Appendix A

Reasoning about programs combining probability and nondeterminism in a probabilistic logic over continuous state spaces

Preliminary Report
about work done during a research visit*
of Klaus Keimel†
at Tsinghua University with Mingsheng Ying

July 8, 2008

1 Introduction

In [19], Ying Mingsheng has proposed to reason about probabilistic sequential programs in a probabilistic logic. His research was motivated by papers of He Jifeng, C. Morgan, A. McIver, K. Seidel [5, 10, 11, 14] and others on probabilistic nondeterministic programs and their semantics over discrete state spaces. R. Tix, G. Plotkin and K. Keimel [16, 18] have extended this work to continuous state spaces. We now propose to investigate, whether Ying's ideas and methods for reasoning about these nondeterministic programs in a probilistic logic can be carried over from discrete to continuous state spaces. We begin by admitting arbitrary topological state spaces. For the stronger results we have to restrict ourselves to continuous domains (see [3]) which are amply used in semantics.

In our presentation we restrict the values of probabilistic predicates to the unit interval, whilst Ying admitted nonnegative real values in general. This restriction is well motivated and the theory becomes smoother. Instead of the unit interval, we then admit more general quantales L as value domains for probabilistic predicates. This is motivated by the fact that our interval valued probabilistic predicates in a space form again a value quantale and that binary probabilistic relations between S and T can alternatively been viewed as unary probabilistic predicates on S with values in the quantale of unary predicates on T. This is a probabilistic generalisation of the fact that binary (Boolean) relations can alternatively be seen as subsets of the direct product $S \times T$ or as set-valued functions from S with values in the powerset of T.

We are able transfer the results of the first four sections of Ying's paper to this topological situation, in particular, we can prove Theorem 12 on the decomposition of strongly monotonic predicate transformers to continuous state spaces.

As a conclusion we are confident, that probabilistic logic as considered by Ying can be generalised fully to the setting of continuous state spaces.

2 Probabilistic predicates on spaces

We replace the truth values $\{0, 1\}$ of classical logic by the elements of the real interval $\mathbb{I} := [0, 1]$ for probabilistic logic. Our basic operations on $\mathbb{I}$ are multiplication $p \cdot q$, negation $\neg p := 1 - p$ and the formation of suprema $\sup_i p_i$ for arbitrary

*Supported by DFG and NSFC

†Fachbereich Mathematik, Technische Universität Darmstadt, Schloßgartenstraße 7, D–64289 Darmstadt, Germany, Keimel@mathematik.tu-darmstadt.de.

families (p_i). They obey the infinite distributivity law

$$p \cdot \sup_i q_i = \sup_i (p \cdot q_i) \tag{D}$$

whilst $p \mapsto \neg p$ converts supprema to infima and vice versa.

We use multiplication

$$(p, q) \mapsto p \cdot q$$

for interpreting conjunction and the residual

$$(p, q) \mapsto p \to q := \sup\{x \in \mathbb{I} \mid p \cdot x \leq q\}$$

for interpreting implication. One may write

$$p \to q = \min(\frac{q}{p}, 1)$$

if one uses the convention $\frac{q}{0} = 1$ for all $q \in \mathbb{I}$. We use

$$p \mapsto \neg p = 1 - p$$

and

$$(p, q) \mapsto p \text{ or } q := p + q - p \cdot q = \neg(\neg p \cdot \neg q$$

for interpreting negation and disjunction, respectively.

Let S be a topological space (e.g., a dcpo with the Scott topology). A *probabilistic predicate on* S is defined to be an arbitrary lsc (= lower semicontinuous) function $\beta \colon S \to \mathbb{I}$. We denote by $\mathcal{L}S$ the set of all these probabilistic predicates on S.

Note that $\mathcal{L}S$ is stable for pointwise formed products , i.e., for $\alpha, \beta \in \mathcal{L}S$, the map $\alpha \cdot \beta$ defined by $(\alpha \cdot \beta)(s) = \alpha(s) \cdot \beta(s)$ belongs again to $\mathcal{L}S$. With respect to the order defined pointwise – $\alpha \leq \beta$ iff $\alpha(s) \leq \beta(s)$ for all $s \in S$ – $\mathcal{L}S$ is a complete lattice. Suprema are formed pointwise, i.e., for any family $(\beta_i)_i$ in $\mathcal{L}S$, $(\sup_i \beta_i)(x) := \sup_i \beta_i(x)$ for all $x \in S$ is lower semicontinuous, hence a member of $\mathcal{L}S$. Similary, finite infima are formed pointwise. Because of the pointwise definition of the operations the infinite distributivity law (D) also holds in $\mathcal{L}S$.

