Transition semantics: intro

Idea: describe the result of executing a **single step** of the Golog program.

- *Given a Golog program δ and a situation s* **compute the situation s' and the program δ' that remains to be executed obtained by executing a single step of δ in s.**

- *Assert when a Golog program δ can be considered* **successfully terminated** *in a situation s.*

Transition semantics: intro

More formally:

- Define the **relation**, named $Trans$ and denoted by "$\longrightarrow$"):

  $$(\delta, s) \longrightarrow (\delta', s')$$

  where δ is a program, s is the situation in which the program is executed, and s' is the situation obtained by executing a single step of δ and δ' is what remains to be executed of δ after such a single step.

- Define a **predicate**. named $Final$ and denoted by "$\surd$":

  $$(\delta, s)^{\surd}$$

  where δ is a program that can be considered (successfully) terminated in the situation s.

Such a relation and predicate can be defined inductively in a standard way, using the so called **transition (structural) rules**

Transition semantics: references

The general approach we follows is is the *structural operational semantics* approach[Plotkin81, Nielson&Nielson99].

This single-step semantics is often call: *transition semantics* or *computation semantics*.

Transition rules for Golog: deterministic constructs

$$Act: \quad \frac{(a,s) \longrightarrow (nil, do(a[s],s))}{true} \quad \text{if } Poss(a[s],s)$$

$$Test: \quad \frac{(\phi?, s) \longrightarrow (nil, s)}{true} \quad \text{if } \phi[s]$$

$$Seq: \quad \frac{(\delta_1;\delta_2,\ s) \longrightarrow (\delta_1';\delta_2, s')}{(\delta_1, s) \longrightarrow (\delta_1'; s')} \qquad \frac{(\delta_1;\delta_2,\ s) \longrightarrow (\delta_2', s')}{(\delta_2, s) \longrightarrow (\delta_2'; s')} \quad \text{if } (\delta_1, s)\surd$$

$$if: \quad \frac{(\textbf{if } \phi \textbf{ then } \delta_1 \textbf{else } \delta_2, s) \longrightarrow (\delta_1', s')}{(\delta_1, s) \longrightarrow (\delta_1', s')} \quad \text{if } \phi[s] \qquad \frac{(\textbf{if } \phi \textbf{ then } \delta_1 \textbf{else } \delta_2, s) \longrightarrow (\delta_2', s')}{(\delta_2, s) \longrightarrow (\delta_2', s')} \quad \text{if } \neg\phi[s]$$

$$while: \quad \frac{(\textbf{while } \phi \textbf{ do } \delta, s) \longrightarrow (\delta'; \textbf{while } \phi \textbf{ do } \delta, s)}{(\delta, s) \longrightarrow (\delta', s')} \quad \text{if } \phi[s]$$

Termination rules for Golog: deterministic constructs

$$Nil: \quad \frac{(nil, s)^{\surd}}{true}$$

$$Seq: \quad \frac{(\delta_1; \delta_2,\ s)^{\surd}}{(\delta_1, s)^{\surd}\ \wedge\ (\delta_2; s)^{\surd}}$$

$$if: \quad \frac{(\textbf{if}\ \phi\ \textbf{then}\ \delta_1 \textbf{else}\ \delta_2, s)^{\surd}}{(\delta_1, s)^{\surd}}\ \text{ if } \phi[s] \qquad \frac{(\textbf{if}\ \phi\ \textbf{then}\ \delta_1 \textbf{else}\ \delta_2, s)^{\surd}}{(\delta_2, s)^{\surd}}\ \text{ if } \neg\phi[s]$$

$$while: \quad \frac{(\textbf{while}\ \phi\ \textbf{do}\ \delta, s)^{\surd}}{true}\ \text{ if } \neg\phi[s] \qquad \frac{(\textbf{while}\ \phi\ \textbf{do}\ \delta, s)^{\surd}}{(\delta, s)^{\surd}}\ \text{ if } \phi[s]$$

