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 a potential application 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. [8]), and the metric space approach (cf. [2]). 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 [8] 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 domain theory to the work of Saheb-Dharjomi [21]. While this was the first to consider modeling probabilistic choice using a domain, the most influential work along this line is without question the PhD thesis of Jones [9], 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 a continuous

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

C. Palamidessi (Ed.): CONCUR 2000, LNCS 1877, pp. 350–365, 2000.

domain is again continuous. 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 initial.

One issue that causes problems is that the difference between nondeterministic choice and probabilistic choice is not clearly understood. Indeed, the title of [9] reveals an identification of probabilistic choice as a form of nondeterminism. Yet probabilistic choice operators are not associative. For example,[1]

$$(p \,{}_{.5}\!+ q) \,{}_{.5}\!+ r = p \,{}_{.25}\!+ (q \,{}_{1/3}\!+ r).$$

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 [17] 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 [18] 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 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., [20] for an introduction).

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

- approaches such as [14,16] 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.
- approaches such as [5] and [15] 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.

[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 [17,6] 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.

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 [21] 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 [9,10] 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 [17] 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 *convex* 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 [17] is one such, and the *Splitting Lemma* (cf. [9] or Lemma 1) implies there is only one such. There is no obvious candidate for a nondeterministic choice operator on this model, even if one drops the convexity 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 possible power domains to apply - 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 lifted to any of these power domains do not satisfy the expected laws. However, we are not far from our desired model. We simply consider the family of *(probability) convex* 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. (This is an idea suggested in [17], but considered there only in the case of the upper power domain, and for which no details are presented.) What is more, in the case of the lower or upper power domains, the models we construct yield a bounded complete domain,[2] when applied to a Scott domain. In addition, the compositions $\mathcal{P}_{PL} \circ \mathcal{P}_{Pr}$ and $\mathcal{P}_{PU} \circ \mathcal{P}_{Pr}$ are

[2] A domain is *bounded complete* if each non-empty subset has a greatest lower bound. Equivalently, each subset with an upper bound has a least upper bound. These objects, when it also is assumed that the domain is ω-algebraic, form what are called *Scott domains*.

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 an important implication for the application of these models 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 [17]. This serves to present a motivating example for our work; it 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 [17] because of the way in which the CSP operators are defined on their model. The next section gives our construction, showing how to build a model supporting both nondeterministic choice and probabilistic choice over any bounded complete domain. We next describe some potential applications of our models, and some of the problems that still need to be resolved to provide meaningful answers to these questions.

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 [1]. 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, denoted $\sqcup D$, 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 (cf. [1]).

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 [1].

Coherent domains: Of particular interest to us is the category COH of *coherent domains* and Scott continuous maps (cf. [1]). These domains are most easily described in topological terms. The Scott topology on a domain P satisfies only weak separation conditions: it is *sober* (which for continuous domains can be seen as a topological statement that P is directed complete), and all open sets are upper sets. In order to refine the topology to obtain a Hausdorff topology, one has only to add certain open lower sets. These are the family $\{P \setminus \uparrow F \mid F \subseteq P \text{ finite}\}$. The common refinement of this topology and the Scott topology is called the *Lawson topology.*

Definition 1. *A domain P is* coherent *if its Lawson topology is compact. Equivalently, the intersection of Scott compact upper sets is again Scott compact.*

Power domains: 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 $\mathcal{P}_L(P) = \{X \subseteq D \mid \emptyset \neq X = \downarrow X \text{ is Scott closed}\}$, ordered by inclusion.

The Upper Power Domain is defined as $\mathcal{P}_U(D) = \{X \subseteq P \mid \emptyset \neq X = \uparrow X \text{ is Scott compact}\}$ 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 a *continuous semilattice:* 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 *(order) 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 (cf. [8]).

