Nondeterminism and Probabilistic Choice: Obeying the Laws

Michael Mislove*

Department of Mathematics
Tulane University
New Orleans, LA 70118
mwm@math.tulane.edu

Abstract. In this paper we describe how to build semantic models that support both nondeterministic choice and probabilistic choice. Several models exist that support both of these constructs, but none that we know of satisfies all the laws one would like. Using domain-theoretic techniques, we show how models can be devised using the "standard model" for probabilistic choice, and then applying modified domain-theoretic models for nondeterministic choice. These models are distinguished by the fact that the expected laws for nondeterministic choice and probabilistic choice remain valid. We also describe some potential applications of our model to aspects of security.

1 Introduction

The most widely employed method for modeling concurrent computation is to take sequential composition as a primitive operator, and then to use nondeterministic choice to generate an interleaving semantics for parallel composition. This approach is well-supported by the models of computation, including both the standard domain-theoretic models (cf. [10]), and the metric space approach (cf. [3]). These and similar approaches to modeling nondeterminism satisfy the basic assumption that nondeterministic choice is a commutative, associative and idempotent operation. In fact, the results from [10] characterize the three fundamental *power domains* in terms of their universal properties as ordered semilattices – i.e., that they each are the object-level of a left adjoint to a forgetful functor from an appropriate category.

More recently, probabilistic choice has been added as a family of operators in the syntax of the language under study. One can trace this research in denotational semantics to the work of Saheb-Dharjomi [24]. While this work was the first to consider modeling probabilistic choice as a domain, the most influential work along this line is without question the PhD thesis of Jones [11], where it was shown that Saheb-Dharjommi's construction could be extended to "measures" having total variation less than 1, and that the probabilistic power domain of

* Partial support provided by the National Science Foundation and the US Office of Naval Research

a continuous domain is again continuous. Perhaps more importantly, Jones provided a finitary characterization of the probabilistic power domain in terms of equations the operators should satisfy. If these equations hold, then her model is universal.

One issue that causes problems in the regard is that the difference between nondeterministic choice and probabilistic choice is not clearly delineated. Indeed, the title of [11] reveals an identification of probabilistic choice as a form of nondeterminism. Yet probabilistic choice operators are not associative. For example,[1]

$$(p \,{}_{.5}\!+ q) \,{}_{.5}\!+ r = p \,{}_{.25}\!+ (q \,{}_{2/3}\!+ r).$$

Still, several authors have attempted to incorporate *both* nondeterministic choice and probabilistic choice within one model. None that we know of has accomplished that goal completely satisfactorily. For example, in [20] a model incorporating probabilistic choice is built by simply applying Jones' probabilistic power domain to the standard failures-divergences model for CSP. But, the natural extension of nondeterministic choice to this model is not idempotent, so a fundamental law of nondeterminism fails in the model. To explain this anomaly, it is argued in [21] that the probability that the process $(p \,{}_{.5}\!+ q) \sqcap (p \,{}_{.5}\!+ q)$ actually acts like p is .25, since each branch resolves the probabilistic choice independently. On the other hand, one might argue that the process in question is supposed to act like one branch, not like both – ie, the probabilistic choice should be resolved *after* the nondeterministic choice is resolved. But models for CSP typically do not discriminate closely enough to keep track of the order in which choices are resolved, something that is reflected by the fact that the nondeterministic choice operator distributes through the probabilistic choice operators.

This brings us to the issue we are interested in confronting: how to build denotational models for more general process algebras which support both nondeterministic choice and probabilistic choice, so that the laws for nondeterministic choice and for probabilistic choice that one expects to hold actually are valid. Our construction relies heavily on domain theory and some of the constructs it provides. The work here is closely related to the emerging area of devising semantic models using coalgebraic techniques (cf., e.g., [23] for an introduction).

There are several approaches that have been put forward for modeling probabilistic choice, including

- approaches such as [16, 18] that focus on state-based models and use probabilistic transition systems to reflect the operational behavior of the system under study. In these approaches, discrete probabilistic models are considered, and the focus is on the probability of a process being in a given state *after* it has executed a given action.

[1] We will use the notation $p \,{}_{\lambda}\!+ q$ to denote a probabilistic choice in which the process has probability λ of acting like p, and probability $1 - \lambda$ of acting like q, where $0 \leq \lambda \leq 1$.

- approaches such as [7] and [17] that use a process algebra in which probabilistic choice is substituted for nondeterministic choice. Here, and in the next case, the focus is on the probability that the process in question acts like one branch or the other from the choices listed.
- approaches such as [20, 4, 8] that extend a process algebra by adding probabilistic choice operators. If the branches have distinct initial actions, then the focus is on the probability of the process executing a given action, rather than on the state after a given action is executed.

The approach nearest our own is the last, but, as just remarked, none of these approaches provides a semantic model in which the laws we are interested in hold. Moreover, there are close links between all these approaches, so they should be viewed as variants of one another. Our goal in this paper is to show how a model supporting both nondeterministic choice and probabilistic choice can be devised, so that the expected laws for nondeterministic choice and for probabilistic choice all hold.

Some more extensive comments about the nature of our results are in order. As stated above, we use domain theory as the basis for the constructions we devise. There is a long history of modeling probabilistic choice in this area, dating back to the seminal work of Saheb-Djarhomi [24] in which a now standard construction of a cpo supporting probabilistic choice was given, beginning with an underlying cpo. This work led to the results in [11, 12] that clarified and expanded the nature of Saheb-Djarhomi's construction, and also showed that this construction, when applied to a continuous domain, yields a continuous domain. This is the construction used in [20] for *probabilistic CSP*, which is simply the probabilistic power domain $\mathcal{P}_{Pr}(\mathbb{FD})$ of the failures-divergences model $\mathbb{FD}$ for untimed CSP. As we noted above, the extension of the nondeterministic choice operation from $\mathbb{FD}$ to $\mathcal{P}_{Pr}(\mathbb{FD})$ is not idempotent. In fact, there is no *affine* idempotent operation on $\mathcal{P}_{Pr}(\mathbb{FD})$ that extends the nondeterministic choice operator on (the image of) $\mathbb{FD}$ (in $\mathcal{P}_{Pr}(\mathbb{FD})$), since the extension used in [20] is one such, and the *splitting lemma* implies there is only one such. There is no obvious candidate for a nondeterministic choice operator on this model, even if one drops the affinity hypothesis.

