Names and Matriculation numbers :
Amrita Bhattacherjee - 441338
Debabrata Ghosh - 441275
Ilya Fradlin - 441264

Probabilistic Programming
Exercise Sheet 4 Solutions
Group 7

P.S. Solutions start from next page!

1.

(a) Given, a Markov Chain $D = (\Sigma, \sigma_I, P)$ with goal set $G \subseteq \Sigma$
Define $\Sigma_? = \Sigma \setminus G$, matrix $A = (a_{ij}) = (P(\sigma,\tau))_{\sigma,\tau \in \Sigma_?}$ and vector $\underset{\sim}{b} = (b_\sigma)_{\sigma \in \Sigma_?}$
where $b_\sigma = \sum_{\gamma \in G} P(\sigma, \gamma)$

We define a partial order on the vectors in V, where these vectors have entries indexed by the states in $\Sigma_?$ with functions of type $\Sigma_? \to [0,1]$.
The partial order is as follows —

$$(V, \text{"}\sqsubseteq\text{"}), \text{ where } \underset{\sim}{v}_1 \sqsubseteq \underset{\sim}{v}_2 \Rightarrow \text{every element of } \underset{\sim}{v}_1 \leq \text{every element of } \underset{\sim}{v}_2 \;;$$

$$\underset{\sim}{v}_1, \underset{\sim}{v}_2 \in V.$$

Note that, every vector in V is of order $|\Sigma_?| \times 1$.

<u>Proof that $(V, \text{"}\sqsubseteq\text{"})$ is a partial order</u> :—

- For all $\underset{\sim}{x} \in V$, $\underset{\sim}{x} = \underset{\sim}{x}$; hence reflexive
- For any $\underset{\sim}{x}_1, \underset{\sim}{x}_2, \underset{\sim}{x}_3 \in V$,

$$x_{1i} \leq x_{2i} \;\forall i = 1(1)|\Sigma_?| \text{ and, } x_{2i} \leq x_{3i} \;\forall i = 1(1)|\Sigma_?| \Rightarrow x_{1i} \leq x_{3i} \;\forall i = 1(1)|\Sigma_?|$$

$\therefore$ $\underset{\sim}{x}_1 \sqsubseteq \underset{\sim}{x}_2$ and $\underset{\sim}{x}_2 \sqsubseteq \underset{\sim}{x}_3 \Rightarrow \underset{\sim}{x}_1 \sqsubseteq \underset{\sim}{x}_3$; hence transitive

- For $\underset{\sim}{x}_1, \underset{\sim}{x}_2 \in V$,
  if $x_{1i} \leq x_{2i} \;\forall i = 1(1)|\Sigma_?|$ and $x_{2i} \leq x_{1i} \;\forall i = 1(1)|\Sigma_?|$
  then $x_{1i} = x_{2i} \;\forall i = 1(1)|\Sigma_?|$

  ie, $\underset{\sim}{x}_1 \sqsubseteq \underset{\sim}{x}_2$ and $\underset{\sim}{x}_2 \sqsubseteq \underset{\sim}{x}_1 \Rightarrow \underset{\sim}{x}_1 = \underset{\sim}{x}_2$; hence anti-symmetric

Therefore, $(V, \text{"}\sqsubseteq\text{"})$ is a partial order.

<u>To prove</u> :—

$f : V \to V$; $x \mapsto Ax + b$ has a least fixed point in this order

By Kleene's fixed point theorem, f has a lfp if —

- $(V, \text{"}\sqsubseteq\text{"})$ is a complete lattice
- f is Scott continuous

<u>Complete lattice</u> —

Here, V is a set of vectors where the vectors have dimension $|\Sigma| \times 1$ and entries in $[0,1]$. Therefore, there exists a well defined order between every pair of elements under $(V, \text{"}\sqsubseteq\text{"})$. Since D is a finite state MC, therefore every subset S has a supremum and infimum in D wrt the relation "$\sqsubseteq$".

Hence, $(V, \sqsubseteq)$ is a complete lattice.

<u>Scott continuity</u> —

We have $f : V \to V : x \mapsto Ax + b$, where A and b are as defined above.

Let, $x_0 = \sqcup S$, where $S \subseteq V$ is a non-empty chain.

Then, $f(x_0) = Ax_0 + b \sqsubseteq Ax + b \;\; \forall x \neq x_0$ and $x \in V$, since A is positive semi-definite and every element of b is non-negative.

