
CSL 765: Introduction to (Logic and Functional) Programming

I semester 2011-12

Sun 09 Oct 2011

11:00-12:00

Minor I

VI LT1

Max Marks 45

-
1. Please answer in the space provided on the question paper. The other sheets are only for rough work and will not be collected.
 2. You may use any paper-based material including your class notes and any other text books.
 3. You are not allowed to share reference material or rough pages during the exam.
 4. You are not allowed to bring into the exam hall any electronic gadgets such as computers, mobile phones or calculators.
 5. Please keep your identity card with you. You may be asked for it at any time for verification.
-

1. **(7 marks)** Prove that the mgu computed by the unification algorithm is idempotent.

Solution. Let θ be the mgu computed in $k > 0$ iterations by the algorithm for a set S of terms. Let $\rho_i = \{t_i/x_i\}$ be the substitution computed in the i -th iteration and let $\theta_i = \rho_i \circ \dots \circ \rho_1 \circ \mathbf{1}$ for $1 \leq i \leq k$. By the termination claim in the unification theorem and the definition of composition of substitutions it is easy to show by induction on i that $\{x_1, \dots, x_i\} \cap FV(\text{ran}(\theta_i)) = \emptyset$. Hence $\text{dom}(\theta) \cap FV(\text{ran}(\theta)) = \emptyset$. Further $\{x_1, \dots, x_i\} \cap FV(\theta_i S) = \emptyset$ for each $1 \leq i \leq k$. Clearly then since there are no variables from the domain of θ in either the range of θ nor in θS , we have $\theta \circ \theta = \theta$ and $\theta(\theta S) = \theta S$.

2. (8+(8+5) =21 marks) Consider the following datatype defined in ML as

```
datatype i = z | s of i | a of i * i
```

(a) Let δ be a basic reduction defined by the following reductions.

$$\begin{array}{lll} \mathbf{a}(\mathbf{z}, x) & \longrightarrow_{\delta} & x \quad (\delta_1) \\ \mathbf{a}(\mathbf{s}(x), y) & \longrightarrow_{\delta} & \mathbf{a}(x, \mathbf{s}(y)) \quad (\delta_2) \\ \mathbf{a}(x, y) & \longrightarrow_{\delta} & \mathbf{a}(y, x) \quad (\delta_3) \end{array}$$

Prove that for any elements u, v, w of this datatype

$$u \longrightarrow_{\delta}^1 v \wedge u \longrightarrow_{\delta}^1 w \Rightarrow \exists x [v \longrightarrow_{\delta}^* x \wedge w \longrightarrow_{\delta}^* x]$$

Solution. If $v \equiv w$ then there is nothing to prove since we may take $x \equiv v \equiv w$. So in the rest of the proof we assume $v \not\equiv w$. We proceed by induction on the structure of u .