Our approach to remedying this problem is to take the construction one step further: we apply a power domain operator to $\mathcal{P}_{Pr}(\mathbb{FD})$. In fact, there are three such power domains - the lower, the upper and the convex power domains. While these produce new nondeterministic choice operators, one soon discovers that the probabilistic choice operators on $\mathcal{P}_{Pr}(\mathbb{FD})$, when extended to any of these power domains do not satisfy the expected laws – once again the model fails to satisfy all the laws expected. However, we are not far from our desired model. We simply consider the family of *affine closed* sets in each of the respective power domains, and we find that in each case, these do provide models where all the laws – both those of nondeterminism and of probabilistic choice – are valid. What is more, in the case of the lower or upper power domains, the models we construct yield a bounded complete domain, when applied to a Scott domain. In particular, the compositions $\mathcal{P}_{PL} \circ \mathcal{P}_{Pr}$ and $\mathcal{P}_{PU} \circ \mathcal{P}_{Pr}$ are

continuous endofunctors of the category BCD of continuous, bounded complete domains – the continuous analogues of Scott domains. Since this category is cartesian closed, one can in principle construct models for the lambda calculus extended to include both probabilistic choice operators and nondeterministic choice operators. Unfortunately, as far as we know, this result does not extend to the case of the convex power domain: while $\mathcal{P}_{PC} \circ \mathcal{P}_{Pr}$ is continuous, we are unable to show it lands back in RB, the category of retracts of bifinite domains. Even so, our models have the added bonus that the probabilistic choice operators do not distribute through the nondeterministic choice operators, which has important implications for the application of the models we build to the area of security. We outline this application in the last section of the paper.

The rest of the paper is organized as follows. In the next section we review some background in domain theory and we review the principal construction of a model for probabilistic choice in domains – the probabilistic power domain, followed by a description of PCSP from [20]. This serves to present a motivating example for our work, which demonstrates how the failure of an expected law in a semantic model can lead to unexpected results in the behavior of a process. Actually, such results are inevitable if one uses the model constructed in [20] because of the way in which the CSP operators are defined on their model. The next section gives our construction, showing how one can build a model supporting both nondeterministic choice and probabilistic choice over any bounded complete domain. Finally, in the last section, we review our results and point out how they relate to some of the other constructions that have been put forward.

2 Domains and the Probabilistic Power Domain

In this section, we review some of the basics we need to describe our results. A good reference for most of this can be found in [2]. To begin, a *partial order* is a non-empty set endowed with a reflexive, antisymmetric and transitive relation. If P is a partial order, then a subset $D \subseteq P$ is *directed* if every finite subset of D has an upper bound in D. We say P is *directed complete* if every directed subset of D has a least upper bound, $\sqcup D$, in P. Such partial orders we call *dcpos*, and we use the term *cpo* for a dcpo that also has a least element, usually denoted $\bot$.

Dcpos can be endowed with a topology that plays a fundamental role in the theory. A subset $U \subseteq P$ is *Scott open* if $U = \uparrow U = \{x \in P \mid (\exists u \in U)\, u \leq x\}$ is an upper set, and, for every directed set D, if $\sqcup D \in U$, then $D \cap U \neq \emptyset$. The Scott continuous functions $f\colon P \to Q$ between dcpos are easy to characterize order-theoretically: they are exactly the maps that preserve the order and also preserve suprema of directed sets – $f(\sqcup D) = \sqcup f(D)$ for all $D \subseteq P$ directed.

The category DCPO of (d)cpos and Scott continuous maps is a cartesian closed category. More precisely, the product of (d)cpos is another such, there is a terminal object among dcpos – the one point dcpo – and there is an *internal hom*: for dcpos P and Q, the family $[P \to Q]$ of continuous maps between them is a dcpo in the pointwise order, and $[P \times Q \to R] \simeq [P \to [Q \to R]]$ for dcpos P, Q and R. What is just as important is that we can find minimal solutions to

domain equations within these categories, assuming the equations are defined by continuous endofunctors defined on DCPO.

Continuous domains: If P is a dcpo and $x \leq y \in P$, then we write $x \ll y$ if and only if $(\forall D \subseteq P \text{ directed})\, y \leq \sqcup D \;\Rightarrow\; (\exists d \in D)\, x \leq d$. P is *continuous* if $\Downarrow y = \{x \in P \mid x \ll y\}$ is directed and $y = \sqcup \Downarrow y$ for all $y \in P$. Unfortunately, the category CON of continuous domains and Scott continuous maps is not cartesian closed. In fact, a classification of the maximal cartesian closed subcategories of CON is given in [2]. Of particular interest to us is the category COH of *coherent domains* and Scott continuous maps (cf. [2]).

Continuous domains admit standard models for nondeterminism, each of which is the object level of a left adjoint to an appropriate forgetful functor. In the case of coherent domains, these *power domains* can be defined as:

The Lower Power Domain is defined as $\mathcal{P}_L(P) = \{X \subseteq D \mid \emptyset \neq X = \downarrow X \text{ Scott closed}\}$, ordered by inclusion.

The Upper Power Domain is defined as $\mathcal{P}_U(D) = \{X \subseteq P \mid \emptyset \neq X = \uparrow X \text{ Scott compact}\}$ ordered by reverse inclusion.

The Convex Power Domain can then be defined as $\mathcal{P}_C(P) = \{X \subseteq P \mid X = \downarrow X \cap \uparrow X \;\wedge\; \downarrow X \in \mathcal{P}_L(P) \;\wedge\; \uparrow X \in \mathcal{P}_U(P)\}$, ordered by $X \sqsubseteq Y$ iff $\downarrow X \subseteq \downarrow Y$ and $\uparrow X \supseteq \uparrow Y$.

