Cantor meets Scott: Domain-Theoretic Foundations for Probabilistic Network Programming

POPL ’17 Submission #18

Abstract

ProbNetKAT is a probabilistic extension of NetKAT with a denotational semantics based on Markov kernels. The language is expressive enough to generate continuous distributions, which raises the question of how to effectively compute in the language. This paper gives an alternative characterization of ProbNetKAT’s semantics using domain theory, which provides the foundations needed to build a practical implementation. The new semantics demonstrates that it is possible to analyze ProbNetKAT programs precisely using approximations of fixpoints and distributions with finite support. We develop an implementation and show how to solve a variety of practical problems including characterizing the expected performance of traffic engineering schemes based on randomized routing and reasoning probabilistically about properties such as loop freedom.

1. Introduction

The recent emergence of software-defined networking (SDN) has led to the development of a number of domain-specific programming languages [13, 46, 49, 72] and reasoning tools [3, 14, 32, 33] for networks. But there is still a large gap between the models provided by these languages and the realities of modern networks. In particular, most existing SDN languages have semantics based on deterministic packet-processing functions, which makes it impossible to encode probabilistic behaviors. This is unfortunate because in the real world, network operators often use randomized protocols and probabilistic reasoning to achieve good performance.

Previous work on ProbNetKAT [13] proposed an extension to the NetKAT language [3, 14] with a random choice operator that can be used to express a variety of probabilistic behaviors. ProbNetKAT has a compositional semantics based on Markov kernels that conservatively extends the deterministic NetKAT semantics and has been used to reason about various aspects of network performance including congestion, fault tolerance, and latency. However, although the language enjoys a number of attractive theoretical properties, there are some major impediments to building a practical implementation: (i) the semantics of iteration is formulated as an infinite process rather than a fixpoint in a suitable order, and (ii) programs can generate continuous distributions in general. These issues make it difficult to determine when a computation has converged to its final value, and there are also challenges related to representing and analyzing distributions with infinite support.

This paper introduces a new semantics for ProbNetKAT, following the approach pioneered by Saheb-Djahromi, Jones, and Plotkin [28, 29, 56, 62, 63]. Whereas the original semantics of ProbNetKAT was somewhat imperative in nature, being based on stochastic processes, the semantics introduced in this paper is purely functional. Nevertheless, the two semantics are closely related—we give a precise, technical characterization of the relationship between them. The new semantics provides a suitable foundation for building a practical implementation, it provides new insights into the nature of probabilistic behavior in networks, and it opens up several interesting theoretical questions for future work.

Our new semantics for ProbNetKAT follows the order-theoretic tradition established in previous work on Scott-style domain theory [1, 64]. In particular, Scott-continuous maps on algebraic and continuous DCPOs play key roles in our development. However, there is an interesting twist: NetKAT and ProbNetKAT are not state-based as with most other probabilistic systems, but are rather throughput-based. A ProbNetKAT program can be thought of as a packet filter that takes an input set of packet histories and generates an output randomly distributed on the measurable space $2^\mathbb{N}$ of sets of packet histories. The closest thing to a “state” is a set of packet histories, and the structure of these sets—e.g., the lengths of the histories they contain and the standard subset relation. Hence, the fundamental domains are not flat domains as in traditional domain theory, but are instead the DCPO of sets of packet histories ordered by the subset relation. Another point of departure from prior work is that the distributions used in the semantics are not subprobability distributions, but actual probability distributions: with probability 1, some set of packets is output, although it may be the empty set.

It is not obvious that such an order-theoretic semantics should exist at all. Traditional probabilistic theory does not take order and compositionality as fundamental structuring principles, but prefers to work in monolithic sample spaces with strong topological properties such as Polish spaces. Prototypical examples of such spaces are the real line, Cantor space, and Baire space. The space of sets of packet histories $2^\mathbb{N}$ is homeomorphic to the Cantor space, and this was the guiding principle in the development of the original ProbNetKAT semantics. Although the Cantor topology enjoys a number of attractive properties (compactness, metrizability, strong separation) that are lost when shifting to the Scott topology, the sacrifice is compensated by a more compelling least-fixpoint characterization of iteration that aligns better with the traditional domain-theoretic treatment. Intuitively, the key insight that underpins our development is the observation that ProbNetKAT programs are monotone as input, then the likelihood of seeing any particular set of packets in the following sense: if a larger set of packet histories is provided as input, the probability of seeing any particular set of packets as a subset of the output set can only increase. From this germ of an idea, we formulate an order-theoretic semantics for ProbNetKAT.

In addition to the strong theoretical motivation for this work, our new semantics also provides a source of practical useful reasoning techniques, notably in the treatment of iteration and approximation. The original paper on ProbNetKAT showed that Kleene star operator satisfies the usual fixpoint equation $P^* = 1 \& P \lor P^*$, and that its finite approximants $P^{(n)}$ converge weakly (but not pointwise) to it. However, it was not characterized as a least fixpoint in any order or as a canonical solution in any sense. This was a bit unsettling and raised questions as to whether it was the “right” definition—questions for which there was no obvious answer. This paper characterizes $P^*$ as the least fixpoint of the Scott-continuous map $X \mapsto 1 \& P \lor X$ on a continuous DCPO of Scott-continuous Markov kernels. This not only corroborates the original definition as the “right” one, but provides a powerful tool for monotone approximation. Indeed, this result implies the correctness of our
implementation, which we have used to build and evaluate real-world applications.

Contributions. This main contributions of this paper are as follows: (i) we develop a domain-theoretic foundation for probabilistic network programming, (ii) using this semantics, we build an implementation of the ProbNetKAT language, and (iii) we evaluate the practical applicability of the language on several case studies.

Outline. The paper is structured as follows: §2 gives a high-level overview of our technical development using a simple running example. §3 reviews basic definitions from domain theory and measure theory. §4 formalizes the syntax and semantics of ProbNetKAT abstractly, in terms of a monad. §5 proves a general theorem relating the Scott and Cantor topologies on $2^H$. Although the Scott topology is much weaker, the two topologies generate the same Borel sets, so the probability measures are the same in both. We also show that the bases of the two topologies are related by a countably infinite-dimensional triangular linear system, which can be viewed as an infinite analog of the inclusion-exclusion principle. The cornerstone of this result is an extension theorem (Theorem 7) that determines when a function on the basic Scott-open sets extends to a measure. §6 gives the new domain-theoretic semantics for ProbNetKAT in which programs are characterized as Markov kernels that are Scott-continuous in their first argument. We show that this class of kernels forms a continuous DCPO, the basis elements being those kernels that drop all but fixed finite sets of input and output packets. §7 shows that ProbNetKAT’s primitives are (Scott-)continuous and its program operators preserve continuity. Other operations such as product and Lebesgue integration are also treated in this framework. In proving these results, we attempt to reuse general results from domain theory whenever possible, relying on the specific properties of $2^H$ only when necessary. We supply complete proofs for folklore results and in cases where we could not find an appropriate original source. We also show that the two definitions of the Kleene star operator—one in terms of an infinite stochastic process and one as the least fixpoint of a Scott-continuous map—coincide. §8 applies the continuity results from §7 to derive monotone convergence theorems. §9 describes an implementation based on §8 and practical applications. §10 reviews related work. We conclude in §11 by discussing open problems and future directions.

2. Overview

This section provides motivation for the ProbNetKAT language and summarizes our technical results using a simple example.

Example. Consider the topology shown in Figure 1 and suppose we are asked to implement a routing application that forwards all traffic to its destination while minimizing congestion, gracefully adapting to shifts in load, and also handling unexpected failures. This problem is known as traffic engineering in the networking literature and has been extensively studied [4, 22, 26, 48, 57]. Note that standard shortest-path routing (SPF) does not solve the problem as stated—in general, it can lead to bottlenecks and also makes the network vulnerable to failures. For example, consider sending a large amount of traffic from $h_1$ to $h_2$; there are two paths in the topology, one via $S_2$ and one via $S_3$, but if we only use a single path we sacrifice half of the available capacity. The most widely-deployed approaches to traffic engineering today are based on using multiple paths and randomization. For example, Equal Cost Multipath Routing (ECMP), which is widely supported on commodity routers, selects a least-cost path for each traffic flow uniformly at random. The intention is to spread the offered load across a large set of paths, thereby reducing congestion without increasing latency.

![Figure 1](image)

ProbNetKAT Language. It is straightforward to write a ProbNetKAT program that captures the essential behavior of ECMP. We first encode routing tables and topology, and then write a program that models the behavior of the entire network.

