

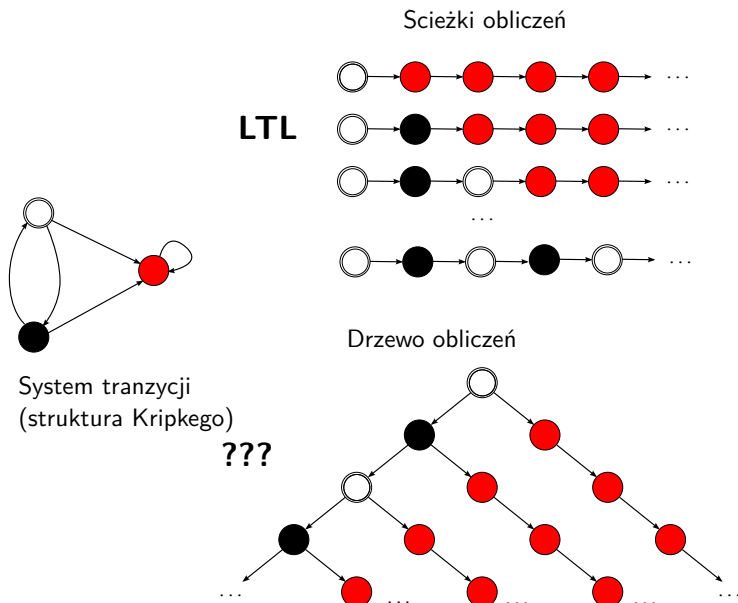
Logika dla informatyków

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

`inf.ug.edu.pl/~amb`

Obliczenia i wnioskowanie o ich własnościach



Logika czasu rozgałęzionego

Ograniczenia logiki LTL

- chcemy powiedzieć, że istnieje ścieżka obliczeń o pewnej własności
- można użyć sztuczki – „nieprawda, że dla każdej ścieżki zachodzi przeciwna własność”
 - mutex: „istnieje ścieżka z dwoma stanami c_1 pomiędzy którymi nie ma stanów spełniających c_2 ”
 - negacja jest równa $G(c_1 \rightarrow c_1 \ W (\neg c_1 \wedge \neg c_1 \ W c_2))$
- ale ta przeciwna własność znowu może zaczynać się od kwantyfikatora szczegółowego
 - mutex: „dla każdego procesu w każdym stanie neutralnym istnieje ścieżka, na której proces zgłasza żądanie wejścia do obszaru krytycznego” – tej własności nie można wyrazić w **LTL**

CTL (Computation Tree Logic)

Gramatyka (w postaci Backusa-Naura)

$$\varphi ::= \top \mid \perp \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid \\ (EX\varphi) \mid (EF\varphi) \mid (EG\varphi) \mid E[\varphi \ U \ \varphi] \mid \\ (AX\varphi) \mid (AF\varphi) \mid (AG\varphi) \mid A[\varphi \ U \ \varphi]$$

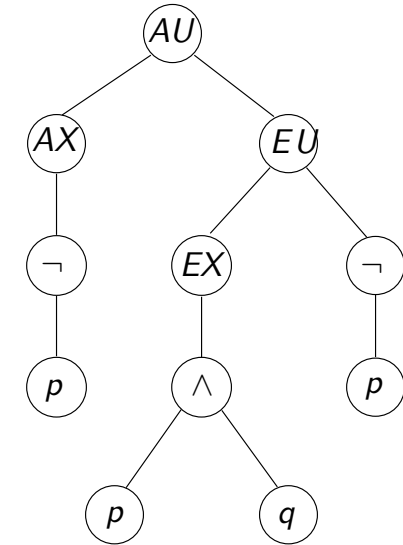
- EX , AX , EF , AF , EG , AG , EU , AU są spójnikami temporalnymi **CTL**; ostatnie dwa są binarne i zapisywane w wymyślny sposób
- spójniki temporalne występują w parach, poprzedzone odpowiednimi „kwantyfikatorami ścieżkowymi” A i E
- EX , AX , EF , AF , EG , AG wiążą najmocniej, a EU , AU oraz $\rightarrow$ – najslabiej

