Due: Thu, 19th March, 12:00 noon

Submission is through give and should be a single pdf file, maximum size 4Mb. Prose should be typed, not handwritten. Use of LaTeX is encouraged, but not required. See the course website for detailed submission instructions.

Discussion of assignment material with others is permitted, but the work submitted *must* be your own in line with the University's plagiarism policy.

Problem 1 (20 marks)

Recall the relation composition operator ; defined as:

$$R_1; R_2 = \{(a, c) \mid \text{there is a } b \text{ with } (a, b) \in R_1 \text{ and } (b, c) \in R_2\}$$

For any set S, and any binary relations $R_1, R_2, R_3 \subseteq S \times S$, prove or give a counterexample to disprove the following:

(a) $(R_1; R_2); R_3 = R_1; (R_2; R_3)$ (4 marks)

(b) $I; R_1 = R_1; I = R_1$ where $I = \{(x, x) \mid x \in S\}$ (4 marks)

(c) $(R_1; R_2)^{\leftarrow} = R_1^{\leftarrow}; R_2^{\leftarrow}$ (4 marks)

(d) $(R_1 \cup R_2); R_3 = (R_1; R_3) \cup (R_2; R_3)$ (4 marks)

(e) $R_1; (R_2 \cap R_3) = (R_1; R_2) \cap (R_1; R_3)$ (4 marks)

Solution

(a) We have:

$$
\begin{array}{lll}
(a,d) \in (R_1;R_2);R_3 & \text{iff} & \text{there exists } c \in S \text{ such that } (a,c) \in R_1;R_2 \text{ and } (c,d) \in R_3 \\
& \text{iff} & \text{there exists } b,c \in S \text{ such that } (a,b) \in R_1 \text{ and } (b,c) \in R_2 \text{ and } (c,d) \in R_3 \\
& \text{iff} & \text{there exists } b \in S \text{ such that } (a,b) \in R_1 \text{ and } (b,d) \in R_2;R_3 \\
& \text{iff} & (a,d) \in R_1;(R_2;R_3)
\end{array}
$$

(b) Suppose $(a,b) \in R$. Then, because $(a,a) \in I$ we have $(a,b) \in I;R$. Also, because $(b,b) \in I$ we have $(a,b) \in R;I$.

Now suppose $(a,b) \in I;R$. Then there exists $c \in S$ such that $(a,c) \in I$ and $(c,b) \in R$. But from the definition of I, the only such c is $c = a$, so $(a,b) \in R$.

Finally suppose $(a,b) \in R;I$. Then there exists $c \in S$ such that $(a,c) \in R$ and $(c,b) \in I$. Again, from the definition of I, the only such c is $c = b$, so $(a,b) \in R$.

(c) This is not correct. Consider $S = \{a,b,c\}$, $R_1 = \{(a,b)\}$ and $R_2 = \{(b,c)\}$. Then,

$$
\begin{array}{ccc}
R_1;R_2 = \{(a,c)\} & & (R_1;R_2)^{\leftarrow} = \{(c,b)\} \\
R_1^{\leftarrow} = \{(b,a)\} & R_2^{\leftarrow} = \{(b,c)\} & R_1^{\leftarrow};R_2^{\leftarrow} = \emptyset
\end{array}
$$

It is in fact possible to show that $(R_1;R_2)^{\leftarrow} = R_2^{\leftarrow};R_1^{\leftarrow}$.

(d) We have:

$$
\begin{array}{lll}
(a,c) \in (R_1 \cup R_2);R_3 & \text{iff} & \text{there exists } b \in S \text{ such that } (a,b) \in R_1 \cup R_2 \text{ and } (b,c) \in R_3 \\
& \text{iff} & \text{there exists } b \in S \text{ such that } (a,b) \in R_1 \text{ and } (b,c) \in R_3\text{, or} \\
& & \quad \text{there exists } b \in S \text{ such that } (a,b) \in R_2 \text{ and } (b,c) \in R_3 \\
& \text{iff} & (a,c) \in R_1;R_3 \text{ or } (a,c) \in R_2;R_3 \\
& \text{iff} & (a,c) \in R_1;R_3 \cup R_2;R_3
\end{array}
$$

