Notite Modele de Securitate

Andrei Cristian
andrei.cristian1@info.uaic.ro

May 23, 2021

Logica propozitionala:

- $\varphi ::= p|\neg\varphi|\varphi \vee \varphi|\varphi \wedge \varphi|\varphi \rightarrow \varphi|\varphi \leftrightarrow \varphi$, $p \in \mathcal{AP}$.
- $\varphi_1 \wedge \varphi_2 = \neg(\varphi_1 \vee \varphi_2)$
- $\varphi_1 \rightarrow \varphi_2 = \neg\varphi_1 \vee \varphi_2$
- $\varphi_1 \leftrightarrow \varphi_2 = (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$

Logica modala:
Structura Kripke $M < W, R, L >$:

1. W = set nevid (cu cuvinte)
2. $R \subseteq W \times W$ = relatia de accesibilitate dintre lumi
3. $L : W \rightarrow 2^{\mathcal{AP}}$ = functia de etichetare

Data o structura Kripke $M =< W, R, L >$, o lume $w \in W$ si doua formule BML φ si ψ, avem:

- $M, w \models p$ ddaca $p \in L(w)$
- $M, w \models \neg\varphi$ ddaca $M, w \not\models \varphi$
- $M, w \models \varphi \vee \psi$ ddaca $M, w \models \varphi$ sau $M, w \models \psi$
- $M, w \models \Box\varphi$ ddaca $\forall t \in W, (w, t) \in R \Rightarrow M, t \models \varphi$
- $M, w \models \Diamond\varphi$ ddaca $\exists t \in W, (w, t) \in R \Rightarrow M, t \models \varphi$

Spunem ca un **model satisface o formula** φ daca pentru **orice lume din model** o satisface. Scriem

$$M \models \varphi \Leftrightarrow M, w \models \varphi, \forall w \in W$$

- O structura Kripke $\mathcal{M}$ este definita peste un frame $\mathcal{F}$ ddaca **exista** o functie de etichetare $L : W \rightarrow 2^{\mathcal{AP}}$ a.i. $M =< W, R, L >$.
- O formula BML φ este **valida intr-un frame** $\mathcal{F}(\mathcal{F} \models \varphi)$ ddaca φ este **global adevarat in orice structura Kripke** $\mathcal{M}$ definita peste $\mathcal{F}$.

Scheme de formula si propietati ale lui R

- **T**: $\Box\varphi \rightarrow \varphi$: reflexiv
- **B**: $\varphi \rightarrow \Box\Diamond\varphi$: simetric
- **D**: $\Box\varphi \rightarrow \Diamond\varphi$: serial
- **4**: $\Box\varphi \rightarrow \Box\Box\varphi$: tranzitiv
- **5** $\Diamond\varphi \rightarrow \Box\Diamond\varphi$: Euclidian
- $(\Box\varphi \rightarrow \Diamond\varphi) \wedge (\Diamond\varphi \rightarrow \Box\varphi)$: functional

KT45 si Agenti multisisistem

- KT45 - Folosit pt. rationamentul despre cunoastere:
  - T: **Adevar**: Agentul Q stie doar lucrurile adevarate
  - 4: **Introspectie pozitiva**: Daca Q stie ceva, at. el stie ca stie
  - 5: **Introspectie negativa**: Daca Q nu stie ceva, at. el stie ca nu stie

$\Box\varphi$	$\Diamond\varphi$
Necesar adevarat ca φ	Este posibil adevarat ca φ
Intotdeauna adevarat ca φ	Candva in viitor φ
Ar trebui sa fie a.i. φ	Este permis sa fie a.i. φ
Agentul Q crede ca φ	φ in concordanta cu credintele lui Q
Agentul Q stie ca φ	Din tot ce cunoaste Q, φ
Dupa orice rulare a P, φ tine	Dupa o rulare a lui P, φ tine

Posibile proprietati ale lui R:

- **reflexiv**: $\forall w \in W, \exists R(x, x)$
- **simetric**: $\forall x, y \in W, \exists R(x, y) \rightarrow R(y, x)$
- **de serie**: $\forall x, \exists y$ a.i. $R(x, y)$
- **tranzitiv**:$\forall x, y, z \in W, \exists R(x, y) \wedge R(y, z) \rightarrow R(x, z)$
- **Euclidian**:$\forall x, y, z \in W, R(x, y) \wedge R(x, z) \rightarrow \exists R(y, z)$
- **functional**:$\forall x, \exists y$ unic a.i. $R(x, y)$.
- **linear**: $\forall x, y, z \in W, R(x, y) \wedge R(x, z) \rightarrow R(y, z) \vee y = z \vee R(z, y)$
- **total**: $\forall x, y \in W, \exists R(x, y) \wedge R(y, x)$
- **echivalenta**: reflexiv, simetric, tranzitiv.

Frameuri

- Un **frame** este o tupla $\mathcal{F} =< W, R >$.

KT45 poate fi aplicat doar la un agent $\rightarrow$ introducem $KT45^n$ pt. **sisteme multiagent**.

- Fie un set de agenti $A = \{1, 2, 3, ..n\}$
- In loc de $\Box$, vom folosi K_i pentru a specifica ce stie agentul i.
- Daca avem $\mathcal{AP} = \{p, q, r, ..\}$, $K_i p$ inseamna ca agentul i cunoaste ca p este adevarat.
- Ex: $K_1 p \wedge K_1 \neg K_2 K_1 p$ inseamna: Agent 1 stie p, si totodata stie ca Agent 2 nu cunoaste ca Agent 1 stie p.

Formule de **logica modala epistemica** sunt definite de:

$$\varphi ::= \top| \perp |p|\neg\varphi|\varphi \vee \varphi|K_i\varphi$$

unde $p \in \mathcal{AP}$ si $i \in \mathcal{A}$.

O structura Kripke pentru logica epistemica este o tupla $\mathcal{K} =< W, L, K_1, .., K_n >$, unde

- W - setul de lumi posibile
- L - functia de etichetare care asigneaza fiecarei stari setul de propozitii care sunt adevarate

$$L : W \to 2^{\mathcal{AP}}$$

- K_i este setul de relatii binare peste W, $\forall i \in 1..n$ (un set de perechi, fiecare pereche fiind formata din doua elemente din W)
- O pereche $(w_1, w_2) \in K_i$ inseamna ca agentul i nu deosebeste singur care dintre lumi $(w_1 or w_2)$ este realitatea
- Fiecare relatie dintre lummi (K_i) este o relatie de echivalenta:
  - reflexivitate: agentul nu vede diferenta dintre lumi
  - simetrie: daca agentul nu face deosebire intre lumile w_1 si w_2, atunci el nu va putea face deosebire intre lumile w_2 si w_1
  - tranzitivitate: daca agentul nu deosebeste w_1 de w_2 si nu deosebeste w_2 de w_3, atunci el nu deosebeste w_1 de w_3

Semantici ale logicii epistemice pentru sisteme multiagent
Semanticile unei formule φ din logica epistemica este definita in conformitate cu o strucutura Kripke
$\mathcal{K} =< W, L, K_1, ..K_n >$ si cu starea sistemului $x \in W$ astfel:

- $K, x \models \top$
- $K, x \not\models \perp$
- $K, x \models p$ ddaca $p \in L(p)$
- ...
- $K, x \models K_i\varphi$ ddaca $\forall x' \in W$ cu $(x, x') \in K_i$, avem ca $K, x' \models \varphi$

Operatori pentru grupuri de agenti

- $E_G\varphi$
  - Oricine din grupul G cunoaste φ
  - Daca $G = \{1, 2, ...n\}$, atunci

$$K, x \models E_G\varphi \Leftrightarrow K, x \models K_1\varphi \wedge K_2\varphi \wedge .. \wedge K_n\varphi$$

