countable family of convex QBSs. We define a convex QBS $\mathop{\&}_{i \in I} X_i$ by

- $\left|\mathop{\&}_{i \in I} X_i\right| = \prod_{i \in I} |X_i|$,
- $\left|\left(\mathop{\&}_{i \in I} X_i\right)^\perp\right| = \{(\eta_i)_{i \in I} \in \prod_{i \in I} \left|X_i^\perp\right| ;\ \forall (x_i)_{i \in I} \in \prod_{i \in I} |X_i|, \sum_{i \in I} \eta_i\, x_i \leq 1\}$,
- $(\eta_i)_{i \in I} \cdot (x_i)_{i \in I} = \sum_{i \in I} \eta_i\, x_i$.

In addition, we let $\bigoplus_{i \in I} X_i = \left(\mathop{\&}_{i \in I} X_i^\perp\right)^\perp$.

For all $j \in I$, we let π_j denote the projection from $\prod_{i \in I} |X_i|$ to X_j, and L_j the map $x_j \mapsto \begin{pmatrix} x_j & \text{if } i = j \\ 0_{X_i} & \text{otherwise} \end{pmatrix}_{i \in I}$ from X_j to $\prod_{i \in I} |X_i|$.

Fact 30. *Let $(X_i)_{i \in I}$ be a countable family of convex QBSs: $\left(\mathop{\&}_{i \in I} X_i, (\pi_i)_{i \in I}\right)$ is a cartesian product of the family $(X_i)_{i \in I}$, and $\left(\bigoplus_{i \in I} X_i, (L_i)_{i \in I}\right)$ is a coproduct of the family $(X_i)_{i \in I}$. In addition, $\mathbb{0}$ is both initial and terminal.*

As in probabilistic coherence spaces, the intuition is that a random value of type $X \,\&\, Y$ is in fact two random values of types X and Y that can be sampled separately, while a random value of type $X \oplus Y$ is one that, every time it is sampled, yields either a value of type X or a value of type Y. In the case of $\&$, this is just an other way of saying we have a cartesian product, while in the case of $\oplus$, the intuition is supported by how it behaves on data types:

Fact 31. *For all countable families $(A_i)_{i \in I}$ of QBSs, the map*

$$[\alpha, \mu] \mapsto \sum_{i \in I} \int_{r \in \alpha^{-1}(A_i)} L_i\Big(\underline{\alpha(r)}\Big)\, \mu(\mathrm{d}r)$$

defines a natural isomorphism between $\underline{\coprod_{i \in I} A_i}$ and $\bigoplus_{i \in I} \underline{A_i}$.

VI. Symmetric maps and tensors

In order to define the exponential modalities, we will need to define the spaces of symmetric maps and symmetric tensors.

For all $n \in \mathbb{N}$, we denote by $\mathrm{Sym}(n)$ the group of permutations of $[n] = \{1, \dots, n\}$.

Definition 32. Let n be a natural number and X, Y convex QBSs. We write $(X)^n \multimap Y$ for $(X, \dots, X) \multimap Y$, where X appears n times.

- an n-linear map $f : (X)^n \multimap Y$ is *symmetric* if $\sigma^* f = f$ for all $\sigma \in \mathrm{Sym}(n)$,
- a test $\eta \in \big((X)^n \multimap Y\big)^\perp$ is *symmetric* if $\sigma_* \eta = \eta$ for all $\sigma \in \mathrm{Sym}(n)$.

If two symmetric maps $f_1, f_2 \in (X)^n \multimap Y$ are such that $\eta f_1 = \eta f_2$ for all symmetric tests η, then $f_1 = f_2$. Indeed, let η be any test in $\big((X)^n \multimap Y\big)^\perp$: then $\sum_{\sigma \in \mathrm{Sym}(n)} \frac{1}{n!} \sigma_* \eta$ is symmetric, so $\left(\sum_\sigma \frac{1}{n!} \sigma_* \eta\right) f_1 = \left(\sum_\sigma \frac{1}{n!} \sigma_* \eta\right) f_2$, which means that $\eta \left(\sum_\sigma \frac{1}{n!} \sigma^* f_1\right) = \eta \left(\sum_\sigma \frac{1}{n!} \sigma^* f_2\right)$; since f_1 and f_2 are symmetric, this implies $\eta f_1 = \eta f_2$. Conversely, any two symmetric tests that coincide on symmetric maps are equal. As a result, we can define convex QBSs of *symmetric maps* and *symmetric tensors*:

Definition 33. Let n be a natural number and X, Y convex QBSs. We define a convex QBS $(X)^n_s \multimap Y$ by

- $\left|\begin{matrix}(X)^n_s \multimap Y \\ (X)^n \multimap Y\end{matrix}\right|$ is the set of all symmetric maps in $(X)^n \multimap Y$,
- $\left|\begin{matrix}\big((X)^n_s \multimap Y\big)^\perp \\ \big((X)^n \multimap Y\big)^\perp\end{matrix}\right|$ is the set of all symmetric tests in $\big((X)^n \multimap Y\big)^\perp$,
- $\eta \cdot_{(X)^n_s \multimap Y} f = \eta \cdot_{(X)^n \multimap Y} f$.

We let $X^{\otimes n} = \big((X)^n \multimap \mathbb{W}\big)^\perp$ and $X^{\otimes_s n} = \big((X)^n_s \multimap \mathbb{W}\big)^\perp$.

For all $n \in \mathbb{N}$, we define a linear map $\mathcal{S}_n : X^{\otimes n} \multimap X^{\otimes_s n}$ by $\mathcal{S}_n = \sum_{\sigma \in \mathrm{Sym}(n)} \frac{1}{n!} \sigma_*$. The restriction of $\mathcal{S}_n$ to $X^{\otimes_s n}$ is the identity.

VII. The exponential modalities

So far, we have defined *linear maps* between QBSs. We would like to define a more general notion of "computable" maps (which we will call *analytic maps*, due to their similarity with power series). Following the paradigm of linear logic [19], the first step will be to define the exponential modality "!" ("of course"). The other exponential modality, "?" ("why not"), can be defined by duality.