Routing: We model the routing tables for the switches using simple ProbNetKAT programs that match on destination addresses and forward packets on the next hop toward their destination. To randomly map packets to least-cost paths, we use the choice operator ($\circ$). For example, the program for switch $S_1$ in Figure 1 is as follows:

$$p_1 \triangleq (\text{sw} = S_1; p_1) \& (\text{sw} = S_2; p_2) \& (\text{sw} = S_3; p_3) \& (\text{sw} = S_4; p_4)$$

The programs for other switches are similar. To a first approximation, this program can be read as a routing table, whose entries are separated by the parallel composition operator ($\&$). The first entry states that packets whose destination is $h_1$ should be forwarded out on port 1 (which is directly connected to $h_1$). Likewise, the second entry states that packets whose destination is host $h_2$ should be forwarded out on port 2, which is the next hop on the unique shortest path to $h_2$. The third entry, however, is different: it states that packets whose destination is $h_3$ should be forwarded out on ports 2 and 4 with equal probability. This divides traffic going to $h_3$ among the clockwise path via $S_2$ and the counter-clockwise path via $S_4$. The final entry states that packets whose destination is $h_4$ should be forwarded out on port 4, which is again the next hop on the unique shortest path to $h_4$. The routing program for the network is the parallel composition of the programs for each switch:

$$p \triangleq (\text{sw} = S_1; p_1) \& (\text{sw} = S_2; p_2) \& (\text{sw} = S_3; p_3) \& (\text{sw} = S_4; p_4)$$

Topology: We model a directed link as a program that matches on the switch and port at one end of the link and modifies the switch and port to the other end of the link. We model an undirected link $l$ as a parallel composition of directed links in each direction. For example, the link between switches $S_1$ and $S_2$ is as follows:

$$l_{1,2} \triangleq (\text{sw} = S_1; \text{pt} = 2; \text{dup}) \& (\text{sw} = S_2; \text{pt} = 1; \text{dup})$$

These examples show that the ProbNetKAT language is a powerful tool for modeling and analyzing complex network systems.
Note that at each hop we use ProbNetKAT’s dup operator to store the headers in the packet’s history, which records the trajectory of the packet as it goes through the network. Histories are useful for tasks such as measuring path length and analyzing link congestion. We model the topology as a parallel composition of individual links:

\[ t \triangleq l_{1,2} \& l_{2,3} \& l_{3,4} \& l_{1,4} \]

To delimit the network edge, we define ingress and egress predicates:

\[ in \triangleq (sw=1; pt=1) \& (sw=2; pt=2) \& \ldots \]
\[ out \triangleq (sw=1; pt=1) \& (sw=2; pt=2) \& \ldots \]

Here, since every ingress is an egress, the predicates are identical.

**Network:** We model the end-to-end behavior of the entire network by combining \( p, t, in \) and \( out \) into a single program:

\[ net \triangleq in ; (p ; t)^* ; p ; out \]

This program models processing each input from ingress to egress across a series of switches and links. Formally it denotes a Markov kernel that, when supplied with an input distribution on packet histories \( \mu \) produces an output distribution \( \nu \).

**Queries:** Having constructed a probabilistic model of the network, we can use standard tools from measure theory to reason about performance. For example, to compute the expected congestion on a given link \( l \), we would introduce a function \( Q \) from sets of packets to \( \mathbb{R} \cup \{\infty\} \) (formally a random variable):

\[ Q(a) \triangleq \sum_{h \in a} \#_i(h) \]

where \( \#_i(h) \) is the function on packet histories that returns the number of times that link \( l \) occurs in \( h \), and then compute the expected value of \( Q \) using integration:

\[ E[Q] = \int Q \, dv \]

We can compute queries that capture other aspects of network performance such as latency, reliability, etc. in similar fashion.

**Limitations.** Unfortunately there are several serious problems with the approach just described:

- One problem is that computing the results of a query can require complicated measure theory since a ProbNetKAT program may generate a continuous distribution in general. Formally, instead of summing over the support of the distribution, we have to use Lebesgue integration in an appropriate measurable space. There are also challenges in representing infinite distributions.

- Another issue is that the semantics of iteration is modeled in terms of an infinite stochastic process rather than a standard fixpoint. The original ProbNetKAT paper showed that it is possible to approximate a program using a series of star-free programs that weakly converge to the correct result, but the approximations need not converge monotonically. This fact makes approximation difficult to use in practice.

- Even worse, many of the queries that we would like to answer are not actually continuous in the Cantor topology, meaning that the weak convergence result does not even apply! The notion of distance on sets of packet histories is \( d(a, b) = 2^{-n} \) where \( n \) is the length of the smallest history in \( a \) but not in \( b \), or vice versa. It is easy to construct a sequence of histories \( h_n \) of length \( n \) such that \( \lim_{n \to \infty} d(h_n, \emptyset) = 0 \) but \( \lim_{n \to \infty} Q(h_n) = \infty \) which is not equal to \( Q(\emptyset) = 0 \).

Together, these issues are significant impediments that make it difficult to apply ProbNetKAT in many practical scenarios.

**Domain-Theoretic Semantics.** This paper develops a new semantics for ProbNetKAT that overcomes these problems and provides the key building blocks needed to engineer a practical implementation. The main insight is that we can formulate the semantics in terms of the Scott topology rather than the Cantor topology. It turns out that these two topologies generate the same Borel sets, and the relationship between them can be characterized using an extension theorem that captures when functions on the basic Scott-open sets extend to a measure. We show how to construct a DCO equipped with a natural partial order that also lifts to a partial order on Markov kernels. We prove that standard program operators are continuous, which allows us to formulate the semantics of the language—in particular Kleene star—using standard tools from domain theory, such as least fixpoints. Finally, we formalize a notion of approximation and prove a monotone convergence theorem.

The problems with the original ProbNetKAT semantics identified above are all solved using the new semantics. Because the new semantics models iteration as a least fixpoint, we can work with finite distributions and star-free approximations that are guaranteed to monotonically converge to the correct result. Moreover, whereas our query \( Q \) was not Cantor continuous, it is straightforward to show that it is Scott continuous. Let \( A \) be an increasing chain \( a_0 \subseteq a_1 \subseteq a_2 \subseteq \ldots \) ordered by inclusion. Scott continuity requires \( \bigcup_{a \in A} Q(a) = Q(\bigcup A) \) which is easy to prove. Hence, the convergence theorem applies and we can compute a monotonically increasing chain of approximations that converge to \( E[Q] \).

**Implementation and Applications.** We developed the first implementation of ProbNetKAT using the new semantics. We built an interpreter for the language and implemented a variety of traffic engineering schemes including ECMP, K-shortest path routing (which provides improved fault tolerance), and oblivious routing [57]. We analyzed the performance of each scheme in terms of congestion and latency on real-world demands drawn from Internet2’s Abilene backbone, and in the presence of link failures. We showed how to use the language to reason probabilistically about reachability properties such as loops and black holes. Figures 1 (b-c) depict the expected throughput and maximum congestion and using shortest paths (SPF) and ECMP on the 4-node topology as computed by our ProbNetKAT implementation. We set the demand from \( h_1 \) to \( h_3 \) to be \( \frac{1}{4} \) units of traffic, and the demand between all other pairs of hosts to be \( \frac{1}{4} \) units. The first graph depicts the maximum congestion induced under successive approximations of the Kleene star, and shows that ECMP achieves much better congestion than SPF. With SPF, the most congested link (from \( S_1 \) to \( S_2 \)) carries traffic from \( h_1 \) to \( h_3 \), from \( h_3 \) to \( h_3 \), and from \( h_1 \) to \( h_3 \), resulting in \( \frac{3}{4} \) total traffic. With ECMP, the same link carries traffic from \( h_1 \) to \( h_3 \), half of the traffic from \( h_3 \) to \( h_3 \), half of the traffic from \( h_1 \) to \( h_3 \), resulting in \( \frac{7}{16} \) total traffic. The second graph depicts the loss of throughput when the same link fails. The total aggregate demand is \( \frac{1}{4} \). With SPF, \( \frac{3}{4} \) units of traffic are dropped leaving \( \frac{1}{2} \) units, which is 60% of the demand, whereas with ECMP only \( \frac{7}{16} \) units of traffic are dropped leaving \( \frac{1}{2} \) units, which is 77% of the demand.

### 3. Preliminaries

This section briefly reviews basic concepts from topology, measure theory, and domain theory, and defines Markov kernels, the objects on which ProbNetKAT’s semantics is based. For a more detailed account, the reader is invited to consult standard texts [1, 9].

**Topology.** A topology \( \mathcal{O} \subseteq 2^X \) on a set \( X \) is a collection of subsets including \( X \) and \( \emptyset \) that is closed under finite intersection and arbitrary union. A pair \((X, \mathcal{O})\) is called a topological space and the sets \( U, V \in \mathcal{O} \) are called the open sets of \((X, \mathcal{O})\). A function \( f : X \to Y \) between topological spaces \((X, \mathcal{O}_X)\) and \((Y, \mathcal{O}_Y)\) is
continuous if the preimage of any open set in $Y$ is open in $X$, i.e. if
$f^{-1}(U) = \{ x \in X | f(x) \in U \} \in \mathcal{O}_X$
for any $U \in \mathcal{O}_Y$.

**Measure Theory.** A $\sigma$-algebra $\mathcal{F} \subseteq 2^X$ on a set $X$ is a collection
of subsets including $X$ that is closed under complement, countable union,
and countable intersection. A measurable space is a pair $(X, \mathcal{F})$. A probability measure $\mu$ over such a space is a function
$\mu : \mathcal{F} \to [0, 1]$ that assigns probabilities $\mu(A) \in [0, 1]$ to the measurable sets $A \subseteq \mathcal{F}$, and satisfies the following conditions:

- $\mu(X) = 1$
- $\mu \left( \bigcup_{i \in I} A_i \right) = \sum_{i \in I} \mu(A_i)$ whenever $\{ A_i \}_{i \in I}$ is a countable collection of disjoint sets.

