Relating Direct and Predicate Transformer Partial Correctness Semantics for an Imperative Probabilistic-Nondeterministic Language

K. Keimel, A. Rosenbusch, T. Streicher
Fachbereich 4 Mathematik, TU Darmstadt
Schloßgartenstr. 7, D-64289 Darmstadt

December 21, 2008

1 Introduction

In [KRS], based on [TKP, KP], a predicate transformer semantics has been derived from a direct *total correctness* semantics for a nondeterministic/probabilistic basic imperative programming language $\mathcal{L}_p$ whose syntax is given (in BNF-form) by

$$P ::= a \mid P; P \mid \mathbf{cond}(b, P, P) \mid \mathbf{while}(b, P) \mid P_p\oplus P \mid P[]P$$

where b ranges over a set BExp of *boolean expressions*, a ranges over a set Act of *basic actions* and p is a real number with $0 < p < 1$.[1] The aim of the current paper is to perform this task for the *partial correctness* case where the direct semantics of a program P is given by a function from the set S of states to $\mathcal{P}_L\mathcal{V}(S)$, the convex lower powerdomain of valuations on S.

Here $\mathcal{V}(S)$ is the set of all subprobability distributions on S which we identify with functions $\mu : S \to [0, 1]$ such that $\sum_{s\in S} \mu(s) \leq 1$. Thus $\mathcal{V}(S)$ is a subdomain of $\mathbb{I}^S$ where $\mathbb{I}$ is the unit interval $[0, 1]$ considered as a domain with the usual order $\leq$. The domain $\mathcal{P}_L\mathcal{V}(S)$ consist of all nonempty convex closed lower subsets of $\mathcal{V}(S)$ ordered by $\subseteq$. With every $f : S \to \mathcal{P}_L\mathcal{V}(S)$ one may associate the function $\mathsf{Wp}(f) : \mathbb{I}^S \to \mathbb{I}^S$ defined as

$$\mathsf{Wp}(f)(\gamma)(s) = \sup_{\mu\in f(s)} \langle \mu, \gamma\rangle$$

where $\langle \mu, \gamma\rangle = \sum_{s\in S} \gamma(s)\cdot\mu(s)$. One may characterize the image of

$$\mathsf{Wp} : [S \to \mathcal{P}_L\mathcal{V}(S)] \to [\mathbb{I}^S \to \mathbb{I}^S]$$

[1] We write $\mathbf{cond}(b, P, Q)$ for the *conditional* usually denoted as **if** b **then** P **else** Q **fi**. and $\mathbf{while}(b, P)$ for the *while loop* usually denoted as **while** b **do** P **od**. The program $P[]Q$ *nondeterministically* executes either P or Q. The program $P_p\oplus Q$ executes P with probability p and Q with probability $1-p$.

as the collection of those Scott-continuous maps $T : \mathbb{I}^S \to \mathbb{I}^S$ whose transpose $\widetilde{T} : S \to [\mathbb{I}^S \to \mathbb{I}]$ factors through the sub-dcpo $\mathcal{G}(S)$ of those Scott-continuous maps $G : \mathbb{I}^S \to \mathbb{I}$ which are *sublinear* in the sense that for all $r \in \mathbb{I}$ and $\gamma, \beta \in \mathbb{I}^S$

(1) $G(r{\cdot}\gamma) = r{\cdot}G(\gamma)$

(2) $G(\gamma + \beta) \leq G(\gamma) + G(\beta)$ whenever $\gamma + \beta \leq \mathbf{1}$

where $\mathbf{1}$ stands for the constant function with value 1 which is the top element of $\mathbb{I}^S$. We will show that $\mathcal{G}(S)$ is isomorphic to $\mathcal{P}_L\mathcal{V}(S)$ via a kind of *Minkowski duality* as given by the isomorphism

$$\Phi : \mathcal{P}_L\mathcal{V}(S) \to \mathcal{G}(S) : A \mapsto (\gamma \mapsto \sup_{\mu \in A} \langle \mu, \gamma \rangle)$$

whose inverse is given by

$$\Psi(G) = \{\mu \in \mathcal{V}(S) \mid G(\gamma) \geq \langle \mu, \gamma \rangle \text{ for all } \gamma \in \mathbb{I}^S\}$$

The developments in this paper are to a large extend dual to those in [KRS]. There is one major difference: in order to describe partial correctness adequately we have to modify this dual approach. Our systematic derivation of predicate transformer semantics will explain why in the partial correctness case the clause for **while**-programs is given by *greatest* whereas in the total correctness case one has to use *least* fixpoints. The benefit of greatest fixpoints is that they support a reasoning technique by *invariants* for while-loops which is not admissible for the total correctness variant studied in [KRS].

Discussion of related work.
Our predicate transformer semantics for the partial correctness case was introduced in [MMa] and later used in the monograph [MMb]. The main difference between the account of [MMa] and our approach is that we start form a direct partial correctness semantics based on the lower powerdomain whereas in [MMa] both partial and total correctness predicate transformer semantics are derived from a direct semantics associating with every program P a function $[\![P]\!] : S \to \mathcal{P}\mathcal{V}(S)$ where $\mathcal{P}$ stands for the Plotkin powerdomain. In [MMa] from this direct semantics they define $\mathsf{ewp}(P)(\gamma)(s) = \inf_{\mu \in [\![P]\!](s)} \langle \mu, \gamma \rangle$ which coincides with the wp of our [KRS] for $\gamma \geq 0$. Based on ewp in [MMa] they define $\mathsf{wlp}(P)(\gamma) = 1 + \mathsf{ewp}(P)(\gamma - 1)$ and notice in footnote 10 of *loc.cit.* that $\mathsf{wlp}(P)(\gamma) = \inf_{\mu \in [\![P]\!](s)} 1 - \langle \mu, 1 - \gamma \rangle$ which thus coincides with our definition of wlp.

As opposed to [MMa] we derive wlp from a direct partial correctness semantics which is based on Minkowski duality allowing us a more conceptual treatment of composition. Moreover, in our Theorem 4.2 we give a detailed verification of the equations allowing one to define wlp by recusrion on the structure of programs.

2 Preliminaries

We denote by $\mathbb{R}$, $\mathbb{R}_+$, and $\mathbb{I}$ the reals, the nonnegative reals, and the unit interval $[0,1]$, respectively, endowed with their usual Hausdorff topology and linear order.

For an arbitrary set S, the spaces $\mathbb{R}^S$, $\mathbb{R}_+^S$ and $\mathbb{I}^S$ of all functions γ from S into $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{I}$, respectively, are endowed with the pointwise defined order

$$\gamma \leq \beta \iff \gamma(s) \leq \beta(s) \text{ for all } s \in S$$

and the topology of pointwise convergence, i.e., the product topology. Note that $\mathbb{I}^S$ is a compact space by Tychonoff's theorem. With respect to the order, we have pointwise defined join and meet operations in all of our three function spaces

$$(\gamma \vee \beta)(s) = \max(\gamma(s), \beta(s))$$
$$(\gamma \wedge \beta)(s) = \min(\gamma(s), \beta(s))$$

Also, $\mathbb{R}^S$ is a real vector space for pointwise defined addition and scalar multiplication. A subset A is *convex*, if $p\beta + (1-p)\gamma \in A$ for all $\beta, \gamma \in A$ and all $p \in \mathbb{I}$. For any $A \subseteq \mathbb{R}^S$, we write $\mathsf{conv}(A)$ for its *convex hull*, the smallest convex set containing A. Note that $\mathbb{I}^S$ is a convex subset of $\mathbb{R}^S$.

We need two basic concepts from domain theory. (For an extensive treatment of domain theory one may consult [GHK$^+$].)

A *bounded directed complete partially ordered set* (a *bdcpo*, for short) is a partially ordered set L in which every directed family $(d_i)_i$, which has an upper bound, has a least upper bound $\sup_i d_i$. If every directed family in L has a least upper bound, then L is called *directed complete* (or a *dcpo*, for short). We also suppose that our dcpos always have a least element denoted by $\perp$ or by 0. A *lower subset* of a poset is a subset A with the property that $x \leq a \in A$ implies $x \in A$. For an arbitrary subset A, we denote by

$$\downarrow A = \{x \mid x \leq a \text{ for some } a \in A\}$$

the lower set generated by A. Note that $\mathbb{I}^S$ is a lower set in $\mathbb{R}_+^S$ and that every nonempty lower subset of $\mathbb{R}_+^S$ contains 0, the smallest element of $\mathbb{R}_+^S$.

A map f from a (b)dcpo L to another (b)dcpo M is said to be *strict*, if it preserves the least element (i.e., $f(0) = 0$); it is said to be *Scott-continuous* if it preserves the order (i.e., $a \leq b \implies f(a) \leq f(b)$) and suprema of (bounded) directed sets (i.e., $f(\sup_i d_i) = \sup_i f(d_i)$ for every (bounded) directed family $(d_i)_i$ in L). The set $[L \to M]$ of all Scott-continuous maps from L to M with the pointwise defined order is again a (b)dcpo with directed suprema being defined pointwise.

$\mathbb{R}_+$ and the function space $\mathbb{R}_+^S$ are examples of bdcpos, and every lower subset of a bdcpo is a bdcpo. $\mathbb{I}$ and $\mathbb{I}^S$ are dcpos and likewise every closed lower subset thereof. Addition $(\gamma, \beta) \mapsto \gamma + \beta$ and the join operation $(\gamma, \beta) \mapsto \gamma \vee \beta$ as well as the scalar multiplication are Scott-continuous on $\mathbb{R}_+$ and $\mathbb{R}_+^S$. It follows that $(\gamma, \beta) \mapsto p\gamma + (1-p)\beta$ is continuous and Scott-continuous for every $p \in \mathbb{I}$.

