דוגמה נגדית counter-example
עד witness

עד ל AGp זה דוגמה נגדית ל $EF(\neg p)$

תכונות safety "בטיחות" - מה אסור שיקרה. בשביל למצוא דוגמה נגדית לתכונת בטיחות, צריך למצוא מסלול למצב שסותר את התכונה הזאת.

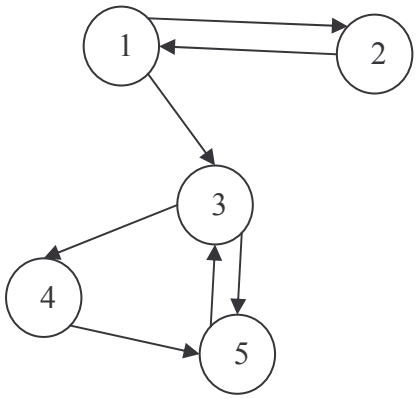
למשל: AGp היא נוסחת תכונת בטיחות, כי היא אומרת שאסור שיהיה מסלול שבו יתקיים $\neg p$.

תכונת liveness "חיות" - מה צריך בסופו של דבר לקרות.
למשל AFp - בכל המסלולים בסופו של דבר צריך להתקיים p. בשביל לסתור תכונת חיות, יש למצוא מסלול אינסופי שסותר את התכונה. למשל, בשביל לסתור את AFp צריך למצוא מסלול שבכולו מתקיים $\neg p$ והוא מסתיים בלולאה שבה תמיד מתקיים $\neg p$.

כלל אצבע: כל תכונת בטיחות ניתנת לרדוקציה לנוסחת AGp

איך נראה עד ל EGf_1? מסלול שבסופו לולאה ובכולו מתקיים f_1.

הגדרה: בהינתן גרף מכוון G, נאמר ש C, תת גרף של G הוא רכיב קשיר היטב strongly-connected - component - scc, אם מכל צומת ב C יש מסלול מכוון לכל צומת אחר ב C דרך צמתים ב C בלבד.



בדוגמה הנ"ל הקבוצות הבאות הן רכיבים קשירים היטב: $\{1,2\},\{3,5\},\{3,4,5\}$

רכיב קשיר היטב הוא <u>טריוויאלי</u> אם יש בו צומת יחיד ללא חוג עצמי ואף צומת אחר מלבדו.

רכיב קשיר היטב הוא <u>מקסימאלי</u> אם הוא לא מוכל ממש באף רכיב קשיר היטב.

בדוגמה הנ"ל הרכיבים הקשירים היטב המקסימאליים הם הקבוצות: $\{1,2\},\{3,4,5\}$
הרכיבים הקשירים היטב הטריוויאליים הם: $\{1\},\{2\},\{3\},\{4\},\{5\}$

קיים אלגוריתם של $Tarjan$ שמוצא את כל הרכיבים הקשירים היטב המקסימאליים בגרף (כולל הטריוויאליים) בזמן $O(|S|+|R|)$ כאשר S היא קבוצת הצמתים ו R היא קבוצת הקשתות בגרף.

בהינתן מבנה: $M=(S,R,L,S_0)$ נגדיר את המבנה $M'=(S',R',L',S_0')$ באופן הבא:

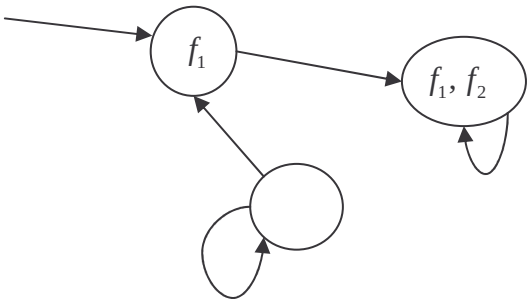
$S'\{s\in S \mid M,s \models f_1\}$ קבוצת המצבים החדשה - כל המצבים שמספקים את הנוסחה f_1 במבנה M.

$R'=\{(s_1,s_2)\in R \mid s_1,s_2\in S'\}$ קבוצת הקשתות החדשה

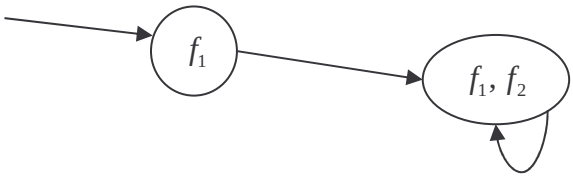
$L'=L|_{S'}$ קבוצת התוויות החדשה

$S_0'=\{s \mid s\in S_0\cap S'\}$ קבוצת המצבים ההתחלתיים החדשה.

