A Denotational Semantics for Low-Level Probabilistic Programs with Nondeterminism

Di Wang[1], Jan Hoffmann[1], and Thomas Reps[2,3]

[1]Carnegie Mellon University
[2]University of Wisconsin
[3]GrammaTech, Inc.

Abstract

Probabilistic programming is an increasingly popular formalism for modeling randomness and uncertainty. Designing semantic models for probabilistic programs has been extensively studied, but is technically challenging. Particular complications arise when trying to account for (i) unstructured control-flow, a natural feature in low-level imperative programs; (ii) general recursion, an extensively used programming paradigm; and (iii) nondeterminism, which is often used to represent adversarial actions in probabilistic models, and to support refinement-based development. This paper presents a denotational-semantics framework that supports the three features mentioned above, while allowing nondeterminism to be handled in different ways. To support both probabilistic choice and nondeterministic choice, the semantics is given over control-flow *hyper*-graphs. The semantics follows an *algebraic* approach: it can be instantiated in different ways as long as certain algebraic properties hold. In particular, the semantics can be instantiated to support nondeterminism among either *program states* or *state transformers*. We develop a new formalization of nondeterminism based on *powerdomains* over *sub-probability kernels*. Semantic objects in the powerdomain enjoy a notion we call *generalized convexity*, which is a generalization of convexity. As an application, the paper sketches an algebraic framework for static analysis of probabilistic programs, which has been proposed in a companion paper.

Keywords— Probabilistic programming, denotational semantics, control-flow hyper-graphs, nondeterminism, powerdomains

1 Introduction

Probabilistic programming provides a powerful framework for implementing randomized algorithms [Barthe et al. 2016], cryptographic protocols [Barthe et al. 2009], cognitive models [Gordon et al. 2014], and machine-learning algorithms [Ghahramani 2015]. One important focus of recent studies on probabilistic programming is to reason *rigorously* about probabilistic programs and systems. The first step in such works is to provide a suitable formal semantics for probabilistic programs.

Despite the fact that lots of existing work focuses on *high*-level probabilistic programs, e.g., lambda calculus [Borgström et al. 2016], higher-order functions [Ehrhard et al. 2018; Heunen et al. 2017], and recursive types [Vákár et al. 2019], we observe that *low*-level features could arise naturally. For

example, when developing a compiler for a probabilistic programming language [Franke et al. 2005; Paige and Wood 2014], we need a semantics for the imperative target language to prove compiler correctness. There have been studies on *denotational* semantics for *well-structured* imperative programs [Bichsel et al. 2018; Jansen et al. 2015; Kaminski et al. 2016; Kozen 1981b, 1985; McIver and Morgan 2001, 2005; Olmedo et al. 2016; Tix et al. 2009], as well as *operational* semantics for *control-flow graphs* (CFGs) based on Markov chains (MCs) and Markov decision processes (MDPs) ([Chatterjee et al. 2016b, 2017; Ferrer Fioriti and Hermanns 2015]). On the one hand, we prefer CFGs as program representations because they enable rich low-level features such as *unstructured* flows, e.g., those introduced by **break** and **continue**. On the other hand, from the perspective of rigorous reasoning, a denotational semantics (i) abstracts from details about program executions and focuses on program *effects*, and (ii) is *compositional* in the sense that the semantics of a program fragment is established from the semantics of the fragment's proper constituents.

Therefore, in this paper, we devise a denotational semantics for low-level probabilistic programs. Our work makes three main contributions:

- We use *hyper-graphs* as the representation for low-level probabilistic programs with unstructured control-flow, general recursion, and nondeterminism.
- We develop a domain-theoretic characterization of a new model of nondeterminism for probabilistic programming, which involves nondeterminacy among *state transformers*, opposed to a common model that involves nondeterminacy among *program states*.
- We devise an *algebraic* framework for denotational semantics. The advantage of having a framework is that it can be instantiated with different models of nondeterminism. We show how to instantiate the framework using two different approaches to formalizing nondeterminism in Ex. 5.2. We also show that for programs without procedure calls and nondeterminism, the resulting denotational semantics is equivalent to a distribution-based operational semantics (§5.2).

We define the denotational semantics *directly* as an interpretation of the *control-flow hyper-graphs* (CFHGs) of low-level probabilistic programs, introduced in §2. Hyper-graphs consist of *hyper-edges*, each of which connects one source node and possibly several destination nodes. For example, probabilistic choices are represented by weighted hyper-edges with *two* destinations. Nondeterminism is then represented by multiple hyper-edges starting in the same node. The interpretation of hyper-edges is also different from standard edges. If the CFHG were treated as a standard graph, the subpaths from each successor of a branching node would be analyzed *independently*. In contrast, our hyper-graph approach interprets a probabilistic-choice hyper-edge with probability p as a function $\lambda a.\lambda b.a\ {}_p\!\oplus\ b$, where ${}_p\!\oplus$ is an operation that weights the subpaths through the two successors by p and $1-p$. In other words, we do not reason about subpaths starting from a node *individually*, instead we analyze these subpaths *jointly* as a probability distribution. If a node has two outgoing probabilistic-choice hyper-edges, it represents two "worlds" of subpaths, each of which carries a probability distribution with respect to the probabilistic choice made in this "world."

Some high-level decision choices about *nondeterminism* arise when we are developing the low-level semantics. Nondeterminism itself is an important feature from two perspectives: (i) it arises naturally from probabilistic models, such as the agent for an MDP [Bellman 1957], or the unknown input distribution for modeling *fault tolerance* [Kattenbelt et al. 2009], and (ii) it is required by the common paradigm of *abstraction* and *refinement*[1] on programs [Dijkstra 1997; McIver and Morgan 2005]. While nondeterminism has been well studied for standard programming languages, the combination of probabilities and nondeterminism turns out to be tricky. One substantial question is *when* the nondeterminism is resolved. A well-studied model for nondeterminism in probabilistic programming is to resolve program inputs *prior to* nondeterminism [den Hartog and de Vink 1999;

[1] Abstraction enables reasoning about a program through its high-level specifications, and refinement allows stepwise software development, where programs are "refined" from specifications to low-level implementations.

$$\begin{array}{lll} \textbf{if} \star & \textbf{then} & \textbf{if prob}(1/2)\ \textbf{then}\ t := 0\ \textbf{else}\ t := 1\ \textbf{fi} \\ & \textbf{else} & \textbf{if prob}(1/3)\ \textbf{then}\ t := 0\ \textbf{else}\ t := 1\ \textbf{fi} \quad \textbf{fi} \end{array}$$

Fig. 1: A nondeterministic, probabilistic program

McIver and Morgan 2001, 2005; Mislove 2000; Mislove et al. 2004; Tix et al. 2009]. This model follows a commonplace principle of semantics research that represents a nondeterministic function as a set-valued function that maps an input to a collection of possible outputs, i.e., an element in $X \to \wp(X)$, where X is a program state space and $\wp(\cdot)$ is the powerset operator. However, it is sometimes desirable to resolve nondeterminism *prior to* program inputs, i.e., a nondeterministic program should represent a collection of elements in $\wp(X \to X)$. For example, one may want to show for every refined version of a nondeterministic program with each nondeterministic choice replaced by a conditional, its behavior on all *inputs* are indistinguishable. We call the common model *nondeterminism-last* and the other *nondeterminism-first*. In §4, we present a domain-theoretic study of nondeterminism-first. Technically, we propose a notion of *generalized convexity* (*g-convexity*, for short), which expresses that a set of *state transformers* is stable under refinements (while standard convexity describes that a set of *states* is stable under refinements), as well as devise a g-convex *powerdomain* that characterizes expressible semantic objects.

To achieve our ultimate goal of developing a denotational semantics, instead of restricting ourselves to one specific model for nondeterminism, we propose a general *algebraic* denotational semantics in §5, which can be instantiated with different treatments of nondeterminism. The semantics is algebraic in the sense that it performs reasoning in some space of program states and state transformers, while the transformers should obey some algebraic laws. For instance, the program command **skip** should be interpreted as the *identity* element for sequencing in an algebra of program-state transformers. In addition, the algebraic approach is a good fit for static analysis of probabilistic programs. In §6, we sketch a static-analysis framework proposed in a companion paper [Wang et al. 2018], as an application of the denotational semantics.

The *algebraic* approach we take in this paper is challenging in the setting of probabilistic programming. In contrast, for standard, non-probabilistic programming languages, it is almost trivial to derive a low-level denotational semantics *once* one has a semantics for well-structured programs at hand. The trick is to first define the semantic operations as a *Kleene algebra* [Conway 1971; Kleene 1951; Kozen 1981a, 1991], which admits an *extend* operation, used for sequencing, a *combine* operation, used for branching, and a *closure* operation, used for looping; then extract from the CFG a *regular expression* that captures all execution paths by Tarjan's path-expression algorithm [Tarjan 1981]; and finally use the Kleene algebra to *reinterpret* the regular expression to obtain the semantics for the CFG. However, this approach fails when both probabilities and nondeterminism come into the picture. Consider the probabilistic program with a *nondeterministic* choice $\star$ in Fig. 1. The program is intended to draw a random value t from either a fair coin flip or a biased one. If one adopts the path-expression approach, one ends up with a regular expression that describes a *single* collection of four program executions: (i) $t := 0$ with probability $1/2$, (ii) $t := 1$ with probability $1/2$, (iii) $t := 0$ with probability $1/3$, and (iv) $t := 1$ with probability $2/3$. The collection does *not* describe the intended meaning, and does *not* even form a well-defined probability distribution—all the probabilities sum up to 2 instead of 1. Intuitively, the path-expression approach fails for probabilistic programs because it can only express the semantics as a collection of executions with probabilities, whereas probabilistic programs actually specify collections of *distributions* over executions.

Although the denotational semantics proposed in this paper supports interesting features including unstructured control-flow, general recursion, and nondeterminism, there are some other important features that the semantics does not support *yet*, such as continuous distributions and higher-order functions. We discuss those missing features in §7, and leave them for future work.

2 An Operational Semantics for Low-Level Probabilistic Programs

In this section, we sketch an operational semantics for an imperative, single-procedure, deterministic,[2] probabilistic programming language, following the approach of Borgström et al.'s distribution-based semantics [Borgström et al. 2016]. We use the operational semantics to (i) illustrate how to model executions of probabilistic programs operationally, and (ii) justify the development of a denotational semantics in later sections.

2.1 A Hyper-Graph Program Model

We define the operational semantics on CFHGs of programs. We adopt a common approach for standard CFGs in which the nodes represent program locations, and edges labeled with instructions describe transitions among program locations (e.g., [Farzan and Kincaid 2015; Lal et al. 2008; Müller-Olm and Seidl 2004]). Instead of standard directed graphs, we make use of *hyper-graphs* [Gallo et al. 1993].

Definition 2.1. A *hyper-graph* H is a quadruple $\langle V, E, v^{\mathsf{entry}}, v^{\mathsf{exit}}\rangle$, where V is a finite set of nodes, E is a set of hyper-edges, $v^{\mathsf{entry}} \in V$ is a distinguished *entry node*, and $v^{\mathsf{exit}} \in V$ is a distinguished *exit node*. A *hyper-edge* is an ordered pair $\langle x, Y\rangle$, where $x \in V$ is a node and $Y \subseteq V$ is an ordered, non-empty set of nodes. For a hyper-edge $e = \langle x, Y\rangle$ in E, we use $src(e)$ to denote x and $Dst(e)$ to denote Y. Following the terminology from graphs, we say that e is an *outgoing edge* of x and an *incoming edge* of each of the nodes $y \in Y$. We assume v^{entry} does not have incoming edges, and v^{exit} has no outgoing edges.

Definition 2.2. A *probabilistic program* contains a finite set of procedures $\{H_i\}_{1\le i\le n}$, where each procedure $H_i = \langle V_i, E_i, v_i^{\mathsf{entry}}, v_i^{\mathsf{exit}}\rangle$ is a *control-flow hyper-graph* (CFHG) in which each node except v_i^{exit} has *at least* one outgoing hyper-edge, and v_i^{exit} has no outgoing hyper-edge. Define $V \stackrel{\text{def}}{=} \bigcup_{1\le i\le n} V_i$. To assign meanings to probabilistic programs modulo *data actions* Act and *deterministic conditions* Cond that *can* be probabilistic, we associate with each hyper-edge $e \in E = \bigcup_{1\le i\le n} E_i$ a *control-flow action* $Ctrl(e)$ that has one of the following three forms:

$$\mathsf{Ctrl} \;::=\; \mathit{seq}[\mathsf{act}],\ \text{where } \mathsf{act} \in \mathsf{Act} \;\mid\; \mathit{cond}[\varphi],\ \text{where } \varphi \in \mathsf{Cond} \;\mid\; \mathit{call}[i \to j],\ \text{where } 1 \le i, j \le n$$

where the number of destination nodes $|Dst(e)|$ of a hyper-edge e is 1 if $Ctrl(e)$ is $\mathit{seq}[\mathsf{act}]$ or $\mathit{call}[i \to j]$, and 2 otherwise.

Example 2.3. Fig. 2(b) shows the CFHG of the program in Fig. 2(a), where v_0 is the entry and v_4 is the exit. The hyper-edge $\langle v_2, \{v_3\}\rangle$ is associated with a sequencing action $seq[n := n+1]$, while $\langle v_1, \{v_2, v_4\}\rangle$ is assigned a deterministic-choice action $cond[\mathbf{prob}(0.5) \wedge \mathbf{prob}(0.5)]$, i.e., an event where two coin flips both show heads.

Note that **break**, **continue** (and also **goto**) are not data actions, and are encoded directly as edges in CFHGs in a standard way. The grammar below defines data actions Act and deterministic conditions Cond that could be used for an arithmetic program, where $p \in [0,1]$, $c \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, and $n \in \mathbb{N}$.

$$\mathsf{Act} ::= x := e \mid x \sim D \mid \mathbf{observe}(\varphi) \mid \mathbf{skip} \qquad \varphi \in \mathsf{Cond} ::= \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid e_1 \le e_2 \mid \mathbf{prob}(p)$$

$$e \in \mathsf{Exp} ::= x \mid c \mid e_1 + e_2 \mid e_1 \times e_2 \qquad D \in \mathsf{Dist} ::= \mathsf{Binomial}(n,p) \mid \mathsf{Uniform}(a,b) \mid \mathsf{Geometric}(p) \mid \cdots$$

Dist stands for a collection of discrete probability distributions. For example, $\mathsf{Binomial}(n,p)$ with $n \in \mathbb{N}$ and $p \in [0,1]$ describes the distribution of the number of successes in n independent experiments, each of which succeeds with probability p; $\mathsf{Uniform}(a,b)$ represents a discrete uniform distribution on $[a,b] \cap \mathbb{Z}$.

[2] The term "deterministic" is used in the sense "not nondeterministic."

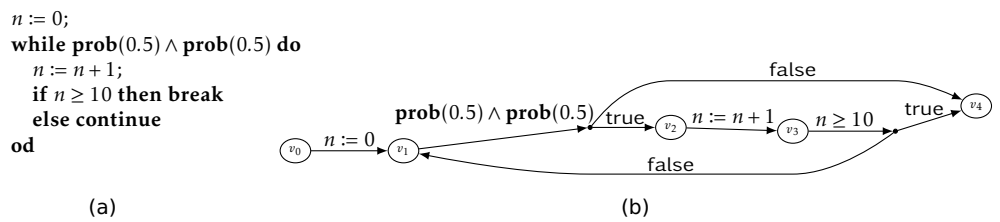

Fig. 2: (a) An example of probabilistic programs; (b) The corresponding CFHG

2.2 A Distribution-Based Small-Step Operational Semantics

The next step is to define a semantics based on CFHGs. We adopt Borgström et al.'s distribution-based small-step operational semantics for lambda calculus [Borgström et al. 2016] to our hyper-graph setting, while we suppress the features of multiple procedures and nondeterminism for now.

Three components are used to define the semantics:

- A *program state space* Ω, e.g., for arithmetic programs, we can define $\Omega \stackrel{\text{def}}{=} \mathsf{Var} \rightharpoonup_{\text{fin}} \mathbb{Q}$, i.e., a set of finite partial maps from program variables to their values.
- A function $[\![\text{act}]\!]$ from program states to *(sub-probability) distributions* over program states for each data action act. A distribution is a function $\Delta : \Omega \to [0,1]$ such that $\sum_{\omega\in\Omega} \Delta(\omega) \le 1$. Intuitively, $[\![\text{act}]\!](\omega)(\omega')$ is the probability that the action act, starting in state $\omega \in \Omega$, halts in a state $\omega' \in \Omega$ [Kozen 1985].
- A $[0,1]$-valued function $[\![\varphi]\!]$ from program states for each deterministic condition φ. Intuitively, $[\![\varphi]\!](\omega)$ is the probability that the condition φ holds in state $\omega \in \Omega$.

