Take-Home Exam of Theoretical Computer Science. June 2011.

1. Let N denote the set of the natural numbers. Show that $f : N \rightarrow N$ such that
$f(x) = \textbf{if } x \leq 3 \textbf{ then } 1 \textbf{ else } x \times f(x-1) \times f(x-2)$
is a primitive recursive function.

2. Let N denote the set of the natural numbers. Show that the inverse f^{-1} of an injection $f : N \rightarrow N$ which is a partial recursive function, is itself a partial recursive function.

3. Let N denote the set of the natural numbers. Let PRF be the set of all partial-recursive-functions from N to N (p.r.f, for short). Show that the set of the total p.r.f. is not a recursive subset of PRF.

4. Let N denote the set of the natural numbers. Consider the function $sum : N \times N \rightarrow N$ defined as follows:

for all $n \in N$, $\quad sum(0, n) = n$
for all $m, n \in N$, $\quad sum(succ(m), n) = succ(sum(m, n))$,

where *succ* is the successor function on the natural numbers.
Show by mathematical induction on two variables, that for all $m, n \in N$, $\quad sum(m, n) = sum(n, m)$.

5. Consider a definite logic program P. Give the definition of (i) an interpretation of P, (ii) a Herbrand interpretation of P, (iii) a model of P, (iv) a Herbrand model of P, and (v) the least Herbrand model of P.

6. Show that $\vdash (\exists x\ [x = t \wedge A(x)]) \leftrightarrow A(t)$ if t is free for x in $A(x)$ and x does not occur in t. Show that the two conditions above are necessary.

7. Given a continuous function $f : D \rightarrow D$, where D is a cpo with bottom. Show that:
(i) $\bigsqcup_{n\in\omega}(\lambda f.f^n(\bot)) \ = \ \lambda f.(\bigsqcup_{n\in\omega} f^n(\bot))$, and
(ii) $fix(f) = f(fix(f))$ where *fix* is defined as follows: $\bigsqcup_{n\in\omega}(\lambda f.f^n(\bot))$.

8. Prove the total correctness of the following program (division in binary arithmetics):

$\{P \geq 0 \wedge Q > 0\}$
$r := P;\quad m := Q;\quad k := 0;\quad q := 0;$
while $r \geq m$ **do** $m := m \times 2;\quad k := k+1$ **od**;
while $m \neq Q$ **do** $m := m / 2;\quad k := k-1;$
if $r \geq m$ **then begin** $r := r - m;\quad q := q + 2^k$ **end**
od
$\{0 \leq r < Q \ \wedge\ P = Q \times q + r\}$

9. Let N be the set of natural numbers. Show that for any $a, b \in N$, for any function $c \in N \rightarrow N$, for any function $f \in N \rightarrow N$ defined by the following equations:

$$f(0) = a \qquad f(1) = b \qquad f(n+2) = c(f(n))$$

we have that the following program:

$\{K \geq 0\}$
$k := K;$
if $even(k)$ **then** $res := a$ **else** $res := b$;
while $k > 1$ **do** $res := c(res);\quad k := k-2$ **od**
$\{res = f(K)\}$

is totally correct.

10. Find the weakest precondition $F(x)$ of the statement $\quad x := 0;$ **while** $Q(x) \wedge x \geq 0$ **do** $x := x + 1$ and the postcondition $Q(x)$. Show that for all formulas $P(x)$ such that the Hoare triple

$\{P(x)\}\ x := 0;$ **while** $Q(x) \wedge x \geq 0$ **do** $x := x + 1\ \{Q(x)\}$

holds, we have that $P(x) \rightarrow Q(x)$.

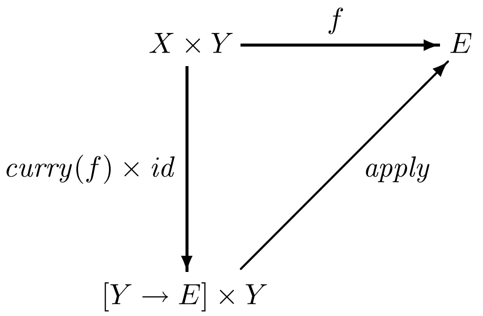
11. Find all formulas $P(x, y)$ such that the Hoare triple

$\{y>1\}$ $x := 0$; **while** $y>x \wedge P(x, y)$ **do** $x := y - 1$ $\{x=0 \wedge y>1\}$

holds. Explain your answer.