Note that these conditions already imply that $\mu(\emptyset) = 0$. Elements $a, b \in X$ are called points or outcomes, and measurable sets $A, B \in \mathcal{F}$ are also called events. The $\sigma$-algebra $\sigma(U)$ generated by a set $U \subseteq X$ is the smallest $\sigma$-algebra containing $U$:

$$\sigma(U) = \bigcap \{ \mathcal{F} \subseteq 2^X | \mathcal{F} \text{ is a } \sigma\text{-algebra and } U \subseteq \mathcal{F} \}.$$  

Note that it is well-defined because the intersection is not empty ($X$ is trivially a $\sigma$-algebra containing $U$) and intersections of $\sigma$-algebras are again $\sigma$-algebras. If $O \subseteq 2^X$ are the open sets of $X$, then the smallest $\sigma$-algebra containing the open sets $B = \sigma(O)$ is the Borel algebra, and the measurable sets $A, B \in \mathcal{B}$ are the Borel sets of $X$.

Let $P_\mu \triangleq \{ a \in X | \mu(\{a\}) > 0 \}$ denote the points (not events!) with non-zero probability. It can be shown that $P_\mu$ is countable. A probability measure is called discrete if $\mu(P_\mu) = 1$. Such a measure can simply be represented by a function $Pr : X \to [0, 1]$ with $Pr(a) = \mu(\{a\})$. If $\mu(P) < \infty$, the measure is called finite and can be represented by a finite map $Pr : \hat{P} : P \to [0, 1]$. In contrast, measures for which $\mu(P_\mu) = 0$ are called continuous, and measures for which $0 < \mu(P_\mu) < 1$ are called mixed. The Dirac measure or point mass puts all probability on a single point $a \in X$:

$$\delta_a(A) = \begin{cases} 1 & a \in A \\ 0 & a \notin A \end{cases}$$

The uniform distribution on $[0, 1]$ is a continuous measure.

A function $f : X \to Y$ between measurable spaces $(X, \mathcal{F}_X)$ and $(Y, \mathcal{F}_Y)$ is called measurable if the preimage of any measurable set in $Y$ is measurable in $X$, i.e. if

$$f^{-1}(A) = \{ x \in X | f(x) \in A \} \in \mathcal{F}_X$$

for all $A \in \mathcal{F}_Y$. If $Y = \mathbb{R} \cup \{-\infty, +\infty\}$, then $f$ is called a random variable and its expected value with respect to a measure $\mu$ on $X$ is given by the Lebesgue integral

$$E[f] \triangleq \int f \, d\mu = \int_{x \in X} f(x) \cdot \mu(dx)$$

If $\mu$ is discrete, the integral simplifies to the sum

$$E[f] = \sum_{x \in X} f(x) \cdot \mu(\{x\}) = \sum_{x \in P_\mu} f(x) \cdot Pr(x)$$

**Markov Kernels.** Imagine a probabilistic transition system with states $X$ that makes a random transition between states at each step. If $X$ is finite, the system can be captured by a transition matrix $T \in [0, 1]^{X \times X}$, where the matrix entry $T_{xy}$ gives the probability that the transition proceeds from state $x$ to state $y$. Each row $T_x$ describes the transition function of a state $x$ and must sum to 1. Suppose that the start state is initially distributed according to the row vector $V \in [0, 1]^X$, i.e. the system starts in state $x \in X$ with probability $V_x$. Then, the state distribution is given by the matrix product $VT \in [0, 1]^X$ after one step and by $V T^n$ after $n$ steps.

Markov kernels generalize this idea to infinite state systems. Given measurable spaces $(X, \mathcal{F}_X)$ and $(Y, \mathcal{F}_Y)$, a Markov kernel with source $X$ and target $Y$ is a function $P : X \times \mathcal{F}_Y \to [0, 1]$ (or equivalently, $X \to \mathcal{F}_Y \to [0, 1]$) that maps each source state $x \in X$ to a distribution over target states $P(x, -) : \mathcal{F}_Y \to [0, 1]$. If the initial distribution is given by a measure $\nu$ on $X$, then the target distribution $\mu$ after one step is given by Lebesgue integration:

$$\mu(A) \triangleq \int_{x \in X} P(x, A) \cdot \nu(dx) \quad (A \in \mathcal{F}_Y)$$

If $\nu$ and $P(x, -)$ are discrete, the integral simplifies to the sum

$$\mu(\{y\}) = \sum_{x \in X} P(x, \{y\}) \cdot \nu(x) \quad (y \in Y)$$

which is just the familiar vector-matrix-product $VT$. Similarly, two kernels $P, Q$ from $X$ to $Y$ and from $Y$ to $Z$, respectively, can be sequentially composed to a kernel $P \circ Q$ from $X$ to $Z$:

$$(P \circ Q)(x, A) \triangleq \int_{y \in Y} P(x, dy) \cdot Q(y, A)$$

This is the continuous analog of the matrix product $TT$. A Markov kernel $P$ must satisfy two conditions:

(i) For each source state $x \in X$, the map $A \to P(x, A)$ must be a probability measure on the target space.

(ii) For each event $A \in \mathcal{F}_Y$ in the target space, the map $x \to P(x, A)$ must be a measurable function.

Condition (ii) is required to ensure that integration is well-defined. A kernel $P$ is called deterministic if $P(a, -)$ is a dirac measure for each $a$.

**Domain Theory.** A partial order (PO) is a pair $(D, \sqsubseteq)$ where $D$ is a set and $\sqsubseteq$ is a reflexive, transitive, and antisymmetrical relation on $D$. For two elements $x, y \in D$ we let $x \sqsubseteq y$ denote their $\sqsubseteq$-least upper bound (i.e., their supremum), provided it exists. Analogously, the least upper bound of a subset $C \subseteq D$ is denoted $\bigsqcup C$, provided it exists. A subset $C \subseteq D$ is directed if for any two $x, y \in C$ there exists some upper bound $x, y \sqsubseteq z$ in $C$. A directed complete partial order (DCPO) is a PO for which any directed subset $C \subseteq D$ has a supremum $\bigsqcup C$ in $D$. If a PO has a least element it is denoted by $\bot$, and if it has a greatest element it is denoted by $\top$. For example, the nonnegative real numbers with infinity $\mathbb{R}_+ \triangleq [0, \infty]$ form a DCPO under the natural order $\leq$ with supreme $\bigsqcup C = \sup C$, least element $\bot = 0$, and greatest element $\top = \infty$. The unit interval is a DCPO under the same order, but with $\bot = 1$. Any powerset $2^X$ is a DCPO under the subset order, with suprema given by union.

A function $f$ from $D$ to $E$ is called (Scott)-continuous if

(i) it is monotone, i.e. $x \sqsubseteq y$ implies $f(x) \sqsubseteq f(y)$, and

(ii) it preserves suprema, i.e. $f(\bigsqcup C) = \bigsqcup f(x)$ for any directed set $C$ in $D$.

Equivalently, $f$ is continuous with respect to the Scott topologies on $D$ and $E$ [1, Proposition 2.3.4], which we define next. The set of all continuous functions $f : D \to E$ is denoted $[D \to E]$.

A subset $A \subseteq D$ is called up-closed (or an upper set) if $a \subseteq A$ and $a \subseteq b$ implies $b \subseteq A$. The smallest up-closed set containing $A$ is called its up-closure and is denoted $A^\uparrow$. $A$ is called Scott-open if it is up-closed and intersects every directed subset $C \subseteq D$ that satisfies $\bigsqcup C \subseteq A$. For example, the Scott-open sets of $\mathbb{R}_+$ are the upper semi-infinite intervals $[r, \infty], r \in \mathbb{R}_+$. The Scott-open sets form a topology on $D$ called the Scott topology.

DCPOs enjoy many useful closure properties:

(i) The cartesian product of any collection of DCPOs is a DCPO with componentwise order and suprema.

(ii) If $E$ is a DCPO and $D$ any set, the function space $D \to E$ is a DCPO with pointwise order and suprema.
The continuous functions \([D \to E]\) between DCPOs \(D\) and \(E\) form a DCPO with pointwise order and suprema.

If \(D\) is a DCPO with least element \(\bot\), then any Scott-continuous self-map \(f \in [[D \to D]]\) has a \(\sqsubseteq\)-least fixpoint, and it is given by the supremum of the chain \(\bot \subseteq f(\bot) \subseteq f(f(\bot)) \subseteq \ldots:\)

\[
\text{lfp}(f) = \bigcup_{n \geq 0} f^n(\bot)
\]

Moreover, the least fixpoint operator, \(\text{lfp} \in [[D \to D]]\) is itself continuous, that is: \(\text{lfp}(\bigcup C) = \bigcup_{f \in C} \text{lfp}(f)\), for any directed set of functions \(C \subseteq [[D \to D]]\).

An element \(a\) of a DCPO is called finite (Abramsky and Jung use the term compact \([1]\)) if for any directed set \(A\), if \(a \subseteq \bigcup A\), then there exists \(b \in A\) such that \(a \sqsubseteq b\). Equivalently, \(a\) is finite if its up-closure \(\{a\}^\uparrow\) is Scott-open. A DCPO is called algebraic if for every element \(b\), the finite elements \(\subseteq\)-below \(b\) form a directed set and \(b\) is the supremum of this set. An element \(a\) of a DCPO approximates another element \(b\), written \(a \ll b\), if for any directed set \(A\), \(a \subseteq c\) for some \(c \in A\) whenever \(b \square A\). A DCPO is called continuous if for every element \(b\), the elements \(\ll\)-below \(b\) form a directed set and \(b\) is the supremum of this set. Every algebraic DCPO is continuous. A set in a topological space is compact-open if it is compact (every open cover has a finite subcover) and open.

Here we recall some basic facts about DCPOs. These are all well-known, but we state them as a lemma for future reference.