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 [21], who showed that the family he defined yields a cpo. The construction later was refined by Jones [9,10] 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 2. *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 [13] who first showed the connection between continuous valuations and measures on the cpo P: 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 [12]. 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. 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 known 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 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 [9] is a fundamental result about the order on simple measures:

Lemma 1 (Splitting Lemma [9]). *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 [9] 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 a continuous endofunctor on CON. That is, each continuous map $f\colon P \to Q$ between (continuous) domains can be lifted to a continuous map $\mathcal{P}_{Pr}(f)\colon \mathcal{P}_{Pr}(P) \to \mathcal{P}_{Pr}(Q)$ by $\mathcal{P}_{Pr}(f)(\mu)(U) = \mu(f^{-1}(U))$. In fact, [9] 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 the following laws (cf. [9]):

Definition 3. *A* probabilistic algebra *is a dcpo A endowed with a continuous mapping $(\lambda, a, b) \mapsto a\ {}_\lambda{+}\ b\colon [0,1] \times A \times A \to A$ so that the following laws hold for all $a, b, c \in A$, $\lambda \in [0,1]$:*

- $a\ {}_\lambda{+}\ b = b\ {}_{1-\lambda}{+}\ a$,
- $(a\ {}_\lambda{+}\ b)\ {}_\rho{+}\ c = a\ {}_{\lambda\rho}{+}\ (b\ {}_{\frac{\rho(1-\lambda)}{1-\lambda\rho}}{+}\ c)$ (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. Moreover, Jones [9] shows that the probabilistic power domain forms the object level of a left adjoint to the category PROB of continuous probabilistic algebra domains and continuous mappings which also preserve the probabilistic choice operators.

2.1 Probabilistic CSP

The model for probabilistic CSP – PCSP as it is denoted – that was devised in [17] 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 [17] 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 [17] 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 of processes in $\mathbb{FD}$ is another such, which combined with the result just cited shows that $\mathbb{FD}$ is a Scott domain. Applying the probabilistic power domain operator to $\mathbb{FD}$ then results in a continuous probabilistic algebra, and this is the model for probabilistic CSP used in [17].

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 $(a \rightarrow STOP)\,{}_\lambda{+}\,(b \rightarrow STOP \;\Box\; c \rightarrow STOP)$, which will act like $a \rightarrow STOP$ with probability λ, and offer the external choice of doing a b or a c with probability $1 - \lambda$. The approach provided in [17] to reasoning about such processes is via weakest precondition semantics, where weakest preconditions for probabilistic processes are represented as random variables.

The extension of the operators of CSP to $\mathcal{P}_{Pr}(\mathbb{FD})$ can be understood in terms of the construction. 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, a unary operator $f\colon \mathbb{FD} \rightarrow \mathbb{FD}$ can be extended to $\mathcal{P}_{Pr}(f)\colon \mathcal{P}_{Pr}(\mathbb{FD}) \rightarrow \mathcal{P}_{Pr}(\mathbb{FD})$ 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

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

  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* $\mathcal{P}_{Pr}(\mathbb{FD})$ *as a whole.*

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

$$(p \,{}_{.5}{+}\, q) \sqcap (p \,{}_{.5}{+}\, q) = p \,{}_{.25}{+}\, ((p \sqcap q) \,{}_{1/3}{+}\, q),$$

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 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. Then 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 [17], the term *duplication* is used for this phenomenon. 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 [18] addresses the question of duplication arising where it is not desired, and 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 ${}_{\lambda}{+}$ 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.

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, so is the associated Q, and in each case, Q is the image of either a closure operator or a kernel operator.

We start with an arbitrary coherent cpo P. We want to construct a coherent domain which contains a copy of P, that admits a projection onto P, and that simultaneously supports both an idempotent nondeterministic choice operation $+$ and probabilistic choice operations ${}_{\lambda}{+}$ satisfying the laws of a probabilistic algebra.

The failures-divergences model $\mathbb{FD}$ is a Scott domain, and the operators from CSP are extended to the model $\mathcal{P}_{Pr}(\mathbb{FD})$ for PCSP constructed in [17] using the categorical results, which can be traced through the construction of $\mathcal{P}_{Pr}(\mathbb{FD}) \subseteq [\Sigma(\mathbb{FD}) \to [0,1]]$. This method of construction forces the lifting of the operations from $\mathbb{FD}$ to this family all to distribute through the probabilistic choice operators. And, since the simple measures are Scott dense in $\mathcal{P}_{Pr}(\mathbb{FD})$ (a result of the

Splitting Lemma 1), it follows that there is no extension of $\sqcap$ to $\mathcal{P}_{Pr}(\mathbb{FD})$ if we require the extension to preserve convex combinations of processes such as $p \,{}_\lambda\!+ q$.