Semantyka logiki CTL

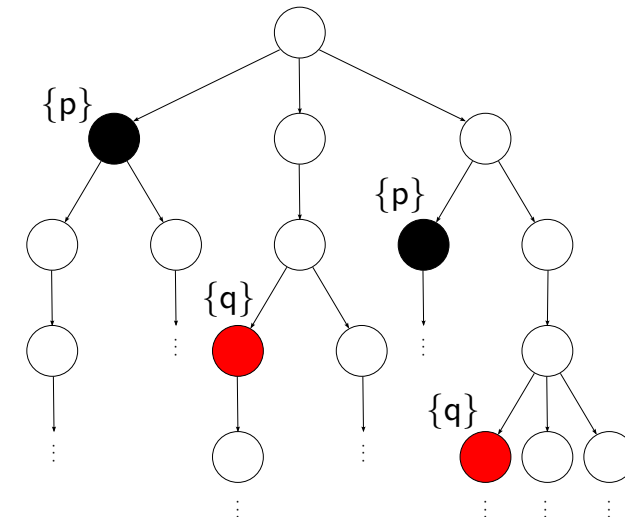
- modele takie same jak dla **LTL** (system tranzycji – stany i tranzycje, spełnialność formuły w stanie modelu)
- formuły atomowe oraz formuły ze spójnikami logiki zdaniowej – oczywista semantyka
- formuła z kwantyfikatorem ścieżkowym A – podobnie jak dla **LTL**: dla każdej ścieżki rozpoczynającej się w danym stanie zachodzi odpowiednia formuła
- formuła z kwantyfikatorem ścieżkowym E – istnieje ścieżka rozpoczynająca się w danym stanie i spełniająca odpowiednią formułę

Składnia formuł – przykłady

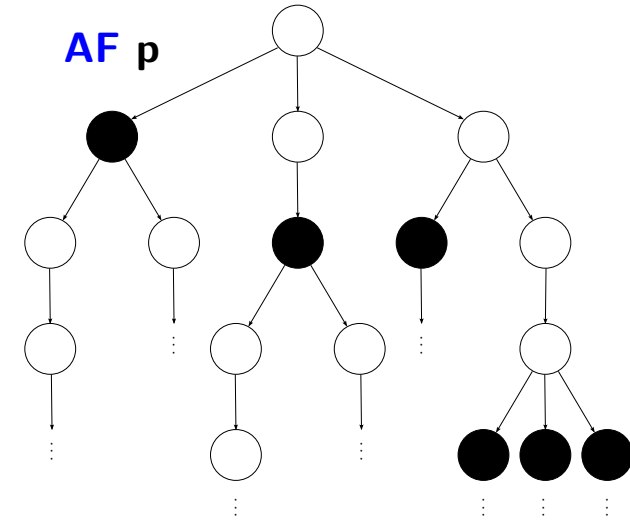
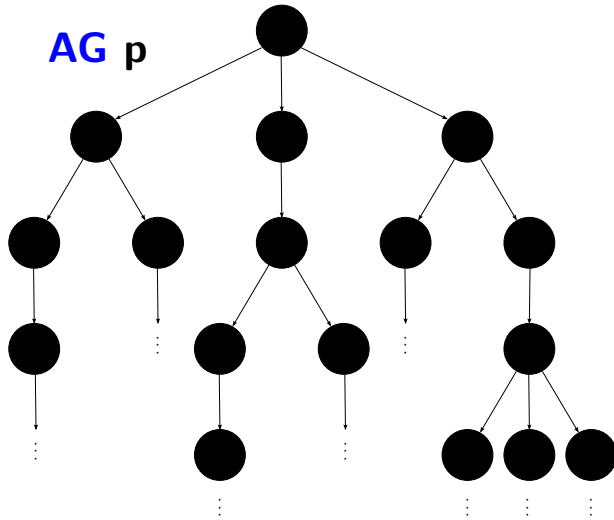
- poprawnych
 - $AG(q \rightarrow EGr)$
 - $AGq \rightarrow EGr$
 - $A[p \ U \ EFq]$
 - $E[A[p_1 \ U \ p_2] \ U \ p_3]$
- niepoprawnych
 - $A\neg G\neg p$
 - $A[(p \ U \ q) \wedge (q \ U \ r)]$
- na rysunku
 $A[AX\neg p \ U \ E[EX(p \wedge q) \ U \ \neg p]]$



