
Γραμμική Χρονική Λογική (Linear Temporal Logic)

Στην ενότητα αυτή θα μελετηθούν τα εξής θέματα:

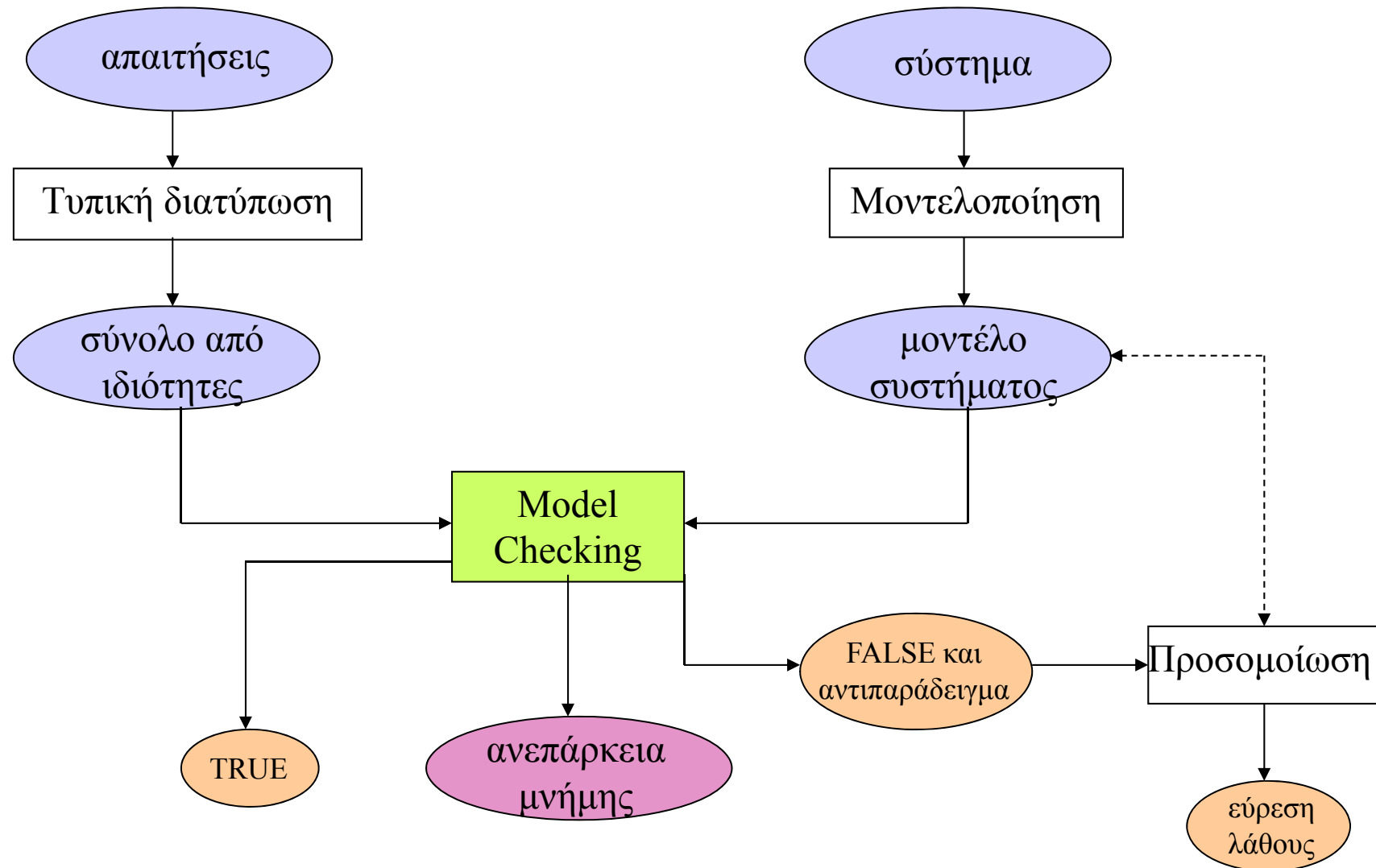
Γραμμική Χρονική Λογική - σύνταξη και ερμηνεία

Διατύπωση ιδιοτήτων

Δομές Kripke

Μοντελοέλεγχος

Model-checking



Ιδιότητες πρωτοκόλλων αμοιβαίου αποκλεισμού

- Σε ένα πρωτόκολλο αμοιβαίου αποκλεισμού (mutual exclusion) συνήθως επιζητούμε ικανοποίηση ιδιοτήτων όπως:
 - *Απαγορεύεται να βρίσκονται περισσότερες από μία διεργασίες στην κρίσιμή τους περιοχή ταυτόχρονα*
 - *Αν σε κάποια χρονική στιγμή μια διεργασία επιθυμεί να μπει στην κρίσιμή της περιοχή, τότε, κάποτε θα της δοθεί η άδεια για να το πράξει*
- Πως μπορούμε να εκφράσουμε τέτοιες ιδιότητες με σαφήνεια και ακρίβεια;

Ιδιότητες φώτων της τροχαίας

- Ιδιότητες που αναμένουμε να ικανοποιούνται από τα φώτα της τροχαίας περιλαμβάνουν
 - Από *κόκκινο* το φως δεν μπορεί να γίνει αμέσως *πράσινο*
 - Στο μέλλον το φως θα ξαναγίνει *πράσινο*
 - Από *κόκκινο* το φως θα γίνει *πράσινο* αφού περάσει από το *κίτρινο* για κάποιο χρονικό διάστημα
- Πως μπορούμε να εκφράσουμε τέτοιες ιδιότητες με σαφήνεια και ακρίβεια;
- Χρησιμοποιώντας *χρονική λογική* (temporal logic).