Thus we may define probabilistic conjunction for two probabilistic predicates by

$$\alpha \cdot \beta$$

and the implication by

$$\alpha \to \beta = \sup\{\chi \in \mathcal{L}S \mid \alpha \cdot \chi \leq \beta\}$$

Disjunction is defined by

$$\alpha \text{ or } \beta = \alpha + \beta - \alpha \cdot \beta$$

Note that $\alpha \cdot \beta$ is in fact lsc: indeed, as α and β are lsc, $1 - \alpha$ and $1 - \beta$ and hence their product $(1 - \alpha)(1 - \beta)$ are usc, whence $\alpha + \beta - \alpha \cdot \beta = 1 - (1 - \alpha) \cdot (1 - \beta)$ is lsc again.

But $\mathcal{L}S$ is not stable for pointwise infima of infinite families. Also, if α is lsc, then $\neg\alpha := 1 - \alpha$ is usc but not lsc, hence not a member of $\mathcal{L}S$ except in the case where α is also usc.

But notice that every function $f \colon S \to \mathbb{I}$ dominates a greatest lsc function $\widehat{f} \colon S \to \mathbb{I}$, namely the pointwise supremum of all lsc functions α below f. We call $\widehat{f}$ the *lsc envelope* of f. We now may describe the infimum of a family α_i in $\mathcal{L}S$ to be the lower semicontinuous envelope of the pointwise infimum

$$\inf_i \alpha_i := \widehat{(s \mapsto \inf_i \alpha_i(s))}$$

and $\alpha \to \beta$ to be the lsc envelope of $\min(\frac{\beta(s)}{\alpha(s)}, 1)$.

Existential quantification for a probabilistic predicate α is defined by

$$\exists x.\alpha(x) := \sup_{x\in S} \alpha(x)$$

. Thus $\exists x$ can be seen as a map from $\mathcal{L}S \to \mathbb{I}$ which preserves arbitrary suprema. Dually, universal quantification is defined by

$$\forall x.\alpha(x) := \inf_{x\in S} \alpha(x)$$

.

Let S and T be topological spaces. A *(binary) probabilistic relation* between T and S is simply a probabilistic predicate on the product space $T \times S$, that is, an lsc function $\rho\colon T \times S \to \mathbb{I}$. For such relations we may define the propositional operators as before and we may define quantification with respect to each of the two variables. For this, let $\rho_y\colon S \to \mathbb{I}$ denote the probabilistic predicate $s \mapsto \rho(y, s)$, and we define

$$\exists y.\rho(y, x) := \sup_{y\in T} \rho_y = \big(s \mapsto \sup_{y\in T} \rho(y, s)\big)$$

$$\forall y.\rho(y, x) := \inf_{y\in T} \rho_y = \big(s \mapsto \inf_{y\in T} \rho(y, s)\big)^\frown$$

where the sup is pointwise, but not the inf which is the lower semicontinuous envelope of the pointwise inf, so that $\exists y.\rho(y, x)$ and $\forall y.\rho(y, x)$ are lsc functions on S, that is, (unary) predicates on S.

3 An abstract formulation

We want to replace the unit interval $\mathbb{I}$ by a more abstract object L.

We require L to be a complete lattice together with an associative commutative multiplication $(a, b) \mapsto a \cdot b$ which satisfies

$$a \cdot \sup_i b_i = \sup_i (a \cdot b_i) \tag{D}$$

This property is equivalent to the conjunction of the following two properties: (1) multiplication is Scott-continuous and (2) $a \cdot (b \vee c) = a \cdot b \vee a \cdot c$. The greatest element of L is supposed to be the identity fir multiplication. We may now define implication to be the residual

$$a \to b = \max\{x \mid a \cdot x \leq b\}$$

Note that the maximum exists, as $a \cdot \sup\{x \mid a \cdot x \leq b\} = \sup\{ax \mid ax \leq b\} \leq b$.