- Case $u \equiv \mathbf{z}$. This case is impossible.
- Case $u \equiv \mathbf{s}(u_1)$. Then $u \longrightarrow_{\delta}^1 v \wedge u \longrightarrow_{\delta}^1 w$ is possible only if for some v_1 and w_1 we have $v \equiv \mathbf{s}(v_1)$, $w \equiv \mathbf{s}(w_1)$ and $u_1 \longrightarrow_{\delta}^1 v_1 \wedge u_1 \longrightarrow_{\delta}^1 w_1$. By the induction hypothesis, there exists x_1 such that $v_1 \longrightarrow_{\delta}^* x_1 \wedge w_1 \longrightarrow_{\delta}^* x_1$ which implies for $x \equiv \mathbf{s}(x_1)$, $v \longrightarrow_{\delta}^* x \wedge w \longrightarrow_{\delta}^* x$.
- Case $u \equiv \mathbf{a}(u_1, u_2)$.
 - Subcase $v \equiv \mathbf{a}(u_2, u_1)$. Choose $x \equiv w$ and we obtain $v \longrightarrow_{\delta}^1 u \longrightarrow_{\delta}^1 w \equiv x$ and the case is proved.
 - Subcase $w \equiv \mathbf{a}(u_2, u_1)$. Choose $x \equiv v$ and we obtain $w \longrightarrow_{\delta}^1 u \longrightarrow_{\delta}^1 v \equiv x$ and the case is proved.
 - Subcase $u_1 \not\equiv \mathbf{s}(u_{11})$, $v \equiv \mathbf{a}(u'_1, u_2)$ where $u_1 \longrightarrow_{\delta}^1 u'_1$. Then if
 - * $w \equiv \mathbf{a}(u''_1, u_2)$ where $u_1 \longrightarrow_{\delta}^1 u''_1$, we get by the induction hypothesis that for some u'''_1 , $u'_1 \longrightarrow_{\delta}^* u'''_1$ and $u''_1 \longrightarrow_{\delta}^* u'''_1$. Choosing $x \equiv \mathbf{a}(u'''_1, u_2)$ we get the required result.
 - * $w \equiv \mathbf{a}(u_1, u'_2)$ where $u_2 \longrightarrow_{\delta}^1 u'_2$. In this case by choosing $x \equiv \mathbf{a}(u'_1, u'_2)$ we get the required result.
 - Subcase $u_1 \equiv \mathbf{s}(u_{11})$. Since $v \not\equiv w$, we may assume without loss of generality that $v \equiv \mathbf{a}(u_{11}, \mathbf{s}(u_2))$ and there are various possibilities for w .
 - * $w \equiv \mathbf{a}(\mathbf{s}(u'_{11}), u_2)$ where $u_{11} \longrightarrow_{\delta}^1 u'_{11}$. Then we have $v \equiv \mathbf{a}(u_{11}, \mathbf{s}(u_2)) \longrightarrow_{\delta}^1 \mathbf{a}(u'_{11}, \mathbf{s}(u_2)) \equiv x$ and $w \equiv \mathbf{a}(\mathbf{s}(u'_{11}), u_2) \longrightarrow_{\delta}^1 \mathbf{a}(u'_{11}, \mathbf{s}(u_2)) \equiv x$.
 - * $w \equiv \mathbf{a}(\mathbf{s}(u_{11}), u'_2)$ where $u_2 \longrightarrow_{\delta}^1 u'_2$. Then clearly $v \equiv \mathbf{a}(u_{11}, \mathbf{s}(u_2)) \longrightarrow_{\delta}^1 \mathbf{a}(u_{11}, \mathbf{s}(u'_2)) \equiv x$ and $w \equiv \mathbf{a}(\mathbf{s}(u_{11}), u'_2) \longrightarrow_{\delta}^1 \mathbf{a}(u_{11}, \mathbf{s}(u'_2)) \equiv x$.

(b) Let γ be a basic reduction on the datatype $\mathbf{i}$ defined by

$$\begin{array}{lll} \mathbf{a}(\mathbf{z}, y) & \longrightarrow_{\gamma} & y \quad (\gamma_1) \\ \mathbf{a}(x, \mathbf{z}) & \longrightarrow_{\gamma} & x \quad (\gamma_2) \\ \mathbf{a}(\mathbf{s}(x), y) & \longrightarrow_{\gamma} & \mathbf{s}(\mathbf{a}(x, y)) \quad (\gamma_3) \\ \mathbf{a}(x, \mathbf{s}(y)) & \longrightarrow_{\gamma} & \mathbf{s}(\mathbf{a}(y, x)) \quad (\gamma_4) \end{array}$$

Let $=_{\delta}$ and $=_{\gamma}$ be the respective equality relations obtained by the compatible, reflexive, symmetric and transitive closures of the relations $\longrightarrow_{\delta}^1$ and $\longrightarrow_{\gamma}^1$ respectively.

i. Prove that for all terms x and y , $x =_{\gamma} y$ implies $x =_{\delta} y$.

Solution.

Let $\mathbf{s}^0(\mathbf{z}) \equiv \mathbf{z}$ and $\mathbf{s}^{(i+1)}(\mathbf{z}) \equiv \mathbf{s}^i(\mathbf{s}(\mathbf{z})) \equiv \mathbf{s}(\mathbf{s}^i(\mathbf{z}))$. The set $N = \{\mathbf{s}^k(\mathbf{z}) \mid k \geq 0\}$ is actually the set of all γ -normal forms and δ -normal forms. We prove the following claim first.