Transition rules: nondeterministic constructs

$$Nondetbranch: \quad \frac{(\delta_1 \mid \delta_2,\ s) \longrightarrow (\delta'_1, s')}{(\delta_1, s) \longrightarrow (\delta'_1, s')} \qquad \frac{(\delta_1 \mid \delta_2,\ s) \longrightarrow (\delta'_2, s')}{(\delta_2, s) \longrightarrow (\delta'_2, s')}$$

$$Nondetchoice: \quad \frac{(\pi\, x.\ \delta(x), s) \longrightarrow (\delta'(t), s')}{(\delta(t), s) \longrightarrow (\delta'(t), s')}$$ *(for any t)*

$$Nondetiter: \quad \frac{(\delta^*, s) \longrightarrow (\delta'; \delta^*, s')}{(\delta, s) \longrightarrow (\delta', s')}$$

Termination rules: nondeterministic constructs

$$Nondetbranch: \quad \frac{(\delta_1 \mid \delta_2,\ s)^{\surd}}{(\delta_1, s)^{\surd} \ \vee\ (\delta_2, s)^{\surd}}$$

$$Nondetchoice: \quad \frac{(\pi\, x.\ \delta(x), s)^{\surd}}{(\delta(t), s)^{\surd}} \quad \textit{(for some } t\textit{)}$$

$$Nondetiter: \quad \frac{(\delta^*, s)^{\surd}}{true}$$

Structural rules

The structural rules have the following schema:

$$\frac{\textsc{consequent}}{\textsc{antecedent}} \quad \text{if } \textsc{side-condition}$$

which is to be interpreted logically as:

$$\forall(\textsc{antecedent} \wedge \textsc{side-condition} \supset \textsc{consequent})$$

where $\forall Q$ stands for the universal closure of all free variables occurring in Q, and, typically, ANTECEDENT, SIDE-CONDITION and CONSEQUENT share free variables.

Given a model of the SitCalc action theory, the structural rules define inductively a relation, namely: **the smallest relation satisfying the rules**.

Examples

Compute the following assuming actions are always possible:

- $(a; b, S_0) \longrightarrow (nil; b, do(a, S_0)) \longrightarrow (nil, do(b(do(a, S_0)))$
- $((a \mid b); c, S_0) \longrightarrow ???$
- $((a \mid b); c; P?, S_0) \longrightarrow ???$
- $(a; (b \mid c), S_0) \longrightarrow ???$
- $((a; b \mid a; c), S_0) \longrightarrow ???$

  where P true iff a is not performed yet.

Evaluation vs. transition semantics

How do we characterize a whole computation using single steps?

First we define the relation, named $Trans^*$, denoted by $\longrightarrow^*$ by the following rules:

$$0steps: \quad \frac{(\delta, s) \longrightarrow^* (\delta, s)}{true}$$

$$nsteps: \quad \frac{(\delta, s) \longrightarrow^* (\delta'', s'')}{(\delta, s) \longrightarrow (\delta', s') \ \wedge \ (\delta', s') \longrightarrow^* (\delta'', s'')} \quad \textit{(for some } \delta', s'\textit{)}$$

Then it can be shown that:

$$(\delta, s_0) \longrightarrow s_f \equiv$$
$$(\delta, s_0) \longrightarrow^* (\delta_f, s_0) \ \wedge \ (\delta_f, s_f)^{\surd} \quad \text{for some } \delta_f$$

Getting logical

Till now we have defined the relation $(\delta, s) \longrightarrow (\delta', s')$ and the predicate $(\delta, s)^{\surd}$ in a single model of the SitCalc action theory of interest.

But what about if the action theory has incomplete information and hence admits several models?

Idea: *Define a logical predicates $Trans(\delta, s, \delta', s')$ and $Final(\delta, s)$ starting from the definitions of the relation $(\delta, s) \longrightarrow (\delta', s')$, and $(\delta, s)^{\surd}$.*

Definition of Do: intro

How: *do we define a logical predicate* $Trans(\delta, s, \delta', s')$ *starting from the definition of the relation* $(\delta, s) \longrightarrow (\delta', s')$*?* and the predicate $(\delta, s)\surd$.

