Prof. Dr. P. Thiemann, Dipl.-Math. A. Bieniusa Summer term 2010

Lecture: Program analysis
Exercise 7
`http://proglang.informatik.uni-freiburg.de/teaching/programanalysis/2010ss/`

1 Control Flow Analysis for an object-oriented language

Program	::=	Class* Exp
Class	::=	**class** Id Var* Method* **end**
Var	::=	**var** Id
Method	::=	**method** Id (Id*) Exp **end**
Exp	::=	Term^l
Term	::=	Int | Exp Op Exp | **false** | **true** | Id := Exp | **if** Exp **then** Exp **else** Exp **end** | **this** | **null** | **new** Id | Exp.Id(Exp*)
Op	::=	$+ \mid - \mid * \mid \& \mid < \mid =$
Id	::=	⟨identifier⟩
Int	::=	⟨integer⟩

Consider the object-oriented mini-language defined above. It implements standard semantics, assuming the following rules:

- All variables are initialized with **null**.
- Assignments evaluate to the expression on the right-hand side.
- You may assume that all instance variables and formal arguments have distinct names. Further, **this** is never used outside classes; when used within a class C, it is renamed to **this-C**.

Define a constraint based 0-CFA for this language which determines for each expression to elements of which type(s) it might evaluate. Possible types are **Bool**, **Int**, and $C \in \mathbf{CName}_*$, where $\mathbf{CName}_*$ is the set of all classes defined in a program.

1. What are $C(l)$ and $r(x)$ in this setting?
2. Define for each kind of expression the set of constraints $\mathcal{C}_*$ it generates.
3. Consider the following type-incorrect program:

   ```
   class C
      method n(i)
        i+1
      end
   end

   (new C).n(true)
   ```

   Give the constraints that are generated for this program together with a minimal solution.
4. How can the results of the 0-CFA be used to reject programs which are not type-correct?

2 Correctness of 0-CFA

1. The following statement was crucial in the correctness proof for 0-CFA (cf. Slide 47 or Fact 3.11 on p. 160):

   $$\Big((\widehat{C},\widehat{p}) \models it^{l_1} \ \wedge\ \widehat{C}(l_1) \subseteq \widehat{C}(l_2)\Big) \quad \Rightarrow \quad (\widehat{C},\widehat{p}) \models it^{l_2} \tag{1}$$

   Prove the statement formally.

2. Reconsider the decision to use $\widehat{\mathbf{Val}} = \mathcal{P}(\mathbf{Term})$ in the correctness proof. Alternatively, we could have chosen $\widehat{\mathbf{Val}} = \mathcal{P}(\mathbf{Exp})$. Show that the specification of the CFA may be modified accordingly, but that then the statement 1 above (and hence the correctness result) would fail.

Submission

- Deadline: 12.07.2010, 14:00, per mail to `bieniusa@informatik.uni-freiburg.de`, or on paper to Annette Bieniusa, Geb. 079, Room 000-14.
- Late submissions will not be marked.
- Do not forget to put your name on the exercise sheet.