A. Defining $!X$

In this subsection, we fix a convex QBS X. We will define the convex QBS $!X$ using a generic construction by Melliès, Tabareau and Tasson [20]. Following their terminology, we call a *pointed object* any pair (Y, u) with Y a convex QBS and $u : Y \multimap \mathbb{W}$, and a *pointed morphism* from (Y, u) to (Z, v) any linear map $f : Y \multimap Z$ such that $u = v \circ f$. In order to apply this construction, we only need to prove two conditions. The first is that $(X \,\&\, \mathbb{W}, (x, r) \mapsto r, (x, r) \mapsto x)$ defines a *free pointed object* over X in the following sense:

Fact 34. *For all pointed objects (Y, u) and all linear maps $f : Y \multimap X$, there exists a unique pointed morphism g form (Y, u) to $(X \,\&\, \mathbb{W}, (x, r) \mapsto r)$ such that $((x, r) \mapsto x) \circ g = f$.*

Proof. Let g be any map from $|Y|$ to $|X \,\&\, \mathbb{W}|$. Then g is a pointed morphism satisfying this hypothesis if and only for all $y \in Y$, $g(y) = (f(y), u(y))$. □

For all $m \in \mathbb{N}$, we denote by $\mathcal{J}_{m+1,m}$ the canonical projection $(X \,\&\, \mathbb{W})^{\otimes_s m+1} \multimap (X \,\&\, \mathbb{W})^{\otimes_s m}$, that is to say, the restriction to $(X \,\&\, \mathbb{W})^{\otimes_s m+1}$ of the unique linear map $(X \,\&\, \mathbb{W})^{\otimes m+1} \multimap (X \,\&\, \mathbb{W})^{\otimes m}$ that sends $(x_1, r_1) \otimes \ldots \otimes (x_{m+1}, r_{m+1})$ to $r_{m+1}(x_1, r_1) \otimes \ldots \otimes (x_m, r_m)$. For all $n \geq m$, we let $\mathcal{J}_{n,m} = \mathcal{J}_{m+1,m} \circ \ldots \circ \mathcal{J}_{n,n-1}$. The second condition we need to prove is that the diagram

$$(X\&\mathbb{W})^{\otimes_s 0} \leftarrow \ldots (X\&\mathbb{W})^{\otimes_s m} \overset{\mathcal{J}_{m+1,m}}{\leftarrow} (X\&\mathbb{W})^{\otimes_s m+1} \ldots$$

has a limit and that this limit commutes with the tensor product: $!X$ will be defined as this limit. The remainder of this section deals with the technical details of how to do this.

The obvious choice for the underlying QBS $|!X|$ is the set of all $(a_n)_{n\in\mathbb{N}} \in \left|\&_{n\in\mathbb{N}} (X \,\&\, \mathbb{W})^{\otimes_s n}\right|$ such that $\mathcal{J}_{n,m}(a_n) = a_m$ for all $m \leq n$. In fact, it would be easy to define a structure of convex QBS on top of this, to prove that it is a limit of the above diagram, and to prove that this limit commutes with tensor products *if* the maps $\mathcal{J}_{n,m}$ had sections. However, they are not even necessarily surjective. Indeed, consider for example the case where $X = \mathbb{W} \oplus \mathbb{W}$, $m = 2$ and $n = 3$. Let $f : (X \,\&\, \mathbb{W})^{\otimes 2} \multimap \mathbb{W}$ be defined by $f((r_0, r_1, r_*) \otimes (s_0, s_1, s_*)) = r_0 s_1 + r_1 s_0$. An elementary computation shows that for all $a \in (X \,\&\, \mathbb{W})^{\otimes 3}$, $f(\mathcal{J}_{3,2}(\mathcal{S}(a))) \leq \frac{2}{3}$, whereas $f\left(\frac{1}{2}(0,1,0) \otimes (1,0,0) + \frac{1}{2}(1,0,0) \otimes (0,1,0)\right) = 1$.

So instead, we will prove that $\mathcal{J}_{n,m}$ has a section *up to a factor that depends only on* m. Namely, for all $m \in \mathbb{N}$, we will define a real number $\rho_m \geq 1$, and for all $m, n \in \mathbb{N}$, we will define a linear map $\mathcal{K}_{m,n} : (X \,\&\, \mathbb{W})^{\otimes_s m} \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$ such that:

- $\mathcal{K}_{m,n} = \frac{1}{\rho_m} \mathcal{J}_{m,n}$ if $m \geq n$,
- $\mathcal{J}_{n,m} \circ \mathcal{K}_{m,n} = \frac{1}{\rho_m} \mathrm{id}_{(X\&\mathbb{W})^{\otimes_s m}}$ if $m \leq n$.

An element of $X^{\otimes n}$ can be seen as a (non-commutative) homogeneous polynomial of degree n. Likewise, an element of $(X \,\&\, \mathbb{W})^{\otimes n}$ can be seen as a (non-necessarily homogeneous) polynomial of degree at most n. For example, $(x, 1) \otimes (y, 1) = (x, 0) \otimes (y, 0) + (x, 0) \otimes (0, 1) + (0, 1) \otimes (y, 0) + (0, 1) \otimes (0, 1)$ represents the polynomial "$x \otimes y + x + y + 1$" (which we put between quotes because this is not a well-defined notation).

Homogeneous polynomials can be extracted from elements of $(X \,\&\, \mathbb{W})^{\otimes_s m}$ as follows: for all $m, n \in \mathbb{N}$, we denote by $\mathcal{M}_{n,m}$ the canonical projection $(X \,\&\, \mathbb{W})^{\otimes_s n} \multimap X^{\otimes_s m}$, that is to say, the restriction to $(X \,\&\, \mathbb{W})^{\otimes_s n}$ of the unique linear map $(X \,\&\, \mathbb{W})^{\otimes n} \multimap X^{\otimes m}$ that maps $(x_1, r_1) \otimes \ldots \otimes (x_n, r_n)$ to $r_{m+1} \ldots r_n \, x_1 \otimes \ldots \otimes x_m$ if $m \leq n$, and to 0 if $m > n$.

For all $m, n \in \mathbb{N}$, we denote by $\mathrm{Inj}(m, n)$ the set of all injections from $[m]$ to $[n]$. We want to define for all $m \leq n$ a section of $\mathcal{J}_{n,m}$ up to a factor that depends only on m. To that end, we will first define for all $m \leq n$ a section of $\mathcal{M}_{n,m}$ up to a factor that depends only on m:

Lemma 35. *For all $m, p > 0$, there exists a unique linear map from $X^{\otimes m}$ to $(X \,\&\, \mathbb{W})^{\otimes_s mp}$ that maps $x_1 \otimes \ldots \otimes x_m$ to*

$$\sum_{j \in \mathrm{Inj}(m,mp)} \frac{1}{m^m} \bigotimes_{k=1}^{mp} \begin{pmatrix} \left(x_{j^{-1}(k)}, 0\right) & \text{if } k \in \mathrm{im}\,(j) \\ (0,1) & \text{if } k \notin \mathrm{im}\,(j) \end{pmatrix}.$$