- Rules correspond to logical conditions;

- The minimal predicate satisfying the rules is expressible in 2nd-order logic by using the formulas of the following form (for $Trans$, similarly for $Final$):

$\forall T.\{$

logical formulas corresponding to the rules

that use the **predicate variable** T in place of the relation

$\} \supset T(\delta, s, \delta', s').$

Definition of Trans

$Trans(\delta, s, \delta', s') \equiv \forall T.[\ \ldots\ \supset T(\delta, s, \delta', s')]$, where ... stands for the conjunction of the universal closure of the following implications:

$$\begin{array}{rcl}
Poss(a[s], s) & \supset & T(a, s, nil, do(a[s], s)) \\
\phi[s] & \supset & T(\phi?, s, nil, s) \\
T(\delta, s, \delta', s') & \supset & T(\delta; \gamma, s, \delta'; \gamma, s') \\
Final(\gamma, s) \wedge T(\delta, s, \delta', s') & \supset & T(\gamma; \delta, s, \delta', s') \\
T(\delta, s, \delta', s') & \supset & T(\delta \mid \gamma, s, \delta', s') \\
T(\delta, s, \delta', s') & \supset & T(\gamma \mid \delta, s, \delta', s') \\
T(\delta^v_x, s, \delta', s') & \supset & T(\pi v.\delta, s, \delta', s') \\
T(\delta, s, \delta', s') & \supset & T(\delta^*, s, \delta'; \delta^*, s') \\
T(\delta^{P_i(\vec{t})}_{[Env:P_i(\vec{t})]}, s, \delta', s') & \supset & T(\{Env; \delta\}, s, \delta', s') \\
T(\{Env; \delta_{P}{}^{\vec{v}_P}_{\vec{t}[s]}\}, s, \delta', s') & \supset & T([Env : P(\vec{t})], s, \delta', s')
\end{array}$$

Definition of Final

$Final(\delta, s) \equiv \forall F.[\ \ldots\ \supset F(\delta, s)]$, where ... stands for the conjunction of the universal closure of the following implications:

$$
\begin{array}{rcl}
True & \supset & F(nil, s) \\
F(\delta, s) \wedge F(\gamma, s) & \supset & F(\delta;\gamma, s) \\
F(\delta, s) & \supset & F(\delta \mid \gamma, s) \\
F(\delta, s) & \supset & F(\gamma \mid \delta, s) \\
F(\delta^v_x, s) & \supset & F(\pi v.\delta, s) \\
True & \supset & F(\delta^*, s) \\
F(\delta^{P_i(\vec{t})}_{[Env:P_i(\vec{t})]}, s) & \supset & F(\{Env;\delta\}, s) \\
F(\{Env;\delta_{P}{}^{\vec{v}_P}_{\vec{t}[s]}, s) & \supset & F([Env : P(\vec{t})], s)
\end{array}
$$

Concurrency

ConGolog is an extension of Golog that incorporates a rich account of concurrency:

- concurrent processes,
- priorities,
- high-level interrupts.

We model concurrent processes by **interleaving**: *A concurrent execution of two processes is one where the primitive actions in both processes occur, interleaved in some fashion.*

It is OK for a process to remain **blocked** for a while, the other processes will continue and eventually unblock it.

Congolog

The ConGolog language is exactly like Golog except with the following additional constructs:

if ϕ **then** δ_1 **else** δ_2,	synchronized conditional
while ϕ **do** δ,	synchronized loop
$(\delta_1 \parallel \delta_2)$,	concurrent execution
$(\delta_1 \rangle\!\rangle \delta_2)$,	concurrency with different priorities
$\delta^{\parallel}$,	concurrent iteration
$< \phi \rightarrow \delta >$,	interrupt.

The constructs **if** ϕ **then** δ_1 **else** δ_2 and **while** ϕ **do** δ are the synchronized: *testing the condition* ϕ *does not involve a transition per se, the evaluation of the condition and the first action of the branch chosen are executed as an atomic unit.*

Similar to test-and-set atomic instructions used to build semaphores in concurrent programming.