**Lemma 1** (DCPO Basic Facts).

(i) Let \(E\) be a DCPO and \(D_1, D_2\) sets. There is a homeomorphism (bicategorical bijection) curvature between the DCPOs \(D_1 \times D_2 \to E\) and \(D_1 \to D_2 \to E\), where the function spaces are ordered pointwise. The inverse of curvature is uncurry.

(ii) In an algebraic DCPO, the open sets \(\{a\}^\uparrow\) for finite \(a\) form a base for the Scott topology.

(iii) An element of an algebraic DCPO is compact-open iff it is a finite union of basic open sets \(\{a\}^\uparrow\).

(iii) The continuous functions \([D \to E]\) between DCPOs \(D\) and \(E\) form a DCPO with pointwise order and suprema.

If \(D\) is a DCPO with least element \(\bot\), then any Scott-continuous self-map \(f \in [[D \to D]]\) has a \(\sqsubseteq\)-least fixpoint, and it is given by the supremum of the chain \(\bot \subseteq f(\bot) \subseteq f(f(\bot)) \subseteq \ldots:\)

\[
\text{lfp}(f) = \bigcup_{n \geq 0} f^n(\bot)
\]

Moreover, the least fixpoint operator, \(\text{lfp} \in [[D \to D]]\) is itself continuous, that is: \(\text{lfp}(\bigcup C) = \bigcup_{f \in C} \text{lfp}(f)\), for any directed set of functions \(C \subseteq [[D \to D]]\).

An element \(a\) of a DCPO is called finite (Abramsky and Jung use the term compact \([1]\)) if for any directed set \(A\), if \(a \subseteq \bigcup A\), then there exists \(b \in A\) such that \(a \sqsubseteq b\). Equivalently, \(a\) is finite if its up-closure \(\{a\}^\uparrow\) is Scott-open. A DCPO is called algebraic if for every element \(b\), the finite elements \(\subseteq\)-below \(b\) form a directed set and \(b\) is the supremum of this set. An element \(a\) of a DCPO approximates another element \(b\), written \(a \ll b\), if for any directed set \(A\), \(a \subseteq c\) for some \(c \in A\) whenever \(b \sqsubseteq A\). A DCPO is called continuous if for every element \(b\), the elements \(\ll\)-below \(b\) form a directed set and \(b\) is the supremum of this set. Every algebraic DCPO is continuous. A set in a topological space is compact-open if it is compact (every open cover has a finite subcover) and open.

Here we recall some basic facts about DCPOs. These are all well-known, but we state them as a lemma for future reference.

**Lemma 1** (DCPO Basic Facts).

(i) Let \(E\) be a DCPO and \(D_1, D_2\) sets. There is a homeomorphism (bicategorical bijection) curvature between the DCPOs \(D_1 \times D_2 \to E\) and \(D_1 \to D_2 \to E\), where the function spaces are ordered pointwise. The inverse of curvature is uncurry.

(ii) In an algebraic DCPO, the open sets \(\{a\}^\uparrow\) for finite \(a\) form a base for the Scott topology.

(iii) An element of an algebraic DCPO is compact-open iff it is a finite union of basic open sets \(\{a\}^\uparrow\).

### 4. ProbNetKAT

This section defines the syntax and semantics of ProbNetKAT formally (see Figure 2).

**Syntax.** A packet \(\pi\) is a record mapping a finite set of fields \(f_1, f_2, \ldots, f_n\) to bounded integers \(n\). Fields include standard header fields such as the source (src) and destination (dst) of the packet, and two logical fields (sw for switch and pt for port) that record the current location of the packet in the network. The logical fields are not present in a physical network packet, but it is convenient to model them as proper header fields. We write \(\pi.f\) to denote the value of field \(f\) of \(\pi\) and \(\pi[f := n]\) for the packet obtained from \(\pi\) by updating field \(f\) to \(n\). We let \(\text{Pk}\) denote the (finite) set of all packets.

A history \(h = \pi::h\) is a non-empty list of packets with head packet \(\pi\) and (possibly empty) tail \(h\). The head packet models the packet’s current state and the tail contains its prior states, which capture the trajectory of the packet through the network. Operationally, only the head packet exists, but it is useful to discriminate between identical packets with different histories. We write \(H\) to denote the (countable) set of all histories.

We differentiate between predicates \((t, u)\) and programs \((p, q)\). The predicates form a Boolean algebra and include the primitives false \((0)\), true \((1)\), and tests \((f = n)\), as well as the standard Boolean operators disjunction \((t \lor u)\), conjunction \((t \land u)\), and negation \((\neg t)\). Programs include predicates \((t)\) and modifications \((f \leftarrow n)\) as primitives, and the operators parallel composition \((p \& q)\), sequential composition \((p ; q)\), and iteration \((p^\ast)\). The primitive dup records the current state of the packet by extending the tail with the head packet. Finally, choice \(p \oplus q\) executes a program with probability \(r\) or \(q\) with probability \(1 - r\). We write \(p \oplus q\) when \(r = 0.5\).

Predicate conjunction and sequential composition use the same syntax \((t; u)\) as their semantics coincide (as we will see shortly). The same is true for disjunction of predicates and parallel composition \((t \lor u)\). The distinction between predicates and policies is merely to restrict negation to predicates and rule out programs like \(\neg (p^\ast)\).

**Example.** Consider the programs

\[
\begin{align*}
p_1 & \triangleq pt=1 \; ; \; (pt:=2 \& pt:=3) \\
p_2 & \triangleq (pt:=2 \& pt:=3) \; ; \; \text{dst} \leftarrow 10.0.0.1 \; ; \; pt \leftarrow 1
\end{align*}
\]
The first program multicasts packets entering at port 1 out of ports 2 and 3, and drops all other packets. The second program matches on packets coming in on ports 2 or 3, modifies their destination to the IP address 10.0.0.1, and sends them out through port 1. The program \( p_1 \land p_2 \) acts like \( p_1 \) for packets entering at port 1, and like \( p_2 \) for packets entering at ports 2 or 3.

**Monads.** We define the semantics of NetKAT programs parametrically over a monad \( \mathcal{M} \). This allows us to give two concrete semantics at once: the classical deterministic semantics (using the identity monad), and the new probabilistic semantics (using the probability monad). For simplicity, we refrain from giving a categorical treatment and simply model a monad in terms of three components:

- a type constructor \( \mathcal{M} \) mapping objects \( X \) to a domain \( \mathcal{M}(X) \);
- an operator \( \eta : X \to \mathcal{M}(X) \) that lifts objects into the domain \( \mathcal{M}(X) \); and
- an infix operator

\[
\gg : \mathcal{M}(X) \to (X \to \mathcal{M}(X)) \to \mathcal{M}(X)
\]

that lifts a function \( f : X \to \mathcal{M}(X) \) to a function \( (\gg f) : \mathcal{M}(X) \to \mathcal{M}(X) \).

These components must satisfy three axioms:

\[
\begin{align*}
\eta(a) & \gg f = f(a) \quad (M1) \\
\mu \gg \eta &= \mu \quad (M2) \\
(\mu \gg f) \gg g &= \mu \gg (\lambda x. f(x) \gg g) \quad (M3)
\end{align*}
\]

The semantics of deterministic programs (not containing probabilistic choices \( p \oplus q \)) uses as underlying objects the set of packet histories \( 2^H \) and the identity monad \( \mathcal{M}(X) = X \); \( \eta \) is the identity function and \( x \gg f \) is simply function application \( f(x) \). The identity monad trivially satisfies the three axioms.

The semantics of probabilistic programs uses the probability (or Giry) monad [17, 29, 58] that maps a measurable space to the domain of probability measures over that space. The operator \( \eta \) maps a to the point mass (or Dirac measure) \( \delta_a \) on \( a \). Composition \( \mu \gg (\lambda a. \nu_a) \) can be thought of as a two-stage probabilistic experiment where the second experiment \( \nu_a \) depends on the outcome \( a \) of the first experiment \( \mu \). Operationally, we first sample from \( \mu \) to obtain a random outcome \( a \); then, we sample from \( \nu_a \) to obtain the final outcome \( b \). What is the distribution over final outcomes? The key is to note that \( \lambda a. \nu_a \) is a Markov kernel (§3), and so composition with \( \mu \) is given by the familiar integral

\[
\mu \gg (\lambda a. \nu_a) = \lambda A. \int_{a \in X} \mu_a(A) \cdot \mu(da)
\]

introduced in (3.1). It is well known that these definitions satisfy the monad axioms [17, 29, 36], (M1) and (M2) are trivial properties of the Lebesgue Integral. (M3) is essentially Fubini’s theorem, which permits changing the order of integration in a double integral.

**Deterministic Semantics.** In deterministic NetKAT (without \( p \oplus q \)), a program \( p \) denotes a function \( [p] \in 2^H \to 2^{2H} \) mapping a set of input histories \( a \in 2^H \) to a set of output histories \( [p](a) \).

A predicate \( t \) maps the input set \( a \) to the subset \( b \subseteq a \) of histories satisfying the predicate. In particular, the false primitive \( 0 \) denotes the function mapping any input to the empty set; the true primitive \( 1 \) is the identity function; the test \( f = n \) retains those histories with field \( f \) of the head packet equal to \( n \); and negation \( \neg t \) returns only those histories not satisfying \( t \). Modification \( f \Rightarrow n \) sets the \( f \)-field of all head-packets to the value \( n \). Duplication \( dup \) extends the tails of all input histories with their head packets, thus permanently recording the current state of the packets.