לדוגמה: אם זהו M



אז M' הוא:



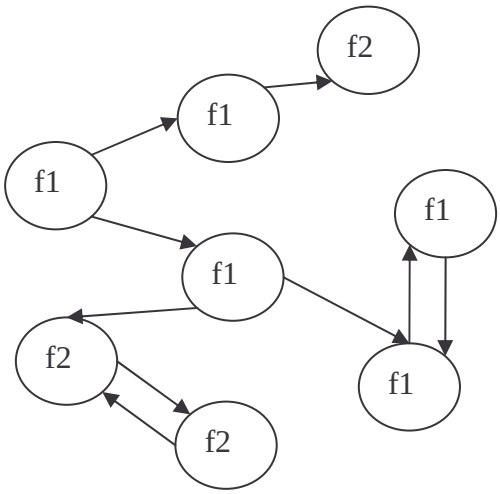
משפט: $M,s \models EGf_1$ אם ורק אם מתקיימים התנאים הבאים:

1. $s\in S'$
2. קיים מסלול ב M' ממצב s לרכיב קשיר היטב מקסימאלי כלשהו, לא טריוויאלי ב M'.

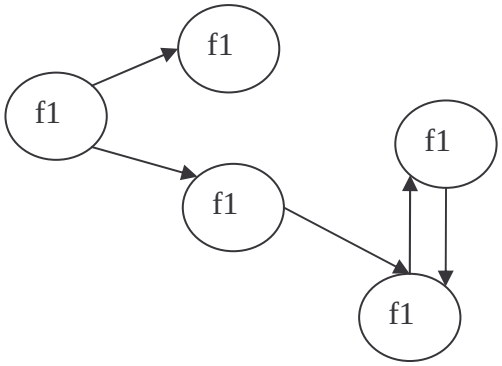
האלגוריתם:

1. בנה את $M'=(S',R',L',S_0')$
2. מצא את כל הרכיבים הקשירים היטב SCC ב M'.
3. סמן כל מצב ברכיב קשיר לא טריוויאלי ב M' ב EGf_1 (כלומר המצב מקיים EGf_1).
4. סמן מצבים ב EGf_1 תוך הליכה אחורנית על R'.

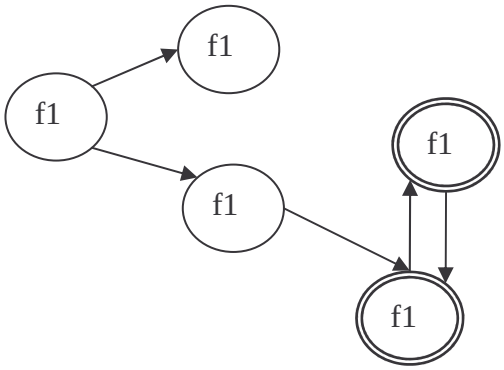
לדוגמה: נתון M



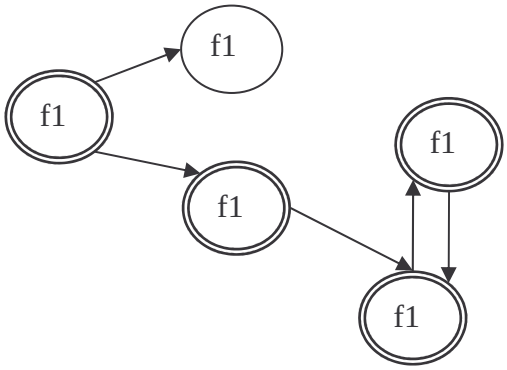
נבנה את M':



נסמן את המצבים שנמצאים ברכיב קשיר היטב לא טריוויאלי:



נסמן את כל המצבים שאפשר להגיע מהם לרכיב קשיר היטב לא טריוויאלי:



הצמתים המסומנים הם הצמתים המקיימים EGf_1.

בדיקת מודל מפורשת: ראינו אלגוריתם ל EXf_1, $E\left(f_1Uf_2\right)$, EGf_1. את כל השאר ניתן לבטא בעזרתם.