Χρονική και τροπική λογική

- “Γλώσσα” για τη διατύπωση ιδιοτήτων συστημάτων που αφορούν συμπεριφορά που μεταβάλλεται με τον χρόνο.
- Τροπικές λογικές (modal logics) αναπτύχθηκαν από φιλόσοφους για τη μελέτη διαφορετικών τρόπων “αλήθειας” (δυνατότητα και αναγκαιότητα, π.χ. “απαραίτητα ισχύει η Φ ”, “δυνατόν να ισχύει η Φ ”).
- Χρονικές λογικές (temporal logics) αποτελούν μια ειδική κατηγορία τροπικών λογικών όπου οι λογικές τιμές των ισχυρισμών μεταβάλλονται με τον χρόνο.
- Τυπικοί κατασκευαστές (χρονικοί τελεστές) είναι
 - $\Diamond p$ ή $F p$: Το p θα συμβεί σε κάποια μελλοντική στιγμή
 - $\Box p$ ή $G p$: Το p θα συμβεί σε κάθε μελλοντική στιγμή
- Η χρονική λογική χρησιμοποιείται συχνά για την προδιαγραφή και επαλήθευση συστημάτων αλληλεπίδρασης.

Ατομικές προτάσεις

- Οι *ατομικές προτάσεις* είναι τα βασικά στοιχεία μιας χρονικής λογικής και αντιστοιχούν σε λογικές εκφράσεις p, q, r που χρησιμοποιούν
 - μεταβλητές δεδομένων (ακέραιοι, λίστες, σύνολα, κλπ) και μεταβλητές ελέγχου (π.χ. program counter)
 - σταθερές (ακέραιοι $0, 1, 2, \dots$, λίστες, σύνολα)
 - κατηγορηματικά σύμβολα ($\geq, \leq, \subseteq, \in$)

Σύνταξη γραμμικής χρονικής λογικής

- Η *Προτασιακή Γραμμική Χρονική Λογική* (PLTL) ορίζεται ως το μικρότερο σύνολο ιδιοτήτων που παράγονται ως εξής:

$$\Phi ::= p \mid \neg\Phi \mid \Phi \vee \Psi \mid \mathbf{X} \Phi \mid \Phi \mathbf{U} \Psi$$

Δηλαδή:

- Κάθε ατομική πρόταση p είναι ιδιότητα
- Αν οι Φ και Ψ είναι ιδιότητες, τότε και οι $\neg\Phi$ και $\Phi \vee \Psi$ είναι ιδιότητες
- Αν η Φ είναι μια ιδιότητα, τότε και η $\mathbf{X} \Phi$ (next) είναι ιδιότητα
- Αν οι Φ και Ψ είναι ιδιότητες, τότε και η $\Phi \mathbf{U} \Psi$ (until) είναι ιδιότητα

Παραγόμενοι τελεστές

$$\Phi \wedge \Psi \equiv \neg (\neg \Phi \vee \neg \Psi)$$

$$\Phi \rightarrow \Psi \equiv \neg \Phi \vee \Psi$$

$$\Phi \leftrightarrow \Psi \equiv (\Phi \rightarrow \Psi) \wedge (\Psi \rightarrow \Phi)$$

$$\text{true} \equiv \neg \Phi \vee \Phi$$

$$\text{false} \equiv \neg \text{true}$$

$$\mathbf{F} \Phi \equiv \text{true} \cup \Phi$$

$$\mathbf{G} \Phi \equiv \neg \mathbf{F} \neg \Phi$$

F (future) είναι η ιδιότητα που εκφράζει το “κάποτε”

G (globally) είναι η ιδιότητα που εκφράζει το “πάντα”

Παραγόμενοι τελεστές (2)

$$\Phi \text{ R } \Psi \quad \equiv \quad \neg \left((\neg \Phi) \cup (\neg \Psi) \right)$$

$$\Phi \text{ W } \Psi \quad \equiv \quad \Phi \text{ R } (\Phi \vee \Psi)$$

R (release)

W (weak until)