Parallel composition \( p \land q \) feeds the input to both \( p \) and \( q \) and takes the union of their outputs. If \( p \) and \( q \) are predicates, a history is thus in the output iff it satisfies at least one of \( p \) or \( q \), so that union acts like logical disjunction on predicates. Sequential composition \( p ; q \) feeds the input to \( p \) and then feeds \( p \)'s output to \( q \) to produce the final result. If \( p \) and \( q \) are predicates, a history is thus in the output iff it satisfies both \( p \) and \( q \), acting like logical conjunction. Iteration \( p^* \) behaves like the parallel composition of \( p \) sequentially composed with itself zero or more times (because \( \varnothing \) is union in \( 2^H \)).

**Probabilistic Semantics.** The semantics of ProbNetKAT is given using the probability monad applied to the set of histories \( 2^H \) (seen as a measurable set). A program \( p \) denotes a function

\[
[p] \in 2^H \to \{ \mu : \mathcal{B} \to [0, 1] \mid \mu \text{ is a probability measure}\}
\]

mapping a set of input histories \( a \) to a distribution over output sets \([p](a)\). Here, \( \mathcal{B} \) denotes the Borel sets of \( 2^H \) (§5). Equivalently, \([p]\) is a Markov kernel with source and destination \((2^H, \mathcal{B})\). The semantics of all primitive programs is identical to the deterministic case, except that they now return point masses on output sets (rather than just output sets). In fact, it follows from (M1) that all programs without choices and iteration are point masses.

Parallel composition \( p \land q \) feeds the input to both \( p \) and \( q \), samples \( b_1 \) and \( b_2 \) from the output distributions \([p](a)\) and \([q](a)\), and returns the union of the samples \( b_1 \cup b_2 \). Probabilistic choice \( p \oplus q \) feeds the input to both \( p \) and \( q \) and returns a convex combination of the output distributions according to \( r \). Sequential composition \( p ; q \) is just sequential composition of Markov kernels. Operationally, it feeds the input to \( p \), obtains a sample \( b \) from \( p \)'s output distribution, and feeds the sample to \( q \) to obtain the final distribution. Iteration \( p^* \) is defined as the least fixpoint of the map on Markov kernels \( X \mapsto 1 \land [p] : X \), which is continuous in a DCPO that we will develop in the following sections. We will show that this definition, which is simple and is based on standard techniques from domain theory, coincides with the semantics proposed in previous work [15].

**Basic Properties.** To clarify the nature of predicates and other primitives, we establish two intuitive properties:

**Lemma 2.** Any predicate \( t \) satisfies \( \tilde{t}(a) = \eta(a \cap b_1) \), where \( b_1 \subseteq 2^H \) is the set of histories satisfying the predicate.

**Proof.** By induction on \( t \), using (M1) in the induction step.

**Lemma 3.** All atomic policies \( p \) (including predicates) satisfy

\[
[p](a) = \eta(\{f_a(h) \mid h \in a\})
\]

for some partial function \( f_a : H \to H \).

**Proof.** Immediate from Figure 2 and Lemma 2.

**Lemma 2** captures the intuition that predicates act like filters. Lemma 3 establishes that the behavior of primitive programs is captured by their behavior on individual histories.

5. Cantor Meets Scott

To define continuous probability measures on an infinite set \( X \), one first needs to endow \( X \) with a topology—some additional structure that, intuitively, captures which elements of \( X \) are close to each other or approximate each other. Although the choice of topology is arbitrary in principle, different topologies induce different notions of continuity and limits, thus profoundly impacting the concepts derived from these primitives. Which topology is the “right” one for \( 2^H \)? A fundamental contribution of this paper is to show that there are (at least) two answers to this question:

- The initial work on ProbNetKAT [15] uses the Cantor topology. This makes \( 2^H \) a standard Borel space, which is well-studied and known to enjoy many desirable properties.
The Scott topology cannot be described in terms of a metric. It is approximated in terms of a distance that is Cantor-continuous: if \( d(a, b) \) is the length of the shortest packet history in the symmetric difference \( \Delta \), then \( f(a) \) is the limit of a sequence of finite measures \( \mu_n \) such that \( \mu_n(A) \rightarrow \mu(A) \) for all measurable \( A \). This gives the following notions of limit and continuity:

- **a** is the limit of a sequence \( a_1, a_2, \ldots \) if for each \( \varepsilon > 0 \), there exists \( N \) such that for all \( n \geq N \), \( d(a_1, a_2) < \varepsilon \).
- A function \( f : \mathbb{H} \rightarrow \mathbb{R} \) is continuous at \( a \) if \( f(a_n) \rightarrow f(a) \) whenever \( a_n \rightarrow a \).

The Scott topology cannot be described in terms of a metric. It is approximated in terms of a distance that is Cantor-continuous: if \( d(a, b) \) is the length of the shortest packet history in the symmetric difference \( \Delta \), then \( f(a) \) is the limit of a sequence of finite measures \( \mu_n \) such that \( \mu_n(A) \rightarrow \mu(A) \) for all measurable \( A \). This gives the following notions of limit and continuity:

- **a** is the limit of a sequence \( a_1, a_2, \ldots \) if for each \( \varepsilon > 0 \), there exists \( N \) such that for all \( n \geq N \), \( d(a_1, a_2) < \varepsilon \).
- A function \( f : \mathbb{H} \rightarrow \mathbb{R} \) is continuous at \( a \) if \( f(a_n) \rightarrow f(a) \) whenever \( a_n \rightarrow a \).

**Example.** To illustrate the difference between Cartesian-continuity and Scott-continuity, consider the function \( f(a) = |a| \) that maps a history set to its (possibly infinite) cardinality. The function is not Cantor-continuous. To see this, let \( h_n \) denote a history of length \( n \) and consider the sequence of singleton sets \( a = \{ h_n \} \). Then \( d(h_n, \emptyset) = 2^{-n} \), i.e., the sequence approaches the empty set as \( n \) approaches infinity. But the cardinality \( |a| = 1 \) does not approach 0. In contrast, the function is easily seen to be Scott-continuous.

As a second example, consider the function \( f(a) = 2^{-k} \), where \( k \) is the length of the smallest history not in \( a \). This function is Cartesian-continuous: if \( d(a_n, a) = 2^{-k} \), then

\[
|f(a_n) - f(a)| \leq 2^{-(n-1)} - 2^{-n} \leq 2^{-n}
\]

Therefore \( f(a_n) \) approaches \( f(a) \) as the function \( d(a_n, a) \) approaches 0. However, the function is not Scott-continuous, as all Scott-continuous functions are monotone.

**Approximation.** The computational importance of limits and continuity comes from the following idea. Assume \( a \) is some complicated (say infinite) mathematical object. If \( a_1, a_2, \ldots \) is a sequence of simple (say finite) objects with limit \( a \), then it may be possible to approximate \( a \) using the sequence \( (a_n) \). This gives us a computational way of working with infinite objects, even though the available resources may be fundamentally finite. Continuity captures precisely when this is possible: we can perform a computation on \( a \) if \( f \) is continuous in \( a \), for then we can compute the sequence \( f(a_1), f(a_2), \ldots \) which (by continuity) converges to \( f(a) \).

We will show later that any measure \( \mu \) can be approximated by a sequence of finite measures \( \mu_1, \mu_2, \ldots \), and that the expected value \( E_\mu[f] \) of a Scott-continuous random variable \( f \) is continuous with respect to the measure. Our implementation exploits this to compute a monotonically improving sequence of approximations for performance metrics such as latency and congestion (§9).

**Notation.** We use lower case letters \( a, b, c \subseteq H \) to denote history sets, uppercase letters \( A, B, C \subseteq \mathbb{H} \) to denote measurable sets (i.e., sets of history sets), and calligraphic letters \( B, O, \cdots \subseteq \mathbb{H} \) to denote sets of measurable sets. For a set \( X \), we let \( \mathcal{L}(X) \triangleq \{ Y \subseteq X \mid |Y| < \infty \} \) denote the finite subsets of \( X \) and \( \mathcal{I}_X \) the characteristic function of \( X \). For a statement \( \phi \), we let \( [\phi] \) denote 1 if \( \phi \) is true and 0 otherwise. For a function \( f : X \rightarrow Y \), we let \( f^{-1}(A) \triangleq \{ x \in X \mid f(x) \in A \} \) denote the preimage function:

\[
f^{-1}(A) \triangleq \{ x \in X \mid f(x) \in A \} \quad f^{-1}(y) \triangleq f^{-1}(\{ y \})
\]

**Cantor and Scott, Formally.** For \( h \in H \) and \( b \in \mathbb{H} \), define

\[
B_h \triangleq \{ c \mid h \subseteq c \} \quad B_b \triangleq \bigcap_{h \subseteq b} B_h = \{ c \mid b \subseteq c \}. \tag{5.3}
\]

The Cantor space topology, denoted \( \mathcal{C} \), is generated by closing \( \{ B_h \mid h \in H \} \) under finite intersection and arbitrary union. The Scott topology of the DPO \( (\mathbb{H}, \subseteq) \), denoted \( \mathcal{O} \), is generated by closing \( \{ B_h \mid h \in H \} \) under the same operations. The Borel algebra \( B \) is the smallest \( \sigma \)-algebra containing the Cantor-open sets, i.e., \( B \equiv \sigma(\mathcal{C}) \). We write \( B_0 \) for the Boolean subalgebra of \( B \) generated by \( \{ B_h \mid h \in b \} \).