Each of these constructs is an ordered semilattice, in that each admits an associative, commutative and idempotent operation that preserves directed suprema (in the first two cases, the operation is simply union, while in the last it is obtained by taking the *convex hull* of the union of the components. Moreover, each is the object level of a left adjoint to a forgetful functor from an appropriate category of ordered semilattice domains and Scott continuous maps to the category of coherent domains and Scott continuous maps.

The probabilistic power domain: We now describe the construction that allows probabilistic choice operators to be added to a domain. This construction was first investigated by Saheb-Djarhomi [24], who showed that the family he defined yields a cpo. The construction later was refined by Jones [11, 12] where it also was shown that the probabilistic power domain of a continuous domain is again continuous. The definition of the more general construction goes as follows.

Definition 1. *If P is a dcpo, then a* continuous valuation *on P is a mapping $\mu\colon \Sigma D \to [0,1]$ defined on the Scott open subsets of P that satisfies:*

1. $\mu(\emptyset) = 0$.
2. $\mu(U \cup V) = \mu(U) + \mu(V) + \mu(U \cap V)$,
3. *μ is monotone, and*
4. $\mu(\cup_i U_i) = \sup_i \mu(U_i)$, *if $\{U_i \mid i \in I\}$ is an increasing family of Scott open sets.*

We order this family pointwise: $\mu \leq \nu \;\Leftrightarrow\; \mu(U) \leq \nu(U)$ $(\forall U \in \Sigma P)$, and we denote the family of continuous valuations on P by $\mathcal{P}_{Pr}(P)$.

It was Lawson [15] who first showed the connection between continuous valuations and measures on the cpo P – indeed, he showed that, in the case P has a countable basis, there is a one-to-one correspondence between regular Borel measures on P and continuous valuations on ΣP. This result has recently been generalized to a much larger category of topological spaces.

The probabilistic power domain construction has been fraught with problems almost from its inception. An excellent discussion of this can be found in [14]. One of the key properties of domain theory has been the ample supply of cartesian closed categories that are closed under each of the constructs the theory has to offer. For example, the constructions needed to build Scott's D_∞ model all leave the category of continuous, bounded complete domains invariant (a domain is *bounded complete* if every non-empty subset has an infimum). It was the fact that the convex power domain does not leave this category invariant that led to the discovery of the cartesian closed category of bifinite domains and Scott continuous maps. *Bifinite domains* are those that can be expressed as the limit of a directed family of finite posets under embedding-projection pairs; they all are algebraic, while the category RB of *retracts of bifinite domains* is a cartesian closed category containing continuous domains such as the unit interval. Since $\mathcal{P}_{Pr}(P)$ is continuous if P is, but never algebraic, the natural question is whether the cartesian closed category RB is closed under this construction. The answer remains unknown. More generally, there is no know cartesian closed category of continuous domains that is closed under the probabilistic power domain operator. This means, in particular, that the only cartesian closed categories which are known to be closed under this construct are CPO and DCPO, the categories of cpos (dcpos) and Scott continuous maps, respectively. This is unsatisfactory, since so little is known about the structure of the objects in these categories.

Among the continuous valuations on a dcpo, the *simple valuations* are particularly easy to describe. They are of the form $\mu = \Sigma_{x \in F} r_x \cdot \delta_x$, where $F \subseteq P$ is a finite subset, δ_x represents point mass at x (the mapping sending an open set to 1 precisely if it contains x, and to 0 otherwise), and $r_x \in [0,1]$ satisfy $\Sigma_{x \in F} r_x \leq 1$. In this case, the *support* of μ is just the family F. The so-called *Splitting Lemma* of [11] is a fundamental result about the order on simple measures:

Lemma 1 (Splitting Lemma [11]). *If $\mu = \Sigma_{x \in F} r_x \cdot \delta_x$ and $\nu = \Sigma_{y \in G} s_y \cdot \delta_y$ are simple valuations, then $\mu \leq \nu$ if and only if there is a family of non-negative real numbers $\{t_{x,y} \mid x \in F, y \in G\}$ satisfying*

1. *For all $x \in F$, $\Sigma_{y \in G} t_{x,y} = r_x$.*
2. *For all $y \in G$, $\Sigma_{x \in F} t_{x,y} \leq s_y$, and*
3. *If $t_{x,y} \neq 0$, then $x \leq y$.*

Moreover, $\mu \ll \nu$ if and only if $\leq$ is replaced by $<$ in 2), and by $\ll$ in 3). □

It follows from this result that the probabilistic power domain of a continuous domain is again continuous. But nothing much more is known about the structure of $\mathcal{P}_{Pr}(P)$; in particular, a simple example is given in [11] of a bounded complete domain P for which $\mathcal{P}_{Pr}(P)$ is not bounded complete.

One fact about the probabilistic power domain that has been established is that it leads to an endofunctor on continuous domains. That is, each continuous map $f\colon P \to Q$ between (continuous) domains can be lifted to a continuous maps $\mathcal{P}_{Pr}(f)\colon \mathcal{P}_{Pr}(P) \to \mathcal{P}_{Pr}(Q)$ by $\mathcal{P}_{Pr}(f)(\mu)(U) = \mu(f^{-1}(U))$. In fact, [11] shows that the resulting functor is a left adjoint, which means that $\mathcal{P}_{Pr}(P)$ is a free object over P in an appropriate category. The category in question can be described in terms of probabilistic choice operators satisfying certain laws. The relevant laws are the following (cf. [11]):

Definition 2. *A* probabilistic algebra *is a dcpo A endowed with a family of Scott continuous operators ${}_\lambda{+}\colon A \times A \to A$, $0 \leq \lambda \leq 1$ such that $(\lambda, a, b) \mapsto a \,{}_\lambda{+}\, b\colon [0,1] \times A \times A \to A$ is continuous and so that the following laws hold for all $a, b, c \in A$:*

- $a \,{}_\lambda{+}\, b = b \,{}_{1-\lambda}{+}\, a$,
- $(a \,{}_\lambda{+}\, b) \,{}_\rho{+}\, c = a \,{}_{\lambda\rho}{+}\, (b \,{}_{\frac{\rho(1-\lambda)}{1-\lambda\rho}}{+}\, c)$ (if $\lambda\rho < 1$).
- $a \,{}_\lambda{+}\, a = a$, *and*
- $a \,{}_1{+}\, b = a$.