Claim. For each x there is a unique $k \geq 0$ such that $x \longrightarrow_{\gamma}^* \mathbf{s}^k(\mathbf{z})$ and $x \longrightarrow_{\delta}^* \mathbf{s}^k(\mathbf{z})$.

$\vdash$ We prove this by induction on the structure of x . Clearly if $x \in N$ there is nothing to prove. In particular the basis when $x \equiv \mathbf{z}$ therefore is proven. For the induction step, consider any x that is not in N . We have the following cases.

- Case $x \equiv \mathbf{s}(x_1)$, where $x_1 \notin N$. But by the induction hypothesis, there exists a unique k_1 such that $x_1 \longrightarrow_{\gamma}^* \mathbf{s}^{k_1}(\mathbf{z})$ and $x_1 \longrightarrow_{\delta}^* \mathbf{s}^{k_1}(\mathbf{z})$. It follows then that $x \longrightarrow_{\gamma}^* \mathbf{s}^{k_1+1}(\mathbf{z})$ and $x \longrightarrow_{\delta}^* \mathbf{s}^{k_1+1}(\mathbf{z})$.

- Case $x \equiv \mathbf{a}(u, v)$ where one or both of u and v is not in δ -normal form. Regardless, by the induction hypothesis we have that there exist unique $i, j \geq 0$ such that

$$u \rightarrow_{\gamma}^* \mathbf{s}^i(\mathbf{z}), u \rightarrow_{\delta}^* \mathbf{s}^i(\mathbf{z}), v \rightarrow_{\gamma}^* \mathbf{s}^j(\mathbf{z}), v \rightarrow_{\delta}^* \mathbf{s}^j(\mathbf{z}). \quad (1)$$

- Subcase $i = 0$. Then $u \equiv \mathbf{z}$ and we have by (γ_1) , (δ_1) that $x \equiv \mathbf{a}(\mathbf{z}, \mathbf{s}^j(\mathbf{z})) \rightarrow_{\gamma}^* \mathbf{s}^j(\mathbf{z})$ and $x \equiv \mathbf{a}(\mathbf{z}, \mathbf{s}^j(\mathbf{z})) \rightarrow_{\delta}^* \mathbf{s}^j(\mathbf{z})$.
- Subcase $j = 0$. Then $v \equiv \mathbf{z}$ and we have by (γ_2) that $x \equiv \mathbf{a}(\mathbf{s}^i(\mathbf{z}), \mathbf{z}) \rightarrow_{\gamma}^* \mathbf{s}^i(\mathbf{z})$ and by first applying (δ_3) and then (δ_1) we have $x \equiv \mathbf{a}(\mathbf{s}^i(\mathbf{z}), \mathbf{z}) \xrightarrow{\delta_3} \mathbf{a}(\mathbf{z}, \mathbf{s}^i(\mathbf{z})) \xrightarrow{\delta_1} \mathbf{s}^i(\mathbf{z})$.
- Subcase $i > 0, j > 0$. Then

$$x \equiv \mathbf{a}(\mathbf{s}^i(\mathbf{z}), \mathbf{s}^j(\mathbf{z})) \xrightarrow{\gamma_3} \mathbf{s}^i(\mathbf{a}(\mathbf{z}, \mathbf{s}^j(\mathbf{z}))) \xrightarrow{\gamma_1} \mathbf{s}^i(\mathbf{s}^j(\mathbf{z})) \equiv \mathbf{s}^{i+j}(\mathbf{z})$$

and

$$\begin{aligned} x &\equiv \mathbf{a}(\mathbf{s}^i(\mathbf{z}), \mathbf{s}^j(\mathbf{z})) \xrightarrow{\delta_2} \mathbf{a}(\mathbf{s}^{i-1}(\mathbf{z}), \mathbf{s}^{1+j}(\mathbf{z})) \xrightarrow{\delta_2} \dots \xrightarrow{\delta_2} \\ &\mathbf{a}(\mathbf{z}, \mathbf{s}^{i+j}(\mathbf{z})) \xrightarrow{\delta_2} \mathbf{s}^{i+j}(\mathbf{z}) \end{aligned}$$

