A PROOF USING THE INDUCTIVE ASSERTION METHOD
draft

W. Drabent, November 25, 1994

We present an example of applying inductive assertion method of [Drabent and Małuszyński, 1988]. The method makes it possible to express and prove run-time properties of logic programs. Such properties are inexpressible in terms of the declarative semantics. We present a proof of Theorem 5.2 of [Apt and Pellegrini, 1994] concerning correctness of executing a program without occur-check. The proof below is simpler than the original one due to using an inductive assertion method. For necessary definitions and explanations see [Apt and Pellegrini, 1994], [Drabent and Małuszyński, 1988] and [Apt and Marchiori, 1994].

We prove that any nicely moded program P with a nicely moded goal G is output driven (hence it is occur check free provided the heads of the clauses are linear). In other words we show that P and G satisfies the following specification

$$\{\neg share(\overline{x},\overline{y}), linear(\overline{y})\}\ p(\overline{x},\overline{y})\ \{\mathbf{true}\}$$

for each predicate symbol p.

PROOF.
We prove that the verification condition of [Drabent and Małuszyński, 1988] holds.

Consider a nicely moded clause

$$p(s_0,t_0) \leftarrow p_1(s_1,t_1),\ldots,p_n(s_n,t_n)$$

where s_i, t_i are tuples of terms in input and output position respectively. (The nicely moded initial goal $\leftarrow Q$ is represented as clause $\mathbf{g} \leftarrow Q$, which is nicely moded). Consider an atom

$$p(s,t)$$

satisfying its precondition. In other words s and t are disjoint and t is linear. (By disjoint we mean that the terms have no variable in common.) Consider a valuation sequence $\rho_0,\ldots,\rho_n$ for the atom and the clause. (By the definition of the valuation sequence, the clause is disjoint from the atom and ρ_0 is a relevant mgu of $p(s,t)$ and $p(s_0,t_0)$).

We have to show that $p_j(s_j,t_j)\rho_{j-1}$ satisfies its precondition for $j=1,\ldots,n$.

Let

$$\alpha \in \mathrm{mgu}(s,s_0).$$

($\mathrm{mgu}(s,s')$ denotes the set of relevant mgu's of s and s'). Then $t\alpha = t$ and by Lemma A.5 of [Apt and Pellegrini, 1994] (10.6 in [Apt, Pellegrini 1992]) there exists

$$\beta \in \mathrm{mgu}(t, t_0\alpha)$$

such that $\beta|_{t_0\alpha}$ is linear and $\mathrm{Rng}(\beta|_{t_0\alpha}) \subseteq \mathrm{Vars}(t)$. Substitution $\alpha\beta$ is a relevant mgu of $p(s,t)$ and $p(s_0,t_0)$ (by Lemma 2.4, ibidem). There exists a renaming η such that

$$\rho_0 = \alpha\beta\eta$$

(by Lemma 2.3, ibidem).

Consider t_j, $1 \leq j \leq n$. By nice-modedness t_j is disjoint from s_0, thus $t_j\alpha = t_j$. Hence $t_j\alpha\beta = t_j\beta = t_j(\beta|_{t_0\alpha})$ (as $\beta = \beta|_{t_0\alpha} \cup \beta|_t$ and $t_0\alpha$ and t are disjoint).

Now t_j and $\beta|_{t_0\alpha}$ are linear and $\mathrm{Rng}(\beta|_{t_0\alpha}) \subseteq \mathrm{Vars}(t)$, hence $t_j\alpha\beta$ is linear (conf. Lemma A.4 (10.5) ibidem). We show that

$$t_j\rho_0 \quad \text{is linear.} \tag{1}$$

Indeed, assume that a variable v occurs twice in $t_j\alpha\beta\eta$. (Remember that $\mathrm{Rng}(\eta) = \mathrm{Dom}(\eta)$). If $v \notin \mathrm{Rng}(\eta)$ then v occurs twice in $t_j\alpha\beta$. If $v \in \mathrm{Rng}(\eta)$ then variable $v\eta^{-1}$ occurs twice in $t_j\alpha\beta$. Contradiction.

Let $\overline{u} = s_0, \ldots, s_j, t_1, \ldots, t_{j-1}$. We show by induction that for $i = 0, \ldots, j-1$

$$t_j\rho_i = t_j\rho_0 \tag{2}$$

$$\overline{u}\rho_i \text{ and } t_j\rho_0 \text{ are disjoint.} \tag{3}$$

By nice-modedness, $\overline{u}$ and t_j are disjoint. Note that $\overline{u}\alpha, t$ and t_j are pairwise disjoint, $\overline{u}\rho_0 = \overline{u}\alpha(\beta|_{t_0\alpha})\eta$ and $t_j\rho_0 = t_j(\beta|_{t_0\alpha})\eta$. For the base step we show that $\overline{u}\rho_0$ and $t_j\rho_0$ are disjoint.

