CTL - Λογική Δένδρου Υπολογισμού
(HR Κεφάλαιο 3.4)

Στην ενότητα αυτή θα μελετηθούν τα εξής θέματα:

Διακλαδωμένες Χρονικές λογικές

CTL – σύνταξη και ερμηνεία

Γραμμική και διακλαδωμένη χρονική λογική

- Γραμμική χρονική λογική:

  οι ιδιότητες αναφέρονται σε (και ελέγχουν) ***όλες** τις δυνατές εκτελέσεις* ενός μοντέλου

  π.χ. η δομή Kripke M ικανοποιεί την ιδιότητα `x<15` **U** `x=100` αν σε *κάθε* εκτέλεση της δομής ισχύει ότι x <15 μέχρις ότου το x πάρει την τιμή 100.

- Διακλαδωμένη χρονική λογική:

  οι ιδιότητες αναφέρονται και ελέγχουν ***τη δενδρική δομή*** του μοντέλου,

  π.χ. η δομή Kripke M ικανοποιεί την ιδιότητα `A (x < 15` **U** `x=100)` αν σε κάθε εκτέλεση της δομής ισχύει ότι x <15 μέχρις ότου το x πάρει την τιμή 100, και,

  η δομή Kripke M ικανοποιεί την ιδιότητα `E (x < 15` **U** `x=100)` αν υπάρχει εκτέλεση της δομής όπου ισχύει ότι x <15 μέχρις ότου το x πάρει την τιμή 100.

Γιατί διακλαδωμένη χρονική λογική;

- *Εκφραστικότητα*: μας δίνει τα μέσα να εκφράσουμε διαφορετική κατηγορία ιδιοτήτων. Για παράδειγμα τη δυνατότητα (και όχι την αναγκαιότητα) να συμβεί κάτι.
  - Ισχύει όμως και το αντίθετο: υπάρχουν ιδιότητες γραμμικών λογικών που δεν μπορούν να εκφραστούν σε διακλαδωμένη λογική.

- *Πολυπλοκότητα μοντελοελέγχου*: Διαφορετικοί αλγόριθμοι για αυτοματοποιημένη επαλήθευση με διαφορετική πολυπλοκότητα χρόνου και χώρου.

Διακλαδωμένες χρονικές λογικές

- Διακλαδωμένες χρονικές λογικής που έχουν προταθεί περιλαμβάνουν
  - Λογική Hennessy – Milner (HML)
  - Λογική Δένδρου Υπολογισμού (Computation Tree Logic – CTL)
  - Επεκταμένη Λογική Δένδρου Υπολογισμού – CTL* (συνδυάζει σε ένα πρότυπο τις CTL και PLTL)
  - μ-calculus χωρίς εναλλαγή
  - μ-calculus

Προτασιακή γραμμική χρονική λογική

- Η Προτασιακή Γραμμική Χρονική Λογική ορίζεται ως το μικρότερο σύνολο ιδιοτήτων που παράγονται από τους πιο κάτω κανόνες
  – κάθε ατομική πρόταση p είναι ιδιότητα
  – Αν οι Φ και Ψ είναι ιδιότητες, τότε και οι $\neg\Phi$ και $\Phi \lor \Psi$ είναι ιδιότητες
  – Αν η Φ είναι μια ιδιότητα, τότε και η **X** Φ (next) είναι ιδιότητα
  – Αν οι Φ και Ψ είναι ιδιότητες, τότε και η Φ **U** Ψ (until) είναι ιδιότητα

Πως μπορούμε να εκφράσουμε ότι σε κάθε δυνατή εκτέλεση είναι πάντα δυνατή η επιστροφή στην αρχική κατάσταση;

G F *start;*

Προτασιακή διακλαδωμένη χρονική λογική

- Επεκτείνουμε την PLTL με ποσοτικούς τελεστές μονοπατιών
  - **A** , όπου **A** φ σημαίνει ότι η ιδιότητα φ ικανοποιείται σε όλες τις εκτελέσεις (μονοπάτια) του μοντέλου
  - **E** , όπου **E** φ σημαίνει ότι υπάρχει εκτέλεση του μοντέλου που ικανοποιεί την ιδιότητα φ

- Ιδιότητες του τύπου **A** φ και **E** φ ονομάζονται *ιδιότητες κατάστασης* (state formulae).

- PLTL ιδιότητες ονομάζονται *ιδιότητες εκτέλεσης* (path formulae).