- $C_G\varphi$
  - Toti agentii din G cunosc φ, iar fiecare dintre ei cunoaste ca toti dintre ei cunosc acest fapt
  - Cunoastere comuna intre agentii din grupul G asupra φ

$$K, x \models C_G\varphi \Leftrightarrow K, x \models E_G^k\varphi, \forall k \in N$$

$$(E_G^0\varphi \equiv \varphi, E_G^1\varphi \equiv E_G\varphi, E_G^2\varphi \equiv E_G E_G\varphi, ...)$$

- $D_G\varphi$
  - Toti agentii din G pot deduce φ daca toti is pun cunostintele in comun
  - Cunostintele distribuite intre agentii din G asupra φ

$$K, x \models D_G\varphi \Leftrightarrow K, y \models \varphi \text{ oricand } K_i(x, y), \forall i \in G$$

Model checking: Verificarea formala necesita:

- Un **model al sistemului**, deobicei format din
  - un set de stari, continand informatii despre valorile variabilelor si contoarelor de program
  - o relatie de tranzitie, care descrie cum sistemul poate sa se schimbe de la o stare la alta
- O **metoda de specificare** pt. a exprima cerintele intr-un mod formal
- Un **set de reguli de dovada** pt. a determina daca modelul satisface cerintele impuse

Modelare sistemelor: posibile comportamente

- O structura Kripke (sau Labelled Transition System) $\mathcal{M}$ peste $\mathcal{AP}$ este o tupla $\mathcal{M} = (S, S_0, \mathcal{AP}, \mathcal{R}, L)$, unde
  - S este un set finit de stari
  - $S_0 \subseteq S$ este setul de stari intiale
  - $\mathcal{AP}$ este setul finit de proprietati atomice
  - $\mathcal{R} \subseteq S \times S$ este relatia de tranzitie care trebuie sa fie totala - pt. fiecare stare $s \in S$ exista o stare $s' \in S$ astfel incat $\mathcal{R}(s, s')$
  - $L : S \to 2^{\mathcal{AP}}$ este o functie care eticheteaza fiecare stare cu setul de propozitii atomice care sunt adevarate in acea stare
- Un **drum** in structura M de la o stare s este *o secventa infinita de stari*

$$\pi = s_0 s_1 s_2 ...$$

  a.i. $\mathcal{R}(s_i, s_{i+1})$ tine pentru toti $i \geq 0$.
- Arborele de calcul a unei structuri Kripke etichetate este **desfasurarea aciclica** a sa.

Logici temporale

- **Linear-time Temporal Logic (LTL)**
  - O formula LTL peste $\mathcal{AP}$ este definita de

$$\varphi ::= p | \neg\varphi | \varphi \vee \varphi | X\varphi | \varphi_1 \mathcal{U} \varphi_2$$

  unde $p \in \mathcal{AP}$.

Precedenta operatorilor		
Operator	Nume	Prioritate
$\neg$	Negare	0
X	Next	0
G	Intotdeauna	0
F	Eventual	0
$\mathcal{U}$	Pana cand	1
$\mathcal{R}$	Release	1
$\wedge$	Conjunctie	2
$\vee$	Disjunctie	2

- **Semantici LTL** Fie $\pi = s_0, s_1, ...$ un drum si φ o formula LTL. Definim notiunea "φ este adevarata in π", notata prin $\pi, 0 \models \varphi$, folosind inductia:
  - $\pi, i \models \top$
  - $\pi, i \models p$ ddaca $p \in L(s_i)$
  - $\pi, i \models \varphi_1 \wedge \varphi_2$ ddaca $\pi, i \models \varphi_1$ si $\pi, i \models \varphi_2$
    $\pi, i \models \varphi_1 \vee \varphi_2$ ddaca $\pi, i \models \varphi_1$ sau $\pi, i \models \varphi_2$
  - $\pi, i \models \neg\varphi$ ddaca $\pi, i \not\models \varphi$
  - $\pi, i \models X\varphi$ ddaca $\pi, i+1 \models \varphi$
  - $\pi, i \models \varphi_1 \mathcal{U} \varphi_2$ ddaca $\exists j \geq i$ a.i. $\pi, j \models \varphi_2$ si $\pi, k \models \varphi_1$ pt toti $i \leq k < j$
  - $\pi, i \models \varphi_1 \mathcal{R} \varphi_2$ ddaca $\forall j \geq i$ a.i $(\forall k \leq j)\pi,\ k \not\models \varphi_1 \rightarrow \pi, j \models \varphi_2$