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. [11]). In particular, it remains an open question whether this functor 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:

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 a proof that $\mathcal{P}_C(P)$ is coherent if P can be found in [1]. The last part then follows from [11]. □

Jones [9] 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, so 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 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 $X, Y \in \mathcal{P}_U(P)$

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

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

Definition 4. *Let P be a probabilistic algebra, and let $X \subseteq P$. We define*

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

We say that X is pconvex *if $X = \langle X \rangle$, and we let $\mathcal{P}_{LP}(P) = \{X \in \mathcal{P}_L(P) \mid X = \langle X \rangle\}$, $\mathcal{P}_{UP}(P) = \{X \in \mathcal{P}_U(P) \mid X = \langle X \rangle\}$, and $\mathcal{P}_{CP}(P) = \{X \in \mathcal{P}_C(P) \mid X = \langle X \rangle\}$. We call these* nondeterministic probability domains*, and we denote by PCOH the category of coherent probabilistic algebras and continuous maps preserving probabilistic choice.*

Theorem 2. *Let P be a probabilistic algebra which is also a coherent domain. Then*

1. $\kappa_L : (\mathcal{P}_L(P), \subseteq) \to (\mathcal{P}_{LP}(P), \subseteq)$ *given by* $\kappa_L(X) = \downarrow\langle X\rangle$ *is a (continuous) closure operator.*
2. $\kappa_U : (\mathcal{P}_U(P), \supseteq) \to (\mathcal{P}_{UP}(P), \supseteq)$ *given by* $\kappa_U(X) = \uparrow\langle X\rangle$ *is a continuous kernel operator.*
3. $\kappa_C : (\mathcal{P}_C(P), \sqsubseteq) \to (\mathcal{P}_{CP}(P), \sqsubseteq)$ *given by* $\kappa_C(X) = \kappa_L(X) \cap \kappa_U(X)$ *is a continuous idempotent operator.*

Furthermore, $\mathcal{P}_{LP}(P)$ and $\mathcal{P}_{UP}(P)$ are bounded complete domains, and $\mathcal{P}_{CP}(P)$ is a coherent domain, and all three are probabilistic algebras. Finally, the first two extend to continuous functors $\mathcal{P}_{LP}, \mathcal{P}_{UP} : \mathsf{PCOH} \to \mathsf{BDC}$, and $\mathcal{P}_{CP}$ extends to a continuous functor $\mathcal{P}_{CP} : \mathsf{PCOH} \to \mathsf{PCOH}$.

Proof. Because P is coherent and the mapping $(\lambda, x, y) \mapsto x \mathbin{_\lambda\!+\!} y : [0,1] \times P \times P \to P$ is continuous, it follows routinely that $\downarrow\langle X\rangle$ is Scott closed if X is, and that $\uparrow\langle X\rangle$ is Scott compact if X is. This implies that

- $\downarrow\langle X\rangle = \bigcap\{Y \in \mathcal{P}_L(P) \mid X \subseteq Y\}$ for all $X \in \mathcal{P}_L(P)$,
- $\uparrow\langle X\rangle = \bigcap\{Y \in \mathcal{P}_U(P) \mid X \subseteq Y\}$ for all $X \in \mathcal{P}_U(P)$, and
- $\downarrow\langle X\rangle \cap \uparrow\langle X\rangle = \bigcap\{Y \in \mathcal{P}_C(P) \mid X \subseteq Y\}$ for all $X \in \mathcal{P}_C(P)$.

The first result just listed implies that $\downarrow X$ is pconvex if X is, and so $\downarrow\langle X\rangle$ is both Scott closed and pconvex. Moreover, it is clear that $X \subseteq \kappa_L(X) = \kappa_L(X)^2$, so that $\kappa_L : \mathcal{P}_L(P) \to \mathcal{P}_L(P)$ is a closure operator. It is routine to show that $\mathcal{P}_{LP}(P)$ is closed in $\mathcal{P}_L(P)$ under directed suprema, so that κ_L is continuous, from which it follows that $\mathcal{P}_{LP}(P)$ is a continuous domain.