⊥

By the previous solution it is clear the $\rightarrow_{\delta}$ is Church-Rosser. and using the above claim we get

$$\begin{array}{ccccc} x & & =_{\delta} & & y \\ \swarrow_{\delta^*} & & \Downarrow & & \swarrow_{\delta^*} \\ & & \exists k : \mathbf{s}^k(\mathbf{z}) & \Rightarrow & \exists k : \mathbf{s}^k(\mathbf{z}) \\ \searrow_{\gamma^*} & & & & \searrow_{\gamma^*} \\ x & & =_{\gamma} & & y \\ \swarrow_{\gamma^*} & & \Uparrow & & \swarrow_{\gamma^*} \\ & & \exists k : \mathbf{s}^k(\mathbf{z}) & & \end{array}$$

- ii. Prove that γ is strongly normalising (whereas δ is not).

Solution. We need to show that there are no infinite sequences of γ reductions. For this purpose it is enough to define a “measure” $\mathbf{m}$ on the terms such that the following properties are guaranteed.

P1. For every normal form $n \in N$, $\mathbf{m}(n) = 0$.

P2. Every term that is not in normal form has a positive measure

P3. Every application of a γ -rule yields a term with a strictly smaller measure i.e. $x \rightarrow_{\gamma}^1 y$ implies $\mathbf{m}(x) > \mathbf{m}(y)$.

For this particular rewrite system we choose $\mathbf{m}$ to be the following:

$$\begin{array}{ll} \#(\mathbf{z}) & \stackrel{df}{=} 1 \\ \#(\mathbf{s}(x)) & \stackrel{df}{=} 1 + \#(x) \\ \#(\mathbf{a}(x, y)) & \stackrel{df}{=} 1 + \#(x) + \#(y) \end{array} \quad \begin{array}{ll} \mathbf{m}(\mathbf{z}) & \stackrel{df}{=} 0 \\ \mathbf{m}(\mathbf{s}(x)) & \stackrel{df}{=} \mathbf{m}(x) \\ \mathbf{m}(\mathbf{a}(x, y)) & \stackrel{df}{=} \mathbf{m}(x) + \mathbf{m}(y) + \#(\mathbf{a}(x, y)) \end{array}$$

It is easy to see that $\mathbf{m}$ satisfies the three properties given above and hence γ is strongly normalizing i.e. all γ -reduction sequences are finite.

Notes and Explanations:

- The terms which are not in normal form are exactly those which have at least one occurrence of the constructor $\mathbf{a}$.
- In particular notice that the measure $\mathbf{m}(x)$ is simply the sum of the number of nodes in each subtree that is rooted at an occurrence of the constructor $\mathbf{a}$. This measure is reduced
 - by eliminating an occurrence of the constructor $\mathbf{a}$ when either γ_1 or γ_2 is applied,
 - by lowering the height of the constructor $\mathbf{a}$ with respect to one of its arguments when either γ_3 or γ_4 is applied.

Notice that the same is not true of applications of δ .

- There is a more “obvious” proof possible by using induction on the structure of terms and not using the measure $\mathbf{m}$. But the proof would be quite long with many cases and sub-cases as in the previous proofs. *This is left as an exercise for you.*
- There is a clever but elegant proof possible by using the notions of computation trees rooted at x and using König’s lemma. *This is left as an exercise for you.*

3. (7+10 = 17 marks)

- (a) Let $\underline{m}$ denote the Church numeral representation of the natural number m . Define a combinator **quorem** in the untyped λ -calculus such that for any natural numbers m, n

$$\mathbf{quorem} \ \underline{m} \ \underline{n} = \begin{cases} \mathbf{pair} \ \underline{0} \ \underline{m} & \text{if } n = 0 \text{ or } n > m \\ \mathbf{pair} \ \underline{m \div n} \ \underline{m \bmod n} & \text{otherwise} \end{cases}$$

You may use any of the named combinators already defined in Gordon's notes without explaining them.