- **Branching-time Temporal Logjc (CTL* si CTL)**
  - **O formula CTL*** peste $\mathcal{AP}$ este definita de

    $$\varphi ::= p|\neg\varphi|\varphi \vee \varphi|E\varphi|A\varphi|X\varphi|\varphi_1 \mathcal{U} \varphi_2$$

    unde $p \in \mathcal{AP}$
  - **O formula CTL** peste $\mathcal{AP}$ este definita de

    $$\varphi ::= p|\neg\varphi|\varphi\vee\varphi|EX\varphi|AX\varphi|E(\varphi_1 \mathcal{U} \varphi_2)|A(\varphi_1 \mathcal{U} \varphi_2)$$

    unde $p \in \mathcal{AP}$
  - **Semantici CTL si CTL*** Fie $\pi = s_0, s_1, s_2, ...$ un drum si φ o formula CTL*. Daca π_i este sufixul lui π incepand cu pozitia i, atunci
    - $\pi, i \models \top$
    - $\pi, i \models p$ ddaca $p \in L(s_i)$
    - $\pi, i \models \neg\varphi$ ddaca $\pi, i \not\models \varphi$
    - $\pi, i \models \varphi_1 \vee \varphi_2$ ddaca $\pi, i \models \varphi_1$ sau $\pi, i \models \varphi_2$
    - $\pi, i \models X\varphi$ ddaca $\pi, i+1 \models \varphi$
    - $\pi, i \models \varphi_1 \mathcal{U} \varphi_2$ ddaca $\exists j \geq i$ a.i. $\pi, j \models \varphi_2$ si $\pi, k \models \varphi_1$ pt toti $i \leq k < j$
    - $\pi, i \models E\varphi$ ddaca exista un drum infinit $\pi' = s'_0, s'_1, ...$ cu $s'_0 = s_i$ si $\pi', 0 \models \varphi$
    - $\pi, i \models A\varphi$ ddaca pt. orice drum infinit $\pi' = s'_0, s'_1, ...$ cu $s'_0 = s_i$ avem $\pi', 0 \models \varphi$

- **Rezolvarea problemelor de verificare model** Definim:

  $$pre_\exists(Y) = \{s \in S \mid \exists s' \in Y\ s.t.\ (s, s') \in \mathcal{R}\}$$

  $$pre_\forall(Y) = \{s \in S \mid \mathcal{R}(s) \subseteq Y\}$$

  Calculeaza $[\![\varphi]\!] = \{s \in S \mid s \models \varphi\}$

  $$[\![p]\!] = \{s \in S \mid p \in L(s)\}$$

  $$[\![\neg\varphi]\!] = S \setminus [\![\varphi]\!]$$

  $$[\![\varphi_1 \vee \varphi_2]\!] = [\![\varphi_1]\!] \cup [\![\varphi_2]\!]$$

  $$[\![EX\varphi]\!] = pre_\exists([\![\varphi]\!])$$

  $$[\![AF\varphi]\!] = MC^{AF}_{CTL}(\varphi)$$

  $$[\![E(\varphi_1 \mathcal{U} \varphi_2]\!] = MC^{EU}_{CTL}(\varphi_1, \varphi 2)$$

  Testeaza daca staterea de input $s \in [\![\varphi]\!]$.