Proof. For all $\eta \in \left|\left((X \,\&\, \mathbb{W})^{\otimes_s mp}\right)^{\perp}\right|$ and all $x_1, \ldots, x_m \in X$,

$$\begin{aligned} 1 &\geq \eta\left((x_1, 1)^{\otimes p} \otimes \ldots \otimes (x_m, 1)^{\otimes p}\right) \\ &\geq \mathrm{Avg}_{j \in \mathrm{Inj}(m,mp)}\, p^m \eta \bigotimes_{k=1}^{mp} \begin{pmatrix} \left(x_{j^{-1}(k)}, 0\right) & k \in \mathrm{im}\,(j) \\ (0,1) & k \notin \mathrm{im}\,(j) \end{pmatrix} \end{aligned}$$

(where Avg stands for average). Indeed, out of the 2^{mp} terms obtained by developing the product $(x_1, 1)^{\otimes p} \otimes \ldots \otimes (x_m, 1)^{\otimes p}$ (where (y, r) is to be read as $(y, 0) + (0, r)$), p^m are of the form: one factor $(x_i, 0)$ for each $i \in [m]$, and all the other factors equal to $(0, 1)$ (and η takes the same value on all such terms, because it is symmetric, so only their number matters). Since there are $\frac{(mp)!}{(mp-m)!}$ injections from $[m]$ to $[mp]$, and since $p^m \frac{(mp-m)!}{(mp)!} \geq \frac{1}{m^m}$, we get

$$1 \geq \sum_{j \in \mathrm{Inj}(m,mp)} \frac{1}{m^m} \eta \bigotimes_{k=1}^{mp} \begin{pmatrix} \left(x_{j^{-1}(k)}, 0\right) & \text{if } k \in \mathrm{im}\,(j) \\ (0,1) & \text{if } k \notin \mathrm{im}\,(j) \end{pmatrix}.$$

□

We denote by $\mathcal{N}_{m,mp}$ the restriction of this map to $X^{\otimes_s m}$: one can check that $\mathcal{M}_{mp,m} \circ \mathcal{N}_{m,mp} = \frac{m!}{m^m} \mathrm{id}_{X^{\otimes_s m}}$. For all $m > 0$ and all $n \in \mathbb{N}$, we define $\mathcal{N}_{m,n} : X^{\otimes_s m} \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$ by $\mathcal{N}_{m,n} = \mathcal{J}_{mp,n} \circ \mathcal{N}_{m,mp}$, where p is smallest positive integer such that $mp \geq n$ (which makes sense because $\mathcal{J}_{mp,n}$ is the identity when $n = mp$). Finally we define $\mathcal{N}_{0,n} : X^{\otimes_s 0} \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$ for all $n \in \mathbb{N}$ by $\mathcal{N}_{0,n}(r) = r \bigotimes_{k=1}^{n} (0, 1)$. One can check that for all $m, n \in \mathbb{N}$,

$$\mathcal{M}_{n,m} \circ \mathcal{N}_{m,n} = \begin{cases} \frac{m!}{m^m} \mathrm{id}_{X^{\otimes_s m}} & \text{if } n \geq m \\ 0 & \text{if } n < m \end{cases}$$

(with the convention that $0^0 = 1$). Intuitively, $\mathcal{N}_{m,n}$ takes a homogeneous polynomial of degree m and, if possible, represents it as an element of $(X \,\&\, \mathbb{W})^{\otimes_s n}$, up to a factor $\frac{m!}{m^m}$.

For all $m \in \mathbb{N}$, we let $\rho_m = \frac{m^m(m+1)}{m!}$. For all $m, n \in \mathbb{N}$, we define $\mathcal{K}_{m,n} : (X \,\&\, \mathbb{W})^{\otimes_s m} \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$ by

$$\mathcal{K}_{m,n} = \sum_{k=0}^{m} \frac{1}{(m+1)} \frac{k^k\, m!}{k!\, m^m} \mathcal{N}_{k,n} \circ \mathcal{M}_{m,k}$$

(which is well-defined because $\frac{k^k}{k!} \leq \frac{m^m}{m!}$ for all $k \leq m$). In other words, for all k, $\mathcal{K}_{m,n}$ extracts from its argument the homogeneous part of degree k, turns that part into an element of $(X \,\&\, \mathbb{W})^{\otimes_s n}$ up to a factor $\frac{1}{\rho_m}$, and then sums all the results. Thus, for all $m, n \in \mathbb{N}$, we do have:

- $\mathcal{K}_{m,n} = \frac{1}{\rho_m} \mathcal{J}_{m,n}$ if $m \geq n$,
- $\mathcal{J}_{n,m} \circ \mathcal{K}_{m,n} = \frac{1}{\rho_m} \mathrm{id}_{(X \& \mathbb{W})^{\otimes_s m}}$ if $m \leq n$.

All this means that the following definition makes sense:

Definition 36. We define a convex QBS $!X$ as follows

- $|!X| = \left\{ \begin{array}{l} (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} (X \,\&\, \mathbb{W})^{\otimes_s n}; \\ \forall m \leq n, a_m = \mathcal{J}_{n,m}(a_n) \end{array} \right\}$
- $\left|(!X)^\perp\right|$ is the set of all families of maps $(f_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathrm{Qbs}\left(\left|(X \,\&\, \mathbb{W})^{\otimes n}\right|, [0, +\infty)\right)$ such that
  - for all n, $\frac{f_n}{\rho_n}$ is in $(X \,\&\, \mathbb{W})^{\otimes n} \multimap \mathbb{W}$ and is symmetric,
  - for all $m \leq n$, $f_m = \rho_m\, f_n \circ \mathcal{K}_{m,n}$,
  - for all $(a_n)_{n\in\mathbb{N}} \in |!X|$, $\sup_{n\in\mathbb{N}} f_n(a_n) \leq 1$,

  with the subset QBS structure,
- $(f_n)_{n\in\mathbb{N}} \cdot_{!X} (a_n)_{n\in\mathbb{N}} = \sup_{n\in\mathbb{N}} f_n(a_n)$.

As stated in the introduction, to make this definition usable, we need to reformulate it in terms of countable sums. To this end, for all $n, k \in \mathbb{N}$, we define a linear map $\mathcal{D}_{n,k} : (X \,\&\, \mathbb{W})^{\otimes_s n} \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$ by $\mathcal{D}_{n,k} = \frac{k^k}{k!} \mathcal{N}_{k,n} \circ \mathcal{M}_{n,k}$. This map extracts the homogeneous part of degree k without changing the type of its argument. In particular, $\mathrm{id}_{(X \& \mathbb{W})^{\otimes_s n}} = \sum_{k=0}^{n} \mathcal{D}_{n,k}$.