Εκφραστικότητα της PLTL

- Η Γραμμική Χρονική Λογική μπορεί να εκφράσει ιδιότητες
 - *ασφάλειας* (safety) : τίποτε “κακό” δεν θα συμβεί, $\mathbf{G} \neg \text{bad}$
 - *βιωσιμότητα* (liveness): κάτι “καλό” τελικά θα συμβεί, $\mathbf{F} \text{good}$
 - *ανταπόκρισης* : π.χ. κάθε αίτηση θα εξυπηρετηθεί
 $\mathbf{G} (\text{req} \rightarrow \mathbf{F} \text{serviced})$
 - *αντιδραστικότητας*: π.χ. $(\mathbf{G} \mathbf{F} \text{enabled}) \rightarrow (\mathbf{G} \mathbf{F} \text{executed})$

Παραδείγματα ιδιοτήτων

- Έστω ΑΠ οι ατομικές προτάσεις που αφορούν τη μεταβλητή x , τους τελεστές $<$, $\geq$, $\leq$ και $=$, και η συνάρτηση $x+c$
- Οι πιο κάτω ιδιότητες είναι νόμιμες PLTL ιδιότητες
 - $\neg (x + 7 < 21) \vee (x = 32)$
 - $\mathbf{F} (x + 12 > 30)$
 - $\mathbf{G} (x \geq 0 \wedge x < 20)$
 - $x = 10 \rightarrow \mathbf{X} (x \geq 11 \mathbf{U} x = 0)$
- Οι πιο κάτω ιδιότητες είναι μη-νόμιμες
 - $\mathbf{F} (x + 12 > y)$
 - $(x + x < 21) \vee \mathbf{U} (x^2 = 32)$
 - $\mathbf{X}(x+4) \vee (x = 32 \wedge \mathbf{F} (x + 12 > 30))$

Ιδιότητες φώτων της τροχαίας

- Από κόκκινο το φως δεν μπορεί να γίνεται αμέσως πράσινο

$$\mathbf{G} \text{ (κόκκινο} \rightarrow \neg \mathbf{X} \text{ πράσινο)}$$

- Στο μέλλον το φως θα ξαναγίνει πράσινο

$$\mathbf{F} \text{ πράσινο}$$

- Από κόκκινο το φως θα γίνει πράσινο αφού περάσει από το κίτρινο για κάποιο χρονικό διάστημα

$$\mathbf{G} \text{ (κόκκινο} \rightarrow (\text{κόκκινο} \mathbf{U} \\ (\text{κίτρινο} \wedge (\text{κίτρινο} \mathbf{U} \text{ πράσινο}))))$$

Ερμηνεία της PLTL

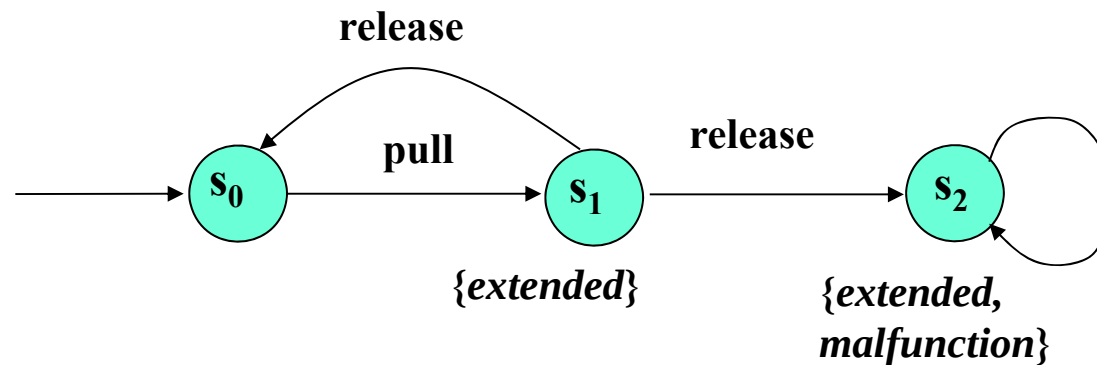
- Η σημασιολογική ερμηνεία της PLTL δίνεται σε σχέση με τις *δομές Kripke*.
- Μια *δομή Kripke* ορίζεται ως μια πλειάδα $M = (S, R, I, \text{Label})$ όπου
 - S είναι ένα αριθμήσιμο σύνολο από καταστάσεις
 - $I \subseteq S$ είναι το σύνολο των αρχικών καταστάσεων
 - $R \subseteq S \times S$ είναι μία σχέση μεταβάσεων, όπου $(s, s') \in R$ αν υπάρχει μετάβαση από την κατάσταση s στην κατάσταση s'
 - $\text{Label} : S \rightarrow 2^{\text{AP}}$ είναι μια συνάρτηση η οποία συνδέει κάθε κατάσταση με τις ατομικές προτάσεις τις οποίες ικανοποιεί.
- Έστω μια κατάσταση $s \in S$. Τότε, $\text{Label}(s)$ είναι το σύνολο των ατομικών προτάσεων που ισχύουν στην κατάσταση s .
- Ονομάζουμε μια ακολουθία από καταστάσεις $s_0 s_1 s_2 \dots$ *μονοπάτι* αν s_0 είναι μια αρχική κατάσταση και $(s_i, s_{i+1}) \in R$ για κάθε $i \geq 0$.

