University of Nottingham

SCHOOL OF COMPUTER SCIENCE
AND INFORMATION TECHNOLOGY

A LEVEL 1 MODULE, SPRING SEMESTER 2000-2001

PROGRAMMING ALGEBRA
(Course G53PAL)

Solutions

Question 1:

a)

$$-x \leq y \equiv x \geq -y$$

The two orderings are the at-most ordering on real numbers and the at-least ordering on real number.

b)

$$p \vee q \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$$

The orderings are $\Rightarrow$ on the Booleans and $\Rightarrow$ lifted pointwise to pairs of Booleans. The upper adjoint is the doubling function.

c) Let nd denote the predicate "not divisible by 3". Then

$$nd.m \Rightarrow b \equiv m / (\textbf{ if } b \textbf{ then } 1 \textbf{ else } 3)$$

The orderings are $\Rightarrow$ on the Booleans and the divisibility ordering on positive numbers.

d)

$$lcm.(m,n) \backslash p \equiv m \backslash p \wedge n \backslash p$$

The orderings are the divisibility ordering on positive numbers and the divisibility ordering on positive numbers lifted pointwise to pairs of numbers. The upper adjoint is the doubling function.

e) We use the standard method of defining an ordering given an associative, symmetric, idempotent operator $+$, namely

$$x \sqsubseteq y \equiv x+y = y$$

So in this case

$$\begin{array}{ll}
 & (p,q) \sqsubseteq (r,s) \\
= & \{ \quad \text{standard definition} \quad \} \\
 & (p,q)+(r,s) \; = \; (r,s) \\
= & \{ \quad \text{definition of } + \quad \} \\
 & (p \vee r \,,\, q \vee s) \; = \; (r,s) \\
= & \{ \quad \text{pairing} \quad \} \\
 & (p \vee r \; = \; r) \wedge (q \vee s \; = \; s) \\
= & \{ \quad \text{definition} \quad \} \\
 & (p \Rightarrow r) \wedge (q \Rightarrow s)
\end{array}$$

The ordering is thus the implication ordering lifted to pairs of booleans. The smallest element is $(\mathit{false},\mathit{false})$ and the largest element is $(\mathit{true},\mathit{true})$.

We have:

$$\begin{array}{ll}
 & (p,q) \times (r,s) \;\; \sqsubseteq \;\; (t,u) \\
= & \{ \quad \text{definition of } \times \text{ and } \sqsubseteq \quad \} \\
 & ((p \wedge r) \vee (q \wedge s) \Rightarrow t) \;\wedge\; ((p \wedge s) \vee (q \wedge r) \Rightarrow u) \\
= & \{ \quad \text{Galois connection defining } \vee \quad \} \\
 & (p \wedge r \Rightarrow t) \wedge (q \wedge s \Rightarrow t) \wedge (p \wedge s \Rightarrow u) \wedge (q \wedge r \Rightarrow u) \\
= & \{ \quad \text{property of } \wedge \quad \} \\
 & (r \Rightarrow (p \Rightarrow t)) \wedge (s \Rightarrow (q \Rightarrow t)) \wedge (s \Rightarrow (p \Rightarrow u)) \wedge (r \Rightarrow (q \Rightarrow u)) \\
= & \{ \quad \text{property of } \wedge \quad \} \\
 & (r \Rightarrow ((p \Rightarrow t) \wedge (q \Rightarrow u))) \wedge (s \Rightarrow ((q \Rightarrow t) \wedge (p \Rightarrow u))) \\
= & \{ \quad \text{definition of } \sqsubseteq \quad \} \\
 & (r,s) \;\; \sqsubseteq \;\; ((p \Rightarrow t) \wedge (q \Rightarrow u) \,,\, (q \Rightarrow t) \wedge (p \Rightarrow u))
\end{array}$$

So we define

$$(p,q) \backslash (t,u) \;\; = \;\; ((p \Rightarrow t) \wedge (q \Rightarrow u) \,,\, (q \Rightarrow t) \wedge (p \Rightarrow u))$$

