

# New Insights into pGCL Semantics

Daniel STAN

Supervised by Friedrich Gretz

June 15, 2016

- 1 pGCL
  - Definiton
  - Probabilities and non-determinism
  - Weakest expectation
    - $W_p$  definition
    - Example by annotations
- 2 Consistence of WP definition
  - Loop definition
  - C.P.O
  - Proof
  - Iterative definition
- 3 Pre-expectation as a resulting expectation
  - MDP point of view
  - Functional point of view

# Index

- 1 pGCL
  - Definiton
  - Probabilities and non-determinism
  - Weakest expectation
- 2 Consistence of WP definition
- 3 Pre-expectation as a resulting expectation

# The probabilistic guarded command language [?]

Extension of GCL, with probabilistic and non-deterministic constructions.

$$P ::= \text{abort} \mid \text{skip} \mid x := \text{expr} \mid P; P \mid \text{if}(G)\{P\}\text{else}\{P\} \mid \\ \text{while}(G)\{P\} \mid P \square P \mid P[p]P$$

# The probabilistic guarded command language [?]

Extension of GCL, with probabilistic and non-deterministic constructions.

$$P ::= \text{abort} \mid \text{skip} \mid x := \text{expr} \mid P; P \mid \text{if}(G)\{P\}\text{else}\{P\} \mid \\ \text{while}(G)\{P\} \mid P \square P \mid P[p]P$$

# Probabilities and non-determinism

Possible non-deterministic strategies :

- Angelic
- Demonic
- Mixed

According to which goal ?

# Weakest pre-condition

In the deterministic non-probabilistic case, we have the weakest pre-condition of a formula  $\phi$ :

$$\text{wp}(P, \phi) = \{\eta \mid \exists \eta'. \eta \xrightarrow{P} \eta' \wedge \eta' \models \phi\}$$

*Qualitative* notion.

# Weakest pre-expectation

## Definition: Expectation

$$f : S \rightarrow \mathbb{R}_{\geq 0}$$

Where  $S = \{\eta : \text{Var} \rightarrow \mathbb{R}\}$  are the possible variable valuations (state).

- Worth of the state  $\eta$ :  $f(\eta)$
- Quantitative notion.
- For any boolean formula  $\phi$ ,  $[\phi] : S \rightarrow \{0, 1\}$
- Usually, expectations are still computed as expressions (PRINSYS)



# Weakest pre-expectation Definition

Deterministic definitions:

$$\text{wp}(\text{skip}, f) = f$$

$$\text{wp}(\text{abort}, f) = 0$$

$$\forall \eta. \text{wp}(x := \text{expr}, f)(\eta) = f(\eta[x \mapsto \text{expr}(\eta)])$$

$$\text{wp}(P_1; P_2, f) = \text{wp}(P_1, \text{wp}(P_2, f))$$

$$\text{wp}(\text{if}(G)\{P_1\}\text{else}\{P_2\}, f) = [G]\text{wp}(P_1, f) + [\neg G]\text{wp}(P_2, f)$$

Consistent with weakest pre-condition.

# Weakest pre-expectation Definition

Deterministic definitions:

$$\text{wp}(\text{skip}, f) = f$$

$$\text{wp}(\text{abort}, f) = 0$$

$$\forall \eta. \text{wp}(x := \text{expr}, f)(\eta) = f(\eta[x \mapsto \text{expr}(\eta)])$$

$$\text{wp}(P_1; P_2, f) = \text{wp}(P_1, \text{wp}(P_2, f))$$

$$\text{wp}(\text{if}(G)\{P_1\}\text{else}\{P_2\}, f) = [G]\text{wp}(P_1, f) + [\neg G]\text{wp}(P_2, f)$$

Consistent with weakest pre-condition.

$$\text{wp}(P_1 \square P_2, f) = \min(\text{wp}(P_1, f), \text{wp}(P_2, f))$$

$$\text{wp}(P_1[p]P_2, f) = p \cdot \text{wp}(P_1, f) + (1 - p) \text{wp}(P_2, f)$$

# Example: annotating backward

$d:=0 \sqcap d:=1$

$c:=0 [p] c:=1$

# Example: annotating backward

$d:=0 \sqcap d:=1$

$c:=0 [p] c:=1$   
 $[d = c]$

# Example: annotating backward

$d:=0 \sqcap d:=1$

$p[d = 0] + (1 - p)[d = 1]$

$c:=0 [p] c:=1$

$[d = c]$

# Example: annotating backward

$$\min(p[0 = 0] + (1 - p)[0 = 1], p[1 = 0] + (1 - p)[1 = 1]) = \min(p, 1 - p)$$

$d := 0 \sqcap d := 1$

$p[d = 0] + (1 - p)[d = 1]$

$c := 0 [p] c := 1$

$[d = c]$

$c:=0[p]c:=1$

$d:=0 \sqcap d:=1$

$$c:=0[p]c:=1$$
$$d:=0 \sqcap d:=1$$
$$[d = c]$$



$c := 0 [p] c := 1$   
 $\min([c = 0], [c = 1])$   
 $d := 0 \sqcap d := 1$   
 $[d = c]$

$$p \cdot \min([0 = 0], [0 = 1]) + (1 - p) \min([1 = 0], [0 = 1]) = p \cdot 0 + (1 - p) \cdot 0$$