We note that the following *distributivity* laws holds:

$$\inf_i (a_i \to b) = (\sup_i a_i) \to b, \quad \sup_i (a \to b_i) = a \to (\sup_i b_i) \tag{AD}$$

We further require L to be accompanied by another complete lattice L° with a dually Scott-continuous associative commutative multiplication and an order anti-isomorphism $a \mapsto \neg a\colon L \to L^\circ$. The inverse order anti-isomorhism from L° to L is also denoted by $\neg$. It is essential that negation is not a homomorphism for multiplication. The operation or on L can be defined by

$$a \text{ or } b := \neg(\neg a \cdot \neg b)$$

This operation is Scott-continuous, as multiplication on L° was required to be dually Scott-continuous and as negation was an order anti-isomorphism. The operation or is associative and commutative as a consequence of the same properties of the multiplication on L°.

The entity $(L, L^\circ, \neg)$ is called a *value domain*.

In the example $L = \mathbb{I}$, we take $L^\circ = \mathbb{I}$ with the usual order and multiplication and $\neg p = 1 - p$.

We now consider L-valued predicates on a space S. For this we equip the complete lattice L with its Scott topology and we call *L-valued predicate* on S every function $\rho\colon S \to L$ which is continuous with respect to the Scott topology on L; we denote by $\mathcal{L}(S, L)$ the set of these L-valued predicates. With respect to the pointwise defined order $\rho \leq \sigma$ iff $\rho(x) \leq \sigma(x)$ for all $x \in S$, $\mathcal{L}(S, L)$ is a complete lattice. The supremum of any family ρ_i in $\mathcal{L}(S, L)$ is formed pointwise, i.e.,

$$(\sup_i \rho_i)(x) = \sup_i \rho_i(x) \text{ for all } x \in S$$

We may define multiplication for L-valued predicates pointwise by

$$(\rho \cdot \sigma)(x) = \rho(x) \cdot \sigma(x)$$

As multiplication is defined pointwise and as multiplication on L satisfies (D), the same holds for the multiplication in $\mathcal{L}(S, L)$. Thus we may define implication for L-valued predicates as the residual

$$\rho \to \sigma = \sup\{\chi \in \mathcal{L}(S, L) \mid \rho \cdot \chi \leq \sigma\}$$

If $f\colon S \to L$ is any function, there is a greatest continuous function $\widehat{f}$ dominated by f, namely the supremum of all the continuous functions dominated by f; we call $\widehat{f}$ the *continuous lower envelope* of f. It can also be given in the following way:

$$\widehat{f}(x) = \sup_{U \in \mathcal{U}_x} \inf_{x \in U} f(x)$$

where $\mathcal{U}_x$ denotes any neighbourhood basis of the point $x \in S$. In $\mathcal{L}(S, L)$, the infimum is given by the continuous lower envelope of the pointwise infimum.

The dual of the lattice $\mathcal{L}(S, L)$ will be defined to be the lattice $\mathcal{L}^\circ(S, L^\circ)$ of function $\rho^\circ\colon S \to L^\circ$ which are continuous with respect to the dual Scott topology on L°. The multiplication on $\mathcal{L}^\circ(S, L^\circ)$ is defined pointwise. Negation for $\rho \in \mathcal{L}(S, L)$ is easily defined pointwise by

$$(\neg\rho)(x) = \neg\rho(x)$$

The map $\neg\rho\colon L \to L^\circ$ is dually Scott-continuous and $\rho \mapsto \neg\rho$ is an order anti-isomorphim.

There are two ways to define the operation or on L-valued predicates: Firstly we may define

$$\rho \text{ or } \sigma := \neg(\neg\rho \cdot \neg\sigma)$$

or we define it pointwise

$$(\rho \text{ or } \sigma)(x) := \rho(x) \text{ or } \sigma(x)$$

One can easily check that the two defintions agree.

For an L-valued predicate we may define quantification:

$$\exists x.\rho := \sup_x \rho(x)$$

$$\forall x.\rho(x) := \inf_x \rho(x)$$

Thus, $\rho \mapsto \exists x.\rho$ maps L-valued predicates to elements in L. This map preserves arbitrary suprema and, hence, is Scott-continuous.