Παράδειγμα (ελατήριο)

Η Δομή Kripke

($S = \{s_0, s_1, s_2\}$, $I = \{s_0\}$, $R = \{(s_0, s_1), (s_1, s_0), (s_1, s_2), (s_2, s_2)\}$,

$\text{Label}(s_1) = \{\text{extended}\}$, $\text{Label}(s_2) = \{\text{extended}, \text{malfunction}\}$)



Μονοπάτια

$p_1 = s_0 s_1 s_0 s_1 s_0 s_1 s_0 \dots$

$p_2 = s_0 s_1 s_2 s_2 s_2 s_2 s_2 \dots$

$p_3 = s_0 s_1 s_0 s_1 s_2 s_2 s_2 \dots$

...

Σημασιολογία της PLTL

- Έστω μονοπάτι $s = s_0 s_1 s_2 \dots$, και ιδιότητα Φ . Ορίζουμε τη σχέση $\models$ όπου

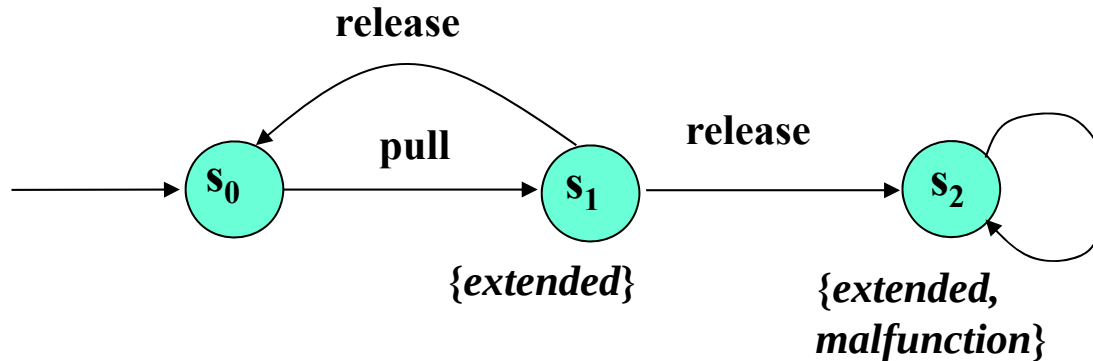
$s \models \Phi$ αν και μόνο αν η ιδιότητα Φ ικανοποιείται στο μονοπάτι s

ως εξής:

$s \models p$	αν και μόνο αν	$p \in \text{Label}(s_0)$
$s \models \neg \Phi$	αν και μόνο αν	δεν ισχύει ότι $s \models \Phi$
$s \models \Phi \vee \Psi$	αν και μόνο αν	$(s \models \Phi)$ ή $(s \models \Psi)$
$s \models \mathbf{X} \Phi$	αν και μόνο αν	$s^1 \models \Phi$
$s \models \Phi \mathbf{U} \Psi$	αν και μόνο αν	υπάρχει $j \geq 0$ τέτοιο ώστε $s^j \models \Psi$ και για κάθε $0 \leq k < j$ $s^k \models \Phi$

Ορισμός: Αν $s = s_0 s_1 s_2 \dots$, s^i είναι το μονοπάτι $s_i s_{i+1} s_{i+2} \dots$.

Παράδειγμα (συν.)



Θεωρήστε το μονοπάτι $p_3 = s_0 s_1 s_0 s_1 s_2 s_2 s_2 \dots$

Ποιες από τις πιο κάτω ιδιότητες ικανοποιούνται;

$p_3 \models extended$ ✗

$p_3 \models \mathbf{x} \text{ extended}$ ✓

$p_3 \models \mathbf{x} \mathbf{x} \text{ extended}$ ✗

$p_3 \models \mathbf{F} \text{ extended}$ ✓

$p_3 \models \mathbf{G} \text{ extended}$ ✗

$p_3 \models \mathbf{F} \mathbf{G} \text{ extended}$ ✓

$p_3 \models \neg \mathbf{F} \mathbf{G} \text{ extended}$ ✗

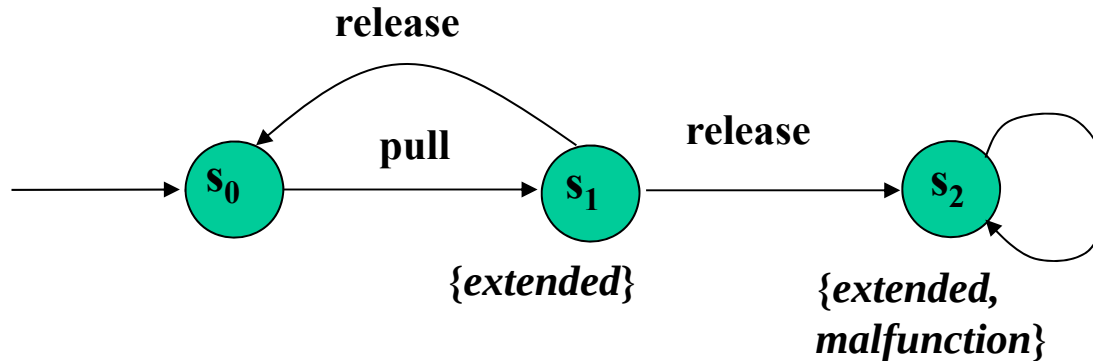
$p_3 \models (\neg extended) \mathbf{U} malfunction$ ✗