The operations ${}_\lambda{+}$ are defined on $\mathcal{P}_{Pr}(P)$ in a pointwise fashion, so for instance, $\mu \,{}_\lambda{+}\, \nu = \lambda\mu + (1-\lambda)\nu$. It then is routine to verify that $\mathcal{P}_{Pr}(P)$ is a probabilistic algebra over P for each dcpo P.

2.1 Probabilistic CSP

The model for probabilistic CSP – PCSP as it is denoted – that was devised in [20] is now easy to describe. It is built by simply applying the probabilistic power domain operator to the failures-divergences model for CSP. But some extra information is provided to allow a better understanding of the structure of the model.

First, it is shown in [20] that $\mathbb{FD}$ is an algebraic cpo: indeed, the compact elements are the "truncated processes" $\{p{\downarrow_n} \mid p \in \mathbb{FD} \;\&\; n \geq 0\}$, where $p{\downarrow_n}$ is the process that acts like p for at most n steps, and then diverges (recall that DIV is the least element of $\mathbb{FD}$). In fact, in [20] it is shown that the n-step truncations of any process form an increasing sequence whose supremum is the original process, and it is easy to show that $p{\downarrow_n}$ is compact for every n. Moreover, the very definition of $\mathbb{FD}$ allows one to conclude that the union of any non-empty family processes in $\mathbb{FD}$ is another such, which combined with the result just cited shows that $\mathbb{FD}$ is a Scott domain – ie, a bounded complete, algebraic cpo. As such, applying the probabilistic power domain operator to $\mathbb{FD}$ results in a continuous probabilistic algebra, and this is the model for probabilistic CSP used in [20].

The syntax of PCSP is not much different from that of CSP. Indeed, PCSP simply adds the family of operators ${}_\lambda{+}$ for $0 \leq \lambda \leq 1$ to the usual family of operators of untimed CSP. So, for example, we can reason about processes such as $(a \to STOP) \,{}_\lambda{+}\, (b \to STOP \;\Box\; c \to STOP)$, which will act like $a \to STOP$ λ percent of the time, and offer the external choice of doing a b or a c the rest of

the time. The approach provided in [20] to reasoning about such processes is via weakest precondition semantics, where weakest preconditions for probabilistic processes are represented as random variables.

An obvious question is how to interpret the operators of CSP in $\mathcal{P}_{Pr}(\mathbb{FD})$. This is accomplished by analyzing the construction itself. Namely, $\mathcal{P}_{Pr}(\mathbb{FD})$ is a set of continuous mappings from the set of Scott open sets of $\mathbb{FD}$ to the unit interval. So, for example, given a unary operator $f\colon \mathbb{FD} \to \mathbb{FD}$, we can extend this to $\mathcal{P}_{Pr}(\mathbb{FD})$ by $\mathcal{P}_{Pr}(f)\colon \mathcal{P}_{Pr}(\mathbb{FD}) \to \mathcal{P}_{Pr}(\mathbb{FD})$ by $\mathcal{P}_{Pr}(f)(\mu)(U) = \mu(f^{-1}(U))$. Similar reasoning shows how to extend operators of higher arity (this relies on the fact that the product of Scott open sets is again Scott open). Two facts emerge from this method:

- If we embed $\mathbb{FD}$ into $\mathcal{P}_{Pr}(\mathbb{FD})$ via the mapping $p \mapsto \delta_p$, then the interpretation of each CSP operator on $\mathbb{FD}$ *extends* to a continuous operator on $\mathcal{P}_{Pr}(\mathbb{FD})$: this means that the mapping from $\mathbb{FD}$ into $\mathcal{P}_{Pr}(\mathbb{FD})$ is compositional for all the operators of CSP. This has the consequence that any laws that the interpretation of CSP operators satisfy on $\mathbb{FD}$ still hold *on the image of* $\mathbb{FD}$ *in* $\mathcal{P}_{Pr}(\mathbb{FD})$.
- The way in which the operators of CSP are extended to the model of PCSP forces all the CSP operators to distribute through the probabilistic choice operators. For example, we have

  $$a \to (p \,{}_\lambda{+}\, q) = (a \to p) \,{}_\lambda{+}\, (a \to q),$$

  for any event a and any processes p and q. This has the result that some of the laws of CSP fail to hold *on all of* $\mathcal{P}_{Pr}(\mathbb{FD})$.

Here is an example illustrating the second point:

Example 1. Consider the process

$$(p \,{}_{.5}{+}\, q) \sqcap (p \,{}_{.5}{+}\, q).$$

The internal choice operator $\sqcap$ is supposed to be idempotent, but using the fact that, when lifted to PCSP, the CSP operators distribute through the probabilistic choice operators, we find that

$$(p \,{}_{.5}{+}\, q) \sqcap (p \,{}_{.5}{+}\, q) = p \,{}_{.25}{+}\, ((p \sqcap q) \,{}_{2/3}{+}\, q),$$

which means that the probability that the process acts like p is somewhere between .25 and .75, depending on how the choice $p \sqcap q$ is resolved. This unexpected behavior can be traced to the fact that $\sqcap$ distributed through ${}_{.5}{+}$ (and through ${}_\lambda{+}$ for all λ). One way to view this is that the resolution of the probabilistic choice in $p \,{}_{.5}{+}\, q$ is like an internal event, and using the CSP paradigm of *maximal progress* under which internal events are always on offer and happen as soon as possible, the probabilistic choice then is resolved at the same time as the *internal* nondeterministic one. From this viewpoint, the processes on either side of $\sqcap$ represent distinct instances of the same processes, but because they are

distinct, the probabilistic choice is resolved independently in each branch. In any case, this shows that the interplay of probabilistic choice and nondeterministic choice can lead to unexpected results which require careful, analysis. In [20], the term *duplication* is used for the phenomenon that this example illustrates.