For the final property we don't need the details of the addition and multiplication operators. We have, for all x, y, z, a

$$\begin{array}{ll}
 & x \times (y+z) \;\; \sqsubseteq \;\; a \\
= & \{ \quad \text{multiplication admits division} \quad \} \\
 & y+z \;\; \sqsubseteq \;\; x \backslash a \\
= & \{ \quad \text{addition is maximum operator} \quad \} \\
 & y \;\; \sqsubseteq \;\; x \backslash a \quad \wedge \quad z \;\; \sqsubseteq \;\; x \backslash a \\
= & \{ \quad \text{step 1 reversed} \quad \}
\end{array}$$

$$x \times y \sqsubseteq a \ \wedge\ x \times z \sqsubseteq a$$

$$= \qquad \{ \quad \text{step 2 reversed} \quad \}$$

$$(x \times y) + (x \times z) \sqsubseteq a$$

Hence, by indirect equality,

$$x \times (y + z) = (x \times y) + (x \times z)$$

Question 2:

a) Given a labelled graph G, the following procedure is used to determin the transitive closure G^+.

```
    $X := G$
    { Invariant: $G^+ = f(X, [k..n))$ }
;   for each $k$, $1 \leq k \leq n$
    do for each pair $(i,j)$, $1 \leq i,j \leq n$
       do $x_{ij} := x_{ij} + x_{ik} \cdot (x_{kk})^* \cdot x_{kj}$
       end_for
    end_for
    { $G^+ = X$ } .
```

The edge labels must be elements of a Kleene algebra. That is, there must be a zero element, a unit element, an addition operator, a multiplication operator and an iteration operator such that: addition is associative, symmetric and idempotent, multiplication is associative and distributes through addition, and star is such that $a^* \cdot b$ is the least fixed point of the function mapping x to $b + a \cdot x$ and $b \cdot a^*$ is the least fixed point of the function mapping x to $b + x \cdot a$.

b) The algebra we use is an algebra of pairs of boolean values. The first component of a pair represents the existence of an even length path in the graph and the second component the existence of an odd length path. The existence of an edge label in the graph is represented by the pair $(\mathsf{false}, \mathsf{true})$. If there is no edge the corresponding matrix entry is $(\mathsf{false}, \mathsf{false})$. The addition, multiplication and star operators are given by

$$(p, q) + (r, s) = (p \vee r\,,\ q \vee s)$$

$$(p, q) \times (r, s) = ((p \wedge r) \vee (q \wedge s)\ ,\ (p \wedge s) \vee (q \wedge r))$$

and

$$(p, q)^* = (\mathsf{true}, q) \ .$$

The unit is $(\mathsf{true}, \mathsf{false})$ and zero is $(\mathsf{false}, \mathsf{false})$. (These claims are easily checked.)

Addition is clearly symmetric, idempotent and associative. Multiplication is clearly symmetric. That it distributes through addition is question 1(e). That it is associative is proved as follows. By expanding the definition of multiplication,

$$((p,q)\times(r,s))\times(u,v) \;=\; (a,b)$$

where

$$a \;=\; (((p\wedge r)\vee(q\wedge s))\wedge u) \;\vee\; (((p\wedge s)\vee(q\wedge r))\wedge v)$$

and

$$b \;=\; (((p\wedge r)\vee(q\wedge s))\wedge v) \;\vee\; (((p\wedge s)\vee(q\wedge r))\wedge u) \;\;.$$

Also,

$$(p,q)\times((r,s)\times(u,v)) \;=\; (c,d)$$

where

$$c \;=\; (p\wedge((r\wedge u)\vee(s\wedge v))) \;\vee\; (q\wedge((r\wedge v)\vee(s\wedge u)))$$

and

$$d \;=\; (p\wedge((r\wedge v)\vee(s\wedge u))) \;\vee\; (q\wedge((r\wedge u)\vee(s\wedge v))) \;\;.$$

An easy calculation then shows that

$$a \;=\; c \;=\; (p\wedge r\wedge u)\vee(p\wedge s\wedge v)\vee(q\wedge r\wedge v)\vee(q\wedge s\wedge u)$$

and

$$b \;=\; d \;=\; (q\wedge s\wedge v)\vee(p\wedge r\wedge v)\vee(p\wedge s\wedge u)\vee(q\wedge r\wedge u) \;\;.$$