We observe that $\mathcal{L}(S, L)$ together with $\mathcal{L}^\circ(S, L^\circ)$ and the negation $\neg$ defined above form again a value domain. We may continue this procedure and consider $\mathcal{L}(S, L)$-valued predicates on a space T and form the complete lattice $\mathcal{L}(T, \mathcal{L}(S, L))$ of these predicates, etc.

Going back to our situation in section 1 with $L = \mathbb{I} = L^\circ$, the probabilistic predicates on S, i.e., the lsc functions $\beta\colon S \to \mathbb{I}$ are just those which are continuous with respect to the Scott topology on $\mathbb{I}$, and those that are continuous with

respect to the dual Scott topology on $\mathbb{I}$ are the usc ones. Thus $\mathcal{L}^\circ S := \mathcal{L}^\circ(S, \mathbb{I})$ is the set of usc functions from S into $\mathbb{I}$. Negation $\beta \mapsto \neg\beta = 1 - \beta$ is an order anti-isomorphism between lsc and usc functions. As $\mathcal{L}S$ together with $\mathcal{L}^\circ S$ and negation between them form a value domain again we may form $\mathcal{L}S$-valued predicates on any space T. They offer an alternative approach to probabilistic relations from T to S as we will see. We take an abstract approach first.

4 Relations and predicates

Through this section let S and T be topological spaces and L together with L° and a negation a value domain.

We consider L-valued relations between T and S to be functions ρ from the product space $T \times S$ to L which are continuous with respect to the Scott topology on L. That is, L-valued relations between T and S are simply L-valued predicates on $T \times S$. The logical operations for relations are defined as for predicates. In addition we may define quantification $\exists y.\rho$ by

$$\exists y.\rho := \sup_y \rho_y$$

$$\forall y.\rho := \sup_y \rho_y$$

where $\rho_y := (x \mapsto \rho(y, x) \in \mathcal{L}(S, L)$. The sup and inf are to be taken with resepct to the complete lattice $\mathcal{L}(S, L)$. Thus existential quantification $\exists y$ maps L-valued relations between T and S to L-valued predicates on S; and this map from relations to predicates preserves arbitrary suprema and, hence, is Scott-continuous .

An alternative approach to an L-valued relations between T and S is that of $\mathcal{L}(S, L)$-valued predicates on T.

Recall that, at the level of sets, we have a canonical bijection between $L^{T\times S}$ and L^{S^T}, where A^B denotes the set of all functions from B to A. To a function $F\colon T \times S \to L$ we associate the function $curry(F)\colon T \to L^S$ defined by

$$curry(F)(y)(x) = F(y, x) \text{ for all } y \in T, x \in S$$

In general, this bijection $curry$ does not restrict to a bijection between $\mathcal{L}(T \times T, L$ and $\mathcal{L}(T, \mathcal{L}(S, L))$, i.e., L-valued relations between T and S and $\mathcal{L}(S, L)$-valued predicates on T. We have to impose stronger hypotheses.

Recall that a space T is called *core compact* T, if its open subsets form a continuous lattice (see e.g. [3,]). We will use the following fact:

Lemma 4.1. *The direct product of two core compact spaces is core compact.*

¿From [3, II-4.6] we use the following fact:

Proposition 4.2. *If S is a core compact space and L an continuous lattice, then the lattice $\mathcal{L}(S, L)$ of L-valued predicates is continuous.*

¿From [3, II-4.10] we finally get that we may identify L-valued binary relations betwen T and S and $\mathcal{L}(T, \mathcal{L}(S, T))$-valued predicates:

Theorem 4.3. *If S and T are core compact spaces and if L is a continuous lattice, then $\mathcal{L}(S, L)$, $\mathcal{L}(T, \mathcal{L}(S, L))$ and $\mathcal{L}(T \times S, L)$ are continuous lattices and the bijection $curry$ on the set level restricts to an order isomorphism between $\mathcal{L}(T \times S, L)$ and $\mathcal{L}(T, \mathcal{L}(S, L))$.*

As L° is order anti-isomorphic to L, it is dually continuous and $\mathcal{L}^\circ(S, L^\circ)$, $\mathcal{L}^\circ(T, \mathcal{L}^\circ(S, L^\circ))$ and $\mathcal{L}^\circ(T \times T, L^\circ)$ are dually continuous lattices and $curry$ restricts to an order isomorphism between $\mathcal{L}^\circ(T \times S, L^\circ)$ and $\mathcal{L}^\circ(T, \mathcal{L}^\circ(S, L^\circ))$.