Solution. It is possible to define two separate recursive functions **quo** and **rem** and then pair their results together to obtain a solution. However, we use the iterative method of repeated subtraction to obtain the result. In both cases we do require to define the *less-than* predicate and the *subtraction* function. We then have the following definitions. Following the convention in Gordon's notes we define for any function **func**

$$\mathbf{func} \stackrel{df}{=} (\mathbf{Y} \ \mathbf{funcfn})$$

where the various functions **funcfn** are defined below

$$\begin{aligned} \mathbf{ltfn} &\stackrel{df}{=} \lambda f \ m \ n [(\mathbf{iszero} \ n) \longrightarrow \mathbf{false} | ((\mathbf{iszero} \ m) \longrightarrow \mathbf{true} | (f \ (\mathbf{pre} \ m) \ (\mathbf{pre} \ n)))] \\ \mathbf{subfn} &\stackrel{df}{=} \lambda f \ m \ n [((\mathbf{iszero} \ m) \longrightarrow m | ((\mathbf{iszero} \ n) \longrightarrow m | (f \ (\mathbf{pre} \ m) \ (\mathbf{pre} \ n)))] \\ \mathbf{qrpfn} &\stackrel{df}{=} \lambda f \ m \ n \ q \ r [(\mathbf{lt} \ r \ n) \longrightarrow (\mathbf{pair} \ q \ r) | (f \ m \ n \ (\mathbf{suc} \ q) \ (\mathbf{sub} \ r \ n))] \end{aligned}$$

Finally we have

$$\mathbf{quorem} \stackrel{df}{=} \lambda m \ n [(\mathbf{iszero} \ n) \longrightarrow (\mathbf{pair} \ \underline{0} \ m) | ((\mathbf{lt} \ m \ n) \longrightarrow (\mathbf{pair} \ \underline{0} \ m) | (\mathbf{qrp} \ m \ n \ \underline{0} \ m))]$$

- (b) Prove that addition is commutative in the Church numerals.

Solution. We have

$$\mathbf{add} \stackrel{df}{=} \lambda m \ n \ f \ x [((m \ f) \ ((n \ f) \ x))]$$

For any natural number k the corresponding Church numeral $\underline{k}$ is defined as $\underline{k} \stackrel{df}{=} \lambda f \ x [(f^k \ x)]$. We then have for any naturals i and j ,

$$\begin{aligned} (\mathbf{add} \ \underline{i} \ \underline{j}) &\longrightarrow_{\beta}^2 \lambda f \ x [((\underline{i} \ f) \ (\underline{j} \ f \ x))] & , & & (\mathbf{add} \ \underline{j} \ \underline{i}) &\longrightarrow_{\beta}^2 \lambda f \ x [((\underline{j} \ f) \ (\underline{i} \ f \ x))] \\ (\underline{i} \ f) &\longrightarrow_{\beta}^1 \lambda x [(f^i \ x)] & , & & (\underline{j} \ f) &\longrightarrow_{\beta}^1 \lambda x [(f^j \ x)] \\ ((\underline{j} \ f) \ x) &\longrightarrow_{\beta}^2 (f^j \ x) & , & & ((\underline{i} \ f) \ x) &\longrightarrow_{\beta}^2 (f^i \ x) \\ ((\underline{i} \ f) \ (\underline{j} \ f \ x)) &\equiv_{\alpha} (\lambda y [(f^i \ y)] \ (f^j \ x)) & , & & ((\underline{j} \ f) \ (\underline{i} \ f \ x)) &\equiv_{\alpha} (\lambda y [(f^j \ y)] \ (f^i \ x)) \\ &\longrightarrow_{\beta}^1 (f^{i+j} \ x) & , & & &\longrightarrow_{\beta}^1 (f^{j+i} \ x) \end{aligned}$$

Hence $(\mathbf{add} \ \underline{i} \ \underline{j}) =_{\beta} (f^{i+j} \ x) \equiv (f^{j+i} \ x) =_{\beta} (\mathbf{add} \ \underline{j} \ \underline{i})$.