Fact 37. *For all families of maps $(f_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathrm{Qbs}\left(\left|(X \,\&\, \mathbb{W})^{\otimes n}\right|, [0, +\infty)\right)$, $(f_n)_{n\in\mathbb{N}} \in \left|(!X)^\perp\right|$ if and only if*

- *for all n, $\frac{f_n}{\rho_n}$ is in $(X \,\&\, \mathbb{W})^{\otimes n} \multimap \mathbb{W}$ and is symmetric,*
- *for all n, $f_{n+1} = f_n \circ \mathcal{J}_{n+1,n} + f_{n+1} \circ \mathcal{D}_{n+1,n+1}$,*
- *for all $(a_n)_{n\in\mathbb{N}} \in |!X|$, $\sum_{n\in\mathbb{N}} f_n \circ \mathcal{D}_{n,n}(a_n) \leq 1$.*

In addition, for all $(a_n)_{n\in\mathbb{N}} \in |!X|$, $(f_n)_{n\in\mathbb{N}} \cdot_{!X} (a_n)_{n\in\mathbb{N}} = \sum_{n\in\mathbb{N}} f_n \circ \mathcal{D}_{n,n}(a_n)$.

For all $n \in \mathbb{N}$, we denote by π_n the canonical projection $!X \multimap (X \,\&\, \mathbb{W})^{\otimes_s n}$. These projections also have sections up to a factor $\frac{1}{\rho_n}$:

Notation 38. Let $n \in \mathbb{N}$. For all $a_n \in (X \,\&\, \mathbb{W})^{\otimes_s n}$, we let $\theta_n(a_n) = \left(\mathcal{K}_{n,m} a_n\right)_{m\in\mathbb{N}}$. This defines a linear map $\theta_n : (X \,\&\, \mathbb{W})^{\otimes_s n} \multimap !X$ that satisfies the equation $\pi_n \circ \theta_n = \frac{1}{\rho_n} \mathrm{id}_{(X \& \mathbb{W})^{\otimes_s n}}$.

With that, it is clear that $!X$ is the limit of the diagram

$$(X \& \mathbb{W})^{\otimes_s 0} \leftarrow \ldots (X \& \mathbb{W})^{\otimes_s m} \overset{\mathcal{J}_{m+1,m}}{\leftarrow} (X \& \mathbb{W})^{\otimes_s m+1} \ldots$$

and that this limit commutes with the tensor product, namely:

Theorem 39. *Let Z,Y be convex QBSs, and let $(\varphi_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \left(Z \multimap Y \otimes (X \,\&\, \mathbb{W})^{\otimes_s n}\right)$ be such that for all $m \leq n$, $\left(\mathrm{id}_Y \otimes \mathcal{J}_{n,m}\right) \circ \varphi_n = \varphi_m$. Then the map*

$$\varphi_\infty : \left\{ \begin{array}{rl} |Z| \to & |Y \otimes !X| \\ z \;\mapsto & \sup_{n\in\mathbb{N}} \rho_n \left(\mathrm{id}_Y \otimes \theta_n\right) \circ \varphi_n(z) \\ & = \sum_{n\in\mathbb{N}} \rho_n \left(\mathrm{id}_Y \otimes (\theta_n \circ \mathcal{D}_{n,n})\right) \circ \varphi_n(z) \end{array} \right.$$

- *is well-defined,*
- *is a linear map from Z to $Y \otimes !X$,*
- *is the only map from $|Z|$ to $|Y \otimes !X|$ such that for all $n \in \mathbb{N}$, $(\mathrm{id}_Y \otimes \pi_n) \circ \varphi_\infty = \varphi_n$.*

As in probabilistic coherence spaces, a random value of $!X$ represents a generator of random values of X whose distribution is itself random.

B. The free commutative comonoid structure on $!X$

Because of Fact 34 and Theorem 39, we know that for all X, $!X$ can be equipped with a structure of commutative comonoid freely generated by X [20, definition in the introduction]. In this subsection, we simply spell out this structure and a few constructions that come from it. This will come in handy when defining and proving statements about analytic maps.

First, note that Theorem 39 turns "!" into a functor from QbsConv to QbsConv, with $(!f)(a_n)_{n\in\mathbb{N}} = ((f \otimes \mathrm{id}_{\mathbb{W}})^{\otimes_s n}(a_n))_{n\in\mathbb{N}}$ for all $f : X \multimap Y$ and all $(a_n)_{n\in\mathbb{N}} \in !X$.

The following notation will be useful to define linear maps from spaces of the form $!X$:

Notation 40. Let X, Y be convex QBSs, $n \in \mathbb{N}$ and $f : (X \,\&\, \mathbb{W})^n \multimap Y$. We denote by

$$\left(\bigotimes_{k=1}^{m} (x_{m,k}, r_{m,k})\right)_{m\in\mathbb{N}} \mapsto f\left((x_{n,1}, r_{n,1}), \ldots, (x_{n,n}, r_{n,n})\right)$$

the linear map $f \circ \pi_n \in !X \multimap Y$.

Definition 41. For all convex QBSs X, using the above notation, we define a linear map $\mathrm{weak}_X : !X \multimap \mathbb{W}$ as

$$\left(\bigotimes_{k=1}^{m} (x_{m,k}, r_{m,k})\right)_{m\in\mathbb{N}} \mapsto 1,$$

a linear map $\mathrm{cont}_X : !X \multimap !X \otimes !X$ as

$$\begin{array}{rl} & \left(\bigotimes_{k=1}^{m} (x_{m,k}, r_{m,k})\right)_{m\in\mathbb{N}} \\ \mapsto & \sup_{p,q\in\mathbb{N}} \left(\begin{array}{l} \left(\rho_p \theta_p \bigotimes_{k=1}^{p} \left(x_{p+q,k}, r_{p+q,k}\right)\right) \\ \otimes \left(\rho_q \theta_q \bigotimes_{k=p+1}^{p+q} \left(x_{p+q,k}, r_{p+q,k}\right)\right) \end{array} \right) \\ = & \sum_{p,q\in\mathbb{N}} \left(\begin{array}{l} \left(\rho_p \theta_p \mathcal{D}_{p,p} \bigotimes_{k=1}^{p} \left(x_{p+q,k}, r_{p+q,k}\right)\right) \\ \otimes \left(\rho_q \theta_q \mathcal{D}_{q,q} \bigotimes_{k=p+1}^{p+q} \left(x_{p+q,k}, r_{p+q,k}\right)\right) \end{array} \right) \end{array}$$

(where composition and application are noted multiplicatively), and a linear map $\mathrm{der}_X : !X \multimap X$ as

$$\left(\bigotimes_{k=1}^{m} \left(x_{m,k}, r_{m,k}\right)\right)_{m\in\mathbb{N}} \mapsto x_{1,1}.$$

As a consequence of Theorem 39, we get:

Proposition 42. *For all convex QBSs X, $(!X, \mathrm{weak}_X, \mathrm{cont}_X)$ is a commutative comonoid freely generated by (X, der_X).*

This is known [21] to imply the following results:

- Let $\mathrm{dig}_X : !X \multimap !!X$ be the unique morphism of comonoids such that $\mathrm{der}_{!X} \circ \mathrm{dig}_X = \mathrm{id}_{!X}$. Then $(!, \mathrm{der}, \mathrm{dig})$ is a comonad. We denote by $\ll$ its Kleisli composition, *i.e.* for all $f \in !X \multimap Y$ and all $g \in !Y \multimap Z$, $g \ll f = g \circ !f \circ \mathrm{dig}_X$.
- Let $\mathrm{store}_{X_1,\dots,X_n} : !X_1 \otimes \dots \otimes !X_n \multimap !(X_1 \,\&\, \dots \,\&\, X_n)$ be the unique morphism of comonoids such that $\mathrm{der}_{X_1 \& \dots \& X_n} \circ \mathrm{store}_{X_1,\dots,X_n} = a_1 \otimes \dots \otimes a_n \mapsto (\mathrm{der}_{X_1}(a_1), \dots, \mathrm{der}_{X_n}(a_n))$. Then $\mathrm{store}_{X_1,\dots,X_n}$ is an isomorphism.
- The Kleisli category of the comonad ! is cartesian closed.

For all convex QBSs X and all $n \in \mathbb{N}$, we denote by $\mathrm{cont}_{X,n}$ the canonical linear map from $!X$ to $(!X)^{\otimes_s n}$. In particular, $\mathrm{cont}_{X,2} = \mathrm{cont}_X$, $\mathrm{cont}_{X,1} = \mathrm{id}_{!X}$, and $\mathrm{cont}_{X,0} = \mathrm{weak}_X$. For all $n \in \mathbb{N}$ and all $m_1, \dots, m_n \in \mathbb{N}$, one can check that

- $(\pi_{m_1} \otimes \dots \otimes \pi_{m_n}) \circ \mathrm{cont}_{X,n} = \pi_{m_1+\dots+m_n}$,
- $\big(\mathrm{cont}_{X,m_1} \otimes \dots \otimes \mathrm{cont}_{X,m_n}\big) \circ \mathrm{cont}_{X,n} = \mathrm{cont}_{X,m_1+\dots+m_n}$ (which is just an other way of saying that $!X$ is a comonoid).

VIII. Analytic maps

In coherence spaces [19], seen as a model of computation, computable functions are represented by *stable maps*. Each coherence space X comes with a universal stable map from X to $!X$, in the sense that a map from X to Y is stable if and only if it can be obtained by composing this universal map with a (necessarily unique) linear map from $!X$ to Y. We use this idea to define analytic maps between convex QBSs, and we prove that convex QBSs and analytic maps form a cartesian closed category.

Definition 43. Let X be a convex QBS. We define a measurable map $\nabla_X : |X| \to |!X|$ by $\nabla_X(x) = \big((x,1)^{\otimes n}\big)_{n\in\mathbb{N}}$.

This map is injective (because $\mathrm{der}_X \circ \nabla_X = \mathrm{id}_X$), and monotone. A useful remark is that its image is exactly the set of "co-idempotent" elements of the comonoid $!X$ (minus $0_{!X}$):

Fact 44. *Let X be a convex QBS. For all $a \in !X$, $\mathrm{cont}_X(a) = a \otimes a$ if and only if $a = 0$ or $a = \nabla_X(\mathrm{der}_X(a))$.*

Proof. One can check from the definition of cont that $\mathrm{cont}(0) = 0 \otimes 0$ and that $\mathrm{cont}(\nabla(x)) = \nabla(x) \otimes \nabla(x)$ for all $x \in X$.

Assume $\mathrm{cont}(a) = a \otimes a$. Then $\pi_0(a) = (\pi_0 \otimes \pi_0)(a) = \pi_0(a)^2$, therefore $\pi_0(a) = 0$ or $\pi_0(a) = 1$. In addition, for all n, $\pi_{n+1}(a) = (\pi_1 \otimes \pi_n) \circ \mathrm{cont}(a) = (\pi_1 \otimes \pi_n)(a \otimes a)$. One can check that $\pi_1(a) = (\mathrm{der}(a), \pi_0(a))$, so by induction, for all $n > 0$, $\pi_n(a) = \pi_1(a)^{\otimes n} = (\mathrm{der}(a), \pi_0(a))^{\otimes n}$. If $\pi_0(a) = 1$, that means $a = \nabla(\mathrm{der}(a))$. If $\pi_0(a) = 0$, that means $\pi_1(a) = \mathcal{J}_{2,1}(\pi_2(a)) = \mathcal{J}_{2,1}((\mathrm{der}(a), 0)^{\otimes 2}) = 0$, so $a = 0$. ☐

The map ∇_X duplicates its input, including side-effects (*i.e.* probabilistic choices and non-termination), and as such it is not linear (unless X is $\mathbb{0}$). However, as one would expect, in the case of data types, values (not side effects) can be duplicated linearly. Namely, for all QBSs A, there exists a unique linear map $\mathrm{copy}_A : \underline{A} \multimap !\underline{A}$ such that for all $x \in A$, $\mathrm{copy}_A(\underline{x}) = \nabla_{\underline{A}}(\underline{x})$ (defined by $\mathrm{copy}_A(\mu) = \int_{x\in A} \nabla_{\underline{A}}(\underline{x})\, \mu(\mathrm{d}x)$).

Definition 45. Let X, Y be convex QBSs. An *analytic map* from X to Y is a (necessarily measurable and monotone) map $f : |X| \to |Y|$ such that there exists a linear map $f_! : !X \multimap Y$ such that $f = f_! \circ \nabla_X$.

The map ∇_X is analytic by definition, and it is universal in the following sense:

Theorem 46. *Let X, Y be convex QBSs and f an analytic map from X to Y. There exists a unique linear map $f_! : !X \multimap Y$ such that $f = f_! \circ \nabla_X$.*