Proposition 4.4. *The map $curry$ preserves all of the logical operations.*

The verification is straightforward. As an example let us show that $curry$ preserves products. Indeed for all y and all x we have $\mathsf{curry}(\rho \cdot \sigma)(y)(x) = (\rho \cdot \sigma)(y,x) = \rho(y,x) \cdot \sigma(y,x) = curry(\rho)(y)(x) \cdot curry(\sigma)(y)(x) = (curry(\rho)(y) \cdot curry(\sigma)(y))(x)$. As this holds for all x, we conclude that $\mathsf{curry}(\rho \cdot \sigma)(y) = curry(\rho)(y) \cdot curry(\sigma)(y) = (curry(\rho) \cdot curry(\sigma))(y)$. As this holds for all y, we conclude that $\mathsf{curry}(\rho \cdot \sigma) = curry(\rho) \cdot curry(\sigma)$.

Altogether we have shown in this section that the logic of binary probabilistic relations on core compact spaces T and S is the same as the logic of $\mathfrak{L}S$-valued predicates on T. And the setting has been put up in such a way that this statement extends to n-ary probabilistic relations inductively.

5 Relational algebra

In this section, R, S, T will be spaces and $(L, L\text{`}\circ, \neg)$ a value domain.

Over continuous spaces the equality relation is not feasable. Equality is not an observable property, it is not semidecidable. In our mathematical model this feature is expressed by the fact that the diagonal in the product space $S \times S$ is not open, hence its characteristic function is not lsc.

Classically the relational product of two relations ρ between T and S and σ between S and R is expressed by:

$$(t,r) \in \rho \circ \sigma \iff \exists s.(t,s) \in \rho \wedge (s,r) \in \sigma$$

Translating this into probabilistic logic we obtain:

Given L-valued relations $\rho \in \mathfrak{L}(T \times S, L)$ and $\sigma \in \mathfrak{L}(S \times R, L)$, their relational product is defined by

$$(\rho \circ \sigma)(s,r) = \sup_{s \in S} \rho(t,s) \cdot \sigma(s,r)$$

The relational product satisfies the infinite distributivity laws

$$\rho \circ (\sup_i \sigma_i) = \sup_i (\rho \circ \sigma_i), \quad (\sup_i \rho_i) \circ \sigma = \sup_i (\rho_i \circ \sigma)$$

and it is associative

$$\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$$

For the proof one uses the infinite distributivity law and the associativity of the multiplication in L.

For a binary L-valued relation ρ on S, we may form its powers $\rho^2 := \rho \circ \rho, \ldots, \rho^{n+1} := \rho^n \circ \rho$. The transitive hull of ρ is given by $\rho^{trans} := \sup_{n \geq 1} \rho^n$. It satisfies $\rho^{trans} \circ \rho^{trans} = \sup_{n \geq 2} \rho^n$.

`it is not clear to me how to define transitivity in this context as we do not have the identity relation.`

Every L-valued relation ρ between T ans S has an obvious converse ρ^{-1} defined by $\rho^{-1}(s,t) = \rho(t,s)$ which is an L-valued relation between S and T. A binary L-valued relation ρ on S is symmetric, if $\rho = \rho^{-1}$. The symmetrisation ρ^{symm} of such a relation ρ, classically given by the statement $(t,s) \in \rho \wedge (t,s) \in \rho^{-1}$ translates into $\rho^{symm}(t,s) = \rho(t,s) \cdot \rho(s,t)$.

`It is an obvious difference between Ying's paper and ours that the identity relation is not on open subset of the product space but a closed subset. Indeed the identity is neither decidable not semidecidable. More generaly, a continuous function from` T `to` S `is not an open relation. But what we can observe is whether` $f(x) \in U$ `for some open set` U`. Thus, instead of looking at relations between` T `and` S`, we have to look for relations between` T `and` $\mathcal{O}S$`. How does this carry over to the probabilistic case? We have to look for lsc functions` $\rho\colon T \times \mathcal{O}S \to \mathbb{I}$ `which are valuations in the second coordinate.`

6 Constructions on probabilistic relations

Let S and T be two spaces and ρ an L-valued probabilistic relation between T and S. We simply write $\mathcal{L}S$ instead of $\mathcal{L}(S, L)$, etc.