Notice, moreover, that dcpos form a cartesian closed category (with exponential objects $[L \to M]$ as described above) and thus provides a model for typed λ-calculus (see e.g. [Plo, Str]). This has the consequence that every λ-definable function is automatically Scott-continuous. This fact will be used later on in a crucial way for simplifying arguments. Occasionally we will informally use the notation of λ-calculus, where $\lambda x.E(x)$ stands for $x \mapsto E(x)$.

The following facts will be useful: The *support* of a $\sigma \in \mathbb{R}_+^S$ is the set $\mathsf{supp}(\sigma) = \{s \in S \mid \sigma(s) > 0\}$. The $\sigma \in \mathbb{R}_+^S$ with finite support form a lower set. We define a relation $\ll$ by $\sigma \ll \gamma$ iff $\mathsf{supp}(\sigma)$ is finite and $\sigma(s) < \gamma(s)$ for all $s \in \mathsf{supp}(\sigma)$. The following properties are immediate from the definition and express that $\mathbb{R}_+^S$ is a continuous poset for which the elements with finite support form a basis in the sense of domain theory:

1. For every $\gamma \in \mathbb{R}_+^S$ the set $\mathop{\downarrow}\gamma =_{def} \{\sigma \in \mathbb{R}_+^S \mid \sigma \ll \gamma\}$ is directed and $\gamma = \sup \mathop{\downarrow}\gamma$.
2. If $\gamma \leq \sup_i \gamma_i$ for some directed family γ_i in $\mathbb{R}_+^S$ and $\sigma \ll \gamma$, then $\sigma \leq \gamma_i$ for some i.
3. If $\sigma \ll \gamma$ and if (γ_i) is a net in $\mathbb{R}_+^S$ converging (pointwise) to γ, then $\sigma \leq \gamma_i$ for some i.

We use these properties for the following observation:

Lemma 2.1. *The closure $\overline{A}$ of a lower set $A \subseteq \mathbb{R}_+^S$ is a lower set in $\mathbb{R}_+^S$. More precisely, γ belongs to the closure of A iff $\mathop{\downarrow}\gamma \subseteq A$.*

Proof. Let B be the set of all γ such that $\mathop{\downarrow}\gamma \subseteq A$. As γ is the supremum of the directed set $\mathop{\downarrow}\gamma$, it is the limit of this directed set considered as a net. Thus, if $\mathop{\downarrow}\gamma \subseteq A$, then $\gamma \in \overline{A}$, and we have proved that $B \subseteq \overline{A}$. Conversely, if $\gamma \in \overline{A}$, then γ is the limit of some net (γ_i) in A. By the third property above, every $\sigma \ll \gamma$ is dominated by some γ_i. As $\gamma_i \in A$ and as A is a lower set, $\sigma \in A$. Thus $\mathop{\downarrow}\gamma \in A$, whence $\gamma \in B$.

For proving that B is a lower set, chose any $\gamma \in B$ and consider a $\beta \leq \gamma$. For any $\tau \ll \beta$ we then have $\tau \ll \gamma = \sup \mathop{\downarrow}\gamma$. By the second property above of the relation $\ll$ it follows that $\tau \leq \sigma$ for some $\sigma \in \mathop{\downarrow}\gamma$. As $\sigma \in A$ and as A is a lower set, we conclude that $\tau \in A$. As this holds for all $\tau \in \mathop{\downarrow}\beta$, we infer that $\beta \in B$. □

As the closure of a convex set is always convex we conclude:

Corollary 2.1. *The closure of a convex lower set in $\mathbb{R}_+^S$ is a convex lower set.*

Let us stress that topological notions, like *closed set*, *closure* $\overline{A}$ of a subset A, *continuous function* always refer to the Hausdorff topologies considered at the beginning of these preliminaries, whilst the term *Scott-continuous* refers to the order theoretical notion of preservation of directed suprema. In this paper we have tried to keep the domain theoretical notions to a minimum, using on the reals the usual topology and the topology of pointwise convergence on our

function spaces. We do not use the Scott topology explicitly. The expert should notice that the previous lemma shows that in our function spaces the Scott-closed sets are just the closed lower sets.

3 Direct Semantics for $\mathcal{L}_p$

Let S be some unspecified (countable) set of states. Basic actions are interpreted as (and identified with) certain functions $a\colon S \to S$.

The set $\mathcal{V}(S)$ of *subprobability distributions* on S consists of all $\mu : S \to \mathbb{I}$ with $\sum_{s\in S} \mu(s) \leq 1$. We may put $\mu(\bot) = 1 - \sum_{s\in S} \mu(s)$ giving rise to a *probability measure* μ on $S_\bot = S \cup \{\bot\}$ with $\mu(A) = \sum_{s\in A} \mu(s)$ for arbitrary $A \subseteq S_\bot$. Note that $\mathcal{V}(S)$ is a closed convex lower subset of $\mathbb{I}^S$, hence also compact.

There is a canonical inclusion

$$\eta\colon S \to \mathcal{V}(S)$$

sending $s \in S$ to the Dirac measure $\eta(s)$ defined by $\eta(s)(t) = 1$ if $s = t$ and $\eta(s)(t) = 0$ otherwise.

The lower powerdomain $\mathcal{P}_L\mathcal{V}(S)$ consists of all **nonempty**, **closed**, **convex**, **lower** sets $A \subseteq \mathcal{V}(S)$ and is ordered by inclusion $A_1 \subseteq A_2$. As $\mathcal{V}(S)$ is compact and Hausdorff, closed subsets are the same as compact ones. The singleton set $\{0\}$ consisting of the zero distribution is the least element of $\mathcal{P}_L\mathcal{V}(S)$. The intersection $\bigcap_{i\in I} A_i$ of any family $(A_i)_{i\in I}$ in $\mathcal{P}_L\mathcal{V}(S)$ belongs again to $\mathcal{P}_L\mathcal{V}(S)$. Thus, $\big(\mathcal{P}_L\mathcal{V}(S)), \subseteq\big)$ is a complete lattice, whence a dcpo. For a directed family $(A_i)_{i\in I}$, the join is the closure of its union $\bigsqcup_i A_i = \overline{\bigcup_{i\in I} A_i}$ by Corollary 2.1. There is a canonical inclusion

$$i\colon \mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S) : \mu \mapsto {\downarrow}\mu$$

which is easily seen to be Scott-continuous. Composing the two canonical maps we obtain a canonical map

$$\varepsilon = i \circ \eta\colon S \to \mathcal{P}_L\mathcal{V}(S) : s \mapsto {\downarrow}\eta(s)$$

The semantics we will define for $\mathcal{L}_p$ will associate with every program P a function $[\![P]\!] : S \to \mathcal{P}_L\mathcal{V}(S)$. For interpreting probabilistic choice ${}_p\oplus$ we need the following lemma.

Lemma 3.1. *For $A_1, A_2 \in \mathcal{P}_L\mathcal{V}(S)$ and $0 < p < 1$, the convex combination*

$$A_1 {}_p\oplus A_2 = pA_1 + (1-p)A_2 = \{p\mu_1 + (1-p)\mu_2 \mid \mu_1 \in A_1, \mu_2 \in A_2\}$$

is again a member of $\mathcal{P}_L\mathcal{V}(S)$.

Proof: Being the image of the compact convex set $A_1 \times A_2$ under under the continuous affine map $(\mu_1, \mu_2) \mapsto p\mu_1 + (1-p)\mu_2$, the set $pA_1 + (1-p)A_2$ is also convex and compact, hence closed. In order to prove that it is a lower set,

let $\mu \leq p\mu_1 + (1-p)\mu_2$ for some $\mu_1 \in A_1$, $\mu_2 \in A_2$. Let $\mu_1' = p\mu_1 \wedge \mu$ and $\mu_2' = \mu - \mu_1'$ Then $\mu = \mu_1' + \mu_2'$ and $\mu_1' \leq p\mu_1, \mu_2' \leq (1-p)\mu_2$. Now let $\mu_1'' = \frac{1}{p}\mu_1'$ and $\mu_2'' = \frac{1}{1-p}\mu_2'$. Then $\mu_1'' \leq \mu_1$ and $\mu_2'' \leq \mu_2$, whence $\mu_1'' \in A_1$ and $\mu_2'' \in A_2$ and $\mu = p\mu_1'' + (1-p)\mu_2'' \in pA_1 + (1-p)A_2$. □

For interpreting [] we use the binary suprema in $\mathcal{P}_L\mathcal{V}(S)$ which exist as we are in a complete lattice. Explicitly, these binary suprema can be described as follows:

Lemma 3.2. *For $A_1, A_2 \in \mathcal{P}_L\mathcal{V}(S)$, the convex hull*

$$A_1 \sqcup A_2 = \mathsf{conv}(A_1 \cup A_2)$$

is again a closed convex lower set and, hence, the smallest member of $\mathcal{P}_L\mathcal{V}(S)$ containing A_1 and A_2.