$p_3 \models G(\neg extended \rightarrow \mathbf{x} \text{ extended})$ ✓

Μοντελοέλεγχος

- $M \models \Phi$ αν και μόνο αν όλα τα μονοπάτια της Kripke δομής M ικανοποιούν την ιδιότητα Φ .
- Κατά το μοντελο-έλεγχο, δοθήσας κάποιας δομής Kripke και μίας ιδιότητας Φ , ελέγχουμε κατά πόσο $M \models \Phi$.

Παράδειγμα (συν.)



Ποιες από τις πιο κάτω ιδιότητες ικανοποιούνται από το σύστημα;

$S \models extended$	✗	$S \models \mathbf{F} \mathbf{G} extended$	✗
$S \models \mathbf{X} extended$	✓	$S \models \neg \mathbf{F} \mathbf{G} extended$	✗
$S \models \mathbf{X} \mathbf{X} extended$	✗	$S \models (\neg extended) \mathbf{U} malfunction$	✗
$S \models \mathbf{F} extended$	✓	$S \models \mathbf{G} (\neg extended \rightarrow \mathbf{X} extended)$	✓
$S \models \mathbf{G} extended$	✗		

Ισοδυναμίες της PLTL

$$\neg \mathbf{G} \Phi \equiv \mathbf{F} \neg \Phi$$

$$\neg \mathbf{F} \Phi \equiv \mathbf{G} \neg \Phi$$

$$\neg \mathbf{X} \Phi \equiv \mathbf{X} \neg \Phi$$

$$\mathbf{G} \mathbf{G} \Phi \equiv \mathbf{G} \Phi$$

$$\mathbf{F} \mathbf{F} \Phi \equiv \mathbf{F} \Phi$$

$$\Phi \mathbf{U} (\Phi \mathbf{U} \Psi) \equiv \Phi \mathbf{U} \Psi$$

$$\mathbf{F} \mathbf{G} \mathbf{F} \Phi \equiv \mathbf{G} \mathbf{F} \Phi$$

$$\mathbf{G} \mathbf{F} \mathbf{G} \Phi \equiv \mathbf{F} \mathbf{G} \Phi$$

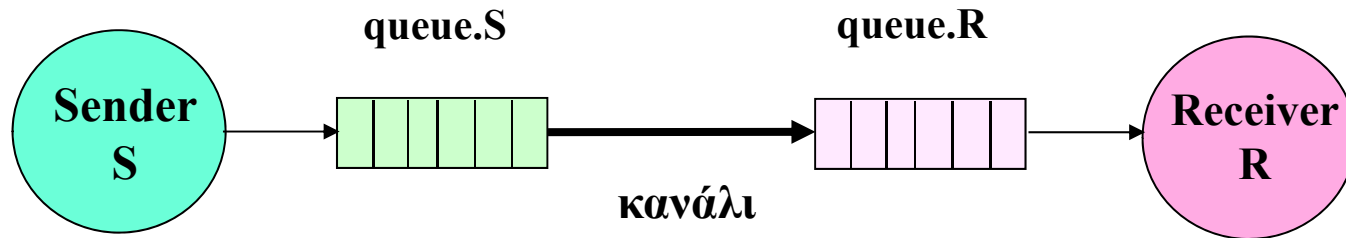
$$\mathbf{X} (\Phi \mathbf{U} \Psi) \equiv (\mathbf{X} \Phi) \mathbf{U} (\mathbf{X} \Psi)$$

$$\Phi \mathbf{U} \Psi \equiv \Psi \vee (\Phi \wedge \mathbf{X} (\Phi \mathbf{U} \Psi))$$

$$\mathbf{F} \Phi \equiv \Phi \vee \mathbf{X} \mathbf{F} \Phi$$

$$\mathbf{G} \Phi \equiv \Phi \wedge \mathbf{X} \mathbf{G} \Phi$$

Προδιαγραφές στην PLTL



- Θα χρησιμοποιήσουμε ατομικές προτάσεις που αφορούν τις μεταβλητές m , m' , $queue.S$, $queue.R$ και τον τελεστή $\in$.
- Ιδιότητα 1: Ένα μήνυμα δεν μπορεί να ανήκει και στις δύο ουρές

$$\mathbf{G} \neg (m \in queue.S \wedge m \in queue.R)$$

- Ιδιότητα 2: Το κανάλι δεν χάνει μηνύματα

$$\mathbf{G} (m \in queue.S \rightarrow \mathbf{F} (m \in queue.R))$$

Προδιαγραφές στην PLTL

- Ιδιότητα 3: *Το κανάλι προωθεί μόνο μηνύματα που προέρχονται από τον S.*

$$\begin{aligned} & (\neg (m \in \text{queue.R})) \wedge \\ \mathbf{G} \ [& (\neg (m \in \text{queue.R}) \wedge \mathbf{F} (m \in \text{queue.R})) \\ & \rightarrow (\neg (m \in \text{queue.R}) \mathbf{U} (m \in \text{queue.S}))] \end{aligned}$$

