מערכות טרנספורמטיביות / תגוביות - תזכורת מההרצאה הראשונה:

	הוכחת נכונות	אימות אוטומטי
מספר המצבים	אינסופי או גדול מאוד	סופי וקטן יחסית (עד 10^{300})
סוג התוכנית	טרנספורמטיבית	ריאקטיבית = תגובתית
מפרט	לוגיקה מסדר ראשון (למשל תחשיב היחסים)	לוגיקה טמפורלית (עיתית)
חישוביות	בלתי כריעה undecidable	כריעה
אוטומציה	עזרה מהמשתמש	אוטומציה מלאה
כלים	Theorem proves	RuleBase

אימות ≡ עימות בין רמות הפשטה שונות של המערכת.

$S \models \varphi_2$ (מצב = גרף, מספק נוסחה בלוגיקה עיתית) - S הוא "מודל" של φ_2.
"בדיקת מודל" model - checking.

<u>לוגיקה עיתית:</u>
$Globaly$ (מסומן ב G או ב □) - תכונה שמתקיימת לכל אורך התוכנית.
לדוגמה: $G\left(\neg at_critical_1 \vee \neg at_critical_2\right)$
(ממערכות הפעלה - לא יתכן ששני חוטים יהיו בקטע הקריטי בו זמנית)

$\Box Future\left(eventually\right)$ - תכונה שתתקיים מתישהו בעתיד.
לדוגמה: $request \rightarrow F\left(granted\right)$
(ממערכות הפעלה - אם תהליך ביקש משאב כלשהו, בסופו של דבר הוא יקבל אותו מתישהו)

נקבל ש: $G\left(p\right) = \neg F\left(\neg p\right)$
(לומר ש P מתקיים תמיד זה כמו לומר שלא יקרה בעתיד שיתקיים "לא P")

GFp - בכל רגע בתוכנית מתקיים שמתישהו בעתיד יתקיים P.

FGp - החל מרגע מסוים בעתיד, P יתקיים לנצח.

$neXt\left(p\right)$ - P יתקיים בצעד הבא. יסומן ב ○ או ב X.
XGp - החל מהצעד הבא, P יתקיים תמיד.
GXp - בכל מצב יתקיים שבמצב הבא P יתקיים. קיבלנו ש $XGp = GXp$

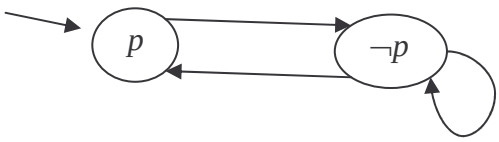
$\left(p\right)Until\left(q\right)$ - יסומן ב U
pUq - מתישהו בעתיד q מתקיים, ועד אז בהכרח p מתקיים.

"אם הודעה 1 נשלחה לפני הודעה 2 אזי הודעה 1 תגיע לפני הודעה 2"
האטומים הם $sent_1, sent_2, received_1, received_2$
$\neg sent_2 U sent_1 \rightarrow \neg received_2 U received_1$

$\left(p\right)Release\left(q\right)$ - יסומן ב R.
pRq - מתקיים q עד שיתקיים p, כולל המצב הראשון שבו יתקיים p. לא בהכרח יתקיים בעתיד p.

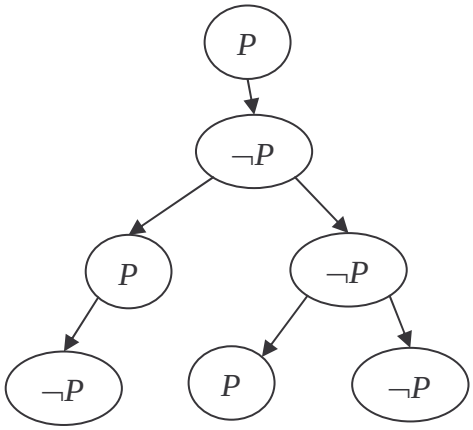
כמתי מסלול: $E - exist$
$A - for \quad all$

למשל עבור הגרף:

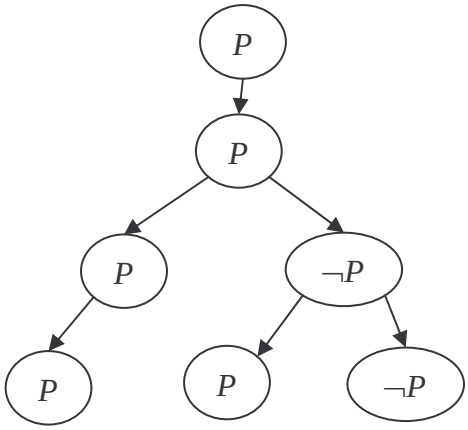


בצומת הימני מתקיים EXp אבל לא מתקיים AXp
זאת אומרת שקיים מסלול בו מתקיים Xp אבל לא בכל מסלול מתקיים Xp .