For the definition of star we have to check that

$$(p,q)^* \;=\; (true,false)+((p,q)\;\times\;(p,q)^*) \;\;.$$

We have:

$$
\begin{array}{cl}
 & (true,false)+((p,q)\;\times\;(p,q)^*) \\
= & \{\quad \text{definition of } (p,q)^* \quad\} \\
 & (true,false)+((p,q)\times(true,q)) \\
= & \{\quad \text{definitions of addition and multiplication} \quad\} \\
 & (true\,,\,(p\wedge q)\vee(q\wedge true)) \\
= & \{\quad \text{calculus} \quad\} \\
 & (true,q) \\
= & \{\quad \text{definition of } (p,q)^* \quad\} \\
 & (p,q)^* \;\;.
\end{array}
$$

We also have to show that

$$(true,q)\;\sqsubseteq\;(r,s) \;\Leftarrow\; (true,false)+((p,q)\times(r,s))\;\sqsubseteq\;(r,s) \;\;.$$

We have,

$(\mathit{true}, \mathit{false}) + ((p,q) \times (r,s)) \;\sqsubseteq\; (r,s)$

$=$ { definitions }

$(\mathit{true} \Rightarrow r) \wedge ((p \wedge s) \vee (q \wedge r) \Rightarrow s)$

$=$ { calculus }

$r = \mathit{true} \wedge (p \wedge s \Rightarrow s) \wedge (q \wedge r \Rightarrow s)$

$=$ { substitution of equals for equals,
properties of implication }

$r = \mathit{true} \wedge q \Rightarrow s$

$=$ { definition of $\sqsubseteq$ }

$(\mathit{true}, q) \;\sqsubseteq\; (r,s)$.

Question 3:

a)

$\mu\langle X{::}\, (X{+}a)^{+}\rangle$

$=$ { $x^{+} = \mu\langle X{::}\, X{\cdot}X + x\rangle$ }

$\mu\langle X{::}\, \mu\langle Y{::}\, Y{\cdot}Y + X + a\rangle\rangle$

$=$ { diagonal rule }

$\mu\langle Y{::}\, Y{\cdot}Y + Y + a\rangle$

$=$ { diagonal rule }

$\mu\langle Y{::}\, \mu\langle X{::}\, Y{\cdot}Y + X + a\rangle\rangle$

$=$ { definition of star, $1^{*} = 1$ }

$\mu\langle Y{::}\, Y{\cdot}Y + a\rangle$

$=$ { $x^{+} = \mu\langle X{::}\, X{\cdot}X + x\rangle$ }

a^{+} .

b) $S = \mu\langle X{::}\, X\{X\} \mid a\rangle$, $T = \mu\langle X{::}\, (X \mid a)\ \{X \mid a\}\rangle$, $U = \mu\langle X{::}\, a\{a\}\rangle$. Equivalently, using the standard notation for regular expressions, $S = \mu\langle X{::}\, X^{+} + a\rangle$, $T = \mu\langle X{::}\, (X{+}a)^{+}\rangle$, $U = \mu\langle X{::}\, a^{+}\rangle$. The equality between S and T is proved as follows:

$\mu\langle X{::}\, X^{+} + a\rangle$

$=$ { rolling rule }

$\mu\langle X{::}\, (X{+}a)^{+}\rangle + a$

$=$ { part (a) }

$a^{+} + a$

$=$ { $a^{+} \supseteq a$ }

$$\begin{array}{ll}
 & \mathsf{a}^{+} \\
= & \{ \quad \text{definition of } \mathsf{T}\text{, part (a)} \quad \} \\
 & \mathsf{T} \ .
\end{array}$$

The function $\langle \mathsf{X}\!:: \mathsf{a}^{+}\rangle$ is constant-valued. So $\mathsf{U}=\mathsf{a}^{+}$. Thus S, T and U are all equal.

c) The language generated by V is the empty language ϕ. We prove this by fixed point induction:

$$\begin{array}{ll}
 & \mathsf{V}\subseteq\phi \\
\Leftarrow & \{ \quad \text{definition of } \mathsf{V}\text{, fixed point induction} \quad \} \\
 & \mathsf{a}\phi\{\mathsf{a}\phi\}\subseteq\phi \\
= & \{ \quad \phi \text{ is zero of concatenation of languages} \quad \} \\
 & \mathit{true} \ .
\end{array}$$