CSC410 Assignment 5

Fall 2020

Angela Zhu, Jiabin He, Ruanfan Chen, Ze Hao Zhou

Problem 1

a) paths:
   3, 4, 5, 7, 8, 9, 15
   3, 7, 8, 9, 15
   3, 4, 5, 7, 11, 12, 13, 15
   3, 7, 11, 12, 13, 15

b) Infeasible path:

Line No.	Assignment	Path Conditions
3, 4, 5	$x \leftarrow -X$ $y \leftarrow -Y$	True AND $X < Y$
7, 8, 9	$x \leftarrow X$ $y \leftarrow Y$	True AND $X < Y$ AND $-X \leq -Y$

   This path is infeasible because its path conditions conflict.
   $X < Y$ and $-X \leq -Y$ $(X \geq Y)$ cannot be satisfied at the same time

c) Assertion violation path:

Line No.	Assignment	Path Conditions
3		True AND $X \geq Y$
7, 8, 9	$x \leftarrow -X$ $y \leftarrow -Y$	True AND $X \geq Y$ AND $X \leq Y$

   From $X \geq Y$ and $X \leq Y$ we have $X = Y$.
   This causes the assertion violation because $X = Y \rightarrow X \nless Y$

Problem 2

a) $\neg r \bigcup (r \wedge (r \bigcup \Box \neg r))$

b) $\Box((r \wedge \bigcirc w) \vee (w \wedge \bigcirc r))$

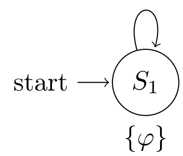
c) $\Box((r \wedge r \bigcup b) \vee (b \wedge b \bigcup w) \vee (w \wedge w \bigcup r))$

d) $\Diamond w \rightarrow \neg((\neg b \bigcup w) \vee (\neg g \bigcup w) \vee (\neg r \bigcup w))$

Problem 3

(a)

The given equivalence "$\varphi \cup \neg\varphi \equiv true$" does not hold.



Counterexample: Let π_a be an infinite path such that $\pi_a :=$

By the definition of satisfiability, $\pi \models true$, but $\pi \not\models \varphi \cup \neg\varphi$ since $\neg\varphi$ never holds on the path.

(b)

The given equivalence "$(\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2) \equiv \Diamond(\Box\varphi_1 \wedge \Box\varphi_2)$" holds, by the proof shown below.

Proof:

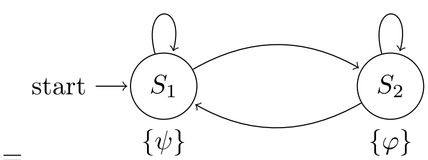
Let π be an arbitrary path. Notice that

$$
\begin{aligned}
\pi \models (\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2) &\text{ iff } (\exists i, \pi[i...] \models \Box\varphi_1) \wedge (\exists j, \pi[j...] \models \Box\varphi_2) && \text{(Def. } \Diamond) \\
&\text{ iff } \exists k, \pi[k...] \models (\Box\varphi_1 \wedge \Box\varphi_2) && \text{(Def. } \wedge \text{, and let } k = \max\{i, j\}) \\
&\text{ iff } \pi \models \Diamond(\Box\varphi_1 \wedge \Box\varphi_2) && \text{(Def. } \Diamond)
\end{aligned}
$$

Thus, $\pi \models (\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2)$ iff $\pi \models \Diamond(\Box\varphi_1 \wedge \Box\varphi_2)$, and hence $(\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2) \equiv \Diamond(\Box\varphi_1 \wedge \Box\varphi_2)$. ■

(c)

The given equivalence "$\Box\Diamond\varphi \to \Box\Diamond\psi \equiv \Box(\varphi \to \Diamond\psi)$" does not hold.



Counterexample: Let π_c be an infinite path such that $\pi_c :=$

Notice that $\pi_c \models \Box\Diamond\varphi \to \Box\Diamond\psi$ (as $\pi_c \not\models \Box\Diamond\varphi$) while $\pi_c \not\models \Box(\varphi \to \Diamond\psi)$ (as the path $\pi_c[1...]$ that reaches S_2 makes $\pi_c[1...] \models \varphi$ but then the infinite looping over S_2 never satisfies ψ.

(d)

The given equivalence "$\varphi \cup (\psi \vee \neg\varphi) \equiv \Box\varphi \to \Diamond\psi$" holds, by the proof shown below.

Proof:

Let π be an arbitrary path. Notice that R.H.S. $\equiv \Box\varphi \to \Diamond\psi \equiv \neg\Box\varphi \vee \Diamond\psi$.