The *point distribution* $\delta(\omega)$ is defined as $\lambda\omega'.[\omega = \omega']$ where $[\psi]$ is an *Iverson bracket* that evaluates to 1 if ψ is true and 0 otherwise. If Δ is a distribution and $r \in [0,1]$, we write $r \cdot \Delta$ for the distribution $\lambda\omega.r \cdot \Delta(\omega)$. If Δ_1, Δ_2 are distributions and $r_1, r_2 \in [0,1]$ satisfy $r_1 + r_2 \le 1$, we write $r_1 \cdot \Delta_1 + r_2 \cdot \Delta_2$ for the distribution $\lambda\omega.r_1 \cdot \Delta_1(\omega) + r_2 \cdot \Delta(\omega)$.

Fig. 3 shows interpretation of the data actions and deterministic conditions given in §2.1, where $\omega(e)$ evaluates expression e in state ω, $[x \mapsto v]\omega$ updates x in ω with v, and $\Delta_D : \mathbb{Q} \to [0,1]$ is the *probability mass function* of the distribution D. If φ does not contain any probabilistic choices $\mathbf{prob}(p)$, then $[\![\varphi]\!](\omega)$ is either 0 or 1. Intuitively, $[\![\varphi]\!](\omega)$ is the probability that φ is true in the state ω, w.r.t. a probability space specified by all the $\mathbf{prob}(p)$'s in φ. Then the probability of $\varphi_1 \wedge \varphi_2$ is defined as the product of the individual probabilities of φ_1 and φ_2, because φ_1 and φ_2 are interpreted w.r.t. probabilistic choices in φ_1 and φ_2, respectively, and these two sets of choices are disjoint, thus independent.

$[\![x := e]\!] \stackrel{\text{def}}{=} \lambda\omega.\delta([x \mapsto \omega(e)]\omega)$ $\quad$ $[\![\mathbf{skip}]\!] \stackrel{\text{def}}{=} \lambda\omega.\delta(\omega)$	$[\![\top]\!] \stackrel{\text{def}}{=} \lambda\omega.1$ $\quad$ $[\![\neg\varphi]\!] \stackrel{\text{def}}{=} \lambda\omega.1 - [\![\varphi]\!](\omega)$
$[\![x \sim D]\!] \stackrel{\text{def}}{=} \lambda\omega.\sum_{v\in\text{supp}(\Delta_D)} \Delta_D(v) \cdot \delta([x \mapsto v]\omega)$	$[\![\mathbf{prob}(p)]\!] \stackrel{\text{def}}{=} \lambda\omega.p$ $\quad$ $[\![e_1 \le e_2]\!] \stackrel{\text{def}}{=} \lambda\omega.[\omega(e_1) \le \omega(e_2)]$
$[\![\mathbf{observe}(\varphi)]\!] \stackrel{\text{def}}{=} \lambda\omega.[\![\varphi]\!](\omega) \cdot \delta(\omega)$	$[\![\varphi_1 \wedge \varphi_2]\!] \stackrel{\text{def}}{=} \lambda\omega.[\![\varphi_1]\!](\omega) \cdot [\![\varphi_2]\!](\omega)$

Fig. 3: Interpretation of data actions and deterministic conditions

Suppose that $P = \langle V, E, v^{\text{entry}}, v^{\text{exit}} \rangle$ is a single-procedure deterministic program. Therefore, each node in P except v^{exit} is associated with *exactly* one hyper-edge. The *program configurations* $T = V \times \Omega$ are pairs of the form $\langle v, \omega \rangle$, where $v \in V$ is a node in the CFHG, and $\omega \in \Omega$ is a program state.

We define *one-step evaluation* as a relation $\langle v, \omega \rangle \longrightarrow \Delta$ between configurations $\langle v, \omega \rangle$ and distributions Δ on configurations, as shown in Fig. 4.

$$\langle v, \omega\rangle \longrightarrow \lambda\langle v', \omega'\rangle.[v' = u] \cdot [\![\mathsf{act}]\!](\omega)(\omega') \qquad \text{where } e = \langle v, \{u\}\rangle \in E, Ctrl(e) = seq[\mathsf{act}]$$
$$\langle v, \omega\rangle \longrightarrow [\![\varphi]\!](\omega) \cdot \delta(\langle u_1, \omega\rangle) + (1 - [\![\varphi]\!](\omega)) \cdot \delta(\langle u_2, \omega\rangle) \qquad \text{where } e = \langle v, \{u_1, u_2\}\rangle \in E, Ctrl(e) = cond[\varphi]$$

Fig. 4: One-step evaluation relation

Example 2.4. For the program in Fig. 2, some one-step evaluations are $\langle v_0, \{n \mapsto 233\}\rangle \longrightarrow \delta(\langle v_1, \{n \mapsto 0\}\rangle)$, $\langle v_1, \{n \mapsto 1\}\rangle \longrightarrow 0.25 \cdot \delta(\langle v_2, \{n \mapsto 1\}\rangle) + 0.75 \cdot \delta(\langle v_4, \{n \mapsto 1\}\rangle)$, *and* $\langle v_3, n \mapsto 9\rangle \longrightarrow \delta(\langle v_1, \{n \mapsto 9\}\rangle)$.

We now define *step-indexed evaluation* as the family of n-indexed relations $\langle v, \omega\rangle \longrightarrow_n \Delta$ between configurations $\langle v, \omega\rangle$ and distributions Δ on program states inductively, as shown in Fig. 5.

$$\langle v, \omega\rangle \longrightarrow_0 \lambda\omega'.0$$
$$\langle v^{\mathsf{exit}}, \omega\rangle \longrightarrow_n \delta(\omega) \qquad \text{if } n > 0$$
$$\langle v, \omega\rangle \longrightarrow_{n+1} \sum_{\tau \in \mathrm{supp}(\Delta)} \Delta(\tau) \cdot \Delta'_\tau \quad \text{where} \langle v, \omega\rangle \longrightarrow \Delta \text{ and } \tau \longrightarrow_n \Delta'_\tau \text{ for any } \tau \in \mathrm{supp}(\Delta)$$

Fig. 5: Step-indexed evaluation relation

Example 2.5. For the program in Fig. 2, some step-indexed evaluations are $\langle v_4, \{n \mapsto 10\}\rangle \longrightarrow_1 \delta(\{n \mapsto 10\})$, $\langle v_1, \{n \mapsto 0\}\rangle \longrightarrow_2 0.75 \cdot \delta(\{n \mapsto 0\})$, *and* $\langle v_1, \{n \mapsto 0\}\rangle \longrightarrow_5 0.75 \cdot \delta(\{n \mapsto 0\}) + 0.1875 \cdot \delta(\{n \mapsto 1\})$.

For the program $P = \langle V, E, v^{\mathsf{entry}}, v^{\mathsf{exit}}\rangle$, we define its semantics $[\![P]\!]_{\mathsf{os}}(\omega) \stackrel{\text{def}}{=} \sup_{n \in \mathbb{N}} \{\Delta \mid \langle v^{\mathsf{entry}}, \omega\rangle \longrightarrow_n \Delta\}$.

Example 2.6. For the program P in Fig. 2, $[\![P]\!]_{\mathsf{os}}(\omega)$ *for any initial state* ω *with* $n \in \mathrm{dom}(\omega)$ *is given by* $\sum_{k=0}^{9}(0.75 \times 0.25^k) \cdot \delta([n \mapsto k]\omega) + 0.00000095367431640625 \cdot \delta([n \mapsto 10]\omega)$.

2.3 Why is a Denotational Semantics Desirable?

We have already shown how probabilistic programs execute *operationally*. As mentioned in §1, we are instead interested in developing a *denotational* semantics, which concentrates on the *effects* of programs and abstracts from how the program executes. This characterization of denotational semantics is indeed beneficial for *rigorous reasoning* about programs, such as static analysis and model checking, because one usually only cares whether programs satisfy certain properties, e.g., if they terminate on all possible inputs. Even better, a denotational semantics is often *compositional*—that is, the property of a whole program can be established from properties of its proper constituents. In other words, one could develop *local*—and thus *scalable*—reasoning techniques based on a denotational semantics. In contrast, the operational semantics in §2.2 is not compositional—it takes into account the whole program P to define $[\![P]\!]_{\mathsf{os}}$.

Another benefit of a denotational semantics is that it is often easier to extend than an operational one. In the rest of this section, we briefly compare the complexity of adding procedure calls and nondeterminism to an operational semantics versus a denotational semantics. To support multiple procedures and procedure calls in the semantics proposed in §2.2, one needs to introduce a notion of *stacks* to keep track of procedure calls, as in [Etessami and Yannakakis 2005, 2015; Olmedo et al. 2016]. Then the program configurations become triples of call stacks, control-flow-graph nodes,

and program states. As a consequence, the one-step and step-indexed evaluation relations in Figs. 4 and 5 would become more complex. However, such an extension is almost trivial for a denotational semantics. Suppose we are able to *compose* semantic objects, e.g, $[\![C_1;C_2]\!]_{\mathsf{ds}} = [\![C_2]\!]_{\mathsf{ds}} \circ [\![C_1]\!]_{\mathsf{ds}}$, where C_1, C_2 are program fragments, $\circ$ denotes a composition operation, and $[\![C]\!]_{\mathsf{ds}}$ gives the denotation of C. If C_1 is indeed a procedure call **call** Q where Q is a procedure, because we can obtain the denotation $[\![Q]\!]_{\mathsf{ds}}$ of Q, we can interpret $[\![\textbf{call } Q; C_2]\!]_{\mathsf{ds}}$ merely as $[\![C_2]\!]_{\mathsf{ds}} \circ [\![Q]\!]_{\mathsf{ds}}$. By this means we do not need to reason about stacks explicitly.

Another important programming feature is nondeterminism. For operational semantics of probabilistic programs, nondeterminism is often formalized using the notion of a *scheduler*, which resolves a nondeterministic choice from the computation that leads up to it (e.g., [Chatterjee et al. 2016b, 2017; Ferrer Fioriti and Hermanns 2015]). When the scheduler is fixed, a program can be executed deterministically (as shown in §2.2). To reason about nondeterministic programs with respect to an operational semantics, one needs to take all possible schedulers into consideration. However, if one only cares about the effects of a program, it is possible to sidestep these schedulers by switching to a denotational semantics. For example, let C_1, C_2 be two program fragments and $[\![C_1]\!]_{\mathsf{ds}}, [\![C_2]\!]_{\mathsf{ds}}$ be their denotations, which should be maps from initial states to a collection of possible final states. Then the denotation $[\![\textbf{if } \star \textbf{ then } C_1 \textbf{ else } C_2 \textbf{ fi}]\!]_{\mathsf{ds}}$ of a nondeterministic-choice between C_1 and C_2 could be something like $\lambda\omega.[\![C_1]\!]_{\mathsf{ds}}(\omega) \cup [\![C_2]\!]_{\mathsf{ds}}(\omega)$. Note that this approach does not need to consider schedulers explicitly.

3 A Summary of Existing Domain-Theoretic Developments

Our development of models for nondeterminism makes great use of existing domain-theoretic studies of powerdomains, thus in this section, we present a brief summary of them. We review some standard notions from domain theory [Abramsky and Jung 1994; Hofmann and Mislove 1981; Mislove 1998], as well as some results on probabilistic powerdomains [Jones 1989; Jones and Plotkin 1989] and nondeterministic powerdomains [den Hartog and de Vink 1999; McIver and Morgan 2001, 2005; Mislove 2000; Mislove et al. 2004; Tix et al. 2009].

3.1 Background from Domain Theory

Let P be a nonempty set with a partial order $\sqsubseteq$, i.e., a *poset*. The *lower closure* of a subset A is defined as $\downarrow A \stackrel{\text{def}}{=} \{x \in P \mid \exists a \in A : x \sqsubseteq a\}$. The *upper closure* of a subset A is defined as $\uparrow A \stackrel{\text{def}}{=} \{x \in P \mid \exists a \in A : a \sqsubseteq x\}$. A subset A satisfying $\downarrow A = A$ is called a *lower set*. A subset A satisfying $\uparrow A = A$ is called an *upper set*. If all elements of P are above a single element $x \in P$, then x is called the *least element*, denoted commonly by $\bot$. A function $f : P \to Q$ between two posets P and Q is *monotone* if for all $x, y \in P$ such that $x \sqsubseteq y$, we have $f(x) \sqsubseteq f(y)$. A subset A of P is *directed* if it is nonempty and each pair of elements in A has an upper bound in A. If A is totally ordered and isomorphic to natural numbers, then A is called an *ω-chain*. If a directed set A has a supremum, then it is denoted by $\bigsqcup^{\uparrow} A$.

A poset D is called *directed complete* or a dcpo if each directed subset A of D has a supremum $\bigsqcup^{\uparrow} A$ in D. A function $f : D \to E$ between two dcpos D and E is *Scott-continuous* if it is monotone and preserves directed suprema, i.e., $f(\bigsqcup^{\uparrow} A) = \bigsqcup^{\uparrow} f(A)$ for all directed subsets A of D.

Let D be a dcpo. For two elements x, y of D, we say that x *approximates* y, denoted by $x \ll y$, if for all directed subsets A of D, we have $y \sqsubseteq \bigsqcup^{\uparrow} A$ implies $x \sqsubseteq a$ for some $a \in A$. We define $\Downarrow A \stackrel{\text{def}}{=} \{x \in D \mid \exists a \in A : x \ll a\}$ and $\Uparrow A \stackrel{\text{def}}{=} \{x \in D \mid \exists a \in A : a \ll x\}$. The dcpo D is called *continuous* if there exists a subset B of D such that for every element x of D, the set $\Downarrow x \cap B$ is directed and $x = \bigsqcup^{\uparrow}(\Downarrow x \cap B)$. The set B is called a *basis* of D.

Let D be a dcpo. A subset A is *Scott-closed* if A is a lower set and is closed under directed suprema. The complement $D \setminus A$ of a Scott-closed subset A is called *Scott-open*. These Scott-open subsets form

the *Scott-topology* on D. The *closure* of a subset A is the smallest Scott-closed set containing A as a subset, denoted by $\overline{A}$.

Let X be a topological space whose open sets are denoted by $\mathcal{O}(X)$. A *cover* $\mathcal{C}$ of a subset A of X is a collection of subsets whose union contains A as a subset. A *sub-cover* of $\mathcal{C}$ is a subset of $\mathcal{C}$ that still covers A. The cover $\mathcal{C}$ is called an *open-cover* if each of its members is an open set. A subset A is *compact* if every open-cover of A contains a finite sub-cover. A subset A is *saturated* if A is an intersection of its neighborhoods. The *saturation* of a subset A is the intersection of its neighborhoods. In dcpo's equipped with the Scott-topology, saturated sets are precisely the upper sets, and the saturation of a subset A is given by $\uparrow A$. The *Lawson-topology* on a dcpo D is generated by Scott-open sets and sets of the form $D \setminus \uparrow x$. A *lens* is a nonempty subset that is the intersection of a Scott-closed subset and a Scott-compact saturated subset. Lenses are always Lawson-closed sets. A continuous dcpo D is called *coherent* if the intersection of any two Scott-compact saturated subsets is also Scott-compact. The Lawson-topology on a coherent dcpo is compact.

We are going to use the following theorems in our technical development.

Proposition 3.1 (Kleene fixed-point theorem). *Suppose $\langle D, \sqsubseteq\rangle$ is a dcpo with a least element $\bot$, and let $f : D \to D$ be a Scott-continuous function. Then f has a least fixed point which is the supremum of the ascending Kleene chain of f (i.e., the ω-chain $\bot \sqsubseteq f(\bot) \sqsubseteq f(f(\bot)) \sqsubseteq \cdots \sqsubseteq f^n(\bot) \sqsubseteq \cdots$), denoted by $\mathrm{lfp}^{\sqsubseteq}_{\bot} f$.*

Proposition 3.2 (Cor. of [Hofmann and Mislove 1981, Hofmann-Mislove theorem]). *Let X be a sober space, i.e., a T_0-space where every nonempty closed set is either the closure of a point or the union of two proper closed subsets. The intersection of a filtered family $\{A_i\}_{i\in\mathcal{I}}$ (i.e., the intersection of any two subsets is in the family) of nonempty compact saturated subsets is compact and nonempty. If such a filtered intersection is contained in an open set U, then $A_i \subseteq U$ for some $i \in \mathcal{I}$. Specifically, continuous dcpos equipped with the Scott-topology and coherent dcpos equipped with the Lawson-topology are sober.*

3.2 Probabilistic Powerdomains

Jones et al.'s pioneer work on probabilistic powerdomains [Jones 1989; Jones and Plotkin 1989] extends the complete partially ordered sets, which are pervasively used in computer science, to model probabilistic computations. Let X be a nonempty countable set. The set of all distributions on X is denoted by $\underline{\mathcal{D}}(X)$, i.e., a *probabilistic powerdomain* over X. Recall that a distribution on X is a function $\Delta : X \to [0,1]$ such that $\sum_{x\in X} \Delta(x) \le 1$, and the point distribution $\delta(x)$ for some $x \in X$ is defined as $\lambda x'.[x = x']$. Distributions are ordered pointwise, i.e., $\Delta_1 \sqsubseteq_D \Delta_2 \stackrel{\text{def}}{=} \forall x \in X : \Delta_1(x) \le \Delta_2(x)$. We define the *probabilistic-choice* of distributions Δ_1, Δ_2 with respect to a weight $p \in [0,1]$, written $\Delta_1 \,{}_p\!\oplus \Delta_2$, as $p \cdot \Delta_1 + (1-p) \cdot \Delta_2$.