  $MC^{AF}_{CTL}(\varphi)$ este calculat astfel:
  - $Y := S;\ Z := [\![\varphi]\!];$
  - **while** $Y \neq Z$ do:
    - $Y = Z;$
    - $Z = Z \cup pre_\forall(Z);$
  - return Y;

  $MC^{EU}_{CTL}(\varphi_1, \varphi_2)$ este calculat astfel:
  - $Y := \emptyset;\ Z := [\![\varphi_2]\!];$
  - **while** $Z \not\subseteq Y$ **do**:
    - $Y = Y \cup Z;$
    - $Z = pre_\exists(Y) \cap [\![\varphi_1]\!]'$
  - return Y;

Un sistem de tranzitii etichetat (LTS) este o tupla $\mathcal{M} =< \mathcal{AP}, S, S_0, \mathcal{R}, L >$, unde

- $\mathcal{AP}$ - setul de etichete (propositii atomice)
- S - setul finit de stari
- $S_0 \in S$ - setul de stari initiale
- $\mathcal{R} \subseteq S \times S$ - relatia de tranzitie
- $L : S \rightarrow 2^{\mathcal{AP}}$ - functia de etichetare (**fiecare stare este etichetata cu un set de propozitii!**)
- O **rulare** (finita/infinita) p in $\mathcal{M}$ este o secventa $p = s_0 s_1 s_2 ...$, unde
  - $s_0 \in S_0$ este o stare initiala a lui $\mathcal{M}$.
  - $\forall i \geq 0,\ s_i, s_{i+1}) \in \mathcal{R}$.
- **trace(p)** $= L(s_0)L(s_1)L(s_2)...$
- **Traces($\mathcal{M}$)** = {trace(p) — p o rulare in $\mathcal{M}$} este setul de **traces** (urme) ale lui $\mathcal{M}$.
- Expresii regulate pentru a exprima proprietati pentru rulari finite.

- Linear-time Temporal Logic (LTL) pt. a exprima propr. pt. rulari infinite.

Sintaxa LTL

$$\varphi ::= p|\neg\varphi|\varphi \vee \varphi|X\varphi|\varphi\mathcal{U}\varphi$$

Definim urmatoarele macro:

- $F\varphi = true\mathcal{U}\varphi$
- $G\varphi = \neg F\neg\varphi$
- $\varphi_1\mathcal{R}\varphi_2 = G\varphi_2 \vee \varphi_2\mathcal{U}(\varphi_1 \wedge \varphi_2)$

Semantici LTL pt. un cuvant
$w = w_0w_1w_2... \in (2^{\mathcal{AP}})^\omega$ si o pozitie $i \geq 0$

- $w, i \models p$ ddaca $p \in w_i$
- $w, i \models \neg\varphi$ ddaca $w, i \not\models \varphi$
- $w, i \models \varphi_1 \vee \varphi_2$ ddaca $w, i \models \varphi_1$ sau $w, i \models varphi_2$
- $w, i \models X\varphi$ ddaca $w, i+1 \models \varphi$
- $w, i \models \varphi_1\mathcal{U}\varphi_2$ ddaca $\exists j \geq i$ a.i. $w, j \models \varphi_2$ si $w, k \models \varphi_1, \forall i \leq k < j$
- **Limbajul lui** φ: $\mathcal{L}(\varphi) = \{w \in (2^{\mathcal{AP}})^\omega | w, 0 \models \varphi\}$

Pt. a verifica daca $\mathcal{M}$ satisface o formula LTL φ:

$$Traces(\mathcal{M}) \subseteq \mathcal{L}(\varphi) \equiv Traces(\mathcal{M}) \cap \mathcal{L}(\neg\varphi) = \emptyset$$

Automat Büchi nedeterminist (NBA) este o tupla
$\mathcal{A} =< 2^{\mathcal{AP}}, Q, Q_0, \delta, T)$, unde