[Forward Direction] (proceeded equivalently by proof of contrapositive):

Assume $\pi \models \neg(\Box\varphi \to \Diamond\psi)$, i.e., $\pi \models \Box\varphi \wedge \neg\Diamond\psi$. Then, we have

$$
\begin{aligned}
&\pi \models \Box\varphi \wedge \neg\Diamond\psi && \text{(by the assumption)} \\
\text{iff } &(\forall i, \pi[i \ldots] \models \varphi) \wedge \neg(\exists j, \pi[j \ldots] \models \psi) && \text{(Def. } \Box \text{ and } \Diamond) \\
\text{iff } &(\forall i, \pi[i \ldots] \models \varphi) \wedge (\forall j, \neg\pi[j \ldots] \models \psi) && \text{(Def. } \neg) \\
\text{iff } &(\forall i, \pi[i \ldots] \models \varphi) \wedge (\forall j, \pi[j \ldots] \models \neg\psi) && \text{(Def. } \neg \text{ and } \models) \\
\text{iff } &\forall k, \pi[k \ldots] \models (\varphi \wedge \neg\psi) && \text{(Def. } \wedge) \\
\text{iff } &\forall k, \pi[k \ldots] \models \neg(\psi \vee \neg\varphi) && \text{(by commutative, double negation and De Morgan's Law)} \\
\text{iff } &\forall k, \neg\pi[k \ldots] \models (\psi \vee \neg\varphi) && \text{(Def. } \models \neg) \\
\text{iff } &\neg\exists k, \pi[k \ldots] \models (\psi \vee \neg\varphi) && \text{(Def. } \forall\neg)
\end{aligned}
$$

Now, $\neg\exists k, \pi[k \dots] \models (\psi \vee \neg\varphi)$, which indicates that $\psi \vee \neg\varphi$ never holds on π nor on its following, then $\pi \not\models \varphi \cup (\psi \vee \neg\varphi)$ by Def. $\neg\cup$, or equivalently, $\pi \models \neg(\varphi \cup (\psi \vee \neg\varphi))$ by Def. $\models \neg$.

Thus, $\neg(\Box\varphi \to \Diamond\psi) \to \neg(\varphi \cup (\psi \vee \neg\varphi))$, and hence $(\varphi \cup (\psi \vee \neg\varphi)) \to (\Box\varphi \to \Diamond\psi)$

[Reverse Direction]

Assume $\pi \models \Box\varphi \to \Diamond\psi$, i.e., $\pi \models \neg\Box\varphi \vee \Diamond\psi$, then either $\pi \models \neg\Box\varphi$ or $\pi \models \Diamond\psi$.

Case 1: Suppose $\pi \models \neg\Box\varphi$, then $\pi \not\models \Box\varphi$ or equivalently, $\neg(\pi \models \Box\varphi)$, so $\neg(\forall i, \pi[i \dots] \models \varphi)$. Then, by expanding $\neg\forall$ and Def. $\neg \models$, we have $\exists j, \pi[j \dots] \models \neg\varphi$, and now let k be the smallest natural number such that $\pi[k \dots] \models \neg\varphi$ ①, then by generalization, we have $(\pi[k \dots] \models \neg\varphi) \vee (\pi[k \dots] \models \psi)$, i.e., $\pi[k \dots] \models \psi \vee \neg\varphi$ ②. Now, we will use proof by contradiction to show $\forall r < k, \pi[r \dots] \models \varphi$ ③ - assume by contradiction $\exists r' < k, \pi[r' \dots] \models \neg\varphi$, but this immediately contradicts to ①. Then, we know

$\exists j, \pi[j \dots] \models (\psi \vee \neg\varphi) \wedge (\forall r < j, \pi[r \dots] \models \varphi)$ (by ② ③, k is the smallest such j)

iff $\pi \models \varphi \cup (\psi \vee \neg\varphi)$ (Def. $\cup$)

Thus, $(\psi \models \neg\Box\varphi) \to (\psi \models \varphi \cup (\psi \vee \neg\varphi))$, and hence $\neg\Box\varphi \to (\varphi \cup (\psi \vee \neg\varphi))$.

Case 2: Suppose $\pi \models \Diamond\psi$, then by using the similar method in Case 1, we have $\exists i, \pi[i \dots] \models \psi$, and let h be the smallest natural number such that $\pi[h \dots] \models \psi$, then by generalization, we have $(\pi[h \dots] \models \psi) \vee (\pi[h \dots] \models \neg\varphi)$, i.e., $\pi[h \dots] \models \psi \vee \neg\varphi$ ④.