We are unable to assign a precise probability to this process acting like p, since we have no way to assign a probability to how $\sqcap$ resolves its choices, precisely since it is *not* a probabilistic choice operator. Further work in [21] addresses the question of duplication arising where it is not desired. Two possible solutions are presented there. Our interest is in studying how to overcome duplication at the nondeterministic choice level.

Since it is the fact that $\sqcap$ distributes through $\mathrel{\not+}$ that causes $\sqcap$ not to be idempotent, one way to avoid this issue would be to craft a model which forces us to resolve $\sqcap$ first, *before* the probabilistic choices are resolved. This should remind the reader of bisimulation, where the question of when nondeterministic choices are resolved changes the meaning of the process, as the following example demonstrates:

$$a.(p+q) \not\sim (a.p) + (a.q),$$

(where $\sim$ denotes bisimulation).

3 Constructing New Models

In this section we show how, given an continuous cpo P, we can construct a domain Q which supports nondeterministic choice and probabilistic choice, so that the choice operator is idempotent. In fact, we can construct three such domains Q, each of which is an analog of one of the power domains. Moreover, if P is bounded complete, then in the first two cases, there is an e-p pair from P into Q. We start with an arbitrary coherent cpo P. We want to construct a coherent domains which contains a copy of P and that admits a projection onto P, and that simultaneously supports both a nondeterministic choice operation $+$ and probabilistic choice operations $\mathrel{\not+}$ satisfying the laws of a probabilistic algebra.

We begin our discussion by considering once again $\mathbb{FD}$, the failures-divergences model for CSP. As remarked earlier, this is a Scott domain – a bounded complete algebraic cpo. By forming $\mathcal{P}_{Pr}(\mathbb{FD})$, [20] construct a model for PCSP. Their method for defining interpretations of the operators from CSP on this model is simply to extend them to $\mathcal{P}_{Pr}(\mathbb{FD})$ in the "natural fashion". Actually, this is a categorical construction, which can be traced through the construction of $\mathcal{P}_{Pr}(\mathbb{FD}) \subseteq [\Sigma(\mathbb{FD}) \to [0,1]]$. It follows from the method of construction that the lifting of the operations from $\mathbb{FD}$ to this family all distribute through the probabilistic choice operators. This is why certain laws from CSP fail in the extension, such as the failure of the extension $\sqcap$ to PCSP to be idempotent.

But this still begs the question of whether the idempotence of nondeterministic choice can be retrieved. One approach might be to search for an alternative

method for extending the operations of CSP – in particular, of extending $\sqcap$ – to $\mathcal{P}_{Pr}(\mathbb{FD})$. The search is in vain if we also require that the extension be *affine* (ie, that it preserve affine combinations of processes such as $p \mathbin{{}_\lambda\!+} q$), since the categorical extension already satisfies this property, and there cannot be two such extensions (because the Splitting Lemma implies the image of $\mathbb{FD}$ generates $\mathcal{P}_{Pr}(\mathbb{FD})$). So, we must seek to extend the construction so as to accommodate another internal choice operator.

A somewhat more esoteric question revolves around the structure of the model $\mathcal{P}_{Pr}(\mathbb{FD})$. Indeed, all that one can confidently assert about the probabilistic power domain of a continuous domain is that it is again continuous, and that the probabilistic power domain of a coherent continuous domain is again coherent (cf. [13]). In particular, the probabilistic power domain is not bounded complete, and it remains an open question whether this operator leaves any cartesian closed category of continuous domains invariant.

In the case of the lower and upper power domains, our approach is to avoid this issue entirely by "dragging" $\mathcal{P}_{Pr}(\mathbb{FD})$ back into the category of bounded complete domains by applying another functor. This is possible because of the following result:

Theorem 1. *If P is a continuous domain, then $\mathcal{P}_L(D), \mathcal{P}_U(D) \in \mathsf{BCD}$, and if P is coherent, then so is $\mathcal{P}_C(P)$. In particular, for any continuous domain P, $\mathcal{P}_L(\mathcal{P}_{Pr}(P))$ and $\mathcal{P}_U(\mathcal{P}_{Pr}(P))$ are both bounded complete and continuous, and $\mathcal{P}_C(\mathcal{P}_{Pr}(P))$ is coherent.*

Proof. One can find a proof that $\mathcal{P}_L(P)$ and $\mathcal{P}_U(P)$ are both bounded complete and continuous if P is continuous, and that $\mathcal{P}_C(P)$ is coherent if P is in [2]. The last part then follows from [13]. □

Jones [11] showed that the probabilistic power domain functor is continuous, and it is well known that the power domain functors $\mathcal{P}_L$, $\mathcal{P}_U$ and $\mathcal{P}_C$ are continuous, we conclude that the compositions $\mathcal{P}_L \circ \mathcal{P}_{Pr}$, $\mathcal{P}_U \circ \mathcal{P}_{Pr}$ and $\mathcal{P}_C \circ \mathcal{P}_{Pr}$ are all continuous. Moreover, the theorem above yields:

Corollary 1. *The compositions $\mathcal{P}_L \circ \mathcal{P}_{Pr}$ and $\mathcal{P}_U \circ \mathcal{P}_{Pr}$ are continuous endofunctors of BCD, and $\mathcal{P}_C \circ \mathcal{P}_{Pr}$ is a continuous endofunctor of COH.* □

However, this is not exactly what we want. The reason is that, if we use the standard approach to extending the operations from P to $\mathcal{P}_L(P)$, $\mathcal{P}_U(P)$ or $\mathcal{P}_C(P)$ in the case P is a probabilistic algebra, we find that the laws we want no longer are valid. For example, for $X, Y \in \mathcal{P}_U(P)$

$$X \mathbin{{}_\lambda\!+} Y = \{x \mathbin{{}_\lambda\!+} y \mid x \in X, y \in Y\}, \text{ so } X \mathbin{{}_\lambda\!+} X = \{x \mathbin{{}_\lambda\!+} y \mid x, y \in X\},$$

and this is not equal to X. In general, $X \mathbin{{}_\lambda\!+} X$ will be larger than X. To remedy this, we proceed as follows.

