CS615 Autumn 2005 Quiz 2

Time: 90 mins — ***Max marks: 20***

1. Consider the infinite set $\mathcal{C}$ of complex numbers of the form $x + i.y$, where $i = \sqrt{-1}$, and x and y are either integers or belong to the set $\{+\infty, -\infty\}$. We will assume that $-\infty < x < +\infty$ for all integers x. We define a partial order $\sqsubseteq$ between elements of this set as follows:
$(x_1 + i.y_1) \sqsubseteq (x_2 + i.y_2)$ if and only if $x_1 \leq x_2$ and $y_1 \geq y_2$. We claim that this partial order forms a complete lattice $\mathcal{L} = (\mathcal{C}, \sqsubseteq)$.

   (a) *[0.5 + 0.5 mark]* What are the top ($\top$) and bottom ($\bot$) elements of $\mathcal{L}$? You must show that there cannot exist any element $x + i.y$ in $\mathcal{L}$ such that $(x + i.y) \sqsubseteq \bot$ and $(x + i.y) \neq \bot$ or $\top \sqsubseteq (x + i.y)$ and $(x + i.y) \neq \top$?

Solution: The first thing to note is that the ordering between elements in $\mathcal{C}$ is best visualized by drawing a pair of axes as shown in Fig. 1.

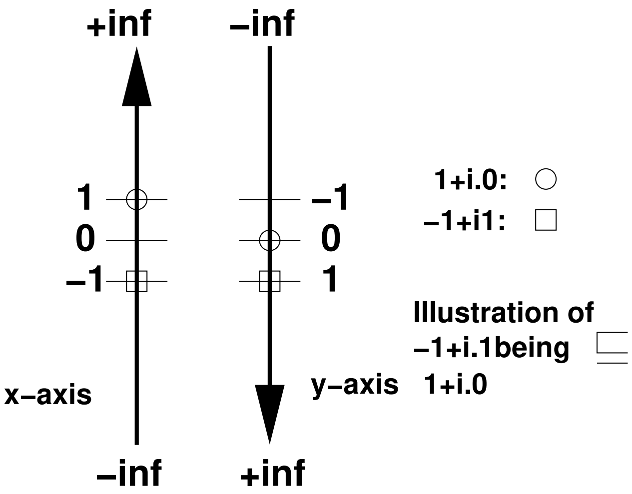

Figure 1:

Every point in $\mathcal{C}$ corresponds to a pair of points – one from the left axis (in which values increase from below to above), and one from the right axis (in which values increase from above to below). With this view, $x + i.y \sqsubseteq x' + i.y'$ iff x is not above x' on the left axis and y is not above y' on the right axis in Fig. 1.
Once you have this picture in mind, the rest of the solutions follow rather easily.
For example, it is easy to see from Fig. 1 that $\top = +\infty, +i.(-\infty)$ and $\bot = -\infty + i.(+\infty)$. Since there exists no integer $x > +\infty$ and no integer $y < -\infty$, it follows that there is no element $x + i.y$ that is either $\sqsubseteq \bot$ and $\neq \bot$, or $\sqsupseteq \top$ and $\neq \top$.

   (b) *[1 + 1 marks]* Give a suitable definition of $lub(x_1 + i.y_1, x_2 + i.y_2)$ and $glb(x_1 + i.y_1, x_2 + i.y_2)$ in this lattice. Justify why your definitions give the *least* and *greatest* bounds respectively.

Solution: From Fig. 1, it is intuitive to see that $lub(x_1 + i.y_1, x_2 + i.y_2) = \max(x_1, x_2) + i.\min(y_1, y_2)$ and $glb(x_1 + i.y_1, x_2 + i.y_2) = \min(x_1, x_2) + i.\max(y_1, y_2)$.
Justification for $lub(x_1 + i.y_1, x_2 + i.y_2) = \max(x_1, x_2) + i.\min(y_1, y_2)$:

   i. Clearly, $\max(x_1, x_2) \geq x_i$ and $\min(y_1, y_2) \leq y_i$ for $i \in \{1, 2\}$. So, $\max(x_1, x_2) + i.\min(y_1, y_2)$ is an upper bound of $x_1 + i.y_1$ and $x_2 + i.y_2$.
   ii. Let $x_3 + i.y_3$ be an upper bound of $x_1 + i.y_1$ and $x_2 + i.y_2$. By definition, $x_3 \geq x_1$, $y_3 \leq y_1$, $x_3 \geq x_2$ and $y_3 \leq y_2$. Therefore, $x_3 \geq \max(x_1, x_2)$ and $y_3 \leq \min(y_1, y_2)$. Hence, $x_3 + i.y_3 \sqsupseteq$

$\max(x_1, x_2) + i.\min(y_1, y_2)$, showing that $\max(x_1, x_2) + i.\min(y_1, y_2)$ is indeed the *least* upper bound.