**Lemma 4.**

1. \( b \subseteq c \iff B_c \subseteq B_b \)
2. \( B_b \cap B_c = B_{b \cup c} \)
3. \( B_b = 2^b \)
4. \( B_b = \bigcap_{h \in \mathcal{L}(b)} B_h \)

Note that if \( b \) is finite, then so is \( B_b \). Moreover, the atoms of \( B_b \) are in one-to-one correspondence with the subsets \( a \subseteq b \), the subset \( a \) determining which \( B_b \) occur positively in the construction of the atom:

\[
A_{ab} \triangleq \bigcap_{h \in a} B_h \cap \bigcap_{h \in b - a} \sim B_h
\]

\[
= B_a - \bigcup_{a \subseteq b - c} B_c = \{ c \in 2^b \mid c \cap a = a \}, \tag{5.4}
\]

where \( c \) denotes proper subset. The atoms \( A_{ab} \) are the basic open sets of the Cantor space. The notation \( A_{ab} \) is reserved for such sets.

**Lemma 5 (Figure 3).** For \( b \) finite and \( a \subseteq b \), \( B_a = \bigcup_{a \subseteq b} A_{ab} \).

**Proof.** By (5.4),

\[
\bigcup_{a \subseteq b} A_{ab} = \bigcup_{a \subseteq b} \{ d \in 2^b \mid d \cap b = c \}
\]

\[
= \{ d \in 2^b \mid a \subseteq d \} = B_a.
\]

**Scott Topology Properties.** Let \( \mathcal{O} \) denote the family of Scott-open sets of \( (\mathbb{H}, \subseteq) \). Following are some facts about this topology:

- The DPO \( (\mathbb{H}, \subseteq) \) is algebraic. The finite elements of \( \mathbb{H} \) are the finite subsets \( a \in \mathcal{L}(H) \), and their up-closures are \( \{ a \} \uparrow = B_a \).
- By Lemma 1(ii), the up-closures \( \{ a \} \uparrow = B_a \) form a base for the Scott topology. The sets \( B_a \) for \( h \in H \) are therefore a subbase.
- Thus, a subset \( B \subseteq \mathbb{H} \) is Scott-open iff there exists \( F \subseteq \mathcal{L}(H) \) such that \( B = \bigcup_{a \in F} B_a \).
The Cantor and Scott topologies have different Borel hierarchies. The Cantor basic open sets are those of the form \( B(\pi, \sigma, \tau) \) = \( B_\pi \cap B_\sigma \), where \( B_\pi \) and \( B_\sigma \) are the basic Cantor-open sets \( A_\pi, A_\sigma \). These are the atoms of the Boolean algebra \( B_\mathcal{O} \), and the family of clopen subsets of \( X \) is a basis for the Cantor topology. The compact-open sets are those of the form \( A_{\sigma(\pi, \tau)} \) = \( \bigcap_{\pi, \sigma, \tau} A(\pi, \sigma, \tau) \), where \( A(\pi, \sigma, \tau) \) are the basic Cantor-open sets. The Scott basic open sets are those of the form \( B(\pi, \sigma) \) = \( B_\pi \cap B_\sigma \), where \( B_\pi \) and \( B_\sigma \) are the basic Scott-open sets. These are the atoms of the Boolean algebra \( B_\mathcal{S} \), and the family of clopen subsets of \( X \) is a basis for the Scott topology.

**Theorem 7.** A function \( \mu : \{ B_n \mid b \text{ finite} \} \rightarrow [0, 1] \) extends to a measure \( \mu : \mathcal{B} \rightarrow [0, 1] \) if and only if for all finite \( b \) and all \( a \subseteq b \),
\[
\sum_{a \subseteq c \subseteq b} (-1)^{|c-a|} \mu(B_c) \geq 0.
\]

Moreover, the extension to \( \mathcal{B} \) is unique.

**Proof.** The condition is clearly necessary by (5.5). For sufficiency and uniqueness, we use the Carathéodory extension theorem. For each atom \( A_{a,b} \) of \( \mathcal{B}_b \), \( \mu(A_{a,b}) \) is already determined uniquely by (5.5) and nonnegative by assumption. For each \( B \in \mathcal{B}_b \), write \( B \) uniquely as a union of atoms and define \( \mu(B) \) to be the sum of the \( \mu(A_{a,b}) \) for all atoms \( A_{a,b} \) of \( \mathcal{B}_b \) contained in \( B \). We must show that \( \mu(B) \) is well-defined. Note that the definition is given in terms of \( b \), and we must show that the definition is independent of the choice of \( b \). It suffices to show that the calculation using atoms of \( b' = b \cup \{ h \} \), \( h \notin b \), gives the same result. Each atom of \( \mathcal{B}_b \) is the disjoint union of two atoms of \( \mathcal{B}_b \):
\[
A_{a,b} = A_{a,(h)},b \cup A_{a,b,(h)}
\]
It suffices to show the sum of their measures is the measure of \( A_{a,b} \):
\[
\mu(A_{a,(h)},b \cup A_{a,b,(h)}) = \sum_{a \subseteq c \subseteq b} (-1)^{|c-a|} \mu(B_c)
\]
\[
= \sum_{a \subseteq c \subseteq b} (-1)^{|c-a|} \mu(B_c) + \sum_{a \subseteq c \subseteq b} (-1)^{|c-a|} \mu(B_c)
\]
\[
= \mu(A_{a,b}) = \mu(A_{a,(h)},b \cup A_{a,b,(h)}).
\]

To apply the Carathéodory extension theorem, we must show that \( \mu \) is countably additive, i.e., that \( \mu(\bigcup_{n} A_n) = \sum_{n} \mu(A_n) \) for any countable sequence \( A_n \in \mathcal{B}_b \) of pairwise disjoint subsets whose union is in \( \mathcal{B}_b \). For a finite sequences \( A_n \in \mathcal{B}_b \), write each \( A_n \) uniquely as a disjoint union of atoms of \( \mathcal{B}_b \) for some sufficiently large \( b \) such that all \( A_n \in \mathcal{B}_b \). Then \( \bigcup_n A_n \in \mathcal{B}_b \), and we must show that the values of the atoms are given by (5.5). The value of \( \mu(A_{a,b}) \) is well-defined and equal to \( \sum_{n} \mu(A_n) \). We cannot have an infinite set of pairwise disjoint nonempty \( A_n \in \mathcal{B}_b \) whose union is in \( \mathcal{B}_b \) by compactness. All elements of \( \mathcal{B}_b \) are clopen sets in the Cantor topology. If \( \bigcup_n A_n \in \mathcal{B}_b \), then \( \{ A_n : n \geq 0 \} \) would be an open cover of \( A \) with no finite subcover.

**Cantor Meets Scott.** We now establish a correspondence between the Cantor and Scott topologies on \( \mathcal{B}_b \). Proofs omitted from this section can be found in Appendix C. Consider the infinite triangular matrix \( E \) and its inverse \( E^{-1} \) with rows and columns indexed by the finite subsets of \( H \), where
\[
E_{ac} = [a \subseteq c] \quad E^{-1}_{ac} = (-1)^{|c-a|} [a \subseteq c].
\]
These matrices are indeed inverses: For \( a, d \in \mathcal{B}_H \),
\[
(E \cdot E^{-1})_{ad} = \sum_{c} E_{ac} \cdot E^{-1}_{cd}
\]
\[
= \sum_{c} [a \subseteq c \cdot [c \subseteq d] \cdot (-1)^{|d-c|}]
\]
\[
= \sum_{a \subseteq c \subseteq d} (-1)^{|d-c|} = [a = d],
\]
thus \( E \cdot E^{-1} = I \) and similarly \( E^{-1} \cdot E = I \).

Recall that the Cantor basic open sets are the elements \( A_{a,b} \) for \( b \) finite and \( a \subseteq b \). Those for fixed finite \( b \) are the atoms of the Boolean algebra \( \mathcal{B}_b \). They form the basis of a \( 2^{|b|} \)-dimensional linear space. The Scott basic open sets \( A_n \) for \( a \subseteq b \) are another basis for the same space. The two bases are related by the matrix \( E[b] \), the \( 2^b \times 2^b \) submatrix of \( E \) with rows and columns indexed by subsets of \( b \). One can show that the finite matrix \( E[b] \) is invertible with inverse \( E[b]^{-1} = (E^{-1})[b] \).

---

1 References to the Borel hierarchy \( \Sigma_0^\mathcal{O} \) and \( \Pi_0^\mathcal{S} \) refer to the Scott topology. The Cantor and Scott topologies have different Borel hierarchies.
Lemma 8. Let $\mu$ be a measure on $2^H$ and $b \in \wp_+(H)$. Let $X, Y$ be vectors indexed by subsets of $b$ such that $X_a = \mu(B_a)$ and $Y_a = \mu(A_a)$ for $a \subseteq b$. Let $E[b]$ be the $2^b \times 2^b$ submatrix of $E$. Then $X \geq E[b] \cdot Y$.

The matrix-vector equation $X = E[b] \cdot Y$ captures the fact that for $a \subseteq b$, $B_a$ is the disjoint union of the atoms $A_{ab}$ of $B_a$ for $a \subseteq c \subseteq b$ (see Figure 3), and consequently $\mu(B_a)$ is the sum of $\mu(A_{ab})$ for these atoms. The inverse equation $X = E[b]^{-1} \cdot Y$ captures the inclusion-exclusion principle for $B_a$.