Proof: The convex hull of $A_1 \cup A_2$ is equal to $\bigcup_{p\in\mathbb{I}} pA_1 + (1-p)A_2$. Being the union of sets that are lower sets by the previous lemma, $\mathsf{conv}(A_1 \cup A_2)$ is a lower set, too. It also is compact and convex, as it is the image of the compact set $[0,1] \times A_1 \times A_2$ under under the continuous affine map $(p, \mu_1, \mu_2) \mapsto p\mu_1 + (1-p)\mu_2$. □

In order to define the semantics of composition we have to to lift every function $f\colon S \to \mathcal{P}_L\mathcal{V}(S)$ to a Scott-continuous function $f^\dagger\colon \mathcal{P}_L\mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S)$ because then we may define $[\![P_1; P_2]\!]$ as $[\![P_2]\!]^\dagger \circ [\![P_1]\!]$. Moreover, in order to define the semantics of recursive programs it is necessary that the lifting operation

$$(-)^\dagger\colon [S \to \mathcal{P}_L\mathcal{V}(S)] \to [\mathcal{P}_L\mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S)]$$

itself is Scott-continuous.

For this purpose it is helpful to exploit the fact (see Appendix A for details) that $\mathcal{P}_L\mathcal{V}(S)$ is isomorphic to the set $\mathcal{G}(S)$ of all Scott-continuous sublinear functions $G\colon \mathbb{I}^S \to \mathbb{I}$ as defined in the Introduction. By definition, $\mathcal{G}(S)$ is a subset containing the least element: the identically zero function of the set $\mathbb{I}^{\mathbb{I}^S}$ of all functions $G\colon \mathbb{I}^S \to \mathbb{I}$. From our preliminaries, replacing there S by $\mathbb{I}^S$, we know that $\mathbb{I}^{\mathbb{I}^S}$ is a complete lattice and a compact convex subset of $\mathbb{R}^{\mathbb{I}^S}$, where the order relation, arbitrary suprema and convex combinations are defined pointwise. It is straightforward to verify that $\mathcal{G}(S)$ is closed under all of these operations:

Lemma 3.3.

(a) *For every family $(G_i)_i$ in $\mathcal{G}(S)$, the (pointwise) supremum $G(\gamma) = \sup_i G_i(\gamma)$ is again a member of $\mathcal{G}(S)$.*

(b) *For G_1 and G_2 in $\mathcal{G}(S)$, the (pointwise defined) convex combination $pG_1 + (1-p)G_2$ is again a member of $\mathcal{G}(S)$, where $p \in \mathbb{I}$.*

Thus $\mathcal{G}(S)$ is a convex subset of $\mathbb{I}^{\mathbb{I}^S}$ closed for arbitrary suprema, hence a dcpo, and it contains the constant zero function. The map $(G_1, G_2) \mapsto pG_1 + (1-p)G_2$ is Scott-continuous for every $p \in \mathbb{I}$.

By Proposition A.1 in the appendix there is an order isomorphism $\Phi\colon \mathcal{P}_L\mathcal{V}(S) \to \mathcal{G}(S)$. Using the notation $\langle \mu, \gamma \rangle = \sum_s \mu(s)\gamma(s)$ introduced in the Introduction, Φ is given by

$$\Phi(A)(\gamma) = \sup_{\mu \in A} \langle \mu, \gamma \rangle \qquad \text{for all } \gamma \in \mathbb{I}^S$$

the inverse being the map $\Psi\colon \mathcal{G}(S) \to \mathcal{P}_L\mathcal{V}(S)$ given by

$$\Psi(G) = \{\mu \in \mathcal{V}(S) \mid \langle \mu, \gamma \rangle \leq G(\gamma) \text{ for all } \gamma \in \mathbb{I}^S\}$$

For convenience, we sometimes write Φ_A for $\Phi(A)$ and Ψ_G for $\Psi(G)$.

Next we show that Φ and Ψ preserve all relevant structure.

Lemma 3.4.

(a) *Φ and Ψ preserve arbitrary joins; in particular, they are strict and Scott-continuous.*

(b) *Φ and Ψ preserve convex combinations, i.e. $\Phi(A_1 \,{}_p\!\oplus A_2) = p\Phi(A_1) + (1-p)\Phi(A_2)$ and $\Psi(pG_1 + (1-p)G_2) = \Psi(G_1) {}_p\!\oplus \Psi(G_2)$.*

Proof: Claim (a) is a consequence of the order isomorphism property and (b) is shown by the following calculation

$$\begin{array}{rcl} p\Phi_{A_1}(\gamma) + (1-p)\Phi_{A_2}(\gamma) & = & p \sup_{\mu_1 \in A_1} \langle \mu_1, \gamma \rangle + (1-p) \sup_{\mu_2 \in A_2} \langle \mu_2, \gamma \rangle \\ & = & \sup_{\mu_1 \in A_1} \langle p\mu_1, \gamma \rangle + \sup_{\mu_2 \in A_2} \langle (1-p)\mu_2, \gamma \rangle \\ & = & \sup_{\mu_1 \in pA_1} \langle \mu_1, \gamma \rangle + \sup_{\mu_2 \in (1-p)A_2} \langle \mu_2, \gamma \rangle \\ & = & \sup_{\mu_1 \in pA_1, \mu_2 \in (1-p)A_2} (\langle \mu_1, \gamma \rangle + \langle \mu_2, \gamma \rangle) \\ & = & \sup_{\mu_1 \in pA_1, \mu_2 \in (1-p)A_2} \langle \mu_1 + \mu_2, \gamma \rangle \\ & = & \sup_{\mu \in pA_1 + (1-p)A_2} \langle \mu, \gamma \rangle \\ & = & \Phi_{pA_1 + (1-p)A_2}(\gamma) \end{array}$$

□

As convex combinations are Scott-continuous in $\mathcal{G}(S)$, the preceding lemma allows us to conclude:

Corollary 3.1. *The operation ${}_p\!\oplus$ is Scott-continuous on $\mathcal{P}_L\mathcal{V}(S)$.*

Note that $\sqcup$ is Scott-continuous on $\mathcal{P}_L\mathcal{V}(S)$, as in any complete lattice the binary join operation is Scott-continuous.

Recall that in continuation semantics (see e.g. [BHM]) a function $f : S \to [\mathbb{I}^S \to \mathbb{I}]$ is lifted to a function

$$f^{\#}\colon [\mathbb{I}^S \to \mathbb{I}] \to [\mathbb{I}^S \to \mathbb{I}] : G \mapsto \lambda\gamma.G\big(\lambda s.f(s)(\gamma)\big)$$

which is Scott-continuous since it is λ-definable. The so defined lifting operation $(-)^{\#}$ validates the laws

$$f^{\#} \circ \eta = f \qquad\qquad g^{\#} \circ f^{\#} = (g^{\#} \circ f)^{\#}$$

where $\eta = \lambda s.\lambda\gamma.\gamma(s)\colon S \to [\mathbb{I}^S \to \mathbb{I}]$. These laws guarantee that $[S \to [\mathbb{I}^S \to \mathbb{I}]]$ is a monoid w.r.t. (Kleisli) composition $f; g = g^{\#} \circ f$ with unit η. The next lemma tells us that this lifting restricts to $\mathcal{G}(S)$.

Lemma 3.5. *For $f\colon S \to \mathcal{G}(S)$ its lifting $f^{\#}$ restricts to a Scott-continuous endomap on $\mathcal{G}(S)$ which preserves convex combinations and binary joins. Moreover, the restricted lifting map*

$$f \mapsto f^{\#}\colon [S \to \mathcal{G}(S)] \to [\mathcal{G}(S) \to \mathcal{G}(S))]$$

is itself Scott-continuous.

Proof: For $f : S \to \mathcal{G}(S) \subseteq [\mathbb{I}^S \to I]$ its lifting $f^{\#}$ is λ-definable and thus Scott-continuous. Moreover, the map $(-)^{\#} : [S \to [\mathbb{I}^S \to \mathbb{I}]] \to [[\mathbb{I}^S \to \mathbb{I}] \to [\mathbb{I}^S \to \mathbb{I}]]$ itself is also λ-definable and thus Scott-continuous.

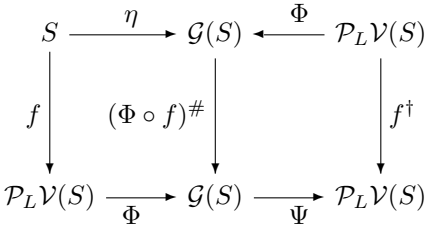
Since $f^{\#}(G)(\gamma) = G(\lambda s.f(s)(\gamma))$ it validates all inequalities holding for G. Thus $f^{\#}$ sends elements of $\mathcal{G}(S)$ to elements of $\mathcal{G}(S)$ and preserves the operations $\vee$ and ${}_p\oplus$ since they are defined pointwise. □

Using the isomorphism $\Phi\colon \mathcal{P}_L\mathcal{V}(S) \to \mathcal{G}(S)$ and its inverse Ψ we can define the lifting of maps $S \to \mathcal{P}_L\mathcal{V}(S)$ as follows

Definition 3.1. *For $f : S \to \mathcal{P}_L\mathcal{V}(S)$ let*

$$f^{\dagger} = \Psi \circ (\Phi \circ f)^{\#} \circ \Phi : \mathcal{P}_L\mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S)$$

as illustrated by



where $\eta(s) = \lambda\gamma.\gamma(s)$.

The so defined $f^{\dagger}$ is Scott-continuous and preserves ${}_p\oplus$ and $\sqcup$. Moreover, this lifting operation $(-)^{\dagger}$ is again Scott-continuous and satisfies the laws

$$f^{\dagger} \circ \eta = f \qquad\qquad g^{\dagger} \circ f^{\dagger} = (g^{\dagger} \circ f)^{\dagger}$$

for all $f, g : S \to \mathcal{P}_L\mathcal{V}(S)$.

Now we are ready to give the clauses for the direct semantics for $\mathcal{L}_p$.