The justification for $glb(x_1 + i.y_1, x_2 + i.y_2) = \min(x_1, x_2) + i.\max(y_1, y_2)$ is similar and left as an exercise.

(c) *[3 marks – **cancelled**]* Consider the function $f : \mathcal{C} \to \mathcal{C}$ such that $f(x + i.y) = (x^2 + i.(-y^2))$, where we define $(-\infty)^2 = (+\infty)^2 = +\infty$. Show that this function is *not* monotonic in the lattice $\mathcal{L}$.

Solution: By the definition of $\sqsubseteq$, $-1 + i.1 \sqsubseteq 0 + i.0$. By definition, $f(-1 + i.1) = 1 + i.(-1)$ and $f(0 + i.0) = 0 + i.0$ (incidentally, also showing that $0 + i.0$ is a fixed point). Since $1 + i.(-1) \not\sqsubseteq 0 + i.0$, we have $f(-1 + i.1) \not\sqsubseteq f(0 + i.0)$ although $-1 + i.1 \sqsubseteq 0 + i.0$. This shows that f is not monotonic.

(d) *[1 + 1 marks]* What are the least and greatest fixed points of f as defined above in lattice $\mathcal{L}$?

Solution: Let $x + i.y$ be a fixed point of f. Then, $f(x + i.y) = x + i.y$. In other words, $x^2 + i.(-y^2) = x + i.y$. It follows that $x^2 = x$ and $-y^2 = y$. This gives $x \in \{0, 1, +\infty\}$ and $y \in \{0, -1, -\infty\}$. Thus, there are a total of 9 fixed points of f corresponding to pairs in $\{0, 1, +\infty\} \times \{0, -1, -\infty\}$.
To find the least fixed point, we must minimize the $x-$ component and maximize the $y-$ component. To find the greatest fixed point, we must do it the other way around.
Therefore, $lfp(f) = 0 + i.0$ and $gfp(f) = \top = +infty + i.(\infty)$.
This shows that the least and greatest fixed points may exist even if f is not monotonic. Thus, the monotonicity of f is a sufficient, not a necessary, condition for the greatest and least fixed points to exist.

(e) *[5 marks]* Now consider the lattice $2^{\mathcal{L}} = (2^{\mathcal{C}}, \subseteq)$ of subsets of $\mathcal{C}$ with the usual set inclusion relation. We wish to define a Galois connection between the lattices $2^{\mathcal{L}}$ and $\mathcal{L}$. Let the abstraction function $\alpha : 2^{\mathcal{C}} \to \mathcal{C}$ be defined as $\alpha(S) = lub(S)$. Define an appropriate concretization function γ so that the pair (α, γ) forms a Galois connection between $2^{\mathcal{L}}$ and $\mathcal{L}$. Show that all the conditions of a Galois connection are satisfied with your definition.

Solution: It is useful to refer back to Fig. 1 here.
Since $\alpha(S) = lub(S)$, it means $\alpha(S) = \max_{x+i.y \in S}(x) + i.\min_{x+i.y \in S}(y)$. Therefore, given an element in $\mathcal{L}$, say $m + i.n$, an appropriate concretization function γ must give back the largest set of points in $\mathcal{L}$ whose lub is $m + i.n$. In other words, we want all those points $x + i.y$ which are such that m is the maximum $x-$ component and n is the minimum $y-$ component of any point. Therefore, $\gamma(m + i.n) = \{x + i.y \mid (x \leq m) \wedge (y \geq n)\}$.
To see that (α, γ) form a Galois connection, we just need to prove the following four properties:

i. α is monotonic: Let $A, B \in 2^{\mathcal{L}}$ and let $A \subseteq B$. Recall that $\alpha(S) = lub(S) = \max_{x+i.y \in S}(x) + i.\min_{x+i.y \in S}(y)$ for all $S \in 2^{\mathcal{L}}$. Since $A \subseteq B$, $\max_{x+i.y \in A}(x) \leq \max_{x+i.y \in B}(x)$, and $\min_{x+i.y \in A}(y) \geq \min_{x+i.y \in B}(y)$. Therefore, $lub(A) \sqsubseteq lub(B)$.

ii. γ is monotonic: Consider $x + i.y$ and $m + i.n$ in $\mathcal{L}$ such that $x + i.y \sqsubseteq m + i.n$. In other words, $x \leq m$ and $y \geq n$. We want to show that $\gamma(x + i.y) \subseteq \gamma(m + i.n)$. Let $p + i.q \in \gamma(x + i.y)$. Then, by definition of γ above, $p \leq x$ and $q \geq y$. But since $x \leq m$ and $y \geq n$, we also have $p \leq m$ and $q \geq n$. It follows that $p + i.q$ must also be in $\gamma(m + i.n)$. Hence, $\gamma(x + i.y) \subseteq \gamma(m + i.n)$.