Transition rules: concurrency

$Conc:$

$$\frac{(\delta_1 \parallel \delta_2,\ s) \longrightarrow (\delta'_1 \parallel \delta_2, s')}{(\delta_1, s) \longrightarrow (\delta'_1, s')} \qquad \frac{(\delta_1 \parallel \delta_2,\ s) \longrightarrow (\delta_1 \parallel \delta'_2, s')}{(\delta_2, s) \longrightarrow (\delta'_2, s')}$$

$PriorConc:$

$$\frac{(\delta_1 \rangle\!\rangle\ \delta_2,\ s) \longrightarrow (\delta'_1 \rangle\!\rangle\ \delta_2, s')}{(\delta_1, s) \longrightarrow (\delta'_1, s')} \qquad \frac{(\delta_1 \rangle\!\rangle\ \delta_2,\ s) \longrightarrow (\delta_1 \rangle\!\rangle\ \delta'_2, s')}{(\delta_2, s) \longrightarrow (\delta'_2, s') \ \wedge\ (\delta_1, s) \not\longrightarrow}$$

$IterConc:$

$$\frac{(\delta^{\parallel}, s) \longrightarrow (\delta' \parallel \delta^{\parallel}, s')}{(\delta, s) \longrightarrow (\delta', s')}$$

$Interrupts:$

$$\frac{(<\phi \rightarrow \delta>, s) \longrightarrow (\delta'; <\phi \rightarrow \delta>, s')}{(\delta, s) \longrightarrow (\delta', s')} \quad \text{if } \phi[s] \ \wedge\ Interrups\_running[s]$$

Termination rules: concurrency

$$Conc: \quad \frac{(\delta_1 \parallel \delta_2,\ s)^{\surd}}{(\delta_1, s)^{\surd} \ \wedge \ (\delta_2, s)^{\surd}}$$

$$PrioConc: \quad \frac{(\delta_1 \rangle\!\rangle\ \delta_2,\ s)^{\surd}}{(\delta_1, s)^{\surd} \ \wedge \ (\delta_2, s)^{\surd}}$$

$$IterConc: \quad \frac{(\delta^{\parallel}, s)^{\surd}}{true}$$

$$Interrupts: \quad \frac{(<\phi \rightarrow \delta>, s)^{\surd}}{true} \quad \text{if } \neg Interrups\_running[s]$$

ConGolog Transition Semantics (cont.)

$$
\begin{aligned}
& Trans(nil, s, \delta, s') \equiv False \\
& Trans(\alpha, s, \delta, s') \equiv \\
& \quad Poss(\alpha[s], s) \wedge \delta = nil \wedge s' = do(\alpha[s], s) \\
& Trans(\phi?, s, \delta, s') \equiv \phi[s] \wedge \delta = nil \wedge s' = s \\
& Trans([\delta_1; \delta_2], s, \delta, s') \equiv \\
& \quad Final(\delta_1, s) \wedge Trans(\delta_2, s, \delta, s') \quad \vee \\
& \quad \exists \delta'. \delta = (\delta'; \delta_2) \wedge Trans(\delta_1, s, \delta', s') \\
& Trans([\delta_1 \mid \delta_2], s, \delta, s') \equiv \\
& \quad Trans(\delta_1, s, \delta, s') \vee Trans(\delta_2, s, \delta, s') \\
& Trans(\pi\, x\, \delta, s, \delta, s') \equiv \exists x. Trans(\delta, s, \delta, s')
\end{aligned}
$$

In this semantics, $Trans$ and $Final$ are predicates that take programs as arguments. So need to introduce terms that denote programs (reify programs). In the third axiom, ϕ is a term that denotes a formula, and $\phi[s]$ stands for $Holds(\phi, s)$, which is true iff the formula denoted by ϕ is true in s. Details are in [DLL00].