(e) This is not correct. Consider $S = \{a,b,c,d\}$ with $R_1 = \{(a,b),(a,c)\}$, $R_2 = \{(b,d)\}$, and $R_3 = \{(c,d)\}$. Then

$$
\begin{array}{ccc}
R_2 \cap R_3 = \emptyset & & R_1;(R_2 \cap R_3) = \emptyset \\
R_1;R_2 = \{(a,d)\} & R_1;R_3 = \{(a,d)\} & R_1;R_2 \cap R_1;R_3 = \{(a,d)\}
\end{array}
$$

Problem 2 (30 marks)

Let $R \subseteq S \times S$ be any binary relation on a set S. Consider the sequence of relations $R^0, R^1, R^2, \ldots$, defined as follows:

$$
\begin{array}{rcl}
R^0 & := & I = \{(x,x) \mid x \in S\}, \text{ and} \\
R^{i+1} & := & R^i \cup (R;R^i) \text{ for } i \geq 0
\end{array}
$$

(a) Prove that if there is an i such that $R^i = R^{i+1}$, then $R^j = R^i$ for all $j \geq i$. (4 marks)

(b) Prove that if there is an i such that $R^i = R^{i+1}$, then $R^k \subseteq R^i$ for all $k \geq 0$. (4 marks)

(c) Let $P(n)$ be the proposition that for all $m \in \mathbb{N}$: $R^n;R^m = R^{n+m}$. Prove that $P(n)$ holds for all $n \in \mathbb{N}$. (8 marks)

(d) If $|S| = k$, explain why $R^k = R^{k+1}$. (*Hint: Show that if* $(a, b) \in R^{k+1}$ *then* $(a, b) \in R^i$ *for some* $i < k + 1$.) (4 marks)

(e) If $|S| = k$, show that R^k is transitive. (4 marks)

(f) If $|S| = k$, show that $(R \cup R^{\leftarrow})^k$ is an equivalence relation. (6 marks)

Solution

(a) Suppose $R^i = R^{i+1}$. Let $P(j)$ be the proposition that $R^j = R^i$. We will prove that $P(j)$ holds for all $j \geq i$.

Base case $j = i$: Clearly $P(i)$ holds as $R^i = R^i$.

Inductive case. Suppose $P(j)$ holds, that is, $R^j = R^i$ for some $j \geq i$. We will show that $P(j+1)$ holds. We have:

$$\begin{aligned} R^{j+1} &= R^j \cup (R; R^j) && \text{(Definition)} \\ &= R^i \cup (R; R^i) && \text{(IH)} \\ &= R^{i+1} && \text{(Definition)} \\ &= R^i && \text{(Given)} \end{aligned}$$

So $P(j)$ implies $P(j+1)$. So by the principle of mathematical induction, $P(j)$ holds for all $j \geq i$.

(b) We first show that if $k \leq j$ then $R^k \subseteq R^j$. We prove this (for any k) by induction on j:

Base case $j = k$: Clearly $R^k \subseteq R^k$.

Inductive case: Suppose $j \geq k$ and $R^k \subseteq R^j$. Then

$$R^k \subseteq R^j \subseteq R^j \cup (R; R^j) = R^{j+1}.$$

Therefore, by the principle of induction, for all k, j, if $k \leq j$ then $R^k \subseteq R^j$.

It follows that if $R^i = R^{i+1}$ then for $k \leq i$ we have $R^k \subseteq R^i$, and for $k \geq i$ we have (from (a)) that $R^k = R^i \subseteq R^i$.

Solution (ctd)

(c) We will prove $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base case $n = 0$: For all m,

$$\begin{aligned} R^{0+m} &= R^m \\ &= I; R^m && \text{(From Q1(b))} \\ &= R^0; R^m && \text{(Def. of } R^0\text{)} \end{aligned}$$

Inductive case. Suppose $P(n)$ holds, that is, for all m, $R^n; R^m = R^{n+m}$. We have, for all m:

$$\begin{aligned} R^{n+1}; R^m &= ((R^n \cup (R; R^n)); R^m && \text{(Definition)} \\ &= (R^n; R^m) \cup ((R; R^n); R^m) && \text{(From Q1(d))} \\ &= (R^n; R^m) \cup (R; (R^n; R^m)) && \text{(From Q1(a))} \\ &= R^{n+m} \cup (R; R^{n+m}) && \text{(IH)} \\ &= R^{n+m+1} && \text{(Definition)} \\ &= R^{(n+1)+m} \end{aligned}$$

So $P(n+1)$ holds. Therefore, by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$.