בהינתן נוסחת CTL, f, בדיקת מודל M של f היא בסיבוכיות זמן של $|f|\cdot|M|$

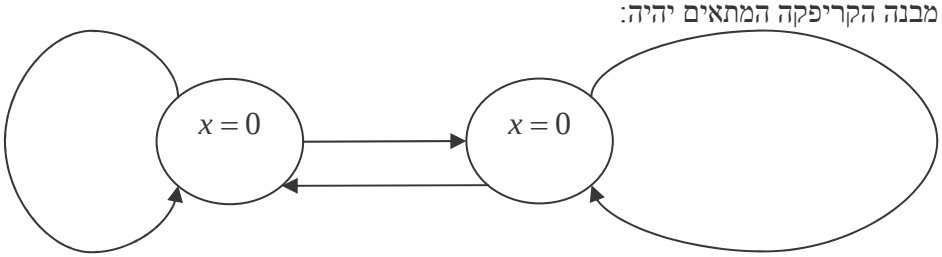
$$EFp = E\left(TrueUp\right)$$
$$AGp = \neg EF\neg p$$

הוגנות:

נניח שיש לנו שני תהליכים שרצים במקביל ומשנים את אותו המשתנה.

$P1$	$P2$
Repeat	*Repeat*
$x=0$	$x=1$

מבנה הקריפקה המתאים יהיה:



נניח שרוצים לבדוק את התכונה הבאה: $AF\left(x=1\right)$ - (בכל מסלול, תמיד בעתיד יתקיים $x=1$)

התכונה לא מתקיימת - קיים מסלול אינסופי סותר - המסלול שנשאר תמיד ב $x=0$.

בפועל, לא יתכן ש $P1$ ירוץ לנצח.

לכן הדוגמה הזאת לא לגיטימית כי זו דוגמה נגדית לא הוגנת (התהליך $P2$ אף פעם לא מתבצע).

נגדיר מבנה קריפקה הוגן Fair Kripke structure:

$M=\left(S,R,L,S_0,H\right)$

S,R,L,S_0 כמו קודם.

$H\subseteq 2^S$ - קבוצת של קבוצות מצבים שמגדירות את דרישות ההוגנות במודל.

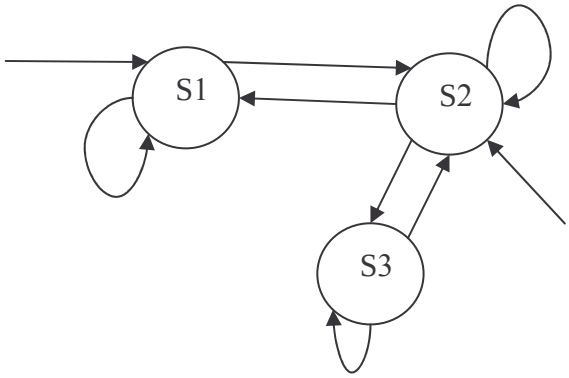
$H=\left\{h_1,h_2,...,h_k\right\}$, $h_i\subseteq S$ קבוצת מצבים מ S.

עבור חישוב אינסופי π נגדיר את $\inf\left(\pi\right)$ להיות קבוצת כל המצבים בהם π עבר אינסוף פעמים:

$\inf\left(\pi\right)=\{s\,|\,s$ עובר אינסוף פעמים ב $\pi\}$

מסלול π הוא הוגן ביחס ל $H=\left\{h_1,h_2,...,h_k\right\}$ אם ורק אם $\forall i:\inf\left(\pi\right)\cap h_i\neq\phi$ $\left(1\le i\le k\right)$

לדוגמה:



$h_1=\left\{s_2,s_3\right\}$

$h_2=\left\{s_1,s_2\right\}$

$\pi_1=s_1,s_1,s_1,...$ המסלול לא הוגן כי $\inf\left(\pi_1\right)\cap h_1=\phi$

$\pi_2=s_2,s_2,s_2,...$ המסלול כן הוגן כי $\inf\left(\pi_2\right)\cap h_1=\inf\left(\pi_2\right)\cap h_2=\left\{s_2\right\}\neq\phi$

$\pi_3=s_2,s_3,s_2,s_3,s_3,s_3,s_3,...$ המסלול לא הוגן כי $\inf\left(\pi_3\right)\cap h_2=\left\{s_3\right\}\cap\left\{s_1,s_2\right\}=\phi$