Assume the contrary, let $v \in \mathrm{Vars}(t_j(\beta|_{t_0\alpha})\eta) \cap \mathrm{Vars}(\overline{u}\alpha(\beta|_{t_0\alpha})\eta)$. We have three cases:

1. $v \prec t_j$ and $v \notin \mathrm{Dom}((\beta|_{t_0\alpha})\eta)$. (Symbol $\prec$ stands for "is a subterm of"). Then $v \not\prec \overline{u}\alpha$. As $v \not\prec t$, $v \notin \mathrm{Rng}(\beta|_{t_0\alpha})$. Hence $v \in \mathrm{Rng}(\eta) = \mathrm{Dom}(\eta)$ and $v \in \mathrm{Dom}((\beta|_{t_0\alpha})\eta)$. Contradiction.

2. $v \in \mathrm{Rng}(\beta|_{t_0\alpha})$ and $v \notin \mathrm{Dom}(\eta)$. Hence $v \notin \mathrm{Rng}(\eta)$, $v \prec t_j(\beta|_{t_0\alpha})$ and $v \prec \overline{u}\alpha(\beta|_{t_0\alpha})$. Also $v \not\prec t_j$ and $v \not\prec \overline{u}\alpha$ because $v \prec t$. As $\beta|_{t_0\alpha}$ is linear, there is exactly one y such that $v \prec y(\beta|_{t_0\alpha})$. Now $y \prec t_j$ and $y \prec \overline{u}\alpha$. Contradiction.

3. $v \in \mathrm{Dom}(\eta)$. Let $x = v\eta^{-1}$. Variable x occurs in $t_j(\beta|_{t_0\alpha})$ and in $\overline{u}\alpha(\beta|_{t_0\alpha})$. The case is reduced to the previous one.

This completes the base case. For the induction step assume that $\overline{u}\rho_{i-1}$ and $t_j\rho_0$ are disjoint and that $t_j\rho_{i-1} = t_j\rho_0$. By the definition of the evaluation sequence

$$\mathrm{Dom}(\sigma_i) \subseteq \mathrm{Vars}(s_i\rho_{i-1}, t_i\rho_{i-1}) \subseteq \mathrm{Vars}(\overline{u}\rho_{i-1})$$

where σ_i is as in the definition, $\rho_i = \rho_{i-1}\sigma_i$. Hence by the inductive assumption $t_j\rho_i = t_j\rho_{i-1}\sigma_i = t_j\rho_0\sigma_i = t_j\rho_0$.

By the definition of the evaluation sequence

$$\mathrm{Rng}(\sigma_i) \cap \mathrm{Vars}(t_j\rho_0) \subseteq \mathrm{Vars}(s_i\rho_{i-1}, t_i\rho_{i-1}) \subseteq \mathrm{Vars}(\overline{u}\rho_{i-1}).$$

Hence

$$\mathrm{Rng}(\sigma_i) \cap \mathrm{Vars}(t_j\rho_0) \subseteq \mathrm{Vars}(\overline{u}\rho_{i-1}) \cap \mathrm{Vars}(t_j\rho_0) = \emptyset.$$

So $\overline{u}\rho_i$ and $t_j\rho_0$ are disjoint as $\mathrm{Vars}(\overline{u}\rho_i) \subseteq \mathrm{Vars}(\overline{u}\rho_{i-1}) \cup \mathrm{Rng}(\sigma_i)$ This completes the induction step.

From (1), (2) and (3) we immediately obtain that $p_j(s_j, t_j)\rho_{j-1}$ satisfies its precondition. This completes the proof. □
Note that linearity of clause heads was not required.

Some parts of the two proofs overlap, most notably Lemma A.5. However our approach relieves us of the burden of considering (arbitrary) LD-derivation. One deals with valuation sequences instead.

References

[Apt and Marchiori, 1994] K. Apt and E. Marchiori. Reasoning about Prolog programs: from modes through types to assertions. *Formal Aspects of Computing*, 1994.

[Apt and Pellegrini, 1994] K. Apt and A. Pellegrini. On the occur-check-free Prolog programs. *ACM ToPLaS*, 16(3):687–726, May 1994.

[Drabent and Małuszyński, 1988] W. Drabent and J. Małuszyński. Inductive assertion method for logic programs. *Theoretical Computer Science*, 59:133–155, June 1988. Special issue with selected papers from TAPSOFT'87, Pisa.