Definition 3.2. *Let* Act *be some set of endofunctions on S and* BExp *be some set of functions from S to $\{0, 1\}$. The* direct semantics *associating to every $\mathcal{L}_p$ program P a function*

$$[\![P]\!]\colon S \to \mathcal{P}_L\mathcal{V}(S)$$

is defined inductively by the following semantic clauses

$$[\![a]\!] = \eta \circ a$$
$$[\![P_1; P_2]\!] = [\![P_2]\!]^\dagger \circ [\![P_1]\!]$$
$$[\![\mathbf{cond}(b, P_1, P_2)]\!](s) = b(s) \cdot [\![P_1]\!](s) + \neg b(s) \cdot [\![P_2]\!](s)$$
$$[\![P_1 {}_p\!\oplus P_2]\!](s) = p \cdot [\![P_1]\!](s) + (1-p) \cdot [\![P_2]\!](s)$$
$$[\![P_1 [\!] P_2]\!](s) = [\![P_1]\!](s) \sqcup [\![P_2]\!](s)$$
$$[\![\mathbf{while}(b, P)]\!] = \mathsf{Minfix} f.\lambda s.\ (b(s) \cdot f^\dagger([\![P]\!](s)) + \neg b(s) \cdot \varepsilon(s))$$

where s ranges over S and $\neg b(s) = 1 - b(s)$. Further, $\mathsf{Minfix} X.E(X)$ denotes the least fixed point of the map $X \mapsto E(X)$ which is well defined, if f ranges over a dcpo with a smallest element and the map $X \mapsto E(X)$ is Scott-continuous, which is the case in our setting above.

Next we give an explicit construction of $f^\dagger : \mathcal{P}_L\mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S)$ from $f : S \to \mathcal{P}_L\mathcal{V}(S)$ which has an immediate intuitive operational reading.

Lemma 3.6. *For $f : S \to \mathcal{P}_L\mathcal{V}(S)$ its lifting $f^\dagger : \mathcal{P}_L\mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S))$ is given by*

$$f^\dagger(A) = \overline{\downarrow \left\{ \sum_s \mu(s)h(s) \mid h \in \prod_{s \in S} f(s) \text{ and } \mu \in A \right\}}$$

for $A \in \mathcal{P}_L\mathcal{V}(S)$. In particular, for $\mu \in \mathcal{V}(S)$ we have

$$f^\dagger(\downarrow\mu) = \overline{\downarrow \left\{ \sum_s \mu(s)h(s) \mid h \in \prod_{s \in S} f(s) \right\}}$$

Proof: Let $A \in \mathcal{P}_L\mathcal{V}(S)$. First we show that the set

$$M_A = \left\{ \sum_s \mu(s)h(s) \mid h \in \prod_s f(s) \text{ and } \mu \in A \right\}$$

is convex. Suppose $\mu_1, \mu_2 \in A$, $h_1, h_2 \in \prod_s f(s)$ and $0 < p < 1$; let $q = 1 - p$. We show that $p \cdot \sum_s \mu_1(s)h_1(s) + q \cdot \sum_s \mu_2(s)h_2(s)$ is also in M_A. For this purpose it suffices to construct an $h \in \prod_s f(s)$ such that

$$p \cdot \sum_s \mu_1(s)h_1(s) + q \cdot \sum_s \mu_2(s)h_2(s) = \sum_s \mu(s)h(s)$$

where $\mu = p \cdot \mu_1 + q \cdot \mu_2 \in A$. An appropriate such $h \in \prod_s f(s)$ can be constructed as follows

$$h(s) = \begin{cases} 0 & \text{if } \mu_1(s) = 0 = \mu_2(s), \\ \frac{p \cdot \mu_1(s) \cdot h_1(s) + q \cdot \mu_2(s) \cdot h_2(s)}{p \cdot \mu_1(s) + q \cdot \mu_2(s)} & \text{otherwise.} \end{cases}$$

The lower set of a convex set is convex and the closure of the lower convex set $\downarrow M_A$ is a lower convex set by Corollary 2.1; thus, $\overline{\downarrow M_A}$ is an element of $\mathcal{P}_L\mathcal{V}(S)$. For showing the desired equality, by Definition 3.1 it suffices to show that

$$(\Phi \circ f)^\#(\Phi(A)) = \Phi(\overline{\downarrow M_A})$$

For this purpose for $\gamma \in \mathbb{I}^S$ we calculate as follows

$$\begin{array}{lcl}
(\Phi \circ f)^{\#}(\Phi(A))(\gamma) & = & \Phi(A)(\lambda s.\, (\Phi \circ f)(s)(\gamma)) = \Phi(A)(\lambda s.\, \Phi(f(s))(\gamma)) \\
& = & \sup_{\mu \in A} \sum_s \mu(s) \cdot \Phi(f(s))(\gamma) \\
& = & \sup_{\mu \in A} \sum_s \mu(s) \cdot \sup_{\nu \in f(s)} \langle \nu, \gamma \rangle \\
& \overset{(*)}{=} & \sup_{\mu \in A} \sup_{h \in \Pi_s f(s)} \sum_s \mu(s) \cdot \langle h(s), \gamma \rangle \\
& = & \sup_{\mu \in A} \sup_{h \in \Pi_s f(s)} \langle \sum_s \mu(s) h(s), \gamma \rangle \\
& = & \sup_{\nu \in M_A} \langle \nu, \gamma \rangle \\
& \overset{(**)}{=} & \sup_{\nu \in \overline{\downarrow M_A}} \langle \nu, \gamma \rangle \\
& = & \Phi(\overline{\downarrow M_A})(\gamma)
\end{array}$$

where $(*)$ follows from the fact that for every $s \in S$ we may choose an $h(s) \in f(s)$ with $\langle h(s), \gamma \rangle$ arbitrarily close to $\sup_{\nu \in f(s)} \langle \nu, \gamma \rangle$ and $(**)$ follows from the fact that the scalar product is Scott-continuous by A.1.
The particular case follows from the fact that $\sum_s \nu(s)h(s) \leq \sum_s \mu(s)h(s)$ whenever $\nu \leq \mu$. □

This lemma is interesting because it admits the following intuitive interpretation: whenever a program P with $f = [\![P]\!]$ is executed in a probabilistic state given by some $\mu \in \mathcal{V}(S)$ then the nondeterministically resulting probabilistic state μ' can be obtained as a directed supremum of probabilistic states below states of the form $\sum_s \mu(s)h(s)$ where $h(s) \in f(s)$ for all $s \in S$. Notice that, in particular, for valuations with finite support $\mu = \sum_{i=1}^n r_i \eta(s_i)$ with $r_i \in \mathbb{I}$ and $\sum_{i=1}^n r_i \leq 1$, we have

$$f^\dagger(\downarrow \mu) = \overline{\left\{ \sum_{i=1}^n r_i g_i(t) \mid g_i \in f(s_i) \text{ for } i = 1, \ldots, n \right\}} = \sum_{i=1}^n r_i f(s_i)$$

from which we conclude that $f^\dagger \circ \downarrow : \mathcal{V}(S) \to \mathcal{P}_L\mathcal{V}(S)$ is the unique extension of f along $\eta : S \to \mathcal{V}(S)$ which is strict, Scott-continuous and preserves convex combinations.

4 From Direct to Predicate Transformer Semantics

The intention of this section is to study a partial correctness predicate transformer semantics for $\mathcal{L}_p$ by deriving it from its direct partial correctness semantics. We first proceed by developing a "dual" version of the predicate transformer semantics developed in [KRS] but now based on the current Minkowski duality which is "dual" to the one considered in [KRS]. Based on this we develop and study a *weakest liberal precondition* (*wlp*) variant supporting the usual technique of reasoning about while-loops by loop invariants (as introduced by Hoare for ordinary deterministic imperative programs) which is not available for the total correctness wp semantics of [KRS].

Recall from the previous section that the interpretation of an $\mathcal{L}_p$ program is a function $S \to \mathcal{P}_L\mathcal{V}(S)$ which by Proposition A.1 may be identified with a function $f : S \to \mathcal{G}(S) \subseteq [\mathbb{I}^S \to \mathbb{I}]$ which uniquely corresponds to a Scott-continuous function $\mathsf{Wp}(f) : \mathbb{I}^S \to \mathbb{I}^S$ as described in the following theorem.

Theorem 4.1. *The function* $\mathsf{Wp} : [S \to \mathcal{G}(S)] \to [\mathbb{I}^S \to \mathbb{I}^S]$ *defined as*

$$\mathsf{Wp}(f)(\gamma)(s) = f(s)(\gamma)$$

is Scott-continuous and one-to-one. The image of Wp *consists of those Scott-continuous functions* $T : \mathbb{I}^S \to \mathbb{I}^S$ *which are sublinear, i.e., which satisfy the conditions*

(1) $T(r{\cdot}\gamma) = r{\cdot}T(\gamma)$

(2) $T(\gamma + \beta) \leq T(\gamma) + T(\beta)$

for all $r \in \mathbb{I}$ *and* $\gamma, \beta \in \mathbb{I}^S$ *with* $\gamma + \beta \leq \mathbf{1}$. *We write* PT *for the image of* Wp.

Proof: The function $\mathsf{Wp}(f)$ is Scott-continuous since it is λ-definable and for the same reason the function Wp itself is Scott-continuous, too.

A function $T : \mathbb{I}^S \to \mathbb{I}^S$ is in the image of Wp iff for all $s \in S$ the function $\lambda\gamma.T(\gamma)(s) \in \mathcal{G}(S)$ which is equivalent to the conditions (1) and (2) which express precisely this requirement. □

For $f : S \to \mathcal{P}_L\mathcal{V}(S)$ the associated predicate transformer $\mathsf{Wp}(\Phi \circ f)$ is also denoted as $\mathsf{Wp}(f)$ and can be described explicitly as follows.

