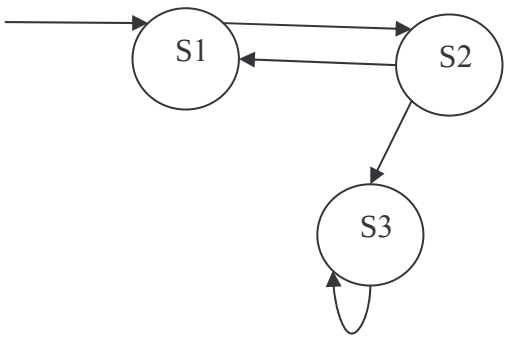
<u>הוגנות</u> fairness (המשך מההרצאה הקודמת)

$H = \{h_1, h_2, ..., h_k\} \subseteq 2^S$

לדוגמה:



$H = \{(s_1, s_2), (s_1, s_3)\}$

מסלול π הוא <u>הוגן</u> ביחס ל H אם ורק אם לכל $h \in H$ מתקיים: $\inf(\pi) \cap \pi \neq \phi$

כאשר: $\inf(\pi) = \{s \mid s$ עובר אינסוף פעמים ב $\pi\}$

אם לדוגמה $\pi_1 = s_1, s_2, s_1, s_2, s_3, s_3, s_3, ...$ אז $\inf(\pi_1) = \{s_3\}$

ואז $\inf(\pi_1) \cap \{s_1, s_2\} = \phi$ ולכן המסלול π_1 לא הוגן ביחס ל H

אם ניקח את המסלול $\pi_2 = s_1, s_2, s_1, s_2, ...$ אז $\inf(\pi_2) = \{s_1, s_2\}$

ואז $\begin{array}{l} \inf(\pi_2) \cap \{s_1, s_2\} = \{s_1, s_2\} \neq \phi \\ \inf(\pi_2) \cap \{s_1, s_3\} = \{s_1\} \neq \phi \end{array}$ ולכן המסלול π_2 כן הוגן ביחס ל H.

$M, s \models_F f_1$ - המבנה M והמצב s מספקים תחת דרישות ההוגנות את נוסחת המצב f_1.

$M, s \models_F AFf_1$ - עבור כל מסלול הוגן π שמתחיל מ s, קיים k כך ש $\pi^k \models f_1$.

$M, s \models_F EFf_1$ - קיים מסלול הוגן π שמתחיל מ s וקיים k כך ש $\pi^k \models f_1$.

$M, s \models_F EGf_1$ - קיים מסלול הוגן π שמתחיל מ s ולכל $k \geq 0$ מתקיים $\pi^k \models f_1$.

הדואליות בין האופרטורים נשמרת כמו במקרה ללא דרישת ההוגנות:

כדי לסתור את $M, s \models_F EFp$ נמצא דוגמה נגדית ע"י מציאת עד ל $M, s \models_F AG\neg p$.

זאת אומרת שנוכיח שלכל מסלול הוגן תמיד מתקיים בו $\neg p$, וזה אומר שלא קיים מסלול הוגן שבו בסופו שלדבר מתקיים p.

אלגוריתם לבדיקת EGf_1 תחת הוגנות: (נסמן: $E_F Gf_1$)

1. נבנה $M' = (S', R', L', H')$ כך ש:

$S' = \{s \mid M, s \models_F f_1\}$ אוסף כל המצבים שמספקים את f_1 תחת דרישות ההוגנות.

$R' = (S' \times S') \cap R$ אוסף כל הקשתות שרלוונטיות רק למצבים ב S'.

$L' = L|_{S'}$ - התוויות שמתאימות למצבים ב S'.

$H' = \{h_i \cap S' \mid h_i \in H\}$ - קבוצת של קבוצות מצבים שמגדירות את דרישות ההוגנות במודל M'.