- Ιδιότητα 4: *Το κανάλι προωθεί μηνύματα με τη σειρά που στέλλονται*

$$\begin{aligned} \mathbf{G} \ (m \in \text{queue.S} \wedge \neg (m' \in \text{queue.S}) \wedge \mathbf{F} (m' \in \text{queue.S}) \\ \rightarrow \mathbf{F} \ (m \in \text{queue.R} \wedge \neg (m' \in \text{queue.R}) \wedge \mathbf{F} (m' \in \text{queue.R}) \\) \end{aligned}$$

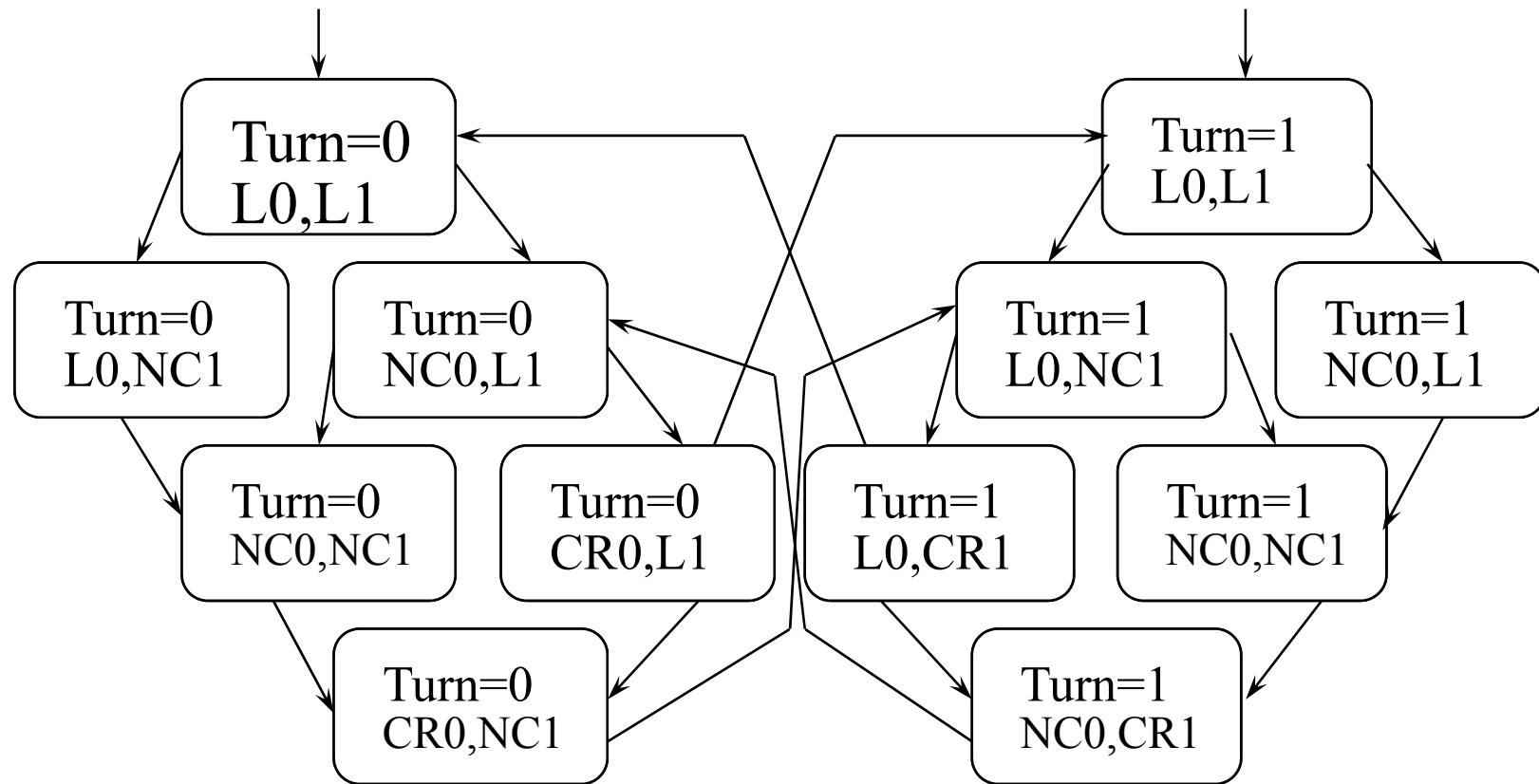
Αμοιβαίος αποκλεισμός

- Θυμηθείτε το παράδειγμα αμοιβαίου αποκλεισμού και το σύστημα μεταβάσεων του (διαφάνειες 2-14 – 2-16).

```
L0: while True do
    NC0: wait(Turn=0);
    CR0: Turn=1
endwhile ||
L1: while True do
    NC1: wait(Turn=1);
    CR1: Turn=0
endwhile
```