Similarly, $\kappa_U(X) = \kappa_U(X)^2$ is the smallest Scott compact upper set containing X, for each $X \in \mathcal{P}_U(P)$. Since $X \subseteq \kappa_U(X)$, we conclude that κ_U is a kernel operator. It is easy to show that $\mathcal{P}_{UP}(P)$ is closed in $\mathcal{P}_U(P)$ under all filtered intersections, and that κ_U is continuous with respect to $\supseteq$. It follows that $\kappa_U : \mathcal{P}_U(P) \to \mathcal{P}_{UP}(P)$ is a continuous kernel operator and then that $\mathcal{P}_{UP}(P)$ is continuous as well.

Finally, using the coherence of P, it is straightforward to show that $\{X \in \mathcal{P}_C(P) \mid X = \langle X\rangle\}$ is closed under directed sups in the Egli-Milner order. In fact, the coherence of P implies that the mapping

$$X \mapsto (\downarrow X, \uparrow X) : \mathcal{P}_{CP}(P) \to \{(X, Y) \in \mathcal{P}_{LP}(P) \times \mathcal{P}_{UP}(P) \mid X \cap Y \neq \emptyset\}$$

is an order isomorphism, whose inverse is $(X, Y) \mapsto X \cap Y$. This implies that $\kappa_C(X) = \kappa_L(\downarrow X) \cap \kappa_U(\uparrow X)$ is continuous, since it is the composition of continuous mappings. This shows $\mathcal{P}_{CP}(P)$ is the image of a continuous selection-retraction pair (cf. [1]), and so $\mathcal{P}_{CP}(P)$ is continuous.

The probabilistic choice operators on each of these domains can be defined by $X \mathbin{_\lambda\!+\!} Y = \{x \mathbin{_\lambda\!+\!} y \mid x \in X, y \in Y\}$, and it follows from the rectangle law (cf. [7]) and the coherence of P that $X \mathbin{_\lambda\!+\!} Y$ is again in the appropriate nondeterministic probabilistic domain. One can argue that each such domain with these operations

satisfies the laws of Mean Values (cf. [7]), which are equivalent to the probabilistic algebra laws of [9]. Since the operations are easily seen to be continuous, it follows that each domain is a probabilistic algebra.

Finally, to show that each of these constructs leads to a continuous functor, it is sufficient to show that each is locally continuous (cf. [1]). For example, in the case of $\mathcal{P}_{LP}$, we need to show that, for P, Q coherent domains which are probabilistic algebras, the mapping $f \mapsto \mathcal{P}_{LP}(f) : \mathcal{P}_{LP}(P) \to \mathcal{P}_{LP}(Q)$ is continuous. If we restrict attention to PCOH, then this is just the restriction of the mapping $\widehat{f} : \Gamma(P) \to \Gamma(Q)$ by $\widehat{f}(X) = \downarrow f(X)$. □

We might use the domain $\mathcal{P}_{UP}(\mathcal{P}_{Pr}(\mathbb{FD}))$ to provide a model for probabilistic CSP, because the upper power domain is the power domain of demonic choice, which reflects how internal nondeterminism is modeled in CSP. The following reveals some of the structure of this object.

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 $\mathcal{P}_{UP}(P)$ 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 $\mathcal{P}_{UP}(\mathcal{P}_{Pr}(P))$.*

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 $\mu = \sqcup_i \Sigma_{x \in F_i} r_x \delta_x$. 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 $x \mapsto \uparrow x : P \to \mathcal{P}_{UP}(P)$ is a morphism of probabilistic algebras by the definition of the operations on $\mathcal{P}_{UP}(P)$.

Finally, if P is bounded complete, we can derive an e-p pair from $\mathcal{P}_{Pr}(P)$ to $\mathcal{P}_{UP} \circ \mathcal{P}_{Pr}(P)$, 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. □

4 Two Potential Applications:

Probabilistic CSP: We have motivated our work by considering probabilistic CSP and the fact that internal nondeterminism is not idempotent on PCSP. In fact, Morgan, et al outline the approach we have taken in [17], where they call the nondeterministic operation *indifferent nondeterminism*, because it is indifferent to how probabilistic choices are resolved. It would now be natural to develop a

model for CSP that uses this construction, and that also includes the other main operators for CSP in a way that the usual laws of CSP are satisfied. However, this is not such a simple task. For example, the external choice operator $\Box$ is idempotent in CSP, but one can argue that it should *not* be idempotent in a model also supporting probabilistic choice.