Definition 3. *Let P be a probabilistic algebra, and let $X \subseteq P$. We define*

$$\langle X \rangle = \{x \mathbin{{}_\lambda\!+} y \mid x, y \in X \ \wedge \ 0 \leq \lambda \leq 1\}.$$

We say that X is affine closed *if $X = \langle X \rangle$. We let*

- $\mathcal{P}_{LA}(P) = \{X \in \mathcal{P}_L(P) \mid X = \langle X \rangle\}$.
- $\mathcal{P}_{UA}(P) = \{X \in \mathcal{P}_U(P) \mid X = \langle X \rangle\}$.
- $\mathcal{P}_{CA}(P) = \{X \in \mathcal{P}_C(P) \mid X = \langle X \rangle\}$.

We call these nondeterministic probability domains.

Theorem 2. *Let P be a probabilistic algebra which is also a coherent domain. Then there are continuous kernel operators*

$$\kappa_L \colon (\mathcal{P}_L(P), \subseteq) \to (\mathcal{P}_{LA}(P), \subseteq) \text{ given by } \kappa_L(X) = \bigcap \{Y \in P_L(P) \mid X \subseteq Y\}.$$

$$\kappa_U \colon (\mathcal{P}_U(P), \supseteq) \to (\mathcal{P}_{UA}(P), \supseteq) \text{ given by } \kappa_U(X) = \bigcap \{Y \in P_U(P) \mid X \subseteq Y\}.$$

$$\kappa_C \colon (\mathcal{P}_C(P), \sqsubseteq) \to (\mathcal{P}_{CA}(P), \sqsubseteq) \text{ given by } \kappa_C(X) = \bigcap \{Y \in P_C(P) \mid X \subseteq Y\}.$$

Furthermore, $\mathcal{P}_{UL}(P)$ and $\mathcal{P}_{UA}(P)$ are bounded complete domains which also are probabilistic algebras, and $\mathcal{P}_{CA}(P)$ is a coherent domain. Finally, each of the first two extend to a continuous functor $\mathcal{P}_{UA} \colon \mathsf{COH} \to \mathsf{BDC}$, and $\mathcal{P}_{CA}$ extends to a continuous functor $\mathcal{P}_{CA} \colon \mathsf{COH} \to \mathsf{COH}$.

Proof. We confine our argument to the case of $\mathcal{P}_{UA}$. If $X \in \mathcal{P}_U(P)$, then the family $A(X) = \{Y \in \mathcal{P}_U(P) \mid X \subseteq Y = \langle Y \rangle\}$ is non-empty (since P is in the family), and it is closed under all intersections (that the intersection of compact sets is again compact follows from the coherence of P). It follows that $\kappa_U(X) = \bigcap A(X)$ is well-defined, and it is routine to argue that κ_U is continuous and idempotent, from which it follows that $(\mathcal{P}_{UA}(P), \supseteq)$ is a continuous coherent domain.

The probabilistic choice operators can be defined on $\mathcal{P}_{UA}(P)$ by

$$X \,{}_\lambda\!+ Y = \{x \,{}_\lambda\!+ y \mid x \in X, y \in Y\},$$

and it follows from the rectangle law (cf. [9]) for P that $X \,{}_\lambda\!+ Y \in \mathcal{P}_{UA}(P)$ for $X, Y \in \mathcal{P}_{UA}(P)$. The continuity of these operations also is easily seen. One can argue that $\mathcal{P}_{UA}(P)$ with these operations satisfies the laws of Mean Values (cf. [9]), which are equivalent to the probabilistic algebra laws of [11]. Since the operations are easily seen to be continuous, it follows that $\mathcal{P}_{UA}(P)$ is a probabilistic algebra.

We note that $(\mathcal{P}_{UA}(P), \supseteq)$ also is an inf-semilattice, being the image of one under a kernel operator. If $f \colon P \to Q$ is a continuous morphism of probabilistic domains (ie, if P and Q are domains with continuous interpretations of the operators ${}_\lambda\!+, \lambda \in [0,1]$ which also are probabilistic algebras), then we can define $\mathcal{P}_{UA}(f) \colon \mathcal{P}_{UA}(P) \to \mathcal{P}_{UA}(Q)$ by $\mathcal{P}_{UA}(f) = (\kappa_U \circ \mathcal{P}_U)(f)$. It is routine to show that $\mathcal{P}_{UA}(f)$ is again a morphism of probabilistic algebras, and that the functor $\mathcal{P}_{UA}$ is locally continuous. It follows that $\mathcal{P}_{UA}$ is a continuous functor. □

In the case of CSP, we consider the domain $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$: Because the upper power domain is the power domain of demonic choice, we have chosen to focus on the the nondeterministic probability domain analogous to the upper

power domain, since this underlies (internal) nondeterministic choice in CSP. We begin with $\mathbb{FD}$ to build our model. The following shows the properties of the associated model.

Theorem 3.