Therefore, order of elements in S are preserved under f. In fact, S is clearly finite. Hence —

$$f(\sqcup S) = \sqcup f(S) \Rightarrow f \text{ is Scott-continuous}$$

w.r.t. this order $(V, \text{"}\sqsubseteq\text{"})$. ∎

$\therefore$ By Kleene's fixpoint theorem, f has lfp

<u>(b)</u>. By Kleene's fixed point theorem, we can approximate the lfp of f by iteratively applying f as follows —

0 : Apply f to $\perp = \underset{\sim}{0}$

1 : Calculate $f(\perp) = b$

2. : Calculate $f(f(\perp)) = f(b) = A\underset{\sim}{b} + \underset{\sim}{b}$

3 : Calculate $f^3(\perp)$, $f^4(\perp)$ and so on

4 : For a large enough $n \in \mathbb{N}$, we should be able to reach lfp $f := \bigsqcup_{n \in \mathbb{N}} f^n(\perp)$

In fact, we essentially calculate —

$$f^n(\perp) = A^{n-1}\underset{\sim}{b} + A^{n-2}\underset{\sim}{b} + \dots + A\underset{\sim}{b} + \underset{\sim}{b}$$

and take $\bigsqcup_{n \in \mathbb{N}} f^n(\perp)$.

2) a) $P:\quad \texttt{if}\ (x>0)\ \{\ x := y+1\ \}\ \texttt{else}\ \{\ \texttt{if}\ (x=0)\ \{\ \texttt{skip}\ \}\ \texttt{else}\ \{\ x := x+1\ \}\ \}$

using Backward Reasoning:

$$wp\,[\![\text{if}(x>0)\{x:=y+1\}\text{else}\{\text{if}(x=0)\{\text{skip}\}\text{else}\{x:x+1\}\}]\!](x>y)$$

$$= ((x>0)\wedge wp[\![x:=y+1]\!](x>y))\vee((x\leq 0)\wedge wp[\![\text{if}(x=0)\{\text{skip}\}\text{else}\{x:=x+1\}]\!](x>y))$$

$$= \underbrace{((x>0)\wedge\underbrace{(y+1>y)}_{\text{true}})}_{(x>0)}\vee((x\leq 0)\wedge(((x=0)\wedge wp[\![\text{skip}]\!](x>y))\vee((x\neq 0)\wedge wp[\![x:=x+1]\!](x>y))))$$

$$= (x>0)\ \vee((x\leq 0)\wedge(x=0)\wedge(x>y))\vee((x\neq 0)\wedge(x+1>y))$$

$$= (0>y)\vee((x\neq 0)\wedge(x+1>y))$$

---

b) $P:\quad \texttt{while}\ (x\geq 1)\ \{\ a := a*x;\ x := x-1\ \}$

$f:\quad a = x!$

The loop characteristic function $\Phi_F(f)$ is:

$$((x\geq 1)\wedge wp[\![a:=a*x\ ;\ x:=x-1]\!](\ X\ ))\vee((x<1)\wedge(a=x!))$$

weve seen in the lecture that $\Phi_F : \mathbb{P}\to\mathbb{P}$ is scott continuous.
using kleene's fixed point theorem we get:

$$\text{lfp}_{\sqsubseteq}\,\Phi_F = \sup_{n\in\mathbb{N}}\ \Phi_F^n(\text{false})$$

$\perp$ in $(\mathbb{P}, \Rightarrow)$

$$\Rightarrow \Phi_f(False) = \Big(\underbrace{(x \geq 1) \land \underbrace{wp[\![a := a*x\ ;\ x := x-1]\!](false)}_{false}}_{false}\Big) \lor \big((x < 1) \land (a = x!)\big)$$

$$= (x<1) \land (a = x!)$$

$$\Phi_f^2(false) = \Phi_f((x<1) \land (a = x!)) =$$

$$= \big((x \geq 1) \land wp[\![a := a\cdot x\ ;\ x := x-1]\!]((x<1) \land (a = x!))\big) \lor \big((x < 1) \land (a = x!)\big)$$

$$= \big((x \geq 1) \land wp[\![a := a\cdot x]\!]((x<2) \land (a = (x-1)!))\big) \lor ((x<1) \land (a = x!))$$

$$= \big((x\geq 1) \land ((x<2) \land (ax = (x-1)!))\big) \lor ((x<1) \land (a = x!))$$