Now, we will show that $\psi \models \varphi \cup (\psi \vee \neg\varphi)$ holds regardless of whether or not $\pi \models \Box\varphi$ holds: if $\pi \models \neg\Box\varphi$, then it satisfies Case 1 and it is done - now assume $\pi \models \Box\varphi$, then $\forall r, \pi[r \dots] \models \varphi$, by Def. $\Box$, which naturally implies that $\forall r' < h, \pi[r' \dots] \models \varphi$ ⑤, then we have

$\exists j, \pi[j \dots] \models (\psi \vee \neg\varphi) \wedge (\forall r' < j, \pi[r' \dots] \models \varphi)$ (by ④ ⑤, h is the smallest such j)

iff $\pi \models \varphi \cup (\psi \vee \neg\varphi)$ (Def. $\cup$)

Thus, $(\psi \models \Diamond\psi) \to (\psi \models \varphi \cup (\psi \vee \neg\varphi))$, and hence $\Diamond\psi \to (\varphi \cup (\psi \vee \neg\varphi))$.

Hence, $(\neg\Box\varphi \vee \Diamond\psi) \to (\varphi \cup (\psi \vee \neg\varphi)$ following the discussion by cases, i.e., $(\Box\varphi \to \Diamond\psi) \to (\varphi \cup (\psi \vee \neg\varphi)$.

Therefore, $\varphi \cup (\psi \vee \neg\varphi) \equiv \Box\varphi \to \Diamond\psi$. ■

(e)

The given equivalence "$\bigcirc\Diamond\varphi \equiv \Diamond \bigcirc \varphi$" holds, by the proof illustrated below.

Proof:

Let π be an arbitrary path. Notice that

$\pi \models \bigcirc\Diamond\varphi$ iff $\pi[1...] \models \Diamond\varphi$ (Def. $\bigcirc$)

iff $\exists k, \pi[1..][k...] \models \varphi$ (Def. $\Diamond$)

iff $\exists k, \pi[k+1...] \models \varphi$ (Def. of paths)

iff $\exists k, \pi[k...][1...] \models \varphi$ (Def. of paths)

iff $\exists k, \pi[k...] \models \bigcirc\varphi$ (Def. $\bigcirc$)

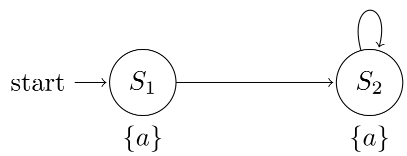
iff $\pi \models \Diamond \bigcirc \varphi$ (Def. $\Diamond$)

Thus, $\pi \models \bigcirc\Diamond\varphi$ iff $\pi \models \Diamond \bigcirc \varphi$, and hence $\bigcirc\Diamond\varphi \equiv \Diamond \bigcirc \varphi$. ■

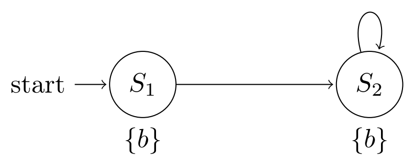
Problem 4

(a)

This formula is satisfiable, as we can find some path $\pi_1 \models \Diamond b \rightarrow (a \cup b)$ and some path $\pi_2 \not\models \Diamond b \rightarrow (a \cup b)$, where π_1 (not satisfying $\Diamond b$ but satisfying $a \cup b$, which makes $\Diamond b \rightarrow (a \cup b)$ hold) is



while π_2 (satisfying $\Diamond b$ but not satisfying $a \cup b$, which makes $\Diamond b \rightarrow (a \cup b)$ fail) is



(b)

This formula is valid, by the proof illustrated below.

Proof:

Let π be an arbitrary infinite path and assume $\pi \models \bigcirc(a \vee \Diamond a)$.

Then, we have

$\pi \models \bigcirc(a \vee \Diamond a)$	(by the assumption)
iff $\pi[1..] \models a \vee \Diamond a$	(Def.$\models \bigcirc$)
iff $(\pi[1..] \models a) \vee (\pi[1..] \models \Diamond a)$	(Def.$\vee$)
iff $(\pi[1..] \models a) \vee (\exists j, \pi[1][j..] \models a)$	(Def.$\models \Diamond$)
iff $(\pi[1..] \models a) \vee (\exists j, \pi[j+1..] \models a)$	(by algebra and definition of paths)
iff $\exists i, \pi[i..] \models a$	(Def. $\vee$, and let $i = j + 1$ where $k \geq 0$)
iff $\pi \models \Diamond a$	(Def. $\Diamond$)

Hence, $\pi \models \Diamond a$. Therefore, $\pi \models \bigcirc(a \vee \Diamond a) \rightarrow \pi \models \Diamond a$. ■