1. *If P is any bounded complete, continuous domain, then there is an e-p pair from P to $\mathcal{P}_{Pr}(P)$.*
2. *If P is a coherent domain that also is a probabilistic algebra, then the there is an injection of P into $\mathcal{P}_{UA}(P)$ that is a morphism of probabilistic algebras.*
3. *If P is a bounded complete continuous domain, then there is an e-p pair from $\mathcal{P}_{Pr}(P)$ to $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(P))$. Moreover, the embedding $e\colon \mathcal{P}_{Pr}(P) \to \mathcal{P}_{UA}(P)$ is a morphism of probabilistic algebras.*

Proof. Since $\mathcal{P}_{Pr}$ is a left adjoint, we can use the unit of the adjunction for the embedding. This is simply the mapping $x \mapsto \delta_x$, which assigns the point mass at x to each point $x \in P$. For the projection mapping, we use the support function: $\mu \mapsto \operatorname{supp}\mu$. For simple measures $\Sigma_{x\in F} r_x \delta_x$, this is simply F. Since each measure is the directed supremum of simple measures, for general μ we can form the "limit" of the family F_i, where $\mu = \sqcup_i \Sigma_{x\in F_i} r_x \delta_x$. (This limit can be thought of as being taken in the convex power domain of P – cf. [19].) The projection mapping then send μ to $\wedge \operatorname{supp}\mu$, for which it is routine to verify the required equations for an e-p pair.

For the second claim, we note that $x \mapsto \uparrow x\colon P \to \mathcal{P}_{UA}(P)$ is a morphism of probabilistic algebras by the definition of the operations on $\mathcal{P}_{UA}(P)$.

Finally, if P is bounded complete, we can derive an e-p pair from $\mathcal{P}_{Pr}(P)$ to $\mathcal{P}_{UA} \circ \mathcal{P}_{Pr}(P)$, whose embedding is the composition of the units: $x \mapsto \uparrow\delta_x$, and whose projection is $X \mapsto \wedge\{\operatorname{supp}\mu \mid \mu \in X\}$. It is once again routine to validate the required equations for an e-p pair. The embedding from $\mathcal{P}_{Pr}(P)$ is just the mapping $x \mapsto \uparrow x$; the projection is gotten via the previous result. Namely, $X \mapsto \delta_{\wedge\{\operatorname{supp}\mu \mid \mu\in X\}}$. Again, the validation of the required equations is routine. □

Thus, we can begin with $\mathbb{FD}$ and generate a bounded complete, continuous domain $\mathcal{P}_{UA}(\mathcal{P}_{Pr}\mathbb{FD})$ that also is a probabilistic algebra.

Example 2. We show that the domain $\mathcal{P}_{UA}(\mathcal{P}_{Pr}\mathbb{FD})$ is a model for PCSP in which internal choice does not distribute over probabilistic choice. First, using the standard categorical approach, we can extend the interpretation of each CSP operator on $\mathcal{P}_{Pr}(\mathbb{FD})$ to $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$, and these extensions all are continuous. Noting that $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ also has an internally defined inf-operation – $(X, Y) \mapsto \kappa(\langle X \cup Y\rangle)$, we then can conclude $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ is a continuous algebra of the same signature as defines the syntax of CSP. Since we can regard CSP as the initial algebra with this signature, it follows that there is a (unique!) algebra homomorphism $[\![\ ]\!]\colon \text{CSP} \to \mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$, and we take this as our semantic map. Actually, this extends to a semantic mapping from PCSP to $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ since the latter is a probabilistic algebra.

To show that internal choice does not distribute over the probabilistic choices $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ we simply note that we have chosen the internally defined inf-operation on $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ as our interpretation of $\sqcap$, and since this operator is idempotent on all of $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$, we conclude that

$$(p \mathrel{{}_{.5}\!+} q) \sqcap (p \mathrel{{}_{.5}\!+} q) = p \mathrel{{}_{.5}\!+} q$$

for any elements of $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$ – in particular, this holds for p and q the denotations of processes from PCSP. But then $\sqcap$ cannot distribute through $\mathrel{{}_{.5}\!+}$, because we would then have the equality

$$p \mathrel{{}_{.5}\!+} q = (p \mathrel{{}_{.5}\!+} q) \sqcap (p \mathrel{{}_{.5}\!+} q) = p \mathrel{{}_{.25}\!+} ((p \sqcap q) \mathrel{{}_{2/3}\!+} q),$$

which would imply that $p \sqcap q = p \mathrel{{}_{.5}\!+} q$, which certainly does not hold, as easy examples show. □

4 Summary and further applications

We have investigated the possibility of building semantic models which support nondeterministic choice and probabilistic choice operators, and in which all the laws of nondeterministic choice and of probabilistic algebras hold. The models we constructed are obtained by following the probabilistic power domain of Jones by modifications of the traditional power domains. We have focused in our examples on CSP, and shown how this approach produces such a model for untimed CSP with probabilistic choice operators added. Moreover, the failures-divergences model, on which our model is built, is a retract of our model. This shows that the model for probabilistic CSP devised in [20] can be improved so that the expected laws hold. Our new domains support both nondeterminism and probabilistic choice; they are the families of non-empty, affine, Scott closed lower sets (affine, compact upper subsets, or affine, Lawson compact convex subsets, respectively) of a coherent, continuous domain, show each of these families also is a probabilistic algebra. These are the only models of this type we know of. In particular, the models defined in several of the papers listed in the references (except, of course, that of [11, 12]) seem not to address this issue.

A question we have left unaddressed is what other laws our new model satisfies. For example, we have not considered the "usual" laws of CSP for the case of $\mathcal{P}_{UA}(\mathcal{P}_{Pr}(\mathbb{FD}))$. This is a very important issue, especially given the tradition of algebraic semantics for CSP and its related languages. And certainly the deterministic choice operator $\Box$ of CSP has been altered in our model, since it inherently depends on $\sqcap$ – for example $(a \to p) \Box (a \to q) = (a \to p) \sqcap (a \to q)$ holds in CSP, but it is unclear whether it holds in our model.

There is another area that our model also should be of interest. In recent work, Roscoe [22] has shown that the security of a multilevel system can be analyzed using CSP. In particular, he shows that such a system (by which we mean a process representing the functioning of the system that users of differing levels of security clearance are using) is secure if the low level user's view of the

system is deterministic, once the high level user's actions have been abstracted away. This approach has the added advantage that secure systems cannot be refined[2] by insecure ones, since deterministic processes are maximal in the models of untimed CSP. The problem with this approach is that it is too restrictive. There are processes representing system behavior that are accepted as being secure, but which nonetheless fall outside this definition, precisely because low's view is nondeterministic.