Proof. It is sufficient to prove that for all $\alpha = (\alpha_n)_{n\in\mathbb{N}}, \beta = (\beta_n)_{n\in\mathbb{N}} \in (!X)^\perp$, if $\alpha\nabla(x) = \beta\nabla(x)$ for all $x \in X$, then $\alpha = \beta$. For all x, by Fact 37, $\alpha\nabla(x) = \sum_{n\in\mathbb{N}} \alpha_n \circ \mathcal{D}_{n,n} \circ \pi_n \circ \nabla(x) = \sum_{n\in\mathbb{N}} \alpha_n\big((x,0)^{\otimes n}\big)$, and similarly for β. In addition, also by Fact 37, in order to prove that $\alpha = \beta$, it is sufficient to prove that for all $n \in \mathbb{N}$, $\alpha_n \circ \mathcal{D}_{n,n} = \beta_n \circ \mathcal{D}_{n,n}$. Therefore, it is sufficient to prove that for all $n \in \mathbb{N}$ and all $x_1, \dots, x_n \in X$, $\alpha_n((x_1,0) \otimes \dots \otimes (x_n,0)) = \beta_n((x_1,0) \otimes \dots \otimes (x_n,0))$. For all $r_1, \dots, r_n \geq 0$ such that $r_1 + \dots + r_n \leq 1$, $\alpha\nabla(r_1 x_1 + \dots + r_n x_n)$ is the sum of an n-variate power series in $r_1, \dots, r_n$ in which the coefficient of the monomial $r_1 \dots r_n$ is equal to $n!\, \alpha_n((x_1,0) \otimes \dots \otimes (x_n,0))$. The same can be said about β, and two n-variate power series that coincide on a subset of $\mathbb{R}^n$ with non-empty interior have the same coefficients, therefore $\alpha_n((x_1,0) \otimes \dots \otimes (x_n,0)) = \beta_n((x_1,0) \otimes \dots \otimes (x_n,0))$. ☐

This allows us to define a structure of convex QBS on the set of analytic maps from X to Y, by simply transporting the structure of $!X \multimap Y$.

Definition 47. Let X, Y be convex QBSs. We define a convex QBS $X \Rightarrow Y$ as follows:

- the underlying set of the QBS $|X \Rightarrow Y|$ is the set of all analytic maps from X to Y,
- $M_{|X\Rightarrow Y|} = \{r \mapsto f_r \circ \nabla_X ;\ (r \mapsto f_r) \in M_{|!X\multimap Y|}\}$,
- $\big|(X \Rightarrow Y)^\perp\big| = \big|(!X \multimap Y)^\perp\big|$,
- $\eta \cdot_{X\Rightarrow Y} f = \eta \cdot_{!X\multimap Y} f_!$,

Since $\mathrm{der}_X \circ \nabla_X = \mathrm{id}_X$, for all $f : X \multimap Y$, f is analytic and $f_! = f \circ \mathrm{der}_X$.

As a consequence of Fact 44, it is easy to prove that $\mathrm{dig}_X \circ \nabla_X = \nabla_{!X} \circ \nabla_X$, and that for all $f : X \Rightarrow Y$, $!f_! \circ \nabla_{!X} = \nabla_Y \circ f_!$. As a result:

Proposition 48. *Let X, Y, Z be convex QBSs. For all analytic maps $f : X \Rightarrow Y$ and $g : Y \Rightarrow Z$, $g \circ f$ is analytic, and $(g \circ f)_! = (g_! \ll f_!)$.*

This means that convex QBSs and analytic maps form a category that is equivalent to the Kleisli category of "!". In particular, it is cartesian closed, with & as a cartesian product and $\Rightarrow$ as an internal hom functor.

There is one last point to check in order to ensure that analytic functions are well-behaved:

Proposition 49. *Let X, Y be convex QBSs. The map $! : |X \multimap Y| \to |!X \multimap !Y|$ is analytic.*

Proof. For all $n \in \mathbb{N}$, we define $\varphi_n : ((X \multimap Y) \,\&\, \mathbb{W})^{\otimes n} \multimap (X \,\&\, \mathbb{W})^{\otimes n} \multimap (Y \,\&\, \mathbb{W})^{\otimes n}$ by $\varphi_n((f_1, r_1) \otimes \ldots \otimes (f_n, r_n))((x_1, s_1) \otimes \ldots \otimes (x_n, s_n)) = (f_1(x_1), r_1 s_1) \otimes \ldots \otimes (f_n(x_n), r_n s_n)$.

Then for all $f : X \multimap Y$ and all $(a_n)_{n\in\mathbb{N}} \in !X$, $(!f)((a_n)_{n\in\mathbb{N}}) = ((f \,\&\, \mathrm{id}_{\mathbb{W}})^{\otimes n}(a_n))_{n\in\mathbb{N}} = (\varphi_n((f, 1)^{\otimes n})(a_n))_{n\in\mathbb{N}} = (\varphi_n(\pi_n(\nabla(f)))(a_n))_{n\in\mathbb{N}}$. ☐

Finally, the connection with power series is given by the following result:

Fact 50. *Let X, Y be convex QBSs. For all $f : X \Rightarrow Y$, there exists a unique family $\left(\frac{\partial_n f}{\rho_n} : (X)^n_s \multimap Y\right)_{n\in\mathbb{N}}$ such that for all $x \in X$, $f(x) = \sum_{n\in\mathbb{N}} \rho_n \frac{\partial_n f}{\rho_n}(x, \ldots, x)$.*

Proof. One can check that both points hold if and only if $\frac{\partial_n f}{\rho_n} = \rho_n\, f_! \circ \theta_n \circ \mathcal{N}_{n,n} \circ \mathcal{S}_n$ for all n. ☐

Corollary 51. *Let A be a QBS and Y a convex QBS. For all $f, g : \underline{A} \Rightarrow Y$, if f and g coincide on finitely-supported measures, then $f = g$.*

Proof. Similar to Theorem 46. ☐

As in probabilistic coherence spaces, there are non-effective analytic maps: take for example $X = \mathbb{W} \oplus \mathbb{W}$, $Y = \mathbb{W}$, and $f = (p_0, p_1) \mapsto 4p_0p_1$. Let $g : (X \,\&\, \mathbb{W})^2 \multimap \mathbb{W}$ be defined by $g((p_0, p_1, p_*), (q_0, q_1, q_*)) = p_0q_1 + q_0p_1$. One can check that for all $n \geq 1$, $\left\|g \circ \mathcal{J}_{2n,2}\right\| \leq \frac{n}{2n-1}$, so $\|g \circ \pi_2\| \leq \frac{1}{2}$ (with $\pi_2 : !X \multimap (X \,\&\, \mathbb{W})^{\otimes_s 2}$). As a result, $f = 2g \circ \pi_2 \circ \nabla_X \in X \Rightarrow Y$, yet it is clear that f is not effective as a map from $S(\{0, 1\})$ to $S(\{0\})$.

IX. Least fixed points

We prove that all analytic maps from a convex QBS to itself have a least fixed point, so this denotational model can interpret recursive programs.

Theorem 52. *Let X be a convex QBS. For all analytic maps $f \in X \Rightarrow X$,*

- *f has a least fixed point $\mathrm{fix}(f) \in X$,*
- *$\mathrm{fix}(f) = \sup_{n\in\mathbb{N}} f^n(0)$.*

Moreover, the map $f \mapsto \mathrm{fix}(f)$ is analytic (that is to say, it is in $(X \Rightarrow X) \Rightarrow X$).

Proof. To get lighter notations, we will omit the "$\circ$" when composing linear maps (as is traditional in linear algebra).