Problem 5

(a) $\forall(\neg g \cup (g \wedge \forall \bigcirc \forall(g \cup (\neg g \wedge \forall \bigcirc \forall(\neg g \cup (g \wedge \forall \bigcirc (\forall\Box\neg g)))))))$

(b) $\exists\Diamond(r \rightarrow \exists \bigcirc b) \wedge \exists\Diamond(w \rightarrow \exists \bigcirc b) \wedge \forall\Box(b \rightarrow \forall \bigcirc \neg r)$

(c) $\exists\Diamond(\neg\exists\Box w \wedge \neg\exists\Box r \wedge \neg\exists\Box g \wedge \neg\exists\Box b)$

(d) $\forall\Box(\neg(w \wedge \exists \bigcirc b) \vee \forall \bigcirc \neg\exists\Diamond(b \wedge \exists \bigcirc w))$

Problem 6

Prove $TS \models \exists(\Phi \cup \Psi) \iff TS' \models \exists\Diamond\Psi$

Proof.
Let I represent the set of initial states of TS, and I' represent the set of initial states of TS'.
It is also assumed, by the definition of TS', that for every initial state $s \in I$, there is a corresponding initial state $s' \in I'$, and vice versa. (This is in terms of states only, not considering whether or not such state has a outgoing transition, as this may be different.)

Forward direction:

1. $TS \models \exists(\Phi \cup \Psi)$ (Assumption)
2. $s \models \exists(\Phi \cup \Psi)$ for arbitrary $s \in I$ (Def. $\models$)
    3. $\exists \pi \in Paths(s)$.
    (i) $\exists j \geq 0.\ \pi[j] \models \Psi$, and
    (ii) $\forall i < j.\ \pi[i] \models \Phi \land \neg\Psi$ (Def. $\models \cup$)
    4. $\exists \pi \in Paths(s')$.
    (i) $\exists j \geq 0.\ \pi[j] \models \Psi$, and
    (ii) $\forall i < j.\ \pi[i] \models \Phi \land \neg\Psi$
    for corresponding $s' \in I'$ ($\forall$ states $n \in \pi[..j]$, by (ii) and Def. of TS', outgoing transitions from n are not eliminated, thus $\pi[0..j]$ is a valid path in $Paths(s')$ of TS')
    5. $s' \models \exists\Diamond\Psi$ (Def. $\models \Diamond$ and (i))
    6. $TS' \models \exists\Diamond\Psi$ (Def. $\models$)
7. $TS \models \exists(\Phi \cup \Psi) \implies TS' \models \exists\Diamond\Psi$

Reverse direction:

8. $TS' \models \exists\Diamond\Psi$ (Assumption)
9. $s' \models \exists\Diamond\Psi$ for arbitrary $s' \in I'$ (Def. $\models$)
    10. $\exists \pi \in Paths(s').\ \exists j \geq 0.\ \pi[j] \models \Psi$ (Def. $\models \Diamond$)

    Case 1: $j = 0$

    11. $\exists \pi \in Paths(s').\ \pi[0] \models \Psi$ (Substitute $j = 0$)
    12. $s' \models \exists(\Phi \cup \Psi)$ (Def. $\cup$)

    Case 2: $j = k + 1$ for $k \geq 0$

    13. $\exists \pi \in Paths(s').\ \pi[k+1] \models \Psi$ (Substitute $j = k + 1$)
    14. $\exists \pi \in Paths(s').\ \pi[k+1] \models \Psi$
    and $\forall i < k + 1.\ \pi[i] \models \Phi \land \neg\Psi$ ($\forall$ states $m \in \pi[..j]$, $m \not\models \Psi$ by Def. of $\Diamond$, and m has an outgoing transition $\rightarrow m \not\models \Psi \lor \neg\Phi$ $\implies m \models \Phi$, by Def. of TS')

15. $s' \models \exists(\Phi \cup \Psi)$ (Def. $\cup$)

16. $s \models \exists(\Phi \cup \Psi)$
for corresponding $s \in I$ ($\forall \pi' \in Paths(s')$. $\exists \pi \in Paths(s)$ s.t. π' is a segment of π, by Def. TS')

17. $TS \models \exists(\Phi \cup \Psi)$ (Def. $\models$)

18. $TS' \models \exists\Diamond\Psi \implies TS \models \exists(\Phi \cup \Psi)$

19. $TS \models \exists(\Phi \cup \Psi) \iff TS' \models \exists\Diamond\Psi$ (7 and 18)

■

Problem 7

$F = a \wedge \Box((a \rightarrow \bigcirc b) \wedge (b \rightarrow \bigcirc a))$

$G = b \wedge \Box((a \rightarrow \bigcirc b) \wedge (b \rightarrow \bigcirc a))$