The following theorems provide a characterization of the probabilistic powerdomains.

Proposition 3.3 ([Jones 1989; Jones and Plotkin 1989; McIver and Morgan 2001; Tix et al. 2009]). *The poset $\langle \underline{\mathcal{D}}(X), \sqsubseteq_D\rangle$ forms a coherent dcpo with a countable basis $\{\sum_{i=1}^n r_i \cdot \delta(x_i) \mid n \in \mathbb{N} \wedge r_i \in \mathbb{Q}_0^+ \wedge \sum_{i=1}^n r_i \le 1 \wedge x_i \in X\}$. It admits a least element $\bot_D \stackrel{\text{def}}{=} \lambda x.0$. Moreover, ${}_p\!\oplus$ is Scott-continuous for all $p \in [0,1]$.*

Proposition 3.4 ([Jones 1989; Tix et al. 2009]). *Every function $f : X \to \underline{\mathcal{D}}(X)$ can be lifted to a unique Scott-continuous linear (in the sense that it preserves probabilistic-choice) map $\widehat{f} : \underline{\mathcal{D}}(X) \to \underline{\mathcal{D}}(X)$.*

3.3 Nondeterministic Powerdomains

When nondeterminism comes into the picture, as we discussed in §1, existing studies usually resolve program inputs *prior to* nondeterminism [den Hartog and de Vink 1999; Jung and Tix 1998; McIver and Morgan 2001, 2005; Mislove 2000; Mislove et al. 2004; Tix et al. 2009]. In §1, we call such a model *nondeterminism-last*, which interprets nondeterministic functions as maps from inputs to sets

of outputs. Let X be a nonempty countable set. A subset A of $\underline{\mathcal{D}}(X)$ is called *convex* if for all $\Delta_1, \Delta_2 \in A$ and all $p \in [0,1]$, we have $\Delta_1 \,{}_p\!\oplus \Delta_2 \in A$. The *convex hull* of an arbitrary subset A is the smallest convex set containing A as a subset, denoted by $conv(A)$. The convexity condition ensures that from the perspective of programming, nondeterministic choices can always be *refined* by probabilistic choices. The *convex powerdomain* $\mathcal{P}\underline{\mathcal{D}}(X)$ over the probabilistic powerdomain $\underline{\mathcal{D}}(X)$ is then defined as convex lenses in $\underline{\mathcal{D}}(X)$ with the *Egli-Milner order* $A \sqsubseteq_P B \stackrel{\text{def}}{=} A \subseteq \downarrow B \wedge \uparrow A \supseteq B$.

The following theorems provide a characterization of the convex powerdomains.

Proposition 3.5 ([McIver and Morgan 2001; Tix et al. 2009]). *The poset $\langle \mathcal{P}\underline{\mathcal{D}}(X), \sqsubseteq_P \rangle$ forms a coherent dcpo. It admits a least element $\bot_P \stackrel{\text{def}}{=} \{\bot_D\}$. For $r_1, r_2 \in [0,1]$ satisfying $r_1 + r_2 \le 1$, we define $r_1 \cdot A + r_2 \cdot B \stackrel{\text{def}}{=} \overline{C} \cap \uparrow C$ where C is $\{r_1 \cdot \Delta_1 + r_2 \cdot \Delta_2 \mid \Delta_1 \in A \wedge \Delta_2 \in B\}$. Then the probabilistic-choice operation is lifted to a Scott-continuous operation as $A \,{}_p\!\oplus_P B \stackrel{\text{def}}{=} p \cdot A + (1-p) \cdot B$. Moreover, it carries a Scott-continuous semilattice operation, called* formal union, *defined as $A \uplus_P B \stackrel{\text{def}}{=} \overline{C} \cap \uparrow C$ where C is $conv(A \cup B)$. Intuitively, the formal union operation stands for nondeterministic choices.*

Proposition 3.6 ([Tix et al. 2009]). *Every function $g : X \to \mathcal{P}\underline{\mathcal{D}}(X)$ can be lifted to a unique Scott-continuous linear (in the sense that it preserves lifted probabilistic-choice) map $\widehat{\widehat{g}} : \mathcal{P}\underline{\mathcal{D}}(X) \to \mathcal{P}\underline{\mathcal{D}}(X)$ preserving formal unions.*

Example 3.7. Consider the following program P where $\star$ can be refined by any deterministic condition involving the program variable t:

$$\textbf{if } \star \textbf{ then } t := t+1 \textbf{ else } t := t-1 \textbf{ fi}$$

and we want to assign a semantic object to it from $X \to \mathcal{P}\underline{\mathcal{D}}(X)$, where the state space $X = \mathbb{Q}$ represents the value of t. Fix an input $t \in \mathbb{Q}$. The data actions $t := t+1$ and $t := t-1$ then take the input to singletons $\{\delta(t+1)\}$ and $\{\delta(t-1)\}$, respectively, in the powerdomain $\mathcal{P}\underline{\mathcal{D}}(\mathbb{Q})$. Thus the nondeterministic-choice is interpreted as $\{\delta(t+1)\} \uplus_P \{\delta(t-1)\}$, which is $\{r \cdot \delta(t+1) + (1-r) \cdot \delta(t-1) \mid r \in [0,1]\}$, for a given $t \in \mathbb{Q}$.

4 Nondeterminism-First

In this section, we develop a new model of nondeterminism—the *nondeterminism-first* approach, which resolves nondeterministic choices *prior to* program inputs—in a domain-theoretic way. This model is inspired by reasoning about a program's behavior on different inputs (as mentioned in §1), which requires nondeterministic functions to be treated as a family of *transformers* (i.e., an element of $\wp(X \to X)$) instead of a set-valued map (i.e., an element of $X \to \wp(X)$). As will be shown in this section, with nondeterminism-first, $t := t+1$ and $t := t-1$ are assigned semantic objects $\{\lambda t.\delta(t+1)\}$ and $\{\lambda t.\delta(t-1)\}$, respectively.

We first introduce *kernels*, then propose a new notion of *generalized convexity* (*g-convexity*, for short), and finally develop a powerdomain for nondeterminism-first. Complete proofs are included in appendix A.

4.1 A Powerdomain for Sub-Probability Kernels

Let X be a nonempty countable set. A function $\kappa : X \to \underline{\mathcal{D}}(X)$ is called a *(sub-probability) kernel*. Intuitively, a kernel maps an input state to a distribution over output states. The set of all such kernels is denoted by $\underline{\mathcal{K}}(X) \stackrel{\text{def}}{=} X \to \underline{\mathcal{D}}(X)$. Kernels are ordered pointwise, i.e., $\kappa_1 \sqsubseteq_K \kappa_2 \stackrel{\text{def}}{=} \forall x \in X : \kappa_1(x) \sqsubseteq_D \kappa_2(x)$.

Theorem 4.1. *The poset $\langle \underline{\mathcal{K}}(X), \sqsubseteq_K \rangle$ forms a coherent dcpo, with $\bot_K \stackrel{\text{def}}{=} \lambda x.\bot_D$ as its least element.*

Let $\mathbb{W}(X) \stackrel{\text{def}}{=} X \to [0,1]$ be the set of functions from X to the interval $[0,1]$. We denote the pointwise comparison by $\dot{\leq}$ and the constant function by $\dot{r}$ for any $r \in [0,1]$. If κ is a kernel and $\phi \in \mathbb{W}(X)$, we write $\phi \cdot \kappa$ for the kernel $\lambda x.\phi(x) \cdot \kappa(x)$. If κ_1, κ_2 are kernels and $\phi_1, \phi_2 \in \mathbb{W}(X)$ such that $\phi_1 + \phi_2 \dot{\leq} \dot{1}$, we write $\phi_1 \cdot \kappa_1 + \phi_2 \cdot \kappa_2$ for the kernel $\lambda x.\phi_1(x) \cdot \kappa_1(x) + \phi_2(x) \cdot \kappa_2(x)$. More generally, if $\{\kappa_i\}_{i \in \mathbb{N}^+}$ is a sequence of kernels, and $\{\phi_i\}_{i \in \mathbb{N}^+}$ is a sequence of functions in $\mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \phi_i \dot{\leq} \dot{1}$, we write $\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i$ for the kernel $\bigsqcup^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i \cdot \kappa_i$. Then we define *conditional-choice* of kernels κ_1, κ_2 conditioning on a function $\phi \in \mathbb{W}(X)$ as $\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2 \stackrel{\text{def}}{=} \phi \cdot \kappa_1 + (\dot{1} - \phi) \cdot \kappa_2$. We define the *composition* of kernels κ_1, κ_2 as $\kappa_1 \otimes \kappa_2 \stackrel{\text{def}}{=} \lambda x.\lambda x''.\sum_{x' \in X} \kappa_1(x)(x') \cdot \kappa_2(x')(x'')$.

Lemma 4.2. *1. The conditional-choice operation ${}_{\phi}\!\diamond$ is Scott-continuous for all $\phi \in \mathbb{W}(X)$.*

2. The composition operation $\otimes$ is Scott-continuous.

4.2 Generalized Convexity

As shown in §3.3, nondeterminism-*last* is captured by convex sets of distributions. However, a more complicated notion of convexity is needed to develop nondeterminism-*first* semantics over kernels. Let X be a nonempty countable set. Every semantic object should be closed under the conditional-choice ${}_{\phi}\!\diamond$ for every function $\phi \in \mathbb{W}(X)$. Recall that the definition $\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2 \stackrel{\text{def}}{=} \phi \cdot \kappa_1 + (\dot{1} - \phi) \cdot \kappa_2$ is similar to a convex combination, except that the coefficients might not only be constants, but can also depend on the state. We formalize the idea by defining a notion of *g-convexity*.

Definition 4.3. A subset A of $\underline{\mathcal{K}}(X)$ is called *g-convex*, if for all sequences $\{\kappa_i\}_{i \in \mathbb{N}^+} \subseteq A$ and $\{\phi_i\}_{i \in \mathbb{N}^+} \subseteq \mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \phi_i = \dot{1}$, then $\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i$ is contained in A.

We now show that some domain-theoretic operations preserve g-convexity.

Lemma 4.4. *Let A be a g-convex subset of $\underline{\mathcal{K}}(X)$. Then*

1. *The saturation $\uparrow A$ and the lower closure $\downarrow A$ are g-convex.*
2. *The closure $\overline{A}$ is g-convex.*

The *g-convex hull* of a subset A of $\underline{\mathcal{K}}(X)$ is the smallest g-convex set containing A as a subset, denoted by $gconv(A)$. Intuitively, $gconv(A)$ enriches A to become a reasonable semantic object that is closed under arbitrary conditional-choice.

Following are some properties of the $gconv(\cdot)$ operator.

Lemma 4.5. *Suppose that A and B are g-convex subsets of $\underline{\mathcal{K}}(X)$. Then $\{\kappa \,{}_{\phi}\!\diamond\, \rho \mid \kappa \in A \wedge \rho \in B\}$ is g-convex for all functions $\phi \in \mathbb{W}(X)$.*

Corollary 4.6. *If A and B are g-convex, then $gconv(A \cup B)$ is given by $\{\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2 \mid \kappa_1 \in A \wedge \kappa_2 \in B \wedge \phi \in \mathbb{W}(X)\}$.*

Proof. It is straightforward to show that $gconv(A \cup B)$ is a superset of $\{\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2 \mid \kappa_1 \in A \wedge \kappa_2 \in B \wedge \phi \in \mathbb{W}(X)\}$. Then it suffices to show this set is indeed g-convex. We conclude the proof by Lem. 4.5. □

For a finite subset F of $\underline{\mathcal{K}}(X)$, as an immediate corollary of Cor. 4.6, by a simple induction we know that $gconv(F) = \{\sum_{\kappa \in F} \phi_\kappa \cdot \kappa \mid \{\phi_\kappa\}_{\kappa \in F} \subseteq \mathbb{W}(X) \wedge \sum_{\kappa \in F} \phi_\kappa = \dot{1}\}$.

Lemma 4.7. *For an arbitrary $A \subseteq \mathcal{K}(X)$, we have*

$$gconv(A) = \{\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i \mid \{\kappa_i\}_{i \in \mathbb{N}^+} \subseteq A \wedge \{\phi_i\}_{i \in \mathbb{N}^+} \subseteq \mathbb{W}(X) \wedge \sum_{i=1}^{\infty} \phi_i = \dot{1}\}.$$

Lemma 4.8. 1. *For an arbitrary $A \subseteq \underline{\mathcal{K}}(X)$, we have $\overline{gconv(A)} = \overline{gconv(\overline{A})}$.*

2. *If $\{A_i\}_{i\in\mathcal{I}}$ is a directed collection of Scott-closed subsets of $\underline{\mathcal{K}}(X)$ ordered by set inclusion, then $\overline{gconv(\bigcup A_i)} = \bigcup \overline{gconv(A_i)}$.*

Lemma 4.9. *Let A and B be Scott-compact g-convex subsets of $\underline{\mathcal{K}}(X)$. Then $gconv(A \cup B)$ is also Scott-compact.*

We now turn to discuss some separation properties for g-convexity.

Lemma 4.10. 1. *If $A \subseteq \underline{\mathcal{K}}(X)$ is g-convex, then for all x, $\{\kappa(x) \mid \kappa \in A\}$ is convex.*

2. *If $A \subseteq \underline{\mathcal{K}}(X)$ is Scott-compact, then for all x, $\{\kappa(x) \mid \kappa \in A\}$ is Scott-compact.*

3. *If $A \subseteq \underline{\mathcal{K}}(X)$ is Scott-closed, then for all x, $\{\kappa(x) \mid \kappa \in A\}$ is Scott-closed.*

Lemma 4.11. *Let us consider subsets of $\underline{\mathcal{K}}(X)$. Suppose that K is a Scott-compact g-convex set and A is a nonempty Scott-closed g-convex set that is disjoint from K. Then they can be separated by a g-convex Scott-open set, i.e., there is a g-convex Scott-open set V including K and disjoint from A.*

Lemma 4.12. *If $K \subseteq \underline{\mathcal{K}}(X)$ is nonempty and Scott-compact, then $gconv(K)$ is Scott-compact.*

4.3 A g-convex Powerdomain for Nondeterminism-First

From the literature, a *Plotkin powertheory* [Abramsky and Jung 1994] is defined by one binary operation $\uplus$, called *formal union*, and the following laws: (i) $A \uplus B = B \uplus A$, (ii) $(A \uplus B) \uplus C = A \uplus (B \uplus C)$, and (iii) $A \uplus A = A$, for all objects A, B, C in the powerdomain. Intuitively, the formal union $\uplus$ represents nondeterministic-choice. Moreover, the formal union induces a semilattice ordering: $A \leq B$ if $A \uplus B = B$. The semilattice ordering is usually not interesting from the perspective of domain theory, however, it is instrumental to describe the relation between conditional-choice and nondeterministic-choice—$A \,{}_{\phi}\!\Diamond\, B \leq A \uplus B$ for all semantic objects A, B—a nondeterministic-choice should *abstract* an arbitrary (possibly probabilistic) conditional-choice.

Let X be a nonempty countable set. As nondeterminism-first interprets programs as collections of input-output transformers, we hope to develop a powerdomain on $\underline{\mathcal{K}}(X)$, i.e., kernels on X. To achieve this goal, we need to (i) identify a collection of well-formed semantic objects in $\wp(\underline{\mathcal{K}}(X))$, which admits a formal-union operation described above, (ii) lift conditional-choice $\,{}_{\phi}\!\Diamond$ and composition $\otimes$ on kernels to the powerdomain properly, and (iii) prove the powerdomain is a dcpo and the operations are Scott-continuous.

Inspired by studies on convex powerdomains [Abramsky and Jung 1994; McIver and Morgan 2001; Tix et al. 2009], we start with the following collection

$$\mathcal{G}\underline{\mathcal{K}}(X) \stackrel{\text{def}}{=} \{S \subseteq \underline{\mathcal{K}}(X) \mid S \text{ a nonempty g-convex lens}\}$$

to be the set of all g-convex lenses of $\underline{\mathcal{K}}(X)$ ordered by Egli-Miler order $A \sqsubseteq_G B \stackrel{\text{def}}{=} A \subseteq \downarrow B \wedge \uparrow A \supseteq B$. We call $\mathcal{G}\underline{\mathcal{K}}(X)$ a *g-convex powerdomain* over kernels on X.

The following theorem establishes a characterization of g-convex powerdomains.

Theorem 4.13. *$\langle \mathcal{G}\underline{\mathcal{K}}(X), \sqsubseteq_G \rangle$ forms a dcpo, with a least element $\bot_G \stackrel{\text{def}}{=} \{\bot_K\}$.*

We now lift conditional-choice $\,{}_{\phi}\!\Diamond$ (where $\phi \in \mathbb{W}(X)$) and composition $\otimes$ for kernels to the powerdomain $\mathcal{G}\underline{\mathcal{K}}(X)$ as follows.

$$A \,{}_{\phi}\!\Diamond_G\, B \stackrel{\text{def}}{=} \overline{\{a \,{}_{\phi}\!\Diamond\, b \mid a \in A \wedge b \in B\}} \cap \uparrow \{a \,{}_{\phi}\!\Diamond\, b \mid a \in A \wedge b \in B\}$$

$$A \otimes_G B \stackrel{\text{def}}{=} \overline{gconv(\{a \otimes b \mid a \in A \wedge b \in B\})} \cap \uparrow gconv(\{a \otimes b \mid a \in A \wedge b \in B\})$$

The operations construct nonempty g-convex lenses by Lemmas 4.4 and 4.12. As conditional-choice and composition operations are Scott-continuous on kernels, the lifted operations are also Scott-continuous in the powerdomain.