$$= \big((x = 1) \land (ax = (x-1)!)\big) \lor ((x<1) \land (a = x!))$$

$$= (a=1) \lor ((x<1) \land (a = x!))$$

$$\Phi^3(false) = \Phi_f\big((a=1) \lor (x<1) \land (a = x!)\big) =$$

$$= \big((x \geq 1) \land wp[\![a := a\cdot x\ ;\ x := x-1]\!]((a=1) \lor (x<1) \land (a = x!))\big) \lor \big((x < 1) \land (a = x!)\big)$$

$$= \big((x \geq 1) \land wp[\![a := a\cdot x]\!]((a=1) \lor ((x<2) \land (a = (x-1)!)))\big) \lor ((x<1) \land (a = x!))$$

$$= ((x \geq 1) \land ((ax = 1) \lor (x<2) \land (ax = (x-1)!))) \lor ((x<1) \land (a = x!))$$

$$= ((a = 1) \lor ((x<1) \land (a = x!))$$

$\Longrightarrow$ Thus, by computing the loop-characteristing functional $\Phi_f(f)$, we found, using Kleene's fixed point theorem ~~that~~ $wp(p, f)$ is in fact $(a=1) \vee ((x<1) \wedge (a=x!_0))$

(3) Monotonicity of weakest pre-expectations

(a) $(D, \sqsubseteq)$ - a complete lattice and $f, g : D \to D$ monotonic such that $\forall\, d \in D,\ f(d) \sqsubseteq g(d)$.

Using extended Knaster-Tarski Theorem, we can directly write $\text{lfp}\, f = \sqcap S$, where $S = \{d \in D \mid f(d) \sqsubseteq d\}$.

Also, $\text{lfp}\ g = \sqcap S'$, where $S' = \{d \in D \mid g(d) \sqsubseteq d\}$

Consider any such S' as above. $\forall\, d \in S' \subseteq D$, $f(d) \sqsubseteq g(d) \sqsubseteq d$. This means all elements d in any set S' also satisfies $\{d \in D \mid f(d) \sqsubseteq d\}$.

So, we have more sets $S = \{d \in D \mid f(d) \sqsubseteq d\}$ than sets S' satisfying $S' = \{d \in D \mid g(d) \sqsubseteq d\}$.

Now, since $\sqcap S$ or $\sqcap S'$ represents intersections of such states and we have more sets likes S than S', by basic properties of intersection $\sqcap S \sqsubseteq \sqcap S'$ which gives us

$$\text{lfp}\ f = \sqcap S \sqsubseteq \sqcap S' = \text{lfp}\ g$$

$$\Rightarrow \text{lfp}\ f \sqsubseteq \text{lfp}\ g \qquad \square$$

(b) For any GCL program P, the function $wp(P) : \mathbb{P} \to \mathbb{P}$ takes a predicate as postcondition and returns the predicate which is the weakest precondition of P w.r.t to the given postcondition.

We consider the ordering $\sqsubseteq = \Rightarrow$ on $\mathbb{P}$.

So, we have $F \sqsubseteq G$ iff $F \Rightarrow G$.

Now, $wp[\![P]\!](F)$ refers to the precondition that reaches/terminates in a state $t \models F$

and hence $wp[\![P]\!](F) \Rightarrow F$

By transitivity of $\Rightarrow$

$wp[\![P]\!](F) \Rightarrow G$ . . . . . . (1)

Similarly, $wp[\![P]\!](G)$ refers to the pre-condition that reaches a state $s \models G$, which gives us $wp[\![P]\!](G) \Rightarrow G$ . . . (2)

So if $H = wp[\![P]\!](G)$, then P starts in state $r \models H$ and terminates in a state $s \models G$.

Now for the post condition G, H can be wp iff. P starts in a state in H and terminates in G. Considering that P can also start from a state in $wp[\![P]\!](F)$ and terminate at G (by ①), either H and $wp[\![P]\!](F)$ are same or $wp[\![P]\!](F)$ can reach H, meaning

$$wp[\![P]\!](F) \Rightarrow H = wp[\![P]\!](G)$$

which proves that $wp(P) : \mathbb{P} \to \mathbb{P}$ is monotonic. $\square$

④ Weakest liberal pre-conditions

ⓐ Without using the diverge statement a GCL program P along with a post-condition f can be such that $wp(P, f) \neq wlp(P, f)$ if we have a loop in the program P as $\forall$ loop-free P $\forall f$, $wlp[\![P]\!](f) = wp[\![P]\!](f)$ by construction.

Consider the following program:

P: while $(x \neq 0)$ $\{ x := x - 1 \}$ and

post-condition

f: $x := 0$.