Corollary 4.1. *For* $f : S \to \mathcal{P}_L\mathcal{V}(S)$ *we have*

$$\mathsf{Wp}(f)(\gamma)(s) = \mathsf{Wp}(\Phi \circ f)(\gamma)(s) = \Phi(f(s))(\gamma) = \sup_{\mu \in f(s)} \langle \mu, \gamma \rangle$$

for all $\gamma \in \mathbb{I}^S$ *and* $s \in S$.

Notice the difference to the total correctness predicate transformer semantics of [KRS] where the formula for Wp employs inf instead of sup. In this sense our Wp is dual to the one of [KRS].

The corresponding predicate transformer semantics dual to the one of [KRS] is given in the next definition and characterised in the subsequent theorem.

Definition 4.1. *For an* $\mathcal{L}_p$ *program* P *let* $\mathsf{wp}(P) = \mathsf{Wp}([\![P]\!])$ *be the* predicate transformer *associated with* P.

Lemma 4.1. *The following equations hold for* wp *and characterise it uniquely*

$$\mathsf{wp}(a)(\gamma) = \gamma \circ a$$
$$\mathsf{wp}(P_1; P_2) = \mathsf{wp}(P_1) \circ \mathsf{wp}(P_2)$$
$$\mathsf{wp}(\mathbf{cond}(b, P_1, P_2))(\gamma) = (b \wedge \mathsf{wp}(P_1)(\gamma)) \vee (\neg b \wedge \mathsf{wp}(P_2)(\gamma))$$
$$\mathsf{wp}(P_1 {}_p\!\oplus P_2)(\gamma) = p \cdot \mathsf{wp}(P_1)(\gamma) + (1{-}p) \cdot \mathsf{wp}(P_2)(\gamma)$$
$$\mathsf{wp}(P_1 [\!] P_2)(\gamma) = \mathsf{wp}(P_1)(\gamma) \vee \mathsf{wp}(P_2)(\gamma)$$
$$\mathsf{wp}(\mathbf{while}(b, P))(\gamma) = \mathsf{Minfix}\ \beta.\ (b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge \gamma)$$

where $\wedge$ *and* $\vee$ *stand for the pointwise infimum and supremum on* $\mathbb{I}^S$*, respectively,* $(\neg b)(s) = 1 - b(s)$ *and* $\mathsf{Minfix}X.E[X]$ *stands for the least fixpoint of the Scott-continuous function* $X \mapsto E[X]$*.*

Proof. The crucial cases are composition and the while-loop whereas all other cases are straightforward and left to the reader. For sake of simplicity we work rather on the side of $\mathcal{G}(S)$ than on the side of the more complicated $\mathcal{P}_L\mathcal{V}(S)$ which does not cause any damage since they are isomorphic by our crucial Proposition A.1.

For $\mathcal{L}_p$-programs P_1 and P_2 we have

$$\begin{array}{rcll}
\mathsf{wp}(P_1;P_2)(\gamma)(s) & = & \mathsf{Wp}([\![P_1;P_2]\!])(\gamma)(s) & \\
& = & \mathsf{Wp}([\![P_2]\!]^{\#} \circ [\![P_1]\!])(\gamma)(s) & \\
& = & ([\![P_2]\!]^{\#} \circ [\![P_1]\!])(s)(\gamma) & \\
& = & [\![P_2]\!]^{\#}([\![P_1]\!](s))(\gamma) & \\
& = & [\![P_1]\!](s)(\lambda s.[\![P_2]\!](s)(\gamma)) & \text{(by def. of } (-)^{\#}) \\
& = & \mathsf{Wp}([\![P_1]\!])(\mathsf{Wp}([\![P_2]\!])(\gamma))(s) & \\
& = & \big(\mathsf{Wp}([\![P_1]\!]) \circ \mathsf{Wp}([\![P_2]\!])\big)(\gamma)(s) &
\end{array}$$

Next we consider the case of while-loops. For $\gamma \in \mathbb{I}^S$ we define the auxiliary functions

$$\begin{array}{l}
h_\gamma(f) := \mathsf{Wp}(f)(\gamma) \\
k(f) := \lambda s{:}S.\, b(s) \cdot f^{\#}([\![P]\!](s)) + \neg b(s) \cdot \eta(s) \\
g(\beta) = (b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge \gamma)
\end{array}$$

One easily checks that h_γ is strict (i.e. preserves the least element) and the diagram

$$\begin{array}{ccc}
\mathcal{G}(S)^S & \xrightarrow{h_\gamma} & \mathbb{I}^S \\
{\scriptstyle k}\downarrow & & \downarrow{\scriptstyle g} \\
\mathcal{G}(S)^S & \xrightarrow[h_\gamma]{} & \mathbb{I}^S
\end{array}$$

commutes from which it follows by Plotkin's Lemma on least fixpoint operators (see [Plo] or [GHK$^+$] II-2.4) that

$$\mathsf{wp}(\mathbf{while}(b,P))(\gamma) = h_\gamma(\mathsf{Minfix}(k)) = \mathsf{Minfix}(g) = \mathsf{Minfix}\,\beta.\,(b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge \gamma)$$

as desired. □

This wp-semantics for $\mathcal{L}_p$ does not quite capture the idea of partial correctness since if f is the least element of $[S \to \mathcal{P}_L\mathcal{V}(S)]$, i.e. $f = \lambda s.\{\lambda s.0\}$, then $\mathsf{wp}(f)(s) = 0$ although from point of view of partial correctness one would (and should!) expect that $\mathsf{wp}(f)(s) = 1$.

This defect will be remedied by introducing a so-called *weakest liberal precondition* (*wlp*) semantics which we are now going to motivate. First consider

the classical case of deterministic non-probabilistic computation where a program gets interpreted as a function $f : S \to S_\perp$. For a given *postcondition* $B \subseteq S$ the *weakest liberal precondition* is defined as $\mathsf{Wlp}(f)(B) = f^{-1}[B \cup \{\perp\}]$. Then for $A \subseteq S$ we have $A \subseteq \mathsf{Wlp}(f)(B)$ iff $\forall s \in A\ (f(s) \neq \perp \Rightarrow f(s) \in B)$, i.e. f is partially correct w.r.t. precondition A and postcondition B – usually written as $\{A\}P\{B\}$ – when $f = [\![P]\!]$.

Now let us extend this idea to deterministic probabilistic computation where programs are modeled as functions $f : S \to \mathcal{V}(S)$. Given a (generalised) postcondition $\gamma \in \mathbb{I}^S$ we define $\mathsf{Wlp}(f)(\gamma)(s)$ as $f(s)(\perp) + \langle f(s), \gamma\rangle$, i.e. the probability that the programs executed in state s diverges or "gives a result in γ". Obviously, we have

$$\begin{array}{rcl} \mathsf{Wlp}(f)(\gamma)(s) & = & 1 - \sum_t f(s)(t) + \sum_t f(s)(t)\cdot\gamma(t) \\ & = & 1 - \sum_t f(s)(t) \cdot (1 - \gamma(t)) \\ & = & 1 - \mathsf{Wp}(f)(1-\gamma)(s) \end{array}$$

and thus $\mathsf{Wlp}(f)(\gamma) = 1 - \mathsf{Wp}(f)(1-\gamma)$.

Now we apply this formula to functions $f : S \to \mathcal{P}_L\mathcal{V}(S)$ and obtain

$$\begin{array}{rcl} \mathsf{Wlp}(f)(\gamma)(s) & = & 1 - \mathsf{Wp}(f)(1-\gamma)(s) \\ & = & 1 - \sup_{\mu\in f(s)} \sum_s \mu(s) \cdot (1 - \gamma(s)) \\ & = & \inf_{\mu\in f(s)} 1 - \sum_s \mu(s) \cdot (1 - \gamma(s)) \\ & = & \inf_{\mu\in f(s)} 1 - \sum_s \mu(s) + \sum_s \mu(s) \cdot \gamma(s) \\ & = & \inf_{\mu\in f(s)} \mu(\perp) + \langle \mu, \gamma\rangle \end{array}$$

This formula is also intuitively correct since for given state s and postcondition γ for $\mu \in f(s)$ the number $\mu(\perp) + \langle \mu, \gamma\rangle$ is the probability of the proposition "diverges or satisfies γ". To err on the side of caution one takes the infimum over all $\mu \in f(s)$. Since $1 - \sum_s \mu(s) \cdot (1 - \gamma(s))$ is antitonic in μ this amounts to considering only maximal elements $\mu \in f(s)$ when taking the infimum.

Definition 4.2. *For $f : S \to \mathcal{P}_L\mathcal{V}(S)$ let $\mathsf{Wlp}(f) : \mathbb{I}^S \to \mathbb{I}^S$ be defined as*

$$\mathsf{Wlp}(f)(\gamma) = \mathbf{1} - \mathsf{Wp}(f)(\mathbf{1} - \gamma)$$

for $\gamma \in \mathbb{I}^S$. For $\mathcal{L}_p$ programs P let

$$\mathsf{wlp}(P) = \mathsf{Wlp}([\![P]\!])$$

i.e.

$$\mathsf{wlp}(P)(\gamma) = \mathbf{1} - \mathsf{wp}(P)(\mathbf{1} - \gamma)$$

for $\gamma \in \mathbb{I}^S$.