Lemma 4.14. *The operations* ${}_{\phi}\Diamond_{G}$ *and* $\otimes_G$ *are Scott-continuous for all* $\phi \in \mathbb{W}(X)$.

Finally, we define a *formal union* operation $\uplus_G$ as in Prop. 3.5 to interpret nondeterministic-choice as $A \uplus_G B \stackrel{\text{def}}{=} \overline{C} \cap \uparrow C$ where C is $gconv(A \cup B)$.

Lemma 4.15. *The formal union* $\uplus_G$ *is a Scott-continuous semilattice operation on* $\mathcal{GK}(X)$.

Example 4.16. Recall the probabilistic program P in Ex. 3.7:

$$\textbf{if } \star \textbf{ then } t \coloneqq t+1 \textbf{ else } t \coloneqq t-1 \textbf{ fi}$$

the state space X is $\mathbb{Q}$*, and we want to show that for any probabilistic refinement* P_r *of P (i.e.,* $\star$ *is refined by* $\textbf{prob}(r)$*), for input values* t_1, t_2 *of t, we have* $\mathbb{E}_{t_1' \sim \Delta_1, t_2' \sim \Delta_2}[t_1' - t_2'] = t_1 - t_2$*, where the program* P_r *ends up with a distribution* Δ_1 *starting with* $t = t_1$ *and* Δ_2 *with* $t = t_2$.

With the g-convex powerdomain $\mathcal{GK}(X)$ *for nondeterminism-first,* $t \coloneqq t+1$ *and* $t \coloneqq t-1$ *are assigned semantic objects* $\{\lambda t.\delta(t+1)\}$ *and* $\{\lambda t.\delta(t-1)\}$*, respectively. Thus the nondeterministic-choice is interpreted as a subset of* $\{\lambda t.\delta(t+1)\} \uplus_G \{\lambda t.\delta(t-1)\}$*, which is* $\{\kappa_r \mid r \in [0,1]\}$*, where* $\kappa_r = \lambda t.r \cdot \delta(t+1) + (1-r) \cdot \delta(t-1)$ *is the kernel for the deterministic refinement* P_r *of P. Therefore for every* $r \in [0,1]$*, we have* $\mathbb{E}_{t_1' \sim \Delta_1, t_2' \sim \Delta_2}[t_1' - t_2'] = \mathbb{E}_{t_1' \sim \kappa_r(t_1), t_2' \sim \kappa_r(t_2)}[t_1'] - \mathbb{E}_{t_1' \sim \kappa_r(t_1), t_2' \sim \kappa_r(t_2)}[t_2'] = (r(t_1+1) + (1-r)(t_1-1)) - (r(t_2+1) + (1-r)(t_2-1)) = t_1 - t_2$.

In contrast, if we started with the convex powerdomain $\mathcal{P}\underline{\mathcal{D}}(X)$ *reviewed in §3.3 for nondeterminism-last, we would obtain the semantic object* $\lambda t.\{r \cdot \delta(t+1) + (1-r) \cdot \delta(t-1) \mid r \in [0,1]\}$ *for the program P, as shown in Ex. 3.7. Now the refinements of P include some* κ *such that* $\kappa(t_1) = 0.5 \cdot \delta(t_1+1) + 0.5 \cdot \delta(t_1-1)$ *and* $\kappa(t_2) = 0.3 \cdot \delta(t_2+1) + 0.7 \cdot \delta(t_2-1)$*, thus we are not able to prove the claim* $\mathbb{E}[t_1' - t_2'] = t_1 - t_2$.

5 An Algebraic Denotational Semantics

The operational semantics described in §2.2 presents a reasonable model for evaluating single-procedure probabilistic programs without nondeterminism. In this section, we develop a general denotational semantics for CFHGs (introduced in §2.1) of multi-procedure probabilistic programs with nondeterminism. The semantics is *algebraic* in the sense that it could be instantiated with different concrete models of nondeterminism, e.g., nondeterminism-last reviewed in §3.3, as well as nondeterminism-first developed in §4.3. We will show the denotational semantics is equivalent to the operational semantics in §2.2 if we suppress procedure calls and nondeterminism in the programming model.

5.1 A Fixpoint Semantics based on Markov Algebras

The algebraic denotational semantics is obtained by composing $Ctrl(e)$ operations along hyper-edges. The semantics of programs is determined by an *interpretation*, which consists of two parts: (i) a *semantic algebra*, which defines a set of possible program meanings, and which is equipped with sequencing, conditional-choice, and nondeterministic-choice operators to compose these meanings, and (ii) a *semantic function*, which assigns a meaning to each data action $\text{act} \in \text{Act}$. The semantic algebras that we use are *Markov algebras* introduced in [Wang et al. 2018]:

Definition 5.1. A *Markov algebra* (MA) over a set Cond of deterministic conditions is a 7-tuple $\mathcal{M} = \langle M, \sqsubseteq_M, \otimes_M, {}_{\phi}\Diamond_{M}, \uplus_M, \bot_M, 1_M \rangle$, where $\langle M, \sqsubseteq_M \rangle$ forms a dcpo with $\bot_M$ as its least element; $\langle M, \otimes_M, 1_M \rangle$ forms a monoid (i.e., $\otimes_M$ is an associative binary operator with 1_M as its identity element); ${}_{\varphi}\Diamond_{M}$ is a binary operator parametrized by a condition $\varphi \in \text{Cond}$; $\uplus_M$ is idempotent,

commutative, associative and for all $a, b \in M$ and $\varphi \in \mathsf{Cond}$ we have $a \,{}_{\varphi}\!\Diamond_M\, b \leq_M a \uplus_M b$ where $\leq_M$ is the semilattice ordering induced by $\uplus_M$ (i.e., $a \leq_M b$ if $a \uplus_M b = b$); and $\otimes_M, {}_{\varphi}\!\Diamond_M, \uplus_M$ are Scott-continuous.

Example 5.2. Let Ω be a nonempty countable set of program states and Cond *be a set of deterministic conditions, the definition and meaning of which are given in §2.1 and §2.2.*

1. *The convex powerdomain $\mathcal{P}\underline{\mathcal{D}}(\Omega)$ admits an MA $\langle \Omega \to \mathcal{P}\underline{\mathcal{D}}(\Omega), \dot{\sqsubseteq}_P, \otimes_P, {}_{\varphi}\!\Diamond_P, \dot{\uplus}_P, \dot{\perp}_P, 1_P \rangle$, where $\dot{\sqsubseteq}_P, \dot{\uplus}_P, \dot{\perp}_P$ are pointwise extensions of $\sqsubseteq_P, \uplus_P, \perp_P$, defined in §3.3, and $g \otimes_P h \stackrel{\text{def}}{=} \widehat{h} \circ g$ where $\widehat{h}$ is given by Prop. 3.6, $g \,{}_{\varphi}\!\Diamond_P\, h \stackrel{\text{def}}{=} \lambda\omega.g(\omega) \,{}_{[\![\varphi]\!](\omega)}\!\oplus_P\, h(\omega)$, as well as $1_P \stackrel{\text{def}}{=} \lambda\omega.\{\delta(\omega)\}$.*
2. *The g-convex powerdomain $\mathcal{G}\underline{\mathcal{K}}(\Omega)$ admits an MA $\langle \mathcal{G}\underline{\mathcal{K}}(\Omega), \sqsubseteq_G, \otimes_G, {}_{\varphi}\!\Diamond_G, \uplus_G, \perp_G, 1_G \rangle$, where $\sqsubseteq_G, \otimes_G, {}_{\varphi}\!\Diamond_G, \uplus_G, \perp_G$ come from §4.3,[3] and $1_G \stackrel{\text{def}}{=} \{\lambda\omega.\delta(\omega)\}$.*

Definition 5.3. An *interpretation* is a pair $\mathscr{I} = \langle \mathcal{M}, [\![\cdot]\!]^{\mathscr{I}} \rangle$, where $\mathcal{M}$ is an MA and $[\![\cdot]\!]^{\mathscr{I}} : \mathsf{Act} \to \mathcal{M}$. We call $\mathcal{M}$ the *semantic algebra* of the interpretation and $[\![\cdot]\!]^{\mathscr{I}}$ the *semantic function*.

Example 5.4. We can lift the interpretation of data actions defined in Fig. 3 to semantic functions with respect to convex or g-convex powerdomains—$\mathscr{P} = \langle \mathcal{P}\underline{\mathcal{D}}(\Omega), [\![\cdot]\!]^{\mathscr{P}} \rangle$ with $[\![\mathsf{act}]\!]^{\mathscr{P}} \stackrel{\text{def}}{=} \lambda\omega.\{[\![\mathsf{act}]\!](\omega)\}$ and $\mathscr{G} = \langle \mathcal{G}\underline{\mathcal{K}}(\Omega), [\![\cdot]\!]^{\mathscr{G}} \rangle$ with $[\![\mathsf{act}]\!]^{\mathscr{G}} \stackrel{\text{def}}{=} \{[\![\mathsf{act}]\!]\}$.

Given a probabilistic program $P = \{H_i\}_{1 \leq i \leq n}$ where each $H_i = \langle V_i, E_i, v_i^{\mathsf{entry}}, v_i^{\mathsf{exit}} \rangle$ is a CFHG, and an interpretation $\mathscr{I} = \langle \mathcal{M}, [\![\cdot]\!]^{\mathscr{I}} \rangle$, we define $\mathscr{I}[P]$ to be the interpretation of the probabilistic program, as the least fixpoint of the function F_P, which is defined as

$$\lambda\mathbf{S}.\lambda v.\begin{cases} \bigsqcup_M \{\widehat{Ctrl(e)}(\mathbf{S}(u_1), \cdots, \mathbf{S}(u_k)) \mid e = \langle v, \{u_1, \cdots, u_k\} \rangle \in E\} & v \neq v_i^{\mathsf{exit}} \text{ for all } i \\ 1_M & \text{otherwise} \end{cases}$$

where $\widehat{Ctrl(e)}$ for different kinds of control-flow actions is defined as follows:

$$\widehat{seq[\mathsf{act}]}(S_1) \stackrel{\text{def}}{=} [\![\mathsf{act}]\!]^{\mathscr{I}} \otimes_M S_1, \quad \widehat{cond[\varphi]}(S_1, S_2) \stackrel{\text{def}}{=} S_1 \,{}_{\varphi}\!\Diamond_M\, S_2, \quad \widehat{call[i \to j]}(S_1) \stackrel{\text{def}}{=} \mathbf{S}(v_j^{\mathsf{entry}}) \otimes_M S_1.$$

The least fixpoint of F_P exists by Prop. 3.1 as well as the following lemma. Hence the semantics of the procedure H_i is given by $[\![H_i]\!]_{\mathsf{ds}} \stackrel{\text{def}}{=} (\mathrm{lfp}^{\dot{\sqsubseteq}_M}_{\dot{\perp}_M} F_P)(v_i^{\mathsf{entry}})$.

Lemma 5.5. *The function F_P is Scott-continuous on the dcpo $\langle V \to M, \dot{\sqsubseteq}_M \rangle$ with $\dot{\perp}_M \stackrel{\text{def}}{=} \lambda v.\perp_M$ as the least element, where $\dot{\sqsubseteq}_M$ is the pointwise extension of $\sqsubseteq_M$.*

Proof. Appeal to the Scott-continuity of the operations $\otimes_M$, ${}_{\varphi}\!\Diamond_M$, and $\uplus_M$. □

5.2 An Equivalence Result

To justify the denotational semantics proposed in §5.1, we go back to the restricted programming language used to define the operational semantics in §2.2. If we suppress the features of multi-procedure and nondeterminism, we should end up with a semantics that is equivalent to the operational semantics $[\![\cdot]\!]_{\mathsf{os}}$.

Lemma 5.6. *Let $P = \langle V, E, v^{\mathsf{entry}}, v^{\mathsf{exit}} \rangle$ be a deterministic single-procedure probabilistic program.*

[3] The conditional-choice is actually interpreted as ${}_{[\![\varphi]\!]}\!\Diamond_G$ in the powerdomain.

1. *If we interpret P using $\mathscr{P} = \langle \mathcal{P}\underline{\mathcal{D}}(\Omega), [\![\cdot]\!]^{\mathscr{P}} \rangle$, we will have $[\![P]\!]_{\mathsf{ds}} = \lambda\omega.\{[\![P]\!]_{\mathsf{os}}(\omega)\}$.*
2. *If we interpret P using $\mathscr{G} = \langle \mathcal{G}\underline{\mathcal{K}}(\Omega), [\![\cdot]\!]^{\mathscr{G}} \rangle$, we will have $[\![P]\!]_{\mathsf{ds}} = \{[\![P]\!]_{\mathsf{os}}\}$.*

Proof. Recall the definition $[\![P]\!] \stackrel{\text{def}}{=} \lambda\omega.\sup_{n\in\mathbb{N}}\{\Delta \mid \langle v^{\mathsf{entry}}, \omega\rangle \longrightarrow_n \Delta\}$. On the other hand, the fixpoint $(\mathrm{lfp}^{\dot{\sqsubseteq}_M}_{\dot{\perp}_M} F_P)(v_i^{\mathsf{entry}})$ is actually obtained by $\bigsqcup^{\uparrow}_{n\in\mathbb{N}} F_P^n(\dot{\perp}_M)(v_i^{\mathsf{entry}})$ by Prop. 3.1. The proof proceeds by induction on n. □

6 Application: Static Analysis for Probabilistic Programs with Nondeterminism

A lot of recent studies on probabilistic programming focus on rigorous reasoning about probabilistic programs (e.g., [Barthe et al. 2012; Batz et al. 2018; Bouissou et al. 2016; Brázdil et al. 2015; Chakarov and Sankaranarayanan 2013, 2014; Chatterjee et al. 2016a; Cousot and Monerau 2012; Gehr et al. 2016; Jansen et al. 2015; Kaminski et al. 2016; Katoen et al. 2010; Monniaux 2000, 2003; Olmedo et al. 2016; Sankaranarayanan et al. 2013]). In this section, we discuss an application of the new denotational semantics as the concrete semantics of a static-analysis framework for probabilistic programs. More details about the static analysis and its soundness proof can be found in a companion paper [Wang et al. 2018].

Definition 6.1. A *pre-Markov algebra* (PMA) over a set Cond of deterministic conditions is a 7-tuple $\mathcal{M}^\sharp = \langle M, \sqsubseteq_M, \otimes_M, {\varphi\diamondsuit}_M, \uplus_M, \perp_M, 1_M\rangle$, which is essentially an MA, except that $\langle M, \sqsubseteq_M\rangle$ forms a complete lattice, and $\otimes_M$, ${\varphi\diamondsuit}_M$, and $\uplus_M$ are only required to be monotone.

Intuitively, PMAs specify *abstract* semantics used in static analyses. We can define interpretations with respect to PMAs in the same way, except that we obtain the least fixpoint $\mathscr{I}^\sharp[P]$ of the function F_P by the Knaster-Tarski theorem, given a probabilistic program P and an interpretation $\mathscr{I} = \langle \mathcal{M}^\sharp, [\![\cdot]\!]^{\mathscr{I}}\rangle$.

Definition 6.2. A *probabilistic over-abstraction* (resp., *under-abstraction*) from an MA $\mathcal{C}$ (i.e., a concrete semantics such as $\mathcal{P}\underline{\mathcal{D}}(\Omega)$ and $\mathcal{G}\underline{\mathcal{K}}(\Omega)$) to a PMA $\mathcal{Y}$ is a concretization mapping, $\gamma : Y \to C$, such that

- $\perp_C \sqsubseteq_C \gamma(\perp_Y)$ (resp., $\gamma(\perp_Y) \sqsubseteq_C \perp_C$),
- $1_C \sqsubseteq_C \gamma(1_Y)$ (resp., $\gamma(1_Y) \sqsubseteq_C 1_C$),
- for all $Q_1, Q_2 \in Y$, $\gamma(Q_1) \otimes_C \gamma(Q_2) \sqsubseteq_C \gamma(Q_1 \otimes_Y Q_2)$ (resp., $\gamma(Q_1 \otimes_Y Q_2) \sqsubseteq_C \gamma(Q_1) \otimes_C \gamma(Q_2)$),
- for all $Q_1, Q_2 \in Y$, $\gamma(Q_1)\ {\varphi\diamondsuit}_C\ \gamma(Q_2) \sqsubseteq_C \gamma(Q_1\ {\varphi\diamondsuit}_Y\ Q_2)$ (resp., $\gamma(Q_1\ {\varphi\diamondsuit}_Y\ Q_2) \sqsubseteq_C \gamma(Q_1)\ {\varphi\diamondsuit}_C\ \gamma(Q_2)$), and
- for all $Q_1, Q_2 \in Y$, $\gamma(Q_1) \uplus_C \gamma(Q_2) \sqsubseteq_C \gamma(Q_1 \uplus_Y Q_2)$, (resp., $\gamma(Q_1 \uplus_Y Q_2) \sqsubseteq_C \gamma(Q_1) \uplus_C \gamma(Q_2)$).