(d) From (b) we have that $R^k \subseteq R^{k+1}$. We will show that $R^{k+1} \subseteq R^k$.

We observe that $(a, b) \in R^j$ if and only if there exists $c_0, \ldots, c_p \in S$, with $p \leq j$, $a = c_0$, $b = c_p$ and $(c_i, c_{i+1}) \in R$ for all $i \in [0, p]$.

Therefore, if $(a, b) \in R^{k+1}$ then either $p \leq k$, in which case $(a, b) \in R^p \subseteq R^k$; or $p = k + 1$. In the latter case, if $|S| = k$ then there must exist $q, r \in [0, p]$ with $q < r$ and $c_q = c_r$. But then the we have $c_0, c_1, \ldots c_q, c_{r+1}, c_{r+2}, \ldots c_p$ as a sequence of $p - (r - q) < k + 1$ elements of S meeting the above observation. Therefore $(a, b) \in R^{p-(r-q)} \subseteq R^k$.

(e) From (d) we have that if $|S| = k$ then $R^k = R^{k+1}$. Now suppose $(a, b) \in R^k$ and $(b, c) \in R^k$. Then

$$\begin{aligned} (a, c) &\in R^k; R^k && \text{(Definition of ;)} \\ &= R^{2k} && \text{(From (c))} \\ &= R^k && \text{(From (a))} \end{aligned}$$

So R^k is transitive.

(f) We need to show that $(R \cup R^{\leftarrow})^k$ is reflexive, symmetric and transitive.

- From (b), we have that $I = (R \cup R^{\leftarrow})^0 \subseteq (R \cup R^{\leftarrow})^k$, so for all $a \in S$ we have that $(a, a) \in (R \cup R^{\leftarrow})^k$. Therefore $(R \cup R^{\leftarrow})^k$ is reflexive.
- From (e) we have that $(R \cup R^{\leftarrow})^k$ is transitive.
- Suppose $(a, b) \in (R \cup R^{\leftarrow})^k$. Following the observation in (d) we have that there exists $c_0, \ldots, c_p \in S$, with $p \leq k$, $a = c_0$, $b = c_p$ and $(c_i, c_{i+1}) \in R \cup R^{\leftarrow}$ for all $i \in [0, p]$. But if $(c_i, c_{i+1}) \in R \cup R^{\leftarrow}$ then $(c_{i+1}, c_i) \in R \cup R^{\leftarrow}$. Therefore, there exists $c_p, c_{p-1}, \ldots, c_0$ with $p \leq k$, $a = c_0$, $b = c_p$ and $(c_{i+1}, c_i) \in R \cup R^{\leftarrow}$ for all $i \in [0, p]$, so $(b, a) \in (R \cup R^{\leftarrow})^k$. Therefore $(R \cup R^{\leftarrow})^k$ is symmetric.

Problem 3 (22 marks)

Let PF denote the set of well-formed propositional formulae made up of propositional variables, $\top$, $\bot$, and the connectives $\neg$, $\wedge$, and $\vee$.

We define the function $\mathsf{dual}(\varphi)$ from PF to PF, which swaps $\wedge$ and $\vee$, as well as $\top$ with $\bot$. We also define $\mathsf{flip}(\varphi)$ from PF to PF, which negates any propositional variables in the formula:

$$\begin{array}{lcl@{\qquad\qquad}lcl}
\mathsf{dual}(p) & = & p & \mathsf{flip}(p) & = & \neg p \\
\mathsf{dual}(\top) & = & \bot & \mathsf{flip}(\top) & = & \top \\
\mathsf{dual}(\bot) & = & \top & \mathsf{flip}(\bot) & = & \bot \\
\mathsf{dual}(\neg\varphi) & = & \neg\mathsf{dual}(\varphi) & \mathsf{flip}(\neg\varphi) & = & \neg\mathsf{flip}(\varphi) \\
\mathsf{dual}(\varphi \wedge \psi) & = & \mathsf{dual}(\varphi) \vee \mathsf{dual}(\psi) & \mathsf{flip}(\varphi \wedge \psi) & = & \mathsf{flip}(\varphi) \wedge \mathsf{flip}(\psi) \\
\mathsf{dual}(\varphi \vee \psi) & = & \mathsf{dual}(\varphi) \wedge \mathsf{dual}(\psi) & \mathsf{flip}(\varphi \vee \psi) & = & \mathsf{flip}(\varphi) \vee \mathsf{flip}(\psi)
\end{array}$$