12. Let us consider a cpo $(D, \sqsubseteq)$. U subset of D is said to be *open* iff (i) $\forall d, e \in D.\ (d \sqsubseteq e$ and $d \in U) \Rightarrow e \in U$, and (ii) for all chains $d_0 \sqsubseteq d_1 \sqsubseteq \ldots$ in D we have $\bigsqcup_{n\in\omega} d_n \in U \ \Rightarrow\ \exists n \in \omega.\ d_n \in U$. Show that: (i) $\emptyset$ and D are open, (ii) any finite intersection of open sets is open, and (iii) the union of any set of open sets is open.

13. Let N be the discrete cpo of the natural numbers. Explain the meaning of the commutativity of the following diagram, where f is a continuous function:



Give the explicit definition of the functions *apply* and $\lambda f.\ curry(f)$, in the case where: (i) $X = Y = E = N$, and (ii) f is $\lambda xy.\ sum(x, y)$, where for all $x, y \in N$, (ii.1) $sum(0, y) = y$, and (ii.2) $sum(succ(x), y) = succ(sum(x, y))$.

14. We say that a binary relation $\prec\ \subseteq X \times X$ is well-founded on a set X iff there is no infinite descending sequence $\ldots \prec x_i \prec \ldots \prec x_1 \prec x_0$ of elements of X. Let $f : A \to B$ be a function and $\prec_B$ be a well-founded relation on B. Show that $\prec_A$ is a well-founded relation on A, where $\prec_A$ is defined as follows: $a \prec_A a'$ iff $f(a) \prec_B f(a')$.

15. Let us consider two cpo's D and E and a continuous function f from D to E. Show that if Q is an inclusive subset of E then $P = f^{-1}(Q)$ is an inclusive subset of D.
Recall that a set P is said to be *inclusive* iff for each ω-chain $d_0 \sqsubseteq d_1 \sqsubseteq \ldots$ in P we have that $(\bigsqcup_{i\in\omega} d_i) \in P$.

16. Let N denote the discrete cpo of the integers and $N_\perp$ denote the flat cpo of the integers. Let us consider the following function, expressed in the REC language:

$ack(m, n) =$ **if** m **then** $n + 1$ **else**
if n **then** $ack(m - 1, 1)$ **else**
$ack(m - 1, ack(m, n - 1))$.

Prove that for all $m, n \geq 0$, (i) $ack(m, n)$ terminates in the call-by-value semantics, and (ii) $ack(m, n)$ terminates in the call-by-name semantics.

17. Consider the following three rewriting rules:

$ack(0, n) \rightarrow s(n)$
$ack(s(m), 0) \rightarrow ack(m, s(0))$
$ack(s(m), s(n)) \rightarrow ack(m, ack(s(m), n))$

where, as usual, the natural numbers $0, 1, 2, \ldots$ are denoted by 0, $s(0)$, $s(s(0))$, …, respectively.

Prove that for all $m, n \geq 0$, every sequence $t_0, t_1, \ldots$ of terms, such that: (i) $t_0 = ack(m, n)$, and (ii) for all $i \geq 0$, t_{i+1} is derived from t_i by applying in *any subterm* of t_i *any* of the above rewriting rules, is finite.

18. Consider the equation $f(x) =$ if $x < 3$ then 1 else $x \times f(x - 1)$ and the associated functional $\varphi = \lambda f.\lambda x.$ if $x < 3$ then 1 else $x \times f(x - 1)$.
(i) Compute the function $\delta_{va} : N \to N_\perp$, where N is the discrete cpo of natural numbers, defined

as the minimal fixpoint of φ in call-by-value semantics. (ii) Compute the function $\delta_{na} : N_\perp \to N_\perp$ defined as the minimal fixpoint of φ in call-by-name semantics.

19. Check whether or not in lazy1 denotational semantics for any $F : \tau \to \tau$, for any environment ρ, we have that $[[F(RF)]]\rho = [[RF]]\rho$, where R is $\mathbf{rec}\ y.(\lambda f.f(yf))$. Do the same check in the case the lazy2 denotational semantics.

20. Check whether or not for any environment ρ,

$$[[\mathbf{rec}\ f.(\lambda x.e)]]\,\rho = [[\lambda x.(\mathbf{let}\ f \Leftarrow (\mathbf{rec}\ f.(\lambda x.e))\ \mathbf{in}\ f(x))]]\,\rho$$

in eager, lazy1, or lazy2 denotational semantics.

21. Show that the bisimulation equivalence in pure CCS is an equivalence relation and not a congruence relation.

22. Assume that, given a formula A, the formula $\nu X.(A \wedge [.]X)$ holds in a state, say s, of a given process. Explain in words the meaning of $\nu X.(A \wedge [.]X)$ for the state s.

Projects.

A1. Define a higher order lazy language, call it EL, which is an extension of the Lazy language and write a Prolog program for the operational semantics of EL.

A2. Write a simple local model checker in Prolog and use it for proving the correctness of a mutual exclusion protocol or a cache coherence protocol.