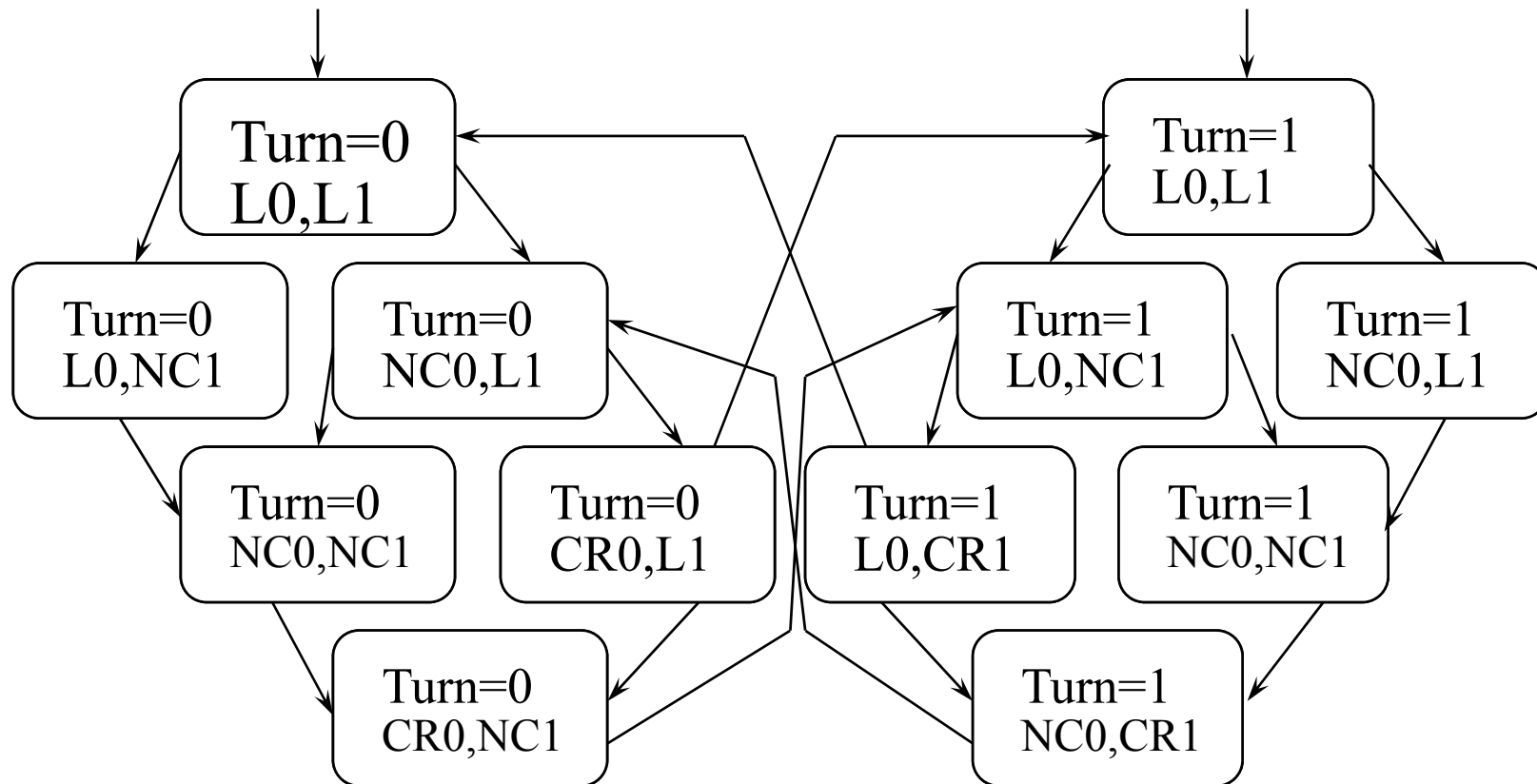
- Ερωτήματα:
 - Υπάρχει περίπτωση κάποια διεργασία να φθάσει σε αδιέξοδο περιμένοντας επ'άπειρω να της δοθεί άδεια πρόσβασης;
 - Υπάρχει περίπτωση να δοθεί και στις δύο διεργασίες άδεια ταυτόχρονα;
- Πως μπορούμε να διατυπώσουμε με σαφήνεια τις πιο πάνω απαιτήσεις και να ελέγχουμε την ικανοποίησή τους από το σύστημα;