ConGolog Transition Semantics (cont.)

$$Trans(\delta^*, s, \delta, s') \equiv \exists \delta'.\delta = (\delta'; \delta^*) \wedge Trans(\delta, s, \delta', s')$$

$$Trans(\textbf{if } \phi \textbf{ then } \delta_1 \textbf{ else } \delta_2, s, \delta, s') \equiv$$
$$\quad \phi(s) \wedge Trans(\delta_1, s, \delta, s') \vee \neg\phi(s) \wedge Trans(\delta_2, s, \delta, s')$$

$$Trans(\textbf{while } \phi \textbf{ do } \delta, s, \delta', s') \equiv \phi(s) \wedge$$
$$\quad \exists \delta''.\ \delta' = (\delta''; \textbf{while } \phi \textbf{ do } \delta) \wedge Trans(\delta, s, \delta'', s')$$

$$Trans([\delta_1 \parallel \delta_2], s, \delta, s') \equiv \exists \delta'.$$
$$\quad \delta = (\delta' \parallel \delta_2) \wedge Trans(\delta_1, s, \delta', s') \vee$$
$$\quad \delta = (\delta_1 \parallel \delta') \wedge Trans(\delta_2, s, \delta', s')$$

$$Trans([\delta_1 \rangle\!\rangle\, \delta_2], s, \delta, s') \equiv \exists \delta'.$$
$$\quad \delta = (\delta' \rangle\!\rangle\, \delta_2) \wedge Trans(\delta_1, s, \delta', s') \vee$$
$$\quad \delta = (\delta_1 \rangle\!\rangle\, \delta') \wedge Trans(\delta_2, s, \delta', s') \wedge$$
$$\quad\quad \neg\exists \delta'', s''.Trans(\delta_1, s, \delta'', s'')$$

$$Trans(\delta^{\parallel}, s, \delta', s') \equiv$$
$$\quad \exists \delta''.\delta' = (\delta'' \parallel \delta^{\parallel}) \wedge Trans(\delta, s, \delta'', s')$$

ConGolog Transition Semantics (cont.)

$Final(nil, s) \equiv True$

$Final(\alpha, s) \equiv False$

$Final(\phi?, s) \equiv False$

$Final([\delta_1; \delta_2], s) \ \equiv \ Final(\delta_1, s) \wedge Final(\delta_2, s)$

$Final([\delta_1 \mid \delta_2], s) \ \equiv \ Final(\delta_1, s) \vee Final(\delta_2, s)$

$Final(\pi\, x\, \delta, s) \equiv \exists x.Final(\delta, s)$

$Final(\delta^*, s) \equiv True$

$Final(\textbf{if } \phi \textbf{ then } \delta_1 \textbf{ else } \delta_2, s) \equiv$

$\quad \phi(s) \wedge Final(\delta_1, s) \ \vee \ \neg\phi(s) \wedge Final(\delta_2, s)$

$Final(\textbf{while } \phi \textbf{ do } \delta, s) \equiv$

$\quad \phi(s) \wedge Final(\delta, s) \ \vee \ \neg\phi(s)$

$Final([\delta_1 \parallel \delta_2], s) \ \equiv \ Final(\delta_1, s) \wedge Final(\delta_2, s)$

$Final([\delta_1 \rangle\!\rangle \delta_2], s) \ \equiv \ Final(\delta_1, s) \wedge Final(\delta_2, s)$

$Final(\delta^{\parallel}, s) \equiv True$

ConGolog Transition Semantics (cont.)

Then, define relation $Do(\delta, s, s')$ meaning that process δ, when executed starting in situation s, has s' as a legal terminating situation:

$$Do(\delta, s, s') \stackrel{\text{def}}{=} \exists\delta'.Trans^*(\delta, s, \delta', s') \wedge Final(\delta', s')$$

where $Trans^*$ is the transitive closure of $Trans$. That is, $Do(\delta, s, s')$ holds iff the starting configuration (δ, s) can evolve into a configuration (δ, s') by doing a finite number of transitions and $Final(\delta, s')$.

$$Trans^*(\delta, s, \delta', s') \stackrel{def}{=} \forall T[\ldots \supset T(\delta, s, \delta', s')]$$

where the ellipsis stands for:

$$\begin{array}{l} \forall s.\ T(\delta, s, \delta, s) \quad \wedge \\ \forall s, \delta', s', \delta'', s''.\ T(\delta, s, \delta', s') \wedge \\ \qquad Trans(\delta', s', \delta'', s'') \supset T(\delta, s, \delta'', s''). \end{array}$$