- $2^{\mathcal{AP}}$ este alfabetul
- Q este setul de stari
- $Q_0 \subseteq Q$ este setul de stari initiale
- $\delta \subseteq Q^{\mathcal{AP}} \times Q$ este relatia de tranzitie
- $T \subseteq Q$ este setul de stari acceptante

NBA - Proprietati de inchidere

- Reuniunea: $\mathcal{A}_\cup =< 2^{\mathcal{AP}}, Q', Q'_0, \delta', T' >$ a.i. $\mathcal{L}(\mathcal{A}_\cup) = \mathcal{L}(\mathcal{A}_1) \cup \mathcal{L}(\mathcal{A}_2)$
  - $\mathcal{A}_1 =< 2^{\mathcal{AP}}, Q_1, Q_0^1, \delta_1, T_1 >$
  - $\mathcal{A}_2 =< 2^{\mathcal{AP}}, Q_2, Q_0^2, \delta_2, T_2 >$
  - $Q' = Q_1 \cup Q_2$
  - $Q'_0 = Q_0^1 \cup Q_0^2$
  - $\delta' = \delta_1 \cup \delta_2$
  - $T' = T_1 \cup T_2$
- Intersectia - **cazul special**
  $\mathcal{A}_\cap =< 2^{\mathcal{AP}}, Q', Q'_0, \delta', T' >$ a.i. $\mathcal{L}(\mathcal{A}_\cap) = \mathcal{L}(\mathcal{A}_1) \cap \mathcal{L}(\mathcal{A}_2)$
  - $\mathcal{A}_1 =< 2^{\mathcal{AP}}, Q_1, Q_0^1, \delta_1, Q_1 >$ **- toate starile din $\mathcal{A}_1$ sunt acceptante**
  - $\mathcal{A}_2 =< 2^{\mathcal{AP}}, Q_2, Q_0^2, \delta_2, T_2 >$
  - $Q' = Q_1 \times Q_2$
  - $Q'_0 = Q_0^1 \times Q_0^2$
  - $((q_1, q_2), a, (q'_1, q'_2)) \in \delta'$ ddaca $(q_1, a, q'_1) \in \delta_1$ si $(q_2, a, q'_2) \in \delta_2$
  - $T' = Q_1 \times T_2$
- Intersectia - **cazul general**
  $\mathcal{A}_\cap =< 2^{\mathcal{AP}}, Q', Q'_0, \delta', T' >$ a.i. $\mathcal{L}(\mathcal{A}_\cap) = \mathcal{L}(\mathcal{A}_1) \cap \mathcal{L}(\mathcal{A}_2)$
  - $\mathcal{A}_1 =< 2^{\mathcal{AP}}, Q_1, Q_0^1, \delta_1, T_1 >$
  - $\mathcal{A}_2 =< 2^{\mathcal{AP}}, Q_2, Q_0^2, \delta_2, T_2 >$
  - $Q' = Q_1 \times Q_2 \times \{1, 2\}$
  - $Q'_0 = Q_0^1 \times Q_0^2 \times \{1\}$
  - $((q_1, q_2, 1), a, (q'_1, q'_2, 1)) \in \delta'$ ddaca $(q_1, a, q'_1) \in \delta_1$, $(q2, a, q'_2) \in \delta_2$ si $q_1 \notin T_1$
    $((q_1, q_2, 1), a, (q'_1, q'_2, 2)) \in \delta'$ ddaca $(q_1, a, q'_1) \in \delta_1$, $(q2, a, q'_2) \in \delta_2$ si $q_1 \in T_1$
    $((q_1, q_2, 2), a, (q'_1, q'_2, 2)) \in \delta'$ ddaca $(q_1, a, q'_1) \in \delta_1$, $(q2, a, q'_2) \in \delta_2$ si $q_2 \notin T_2$
    $((q_1, q_2, 2), a, (q'_1, q'_2, 1)) \in \delta'$ ddaca $(q_1, a, q'_1) \in \delta_1$, $(q2, a, q'_2) \in \delta_2$ si $q_2 \in T_2$
  - $T' = \{q_1, q_2, 2) | q_1 \in Q_1$ si $q_2 \in T_2\}$
- Complementul: $\overline{\mathcal{A}_1} =< 2^{\mathcal{AP}}, Q', Q'_0, \delta', T' >$ a.i. $\mathcal{L}(\overline{\mathcal{A}_1}) = \overline{\mathcal{L}(\mathcal{A}_1)}$ **- greu de complimentat automate Büchi**, dar
  $\mathcal{L}(\mathcal{A}_1) = \mathcal{L}(\varphi)$ pt. unele formule LTL si $\overline{\mathcal{L}(\mathcal{A}_1)} = \mathcal{L}(\neg\varphi)$. **Construim direct automatul pt.** $\neg\varphi$ (daca stim φ).