We can see, to calculate $wp(P, f)$, $\Phi(X) = (x = 0 \wedge x = 0) \vee (x \neq 0 \wedge wp[\![x := x-1]\!](X))$

$$= (x = 0) \vee (x \neq 0 \wedge wp[\![x := x-1]\!](X))$$

$\Phi^0(false) = false$, $\Phi^1(false) = (x = 0) \vee (x \neq 0 \wedge wp[\![x := x-1]\!](false))$

$$= (x = 0) \vee (x \neq 0 \wedge false)$$

$$= (x = 0) \vee false = (x = 0)$$

$\Phi^2(false) = (x = 0) \vee (x \neq 0 \wedge wp[\![x := x-1]\!](x = 0))$

$$= (x = 0) \vee (x \neq 0 \wedge x - 1 = 0)$$

$$= (x = 0) \vee (x = 1)$$

. . . .

$\Phi^n(false) = (x = 0) \vee (x = 1) \dots \vee (x = n)$

$$\Rightarrow \sup_{n \in \mathbb{N}} \Phi^n(false) = \bigvee_{k=0}^{n} (x = k) = x \geq 0,$$

or $x \in \mathbb{N}$

So, starting with $x \geq 0$ terminates with $x = 0$, starting with $x < 0$ doesn't terminate.

While $wlp(P, f) = true$

So, $wp(P, f) \neq wlp(P, f)$.

(6) P: while $(x \neq 0)$ $\{x := x-2\}$

$$\underbrace{\varphi(X) = (x=0 \wedge f) \vee (x \neq 0 \wedge wlp[\![x := x-2]\!](X))}_{\text{loop characteristics fn } \Psi_f(x)}$$

$wlp[\![P]\!](f) = gfp\, X.\ \Psi_f(X)$.

We know from construction of wlp and Kleene's fixed-point theorem that $gfp\ \Psi_f = \inf_{n \in \mathbb{N}} \Psi_f^{\,n}(true)$

Let us perform the fixed point iteration for φ as:

0. $\varphi^0(true) = true$

1. $\varphi^1(true) = (x=0 \wedge f) \vee (x \neq 0 \wedge wlp[\![x := x-2]\!](true))$

$= (x=0 \wedge f) \vee (x \neq 0 \wedge true)$

$= (x=0 \wedge f) \vee (x \neq 0)$

We can consider $f: x := 2n+1$, $n \in$ Integer

i.e. $x := \pm 1, \pm 3, \pm 5, \ldots$

Assume $x := 1$ WLOG,

$\varphi^1(true) = (x := 0 \wedge x = 1) \vee (x \neq 0)$

$= (x \neq 0)$

$\varphi^2(true) = (x=0 \wedge f) \vee (x \neq 0 \wedge wlp[\![x := x-2]\!](x \neq 0))$

$= (x=0 \wedge x=1) \vee (x \neq 0 \wedge x-2 \neq 0)$

$=$ false $\vee (x(x-2) \neq 0)$

$= x(x-2) \neq 0$.

In this way we'll get $x(x-2) \ldots (x-2n) \neq 0$.

Now, we can see that P does not terminate if $x(x-2) \ldots (x-2n) \neq 0$, which is true for all $x :=$ odd numbers! i.e. $x := 2n+1$, $n \in I$.

ⓒ Rules for constructing the wlp (weakest liberal pre-condition) gives us that for atomic program lines skip & (assignment) $x := E$ the rules are exactly the same. For the remaining programs without the existence of loop, definitions differ only in the fact that we use wlp instead of wp on the program lines. So, in case of non-termination which only happens for loops both wp and wlp are structurally same.

So, for $\forall$ loop-free P $\forall_{\text{post-condition}} f$, $wp(P, f) = wlp(P, f)$.

Now when we look at while rule we can prove:

$$(\star)\begin{cases} lfp X. ((\varphi \wedge wlp[\![P]\!](X)) \vee (\neg\varphi \wedge f)) \\ \sqsubseteq gfp X. ((\varphi \wedge wlp[\![P]\!](X)) \vee (\neg\varphi \wedge f)) \end{cases}$$

which actully will correspond to what we want to prove: (by defenition)

$$(1) \quad wp(P, f) \sqsubseteq wlp(P, f).$$

using the hint in the question we know that wlp is monotonic, thus by using knaster Tarski, we know all the fixed points are forming a complete lattice thus

The order $(\star)$ holds proving the order (1) we were asked.