The reason that nondeterministic processes are viewed as insecure is that each process in models of CSP is the nondeterministic choice of its deterministic refinements, and allowing low to have a nondeterministic view of the system – even with high's actions abstracted away – allows for the possibility that low could reliably refine what is seen to a less deterministic process that would support a covert channel from high to low. For example, if low sees actions that he can reason are one of two types – sends or receives, for example – he can then draw conclusions about high level activity on the system.

The potential application of the work described here would be to implement the system's choice using probabilistic choice. Then it would be impossible for low to reliably refine his seemingly nondeterministic view. But, if high could predict the way in which the system were going to resolve its choices – for example, if those choices could be viewed as having been resolved before high makes his choices about which events to participate in, then a covert channel could be set up between high and low. This is possible in a system where the system's choice distribute through those of high, and that is why the model of [20] is viewed as unsatisfactory for this application. Since our model implements nondeterministic (ie, high's) choices, and probabilistic (ie, the system's) choices, and since the nondeterministic choices do not distribute through the probabilistic choices, our model has the possibility of providing a setting in which the security results of Roscoe could be extended to more general settings.

5 Acknowledgement

The author wishes to thank JOËL OUAKNINE and STEVEN SHALIT for providing stimulating conversations about this work.

References

1. S. Abramsky, *A domain equation for bisimulation, Information and Computation* **92** (1991), pp. 161–218.
2. S. Abramsky and A. Jung, *Domain Theory*, In: S. Abramsky, D. M. Gabbay and T. S. E. Maibaum, editors, *Handbook of Logic and Computer Science,* **3**, Clarendon Press (1994), pp. 1–168.

[2] In CSP models, a process p *refines* a process q if every behavior of p also is a behavior of q. That is, q is more nondeterministic than p. This notion is the basis of for reasoning about specification in CSP.

3. P. America and J. J. R. R. Rutten, *Solving reflexive domains equations in a category of complete metric spaces, Journal of Compuer Systems and Sciences* **39** (1989), pp. 343–375.
4. C. Baier and M. Kwiatkowska, *Domain equations for probabilistic processes, Electronic Notes in Theoretical Computer Science* **7** (1997), URL: `http://www.elsevier.nl/locate/entcs/volume7`
5. S. D. Brookes and A. W. Roscoe, *An improved failures model for communicating processes*, *Lecture Notes in Computer Science* **197** (1985), pp. 281 - 305.
6. E. P. de Vink and J. J. M. M. Rutten, *Bisimulation for probabilistic transition systems: a coalgebraic approach,* CWI preprint, October, 1998.
7. H. Hansson and B. Jonsson, *A calculus for communicating systems with time and probability, Proceedings* of the 11th Symposium on Real Time Systems, 1990.
8. J. I. den Hartog and E. P. de Vink, *Mixing up nondeterminism and probability: A preliminary report*, *Electronic Notes in Theoretical Computer Science* **22** (1997), URL: `http://www.elsevier.nl/locate/entcs/volume22.html`.
9. R. Heckmann, *Probabilistic domains, Proceedings* of CAAP '94, *Lecture Notes in Computer Science* **787** (1994), pp. 142–156.
10. M. Hennessy and G. Plotkin, *Full abstraction for a simple parallel programming language,* Lecture Notes in Computer Science **74** (1979), Springer-Verlag.
11. C. Jones, "Probabilistic Non-determinism," PhD Thesis, University of Edinburgh, 1990. Also published as Technical Report No. CST-63-90.
12. C. Jones and G. Plotkin, *A probabilistic powerdomain of evaluations, Proceedings* of 1989 Symposium on Logic in Computer Science, IEEE Computer Society Press, 1989, pp. 186–195.
13. A. Jung, *Lawson-compactness for the probabilistic powerdomain,* Preprint, 1997.
14. A. Jung and R. Tix, *The troublesome probabilistic powerdomain, Electronic Notes in Theoretical Computer Science* **7** (1998), URL: `http://www.elsevier.nl/locate/entcs/volume7.html`
15. J. D. Lawson, *Valuations on continuous lattices,* In: Rudolf-Eberhard Hoffmann, editor, *Continuous Lattices and Related Topics, Mathematik Arbeitspapiere* **27** (1982), Universität Bremen, pp. 204–225.
16. K. Larsen and A. Skou, *Bisimulation through probabilistic testing, Information and Computation* **94** (1991), pp. 456–471.
17. G. Lowe, "Probabilities and Priorities in Timed CSP," DPhil Thesis, University of Oxford, 1991.
18. N. Lynch and R. Segala, *Probabilistic simulations for probabilistic processes,Proceedings* of CONCUR'94, *Lecture Notes in Computer Science* **836** (1994), pp. 481–496.
19. M. Mislove, *Topology, domain theory and theoretical computer science, Topology and Its Applications* (1999), pp.
20. C. Morgan, A. McIver, K. Seidel and J. Sanders, *Refinement-oriented probability for CSP,* University of Oxford Technical Report, 1994.
21. C. Morgan, A. McIver, K. Seidel and J. Sanders, *Argument duplication in probabilistic CSP,* University of Oxford Technical Report, 1995.
22. A. W. Roscoe. CSP and determinism in security modeling. In *IEEE Symposium on Security and Privacy.* IEEE Computer Society Press, 1995.
23. J. J. M. M. Rutten and D. Turi, *On the foundations of final semantics: Non-standard sets, metric spaces and partial orders, Proceedings* of the REX'92 Workshop, *Lecture Notes in Computer Science* **666** (1993), pp. 477–530.
24. N. Saheb-Djahromi, *CPOs of measures for nondeterminism, Theoretical Computer Science* **12** (1980), pp. 19–37.