In fact, more can be said about the structure of $E$. For any $b \in 2^H$, finite or infinite, let $E[b]$ be the submatrix of $E$ with rows and columns indexed by the subsets of $b$. If $a \cap b = \emptyset$, then $E[a \cup b] = E[a] \otimes E[b]$, where $\otimes$ denotes Kronecker product. The formation of the Kronecker product requires a notion of pairing on indices, which in our case is given by disjoint set union. For example,

$$E[\{h_1\}] = \begin{pmatrix} \sigma & (h_1) \\ \{h_1\} & 1 & 1 \end{pmatrix} E[\{h_2\}] = \begin{pmatrix} \sigma & (h_2) \\ \{h_2\} & 1 & 1 \end{pmatrix}$$

$E[\{h_1, h_2\}] = E[\{h_1\}] \otimes E[\{h_2\}]$

The order is defined pointwise on kernels regarded as functions $2^H \times \Omega \to [0,1]$, and is Scott-continuous with respect to the order $\sqsubseteq$ on $\mathcal{M}(2^H)$.

We will show later that all ProbNetKAT programs give rise to continuous kernels.

Theorem 9. The probability measures on $(2^H, B)$ are in one-to-one correspondence with matrices $M, N \in \mathbb{R}^{P_0(H) \times P_0(H)}$ such that

(i) $M$ is diagonal with entries in $[0,1]$.
(ii) $N$ is nonnegative, and
(iii) $N = E^{-1} M E$.

The correspondence associates the measure $\mu$ with the matrices

$$N_{ab} = \mu(A_{ab}) \quad M_{ab} = [a = b] \cdot \mu(B_a).$$

6. A DCPO on Markov Kernels

In this section we define a continuous DCPO on Markov kernels. Proofs omitted from this section can be found in Appendix D.

For measures $\mu, \nu$ on $2^H$, define $\mu \sqsubseteq \nu$ if $\mu(B) \leq \nu(B)$ for all $B \in \mathcal{O}$. This order was first defined by Saheb-Djahromi [63].

Theorem 10 ([63]). The probability measures on the Borel sets generated by the Scott topology of an algebraic DCPO ordered by $\sqsubseteq$ form a DCPO.

As noted, $(2^H, B)$ is an algebraic DCPO, so Theorem 10 applies. In this case, the bottom element is $\delta_\emptyset$ and top element is $\delta_H$.

7. Continuity and Semantics of Iteration

This section develops the technology needed to establish that all ProbNetKAT programs give continuous Markov kernels and that all program operators are themselves continuous. These results are needed for the least fixpoint characterization of iteration and also pave the way for our approximation results (§8).

The main fact that underpins the results in this section is that Lebesgue integration respects the order on measures and the order on functions:

Theorem 14. Integration is Scott-continuous in both arguments:

(i) For any Scott-continuous function $f : 2^H \to [0, \infty]$, the map

$$\mu \mapsto \int f \, d\mu$$

is Scott-continuous with respect to the order $\sqsubseteq$ on $\mathcal{M}(2^H)$.
(ii) For any probability measure $\mu$, the map

$$f \mapsto \int f \, d\mu$$

is Scott-continuous with respect to the order on $[2^H, [0, \infty]]$.

The proofs of the remaining results in this section are somewhat long and mostly routine, but can be found in Appendix E.
We now formalize a notion of approximation for ProbNetKAT as defined in the Cantor topology. Let \( \mu \) be a Cantor-continuous random variable. Let \( \nu \) denote the output distribution and its approximations. Then \( E[Q] \leq E_\nu[Q] \leq \ldots \) and \( \sup_{\nu_n} E[Q] = E[Q] \).

Proof. By induction on \( p \) and continuity of the operators.

This means that any program can be approximated using only finite distributions! In particular, we can compute the results of many queries without ever having to worry about continuous distributions:

**Theorem 21.** The approximants of a program \( P \) form a \( \subseteq \)-increasing chain with supremum \( P \), that is

\[
[\mu]_1 \subseteq [\mu]_2 \subseteq \ldots \quad \text{and} \quad \bigcup_{n \geq 0} [\mu]_n = [\mu]
\]

Proof. Follows directly from Theorems 21 and 14.

The rest of this section gives more general approximation results for measures and kernels on \( 2^H \). We present an implementation based on \([-1,1]\), and applications of the above results to compute expectations in the next section.

A measure is a finite discrete measure if it is of the form \( \sum_{a \in F} r_a \delta_a \), where \( F \in \mathcal{V}_\infty(\mathcal{V}_\infty(H)) \) is a finite set of finite subsets of packet histories \( H \), \( r_a \geq 0 \) for all \( a \in F \), \( \sum_{a \in F} r_a = 1 \). Without loss of generality, we can write any such measure in the form \( \sum_{a \in b} r_a \delta_a \) for any \( b \in \mathcal{V}_\infty(H) \) such that \( \bigcup F \subseteq b \) by taking \( r_a = 0 \) for \( a \in 2^H \setminus F \).

Saheb-Djahromi [63, Theorem 3] shows that every measure is a supremum of a directed set of finite discrete measures. This implies that the measures form a continuous DCPO with basis consisting of the finite discrete measures. In our model, the finite discrete measures have a particularly nice characterization:

For \( \mu \) a measure and \( b \in \mathcal{V}_\infty(H) \), define the restriction of \( \mu \) to \( b \) to be the finite discrete measure \( \mu \mid b \triangleq \sum_{a \subseteq b} \mu(A_a) \delta_a \).

**Theorem 23.** The set \( \{ \mu \mid b \mid b \in \mathcal{V}_\infty(H) \} \) is a directed set with supremum \( \mu \). Moreover, the DCPO of measures is continuous with basis consisting of the finite discrete measures.

We can lift the result to continuous kernels, which implies that every program is approximated arbitrarily closely by programs whose outputs are finite discrete measures.

**Corollary 24.** Let \( b \in \mathcal{V}_\infty(H) \). Then \( (P \mid b)(a, -) = P(a, -) \mid b \).

8. Approximation

We now formalize a notion of approximation for ProbNetKAT programs. Given a program \( p \), we define the \( n \)-th approximant \([p]_n\) inductively as

\[
[p]_n = \begin{cases} p & \text{for } \langle p \rangle \text{ primitive} \\ [q \oplus r]_n = [q]_n \oplus [r]_n \\ [q \& r]_n = [q]_n \& [r]_n \\ [q \cdot r]_n = [q]_n \cdot [r]_n \\ [q]_n = ([q]_n)^{(n)} \end{cases}
\]

Intuitively, \([p]_n\) is just \( p \) where iteration \(-^*\) is replaced by bounded iteration \(-^{(n)}\). Let \([p]_n\) denote the Markov kernel obtained from the \( n \)-th approximant: \([p]_n\).

**Theorem 17.** The following semantic operations are continuous functions of the DCPO of continuous kernels: product, parallel composition, curry, sequential composition, choice, iteration. (Figure 4.)

The semantics of iteration presented in [15], defined in terms of an infinite process, coincides with the least fixpoint semantics presented here. The key observation is the relationship between weak convergence in the Cantor topology and fixpoint convergence in the Scott topology:

**Theorem 18.** Let \( A \) be a directed set of probability measures with respect to \( \subseteq\) and let \( f : 2^H \rightarrow [0,1] \) be a Cantor-continuous function. Then

\[
\lim_{\mu \in A} \int_{c \in 2^H} f(c) \cdot d\mu = \int_{c \in 2^H} f(c) \cdot d(\bigcup A).
\]

This theorem implies that \( P^{(n)} \) weakly converges to \( P^* \) in the Cantor topology. [15] showed that \( P^{(n)} \) also weakly converges to \( P^\# \) in the Cantor topology, where we let \( P^\# \) denote the iterate of \( P \) as defined in [15]. But since \((2^H, C)\) is a Polish space, this implies that \( P^* = P^\# \).

**Lemma 19.** In a Polish space \( D \), the values of

\[
\int_{a \in D} f(a) \cdot \mu(da)
\]

for continuous \( f : D \rightarrow [0,1] \) determine \( \mu \) uniquely.

**Corollary 20.** \( P^\# = \bigcup_n P^{(n)} = P^* \).

9. Implementation and Case Studies

We built an interpreter for ProbNetKAT in OCaml that implements the denotational semantics as presented in Figure 2. Given a query,
we briefly describe how we model the components of a network in NetKAT implementations of each of the following routing schemes: engineering (TE) approaches have been explored. We built ProbNetKAT, extending the encodings from net2's Abilene backbone. Before presenting our case studies, we briefly describe how we model the components of a network in ProbNetKAT, extending the encodings from §2.

**Routings.** In the networking literature, a large number of traffic engineering (TE) approaches have been explored. We built ProbNetKAT implementations of each of the following routing schemes:

- **Equal Cost Multipath Routing (ECMP):** The network uses all least-cost paths between each source-destination pair, and maps incoming traffic flows onto those paths randomly. Using multiple paths generally reduces congestion and increases throughput, but this scheme can perform poorly when multiple paths traverse the same bottleneck link.

- **k-Shortest Paths (KSP):** The network uses the top k-shortest paths between each pair of hosts, and again maps incoming traffic flows onto those paths randomly. This approach inherits the performance benefits of ECMP and also provides improved fault-tolerance properties since it always spreads traffic across k distinct paths.

- **Multipath Routing (Multi):** This is similar to KSP, except that it makes an independent choice from among the k-shortest paths at each hop rather than just once at ingress. This approach dynamically routes around bottlenecks and failures but can use extremely long paths—even ones containing loops.