We define the *domain* and *range* of ρ to be the probabilistic predicates on T and S, respectively, given by

$$(\operatorname{dom}\rho)(t) := \sup_s \rho(t,s), \quad (\operatorname{range}\rho)(s) = \sup_t \rho(t,s)$$

Again these definitions are modelled on the nonprobabilistic ones

$$t \in \operatorname{dom}\rho \iff \exists s.(t,s) \in \rho, \quad s \in \operatorname{range}\rho \iff \exists t.(t,s) \in \rho$$

Every Scott-continuous map $t\colon \mathcal{L}S \to \mathcal{L}T$ will be called a *predicate transformer*.

Let us turn to the *angelic* and *demonic predicate transformers* $\{\rho\}$ and $[\rho]$ associated with a relation ρ. These will transform predicates on S into predicates on T. Classically, for a postcondition β on S, we have

$$t \in \{\rho\}(\beta) \iff \exists s.(t,s) \in \rho \wedge s \in \beta$$

$$t \in [\rho](\beta) \iff \forall s.(t,s) \in \rho \to s \in \beta$$

(In other contexts, these are just the two ways to define the inverse image of of a subset under a relation.) Translating this into probabilistic logic, we obtain

$$\{\rho\}(\beta)(t) := \sup_s \rho(t,s) \cdot \beta(s), \quad [\rho](\beta) := \widehat{\big(t \mapsto \inf_{s\in S}(\rho(t,s) \to \beta(s))\big)}$$

`the predicate transformers are continuous and preserve ...???` Note that $\rho(t,s) \to \beta(s)$ is not continuous in s. But this does not do any harm.

Claim:

$$\{\rho \circ \sigma\} = \{\rho\} \circ \{\sigma\}, \quad [\rho \circ \sigma] = [\rho] \circ [\sigma]$$

The first of these equations is straightforward from the definitions. For the second one has to use the law (AD) which holds in any value domain.

We have an obvious embedding of L in $\mathcal{L}S$ by mapping every $a \in L$ to the constant function c_a with value a. This map preserves arbitrary suprema and multiplication. There is an adjoint $\alpha \mapsto \underline{\alpha} := \max\{a \in L \mid c_a \le \alpha\}$. An equivalent definition is $\underline{\alpha} = \inf_{s\in S} \alpha(s)$. The adjoint preserves arbitrary infima, but not suprema or multiplication, in general. There are exceptions. If S has a smallest element $\bot$, then $\underline{\alpha} = \alpha(\bot)$ and consequently $\sup_i \underline{\alpha_i} = \sup_i \alpha_i(\bot) = \underline{\sup_i \alpha_i}$.

For two L-valued predicates α and β on S, the *implication strength* is defined to be

$$str(\alpha \to \beta) := \underline{\alpha \to \beta}$$

One can also say that $str(\alpha \to \beta) = \max\{a \in L \mid a \cdot \alpha \le \beta\}$. In particular, $str(\alpha \to \beta) = 1$ if and only if $\alpha \le \beta$.

A predicate transformer $t\colon \mathcal{L}S \to \mathcal{L}T$ will be called *monotone* if $\alpha \le \beta \implies t(\alpha) \le t(\beta)$ and *strongly monotone* if $str(\alpha \to \beta) \le str(t(\alpha) \to t(\beta))$.

Lemma 6.1. *Every strongly monotone predicate transformer t is monotone. If t is monotone and homogeneous, then it is strongly monotone.*

Proof. If $\alpha \le \beta$ then $str(\alpha \to \beta) = 1$; hence, if t is strongly monotone, $str(\alpha \to \beta) \le str(t(\alpha) \to t(\beta))$ implies $str(t(\alpha) \to t(\beta)) = 1$, whence $t(\alpha) \le t(\beta)$. Thus t is monotone. Conversely, Let $a \le str(\alpha \to \beta)$. Then $a \cdot \alpha \le \beta$. Using the monotonicity of t, we conclude that $t(a \cdot \alpha) \le t(\beta)$. Using the homogeneity of t, we obtain $a \cdot t(\alpha) \le t(\beta)$, whence $a \le str(t(\alpha) \to t(\beta))$. We conclude that $str(\alpha \to \beta)) \le str(t(\alpha) \to t(\beta))$ □