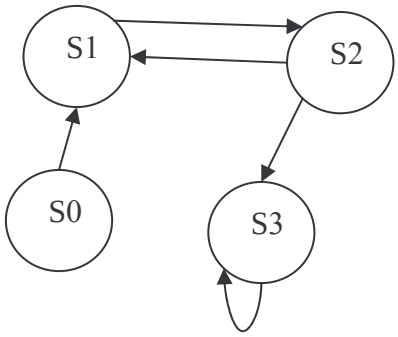
(השלבים הבאים מתבצעים רק על צמתים מתוך M')

2. נמצא את כל הרכיבים הקשירים הלא טריוויאליים היטב המקסימאליים ב M'.
3. נסמן את הרכיבים <u>ההוגנים</u> ב $E_F Gf_1$

רכיב קשיר היטב c המורכב מקבוצת המצבים S_c הוא <u>הוגן</u> ביחס ל $H=\{h_1,h_2,...h_n\}$ אם לכל $1\le i\le n$ מתקיים: $h_i \cap S_c \ne \phi$.

4. סמן מצבים ב $E_F Gf_1$ תוך הליכה אחורה ממצבים שמסומנים ב $E_F Gf_1$.

לדוגמה: נניח שהיה לנו מבנה M והפעלנו עליו את השלב הראשון באלגוריתם וקיבלנו מבנה חדש M'



כך שכל הצמתים ב M' מספקים את f_1

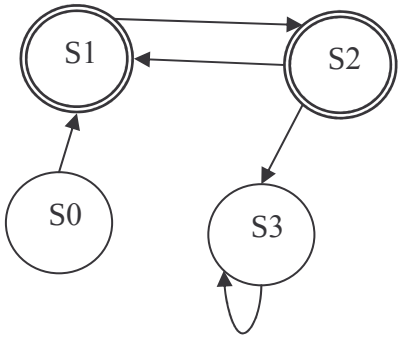
$$H=\{h_1=(s_1,s_2),h_2=(s_1,s_3)\}$$

הרכיבים הקשירים היטב המקסימאליים הלא טריוויאליים הם: $\{(s_1,s_2),(s_3)\}$

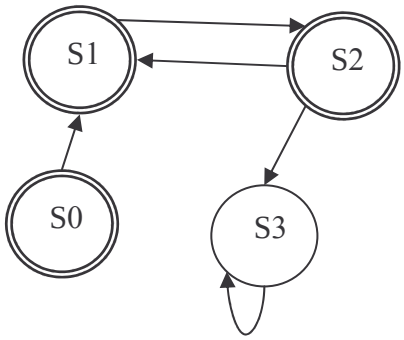
הרכיב (s_3) איננו הוגן כי $(s_3)\cap\underbrace{(s_1,s_2)}_{h_1}=\phi$

הרכיב (s_1,s_2) הוא כן הוגן כי
$$(s_1,s_2)\cap(s_1,s_2)=(s_1,s_2)\ne\phi$$
$$(s_1,s_2)\cap(s_1,s_3)=(s_3)\ne\phi$$

לכן נסמן ב $E_F Gf_1$ את s_1,s_2:



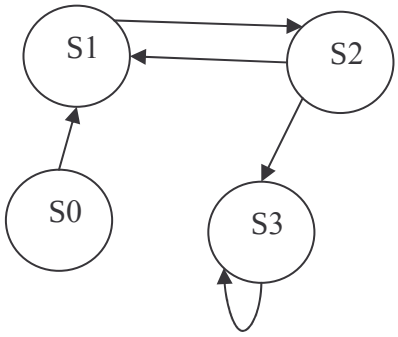
כעת נלך אחורה ונסמן גם את s_0:



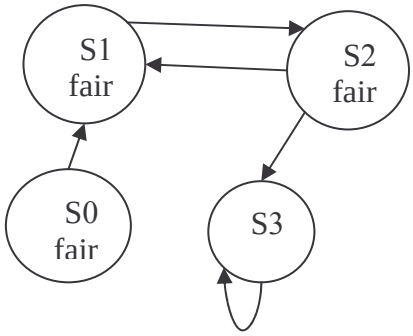
המצבים שסומנו הם אלו שמקיימים את הנוסחה $E_F Gf_1$

אלגוריתמים לסימון הנוסחאות: $E_F f_1 UF_2$, $E_F Xf_1$

1. נסמן את כל המצבים מהם יוצא מסלול הוגן. נסמן במשתנה "$fair$" את כל המצבים שמספקים $E_F G(true)$.



$H = \{h_1 = (s_1, s_2), h_2 = (s_1, s_3)\}$.