Indeed, consider the process $(p \,{}_{.5}\!+\! q)\Box(p' \,{}_{1/3}\!+\! q')$. In order for $\Box$ to be external nondeterminism, the environment should be able to select from the available actions. But this cannot be determined until the probabilistic choices are resolved – ie, ${}_{.5}\!+$ and ${}_{1/3}\!+$ must be resolved *before* $\Box$ for this to make computational sense. It is not hard to show that this implies that $\Box$ cannot be idempotent in the model, which means it must satisfy some other laws. Most appealing is that $\Box$ distribute through the probabilistic choice operators, as in PCSP, since, as we have seen, this implies $\Box$ is not idempotent.

Going beyond this discussion, one can also ask what other laws should hold in a model for CSP that also supports probabilistic choice operators. One law we believe should hold is the familiar law that $\Box$ reverts to $\sqcap$ if both branches begin with the same action: $(a \to p)\Box(a \to q) = a \to (p \sqcap q)$. Unfortunately, it is not clear how to build a model for CSP in which this law holds, in which $\Box$ distributes through the probabilistic operators, and in which $\sqcap$ is idempotent. This is the focus of ongoing, collaborative research with Gavin Lowe.

Security and information flow: The area which motivated the work reported in this paper has to do with security and information flow. Imagine a system in which there are users of varying security levels, and in which it is required that information about what the High level users are doing is not supposed to flow to the Low level users in the system. A particular concern in this setting is the potential for a covert channel by which information could pass from High to Low. An approach to modeling this situation generally assumes that all participants – both High level users and Low level users, know the process that represents what the system S may do, and it is also assumed that the system can be modeled as $P = H_{High} \|_{High \cup Low} S_{High \cup Low} \|_{Low} L$, where H represents High and L represents Low. The intention is that H interacts using High's alphabet of actions, and L interacts using Low's alphabet of actions, and the system S is required to interact on both alphabets.

Results in this area have been developed by Roscoe and his colleagues [19], and a brief summary of the results can be stated as follows. One way to ensure that no information flows from High to Low is to be sure that the system always looks deterministic to Low, no matter what High does. One way to express this is that, after two traces t and t' which have the property that $t|_{Low} = t'|_{Low}$, then $(P/t) \setminus H = (P/t') \setminus H$. That is, what Low sees (H's actions are hidden from view) is the same after two traces which have the same Low events in them. Unfortunately, this is not quite right, since hiding H's actions allows H to block actions, thus passing information to Low. So Roscoe generalizes this by obfuscating High's actions appropriately. And, the result he obtains is that, if such a system looks deterministic to Low, then it is secure.

This approach has some shortcomings. Here are some examples:

1. Consider $S = (h_1 \to l_1 \to S)\Box(h_2 \to l_2 \to S)$. This is obviously insecure, since L will know which action H has done according to which he can do.
2. On the other hand, $S = (h_1 \to (l_1 \sqcap l_2) \to S)\Box(h_2 \to (l_1 \sqcap l_2) \to S)$ avoids the problem in the first example, but it is still insecure, since L can deduce that H has executed some action if he can do an action.
3. Finally, the process $S = ((h_1 \to (l_1 \sqcap l_2) \to S)\Box(h_2 \to (l_1 \sqcap l_2) \to S)) \sqcap ((l_1 \sqcap l_2) \to S)$ avoids the problems of both examples. While this process should be considered secure, it falls outside the scope of Roscoe's analysis because L's view is $l_1 \sqcap l_2$, which is nondeterministic.

From these examples it should be clear that there is considerable latitude for secure processes S for which Low's view is nondeterministic. But the *refinement paradox*, under which a process that is secure can have a more deterministic refinement which is insecure means that security can be quite difficult to reason about in the presence of nondeterminism.