Construirea unui NBA dintr-o formula LTL este facuta in 3 pasi:

1. Rescrierea formulei in **Forma Normala Negativa (NNF)** si **aplicarea regulilor de rescriere**.
2. Transformarea formulei LTL intr-un **Automat Büchi Generalizat (GBA)**.
3. Transformarea GBA-ului intr-un NBA.

1. Din LTL in NBA - Rescrierea

- O formula este in NNF daca este de urmatoarea sintaxa:

  $$\varphi ::= \top | \perp | p | \neg p | \varphi \vee \varphi | \varphi \wedge \varphi | X\varphi | \varphi\mathcal{U}\varphi | \varphi\mathcal{R}\varphi$$

- Scrie formula in NNF
- Negarea apare doar in fata literalilor
- Foloseste urmatoarele identitati pt. propagarea negatiei:

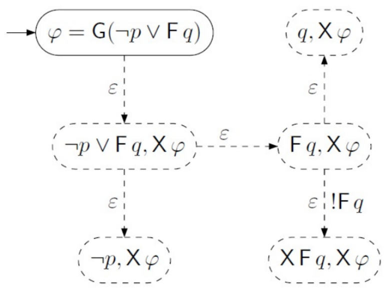
$$\neg\neg\varphi \equiv \varphi$$
$$\neg X\varphi \equiv X\neg\varphi$$
$$\neg G\varphi \equiv F\neg\varphi$$
$$\neg F\varphi \equiv G\neg\varphi$$
$$\neg(\varphi_1\mathcal{U}\varphi_2) \equiv (\neg\varphi_1)\mathcal{R}(\neg\varphi_2)$$
$$\neg(\varphi_1\mathcal{R}\varphi_2) \equiv (\neg\varphi_1)\mathcal{U}(\neg\varphi_2)$$

2. Din LTL in NBA - Din LTL in GBA

- O stare a automatului $\mathcal{A}_\varphi$ este un **set consistent Z** de subformule ale lui φ.
- Un set $Z \subseteq Sub(\varphi)$ este **consistent** daca nu contine $\perp$ sau o pereche $\{\psi, \neg\psi\}$.
- Daca o rulare ρ pe un cuvant w incepe in Z si satisface conditia de acceptare, atunci