The idea behind the proof is to express $\sup_{n\in\mathbb{N}} f^n(0)$ as a countable sum. First, we define a linear map

$$\varphi : \begin{cases} !X & \multimap & !X \\ (a_n)_{n\in\mathbb{N}} & \mapsto & \left(\sum_{k>0}^{k\leq n} \mathcal{D}_{n,k} a_n\right)_{n\in\mathbb{N}} \end{cases},$$

so that for all $a \in !X$, $a = \varphi(a) + \pi_0(a)\nabla(0)$. To make the following reasoning clearer, we will write $a - \pi_0(a)\nabla(0)$ for $\varphi(a)$.

For all $g \in X \Rightarrow X$, since $\pi_0\left(!g_!\ \mathrm{dig}\left(\nabla(0)\right)\right) = \pi_0\left(\nabla(g(0))\right) = 1$, we write $!g_!\ \mathrm{dig}\left(\nabla(0)\right) - \nabla(0)$ for $\varphi\left(!g_!\ \mathrm{dig}\left(\nabla(0)\right)\right)$.

For all $n > 0$, we define an analytic map $\beta_n : (X \Rightarrow X) \Rightarrow X$ as

$$g \mapsto \mathrm{der}\,(!g_!\ \mathrm{dig})^{n-1}\left(!g_!\ \mathrm{dig}\left(\nabla(0)\right) - \nabla(0)\right),$$

so that for all $n \in \mathbb{N}$ and all $g \in X \Rightarrow X$, $g^n(0) = \sum_{k=1}^n \beta_k(g)$.

For all $\eta \in X^\perp$ and all $n \in \mathbb{N}$, $\sum_{k=1}^n \eta\beta_k\,(f) = \eta f^n(0) \leq 1$, so $\sum_{k\geq 1} \beta_k(f) \in X$ is well-defined: we denote it by $\mathrm{fix}(f)$.

One can check that for all $(x_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$ and all $\xi \in (!X)^\perp$, $\xi\,\nabla\left(\sum_{n\in\mathbb{N}} x_n\right) = \sup_{n\in\mathbb{N}} \xi\,\nabla\left(\sum_{k\leq n} x_k\right)$. Therefore, for all $\eta \in X^\perp$,

$$\begin{aligned}
& \eta f(\mathrm{fix}(f)) = (\eta f_!)\left(\nabla\left(\mathrm{fix}(f)\right)\right) \\
= \;& (\eta f_!)\left(\nabla\left(\textstyle\sum_{n\geq 1} \beta_n(f)\right)\right) \\
= \;& \sup_{n\in\mathbb{N}} (\eta f_!)\left(\nabla\left(\textstyle\sum_{k\geq 1}^{k\leq n} \beta_k(f)\right)\right) \\
= \;& \sup_{n\in\mathbb{N}} (\eta f_!)\left(\nabla\left(f^n(0)\right)\right) \\
= \;& \sup_{n\in\mathbb{N}} \eta f^{n+1}(0) = \textstyle\sum_{n\geq 1} \eta\beta_n(f) \\
= \;& \eta\left(\mathrm{fix}(f)\right),
\end{aligned}$$

so $f\left(\mathrm{fix}(f)\right) = \mathrm{fix}(f)$. Moreover, $\mathrm{fix} \in (X \Rightarrow X) \Rightarrow X$, with $\mathrm{fix}_! = \sum_{n\geq 1} \beta_{n!}$. ☐

X. A toy probabilistic language

As an example, we briefly describe a language for which the category of convex QBSs and analytic maps provides an extensional denotational semantics. It can be described as call-by-name PCF with a type for real numbers, primitives for randomly generated reals, a construction to force call-by-value evaluation on data types, and a conditional branching instruction. The types of this language are defined by:

$$A, B := \mathbb{R} \mid A \times B \mid A + B \mid A \to B.$$

We call types written without "$\to$" *data types*. Terms are defined by:

$$\begin{aligned}
t, u, v := \;& x \mid \lambda x.\, t \mid tu \mid \mathrm{fix}\, x.\, t \mid (t, u) \mid Lt \mid Ru \\
\mid\; & \text{match } t \text{ with } (x, y) \mapsto u \\
\mid\; & \text{match } t \text{ with } Lx \mapsto u\,; Ry \mapsto v \\
\mid\; & f(t_1, \ldots, t_n) \quad (f \in \mathrm{Qbs}(\mathbb{R}^n, S(\mathbb{R}))) \\
\mid\; & \text{if } t \text{ then } u \text{ else } v \\
\mid\; & \text{eval } t \text{ as } x \text{ in } u,
\end{aligned}$$

where eval is used on data types to force evaluation, and if tests whether a real number is non-zero. The only typing rule that requires attention is that of eval. The rule is: for all data types D,

$$\frac{\Gamma \vdash t : D \qquad \Gamma, x : D \vdash u : A}{\Gamma \vdash \mathrm{eval}\, t \,\mathrm{as}\, x \,\mathrm{in}\; u : A}.$$

To each type A, we associate a convex QBS $[\![A]\!]$, following Girard's call-by-name translation [9]:

$$[\![\mathbb{R}]\!] = \underline{\mathbb{R}} \qquad [\![A \times B]\!] = [\![A]\!] \,\&\, [\![B]\!]$$
$$[\![A \to B]\!] = [\![A]\!] \Rightarrow [\![B]\!] \quad [\![A + B]\!] = ![\![A]\!] \oplus ![\![B]\!].$$

We interpret each valid typing judgement $x_1 : A_1, \ldots, x_n : A_n \vdash t : B$ by an analytic map $[\![t]\!] : [\![A_1]\!] \,\&\, \ldots \,\&\, [\![A_n]\!] \Rightarrow [\![B]\!]$. As with types, we follow Girard's translation, and the only construction that requires attention is eval. Intuitively, the program "$\mathrm{eval}\;\; t \;\; \mathrm{as} \;\; x \;\; \mathrm{in} \;\; u$" samples t exactly once and then copies the resulting data as many times as needed by u. In order to interpret it, we define for all data types D a linear map $\mathrm{copyData}_D : [\![D]\!] \multimap ![\![D]\!]$ that represents this copying operation. Namely, we let $\mathrm{copyData}_{\mathbb{R}} = \mathrm{copy}_{\mathbb{R}} : \underline{\mathbb{R}} \multimap !\underline{\mathbb{R}}$; $\mathrm{copyData}_{D_1+D_2} \circ L_j = !L_j \circ \mathrm{dig}_{[\![D_j]\!]} \circ \mathrm{copyData}_{D_j} \circ \mathrm{der}_{[\![D_j]\!]}$ for $j \in \{1, 2\}$; and $\mathrm{copyData}_{D_1 \times D_2} = \mathrm{store}_{[\![D_1]\!],[\![D_2]\!]} \circ ((a, b) \mapsto a \otimes b) \circ (\mathrm{copyData}_{D_1} \,\&\, \mathrm{copyData}_{D_2})$. Then we let

$$[\![\mathrm{eval}\; t \;\mathrm{as}\; x \;\mathrm{in}\; u]\!] = [\![u]\!]_! \circ \mathrm{copyData}_D \circ [\![t]\!]$$

(assuming for simplicity that u has no free variable but x – the general expression is similar but more cumbersome).