One motivation for the present work is to devise a model for CSP which also supports probabilistic choice operators. Such a model could then be a setting to test processes such as S above to reveal insecure behavior. The idea would be to replace the nondeterminism in S with probabilistic choice, and to see if the resulting system passed the test for secure behavior. For example, the last example above could be rewritten

$$S = ((h_1 \to (l_1 \,{}_{.5}{+}\, l_2) \to S)\Box(h_2 \to (l_1 \,{}_{.5}{+}\, l_2) \to S)) \sqcap ((l_1 \,{}_{.5}{+}\, l_2) \to S),$$

which now is deterministic (because the probabilistic choice of deterministic processes is deterministic), and so security is not compromised. Since using any probabilities in this process results in a secure one, we would be safe in deducing that the associated process

$$S = ((h_1 \to (l_1 \sqcap l_2) \to S)\Box(h_2 \to (l_1 \sqcap l_2) \to S)) \sqcap ((l_1 \sqcap l_2) \to S)$$

also is secure, even though it is nondeterministic from Low's viewpoint.

5 Summary

The approach we have taken essentially builds on an idea proposed in [17] to use the pconvex subsets of a power domain to model probabilistic choice and nondeterminism simultaneously. This approach actually provides some interesting new models in which all the laws one might expect hold. But there is much left to be done here. In particular, using these models for a fully abstract denotational semantics of a language for which there is an operational semantics is an obvious goal. In addition, finding a model for CSP that supports all the operators would shed light on the model of PCSP from [17]. And, similarly, such a model could be used for reasoning about the security concerns we just described.

References

1. 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. 353, 354, 359, 360, 361
2. P. America and J. J. R. R. Rutten, *Solving reflexive domains equations in a category of complete metric spaces, Journal of Computer Systems and Sciences* **39** (1989), pp. 343–375. 350
3. S. D. Brookes and A. W. Roscoe, *An improved failures model for communicating processes*, *Lecture Notes in Computer Science* **197** (1985), pp. 281 - 305.
4. E. P. de Vink and J. J. M. M. Rutten, *Bisimulation for probabilistic transition systems: a coalgebraic approach,* CWI preprint, October, 1998.
5. H. Hansson and B. Jonsson, *A calculus for communicating systems with time and probability, Proceedings* of the 11th Symposium on Real Time Systems, 1990. 351
6. 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. 352
7. R. Heckmann, *Probabilistic domains, Proceedings* of CAAP '94, *Lecture Notes in Computer Science* **787** (1994), pp. 142–156. 360, 361
8. M. Hennessy and G. Plotkin, *Full abstraction for a simple parallel programming language,* Lecture Notes in Computer Science **74** (1979), Springer-Verlag. 350, 354
9. C. Jones, "Probabilistic Non-determinism," PhD Thesis, University of Edinburgh, 1990. Also published as Technical Report No. CST-63-90. 350, 351, 352, 355, 356, 359, 361
10. 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. 352, 355
11. A. Jung, *Lawson-compactness for the probabilistic powerdomain,* Preprint, 1997. 359
12. A. Jung and R. Tix, *The troublesome probabilistic powerdomain, Electronic Notes in Theoretical Computer Science* **13** (1998), URL: http://www.elsevier.nl/locate/entcs/volume13.html. 355
13. 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. 355
14. K. Larsen and A. Skou, *Bisimulation through probabilistic testing, Information and Computation* **94** (1991), pp. 456–471. 351
15. G. Lowe, "Probabilities and Priorities in Timed CSP," DPhil Thesis, University of Oxford, 1991. 351
16. N. Lynch and R. Segala, *Probabilistic simulations for probabilistic processes,Proceedings* of CONCUR'94, *Lecture Notes in Computer Science* **836** (1994), pp. 481–496. 351
17. C. Morgan, A. McIver, K. Seidel and J. Sanders, *Refinement-oriented probability for CSP,* University of Oxford Technical Report, 1994. 351, 352, 353, 356, 357, 358, 361, 363
18. C. Morgan, A. McIver, K. Seidel and J. Sanders, *Argument duplication in probabilistic CSP,* University of Oxford Technical Report, 1995. 351, 358
19. A. W. Roscoe. CSP and determinism in security modeling. In *IEEE Symposium on Security and Privacy.* IEEE Computer Society Press, 1995. 362

20. 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. 351
21. N. Saheb-Djahromi, *CPOs of measures for nondeterminism, Theoretical Computer Science* **12** (1980), pp. 19–37. 350, 352, 355