$$w, 0 \models \bigwedge_{\psi \in Z} \psi.$$

- Singura stare initiala a lui $\mathcal{A}_\varphi$ este $Z = \{\varphi\}$.
- Tranzitiile catre urmatoarele stari sunt date de formule de forma $X\psi$ de la Z.
- Z trebuie redus a.i. toate formulele din Z sa fie fie literali, fie de forma $X\psi$.
- Reducere folosind $\epsilon - tranzitii$ pt. seturi arbitrare Y de formule
  - $\psi = \psi_1 \wedge \psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_1, \psi_2\}$
  - $\psi = \psi_1 \vee \psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_1\}$, $Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_2\}$
  - $\psi = \psi_1 \mathcal{R} \psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_1, \psi_2\}$, $Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_2, X\psi\}$
  - $\psi = G\psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_2, X\psi\}$
  - $\psi = \psi_1 \mathcal{U} \psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_2\}$, $Y \xrightarrow[!\psi]{\epsilon} Y \backslash \{\psi\} \cup \{\psi_1, X\psi\}$
  - $\psi = F\psi_2 : Y \xrightarrow{\epsilon} Y \backslash \{\psi\} \cup \{\psi_2\}$, $Y \xrightarrow[!\psi]{\epsilon} Y \backslash \{\psi\} \cup \{X\psi\}$
  - $!\psi$ inseamna ψ a fost amanat
- $Y \xrightarrow[*]{\epsilon} Z$ daca exista o secventa de ϵ-tranzitii de la Y la Z: $Red(Y) = \{Z \text{ consistent si redus} \mid Y \xrightarrow[*]{\epsilon} Z\}$ $Red_\alpha(Y) = \{Z$ consistent si redus $\mid Y \xrightarrow[*]{\epsilon} Z$ fara a se folosi o muchie marcata cu $!\alpha\}$ (vezi Figure 1)
- Fie $\Sigma_z = \{a \in 2^{\mathcal{AP}} | \forall p \in \mathcal{AP}, (p \in Z \rightarrow p \in a)$ si $(\neg p \in Z \rightarrow p \notin a)\}$
- Fie $U(\varphi) = \{\psi \in Sub(\varphi) | \psi = \psi_1 \mathcal{U} \psi_2$ sau $\psi = F(\psi_1)\}$ setul de formule *until* ale lui φ
- Fie $next(Z) = \{\varphi | X\varphi \in Z\}$
- GBA pentru φ este $B_\varphi =< 2^{\mathcal{AP}}, Q, Q_0, \delta, (T_\alpha)_{\alpha \in U(\varphi)} >$
  - $Q = 2^S ub(\varphi)$
  - $Q_0 = \{\{\varphi\}\}$
  - $\delta = \{Y \xrightarrow{a} next(Z) | Y \in Q, a \in \Sigma_Z$ si $Z \in Red(Y)\}$
  - $\forall \alpha \in U(\varphi), T_\alpha = \{Y \xrightarrow{a} next(Z) | Y \in Q, a \in \Sigma_Z$ si $Z \in Red_\alpha(Y)\}$ (vezi Figure 2)



$Red(\{\varphi\}) = \{\{\neg p, X\varphi\}, \{q, X\varphi\}, \{XFq, X\varphi\}\}$

$Red_{Fq}(\{\varphi\}) = \{\{\neg p, X\varphi\}, \{q, X\varphi\}\}$

Figure 1: $\varphi = G(\neg p \vee Fq)$

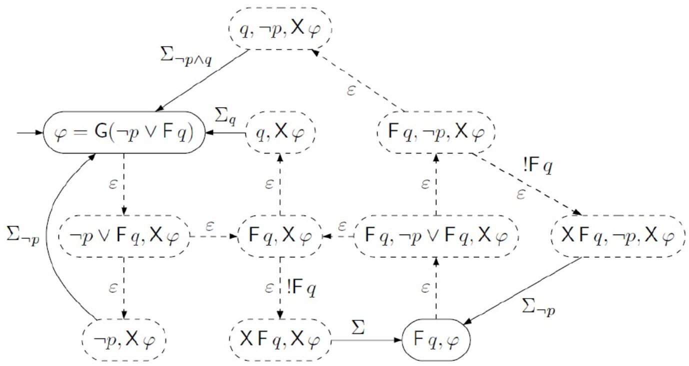


Figure 2: $\varphi = G(\neg p \vee Fq)$

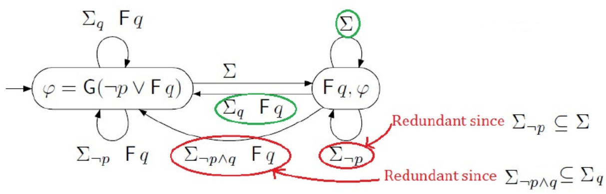


Figure 3: $\varphi = G(\neg p \vee Fq)$