A probabilistic abstraction leads to a sound analysis:

Theorem 6.3. *Let $\mathscr{C}$ and $\mathscr{Y}$ be interpretations over an MA $\mathcal{C}$ and a PMA $\mathcal{Y}$; let γ be a probabilistic over-abstraction (resp., under-abstraction) from $\mathcal{C}$ to $\mathcal{Y}$; and let P be an arbitrary program. If for all data actions* act, $[\![\mathrm{act}]\!]^{\mathscr{C}} \sqsubseteq_C \gamma([\![\mathrm{act}]\!]^{\mathscr{Y}})$ *(resp., $\gamma([\![\mathrm{act}]\!]^{\mathscr{Y}}) \sqsubseteq_C [\![\mathrm{act}]\!]^{\mathscr{C}}$), then we have $\mathscr{C}[P] \dot{\sqsubseteq}_C \dot{\gamma}(\mathscr{Y}^\sharp[P])$ (resp., $\dot{\gamma}(\mathscr{Y}^\sharp[P]) \dot{\sqsubseteq}_C \mathscr{C}[P]$).*

7 Discussion

7.1 Continuous Distributions

One of the most important features of probabilistic programming is *continuous* probability distributions over real numbers, such as Gaussian distributions. Notions from measure theory, such as *measures* and *kernels*, are extensively used to model continuous distributions in probabilistic programming. Kozen studied the relation between deterministic probabilistic programs and continuous distributions via a metric on measures [Kozen 1981b]. Many approaches use probability kernels [Kozen 1985; Smolka et al. 2017], sub-probability kernels [Borgström et al. 2016], and s-finite kernels [Bichsel et al. 2018; Staton 2017]. A different approach uses measurable functions $A \to \mathcal{D}(\mathbb{R}_{\geq 0} \times B)$ where $\mathcal{D}(S)$ stands for the set of all probability measures on S [Staton et al. 2016]. For higher-order languages, Jones and Plotkin [Jones 1989; Jones and Plotkin 1989] have developed a probabilistic powerdomain that consists of continuous *evaluations*, which are a reformulation of distributions in domain theory, on a state space. They show that the powerdomain can be used to solve recursive domain equations. Smolka et al. [Smolka et al. 2017] study the semantics of probabilistic networks. Ehrhard et al. [Ehrhard et al. 2018] provide a Cartesian-closed category on stable and measurable maps between cones, and use it to give a semantics for probabilistic PCF.

However, those measure-theoretic developments do not work properly when nondeterminism comes into the picture. To overcome this challenge, people have been adapting domain-theoretic results. McIver and Morgan build a Plotkin-style powerdomain over probability distributions on a discrete state space [McIver and Morgan 2001, 2005]. Mislove et al. [Mislove 2000; Mislove et al. 2004] study powerdomain constructions for probabilistic CSP. Tix et al. [Tix et al. 2009] generalize McIver and Morgan's results to continuous state spaces, and construct three powerdomains for the extended probabilistic powerdomains. Although there has been a lot of work on this direction, one has to keep in mind that the domain-theoretic notion of "continuous" distributions is different from the notion in measure theory—instead, the domain-theoretic studies are focused on *computable* distributions. In other words, real numbers are realized by some computable models, such as *partial reals* [Escardó 1996]. These models would become unsatisfactory when one wants to *observe* a random value drawn from a continuous distribution, e.g., the meaning of $x := \mathsf{Normal}(0,1); \mathbf{if}\ x = 0\ \mathbf{then}\ \cdots\ \mathbf{fi}$ is not expressible. We leave the semantic development of combining nondeterminism and continuous distributions (from a measure-theoretic perspective) for future work.

7.2 Higher-Order Functions

In functional programming, higher-order functions are functions that can take functions as arguments, as well as return a function as a result. Some probabilistic programming languages, such as Church [Goodman et al. 2008], are indeed functional programming languages and can express higher-order functions. While operational models for probabilistic functional programming have been proposed [Borgström et al. 2016], developing a denotational semantics for higher-order probabilistic programming has been an open problem for years.

The major challenge is to propose a Cartesian-closed category for semantic objects of probabilistic programming. Intuitively, the Cartesian-closure property ensures that if type A and type B are two objects in the category, then the function space B^A (i.e., an object for the arrow type $A \to B$) is also contained in the category. The category of measures is clearly *not* Cartesian-closed; a lot of probabilistic powerdomains also do *not* admit a Cartesian-closed category [Jung and Tix 1998]. Recently, Heunen et al. [Heunen et al. 2017] propose quasi-Borel measures for higher-order functions in probabilistic programming. The measure-theoretic approach is further extended by Vákár et al. [Vákár et al. 2019] to support recursive types. However, it is unclear how to model nondeterminism in the framework of quasi-Borel measures. We leave the combination of nondeterminism and higher-order functions for future work.

8 Conclusion

We have developed a framework for denotational semantics of low-level probabilistic programs with unstructured control-flow, general recursion, and nondeterminism, represented by control-flow hypergraphs. The semantics is algebraic and it can be instantiated with different models of nondeterminism. We have demonstrated two instantiations with nondeterminism-first and nondeterminism-last, respectively. We have proposed a powerdomain for nondeterminism-first that consists of collections of kernels and enjoys generalized convexity. As an application, we have reviewed a static-analysis framework for probabilistic programs, which has been proposed in a companion paper.

In the future, we plan to combine continuous distributions and higher-order functions with nondeterminism in our semantics framework. We will also work on models of nondeterminism, especially nondeterminism-first, and investigate its connection with relational reasoning. Another research direction is to develop more formal reasoning techniques based on the denotational semantics.

Acknowledgments

This work was supported, in part, by a gift from Rajiv and Ritu Batra; by AFRL under DARPA MUSE award FA8750-14-2-0270, DARPA STAC award FA8750-15-C-0082 and DARPA AA award FA8750-18-C-0092; by ONR under grant N00014-17-1-2889; by NSF under SaTC award 1801369, SHF grant 1812876, and CAREER award 1845514; and by the UW-Madison OVRGE with funding from WARF.

References

S. Abramsky and A. Jung. 1994. Domain Theory. In *Handbook of Logic in Computer Science*. Oxford University Press Oxford, UK.

G. Barthe, T. Espitau, M. Gaboardi, B. Grégoire, J. Hsu, and P.-Y. Strub. 2016. A Program Logic for Probabilistic Programs. Available on: https://justinh.su/files/papers/ellora.pdf.

G. Barthe, B. Grégoire, and S. Zanella Béguelin. 2009. Formal Certification of Code-based Cryptographic Proofs. In *Princ. of Prog. Lang. (POPL'09)*.

G. Barthe, B. Köpf, F. Olmedo, and S. Zanella Béguelin. 2012. Probabilistic Relational Reasoning for Differential Privacy. In *Princ. of Prog. Lang. (POPL'12)*.

Kevin Batz, B. L. Kaminski, J.-P. Katoen, and C. Matheja. 2018. How long, O Bayesian network, will I sample thee?. In *European Symp. on Programming (ESOP'18)*.

R. Bellman. 1957. A Markovian Decision Process. *Indiana Univ. Math. J.* 6 (1957). Issue 4.

B. Bichsel, T. Gehr, and M. Vechev. 2018. Fine-grained Semantics for Probabilistic Programs. In *European Symp. on Programming (ESOP'18)*.

J. Borgström, U. D. Lago, A. D. Gordon, and M. Szymczak. 2016. A Lambda-Calculus Foundation for Universal Probabilistic Programming. In *Int. Conf. on Functional Programming (ICFP'16)*.

O. Bouissou, E. Goubault, S. Putot, A. Chakarov, and S. Sankaranarayanan. 2016. Uncertainty Propagation Using Probabilistic Affine Forms and Concentration of Measure Inequalities. In *Tools and Algs. for the Construct. and Anal. of Syst. (TACAS'16)*.

T. Brázdil, S. Kiefer, A. Kučera, and I. H. Vařeková. 2015. Runtime Analysis of Probabilistic Programs with Unbounded Recursion. *J. Comput. Syst. Sci.* 81 (February 2015). Issue 1.

A. Chakarov and S. Sankaranarayanan. 2013. Probabilistic Program Analysis with Martingales. In *Computer Aided Verif. (CAV'13)*.

A. Chakarov and S. Sankaranarayanan. 2014. Expectation Invariants for Probabilistic Program Loops as Fixed Points. In *Static Analysis Symp. (SAS'14)*.

K. Chatterjee, H. Fu, and A. K. Goharshady. 2016a. Termination Analysis of Probabilistic Programs Through Positivstellensatz's. In *Computer Aided Verif. (CAV'16)*.

K. Chatterjee, H. Fu, P. Novotný, and R. Hasheminezhad. 2016b. Algorithmic Analysis of Qualitative and Quantitative Termination Problems for Affine Probabilistic Programs. In *Princ. of Prog. Lang. (POPL'16)*.

K. Chatterjee, P. Novotný, and Đ. Žikelić. 2017. Stochastic Invariants for Probabilistic Termination. In *Princ. of Prog. Lang. (POPL'17)*.

J. H. Conway. 1971. *Regular algebra and finite machines*. London: Chapman and Hall.

P. Cousot and M. Monerau. 2012. Probabilistic Abstract Interpretation. In *European Symp. on Programming (ESOP'12)*.

J. I. den Hartog and E. P. de Vink. 1999. Mixing Up Nondeterminism and Probability: a preliminary report. *Electr. Notes Theor. Comp. Sci.* 22 (1999).

E. W. Dijkstra. 1997. *A Discipline of Programming*. Prentice-Hall.

T. Ehrhard, M. Pagani, and C. Tasson. 2018. Measurable Cones and Stable, Measurable Functions. In *Princ. of Prog. Lang. (POPL'18)*.

M. H. Escardó. 1996. PCF extended with real numbers. *Theor. Comp. Sci.* 162 (August 1996). Issue 1.

K. Etessami and M. Yannakakis. 2005. Recursive Markov Chains, Stochastic Grammars, and Monotone Systems of Nonlinear Equations. In *Symp. on Theor. Aspects of Comp. Sci. (STACS'05)*.

K. Etessami and M. Yannakakis. 2015. Recursive Markov Decision Processes and Recursive Stochastic Games. *J. ACM* 62 (May 2015). Issue 2.

A. Farzan and Z. Kincaid. 2015. Compositional Recurrence Analysis. In *Formal Methods in Compiter-Aided Design (FMCAD'15)*.

L. M. Ferrer Fioriti and H. Hermanns. 2015. Probabilistic Termination: Soundness, Completeness, and Compositionality. In *Princ. of Prog. Lang. (POPL'15)*.

B. Franke, M. O'Boyle, J. Thomson, and G. Fursin. 2005. Probabilistic Source-Level Optimisation of Embedded Programs. In *Lang., Comp., and Tools for Embeded Syst. (LCTES'05)*.

G. Gallo, G. Longo, S. Pallottino, and S. Nguyen. 1993. Directed Hypergraphs and Applications. *Disc. Appl. Math.* 42 (April 1993). Issue 2.

T. Gehr, S. Misailovic, and M. Vechev. 2016. PSI: Exact Symbolic Inference for Probabilistic Programs. In *Computer Aided Verif. (CAV'16)*.

Z. Ghahramani. 2015. Probabilistic machine learning and artificial intelligence. *Nature* (2015).

N. D. Goodman, V. K. Mansinghka, D. M. Roy, and J. B. Tenenbaum. 2008. Church: a language for generative models. In *Uncertainty in Artif. Intelligence*.

A. D. Gordon, T. A. Henzinger, A. V. Nori, and S. K. Rajamani. 2014. Probabilistic Programming. In *Future of Softw. Eng. (FOSE'14)*.

C. Heunen, O. Kammar, S. Staton, and H. Yang. 2017. A Convenient Category for Higher-Order Probability Theory. In *Logic in Computer Science (LICS'17)*.

K. H. Hofmann and M. Mislove. 1981. Local compactness and continuous lattices. In *Continuous Lattices*.

N. Jansen, B. L. Kaminski, J.-P. Katoen, F. Olmedo, F. Gretz, and A. K. McIver. 2015. Conditioning in Probabilistic Programming. *Electr. Notes Theor. Comp. Sci.* 319 (December 2015).

C. Jones. 1989. *Probabilistic Non-determinism*. Ph.D. Dissertation. University of Edinburgh.

C. Jones and G. Plotkin. 1989. A Probabilistic Powerdomain of Evaluations. In *Logic in Computer Science (LICS'89)*.

A. Jung and R. Tix. 1998. The Troublesome Probabilistic Powerdomain. *Electr. Notes Theor. Comp. Sci.* 13 (1998).

B. L. Kaminski, J.-P. Katoen, C. Matheja, and F. Olmedo. 2016. Weakest Precondition Reasoning for Expected Run—Times of Probabilistic Programs. In *European Symp. on Programming (ESOP'16)*.

J.-P. Katoen, A. K. McIver, L. A. Meinicke, and C. C. Morgan. 2010. Linear-Invariant Generation for Probabilistic Programs: Automated Support for Proof-Based Methods. In *Static Analysis Symp. (SAS'10)*.

M. Kattenbelt, M. Kwiatkowska, G. Norman, and D. Parker. 2009. Abstraction Refinement for Probabilistic Software. In *Verif., Model Checking, and Abs. Interp. (VMCAI'09)*.

S. C. Kleene. 1951. Representation of Events in Nerve Nets and Finite Automata. Available on https://www.rand.org/pubs/research_memoranda/RM704.html.

D. Kozen. 1981a. On induction vs. *-continuity. In *Workshop on Logic of Programs*.

D. Kozen. 1981b. Semantics of Probabilistic Programs. *J. Comput. Syst. Sci.* 22 (June 1981). Issue 3.

D. Kozen. 1985. A Probabilistic PDL. *J. Comput. Syst. Sci.* 30 (April 1985). Issue 2.

D. Kozen. 1991. A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events. *J. Information and Computation* 110 (May 1991). Issue 2.

A. Lal, T. Touili, N. Kidd, and T. Reps. 2008. Interprocedural Analysis of Concurrent Programs Under a Context Bound. In *Tools and Algs. for the Construct. and Anal. of Syst. (TACAS'08)*.

A. K. McIver and C. C. Morgan. 2001. Partial correctness for probabilistic demonic programs. *Theor. Comp. Sci.* 266 (September 2001). Issue 1.

A. K. McIver and C. C. Morgan. 2005. *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer Science+Business Media, Inc.

M. Mislove. 1998. Topology, domain theory and theoretical computer science. *Topology and its Applications* 89 (November 1998). Issue 1.

M. Mislove. 2000. Nondeterminism and Probabilistic Choice: Obeying the Laws. In *Concurrency Theory*.

M. Mislove, J. Ouaknine, and J. Worrell. 2004. Axioms for Probability and Nondeterminism. *Electr. Notes Theor. Comp. Sci.* 96 (June 2004).

D. Monniaux. 2000. Abstract Interpretation of Probabilistic Semantics. In *Static Analysis Symp. (SAS'00)*.

D. Monniaux. 2003. Abstract Interpretation of Programs as Markov Decision Processes. In *Static Analysis Symp. (SAS'03)*.

M. Müller-Olm and H. Seidl. 2004. Precise Interprocedural Analysis through Linear Algebra. In *Princ. of Prog. Lang. (POPL'04)*.

F. Olmedo, B. L. Kaminski, J.-P. Katoen, and C. Matheja. 2016. Reasoning about Recursive Probabilistic Programs. In *Logic in Computer Science (LICS'16)*.

B. Paige and F. Wood. 2014. A Compilation Target for Probabilistic Programming Languages. In *Int. Conf. on Machine Learning (ICML'14)*.

S. Sankaranarayanan, A. Chakarov, and S. Gulwani. 2013. Static Analysis for Probabilistic Programs: Inferring Whole Program Properties from Finitely Many Paths. In *Prog. Lang. Design and Impl. (PLDI'13)*.

S. Smolka, P. Kumar, N. Foster, D. Kozen, and A. Silva. 2017. Cantor meets Scott: Semantic Foundations for Probabilistic Networks. In *Princ. of Prog. Lang. (POPL'17)*.

S. Staton. 2017. Commutative Semantics for Probabilistic Programming. In *European Symp. on Programming (ESOP'17)*.

S. Staton, H. Yang, C. Heunen, and O. Kammar. 2016. Semantics for probabilistic programming: higher-order functions, continuous distributions, and soft constraints. In *Logic in Computer Science (LICS'16)*.

R. E. Tarjan. 1981. A Unified Approach to Path Problems. *J. ACM* 28 (July 1981). Issue 3.

R. Tix, K. Keimel, and G. Plotkin. 2009. Semantic Domains for Combining Probability and Non-Determinism. *Electr. Notes Theor. Comp. Sci.* 222 (February 2009).