Since this is a call-by-name calculus, each member of a pair is sampled independently. If we want a pair whose members are correlated, we need to wrap it inside a constructor. For example, the program "$\mathrm{eval}\; \mathrm{uniform}(\underline{0}, \underline{1}) \;\mathrm{as}\; x \;\mathrm{in}\; L(x, x)$" always produces pairs with identical members: its denotation is $L_1(\int_0^1 \nabla(\underline{x}, \underline{x})\lambda(\mathrm{d}x))$, where λ denotes the uniform measure.

We could just as well have chosen to interpret a call-by-value calculus, using Girard's call-by-value translation. In fact, the whole discussion so far suggests that probabilistic languages might benefit from linear typing, which makes it possible to mix features from both styles: this is what convex QBSs would be best-suited to interpret.

XI. Conclusion

We described a model of probabilistic programming (in the narrow sense) that is not limited to discrete probabilities, is compatible with integration, interprets all the connectives of linear logic, and in which all functions have a least fixed point.

A clear direction for future research is to investigate convex QBSs themselves. For example, if we equip the language from Section X with an operational semantics, do we have full abstraction? Do initial algebras exist for functors written in terms of all or some of the connectives of linear logic? (In other words, do we have inductive types?) What about final co-algebras? In addition, it would be interesting to know how this model relates with probabilistic coherence spaces: do they coincide on countable types? One should also investigate how to get rid of non-effective maps between data types, perhaps by looking for a different (non-free) exponential modality. An other direction would be to extend convex QBSs to a model of probabilistic programming in the broad sense [15], [16], that is to say, one capable of describing statistical models rather than just programs that make random choices. Staton's work [15] suggests that the first step would be to require stability under integration for all s-finite measures (*i.e.* drop the bound on the result) and move the (non-measurable) norm to the structure – going from convex to "linear" QBSs, so to speak. On a different line, replacing $[0, 1]$-valued linear tests with tests valued in the unit disc of $\mathbb{C}$ might be a starting point for a model of quantum computation (though this would require leaving the comfort of absolute convergence). Similarly, using tests whose values are intervals included in $[0, 1]$, in the spirit of differential program semantics [22], could yield higher-order versions of such concepts as local differential privacy [23], [24].

References

[1] N. Saheb-Djahromi, "Cpo's of measures for nondeterminism," *Theoretical Computer Science*, vol. 12, no. 1, pp. 19 – 37, 1980.

[2] D. Kozen, "Semantics of probabilistic programs," *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 328 – 350, 1981.

[3] A. Jung and R. Tix, "The troublesome probabilistic powerdomain," *Electronic Notes in Theoretical Computer Science*, vol. 13, pp. 70 – 91, 1998, comprox III, Third Workshop on Computation and Approximation.

[4] V. Danos and R. S. Harmer, "Probabilistic game semantics," *ACM Trans. Comput. Logic*, vol. 3, no. 3, p. 359–382, Jul. 2002.

[5] U. Dal Lago and N. Hoshino, "The geometry of bayesian programming," in *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2019, pp. 1–13.

[6] O. Kallenberg, *Random Measures, Theory and Applications*. Springer International Publishing, 01 2017, vol. 77.

[7] P. Panangaden, "The category of markov kernels," *Electronic Notes in Theoretical Computer Science*, vol. 22, pp. 171 – 187, 1999, pROBMIV'98, First International Workshop on Probabilistic Methods in Verification.

[8] V. Danos and T. Ehrhard, "Probabilistic coherence spaces as a model of higher-order probabilistic computation," *Information and Computation*, vol. 209, no. 6, pp. 966 – 991, 2011.

[9] J.-Y. Girard, "Linear logic," *Theoretical Computer Science*, vol. 50, no. 1, pp. 1 – 101, 1987.

[10] T. Ehrhard, M. Pagani, and C. Tasson, "Measurable cones and stable, measurable functions: A model for probabilistic higher-order programming," *Proc. ACM Program. Lang.*, vol. 2, no. POPL, Dec. 2017.

[11] M. Vákár, O. Kammar, and S. Staton, "A domain theory for statistical probabilistic programming," 2018.

[12] S. Slavnov, "Linear logic in normed cones: probabilistic coherence spaces and beyond," 2019.

[13] F. Dahlqvist and D. Kozen, "Semantics of higher-order probabilistic programs with conditioning," *Proc. ACM Program. Lang.*, vol. 4, no. POPL, Dec. 2019.

[14] C. Heunen, O. Kammar, S. Staton, and H. Yang, "A convenient category for higher-order probability theory," in *Proceedings of the 32nd Annual ACM/IEEE Symposium on Logic in Computer Science*, ser. LICS '17. IEEE Press, 2017.

[15] S. Staton, "Commutative semantics for probabilistic programming," in *Programming Languages and Systems*. Springer Berlin Heidelberg, 2017, pp. 855–879.

[16] N. L. Ackerman, C. E. Freer, and D. M. Roy, "On the computability of conditional probability," *Journal of the ACM*, vol. 66, no. 3, p. 1–40, Jun 2019. [Online]. Available: http://dx.doi.org/10.1145/3321699

[17] T. Leinster, "Higher operads, higher categories," *arXiv preprint math/0305049*, 2003.

[18] M. Giry, "A categorical approach to probability theory," in *Categorical Aspects of Topology and Analysis*. Springer Berlin Heidelberg, 1982, pp. 68–85.

[19] J. Girard, *The Blind Spot: Lectures on Logic*. European Mathematical Society, 2011.

[20] P.-A. Melliès, N. Tabareau, and C. Tasson, "An explicit formula for the free exponential modality of linear logic," in *36th International Colloquium on Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, vol. 5556/2009. Springer, Jul. 2009, pp. 247–260.

[21] Y. Lafont, "The linear abstract machine," *Theoretical Computer Science*, vol. 59, no. 1, pp. 157 – 180, 1988.

[22] U. D. Lago, F. Gavazzo, and A. Yoshimizu, "Differential Logical Relations, Part I: The Simply-Typed Case," in *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), 2019.

[23] A. Evfimievski, J. Gehrke, and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," in *Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, ser. PODS '03. Association for Computing Machinery, 2003, p. 211–222.

[24] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" in *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008, pp. 531–540.