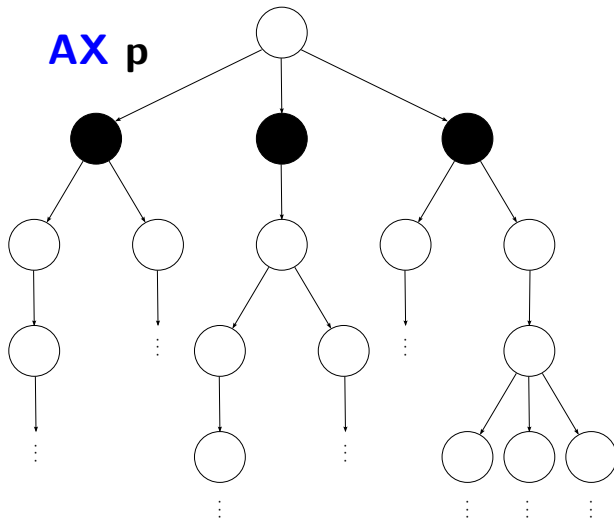
CTL



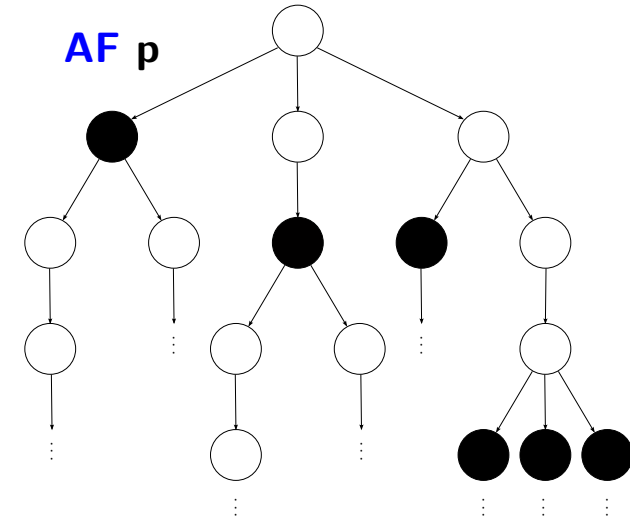
Semantyka CTL – spójnik AF



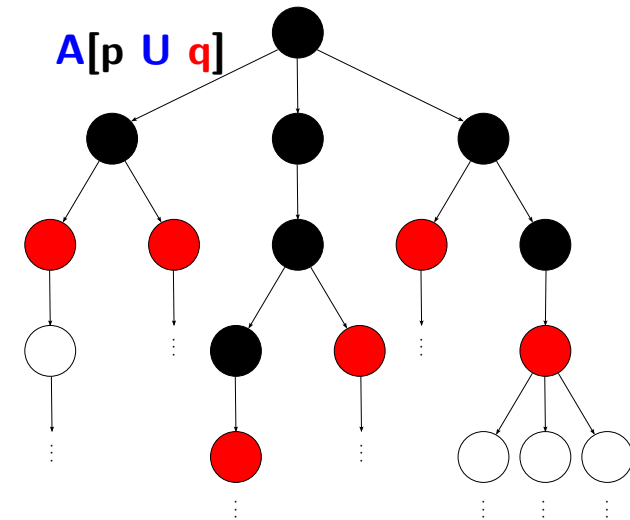
Semantyka CTL – spójnik AX



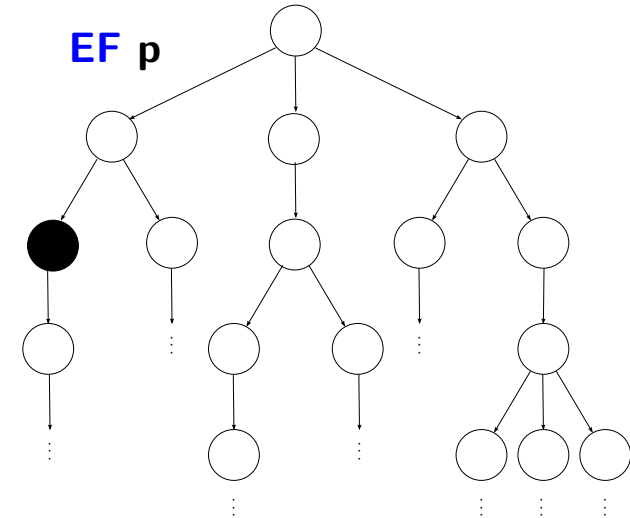
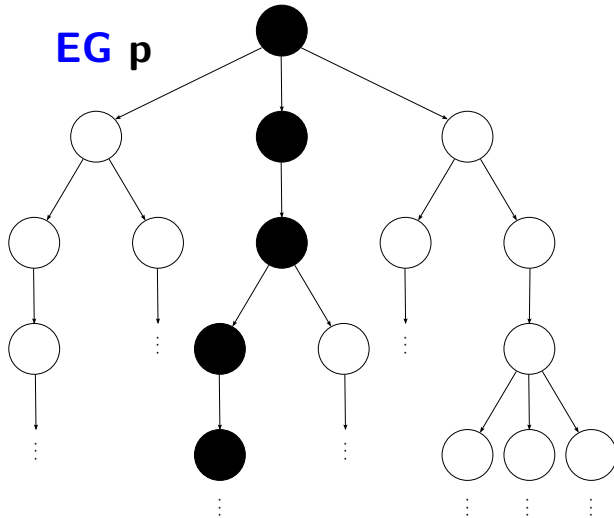
Semantyka CTL – spójnik AF



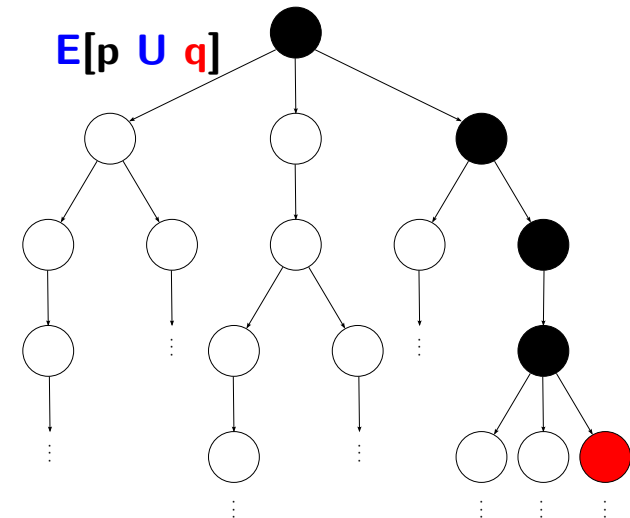
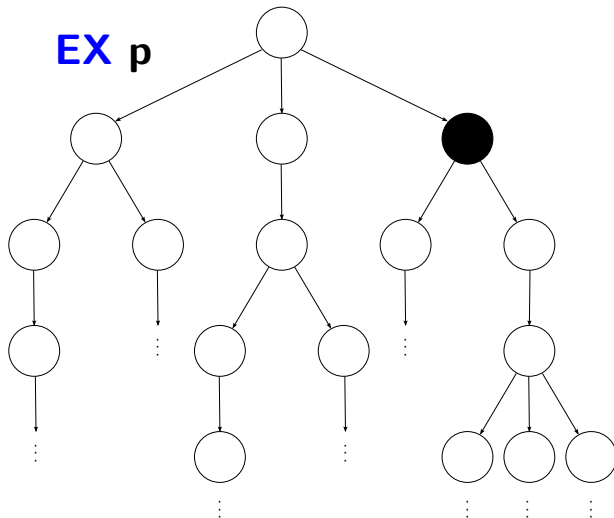
Semantyka CTL – spójnik AU



Semantyka CTL – spójnik EF



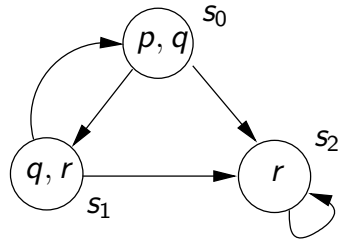
Semantyka CTL – spójnik EU



Semantyka CTL – przykłady formuł

jest prawdą, że:

- $\mathcal{M}, s_0 \models p \wedge q$
- $\mathcal{M}, s_0 \models \neg r$
- $\mathcal{M}, s_0 \models EX(q \wedge r)$
- $\mathcal{M}, s_0 \models \neg AX(q \wedge r)$
- $\mathcal{M}, s_0 \models \neg EF(p \wedge r)$
- $\mathcal{M}, s_1 \models EG r$
- $\mathcal{M}, s_0 \models AF r$
- $\mathcal{M}, s_0 \models A[(p \wedge q) \cup r]$
- $\mathcal{M}, s_0 \models AG EF EG r$



$\mathcal{M} = (S, \rightarrow, L)$

Przykładowe formuły c.d.