M. Vákár, O. Kammar, and S. Staton. 2019. A Domain Theory for Statistical Probabilistic Programming. In *Princ. of Prog. Lang. (POPL'19)*.

D. Wang, J. Hoffmann, and T. Reps. 2018. PMAF: An Algebraic Framework for Static Analysis of Probabilistic Programs. In *Prog. Lang. Design and Impl. (PLDI'18)*.

A Proofs

A.1 Thm. 4.1

Proof. We equip X with the discrete topology. We define $X_\perp = X \cup \{\perp\}$ with a distinguished least element $\perp$ and thus $X_\perp$ is a flat domain. Then $X_\perp$ is a bounded-complete domain. The Scott-compact subsets of $X_\perp$ are precisely finite subsets of X and all subsets that contain $\perp$. Thus $X_\perp$ is coherent. By [Abramsky and Jung 1994, Ex. 4.3.11.14], we know that $X_\perp$ is an FS-domain.

By Prop. 3.3 we know that $\underline{\mathcal{D}}(X)$ is coherent. Moreover, $\underline{\mathcal{D}}(X)$ is also bounded-complete. Thus $\underline{\mathcal{D}}(X)$ is an FS-domain. By [Abramsky and Jung 1994, Thm. 4.2.11], we know that $[X_\perp \to \underline{\mathcal{D}}(X)]$ is an FS-domain.

Let $s \overset{\text{def}}{=} \lambda f.f$ and $r \overset{\text{def}}{=} \lambda g.\lambda x.\textbf{if } x = \perp \textbf{ then } \perp_D \textbf{ else } g(x)$. Then $s : [X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)] \to [X_\perp \to \underline{\mathcal{D}}(X)]$, $r : [X_\perp \to \underline{\mathcal{D}}(X)] \to [X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$, and $r \circ s$ is the identity on $[X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$, where $[A \xrightarrow{\perp!} B]$ stands for continuous functions from a dcpo A to a dcpo B that preserve the least element. Hence $[X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$ is a retract of $[X_\perp \to \underline{\mathcal{D}}(X)]$. By [Abramsky and Jung 1994, Prop. 4.2.12], we know that $[X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$ is also an FS-domain.

For any f in $[X \to \underline{\mathcal{D}}(X)]$, we could define a function $g \overset{\text{def}}{=} \lambda x.\textbf{if } x = \perp \textbf{ then } \perp_D \textbf{ else } f(x)$. For any g in $[X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$, we could define a function $f \overset{\text{def}}{=} \lambda x.g(x)$. Thus $[X \to \underline{\mathcal{D}}(X)]$ is homeomorphic to $[X_\perp \xrightarrow{\perp!} \underline{\mathcal{D}}(X)]$, and we know that $[X \to \underline{\mathcal{D}}(X)]$ is also an FS-domain. By [Abramsky and Jung 1994, Thm. 4.2.18], we know that $[X \to \underline{\mathcal{D}}(X)]$ is coherent. Because the topology on X is discrete, $[X \to \underline{\mathcal{D}}(X)]$ is precisely $X \to \underline{\mathcal{D}}(X)$. Thus we conclude that $\underline{\mathcal{K}}(X)$ is coherent. □

A.2 Lem. 4.2

Proof.

1. Monotonicity is trivial. It then suffices to show that for all directed set $A \subseteq \underline{\mathcal{K}}(X)$, $\phi \cdot (\bigsqcup^\uparrow A) = \bigsqcup^\uparrow_{\kappa \in A} \phi \cdot \kappa$. Let $\kappa' \overset{\text{def}}{=} \bigsqcup^\uparrow A$. We conclude the proof by $\bigsqcup^\uparrow_{\kappa \in A} \phi(x) \cdot \kappa(x) = \phi(x) \cdot \bigsqcup^\uparrow_{\kappa \in A} \kappa(x) = \phi(x) \cdot (\bigsqcup^\uparrow A)(x) = \phi(x) \cdot \kappa'(x)$ for any x.
2. Monotonicity is trivial.

   Left-Scott-continuity. For all directed set $A \subseteq \underline{\mathcal{K}}(X)$ and all $\rho \in \underline{\mathcal{K}}(X)$, we want to show that $(\bigsqcup^\uparrow A) \otimes \rho = \bigsqcup^\uparrow_{\kappa \in A} \kappa \otimes \rho$. Let $\kappa' \overset{\text{def}}{=} \bigsqcup^\uparrow A$. Then it is sufficient to show that for all x and x'', $\int \kappa'(x)(dx')\rho(x')(x'') = \bigsqcup^\uparrow_{\kappa \in A} \int \kappa(x)(dx')\rho(x')(x'')$. Because A is directed and $\underline{\mathcal{K}}(X)$ is ordered pointwise, $\{\kappa(x) \mid \kappa \in A\}$ is also directed in $\underline{\mathcal{D}}(X)$. By [Jones and Plotkin 1989, Thm. 3.3] , the right-hand-side is equal to $\int (\bigsqcup^\uparrow_{\kappa \in A} \kappa(x))(dx')\rho(x')(x'')$. We conclude the proof by $\kappa'(x) = \bigsqcup^\uparrow_{\kappa \in A} \kappa(x)$ by the definition of κ'.

   Right-Scott-continuity. For all directed set $A \subseteq \underline{\mathcal{K}}(X)$ and all $\rho \in \underline{\mathcal{K}}(X)$, we want to show that $\rho \otimes (\bigsqcup^\uparrow A) = \bigsqcup^\uparrow_{\kappa \in A} \rho \otimes \kappa$. Let $\kappa' \overset{\text{def}}{=} \bigsqcup^\uparrow A$. Then it is sufficient to show that for all x and x'', $\int \rho(x)(dx')\kappa'(x')(x'') = \bigsqcup^\uparrow_{\kappa \in A} \int \rho(x)(dx')\kappa(x')(x'')$. Because A is directed and $\underline{\mathcal{K}}(X)$ as well as $\underline{\mathcal{D}}(X)$ are ordered pointwise, $\{\lambda x'.\kappa(x')(x'') \mid \kappa \in A\}$ is directed and bounded. By [Jones and Plotkin 1989, Thm. 3.1], the right-hand-side is equal to $\int \rho(x)(dx')(\bigsqcup^\uparrow_{\kappa \in A} \lambda x'.\kappa(x')(x''))(x')$. We conclude the proof by $\lambda x'.\kappa'(x')(x'') = \bigsqcup^\uparrow_{\kappa \in A} \lambda x'.\kappa(x')(x'')$ by the definition of κ'.

□

A.3 Lem. 4.4

Proof. 1. Straightforward by the fact that if $\kappa_i \sqsubseteq_K \rho_i$ for all $i \in \mathbb{N}$, then $\sum_{i=0}^{\infty} \phi_i \cdot \kappa_i \sqsubseteq_K \sum_{i=0}^{\infty} \phi_i \cdot \rho_i$.

2. The Scott-closure of A can be obtained by $\overline{A} = \{\bigsqcup^{\uparrow} B \mid B \subseteq \downarrow A, B \text{ directed}\}$ [Tix et al. 2009]. For any $\{\kappa_i\}_{i \in \mathbb{N}^+} \subseteq \overline{A}$, there are directed subsets B_i of $\downarrow A$ such that $\kappa_i = \bigsqcup^{\uparrow} B_i$ for all $i \in \mathbb{N}^+$. For any $\{\phi_i\}_{i \in \mathbb{N}^+} \subseteq \mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \phi_i = \dot{1}$, we have

$$
\begin{aligned}
\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i &= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i \cdot \kappa_i \\
&= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i \cdot \left(\bigsqcup\nolimits^{\uparrow} B_i\right) \\
&= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \bigsqcup\nolimits^{\uparrow}_{\rho_i \in B_i} \phi_i \cdot \rho_i \\
&= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \bigsqcup\nolimits^{\uparrow}_{\forall i : \rho_i \in B_i} \sum_{i=1}^{n} \phi_i \cdot \rho_i \\
&= \bigsqcup\nolimits^{\uparrow}_{\forall i : \rho_i \in B_i} \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i \cdot \rho_i \\
&= \bigsqcup\nolimits^{\uparrow}_{\forall i : \rho_i \in B_i} \sum_{i=1}^{\infty} \phi_i \cdot \rho_i
\end{aligned}
$$

where $\sum_{i=1}^{\infty} \phi_i \cdot \rho_i$ is indeed contained in $\downarrow A$ by its g-convexity and hence $\{\sum_{i=1}^{\infty} \phi_i \cdot \rho_i \mid \forall i : \rho_i \in B_i\}$ is a directed subset of $\downarrow A$, thus $\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i$ is contained in $\overline{A}$.

□

A.4 Lem. 4.5

Proof. Let $\{\eta_i\}_{i\in\mathbb{N}^+}$ be any sequence in $\{\kappa \mathrel{}_\phi\!\diamond \rho \mid \kappa \in A \wedge \rho \in B\}$, and $\eta_i = \kappa_i \mathrel{}_\phi\!\diamond \rho_i$ such that $\kappa_i \in A, \rho_i \in B$ for all $i \in \mathbb{N}^+$. For any $\{\psi_i\}_{i\in\mathbb{N}^+} \subseteq \mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \psi_i = \dot{1}$, we have

$$
\begin{aligned}
\sum_{i=1}^{\infty} \psi_i \cdot \eta_i &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} \psi_i \cdot \eta_i \\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} \psi_i \cdot (\kappa_i \mathrel{}_\phi\!\diamond \rho_i) \\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} \psi_i \cdot (\phi \cdot \kappa_i + (\dot{1} - \phi) \cdot \rho_i) \\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} ((\psi_i \phi) \cdot \kappa_i + (\psi_i - \psi_i \phi) \cdot \rho_i) \\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} (\sum_{i=1}^{n} (\psi_i \phi) \cdot \kappa_i + \sum_{i=1}^{n} (\psi_i - \psi_i \phi) \cdot \rho_i) \\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} (\psi_i \phi) \cdot \kappa_i + \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} (\psi_i - \psi_i \phi) \cdot \rho_i \\
&= \phi \cdot \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} \psi_i \cdot \kappa_i + (\dot{1} - \phi) \cdot \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}} \sum_{i=1}^{n} \psi_i \cdot \rho_i \\
&= (\sum_{i=1}^{\infty} \psi_i \cdot \kappa_i) \mathrel{}_\phi\!\diamond (\sum_{i=1}^{\infty} \psi_i \cdot \rho_i).
\end{aligned}
$$

Because A and B are g-convex, we know that $\sum_{i=0}^{\infty} \psi_i \cdot \kappa_i \in A$ and $\sum_{i=1}^{\infty} \psi_i \cdot \rho_i \in B$. Hence $\sum_{i=1}^{\infty} \psi_i \cdot \eta_i$ is contained in $\{\kappa \mathrel{}_\phi\!\diamond \rho \mid \kappa \in A \wedge \rho \in B\}$. □

A.5 Lem. 4.7

Proof. It is straightforward to show that $gconv(A)$ is a superset of the right-hand-side. Then we want to show the right-hand-side is indeed g-convex, which indicates the desired equality by the definition of $gconv(A)$.

Suppose $\{\kappa_i\}_{i\in\mathbb{N}^+}$ are contained in the right-hand-side. Then for all $i \in \mathbb{N}^+$, there exists $\{\kappa_{i,j}\}_{j\in\mathbb{N}^+} \subseteq A$ and $\{\phi_{i,j}\}_{j\in\mathbb{N}^+}$ such that $\sum_{j=1}^{\infty} \phi_{i,j} = \dot{1}$ and $\kappa_i = \sum_{j=1}^{\infty} \phi_{i,j} \cdot \kappa_{i,j}$. It is sufficient to show that for all

$\{\phi_i\}_{i\in\mathbb{N}^+}, \sum_{i=1}^{\infty}\phi_i\cdot\kappa_i$ is contained in the right-hand-side. We have

$$\begin{aligned}\sum_{i=1}^{\infty}\phi_i\cdot\kappa_i &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\kappa_i\\ &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\sum_{j=1}^{\infty}\phi_{i,j}\cdot\kappa_{i,j}\\ &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\bigsqcup\nolimits^{\uparrow}_{m\in\mathbb{N}}\sum_{j=1}^{m}\phi_{i,j}\cdot\kappa_{i,j}\\ &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N},m\in\mathbb{N}}\sum_{1\le i\le n,1\le j\le m}(\phi_i\phi_{i,j})\cdot\kappa_{i,j}.\end{aligned}$$

Let $\theta:\mathbb{N}^+\times\mathbb{N}^+\to\mathbb{N}^+$ be a bijection. Let $\rho_k \overset{\text{def}}{=} \kappa_{i,j}$ and $\psi_k \overset{\text{def}}{=} \phi_i\phi_{i,j}$ such that $(i,j)=\theta^{-1}(k)$. Then $\sum_{k=1}^{\infty}\psi_k = \sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\psi_{\theta(i,j)} = \sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\phi_i\phi_{i,j} = \sum_{i=1}^{\infty}\phi_i\sum_{j=1}^{\infty}\phi_{i,j} = \sum_{i=1}^{\infty}\phi_i\cdot\dot{1} = \sum_{i=1}^{\infty}\phi_i = \dot{1}$. We now have

$$\begin{aligned}\bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N},m\in\mathbb{N}}\sum_{1\le i\le n,1\le j\le m}(\phi_i\phi_{i,j})\cdot\kappa_{i,j} &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N},m\in\mathbb{N}}\sum_{1\le i\le n,1\le j\le m}\psi_{\theta(i,j)}\cdot\rho_{\theta(i,j)}\\ &= \bigsqcup\nolimits^{\uparrow}_{l\in\mathbb{N}}\sum_{k=1}^{l}\psi_k\cdot\rho_k\\ &= \sum_{k=1}^{\infty}\psi_l\cdot\rho_l\end{aligned}$$

that is indeed contained in the right-hand-side. The second last equation is established as follows:

- To show $\bigsqcup^{\uparrow}_{n\in\mathbb{N},m\in\mathbb{N}}\sum_{1\le i\le n,1\le j\le m}\psi_{\theta(i,j)}\cdot\rho_{\theta(i,j)} \sqsubseteq_K \bigsqcup^{\uparrow}_{l\in\mathbb{N}}\sum_{k=1}^{l}\psi_k\cdot\rho_k$: Fix $n_o\in\mathbb{N}$ and $m_o\in\mathbb{N}$. Let $l_o \overset{\text{def}}{=} \max_{1\le i\le n_o,1\le j\le m_o}\theta(i,j)$. Then we conclude by $\sum_{1\le i\le n_o,1\le j\le m_o}\psi_{\theta(i,j)}\cdot\rho_{\theta(i,j)} \sqsubseteq_K \sum_{k=1}^{l_o}\psi_k\cdot\rho_k$.
- To show $\bigsqcup^{\uparrow}_{l\in\mathbb{N}}\sum_{k=1}^{l}\psi_k\cdot\rho_k \sqsubseteq_K \bigsqcup^{\uparrow}_{n\in\mathbb{N},m\in\mathbb{N}}\sum_{1\le i\le n,1\le j\le m}\psi_{\theta(i,j)}\cdot\rho_{\theta(i,j)}$: Fix $l_o\in\mathbb{N}$. Let $n_o \overset{\text{def}}{=} \max_{1\le k\le l_o}\theta^{-1}(k).\mathbf{fst}$ and $m_o \overset{\text{def}}{=} \max_{1\le k\le l_o}\theta^{-1}(k).\mathbf{snd}$. Then we conclude by $\sum_{k=1}^{l_o}\psi_k\cdot\rho_k \sqsubseteq_K \sum_{1\le i\le n_o,1\le j\le m_o}\psi_{\theta(i,j)}\cdot\rho_{\theta(i,j)}$.

□

A.6 Lem. 4.8

Proof. 1. The $\subseteq$-direction is straightforward. For the $\supseteq$-direction, we have

$$gconv(\overline{A}) = \{\sum_{i=1}^{\infty}\phi_i\cdot\kappa_i \mid \{\kappa_i\}_{i\in\mathbb{N}^+}\subseteq\overline{A}\wedge\{\phi_i\}_{i\in\mathbb{N}^+}\subseteq\mathbb{W}(X)\wedge\sum_{i=1}^{\infty}\phi_i=\dot{1}\}$$

by Lem. 4.7 and $\overline{A} = \{\bigsqcup^{\uparrow}B \mid B\subseteq{\downarrow}A, B \text{ directed}\}$. Let $\kappa \overset{\text{def}}{=} \sum_{i=1}^{\infty}\phi_i\cdot\kappa_i$ be an element of $gconv(\overline{A})$ where $\{\kappa_i\}_{i\in\mathbb{N}^+}\subseteq\overline{A}$. Then for all $i\in\mathbb{N}^+$, there exists a directed $B_i\subseteq{\downarrow}A$ satisfying $\kappa_i = \bigsqcup^{\uparrow}B_i$.