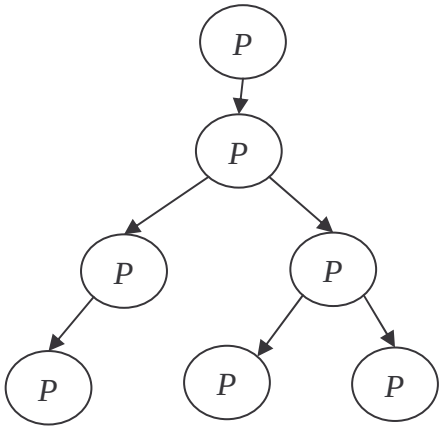
<u>Computational Tree Logic = CTL</u>



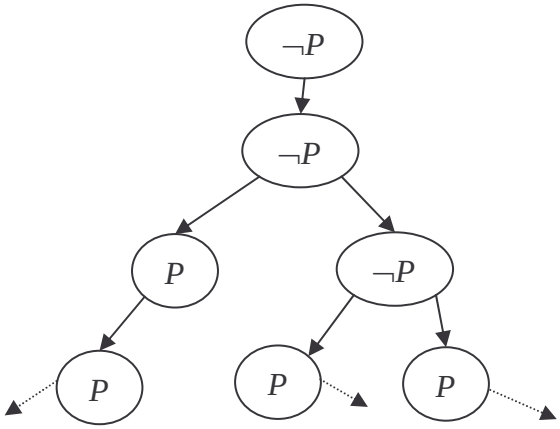
לדוגמה: הגרף הבא מקיים EGp , לדוגמה, עבור המסלול השמאלי ביותר.



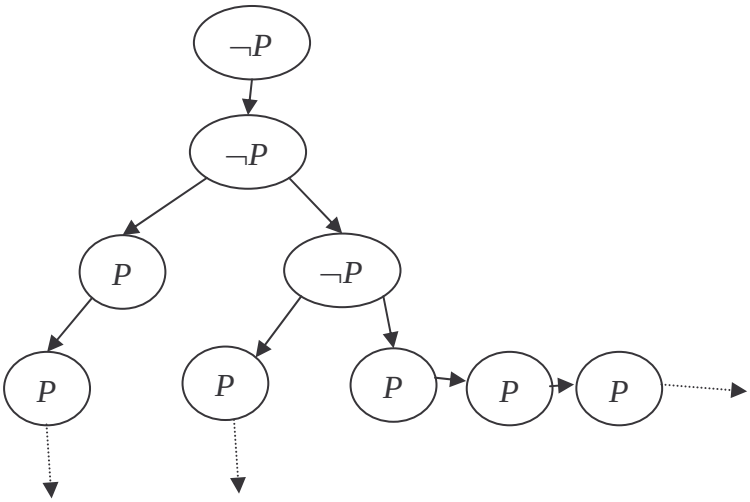
לדוגמה: הגרף הבא מקיים AGp - בכל מסלול תמיד מתקיים p



לדוגמה, הגרף הבא מקיים AFp - בכל מסלול, מתישהו יתקיים p :



לדוגמה, הגרף הבא מקיים $AF\left(EGp\right)$ - בכל מסלול, מתישהו בעתיד יתקיים, שקיים המשך למסלול שבו תמיד יתקיים p .



לדוגמה: $EG\left(EFp\right)$ - קיים מסלול, שלכל אורכו תמיד קיים שמתישהו בעתיד יתקיים p

נתונה קבוצת נוסחאות אטומיות Ap

<u>נוסחאות מצב</u>

1. $p \in Ap$ היא נוסחת מצב.
2. אם f, g נוסחאות מצב, אז גם $f \vee g$ היא נוסחת מצב, וגם $\neg f$ היא נוסחת מצב.
3. אם f נוסחת מסלול, אזי Ef היא נוסחת מצב.

<u>נוסחאות מסלול</u>

1. נוסחת מצב.
2. אם f, g נוסחאות מסלול, אז גם $f \vee g$, $f\neg$, fUg, Xf הן נוסחאות מסלול.

השפה CTL^*, לוגיקה עיתית. זוהי קבוצת <u>נוסחאות המצב</u> שמוגדרות ע"י החוקים הנ"ל.
נוסחאות CTL^* מתפרשות מעל מבנה קריפקה

טענה: האופרטורים U, X מספיקים כדי להגדיר את R, F, G.

$$F(p) = (True)U(p)$$

$$G(p) = \neg F(\neg p) = \neg((True)U(\neg p))$$

מבנה קריפקה מוגדר מעל קבוצת משתנים אטומיים Ap.

$$M = (S, R, S_0, L)$$

S - קבוצת מצבים

R - רלצית מעברים שלמה (לכל מצב יש מצב עוקב) $\forall s \exists s' (s, s') \in R$. $R \subseteq S \times S$

$S_0 \subseteq S$ - קבוצת מצבים התחלתיים.

$L : S \to 2^{Ap}$ - פונקצית סימון מצבים $(Labaling)$ שמתאימה לכל מצב את תת הקבוצה של Ap שמתקיימת בו.

מסלול (חישוב) שמתחיל ממצב s ב M: סדרת מצבים $\pi = s_0, s_1, s_2, \ldots$ כך ש $s = s_0$ ולכל i מתקיים $(s_i, s_{i+1}) \in R$

π^i = המסלול π החל ממצב s_i.