- winda jadąca w górę i mijająca pierwsze piętro nie zatrzyma się, jeśli są wezwania do jazdy na piąte piętro:
 $AG(\text{piętro_1} \wedge w_górę \wedge na_piętro_5 \rightarrow A[w_górę \cup \text{piętro_5}])$
- winda może nieruchomo stać na trzecim piętrze:
 $AG(\text{piętro_3} \wedge nieruchoma \rightarrow EG(\text{piętro_3} \wedge nieruchoma))$
- proces może zawsze zażądać wejścia do sekcji krytycznej:
 $AG(n \rightarrow EX t)$
- procesy nie muszą wchodzić do sekcji krytycznej po kolei:
 $EF(c_1 \wedge E[c_1 \cup (\neg c_1 \wedge E[\neg c_2 \cup c_1])])$

Przykładowe formuły

- może się okazać, że po włączeniu urządzenie nie jest gotowe do pracy:
 $EF(włącz \wedge \neg gotowe)$
- każde żądanie będzie kiedyś potwierdzone:
 $AG(\text{żądanie} \rightarrow AF \text{potwierdzenie})$
- pewien proces ma gwarancję, że będzie nieskończenie wiele razy umożliwiany: $AG AF \text{umożliwiony}$
- jeśli proces jest umożliwiony nieskończenie wiele razy, to jest również wykonany nieskończenie wiele razy – jest to przykład własności niewyraźnej w logice **CTL**, np.
 - $AG AF \text{umożliwiony} \rightarrow AG AF \text{działa}$
jest znacznie słabszą formułą (więcej żąda w założeniu)
- inny proces na pewno kiedyś zostanie zakleszczony:
 $AF AG \text{zakleszczony}$
- zawsze można wrócić do punktu wyjścia: $AG EF \text{początek}$

Równoważności formuł CTL

- „kwantyfikatory ścieżkowe” A i E przebiegają zbiory ścieżek, a spójniki F i G „kwantyfikują” po stanach na danej ścieżce
- działają więc prawa deMorgana:

$$\neg AF \varphi \equiv EG \neg \varphi, \quad \neg EF \varphi \equiv AG \neg \varphi, \quad \neg AX \varphi \equiv EX \neg \varphi$$

$$AF \varphi \equiv A[\top \cup \varphi], \quad EF \varphi \equiv E[\top \cup \varphi]$$

$$A[\varphi \cup \psi] \equiv \neg(E[\neg \psi \cup (\neg \varphi \wedge \neg \psi)] \vee EG \neg \psi)$$

Twierdzenie

Minimalny zbiór spójników **CTL** zawiera jeden z $\{AX, EX\}$, jeden z $\{EG, AF, AU\}$ oraz EU (potrzebny, bo w **CTL** brak W i R).

Logika CTL*

- wiele formuł **LTL** ma łatwe tłumaczenie na **CTL**
- ale formuła $F p \rightarrow F q$ nie da się przetłumaczyć
- formuła **CTL** musi mieć połączony kwantyfikator dla ścieżki i dla stanu na ścieżce
- nie można dla jednej ścieżki umieścić dwóch kwantyfikatorów jak powyżej
- CTL*** nie narzuca takich ograniczeń
 - $A[F p \rightarrow F q]$ – powyższa formuła LTL, na każdej ścieżce, jeśli ma się zdarzyć p to i q również
 - $A[(p U r) \vee (q U r)]$ – są ścieżki dwóch rodzajów
 - $A[X p \vee X X p]$ – najdalej za dwa kroki p
 - $E[GF p]$ – istnieje ścieżka, na której p zachodzi nieskończenie wiele razy