Induction principles

From such definitions, natural “induction principles” emerge:

These are principles saying that to prove that a property P holds for instances of $Trans$ and $Final$, it suffices to prove that the property P is closed under the assertions in the definition of $Trans$ and $Final$, i.e.:

$$\Phi_{Trans}(P, \delta_1, s_1, \delta_2, s_2) \equiv P(\delta_1, s_1, \delta_2, s_2)$$
$$\Phi_{Final}(P, \delta_1, s_1) \equiv P(\delta_1, s_1)$$

Theorem: The following sentences are consequences of the second-order definitions of $Trans$ and $Final$ respectively:

$$\forall P.[\forall \delta_1, s_1, \delta_2, s_2.\, \Phi_{Trans}(P, \delta_1, s_1, \delta_2, s_2) \equiv P(\delta_1, s_1, \delta_2, s_2)] \supset \forall \delta, s, \delta', s'.\, Trans(\delta, s, \delta', s') \supset P(\delta, s, \delta', s')$$

$$\forall P.[\forall \delta_1, s_1.\, \Phi_{Final}(P, \delta_1, s_1) \equiv P(\delta_1, s_1)] \supset \forall \delta, s.\, Final(\delta, s, \delta', s') \supset P(\delta, s)$$

Proof

We prove only the first sentence. The proof of the second sentence is analogous.

By definition we have:

$$\begin{aligned}\forall \delta, s, \delta', s'. Trans(\delta, s, \delta', s') \;\equiv\\ \forall P.[\forall \delta_1, s_1, \delta_2, s_2.\, \Phi_{Trans}(P, \delta_1, s_1, \delta_2, s_2) \equiv P(\delta_1, s_1, \delta_2, s_2)]\\ \supset\; P(\delta, s, \delta', s')\end{aligned}$$

By considering the only-if part of the above equivalence, we get:

$$\begin{aligned}\forall \delta, s, \delta', s'. Trans(\delta, s, \delta', s') \;\wedge\\ \forall P.[\forall \delta_1, s_1, \delta_2, s_2.\, \Phi_{Trans}(P, \delta_1, s_1, \delta_2, s_2) \equiv P(\delta_1, s_1, \delta_2, s_2)]\\ \supset\; P(\delta, s, \delta', s')\end{aligned}$$

So moving the quantifiers around we get:

$$\begin{aligned}\forall P.[\forall \delta_1, s_1, \delta_2, s_2.\, \Phi_{Trans}(P, \delta_1, s_1, \delta_2, s_2) \equiv P(\delta_1, s_1, \delta_2, s_2)] \;\wedge\\ \forall \delta, s, \delta', s'. Trans(\delta, s, \delta', s')\\ \supset\; P(\delta, s, \delta', s')\end{aligned}$$

and hence the thesis.

Bisimulation

Bisimulation is a relation $\sim$ satisfing the condition:

$$
\begin{aligned}
&(\delta_1, s_1) \sim (\delta_2, s_2) \;\supset \\
&\qquad (\delta_1, s_1)^{\surd} \equiv (\delta_2, s_2)^{\surd} \quad \wedge \\
&\qquad \forall(\delta_1', s_1').(\delta_1, s_1) \longrightarrow (\delta_1', s_1') \supset \\
&\qquad\qquad \exists(\delta_2', s_2').(\delta_2, s_2) \longrightarrow (\delta_2', s_2') \;\wedge\; (\delta_1', s_1') \sim (\delta_2', s_2') \quad \wedge \\
&\qquad \forall(\delta_2', s_2').(\delta_2, s_2) \longrightarrow (\delta_2', s_2') \supset \\
&\qquad\qquad \exists(\delta_1', s_1').(\delta_1, s_1) \longrightarrow (\delta_1', s_1') \;\wedge\; (\delta_2', s_2') \sim (\delta_1', s_1')
\end{aligned}
$$

(δ_1, s_1) and (δ_2, s_2) are **bisimilar** if there **exists a bisimulation** between the two.

Note: it can be shown that bisimilarity is an equivalence relation.