$c := 0 [p] c := 1$

$\min([c = 0], [c = 1])$

$d := 0 \sqcap d := 1$

$[d = c]$

# Index

1 pGCL

2 Consistence of WP definition

- Loop definition
- C.P.O
- Proof
- Iterative definition

3 Pre-expectation as a resulting expectation

# Loop definition

Intuition: assume  $\text{wp}(\text{while}(G)\{P\}, f)$  defined

Then (unfolding once):

$$\begin{aligned}\text{wp}(\text{while}(G)\{P\}, f) &= \text{wp}(\text{if}(G)\{P; \text{while}(G)\{P\}\}\text{else}\{\text{skip}\}, f) \\ &= [G]\text{wp}(P, \text{wp}(\text{while}(G)\{P\}, f)) + [\neg G]f\end{aligned}$$

# Loop definition

Intuition: assume  $\text{wp}(\text{while}(G)\{P\}, f)$  defined

Then (unfolding once):

$$\begin{aligned}\text{wp}(\text{while}(G)\{P\}, f) &= \text{wp}(\text{if}(G)\{P; \text{while}(G)\{P\}\}\text{else}\{\text{skip}\}, f) \\ &= [G]\text{wp}(P, \text{wp}(\text{while}(G)\{P\}, f)) + [\neg G]f\end{aligned}$$

$$X = [G]\text{wp}(P, X) + [\neg G]f$$

Fix-point existence ? Unicity ?

# Directed Complete partial order

## Definition: Directed Set

$D \neq \emptyset$  directed if:

$$\forall x, y \in D \Rightarrow \exists z \in D. \begin{cases} z \geq x \\ z \geq y \end{cases}$$

## Definition: Complete Partial Order

$E$  cpo if:

$\forall D \subseteq E, D$  directed  $\Rightarrow \sup D \in E$  exists

# Directed Complete partial order

## Definition: Directed Set

$D \neq \emptyset$  directed if:

$$\forall x, y \in D \Rightarrow \exists z \in D. \begin{cases} z \geq x \\ z \geq y \end{cases}$$

## Definition: Complete Partial Order

$E$  cpo if:

$\forall D \subseteq E, D$  directed  $\Rightarrow \sup D \in E$  exists

In our case:

- $E$ : expectation functions set
- Point-wise order
- $\forall \eta \in S, (\sup_{f \in D} f)(\eta) = \sup_{f \in D} (f(\eta))$

# Scott-continuity

## Definition: Scott-Continuous Function

For  $P$  and  $Q$  two cpo, and  $F : P \rightarrow Q$ .  $F$  is said to be Scott-continuous if

- If  $D$  is directed,  $F(D)$  is directed
- and  $F(\sup D) = \sup F(D)$

## Theorem: Kleene fix-point theorem (1938)

Let  $F : P \rightarrow P$  a Scott-continuous function and assume that  $P$  has a smallest element  $0$ .

Then  $F$  has a unique, least fixed point, which is  $\sup_{n \geq 0} F^n(0)$



# Scott-continuity

## Definition: Scott-Continuous Function

For  $P$  and  $Q$  two cpo, and  $F : P \rightarrow Q$ .  $F$  is said to be Scott-continuous if

- If  $D$  is directed,  $F(D)$  is directed
- and  $F(\sup D) = \sup F(D)$

## Theorem: Kleene fix-point theorem (1938)

Let  $F : P \rightarrow P$  a Scott-continuous function and assume that  $P$  has a smallest element  $0$ .

Then  $F$  has a unique, least fixed point, which is  $\sup_{n \geq 0} F^n(0)$

Here:  $0$  is the constant expectation function equals to  $0$ .

# Consistence of wp

## Theorem: wp Soundness

*For any program  $P$ ,  $\text{wp}(P, \cdot)$  is Scott-continuous.*

So  $\text{wp}(\text{while}(G)\{P\}, f)$  is well defined.

# Sketch of the proof (1/2)

Structural induction on  $P$ .

Probabilistic case:

- Apply definition and induction hypothesis:

$$\sup_{f \in D} (\rho \cdot \text{wp}(P_1, f) + \sup_{f \in D} ((1 - \rho) \text{wp}(P_2, f))) \stackrel{?}{=} \sup_{f \in D} ((\rho \cdot \text{wp}(P_1, f) + (1 - \rho) \cdot \sup_{f \in D} \text{wp}(P_2, f)))$$

- " $\geq$ " is obvious.
- Assume (point-wise) inequality " $\leq$ " is not satisfied for some state  $\eta$ , that is to say " $>$ " holds.