Since all $\mathsf{Wlp}(f)$ are Scott-continuous and $\gamma \mapsto \mathbf{1}-\gamma$ is an order anti-isomorphism of $\mathbb{I}^S$ it follows that

Lemma 4.2. *For all $f : S \to \mathcal{P}_L\mathcal{V}(S)$ the function $\mathsf{Wlp}(f) : \mathbb{I}^S \to \mathbb{I}^S$ preserves infima of down-directed families.*

This allows us to prove

Theorem 4.2. *The following equations hold for* wlp *and characterize it uniquely*

$$\mathsf{wlp}(a)(\gamma) = \gamma \circ a$$
$$\mathsf{wlp}(P;Q) = \mathsf{wlp}(P) \circ \mathsf{wlp}(Q)$$
$$\mathsf{wlp}(\mathbf{cond}(b,P,Q))(\gamma) = (b \wedge \mathsf{wlp}(P)(\gamma)) \vee (\neg b \wedge \mathsf{wlp}(Q)(\gamma))$$
$$\mathsf{wlp}(P_p \oplus Q)(\gamma) = p \cdot \mathsf{wlp}(P)(\gamma) + (1-p) \cdot \mathsf{wlp}(Q)(\gamma)$$
$$\mathsf{wlp}(P [] Q)(\gamma) = \mathsf{wlp}(P)(\gamma) \wedge \mathsf{wlp}(Q)(\gamma)$$
$$\mathsf{wlp}(\mathbf{while}(b,P))(\gamma) = \mathsf{Maxfix}\ \beta.\ (b \wedge \mathsf{wlp}(P)(\beta)) \vee (\neg b \wedge \gamma)$$

where $\wedge$ *and* $\vee$ *stand for the pointwise infimum and supremum on* $\mathbb{I}^S$*, respectively,* $(\neg b)(s) = 1 - b(s)$ *and* $\mathsf{Maxfix}X.E[X]$ *stands for the greatest fixpoint of the function* $X \mapsto E[X]$*.*

Proof. We just check the first two and the last two equations. The remaining two cases are routine.
For basic programs a we have

$$\begin{array}{rclcl} \mathsf{wlp}(a)(\gamma)(s) & = & (1 - \mathsf{wp}(a)(1-\gamma))(s) & = & 1 - \mathsf{wp}(a)(1-\gamma)(s) \\ & = & 1 - (1-\gamma)(a(s)) & = & 1 - (1 - \gamma(a(s))) = \gamma(a(s)) \\ & = & (\gamma \circ a)(s) & & \end{array}$$

For sequential compositions $P;Q$ we have using Lemma 4.1 that

$$\begin{array}{rcl} \mathsf{wlp}(P;Q)(\gamma) & = & 1 - \mathsf{wp}(P;Q)(1-\gamma) \\ & = & 1 - \mathsf{wp}(P)(\mathsf{wp}(Q)(1-\gamma)) \\ & = & 1 - \mathsf{wp}(P)(1 - (1 - \mathsf{wp}(Q)(1-\gamma))) \\ & = & \mathsf{wlp}(P)(1 - \mathsf{wp}(Q)(1-\gamma)) \\ & = & \mathsf{wlp}(P)(\mathsf{wlp}(Q)(\gamma)) \\ & = & (\mathsf{wlp}(P) \circ \mathsf{wlp}(Q))(\gamma) \end{array}$$

For nondeterministic choice $P [] Q$ we have using Lemma 4.1 that

$$\begin{array}{rcl} \mathsf{wlp}(P [] Q)(\gamma) & = & 1 - \mathsf{wp}(P [] Q)(1-\gamma) \\ & = & 1 - (\mathsf{wp}(P)(1-\gamma) \vee \mathsf{wp}(Q)(1-\gamma)) \\ & = & (1 - \mathsf{wp}(P)(1-\gamma)) \wedge (1 - \mathsf{wp}(Q)(1-\gamma)) \\ & = & \mathsf{wlp}(P)(\gamma) \wedge \mathsf{wlp}(Q)(\gamma) \end{array}$$

Finally we consider while-loops $\mathbf{while}(b,P)$. For $\gamma \in \mathbb{I}^S$ let $F_\gamma : \mathbb{I}^S \to \mathbb{I}^S$ be defined as

$$F_\gamma(\beta) = (b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge (1-\gamma))$$

for $\beta \in \mathbb{I}^S$. Since F_γ is Scott-continuous the function $G_\gamma : \mathbb{I}^S \to \mathbb{I}^S$ defined as

$$G_\gamma(\beta) = 1 - F_\gamma(1-\beta)$$

preserves infima of down-directed families. Moreover, one easily checks that

$$G^n_\gamma(\beta) = 1 - F^n_\gamma(1-\beta)$$

for all $n \in \omega$ and $\beta \in \mathbb{I}^S$. Using Lemma 4.1 we calculate as follows

$$\begin{array}{lcl}
\mathsf{wlp}(\mathbf{while}(b,P))(\gamma) & = & 1 - \mathsf{wp}(\mathbf{while}(b,P))(1-\gamma) \\
& = & 1 - \mathsf{Minfix}\ \beta.\ (b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge (1-\gamma)) \\
& = & 1 - \sup_{n\in\omega} F^n_\gamma(0) \\
& = & \inf_{n\in\omega} 1 - F^n_\gamma(0) \\
& = & \inf_{n\in\omega} 1 - F^n_\gamma(1-1) \\
& = & \inf_{n\in\omega} G^n_\gamma(1) \\
& \overset{(*)}{=} & \mathsf{Maxfix}\ \beta.\ G_\gamma(\beta) \\
& \overset{(**)}{=} & \mathsf{Maxfix}\ \beta.\ (b \wedge \mathsf{wlp}(P)(\beta)) \vee (\neg b \wedge \gamma)
\end{array}$$

where $(*)$ follows from the fact that G_γ preserves infima of down-directed families and $(**)$ follows from the following calculation

$$\begin{array}{lcl}
G_\gamma(\beta) & = & 1 - F_\gamma(1-\beta) \\
& = & 1 - (b \wedge \mathsf{wp}(P)(1-\beta)) \vee (\neg b \wedge (1-\gamma))) \\
& \overset{(\dagger)}{=} & (b \wedge (1 - \mathsf{wp}(P)(1-\beta))) \vee (\neg b \wedge (1-(1-\gamma))) \\
& = & (b \wedge \mathsf{wlp}(P(\beta)) \vee (\neg b \wedge \gamma)
\end{array}$$

where $(\dagger)$ follows by case analysis on $b(s)$. □

We conclude this section by observing that the clause for $\mathsf{wlp}(\mathbf{while}(b,P))$ suggests a principle of *reasoning about while loops via invariants*. First recall (from the Knaster-Tarski fixpoint theorem) that for a monotonic $T : \mathbb{I}^S \to \mathbb{I}^S$ its greatest fixpoint $\mathsf{Maxfix}\ \beta.\ T(\beta)$ is the supremum of all postfixpoints $\beta \leq T(\beta)$. Instantiating T by $T(\beta) = (b \wedge \mathsf{wlp}(P)(\beta)) \vee (\neg b \wedge \gamma)$ (for some $\gamma \in \mathbb{I}^S$) and noting that $\mathsf{wlp}(\mathbf{while}(b,P))(\gamma) = \mathsf{Maxfix}\ \beta.\ T(\beta)$ it is a sufficient condition for $\beta \leq \mathsf{wlp}(\mathbf{while}(b,P))(\gamma)$ that $\beta \leq T(\beta) = (b \wedge \mathsf{wlp}(P)(\beta)) \vee (\neg b \wedge \gamma)$, i.e. that

(1) $\beta(s) \leq \mathsf{wlp}(P)(\beta)(s)$ whenver $b(s)$ and

(2) $\beta(s) \leq \gamma(s)$ whenever $\neg b(s)$.

Notice that for $\mathsf{wp}(\mathbf{while}(b,P))$ such a reasoning principle by invariants is not available. Recall form [KRS] that $\mathsf{wp}(\mathbf{while}(b,P))(\gamma) = \mathsf{Minfix}\ \beta.\ T(\beta)$ where $T(\beta) = (b \wedge \mathsf{wp}(P)(\beta)) \vee (\neg b \wedge \gamma)$ where MinFix stands for least fixpoint. Since by Tarski's fixpoint theorem $\mathsf{Minfix}\ \beta.\ T(\beta)$ is the infimum of all prefix points $T(\beta) \leq \beta$ of T we have $\mathsf{wp}(\mathbf{while}(b,P))(\gamma) \leq \beta$ iff $T(\beta) \leq \beta$, i.e. iff

(1) $\mathsf{wlp}(P)(\beta)(s) \leq \beta(s)$ whenver $b(s)$ and

(2) $\gamma(s) \leq \beta(s)$ whenever $\neg b(s)$.

But, alas, this does not allow us to prove $\beta \leq \mathsf{wp}(\mathbf{while}(b,P))$ as we would like when trying to show that precondition β ensures that postcondition γ holds after executing $\mathbf{while}(b,P)$.

Thus, unlike the wp semantics of [KRS] the wlp semantics of the current paper does support a reasoning principle by invariants for while-loops.

5 Conclusion and Possible Future Work

In [KRS] we have developed a direct total correctness semantics for $\mathcal{L}_p$ and in this paper we have preformed the same task for partial correctness. In both cases it was crucial to characterise the powerdomain of $\mathcal{V}(S)$ in terms of certain "good" Scott-continuous functionals from $\mathbb{I}^S$ to $\mathbb{I}$, a kind of correspondence we have baptized "Minkowsky duality" since this characterisation is inspired by [Min]. Though Minkowsky duality for the partial correctness case is slightly simpler than for the total correctness case it was crucial in both cases to appeal to (an appropriate form of) the Hahn-Banach Theorem for topological vector spaces. In Lemma 9 of [KRS] and Lemma 3.6 of the current paper we have established the equivalence of our formulation of the direct semantics to the one considered in [MMb] where a more intuitive, but technically less convenient construction of lifting is used.