- **Oblivious Routing (Räcke):** The network forwards traffic using a pre-computed probability distribution on carefully constructed overlays. The distribution is constructed in such a way that guarantees worst-case congestion within a polylogarithmic factor of the optimal scheme, regardless of the demands for traffic.

Note that all of these schemes rely on some form of randomization and hence are probabilistic in nature.

**Traffic Model.** Network operators often use traffic models constructed from historical data to predict future performance. We built a small OCaml tool that translates traffic models into ProbNetKAT programs using a simple encoding. Assume that we are given a traffic matrix (TM) that relates pairs of hosts \((u, v)\) to the amount of traffic that will be sent from \(u\) to \(v\). By normalizing each TM entry using the aggregate demand \(\sum_{(u,v)} TM(u,v)\), we get a probability distribution \(d\) over pairs of hosts. For a pair of source and destination \((u, v)\), the associated probability \(d(u,v)\) denotes the amount of traffic from \(u\) to \(v\) relative to the total traffic. Assuming uniform packet sizes, this is also the probability that a random packet generated in the network has source \(u\) and destination \(v\). So, we can encode a TM as a program that generates packets according to \(d\):

\[
inp \triangleq \bigoplus_{d(u,v)} \pi(u,v)!
\]

where \(\pi(u,v)! \triangleq \text{src} \leftarrow u; \text{dst} \leftarrow v; \text{sw} \leftarrow u\) \(\pi(u,v)!\) generates a packet at \(u\) with source \(u\) and destination \(v\). For any (non-empty) input, \(\text{inp}\) generates a distribution \(\mu\) on packet histories which can be fed to the network program. For instance, consider a uniform traffic distribution for our 4-switch example where each node sends equal traffic to every other node. There are twelve \((u,v)\) pairs with \(u \neq v\). So, \(d(u,v)_{u \neq v} = \frac{1}{12}\) and \(d(u,u) = 0\). We also store the aggregate demand as it is needed to model queries such as expected link congestion, throughput etc.

**Queries.** Our implementation can be used to answer probabilistic queries about a variety of network performance properties. §2 showed an example of using a query to compute expected congestion. We can also measure expected mean latency in terms of path length:

\[
\text{let path_length } (h:\text{Hist.t}) : \text{Real.t} = \\
\text{Real.of_int } (\text{Hist.length } h) / 2 + 1
\]

\[
\text{let lift_query_avg } (q:\text{Hist.t} -> \text{Real.t}) : (\text{HSet.t} -> \text{Real.t}) = \\
\text{fun hset -> } \\
\text{let n = HSet.length hset in } \\
\text{if n = 0 then Real.zero else } \\
\text{let sum = HSet.fold hset \~\text{init}Real.zero \~\text{f}(\text{fun acc h -> Real.(acc + q h)}) in } \\
\text{Real.(sum / of_int n)}
\]

The latency function \(\text{path_length}\) counts the number of switches in a history. We lift this function to sets and compute the expectation \(\text{lift_query_avg}(\text{query})\) by computing the average over all histories in the set (after discarding empty sets).

**Case Study: Abilene.** To demonstrate the applicability of ProbNetKAT for reasoning about a real network, we performed a case study based on the topology and traffic demands from Internet2’s Abilene backbone network as shown in Figure 5 (a). We evaluate the
traffic engineering approaches discussed above by modeling traffic matrices based on NetFlow traces gathered from the production network. A sample TM is depicted in Figure 5 (b).

Figures 3 (c,d,g) show the expected maximum congestion, throughput and mean latency. Because we model a network using the Kleene star operator, we see that the values converge monotonically as the number of iterations used to approximate Kleene star increases, as guaranteed by Theorem 22.

Failures. Network failures such as a faulty router or a link going down are common in large networks [16]. Hence, it is important to be able to understand the behavior and performance of a network in the presence of failures. We can incorporate a failure models by assigning empirically measured probabilities to various components—e.g., we can modify our encoding of the topology so that every link in the network drops packets with probability \( \frac{1}{10} \):

\[
\ell_{1,2} \triangleq sw = S_1 : pt = 2 : dup ; (sw \leftarrow S_2 : pt \leftarrow 1 : dup) \triangleq 0 \\
\& sw = S_2 : pt = 1 : dup ; (sw \leftarrow S_1 : pt \leftarrow 2 : dup) \triangleq 0
\]

Figures 5 (e-f) show the network performance for Abilene under this failure model. As expected, congestion and throughput decrease as more packets are dropped. As every links drops packets probabilistically, the relative fraction of packets delivered using longer links decreases—hence, there is a decrease in mean latency.

Loop detection. Forwarding loops in a network are extremely undesirable as they increase congestion and can even lead to black holes. With probabilistic routing, not all loops will necessarily result in a black hole—if there is a non-zero probability of exiting a loop, every packet entering it will eventually exit. Consider the example of random walk routing in the four-node topology from Figure 1. In a random walk, a switch either forwards traffic directly to its destination or to a random neighbor. As packets are never duplicated and only exit the network when they reach their destination, the total throughput is equivalent to the fraction of packets that exit the network. The fraction of packets exiting increases monotonically with number of iterations and converges to 1. Moreover, histories can be queried to test if it encountered a topological loop by checking for duplicate locations.

Hence, given a model that computes all possible history prefixes that appear in the network, we can query it for presence of loops. We do this by removing \textit{out} from our standard network model and using \textit{in} : (p ; t) \* ; p instead. This program generates the required distribution on history prefixes. Moreover, if we generalize packets with wildcard fields, similar to HSA [32], we can check for loops symbolically. We have extended our implementation in this way, and used it to check whether the network exhibits loops on a number of routing schemes based on probabilistic forwarding.

10. Related Work

This paper builds on previous work on NetKAT [3, 14] and ProbNetKAT [15]. The main contribution of this paper is to develop a new semantics for ProbNetKAT based on ordered domains as well as applications to real-world networking problems.

Domain Theory. The domain-theoretic treatment of probability measures goes back to the seminal work of Saheb-Djahromi [63], who was the first to identify and study the CPO of probability measures. Jones and Plotkin [28, 29] generalized and extended this work by giving a category-theoretical treatment and proving that the probabilistic powerdomain is a monad. It is an open problem if there exists a cartesian-closed category of continuous DCPOs that is closed under the probabilistic powerdomain; see [30] for a discussion. This is an issue for higher-order probabilistic languages, but not for ProbNetKAT, which is strictly first-order. Edalat [10–12] gives a computational account of measure theory and integration for general metric spaces based on domain theory. More recent papers on probabilistic powerdomains are [19, 23, 30]. All this work is ultimately based on the pioneering ideas of Scott [64].

Probabilistic Logic and Semantics. Computational models and logics for probabilistic programming have been extensively studied. Denotational and operational semantics for probabilistic while programs were first studied by Kozen [37]. Early logical systems for reasoning about probabilistic programs were proposed in [38, 59, 62]. There are also numerous recent efforts [18, 20, 39, 42, 47]. Probabilistic programming in the context of artificial intelligence has also been extensively studied in recent years [5, 61]. Probabilistic automata in several forms have been a popular model going back to the early work of Paz [54], as well as more recent efforts [45, 65, 66]. Denotational models combining probability and nondeterminism have been proposed by several authors [44, 69, 70], and general models for labeled Markov processes, primarily based on Markov kernels, have been studied extensively [8, 51, 52].

Our semantics is also related to the work on event structures [50, 71]. A (Prob)NetKAT program denotes a simple (probabilistic) event structure: packet histories are events with causal dependency given by extension and with all finite subsets consistent. We have to yet explore whether the event structure perspective on our semantics could lead to further applications and connections to e.g. (concurrent) games.

Networking. Network calculus is a general framework for analyzing network behavior using tools from queuing theory [6]. It has been used to reason about quantitative properties such as latency, bandwidth, and congestion. The stochastic branch of network calculus provides tools for reasoning about the probabilistic behavior, especially in the presence of statistical multiplexing, but is often considered difficult to use. In contrast, ProbNetKAT is a self-contained framework based on a precise denotational semantics.

Traffic engineering has been extensively studied in recent years and a wide variety of approaches have been proposed for data-center networks [2, 27, 55, 67, 73] and wide-area networks [4, 22, 24, 26, 31, 48, 57, 68]. These approaches try to optimize various metrics such as congestion, throughput, latency, fault tolerance, fairness etc. Optimal techniques often have high overheads [7]. As a result, oblivious [4, 34] and hybrid approaches [24, 26] with near-optimal performance have gained adoption.

11. Conclusion

This paper presents a new order-theoretic semantics for ProbNetKAT in the style of classical domain theory. The semantics allows a standard least-fixpoint treatment of iteration, and enables new modes of reasoning about the probabilistic network behavior. We have used these theoretical tools to analyze several randomized routing protocols on real-world data.

Previous work on deterministic NetKAT included a decision procedure and a sound and complete axiomatization. In the presence of probabilities we expect a decision procedure will be hard to devise, as witnessed by several undecidability results on probabilistic automata. We intend to explore decision procedures for restricted fragments of the language. Another interesting direction is to compile ProbNetKAT programs into suitable automata that can then be analyzed by a probabilistic model checker such as PRISM [41]. A sound and complete axiomatization remains subject of further investigation, we can draw inspiration from recent work [40, 43]. Another interesting direction for future work is to develop a weighted version of NetKAT, where instead of probabilities we consider weights from an arbitrary semiring, opening up several other applications—e.g. in cost analysis. Finally, we would like to explore efficient implementation techniques including compilation, as well as approaches based on sampling, following several other probabilistic languages [5, 53].
References