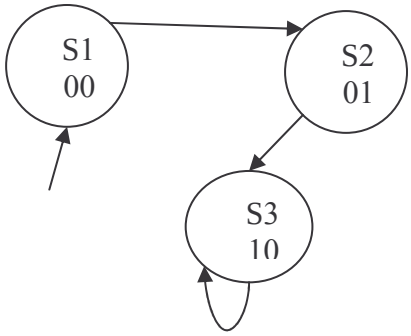
2. כיצד נדע האם מתקיים $E_F Xf_1$? לו היינו מחפשים רק EXf_1 היינו מסמנים את כל המצבים שיש להם בן שמקיים f_1. לכן במקום זאת נסמן את כל המצבים שיש להם בן שמקיים $fair \wedge f_1$.
בדוגמה שלעיל, הצמתים שיקיימו את $E_F Xf_1$ הם s_0, s_1, s_2

3. כיצד נדע האם מתקיים $E_F f_1 UF_2$? נחפש במקום זאת את המצבים שמקיימים את $Ef_1 U(f_2 \wedge fair)$

בדיקת מודל סימבולית (Symbolic model-checking)

פונקציה מאפיינת של קבוצה - בהינתן קבוצה U ותת קבוצה שלה A, הפונקציה המאפיינת של A, שתסומן ב f_A מוגדרת כך: $f_A(\mathrm{a} \in \mathrm{U}) = \begin{cases} 1 & \mathrm{a} \in \mathrm{A} \\ 0 & \mathrm{a} \notin \mathrm{A} \end{cases}$

יצוג מבנה קריפקה באמצעות נוסחאות בינאריות:
נסמן את המצבים בביטים:



המשתנים הם v_1, v_2 כאשר v_1 הוא הביט השמאלי ו v_2 הוא הביט הימני.
תיאור המצבים בעזרת פונקציות מאפיינות.

$$f_{\{s_1\}} = \neg v_1 \wedge \neg v_2$$
$$f_{\{s_2\}} = \neg v_1 \wedge v_2$$
$$f_{\{s_3\}} = v_1 \wedge \neg v_2$$

הפונקציה המאפיינת של S היא: $f_S = (\neg v_1 \wedge \neg v_2) \vee (\neg v_1 \wedge v_2) \vee (v_1 \wedge \neg v_2)$
האם המצב 11 שייך ל S? כלומר האם $v_1 = T, v_2 = T$ מספק את f_S.
נציב ונקבל: $f_S(v_1 = T, v_2 = T) = (\neg T \wedge \neg T) \vee (\neg T \wedge T) \vee (T \wedge \neg T) = F$ ולכן המצב 11 לא שייך ל S.

איך נייצג את הקשתות במבנה קריפקה?
תיאור הקשתות בעזרת פונקציות מאפיינות:
נחזיק שני עותקים של כל משתנה:
$v_1, \ldots, v_n$ לתיאור המצב הנוכחי.
$v_1', \ldots, v_n'$ לתיאור המצב הבא.
לדוגמה, את המעבר $s_1 \to s_2$ נתאר באמצעות $\underbrace{\neg v_1 \wedge \neg v_2}_{\text{המצב הנוכחי}} \wedge \underbrace{\neg v_1' \neg v_2'}_{\text{המצב הבא}}$

הפונקציה המאפיינת של קבוצת המעברים האפשריים f_R תהיה:

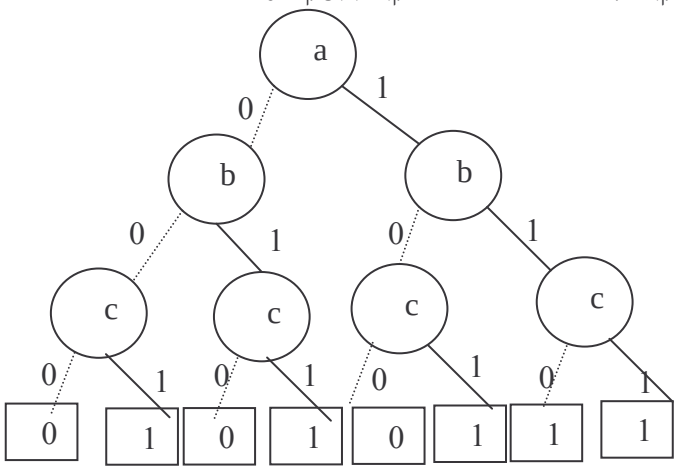
$$f_R = \underbrace{(\neg v_1 \wedge \neg v_2 \wedge \neg v_1' \wedge v_2')}_{(s_1, s_2)} \vee \underbrace{(\neg v_1 \wedge v_2 \wedge v_1' \wedge \neg v_2')}_{(s_2, s_3)} \vee \underbrace{(v_1 \wedge \neg v_2 \wedge v_1' \wedge \neg v_2')}_{(s_3, s_3)}$$