The wp-semantics for the partial correctness case (see Lemma 4.1) is "angelic" in the sense that for nondeterministic choice we have

$$\mathsf{wp}(P_1 [] P_2)(\gamma) = \mathsf{wp}(P_1)(\gamma) \vee \mathsf{wp}(P_2)(\gamma)$$

whereas the wp-semantics for the total correctness case is "demonic" in the sense that for nondeterministic choice we have

$$\mathsf{wp}(P_1 [] P_2)(\gamma) = \mathsf{wp}(P_1)(\gamma) \wedge \mathsf{wp}(P_2)(\gamma)$$

The wlp-semantics for the partial correcntess case is "demonic" in the sense that for nondeterministic choice we have

$$\mathsf{wlp}(P_1 [] P_2)(\gamma) = \mathsf{wlp}(P_1)(\gamma) \wedge \mathsf{wlp}(P_2)(\gamma)$$

What's missing is the wlp-semantics for the total correctness case. But also in the total correctness case we can again define $\mathsf{wlp}(P)(\gamma) = 1 - \mathsf{wp}(P)(1-\gamma)$ and with arguments like in the proof of Theorem 4.2 of the current paper we can prove a characterisation of wlp for the total correctness case which differs from the one for the partial correctness case only in the clause for nondeterministic choice, namely

$$\mathsf{wlp}(P_1 [] P_2)(\gamma) = \mathsf{wlp}(P_1)(\gamma) \vee \mathsf{wlp}(P_2)(\gamma)$$

which now takes an "angelic" form.

But notice that both for total and partial correctness weakest preconditions for while-loops are computed as least fixpoints whereas weakest liberal preconditions for while-loops are computed as greatest fixpoints and only the latter support a principle of reasoning by loop invariants.

In future work we want to investigate to which extent it holds that

$$\mathsf{wp}(P)(\gamma) = \mathsf{wlp}(P)(\gamma) \wedge \mathsf{wp}(P)(1)$$

i.e. that "wp = wlp + termination".

Moreover, it seems to be worthwhile to study an *operational* semantics for $\mathcal{L}_p$ and to relate it to the denotational semantics studied in [KRS] and the current paper by proving that they stand in the relation of computational adequacy (as explained e.g. in [Str]).

A Appendix

Although for semantics the case of a countable set of states is the most relevant one, the following developments hold for any set S considered as a discrete set without any topology or order.

We consider the linear subspace ℓ^∞ of the vector space $\mathbb{R}^S$ consisting of all bounded functions $\gamma\colon S \to \mathbb{R}$. We equip this linear subspace with the topology of pointwise convergence, that is, the topology induced by the product topology on $\mathbb{R}^S$ as in the preliminary section 2, and with the pointwise defined order $\beta \leq \gamma$ iff $\beta(s) \leq \gamma(s)$ for all $s \in S$. The positive cone, i.e. the set of all nonnegative functions $\gamma \in \ell^\infty$, is denoted by ℓ^∞_+.

As before, we use the notation $\mathbf{1}$ for the constant function with value 1. Then $\mathbb{I}^S = \{\gamma \in \ell^\infty_+ \mid \gamma \leq \mathbf{1}\}$ is a compact convex lower subset of ℓ^∞_+.

In ℓ^∞ we consider the linear subspace ℓ^1 of all functions $\mu\colon S \to \mathbb{R}$ such that $\sum_{s\in S} |\mu(s)| < +\infty$. The positive cone, i.e. the set of all nonnegative functions $\gamma \in \ell^1$, is denoted by ℓ^1_+. It contains the set $\mathcal{V}(S)$ of subprobability distributions on S as a compact convex lower subset.

The following lemma is the order dual of [KRS, Lemma A.1]:

Lemma A.1. *If $A \subseteq \mathbb{I}^S$ is convex (resp. compact) then its lower saturation $\downarrow A = \{\gamma \in \ell^\infty \mid \gamma \leq \alpha$ for some $\alpha \in A\}$ is also convex (resp. compact).*

Recall that a function f from a topological space X into $\mathbb{R}$ (or into a subset of $\mathbb{R}$) is *lower semicontinuous* if the set of all $x \in X$ such that $f(x) > r$ is open in X for every $r \in \mathbb{R}$. Next we note (see [KRS, Lemma A.2]) that, in our setting, lower semicontinuity is equivalent to Scott continuity, a fact that will be used subsequently without further mention.

Lemma A.2. *A function f from ℓ^∞_+ $\big(\ell^1_+,\ \mathbb{I}^S,\ \mathcal{V}(S)$, respectively$\big)$ to $\mathbb{R}_+$ is Scott-continuous if and only if it is order preserving and lower semicontinuous.*

Let V_+ be any of the positive cones ℓ^∞_+, ℓ^1_+. A function $f\colon V_+ \to \mathbb{R}_+$ is called

homogeneous if $f(r\gamma) = rf(\gamma)$ for all $r \in \mathbb{R}_+$

subadditive if it satisfies $f(\gamma + \beta) \leq f(\gamma) + f(\beta)$

sublinear if it is homogeneous and subadditive

linear if its is homogeneous and additive: $f(\gamma + \beta) = f(\gamma) + f(\beta)$.

In V_+, consider the closed convex lower subset $K = \mathbb{I}^S, \mathcal{V}(S)$, respectively. We want to apply the above terminology to functions $g\colon K \to \mathbb{I}$. As addition and scalar multiplication lead out of K, we have to modify the definition in the following way: A function $g\colon K \to \mathbb{I}$ is called

homogeneous if $g(r\gamma) = rg(\gamma)$ for all $r \in \mathbb{I}$

subadditive if $g(\gamma + \beta) \leq g(\gamma) + g(\beta)$ whenever $\gamma + \beta \in K$

sublinear if it is homogeneous and subadditive

linear if it is homogeneous and *additive*: $g(\gamma+\beta)=g(\gamma)+g(\beta)$ whenever $\gamma+\beta\in K$.

Each homogeneous functional $g\colon K\to\mathbb{I}$ has a unique extension to a homogeneous functional $\widehat{g}\colon V_+\to\mathbb{R}_+$: for $\beta\in V_+$ there is a $\gamma\in K$ such that $\beta=r\gamma$ for some $r\in\mathbb{R}_+$, and if we set $\widehat{g}(\beta)=rg(\gamma)$ this value is independent of the choice of γ in K because of homogeneity.

The extension $\widehat{g}\colon V_+\to\mathbb{R}_+$ of a homogeneous functional $g\colon K\to\mathbb{I}$ is sublinear, linear, and Scott-continuous, respectively, if g is.

Although being defined as a subspace of ℓ_+^∞, the cone ℓ_+^1 should rather be considered as the dual of ℓ_+^∞ and vice versa as described in subsequent Lemma A.3 which is proved in [KRS]. For $\mu\in\ell_+^1$ and $\gamma\in\ell_+^\infty$ we use the notation

$$\langle\mu,\gamma\rangle=\sum_s\mu(s)\gamma(s)$$

Note that the infinite sum converges since $0\le\mu(s)\gamma(s)\le\mu(s)\cdot M$, where M is an upper bound of γ, and since $\sum_s\mu(s)$ converges by definition.

Lemma A.3.

(a) *The mapping* $(\mu,\gamma)\mapsto\langle\mu,\gamma\rangle\colon\ell_+^1\times\ell_+^\infty\to\mathbb{R}_+$ *is bilinear and Scott-continuous.*

(b) *For every Scott-continuous linear functional* $f\colon\ell_+^\infty\to\mathbb{R}_+$ *there is a (unique)* $\mu\in\ell^1$ *such that* $f(\gamma)=\langle\mu,\gamma\rangle$*, and for every Scott-continuous linear functional* $g\colon\ell_+^1\to\mathbb{R}_+$ *there is a (unique)* $\gamma\in\ell_+^\infty$ *such that* $g(\mu)=\langle\mu,\gamma\rangle$*.*

¿From Lemma A.3 we deduce a duality between $\mathbb{I}^S$ and $\mathcal{V}(S)$ as follows.

Corollary A.1.

(a) *The function* $(\mu,\gamma)\mapsto\langle\mu,\gamma\rangle\colon\mathcal{V}(S)\times\mathbb{I}^S\to\mathbb{I}$ *is bilinear and Scott-continuous.*

(b) *For every Scott-continuous linear functional* $f\colon\mathbb{I}^S\to\mathbb{I}$*, there is a (unique)* $\mu\in\mathcal{V}(S)$ *such that* $f(\gamma)=\langle\mu,\gamma\rangle$ *for all* $\gamma\in\mathbb{I}^S$ *and for every Scott-continuous linear functional* $g\colon\mathcal{V}(S)\to\mathbb{I}$ *there is a (unique)* $\gamma\in\mathbb{I}^S$ *such that* $g(\mu)=\langle\mu,\gamma\rangle$ *for all* $\mu\in\mathcal{V}(S)$*.*

Note. Every Scott-continuous linear functional $f\colon\mathbb{I}^S\to\mathbb{I}$ is not only lower semicontinuous by Lemma A.2, but also upper semicontinuous and hence continuous. In contrast most Scott-continuous linear functionals on $\mathcal{V}(S)$ are not upper semicontinuous (see [KRS]).

