<u>שאלה 1:</u>

בשאלה זו נדון באלגוריתם Bounded Model Checking (BMC) שנלמד בהרצאה לבדיקת AGp.

נתון מבנה קריפקה M שמיוצג ע"י נוסחאות CNF.

(א) בעת חישוב הנוסחה עבור רלציית המעברים R קרתה "תקלה" וחלק מהפסוקיות בנוסחת ה- CNF הושמטו. נסמן את הנוסחה שהתקבלה ב- R_1. נריץ בדיקת ספיקות של נוסחה φ שהיא נוסחת BMC עבור M, k ו- AGp תוך שימוש ב- R_1 במקום R.

i. האלגוריתם מחזיר "*sat*". האם $M \not\models_k AGp$?

פתרון: לא בהכרח - אם מורידים פסוקיות מנוסחה שמייצגת קשת בגרף, עלולים ליצור קשתות נוספות ובכך לאפשר מסלולים שלא היו קיימים וכך למצוא מסלול שסותר את AGp.

ii. האלגוריתם מחזיר "*unsat*". האם $M \models_k AGp$?

פתרון: נכון - בסך הכל הוספנו עוד מסלולים לגרף. אם לא הצלחנו לספק את הנוסחה עם מסלולים נוספים, אין סיכוי שנצליח לספק אותה עם פחות מסלולים. לכן בכל המסלולים יתקיים AGp.

<u>נמקו</u> את תשובותיכם.

(ב) חזרו על הסעיף הקודם (על שני חלקיו) כאשר הפעם בעת חישוב הנוסחה עבור R נוספו פסוקיות CNF. נוסחת ה- BMC שהתקבלה מסומנת ב- R_2 והאלגוריתם לבדיקת ספיקות השתמש בה במקום ב-R.

פתרון: כעת התשובה הפוכה. הוספת פסוקיות CNF **<u>מקטינה</u>** את רלצית המעברים ולכן מקטינה את הסיכוי למצוא מסלול הסותר את הנוסחה AGp.

<u>שאלה 2:</u>

נתון מבנה קריפקה M שמיוצג ע"י נוסחאות CNF , כלומר

- $\bar{v} = v_1, \ldots, v_n$ וקטור המשתנים.
- $S(\bar{v})$ היא נוסחת CNF שמייצגת את קבוצת המצבים של M.
- $R(\bar{v}, \bar{v}')$ היא נוסחת CNF שמייצגת את רלציית המעברים של M.
- $I(\bar{v})$ היא נוסחת CNF שמייצגת את קב' המצבים התחיליים של M.
- לכל $p \ni AP$, $p(\bar{v})$ היא נוסחת CNF שמייצגת את קבוצת המצבים המספקים את p.

נתונים שני מצבים s_1, s_2 כך ש $s_1 \neq s_2$ ונתונה נוסחה אטומית $p \in AP$. מעוניינים למצוא את המסלול <u>הקצר ביותר</u> מ- s_1 ל- s_2 המקיים את שתי הדרישות הבאות:

(א) זהו מסלול באורך <u>זוגי</u> (אורך מסלול נמדד בקשתות), <u>וגם</u>

(ב) כל המצבים על המסלול מספקים את p.

שימו לב: בשאלה זו מדובר על מסלולים <u>סופיים</u>.

הציעו אלגוריתם שמטרתו למצוא מסלול כנ"ל. על האלגוריתם לפעול באופן דומה ל- Bounded Model Checking (BMC) מבוסס SAT.

האלגוריתם עוצר ומחזיר מסלול מתאים אם קיים כזה ועוצר ועונה "לא" אם לא קיים.

נמקו את נכונות האלגוריתם ועצירתו.

פתרון:
נבדוק את הנוסחה הבאה באמצעות אלגוריתם SAT.
$S_1(\overline{v}_0) \wedge R(\overline{v}_0, \overline{v}_1) \wedge R(\overline{v}_1, \overline{v}_2) \wedge S_2(\overline{v}_2) \wedge p(\overline{v}_0) \wedge p(\overline{v}_1) \wedge p(\overline{v}_2)$
אם היא תצליח לספק את הנוסחה, אז המסלול $\overline{v}_0, \overline{v}_1, \overline{v}_2$ הוא המסלול המתאים.
אם לא, אז נבנה נוסחה חדשה, דומה, עבור מסלול עם ארבע קשתות.
נמשיך כך עד שנגיע למסלול עם $2 \cdot 2^{|v|} - 2$ ($|v|$ הוא גודל הווקטור לייצוג המצבים. לכן $2^{|v|}$ הוא מספר המצבים. בכל מצב ניתן לבקר פעמים, פעם בביקור אי זוגי ופעם בביקור זוגי.)
אם עדין לא הצלחנו לספק את הנוסחה, אז נודע שלא קיים מסלול מתאים.

for i=1 to $2^{|V|-1}$
{
$F_{2i} \leftarrow S_1(\overline{v}_0) \wedge S_2(\overline{v}_i) \wedge_{j=0}^{2i} \left[p(\overline{v}_j) \right] \wedge_{j=0}^{i-1} \left[R(\overline{v}_{2j}, \overline{v}_{2j+1}) \wedge R(\overline{v}_{2j+1}, \overline{v}_{2j+2}) \right]$
if SAT(F_{2i}) return satisfying assignment
}
return NULL;

שאלה 3

נגדיר שפה טפורלית חדשה $\exists$CTL שהיא הרחבה של CTL.
φ היא נוסחת $\exists$CTL אם $\varphi = \exists q.\varphi_1$, φ_1 היא נוסחת CTL ו- q נוסחה אטומית פסוקית.
בהינתן מבנה $M = (S, R, L)$ ומצב s ב- M נאמר ש- $M, s \models \exists q.\varphi_1$, אם קיים מבנה $M' = (S, R, L')$ (כאשר S, R הם כמו ב- M) כך שלכל $t \in S$ מתקיים $L(t) \setminus \{q\} = L'(t) \setminus \{q\}$ וכן $M', s \models \varphi_1$.
(M' זהה ל- M מלבד שב- M' מותר להוריד או להוסיף סימוני q על המצבים).
(א) הציעו מבנה M ומצב s ב- M כך ש- $M, s \not\models \exists q.(EF(p \wedge q) \wedge EF(p \wedge \neg q))$ כאשר $p, q \in AP$. נמקו.

פתרון: נשתמש במבנה שמכיל מצב אחד בלבד. הנוסחה $\left(EF(p \wedge q) \wedge EF(p \wedge \neg q)\right)$ היא סתירה במודל זה, ללא תלות בשאלה האם המצב היחיד מספק את p או את q. לכן המודל לא מספק את נוסחת ה $\exists CTL$.

(ב) הציעו אלגוריתם לבדיקת מודל שבהינתן מבנה M ונוסחה $\exists q.E((r \wedge \neg q)U(p \wedge q))$, כאשר $p, q, r \in AP$, מחזיר את קבוצת המצבים שמספקים את הנוסחה.
על האלגוריתם להיות בסיבוכיות ליניארית בגודל המבנה והנוסחה.
נמקו את תשובתכם.

פתרון: נפעיל את האלגוריתם לסימון מצבים המספקים את הנוסחה $E(rUp)$. את ה q-ים ואת ה $\neg q$-ים נתאים למסלול שנמצא.
הסיבוכיות מתאימה כי האלגוריתם לסימון מצבים המספקים את $E(rUp)$ הוא אלגוריתם ליניארי.