Lemma 6.2. *For an L-valued relation ρ between T and S, the angelic update $\{\rho\}$ is homogeneous.*

Proof. Let $\alpha \in \mathcal{L}S$ and $a \in L$. Then $a \cdot \{\rho\}(\alpha)(t) = a \cdot \sup_s \rho(t,s) \cdot \alpha(s) = \sup_s \rho(t,s) \cdot a \cdot \alpha(s) = \{\rho\}(a \cdot \alpha)$. This shows that the angelic update is homogeneous. □

Lemma 6.3. *(a) For an L-valued relation ρ between T and S, the angelic and the demonic updates are strongly monotone. (b) If (t_i) is a family of strongly monotone predicate transformers, then $\sup_i t_i$ and $\inf_i t_i$ are also strongly monotone. (c) The composition of strongly monotone predicated transformers is strongly monotone.*

Proof. (a) For the angelic update this follows from the two previous lemmas. For the demonic update, consider $\alpha, \beta \in \mathcal{L}S$. Let $a \leq str(\alpha \to \beta)$, i.e., $a \cdot \alpha \leq \beta$. As $\rho_s \cdot (\rho_s \to \alpha(s)) \leq \alpha(s)$ by definition, we have $\rho_s \cdot a \cdot (\rho_s \to \alpha(s)) \leq a \cdot \alpha(s) \leq \beta(s)$. Hence $a \cdot (\rho_s \to \alpha(s)) \leq (\rho_s \to \beta(s))$ for all s. We conclude that $a \cdot [\rho](\alpha) = a \cdot \inf_s(\rho_s \to \alpha(s)) = \inf_s a \cdot (\rho_s \to \alpha(s)) \leq \inf_s(\rho_s \to \beta(s)) = [\rho](\beta)$ and we finally have $a \cdot [\rho](\alpha) \leq [\rho](\beta)$, i.e., $a \leq str([\rho](\alpha) \to [\rho](\beta))$. As this holds in particular for $a = str(\alpha \to \beta)$, we have our desired result. The proof of (b) and (c) is straightforward. □

Theorem 6.4. *Suppose that L is a continous lattice and S, T are core compact spaces. A predicate transformer $t\colon \mathcal{L}S \to \mathcal{L}T$ is strongly monotonic if and only if it has a decomposition $t = [\sigma] \circ \{\rho\}$ for the angelic update of some relation ρ and the demonic update of some relation σ.*

Proof. By the previous lemma, the composition $t = [\sigma] \circ \{\rho\}$ of the angelic update of some relation ρ and the demonic update of some relation σ is strongly monotonic. Let us prove the converse.

Given a strongly monotonic t, define a relation ρ between T and $\mathcal{L}S$ and a relation σ beween $\mathcal{L}S$ and S by

$$\rho(y, \alpha) := t(\alpha)(y)$$

$$\sigma(\alpha, x) = \alpha(x)$$

Thus, σ is an evaluation map and ρ is composed by t, which is continuous by hypothesis, and an evaluation map. Under our hypotheses, the evaluation maps are continuous (see [3, II-4.5(iii) and II-4.6]. Thus ρ and σ are continuous.

Let us make explicit the demonic update $[\sigma]\colon \mathcal{L}S \to \mathcal{L}\mathcal{L}S$: For $\alpha \in \mathcal{L}S$, $[\sigma](\alpha)$ is the continuous lower envelope of the function $\beta \mapsto \inf_x(\sigma(\beta, x) \to \alpha(x)) = \inf_x(\beta(x) \to \alpha(x))$ which is $\beta \mapsto str(\beta \to \alpha)$.

Let us make explicit the angelic update of $\{\rho\}\colon \mathcal{L}\mathcal{L}S \to \mathcal{L}T$: For $A \in \mathcal{L}\mathcal{L}S$, $\{\rho\}(A)$ is a map from T to L. For every $y \in T$ we have: $\{\rho\}(A)(y) = \sup_\beta \rho(y, \beta) \cdot A(\beta) = \sup_\beta t(\beta)(y) \cdot A(\beta)$, whence $\{\rho\}(A) = \sup_\beta t(\beta) \cdot A(\beta)$.