# Sketch of the proof (2/2)

- Find some  $(g_1, g_2) \in D^2$  such that

$$\begin{aligned} & p \cdot \text{wp}(P_1, g_1)(\eta) + (1 - p) \text{wp}(P_2, g_2)(\eta) > \\ & \sup_{f \in D} ((p \cdot \text{wp}(P_1, f) + (1 - p) \text{wp}(P_2, f))(\eta)) \end{aligned}$$

- However,  $\exists g \in D. g \geq g_1 \wedge g \geq g_2$
- Apply monotonicity of wp

This case shows the use of cpo structure of the expectation functions set.

# Iterative definition of the loop

$$\text{wp}(\text{while}(G)\{P\}, f) = \lim_{n \rightarrow \infty} \underbrace{\text{if}(G)\{P\} \dots \text{if}(G)\{P\}}_{n \text{ times}}; \text{if}(G)\{\text{abort}\}$$

- *Bounded* loop, with untermination (abort)
- Allows proof by induction and limit arguments

# Index

- 1 pGCL
- 2 Consistence of WP definition
- 3 Pre-expectation as a resulting expectation
  - MDP point of view
  - Functional point of view

# MDP versus WP [?]

For a given pre-expectation  $f$ .

- pGCL program converted into a parametric Markovian Decision Process
- On every final state with valuation  $\eta$ , attach reward  $f(\eta)$

## MDP expected rewards as MDP

$\text{wp}(P, f)(\eta)$  is the minimal expected reward after the MDP's run.

- Non-determinism implies choosing some transitions, ie having a strategy.
- Minimal value = Demonic strategy.

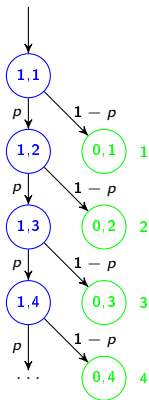
# Example of MDP

```

v := 1
c := 1
while( c != 0 ) {
  v++ [p] c:= 0
}

```

$$\text{wp}(P, v) = \frac{1}{1-p}$$



$$\mathbb{E}(\text{Rew}) = \frac{1}{1-p}$$



# Functionnal point of view

- Idea from MDP characterization:  $\text{wp}$  is a final expectation
- $[\?]$ : programs are measurable functions
- No further assumption on  $f$

# Functional semantics

For  $P$  pGCL program, let  $\tilde{P}$  its functional semantics

$$\tilde{P} : S \longrightarrow S \uplus \{\perp\}$$

Where  $\perp$  is an extra token for non-termination.

For example:

$$\widetilde{P_1; P_2}(\eta) = \begin{cases} \tilde{P}_2(\eta') & \text{If } \eta' \neq \perp \text{ Where we have computed } \eta' = \tilde{P}_1(\eta) \\ \perp & \text{Otherwise} \end{cases}$$

# WP as an expectation

## Theorem: WP as resulting expectation

*For  $P$  without non-deterministic choice,  $f(\tilde{P}(\eta))$  is a discrete random variable and:*

$$\text{wp}(P, f)(\eta) = \mathbb{E}[f(\tilde{P}(\eta))]$$

# Negative expectations ?

```
v := 1
c := 1
while( c != 0 ) {
    v++ [p] c:= 0
}
```

# Negative expectations ?

```

v := 1
c := 1
while( c != 0 ) {
    v++  $\left[\frac{1}{2}\right]$  c := 0
}
v :=  $-\frac{2^v}{v} \left[\frac{1}{2}\right] 2^v \cdot \frac{v+1}{v^2}$ 

```

$$\mathbb{E}(v) = ?$$

# Negative expectations ?

```

v := 1
c := 1
while( c != 0 ) {
    v++  $\left[\frac{1}{2}\right]$  c := 0
}
v :=  $-\frac{2^v}{v} \left[\frac{1}{2}\right] 2^v \cdot \frac{v+1}{v^2}$ 

```

$$\mathbb{E}(v) = ?$$

- Summation order matters.
- Giving a definition of wp for negative expectations  $\Rightarrow$  break the link with expectation characterizations.

# Conclusions (1/2)

- Different semantics for pGCL
- Iterative definition of the loop
- $\text{wp}$  is in fact a pre-expectation

# Conclusions (1/2)

- Different semantics for pGCL
- Iterative definition of the loop
- $\text{wp}$  is in fact a pre-expectation
- Other semantics:
  - Encoding to Probabilistic Process Algebra
  - Unifying Programming Theory (except loop definition)
- Extension to other data types (arrays, recursion)



## Conclusions: Further work (2/2)

- Reducing the MDP state space
- Definition of UTP loop

Thank you

# Bibliography