iii. $\gamma(\alpha(S)) \supseteq S$ for all $S \in 2^{\mathcal{L}}$: Let $S \in 2^{\mathcal{L}}$ and let $p + i.q = \alpha(S) = lub(S)$, Consider a point $x + i.y \in S$. By definition of the lub, $p \geq x$ and $q \leq y$. Since $\gamma(\alpha(S)) = \gamma(p + i.q) = \{s + i.t \mid (s \leq p) \wedge (t \geq q)\}$, it follows that $x + i.y \in \gamma(\alpha(S))$. Therefore, if $x + i.y \in S$, it is also in $\gamma(\alpha(S))$, i.e., $\gamma(\alpha(S)) \supseteq S$

iv. $\alpha(\gamma(p + i.q)) \sqsubseteq p + i.q$ for all $p + i.q \in \mathcal{L}$: By definition, $\gamma(p + i.q) = \{s + i.t \mid (s \leq p) \wedge (t \geq q)\}$. Therefore, $\alpha(\gamma(p + i.q)) = lub(\gamma(p + i.q)) = p + i.q$.

(f) *[7 marks]* Consider the function $g : 2^{\mathcal{C}} \to 2^{\mathcal{C}}$ defined as $g(S) = \{1 + i.1\} \cup (\{1 + i.(-1)\} \cap \{f(x + i.y) \mid (x + i.y) \in S\})$. Find an upper approximation to the least fixed point of g using abstract interpretation, where the abstract domain is $\mathcal{L}$ and the Galois connection between $2^{\mathcal{L}}$ and $\mathcal{L}$ is as defined above. You must show all steps of your calculation.

Solution: The first observation we make is that $\{1+i.(-1)\} \cap \{f(x+i.y) \mid (x+i.y) \in S\}$ is either $\{1+i.(-1)\}$ or $\emptyset$. Therefore, for any S, $g(S)$ is either $\{1+i.1\}$ or $\{1+i.1, 1+i.(-1)\}$.

Next, we note that since $f(x+i.y) = x^2 + i.(-y^2)$, for $\{f(x+i.y) \mid (x+i.y) \in S\}$ to have a non-empty intersection with $\{1+i.(-1)\}$, at least one of $\{1+i.1, 1+i.(-1), (-1)+i.1, (-1)+i.(-1)\}$ must be present in S. Therefore, if $S \cap \{1+i.1, 1+i.(-1), (-1)+i.1, (-1)+i.(-1)\} \neq \emptyset$, $g(S) = \{1+i.1, i+i.(-1)\}$. In all other cases, $g(S) = \{1+i.1\}$.

Let $G : \mathcal{C} \rightarrow \mathcal{C}$ be the abstract function corresponding to g. We know that $G(p+i.q) = \alpha(g(\gamma(p+i.q)))$ – recall that $G = \alpha \circ g \circ \gamma$.

By definition, $\gamma(p+i.q) = \{s+i.t \mid (s \leq p) \wedge (t \geq q)\}$. Therefore, $\gamma(p+i.q)) \cap \{1+i.1, 1+i.(-1), (-1)+i.1, (-1)+i.(-1)\} \neq \emptyset$ iff $p \geq -1$ and $q \leq 1$. Hence, $g(\gamma(p+i.q)) = \{1+i.1, 1+i.(-1)\}$ if $p \geq -1$ and $q \leq 1$; otherwise, $g(\gamma(p+i.q)) = \{1+i.1\}$. It follows that $G(p+i.q) = \alpha(g(\gamma(p+i.q))) = lub(g(\gamma(p+i.q)))$ equals $1+i.(-1)$ if $p \geq -1$ and $q \leq 1$, and equals $1+i.1$ otherwise. We have thus obtained a crisp definition of G.

To find an upper approximation to the least fixed point of g, we must compute the least fixed point of G and then concretize it using γ. To compute the lfp of G, we start by computing $G(\perp_{\mathcal{L}}) = G(-\infty + i.(+\infty))$, and then keep applying G until a fixed point is reached. Using the definition of G obtained above, we get $G(-\infty + i.(+\infty)) = 1+i.1$, $G(1+i.1) = 1+i.(-1)$ and $G(1+i.(-1)) = 1+i.(-1)$. Therefore, $lfp(G) = 1+i.(-1)$.

It follows that an upper approximation to $lfp(g)$ is $\gamma(1+i.(-1)) = \{x+i.y \mid (x \leq 1) \wedge (y \geq -1)\}$. If you tried computing the lfp of g directly, you would see that it is $\{1+i.1, 1+i.(-1)\}$. So the above result is definitely an upper-approximation (not very good though) of $lfp(g)$.