Altogether we obtain $\{\rho\}([\sigma](\alpha)) = \sup_\beta t(\beta) \cdot str(\beta \to \alpha)$. Considering the special case $\alpha = \beta$ we obtain $\sup_\beta t(\beta) \cdot str(\beta \to \alpha) \geq < t(\alpha) \cdot str(\alpha \to \alpha) = t(\alpha) \cdot 1 = t(\alpha)$. Conversely, by our hypothesis of strong monotonicity, $str(\beta \to \alpha) \leq str(t(\beta) \to t(\alpha))$, whence $\sup_\beta t(\beta) \cdot str(\beta \to \alpha) \leq \sup_\beta t(\beta) \cdot str(t(\beta) \to t(\alpha)) \leq t(\alpha)$ by the definition of $str(t(\beta) \to t(\alpha))$. This proves that $\{\rho\}([\sigma](\alpha)) = t(\beta)$, whence $\{\rho\} \circ [\sigma] = t$ □

References

[1] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Clarendon Press, 1994.

[2] M. Alvarez-Manilla, A. Jung, and K. Keimel. The probabilistic powerspace for stably compact spaces. *Theoretical Computer Science*, 328:221–244, 2004.

[3] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. W. Mislove, and D. S. Scott. *Continuous Lattices and Domains*, volume 93 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2003.

[4] G. Gierz and K. Keimel. Halbstetige Funktionen und stetige Verbände. In R.-E. Hoffman, editor, *Continuous Lattices and Related Topics*, volume 27 of *Mathematische Arbeitspapiere*. Universität Bremen, 1982, pages 59–67.

[5] He Jifeng, A. McIver, and K. Seidel. Probabilistic models for the guarded command language. *Science of Computer Programming*, 28:171–192, 1997.

[6] C. Jones. *Probabilistic non-determinism*. PhD thesis, Department of Computer Science, University of Edinburgh, Edinburgh, 1990. 201pp.

[7] A. Jung and R. Tix. The troublesome probabilistic powerdomain. In A. Edalat, A. Jung, K. Keimel, and M. Kwiatkowska, editors, *Proceedings of the Third Workshop on Computation and Approximation*, volume 13 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers B.V., 1998. Available from `www.elsevier.nl/cas/tree/store/tcs/free/noncas/pc/menu.htm`, 23 pp.).

[8] O. Kirch. Bereiche und Bewertungen. Master's thesis, Technische Hochschule Darmstadt, June 1993. 77pp., `www.mathematik.tu-darmstadt.de/ags/ag14/papers/kirch/`.

[9] D. Kozen. Semantics of probabilistic programs. *J. Comp. System Sci.*, 22:328–350, 1981.

[10] A. McIver and C. Morgan. Partial correctness for probablistic demonic programs. *Theoretical Computer Science*, 266:513–541, 2001.

[11] A. McIver, and C. Morgan, . Specification and Refinement of Probabilistic Systems. *Monographs in Computer Science*, Springer Verlag, 2004, 402 pages.

[12] M. Mislove. Nondeterminism and probabilistic choice: Obeying the laws. In *Proc. 11th CONCUR*, volume 1877 of *Lecture Notes in Computer Science*, pages 350–364. Springer Verlag, 2000.

[13] M. Mislove, J. Ouaknine and J. Worrell. Axioms for probability and nondeterminism, In: Proc. EXPRESS'03, ENTCS 91(3), 2003.

[14] C. Morgan, A. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 8(1):1–30, January 1999.

[15] R. Tix. Stetige Bewertungen auf topologischen Räumen. Master's thesis, Technische Hochschule Darmstadt, June 1995. 51pp., `www.mathematik.tu-darmstadt.de/ags/ag14/papers/tix/`.

[16] R. Tix. *Continuous D-cones: Convexity and Powerdomain Constructions*. PhD thesis, Technische Universität Darmstadt, 1999. Shaker Verlag, Aachen.

[17] R. Tix. Some results on Hahn-Banach type theorems for continuous d-cones. *Theoretical Computer Science*, 264:205–218, 2001.

[18] R. Tix, K. Keimel, G.D. Plotkin. Semantic Domains Combining Probabilty and Nondeterminism. *Electronic Notes in Theoretical Computer Science*, 129:1–104, 2005.

[19] M. Ying. Reasoning about probabilistic sequential programs in a probabilistic logic. Acta Informatica 39, 315 – 389 (2003).