

# Deriving Predicate Transformer Semantics for pGCL from its Direct Semantics

(K. Keimel, A. Rosenbusch, T. Streicher)

In [McM] McIver and Morgan have introduced pGCL, an imperative programming language with guarded command incorporating both *erratic* and *probabilistic* nondeterminism. For verifying pGCL programs they associate with every pGCL program  $P$  a predicate transformer  $\text{wp}(P) : \mathcal{E}(S) \rightarrow \mathcal{E}(S)$  where  $S$  is a countable set of states and  $\mathcal{E}(S) = [0, 1]^S$  ordered pointwise. We show how to derive McIver and Morgan's *predicate transformer semantics* from a more intuitive *direct semantics* associating with every program  $P$  a function  $\llbracket P \rrbracket : S \rightarrow \mathcal{P}_U(\mathcal{V}(S))$  where  $\mathcal{P}_U$  is the upper (or Smyth) powerdomain and  $\mathcal{V}(S)$  the probabilistic powerdomain of  $S_\perp$  which for convenience can be identified with the set of function  $\mu : S \rightarrow [0, 1]$  with  $\sum_{s \in S} \mu(s) \leq 1$  (of course, for  $A \subseteq S$  we define  $\mu(A)$  as  $\sum_{s \in A} \mu(s)$ ).

Following a suggestion in [TKP] we define for  $f : S \rightarrow \mathcal{P}_U(\mathcal{V}(S))$  its associated predicate transformer  $\text{wp}(f) : \mathcal{E}(S) \rightarrow \mathcal{E}(S)$  as

$$\text{wp}(f)(B)(s) = \inf_{\mu \in f(s)} \sum_{t \in S} B(t) \cdot \mu(t)$$

We show that the function  $\text{wp} : \text{pGCL} \rightarrow [\mathcal{E}(S) \rightarrow \mathcal{E}(S)]$  defined as  $\text{wp}(P) = \text{wp}(\llbracket P \rrbracket)$  satisfies the equations used for defining  $\text{wp}$  in [McM].

We also discuss the *partial correctness* case where with every  $f : S \rightarrow \mathcal{P}_U(\mathcal{V}(S))$  and  $B \subseteq S$  we associate its *weakest liberal precondition*

$$\text{wlpr}(f)(B)(s) = \inf_{\mu \in f(s)} \mu(\perp) + \sum_{t \in S} B(t) \cdot \mu(t) = \inf_{\mu \in f(s)} 1 + \sum_{s \in S} (1 - B(t)) \cdot \mu(t)$$

where  $\mu(\perp) = 1 - \sum_{s \in S} \mu(s)$ . We show that the function  $\text{wlpr} : \text{pGCL} \rightarrow [\mathcal{E}(S) \rightarrow \mathcal{E}(S)]$  defined as  $\text{wlpr}P = \text{wlpr}(\llbracket P \rrbracket)$  satisfies the defining equations given in [McM]. Since  $\text{wlpr} : [S \rightarrow \mathcal{P}(\mathcal{V}(S))] \rightarrow \mathcal{E}(S) \rightarrow \mathcal{E}(S)$  is antitonic in its first argument the weakest liberal precondition for loops is computed by – somewhat suprisingly – taking greatest fixpoints.

## References

- [McM] A. McIver, C. Morgan *Abstraction, Refinement and Proof for Probabilistic Systems* Monograph in Computer Science, Springer Verlag (2005).
- [TKP] R. Tix, K. Keimel and G. Plotkin *Semantic Domains for Combining Probability and Non-Determinism* ENTCS 129 (2005).