We now consider the powerdomain $\mathcal{P}_L\mathcal{V}(S)$ of all nonempty, closed, convex, lower subsets of $\mathcal{V}(S)$. We want to establish a Minkowski type correspondence between the sets $A\in\mathcal{P}_L\mathcal{V}(S)$ and certain functionals $G\colon\mathbb{I}^S\to\mathbb{I}$ similar to the dual argument in [KRS].

To every $A\in\mathcal{P}_L\mathcal{V}(S)$ we associate the functional $\Phi_A\colon\mathbb{I}^S\to\mathbb{I}$ defined by

$$\Phi_A(\gamma)=\sup_{\mu\in A}\langle\mu,\gamma\rangle$$

Being the (pointwise) supremum of continuous linear functionals, Φ_A is sublinear and lower semicontinuous. As linear functionals are order preserving, Φ_A is order preserving, too. Thus Φ_A is Scott-continuous.

Conversely, for a Scott-continuous sublinear functional $G\colon \mathbb{I}^S \to \mathbb{I}$ let

$$\Psi_G = \{\mu \in \mathcal{V}(S) \mid \langle \mu, \gamma\rangle \leq G(\gamma) \text{ for all } \gamma \in \mathbb{I}^S\}$$

Lemma A.4. *Ψ_G is a closed, convex, lower subset of $\mathcal{V}(S)$.*

Proof: Clearly, Ψ_G is a lower set. As G is sublinear, Ψ_G is convex. In order to show that Ψ_G is closed, by Lemma 2.1 it suffices to show the following: If μ has the property that $\sigma \in \Psi_G$ for every $\sigma \ll \mu$, then $\mu \in \Psi_G$. So suppose that $\sigma \in \Psi_G$ for every $\sigma \ll \mu$. For every $\gamma \in \mathbb{I}^S$ we then have $\langle \sigma, \gamma\rangle \leq G(\gamma)$. As μ is the directed supremum of the $\sigma \ll \mu$, Lemma A.3(1) implies that $\langle \mu, \gamma\rangle = \langle \sup_{\sigma\ll\mu} \sigma, \gamma\rangle = \sup_{\sigma\ll\mu}\langle \sigma, \gamma\rangle \leq G(\gamma)$. □

We are now ready for our main result of this Appendix. In its proof we will use the following standard Hahn-Banach separation theorems (a convenient reference is e.g. [DS, Theorem V.2.8 ff.]): If A is a closed convex subset of a locally convex topological vector space V then for every $b \in V \setminus A$ there is a continuous linear functional $f\colon V \to \mathbb{R}$ and a real number s such that $f(a) \leq s < f(b)$ for all $a \in A$.

Proposition A.1. *$A \mapsto \Phi_A$ and $G \mapsto \Psi_G$ are mutually inverse order isomorphisms between the collection $\mathcal{P}_L\mathcal{V}(S)$ of all nonempty closed convex lower subsets of $\mathcal{V}(S)$ and the set $\mathcal{G}(S)$ of all Scott-continuous sublinear functionals $G\colon \mathbb{I}^S \to \mathbb{I}$.*

Proof: We first prove that $A = \Psi(\Phi_A)$ for every $A \in \mathcal{P}_L\mathcal{V}(S)$. Clearly, $A \subseteq \Psi(\Phi_A)$. For the converse inclusion suppose that $\nu \notin A$. The lower set $\downarrow A$ generated by A in ℓ^1 is closed and convex by Lemma A.1, as every closed subset of $\mathcal{V}(S)$ is compact. By the above mentioned Hahn-Banach separation theorem, there is a continuous linear functional f on ℓ^1 such that $f(\nu) > f(\mu)$ for all $\mu \in \downarrow A$.

We now show that f maps ℓ^1_+ to $\mathbb{R}_+$ or, equivalently, that f maps $-\ell^1_+$ to $-\mathbb{R}_+$. We choose a fixed $\mu \in -\ell^1_+$. Then $r\mu \in -\ell^1_+$, whence $r\mu \in \downarrow A$ for every $r > 0$. Thus $rf(\mu) = f(r\mu) < f(\nu)$ for every $r > 0$, whence $f(\mu) \leq 0$.

As every continuous linear functional on ℓ^1_+ is order preserving and lower semicontinuous, hence Scott-continuous, Lemma A.3 tells us that there is a $\gamma \in \ell^\infty_+$ such that $f(\mu) = \langle \mu, \gamma\rangle$ for all $\mu \in \ell^1_+$. Replacing γ by $\frac{1}{m}\gamma$ (for a sufficiently big $m \in \mathbb{N}$) we may suppose that $\gamma \in \mathbb{I}^S$ and we have $\langle \nu, \gamma\rangle > \langle \mu, \gamma\rangle$ for all $\mu \in A$ and thus $\nu \notin \Psi(\Phi_A)$ as desired.

Now suppose $G\colon \mathbb{I}^S \to \mathbb{I}$ is a Scott-continuous sublinear functional. We will show that $G = \Phi(\Psi_G)$, i.e. $G(\gamma) = \sup_{\mu\in\Psi_G}\langle \mu, \gamma\rangle = \sup\{\langle \mu, \gamma\rangle \mid \mu \in \mathcal{V}(S), \langle \mu, \gamma\rangle \leq G(\gamma) \text{ for all } \gamma \in \mathbb{I}^S\}$ for all $\gamma \in \mathbb{I}^S$. As by Corollary A.1 the elements $\mu \in \mathcal{V}(S)$ are in a one-to-one correspondence with the Scott-continuous linear functionals $f\colon \mathbb{I}^S \to \mathbb{I}$, we have to show that, for all $\gamma \in \mathbb{I}^S$

$$G(\gamma) = \sup\{f(\gamma) \mid f\colon \mathbb{I}^S \to \mathbb{I} \text{ linear, Scott-continuous, and } G \geq f \text{ on } \mathbb{I}^S\}$$

For the proof we fix a $\gamma \in \mathbb{I}^S$. We will show that for every $r < G(\gamma)$, there is a Scott-continuous linear functional $f\colon \mathbb{I}^S \to \mathbb{I}$ such that $G \geq f$ on $\mathbb{I}^S$ and $f(\gamma) \geq r$. If $G(\gamma) = 0$, we may choose for f the zero functional. Thus, we may suppose $G(\gamma) > r > 0$.

We consider the unique homogeneous extension $\widehat{G}\colon \ell^\infty_+ \to \mathbb{R}_+$ of G. The extended functional $\widehat{G}$ is Scott-continuous and sublinear. We search for a continuous linear functional $f\colon \ell^\infty_+ \to \mathbb{R}_+$ such that $\widehat{G} \geq f$ and $f(\gamma) \geq r$.

We form the set $A = \{\beta \in \ell^\infty_+ \mid \widehat{G}(\beta) \leq r\}$. As $\widehat{G}$ is Scott-continuous and sublinear, A is a closed convex lower set in ℓ^∞_+ with $\gamma \notin A$. By A.1, the lower saturation $\downarrow A$ of A in ℓ^∞ is also closed and convex. In ℓ^∞ we may apply the Hahn-Banach separation theorem cited above and obtain a continuous linear functional f on ℓ^∞ such that $\sup f(A) < f(\gamma)$. As in the first part of this proof one shows that $f(\beta) \geq 0$ for every $\beta \geq 0$. After multiplying f with an appropriate scalar, we may suppose that $\sup f(A) = r$. Then $G(\beta) \leq r$ implies $f(\beta) \leq r$. By the homogeneity of G and f we conclude that $f \leq G$ on $\mathbb{I}^S$ and $f(\gamma) > r$ as desired. □

References

[BHM] N. Benton, J. Hughes, E. Moggi *Monads and Effects* pp.42-122 in *Applied Semantics* Lecture Notes in Computer Science **2395**, Springer Verlag (2002).

[DS] N. Dunford, J. T. Schwartz *Linear Operators, Part I: General Theory.* Interscience Publ., New York (1967).

[GHK+] G. Gierz, K. H. Hofmann, J. D. Lawson, M. W. Mislove, D. S. Scott *Continuous Lattices and Domains.* Cambridge University Press (2003).

[Hec] R. Heckmann, *Power domains and second-order predicates.* Theoretical Computer Science, **111**, 59–88, 1993.

[KP] K. Keimel, G. Plotkin *Predicate Transformers for Convex Powerdomains.* Mathematical Structures in Computer Science (to appear).

[KRS] K. Keimel, A. Rosenbusch, T. Streicher *Relating Direct and Predicate Transformer Semantics for an Imperative Probabilistic-Nondeterministic Language.* accepted for APAL (2008).

[MMa] A. McIver, C. Morgan *Partial correctness for probabilistic demonic programs.* Theoretical Computer Science 266, 513–541 (2001).

[MMb] A. McIver, C. Morgan *Abstraction, refinement and proof for probabilistic systems.* Monographs in Computer Science, Springer (2005).

[Min] H. Minkowski *Volumen und Oberfläche.* Mathematische Annalen **57**, 447–495 (1903).

[TKP] R. Tix, K. Keimel, G. Plotkin *Semantic domains for combining probability and nondeterminism.* Electronic Notes in Theoretical Computer Science **129**, Elsevier (2005).

[Plo] G. Plotkin *Domain Theory.* Lecture Notes available from the author's homepage.

[Smy] M. B. Smyth Power domains and predicate transformers: a topological view, *Proc. 10th ICALP* (ed. J. Díaz), Lecture Notes in Computer Science, **154**, 662–675, Springer-Verlag (1983).

[Str] T. Streicher *Domain-theoretic Foundations of Functional Programming.* World Scientific (2006).