(a) For the formula $\varphi = p \vee (q \wedge \neg r)$:

(i) What is $\mathsf{dual}(\varphi)$? (4 marks)

(ii) What is $\mathsf{flip}(\varphi)$? (4 marks)

Solution

(i)

$$\begin{array}{rcl}
\mathsf{dual}(\varphi) & = & \mathsf{dual}(p \vee (q \wedge \neg r)) \\
& = & \mathsf{dual}(p) \wedge \mathsf{dual}(q \wedge \neg r) \\
& = & p \wedge (\mathsf{dual}(q) \vee \mathsf{dual}(\neg r)) \\
& = & p \wedge (q \vee \neg\mathsf{dual}(r)) \\
& = & p \wedge (q \vee \neg r).
\end{array}$$

(ii)

$$\begin{array}{rcl}
\mathsf{flip}(\varphi) & = & \mathsf{flip}(p \vee (q \wedge \neg r)) \\
& = & \mathsf{flip}(p) \vee \mathsf{flip}(q \wedge \neg r) \\
& = & \neg p \vee (\mathsf{flip}(q) \wedge \mathsf{flip}(\neg r)) \\
& = & \neg p \vee (\neg q \wedge \neg\mathsf{flip}(r)) \\
& = & \neg p \vee (\neg q \wedge \neg\neg r).
\end{array}$$

(Note that it is $\neg\neg r$, not r.)

(b) Prove that for all $\varphi \in PF$: $\mathsf{flip}(\varphi)$ is logically equivalent to $\neg\mathsf{dual}(\varphi)$. (14 marks)

Solution

Let $P(\varphi)$ be the proposition that $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$. We will show that $P(\varphi)$ holds for all $\varphi \in PF$ by structural induction.

Base case ($\top$): $\mathsf{dual}(\top) = \bot \equiv \neg\top = \neg\mathsf{flip}(\top)$. So $P(\top)$ holds.

Base case ($\bot$): $\mathsf{dual}(\bot) = \top \equiv \neg\bot = \neg\mathsf{flip}(\bot)$. So $P(\bot)$ holds.

Base case (p): For any propositional variable p we have

$$\mathsf{dual}(p) = p \equiv \neg\neg p = \neg\mathsf{flip}(p).$$

So $P(p)$ holds.

Inductive case ($\neg\varphi$): Suppose $P(\varphi)$ holds, that is $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$. Then

$$\begin{aligned} \mathsf{dual}(\neg\varphi) &= \neg\mathsf{dual}(\varphi) \quad \text{(Definition of dual)} \\ &\equiv \neg(\neg\mathsf{flip}x(\varphi)) \quad \text{(IH)} \\ &= \neg\mathsf{flip}(\neg\varphi) \quad \text{(Definition of flip)} \end{aligned}$$

So $P(\neg\varphi)$ holds.

Inductive case ($\varphi \wedge \psi$): Suppose $P(\varphi)$ and $P(\psi)$ hold. That is, $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$ and $\mathsf{dual}(\psi) \equiv \neg\mathsf{flip}(\psi)$. Then

$$\begin{aligned} \mathsf{dual}(\varphi \wedge \psi) &= \mathsf{dual}(\varphi) \vee \mathsf{dual}(\psi) \quad \text{(Definition of dual)} \\ &\equiv (\neg\mathsf{flip}(\varphi)) \vee (\neg\mathsf{flip}(\psi)) \quad \text{(IH)} \\ &\equiv \neg(\mathsf{flip}(\varphi) \wedge \mathsf{flip}(\psi)) \quad \text{(De Morgan's law)} \\ &= \neg\mathsf{flip}(\varphi \wedge \psi). \quad \text{(Definition of flip)} \end{aligned}$$

So $P(\varphi \wedge \psi)$ holds.