Then we have

$$\begin{aligned}
\sum_{i=1}^{\infty}\phi_i\cdot\kappa_i &= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\kappa_i\\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\bigsqcup\nolimits^{\uparrow}B_i\\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\bigsqcup\nolimits^{\uparrow}_{\rho_i\in B_i}(\phi_i\cdot\rho_i)\\
&= \bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\bigsqcup\nolimits^{\uparrow}_{\forall i:\rho_i\in B_i}\sum_{i=1}^{n}\phi_i\cdot\rho_i\\
&= \bigsqcup\nolimits^{\uparrow}_{\forall i:\rho_i\in B_i}\bigsqcup\nolimits^{\uparrow}_{n\in\mathbb{N}}\sum_{i=1}^{n}\phi_i\cdot\rho_i\\
&= \bigsqcup\nolimits^{\uparrow}_{\forall i:\rho_i\in B_i}\sum_{i=1}^{\infty}\phi_i\cdot\rho_i.
\end{aligned}$$

Because $\rho_i\in B_i\subseteq{\downarrow}A$, there exists $\eta_i\in A$ satisfying $\rho_i\sqsubseteq_K\eta_i$ for all $i\in\mathbb{N}^+$, and thus $\sum_{i=1}^{\infty}\phi_i\cdot\eta_i\in gconv(A)$. We also know that $\sum_{i=1}^{\infty}\phi_i\cdot\rho_i\sqsubseteq_K\sum_{i=1}^{\infty}\phi_i\cdot\eta_i$, thus $\sum_{i=1}^{\infty}\phi_i\cdot\rho_i\in{\downarrow}gconv(A)$. Therefore $\sum_{i=1}^{\infty}\phi_i\cdot\kappa_i\in\overline{gconv(A)}$. By $gconv(\overline{A})\subseteq\overline{gconv(A)}$ we conclude that $\overline{gconv(\overline{A})}\subseteq\overline{gconv(A)}$.

2. For the $\supseteq$-direction, we have

$$\begin{aligned}
&gconv(\bigcup A_i)\supseteq gconv(A_i)\\
\Longrightarrow\ &\overline{gconv(\bigcup A_i)}\supseteq\overline{gconv(A_i)}\\
\Longrightarrow\ &\overline{gconv(\bigcup A_i)}\supseteq\bigcup\overline{gconv(A_i)}\\
\Longrightarrow\ &\overline{gconv(\bigcup A_i)}\supseteq\overline{\bigcup\overline{gconv(A_i)}}.
\end{aligned}$$

For the $\subseteq$-direction, we know that

$$gconv(\bigcup A_i)=\{\sum_{j=1}^{\infty}\phi_j\cdot\kappa_j\mid\{\kappa_j\}_{j\in\mathbb{N}^+}\subseteq\bigcup A_i\wedge\{\phi_j\}_{j\in\mathbb{N}^+}\subseteq\mathbb{W}(X)\wedge\sum_{j=1}^{\infty}\phi_j=\dot{1}\}$$

by Lem. 4.7. Let $\kappa\overset{\text{def}}{=}\sum_{j=1}^{\infty}\phi_j\cdot\kappa_j$ be an element of $gconv(\bigcup A_i)$ where $\{\kappa_j\}_{j\in\mathbb{N}}\subseteq\bigcup A_i$. For all $n\in\mathbb{N}$, because $\{A_i\}_{i\in\mathcal{I}}$ is directed, there exists $A_{o(n)}$ satisfying $\{\kappa_1,\cdots,\kappa_n\}\subseteq A_{o(n)}$. Thus $\sum_{j=1}^{n}\phi_j\cdot\kappa_j\in\overline{gconv(A_{o(n)})}$. By the definition of Scott-closure, we know that $\bigsqcup^{\uparrow}_{n\in\mathbb{N}}\sum_{j=1}^{n}\phi_j\cdot\kappa_j\in\overline{\bigcup\overline{gconv(A_i)}}$. Thus κ is contained in the right-hand-side and $gconv(\bigcup A_i)\subseteq\overline{\bigcup\overline{gconv(A_i)}}$. Hence we conclude that $\overline{gconv(\bigcup A_i)}\subseteq\overline{\bigcup\overline{gconv(A_i)}}$.

□

A.7 Lem. 4.9

Proof. $[0,1]$ equipped with its usual linear order forms a Scott-compact topology. By Tychonoff's theorem we know that $X\to[0,1]$ with the product topology is a Scott-compact space. Hence

$\Gamma \stackrel{\text{def}}{=} \{(\phi, \dot{1} - \phi) \mid \phi \in \mathbb{W}(X)\}$ is also a Scott-compact space. The map from $\Gamma \times \underline{\mathcal{K}}(X) \times \underline{\mathcal{K}}(X)$ to $\underline{\mathcal{K}}(X)$ defined by $((\phi, \dot{1} - \phi), \kappa_1, \kappa_2) \mapsto \kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2$ is Scott-continuous. By Cor. 4.6 we know that $gconv(A \cup B)$ is precisely the image of the Scott-compact set $\Gamma \times A \times B$. Because Scott-continuous functions preserve Scott-compactness, we conclude that $gconv(A \cup B)$ is also Scott-compact. □

A.8 Lem. 4.10

Proof. 1. Let $x \in X$, $\kappa_1, \kappa_2 \in A$, and $p \in [0,1]$. We want to show that $p \cdot \kappa_1(x) + (1-p) \cdot \kappa_2(x) \in \{\kappa(x) \mid \kappa \in A\}$. Let $\phi \stackrel{\text{def}}{=} \lambda x.p$. Then $\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2 \in A$ because of g-convexity. We conclude the proof by $(\kappa_1 \,{}_{\phi}\!\diamond\, \kappa_2)(x) = \phi(x) \cdot \kappa_1(x) + (1 - \phi(x)) \cdot \kappa_2(x) = p \cdot \kappa_1(x) + (1-p) \cdot \kappa_2(x)$.

2. Let $x \in X$. Let $F(\kappa) \stackrel{\text{def}}{=} \kappa(x)$ be a map from $\underline{\mathcal{K}}(X)$ to $\underline{\mathcal{D}}(X)$. Because F is Scott-continuous and Scott-continuous functions preserve Scott-compactness, we conclude that $F(A)$ is Scott-compact because A is Scott-compact.

3. Straightforward by the fact that $\underline{\mathcal{K}}(X) = X \to \underline{\mathcal{D}}(X)$ and $\underline{\mathcal{K}}(X)$ is ordered pointwise.

□

A.9 Lem. 4.11

Proof. We claim that there exists $x \in X$ such that $K(x) \cap A(x) = \emptyset$.

If not, then for all $x \in X$ there is $K(x) \cap A(x) \neq \emptyset$. Hence we can define a kernel κ such that $\kappa(x) \in K(x) \cap A(x)$ for every x. We want to show that $\kappa \in A$ and $\kappa \in K$. This follows from g-convexity of A and K: suppose $\kappa(x) = \kappa_x(x)$ such that $\kappa_x \in K$ for all x, then $\kappa = \sum_{x \in X} (\lambda x'.[x = x']) \cdot \kappa_x$. This contradicts the fact that K and A are disjoint.

Let $x \in X$ such that $K(x) \cap A(x) = \emptyset$. By Lem. 4.10(ii)(iii) we know that $K(x)$ is Scott-compact and $A(x)$ is Scott-closed. By [Tix et al. 2009, Thm. 3.8] we know that there exist a Scott-continuous linear map F and an a in $\overline{\mathbb{R}_0^+}$ such that $F(\mu) > a > 1 \geq F(\nu)$ for all μ in $K(x)$ and ν in $A(x)$. Let $V \stackrel{\text{def}}{=} \{\kappa \mid F(\kappa(x)) > a\}$ be a Scott-open subset of $\underline{\mathcal{K}}(X)$. Then we know that $K \subseteq V$ and $A \cap V = \emptyset$. Then it suffices to show that V is g-convex. For any $\{\kappa_i\}_{i \in \mathbb{N}^+} \subseteq V$ and $\{\phi_i\}_{i \in \mathbb{N}^+} \subseteq \mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \phi_i = \dot{1}$. Then

$$
\begin{aligned}
F((\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i)(x)) &= F(\sum_{i=1}^{\infty} \phi_i(x) \cdot \kappa_i(x)) \\
&= F(\bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i(x) \cdot \kappa_i(x)) \\
&= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} F(\sum_{i=1}^{n} \phi_i(x) \cdot \kappa_i(x)) \\
&= \bigsqcup\nolimits^{\uparrow}_{n \in \mathbb{N}} \sum_{i=1}^{n} \phi_i(x) \cdot F(\kappa_i(x)) \\
&> a
\end{aligned}
$$

hence $\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i \in V$. □

A.10 Lem. 4.12

Proof. It suffices to show that any open-cover of K is an open-cover of $gconv(K)$. Let $\mathcal{C}$ be an open-cover of K. Let $U = \bigcup \mathcal{C}$. If $gconv(K)$ is not contained in U, then by Lem. 4.7, there exist

$\{\kappa_i\}_{i\in\mathbb{N}^+} \subseteq K$ and $\{\phi_i\}_{i\in\mathbb{N}^+} \subseteq \mathbb{W}(X)$ such that $\sum_{i=1}^{\infty} \phi_i = \dot{1}$ and $\kappa \overset{\text{def}}{=} \sum_{i=1}^{\infty} \phi_i \cdot \kappa_i \in gconv(K) \setminus U$. Let $A = \downarrow\kappa$ be a Scott-closed set, then A is disjoint from U, and thus disjoint from K. Similar to the proof of Lem. 4.11, we claim that there exist $x \in X$ and a Scott-continuous linear map F and an $a \in \overline{\mathbb{R}_0^+}$ such that $F(\mu) > a > 1 \geq F(\nu)$ for all μ in $K(x)$ and $\nu \in A(x)$. Then $F(\kappa(x)) = F((\sum_{i=1}^{\infty} \phi_i \cdot \kappa_i)(x)) = F(\sum_{i=1}^{\infty} \phi_i(x) \cdot \kappa_i(x)) = \bigsqcup^{\uparrow}_{n\in\mathbb{N}} F(\sum_{i=1}^{n} \phi_i(x) \cdot \kappa_i(x)) = \bigsqcup^{\uparrow}_{n\in\mathbb{N}} \phi_i(x) \cdot F(\kappa_i(x)) > a > 1$, but because $\kappa \in A$ we also know that $F(\kappa(x)) \leq 1$. We then conclude the proof by contradiction. □

A.11 Thm. 4.13

Proof. It is straightforward to show that $\langle \mathcal{GK}(X), \sqsubseteq_G \rangle$ forms a poset and $\perp_G$ is the least element. Then it suffices to show the powerdomain admits directed suprema. For a directed collection $\mathcal{A} = \{A_i\}_{i\in\mathcal{I}} \subseteq \mathcal{GK}(X)$, we define $\bigsqcup^{\uparrow}_i A_i \overset{\text{def}}{=} \overline{\bigcup_i \downarrow A_i} \cap \bigcap_i \uparrow A_i$. We now show $\bigsqcup^{\uparrow}_i A_i$ is indeed the least upper bound of $\mathcal{A}$.

We already know $\underline{\mathcal{K}}(X)$ is coherent by Thm. 4.1. Observe that $\bigsqcup^{\uparrow}_i A_i = \overline{\bigcup_i \downarrow A_i} \cap \bigcap_i \uparrow A_i = \bigcap_i (\overline{\bigcup \uparrow A_i} \cap \uparrow A_i)$ and $\{\overline{\bigcup \uparrow A_i} \cap \uparrow A_i\}_{i\in\mathcal{I}}$ is a filtered family of nonempty lenses, or more generally, nonempty Lawson-closed subsets thus nonempty Lawson-compact subsets because of the coherence of $\underline{\mathcal{K}}(X)$. By Prop. 3.2 we know the filtered family admits a nonempty intersection. Thus $\bigsqcup^{\uparrow}_i A_i$ is a nonempty lens that is indeed g-convex by Lem. 4.4 and the g-convexity of A_i's. In this way we show that $\bigsqcup^{\uparrow}_i A_i \in \mathcal{GK}(X)$.

Let $B \overset{\text{def}}{=} \bigsqcup^{\uparrow}_i A_i$. To show that B is the least upper bound of $\mathcal{A}$, we claim that $\downarrow B = \overline{\bigcup_i \downarrow A_i}$ and $\uparrow B = \bigcap_i \uparrow A_i$. If so, then B is obviously an upper bound of $\mathcal{A}$ and if $A_i \sqsubseteq_G B'$ for all $i \in \mathcal{I}$, then $\downarrow A_i \subseteq \downarrow B'$ and $\uparrow A_i \supseteq \uparrow B'$ for all $i \in \mathcal{I}$, thus $\downarrow B = \overline{\bigcup_i \downarrow A_i} \subseteq \downarrow B'$ and $\uparrow B = \bigcap_i \uparrow A_i \supseteq \uparrow B'$, or equivalently, $B \sqsubseteq_G B'$. Since B' is arbitrarily chosen, we can conclude that B is the least upper bound of $\mathcal{A}$. We adapt proofs from [Tix et al. 2009] as follows.

- To show $\downarrow B = \overline{\bigcup_i \downarrow A_i}$: Inclusion is trivial. For the reverse inclusion, it is sufficient to show $\downarrow B \supseteq \bigcup_i \downarrow A_i$ since $\downarrow B$ is Scott-closed. Fix $x \in \downarrow A_i$ for some $i \in \mathcal{I}$. Then there exists $y \in A_i$ such that $x \sqsubseteq_K y$. For all $j \in \mathcal{I}$ satisfying $A_i \sqsubseteq_G A_j$, there exists $z \in A_j$ such that $y \sqsubseteq_K z$. Therefore $\uparrow x \cap \overline{\bigcup_i \downarrow A_i} \cap \uparrow A_j \neq \emptyset$. Again a filtered family of nonempty Lawson-compact sets admits a nonempty intersection by Prop. 3.2, we have $\uparrow x \cap \overline{\bigcup_i \downarrow A_i} \cap \bigcap_j \uparrow A_j \neq \emptyset$, i.e., $\uparrow x \cap B \neq \emptyset$, thus $x \in \downarrow B$.
- To show $\uparrow B = \bigcap_i \uparrow A_i$: Inclusion is trivial. For the reverse inclusion, fix $x \in \bigcap_i \uparrow A_i$. Then we have $\downarrow x \cap \overline{\bigcup_i \downarrow A_i} \cap \uparrow A_j \neq \emptyset$ for all $j \in \mathcal{I}$. By a similar reasoning to the previous case we have $\downarrow x \cap \overline{\bigcup_i \downarrow A_i} \cap \bigcap_j \uparrow A_j \neq \emptyset$, i.e., $\downarrow x \cap B \neq \emptyset$, thus $x \in \uparrow B$.

□

A.12 Lem. 4.14

Proof. The only nontrivial part of the proof is to show $\otimes_G$ preserves directed suprema. Firstly we claim that $\downarrow(A \otimes_G B) = \overline{gconv(\{a \otimes b \mid a \in \downarrow A \wedge b \in \downarrow B\})}$ and $\uparrow(A \otimes_G B) = \uparrow gconv(\{a \otimes b \mid a \in \uparrow A \wedge b \in \uparrow B\})$. Let's write $A \dot{\otimes} B$ for $\{a \otimes b \mid a \in A \wedge b \in B\}$.

- To show $\downarrow(A \otimes_G B) = \overline{gconv(\downarrow A \dot{\otimes} \downarrow B)}$: Inclusion is trivial. For the reverse inclusion, we have $\overline{gconv(\downarrow A \dot{\otimes} \downarrow B)} \subseteq \overline{gconv(\downarrow(A \dot{\otimes} B))} = \overline{gconv(\overline{\downarrow(A \dot{\otimes} B)})} = \overline{gconv(\overline{A \dot{\otimes} B})} = \overline{gconv(A \dot{\otimes} B)} \subseteq \downarrow(A \otimes_G B)$ by Lem. 4.8(i) and Lawson-compactness of $A \otimes_G B$.
- To show $\uparrow(A \otimes_G B) = \uparrow gconv(\uparrow A \dot{\otimes} \uparrow B)$: Inclusion is trivial. For the reverse inclusion, we have $\uparrow gconv(\uparrow A \dot{\otimes} \uparrow B) \subseteq \uparrow gconv(\uparrow(A \dot{\otimes} B)) \subseteq \uparrow gconv(A \dot{\otimes} B) \subseteq \uparrow(A \otimes_G B)$.

Then it suffices to show that $\otimes_G$ is Scott-continuous in the space of down-closures (i.e., $\{\downarrow A \mid A \in \mathcal{GK}(X)\}$), as well as in the space of up-closures (i.e., $\{\uparrow A \mid A \in \mathcal{GK}(X)\}$).