Η δομή Kripke



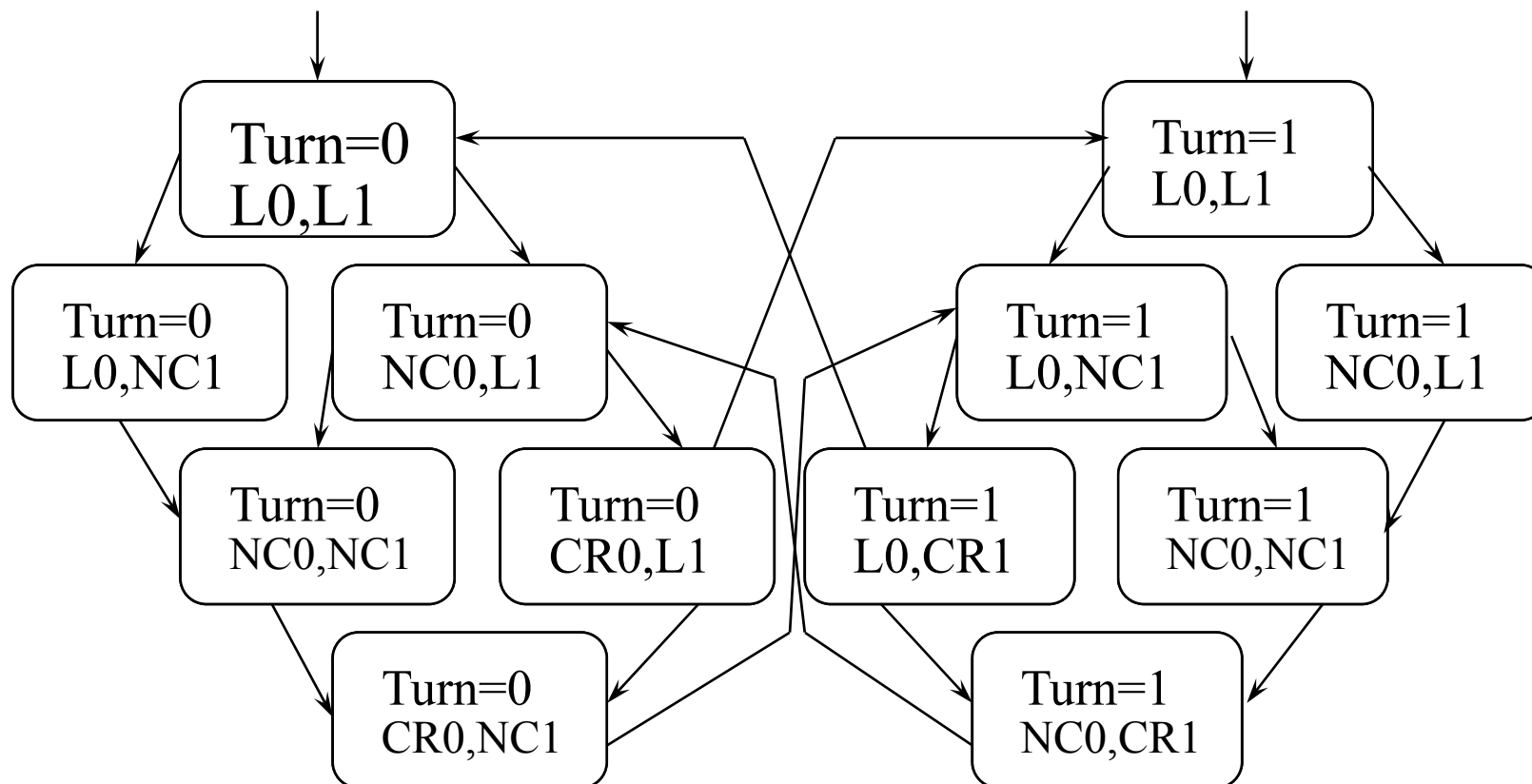
$$G \neg (PC0=CR0 \wedge PC1=CR1)$$

Ποτέ δεν ισχύει ότι και οι δύο διεργασίες
έχουν πάρει ταυτόχρονα άδεια



$G \text{ (Turn=0} \rightarrow F \text{ Turn=1)}$

Πάντα αν Turn=0 στο μέλλον Turn = 1



Παραλλαγές της PLTL

- Παραλλαγές της PLTL περιλαμβάνουν
 - γενικεύσεις που επιτρέπουν και μονοπάτια πεπερασμένου μήκους
 - προσθήκες τελεστών που επιτρέπουν συλλογισμούς για το παρελθόν
π.χ. $\underline{X} \Phi$ εκφράζει ότι η Φ ικανοποιείται στην προηγούμενη κατάσταση
 $\underline{G} \Phi$ εκφράζει ότι η Φ ικανοποιείται σε κάθε προηγούμενη κατάσταση
 - προσθήκες τελεστών που επιτρέπουν συλλογισμούς για χρονικές ιδιότητες
π.χ. $F^{<t} \Phi$ εκφράζει ότι η Φ ικανοποιείται στο μέλλον σε λιγότερες από t μονάδες χρόνου
 - πρωτοβάθμιους κατασκευαστές, κλπ.