Inductive case ($\varphi \vee \psi$): Suppose $P(\varphi)$ and $P(\psi)$ hold. That is, $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$ and $\mathsf{dual}(\psi) \equiv \neg\mathsf{flip}(\psi)$. Then

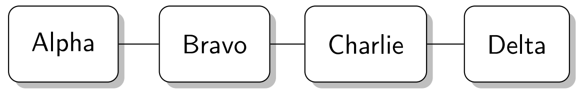
$$\begin{aligned} \mathsf{dual}(\varphi \vee \psi) &= \mathsf{dual}(\varphi) \wedge \mathsf{dual}(\psi) \quad \text{(Definition of dual)} \\ &\equiv (\neg\mathsf{flip}(\varphi)) \wedge (\neg\mathsf{flip}(\psi)) \quad \text{(IH)} \\ &\equiv \neg(\mathsf{flip}(\varphi) \vee \mathsf{flip}(\psi)) \quad \text{(De Morgan's law)} \\ &= \neg\mathsf{flip}(\varphi \vee \psi). \quad \text{(Definition of flip)} \end{aligned}$$

So $P(\varphi \vee \psi)$ holds.

By the principle of induction, $P(\varphi)$ holds for all $\varphi \in PF$.

Problem 4 (28 marks)

Four wifi networks, Alpha, Bravo, Charlie and Delta, all exist within close proximity to one another as shown below.



Networks connected with an edge in the diagram above can interfere with each other. To avoid interference networks can operate on one of two channels, hi and lo. Networks operating on different channels will not interfere; and neither will networks that are not connected with an edge.

Our goal is to determine (algorithmically) whether there is an **assignment of channels to networks** so that there is no interference. To do this we will transform the problem into a problem of determining if a propositional formula can be satisfied.

(a) Carefully defining the propositional variables you are using, write **propositional formulae** for each of the following requirements: (4 marks)

- (i) φ_1: Alpha uses channel hi or channel lo; and so does Bravo, Charlie and Delta. (4 marks)
- (ii) φ_2: Alpha does not use both channel hi and lo; and the same for Bravo, Charlie and Delta. (4 marks)
- (iii) φ_3: Alpha and Bravo do not use the same channel; and the same applies for all other pairs of networks connected with an edge. (4 marks)

(b)

- (i) Show that $\varphi_1 \wedge \varphi_2 \wedge \varphi_3$ is satisfiable; so the requirements can all be met. Note that it is sufficient to give a satisfying truth assignment, you do not have to list all possible combinations. (6 marks)
- (ii) Based on your answer to the previous question, which channels should each network use in order to avoid interference? (6 marks)

Solution

Let

Variable	Represent the proposition that:	Variable	Represent the proposition that:
A_h	Alpha uses channel hi	A_l	Alpha uses channel lo
B_h	Bravo uses channel hi	B_l	Bravo uses channel lo
C_h	Charlie uses channel hi	C_l	Charlie uses channel lo
D_h	Delta uses channel hi	D_l	Delta uses channel lo

(a) Then we can define the requirements as follows:

(i) $\varphi_1 = (A_h \vee A_l) \wedge (B_h \vee B_l) \wedge (C_h \vee C_l) \wedge (D_h \vee D_l)$.

(ii) $\varphi_2 = \neg(A_h \wedge A_l) \wedge \neg(B_h \wedge B_l) \wedge \neg(C_h \wedge C_l) \wedge \neg(D_h \wedge D_l)$.

(iii) $\varphi_3 = \neg((A_h \wedge B_h) \vee (A_l \wedge B_l)) \wedge \neg((B_h \wedge C_h) \vee (B_l \wedge C_l)) \wedge \neg((C_h \wedge D_h) \vee (C_l \wedge D_l))$.

(b) (i) One truth assignment could be defined as:

$$v(A_h) = v(B_l) = v(C_h) = v(D_l) = \texttt{true}$$
$$v(A_l) = v(B_h) = v(C_l) = v(D_h) = \texttt{false}$$

Under this assignment we see that $v(\varphi_1) = v(\varphi_2) = v(\varphi_3) = \texttt{true}$, so $v(\varphi_1 \wedge \varphi_2 \wedge \varphi_3) = \texttt{true}$ and hence the requirements can all be met.

(ii) In general, if the truth assignment sets A_h to `true` then the proposed solution is that Alpha uses channel hi and if the truth assignment sets A_l to `true` then the proposed solution is that Alpha uses channel lo (and similarly for Bravo, Charlie, and Delta). Note that φ_2 ensures that in any satisfying assignment at most one of A_h or A_l will be set to `true` (and likewise for the other variables), so Alpha will never be assigned to two channels; and φ_1 ensures that in any satisfying assignment at least one of A_h or A_l will be set to `true`, so Alpha will be assigned at least one channel.

In our particular example, the proposed solution is: Alpha and Charlie use channel hi; Bravo and Delta use channel lo.