Zależności pomiędzy logikami LTL, CTL i CTL*

- $E[GF p]$ – istnieje ścieżka z nieskończoną liczbą wystąpień p – nie należy ani do **LTL** ani do **CTL**
- $AG EF p$ – zawsze możemy dojść do własności p – nie należy do **LTL**, należy do **CTL**
- $A[GF p \rightarrow F q]$ – dla wszystkich ścieżek, jeśli jest nieskończenie wiele żądań p , to zostaną one zaspokojone q – nie należy do **CTL**, ale należy do **LTL**
- $AG(p \rightarrow AF q)$ – zawsze po p nastąpi kiedyś q – należy do **CTL** i do **LTL** (w zapisie $G(p \rightarrow F q)$)

Logika CTL*

Gramatyka:

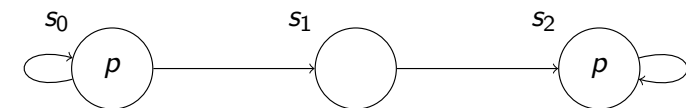
$$\varphi ::= \top \mid p \mid A[\alpha] \mid E[\alpha] \mid (\neg \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi)$$

$$\alpha ::= \varphi \mid (X \varphi) \mid (F \varphi) \mid (G \varphi) \mid (\varphi U \varphi) \mid (\neg \alpha) \mid (\alpha \wedge \alpha) \mid (\alpha \vee \alpha)$$

- formuły φ dotyczą stanów, semantyka $\mathcal{M}, s \models \varphi$
- formuły α dotyczą ścieżek, semantyka $\mathcal{M}, \pi \models \alpha$
- formuły **LTL** mogą być przekształcone w formuły **CTL***: $\alpha \mapsto A[\alpha]$
- formuły **CTL** są formułami **CTL***, mianowicie formuły ścieżkowe zaczynają się od spójnika X, F, G lub U .

LTL, CTL, CTL*, dalsze przykłady

- $FG p$ – na każdej ścieżce ustabilizuje się p
nie da się wyrazić w **CTL**:



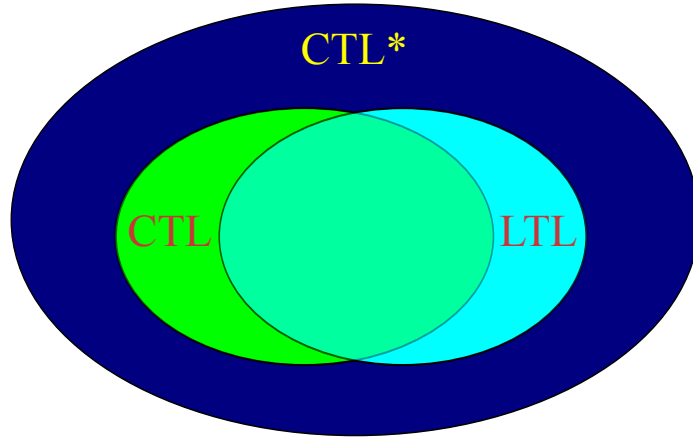
$AF AG p$ jest mocniejsze – na każdej ścieżce dojdziemy do punktu, na którym musi być nieodwołalnie p

na pętli s_0 nie dojdziemy do stanu, w którym jest $AG p$

$AF EG p$ zachodzi ale jest oczywiście słabszym warunkiem
gdyby stan s_1 też miał pętlę, to powyższa formuła byłaby nadal spełniona (istnieje możliwość stabilizacji) ale formuła LTL nie byłaby spełniona (nie każda ścieżka gwarantuje p)

- $FX p \Leftrightarrow XF p$ w LTL
w CTL $AX AF p$ znaczy to samo ale $AF AX p$ jest silniejsze

Zależności pomiędzy logikami LTL, CTL i CTL*



Operatory Boolowskie w CTL

- $A[F p \rightarrow F q]$ nie należy do **CTL** (dowód niełatwy)
- $E[F p \wedge F q]$ można przetłumaczyć na **CTL** – istnieje ścieżka, na której zdarzy się kiedyś i p i q , nie wiadomo co prędkiej, ale na pewno można stwierdzić $EF(p \wedge EF q) \vee EF(q \wedge EF p)$
- podobnie można potraktować $E[p_1 U q_1 \wedge p_2 U q_2]$
- $E[\neg(p U q)]$ można wyrazić $E(\neg q U (\neg p \wedge \neg q)) \vee EG\neg q$