- Let a directed family $\{A_i\}_{i\in\mathcal{I}}$ (ordered by inclusion) and B be nonempty Scott-closed g-convex subsets of $\underline{\mathcal{K}}(X)$. We want to show that $\overline{gconv(\overline{\bigcup A_i}\dot{\otimes}B)} = \overline{\bigcup \overline{gconv(A_i\dot{\otimes}B)}}$, i.e., the left-Scott-continuity. Indeed, we have $\overline{gconv(\overline{\bigcup A_i}\dot{\otimes}B)} = \overline{gconv(\overline{\bigcup A_i}\dot{\otimes}B)} = \overline{gconv(\overline{(\bigcup A_i)\dot{\otimes}B})} = \overline{gconv((\bigcup A_i)\dot{\otimes}B)} = \overline{gconv(\bigcup(A_i\dot{\otimes}B))} = \overline{\bigcup gconv(A_i\dot{\otimes}B)}$ by Lem. 4.8 and Scott-continuity of $\otimes$ from Lem. 4.2(ii). The right-Scott-continuity is proved in a similar way.
- Let a directed family $\{A_i\}_{i\in\mathcal{I}}$ (ordered by reverse inclusion) and B be nonempty Scott-compact saturated g-convex subsets of $\underline{\mathcal{K}}(X)$. We want to show that $\uparrow gconv((\bigcap A_i)\dot{\otimes}B) = \bigcap \uparrow gconv(A_i\dot{\otimes}B)$. Inclusion is trivial. For the reverse inclusion, choose any g-convex Scott-open set U containing $\uparrow gconv(\bigcap A_i\dot{\otimes}B)$. As every g-convex Scott-compact saturated subset of a dcpo is the intersection of its g-convex Scott-open neighborhoods (by Lem. 4.11), it suffices to prove that the right-hand-side is contained in U. Observe that $gconv((\bigcap A_i)\dot{\otimes}B) \subseteq U$ and also $(\bigcap A_i)\dot{\otimes}B \subseteq U$, as $\otimes$ is Scott-continuous by Lem. 4.2(ii) and $\bigcap A_i$ and B are Scott-compact saturated, we know that $\bigcap A_i$ and B have Scott-open neighborhoods V and W respectively such that $V\dot{\otimes}W \subseteq U$. Because $\bigcap A_i \subseteq V$, by Prop. 3.2 we know there is an i such that $A_i \subseteq V$. Therefore $A_i\dot{\otimes}B \subseteq V\dot{\otimes}W \subseteq U$, and because U is g-convex, we know $gconv(A_i\dot{\otimes}B) \subseteq U$. Recall that U is Scott-open, we conclude that $\bigcap \uparrow gconv(A_i\dot{\otimes}B) \subseteq U$. The right-Scott-continuity is proved in a similar way.

□

A.13 Lem. 4.15

Proof. It is straightforward to show that $\uplus_G$ is idempotent, commutative, and associative, i.e., $\uplus_G$ is a semilattice operation. Similar to the argument in the proof of Lem. 4.14, it suffices to show the Scott-continuity of $\uplus_G$ with respect to lower closures as well as upper closures.

- Let a directed family $\{A_i\}_{i\in\mathcal{I}}$ (ordered by inclusion) and B be nonempty Scott-closed g-convex subsets of $\underline{\mathcal{K}}(X)$. We want to show $\overline{gconv(\overline{\bigcup A_i} \cup B)} = \overline{\bigcup \overline{gconv(A_i \cup B)}}$. Indeed, we have $\overline{gconv(\overline{\bigcup A_i} \cup B)} = \overline{gconv(\overline{\overline{\bigcup A_i} \cup B})} = \overline{gconv(\overline{\bigcup A_i \cup B})} = \overline{gconv(\bigcup A_i \cup B)} = \overline{gconv(\bigcup(A_i \cup B))} = \overline{\bigcup \overline{gconv(A_i \cup B)}}$ by Lem. 4.8.
- Let a directed family $\{A_i\}_{i\in\mathcal{I}}$ (ordered by reverse inclusion) and B be nonempty Scott-compact saturated g-convex subsets of $\underline{\mathcal{K}}(X)$. We want to show that $\uparrow gconv((\bigcap A_i)\cup B) = \bigcap \uparrow gconv(A_i \cup B)$. Inclusion is trivial. For reverse inclusion, it suffices to show that for every open set U that is a neighborhood of $\uparrow gconv((\bigcap A_i) \cup B)$, we have U contains the right-hand-side as a subset by Lem. 4.11. Observe that $gconv((\bigcap A_i) \cup B) \subseteq U$ thus $(\bigcap A_i) \cup B \subseteq U$. Since $\bigcap A_i$ and B are Scott-compact saturated, there exist Scott-open neighborhoods V and W of $\bigcap A_i$ and B, respectively, such that $V \cup W \subseteq U$. Then by Prop. 3.2 we know that there exists $i \in \mathcal{I}$ such that $A_i \subseteq V$ by the fact that $\bigcap A_i \subseteq V$. Thus $A_i \cup B \subseteq V \cup W \subseteq U$. Recall that U is g-convex, we have $gconv(A_i \cup B) \subseteq U$. Moreover, U is Scott-open, thus saturated, hence we conclude that $\bigcap \uparrow gconv(A_i \cup B) \subseteq U$.

□

A.14 Lem. 5.6

Lemma A.1. *For any configuration $\langle v, \omega\rangle$, there is at most one Δ such that $\langle v, \omega\rangle \longrightarrow \Delta$.*

Proof. Straightforward. □

Lemma A.2. $\longrightarrow$ *is a kernel.*

Proof. Lem. A.1 tells us that $\longrightarrow$ can be seen as a function $\hat{\longrightarrow}$ defined as follows:

$$\hat{\longrightarrow}(x)(y) \stackrel{\text{def}}{=} \begin{cases} \Delta(y) & \text{if } x \longrightarrow \Delta \\ 0 & \text{otherwise} \end{cases}.$$

For any x, it is straightforward to show that $\hat{\longrightarrow}(x)$ is a distribution. □

Lemma A.3. $\longrightarrow_n$ *is a kernel for all* $n \in \mathbb{N}$.

Proof. By induction on n:

- $\longrightarrow_0$ can be seen as the everywhere-zero function $\hat{\longrightarrow}_0$ which is trivially a kernel.
- $\longrightarrow_{n+1}$ can be seen as the function defined as follows:

$$\hat{\longrightarrow}_{n+1}(\langle v, \omega\rangle)(\omega') \stackrel{\text{def}}{=} \begin{cases} [\omega = \omega'] & v = v^{\mathsf{exit}} \\ \displaystyle\sum_{\tau \in \mathrm{supp}(\Delta)} \Delta(\tau) \cdot \hat{\longrightarrow}_n(\tau)(\omega') & \langle v, \omega\rangle \longrightarrow \Delta \cdot \end{cases}$$

  For any x, it is straightforward to show that $\hat{\longrightarrow}_{n+1}(x)$ is a distribution given that $\hat{\longrightarrow}_n$ is a kernel.

□

Now we prove Lem. 5.6.

Proof. It is sufficient to show that

$$\lambda\omega.\ \sup_{n\in\mathbb{N}}\{\hat{\longrightarrow}_n\}(\langle v^{\mathsf{entry}}, \omega\rangle) = (\mathrm{lfp}^{\dot{\sqsubseteq}_K}_{\lambda v.\perp_K} F_P)(v^{\mathsf{entry}})$$

and we are instead going to show for all $n \in \mathbb{N}$ and $v \in V$ the following holds

$$\lambda\omega.\hat{\longrightarrow}_n(\langle v, \omega\rangle) = F_P^n(\lambda v.\perp_K)(v).$$

By induction on n, the base case is trivial because both sides compute to $\perp_K$. Suppose that for some n, the equality holds for all $v \in V$. Then for all $v \in V$, we want to show that

$$\lambda\omega.\hat{\longrightarrow}_{n+1}(\langle v, \omega\rangle) = F_P^{n+1}(\lambda v.\perp_K)(v).$$

- If v is not associated with any edges, then $\hat{\longrightarrow}_{n+1}(\langle v, \omega\rangle)(\omega') = [\omega = \omega']$ for all ω and ω'. The right-hand-side computes to $F_P(F_P^n(\lambda v.\perp_K))(v)$ and by the definition of F_P we know it is equal to $\lambda\omega.\lambda\omega'.[\omega = \omega']$.
- If v is associated with $e = \langle v, \{u_1, \cdots, u_k\}\rangle$, then we know $\lambda\omega.\hat{\longrightarrow}_n(\langle u_i, \omega\rangle) = F_P^n(\lambda v.\perp_K)(u_i)$ for all i by induction hypothesis.
  - If $Ctrl(e) = seq[\mathrm{act}]$, then the right-hand-side is equal to $[\![\mathrm{act}]\!] \otimes F_P^n(\lambda v.\perp_K)(u_1)$. The left-hand-side is

$$\begin{aligned} & \lambda\omega.\lambda\omega'.\sum_{\tau} \hat{\longrightarrow}(\langle v, \omega\rangle)(\tau) \cdot \hat{\longrightarrow}_n(\tau)(\omega') \\ = \ & \lambda\omega.\lambda\omega'.\sum_{\omega''} [\![\mathrm{act}]\!](\omega)(\omega'') \cdot \hat{\longrightarrow}_n(\langle u_1, \omega''\rangle)(\omega') \\ = \ & [\![\mathrm{act}]\!] \otimes F_P^n(\lambda v.\perp_K)(u_1). \end{aligned}$$

– If $Ctrl(e) = cond[\varphi]$, then the right-hand-side is equal to $F_P^n(\lambda v.\bot_K)(u_1) \,{}_{[\![\varphi]\!]}\!\diamond F_P^n(\lambda v.\bot_K)(u_2)$. The left-hand-side is

$$\begin{aligned}
&\lambda\omega.\lambda\omega'.\sum_{\tau} \hat{\longrightarrow}(\langle v,\omega\rangle)(\tau)\cdot \hat{\longrightarrow}_n(\tau)(\omega') \\
=\ &\lambda\omega.\lambda\omega'.(\sum_{\omega''}[\![\varphi]\!](\omega)\cdot\delta(\omega)(\omega'')\cdot \hat{\longrightarrow}_n(\langle u_1,\omega''\rangle)(\omega') + \sum_{\omega''}(1-[\![\varphi]\!](\omega))\cdot\delta(\omega)(\omega'')\cdot \hat{\longrightarrow}_n(\langle u_2,\omega''\rangle)(\omega')) \\
=\ &\lambda\omega.\lambda\omega'.([\![\varphi]\!](\omega)\cdot \hat{\longrightarrow}_n(\langle u_1,\omega\rangle)(\omega') + (1-[\![\varphi]\!](\omega))\cdot \hat{\longrightarrow}_n(\langle u_2,\omega\rangle)(\omega')) \\
=\ &\lambda\omega.\lambda\omega'.([\![\varphi]\!](\omega)\cdot F_P^n(\lambda v.\bot_K)(u_1)(\omega)(\omega') + (1-[\![\varphi]\!](\omega))\cdot F_P^n(\lambda v.\bot_K)(u_2)(\omega)(\omega')) \\
=\ &F_P^n(\lambda v.\bot_K)(u_1) \,{}_{[\![\varphi]\!]}\!\diamond F_P^n(\lambda v.\bot_K)(u_2).
\end{aligned}$$

Thus we conclude the proof.

□

A.15 Thm. 6.3

Proof. We only show the proof for the over-approximations. By definition, we have $\mathscr{C}[P] = \mathrm{lfp}^{\dot{\sqsubseteq}_C}_{\dot{\bot}_C} F_P^{\mathscr{C}} = \bigsqcup^{\uparrow}_{n\in\mathbb{N}}(F_P^{\mathscr{C}})^n(\dot{\bot}_C)$, and $\mathscr{Y}^\sharp[P] = \mathrm{lfp}^{\dot{\sqsubseteq}_Y}_{\dot{\bot}_Y} F_P^{\mathscr{Y}}$ obtained by Knaster-Tarski. Then it suffices to show that for every $n\in\mathbb{N}$, we have $(F_P^{\mathscr{C}})^n(\dot{\bot}_C)\dot{\sqsubseteq}_C\dot{\gamma}(\mathscr{Y}^\sharp[P])$. Now we proceed by induction on n.

- If $n = 0$, the result follows immediately because $\bot_C$ is the least element in $\mathcal{C}$.
- Suppose that $(F_P^{\mathscr{C}})^k(\dot{\bot}_C)\dot{\sqsubseteq}_C\dot{\gamma}(\mathscr{Y}^\sharp[P])$ for some $k\in\mathbb{N}$. Let's denote the left hand side by LHS and $\mathscr{Y}^\sharp[P]$ by SOL. We want to show that $F_P^{\mathscr{C}}(LHS)\dot{\sqsubseteq}_C\dot{\gamma}(SOL)$. This expands to $F_P^{\mathscr{C}}(LHS)(v)\sqsubseteq_C \gamma(SOL(v))$ for all $v\in V$. We proceed by a case analysis on the kind of edges leaving v.
  1. If $v = v_i^{\mathsf{exit}}$ for some i, then $F_P^{\mathscr{C}}(LHS)(v) = 1_C$. Then we can conclude this case by showing that $SOL(v) = 1_Y$. By definition of SOL, we know that $F_P^{\mathscr{Y}}(SOL) = SOL$, thus $F_P^{\mathscr{Y}}(SOL)(v) = SOL(v)$. By definition of $F_P^{\mathscr{Y}}$, we know that $F_P^{\mathscr{Y}}(SOL)(v) = 1_Y$.
  2. If $v\neq v_i^{\mathsf{exit}}$ for all i, we have

$$\begin{aligned}
F_P^{\mathscr{C}}(LHS)(v) &= \bigsqcup\!\!\!\bigsqcup_C\{\widehat{Ctrl(e)}(LHS(u_1),\cdots,LHS(u_k)) \mid e=\langle v,\{u_1,\cdots,u_k\rangle\in E\} \\
&\sqsubseteq_C \bigsqcup\!\!\!\bigsqcup_C\{\widehat{Ctrl(e)}(\gamma(SOL(u_1)),\cdots,\gamma(SOL(u_k))) \mid e=\langle v,\{u_1,\cdots,u_k\}\rangle\in E\}.
\end{aligned}$$

     If we can prove that for any kind of $Ctrl(e)$ it holds that $\widehat{Ctrl(e)}(\gamma(x_1),\cdots,\gamma(x_k)) \sqsubseteq_C \gamma(\widehat{Ctrl(e)}(x_1,\cdots,x_k))$, then we can conclude the case by the following argument:

$$\begin{aligned}
F_P^{\mathscr{C}}(LHS)(v) &\sqsubseteq_C \bigsqcup\!\!\!\bigsqcup_C\{\gamma(\widehat{Ctrl(e)}(SOL(u_1),\cdots,SOL(u_k))) \mid e=\langle v,\{u_1,\cdots,u_k\rangle\in E\} \\
&\sqsubseteq_C \gamma(\bigsqcup\!\!\!\bigsqcup_Y\{\widehat{Ctrl(e)}(SOL(u_1),\cdots,SOL(u_k)) \mid e=\langle v,\{u_1,\cdots,u_k\}\in E\rangle\}) \\
&= \gamma(F_P^{\mathscr{Y}}(SOL)(v)) \\
&= \gamma(SOL(v)).
\end{aligned}$$

     Now consider the form of $Ctrl(e)$.

     – $Ctrl(e) = seq[\mathrm{act}]$: We want to show that $\widehat{seq[\mathrm{act}]}(\gamma(x_1))\sqsubseteq_C\gamma(\widehat{seq[\mathrm{act}]}(x_1))$. It is equivalent to $[\![\mathrm{act}]\!]^{\mathscr{C}}\otimes_C\gamma(x_1)\sqsubseteq_C\gamma([\![\mathrm{act}]\!]^{\mathscr{Y}}\otimes_Y x_1)$. Indeed, we have

$$[\![\mathrm{act}]\!]^{\mathscr{C}}\otimes_C\gamma(x_1)\sqsubseteq_C\gamma([\![\mathrm{act}]\!]^{\mathscr{Y}})\otimes_C\gamma(x_1)\sqsubseteq_C\gamma([\![\mathrm{act}]\!]^{\mathscr{Y}}\otimes_Y x_1)$$

     by assumption, monotonicity of $\otimes_C$, and properties of γ.

– $Ctrl(e) = cond[\varphi]$: We want to show that $\widehat{cond[\varphi]}(\gamma(x_1), \gamma(x_2)) \sqsubseteq_C \gamma(\widehat{cond[\varphi]}(x_1, x_2))$. It is equivalent to $\gamma(x_1)\ {}_{\varphi}\Diamond_C\ \gamma(x_2) \sqsubseteq_C \gamma(x_1\ {}_{\varphi}\Diamond_Y\ x_2)$. Appeal to properties of γ.

– $Ctrl(e) = call[i \to j]$: We want to show that $\widehat{call[i \to j]}(\gamma(x_1)) \sqsubseteq_C \gamma(\widehat{call[i \to j]}(x_1))$. It is equivalent to $LHS(v_j^{\mathsf{entry}}) \otimes_C \gamma(x_1) \sqsubseteq_C \gamma(SOL(v_j^{\mathsf{entry}}) \otimes_Y x_1)$. Indeed, we have

$$LHS(v_j^{\mathsf{entry}}) \otimes_C \gamma(x_1) \sqsubseteq_C \gamma(SOL(v_j^{\mathsf{entry}})) \otimes_C \gamma(x_1) \sqsubseteq_C \gamma(SOL(v_j^{\mathsf{entry}}) \otimes_Y x_1)$$

by induction hypothesis, monotonicity of $\otimes_C$, and properties of γ.

□