האם הקשת (s_3, s_1) נמצאת בקבוצת המעברים R?
נציב בפונקציה את $v_1 = T, v_2 = F, v_1' = F, v_2' = F$ ונבדוק האם נקבל T או F.

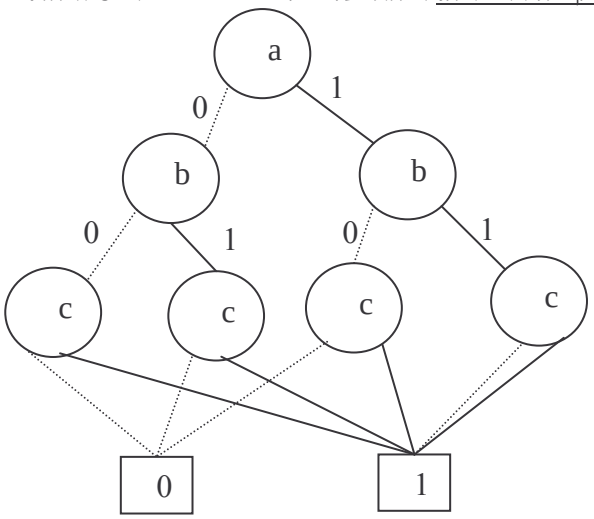
BDD - Binary Decision Diagram - מבנה נתונים לטיפול יעיל בנוסחאות בוליאניות.
מתחיל בעץ בינארי:

נניח שמטפלים בנוסחה $(a \wedge b) \vee c$

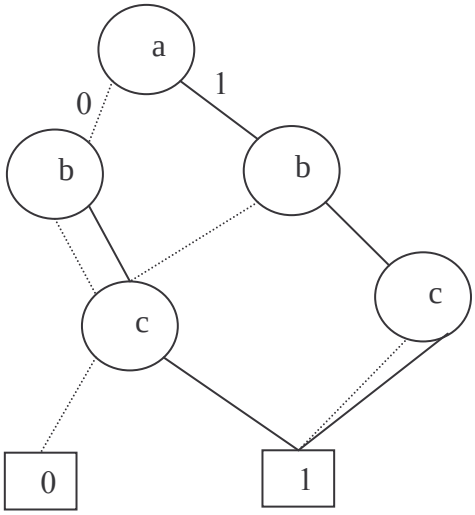
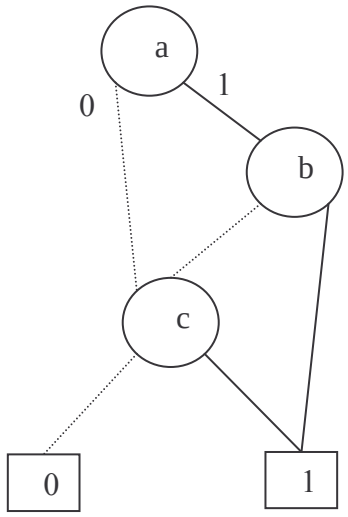
קו שלם - 1 קו מרוסק - 0



<u>רדוקציה ראשונה:</u> איחוד עלים לשני מצבים - אפס ואחד.



<u>רדוקציה שניה:</u> איחוד תתי עצים איזומורפיים.



<u>רדוקציה שלישית</u>: הורדת משתנים מיותרים (שאין להם השפעה על התוצאה) למשל בדוגמה שלנו המשתנה c הימני הינו מיותר כי גם הענף הימני שלו וגם השמאלי מובילים ל- 1 ולכן אין לו השפעה על התוצאה. כך גם המשתנה b השמאלי.