Πως μπορούμε να εκφράσουμε ότι σε κάθε δυνατή εκτέλεση είναι πάντα δυνατή η επιστροφή στην αρχική κατάσταση; **A*G*** **E*F*** `start`*!*

CTL (Computation Tree Logic)

Η CTL ορίζεται ως το μικρότερο σύνολο ιδιοτήτων που παράγονται ως εξής:

$$\Phi, \Psi ::= p \mid \neg\Phi \mid \Phi \vee \Psi \mid \mathbf{A}\ \varphi \mid \mathbf{E}\ \varphi$$

$$\varphi ::= \mathbf{X}\ \Phi \mid \Phi\ \mathbf{U}\ \Psi$$

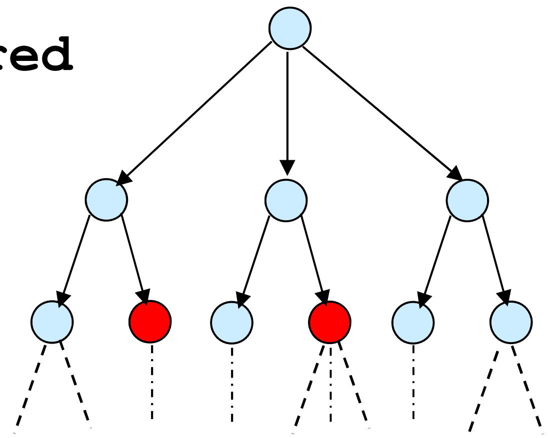
1. Ιδιότητες κατάστασης – Φ
   - κάθε ατομική πρόταση p είναι ιδιότητα *κατάστασης*
   - Αν οι Φ και Ψ είναι ιδιότητες *κατάστασης*, τότε και οι $\neg\Phi$ και $\Phi \vee \Psi$ είναι ιδιότητες *κατάστασης*
   - Αν η φ είναι μια ιδιότητα *εκτέλεσης*, τότε οι $\mathbf{A}\ \varphi$ και η $\mathbf{E}\ \varphi$ είναι ιδιότητες *κατάστασης*
2. Ιδιότητες εκτέλεσης – φ
   - Αν οι Φ και Ψ είναι ιδιότητες *κατάστασης*, τότε οι $\mathbf{X}\ \Phi$ και $\Phi\ \mathbf{U}\ \Psi$ είναι ιδιότητες *εκτέλεσης*

Παραγόμενοι τελεστές

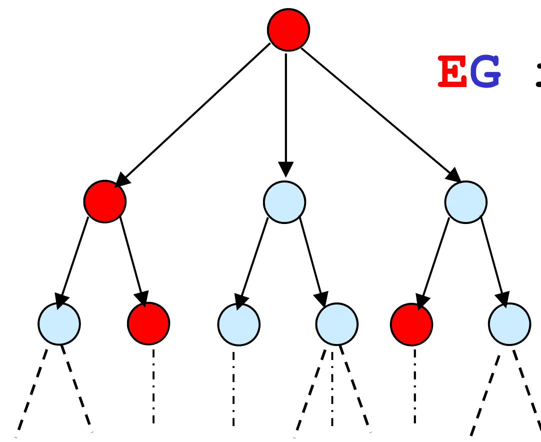
$\mathbf{F}\ \Phi$	$\equiv$	$\mathrm{true}\ \mathbf{U}\ \Phi$	
$\mathbf{G}\ \Phi$	$\equiv$	$\neg\ \mathbf{F} \neg\ \Phi$	
$\mathbf{EF}\ \Phi$	$\equiv$	$\mathbf{E}(\mathrm{true}\ \mathbf{U}\ \Phi)$	δυνατόν Φ
$\mathbf{AG}\ \Phi$	$\equiv$	$\neg\ \mathbf{EF} \neg\ \Phi$	σταθερά Φ
$\mathbf{AF}\ \Phi$	$\equiv$	$\mathbf{A}(\mathrm{true}\ \mathbf{U}\ \Phi)$	αναπόφευκτα Φ
$\mathbf{EG}\ \Phi$	$\equiv$	$\neg\ \mathbf{AF} \neg\ \Phi$	δυνατόν πάντα Φ

Παράδειγμα

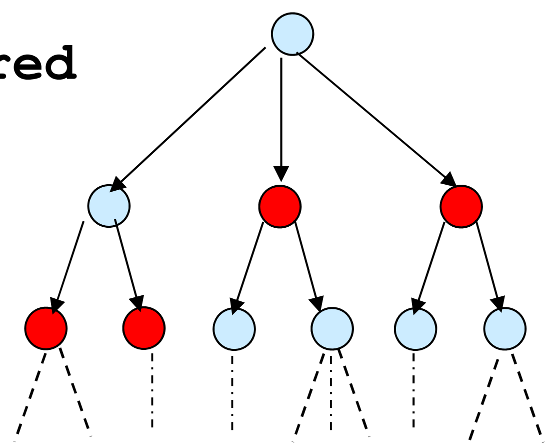
EF red



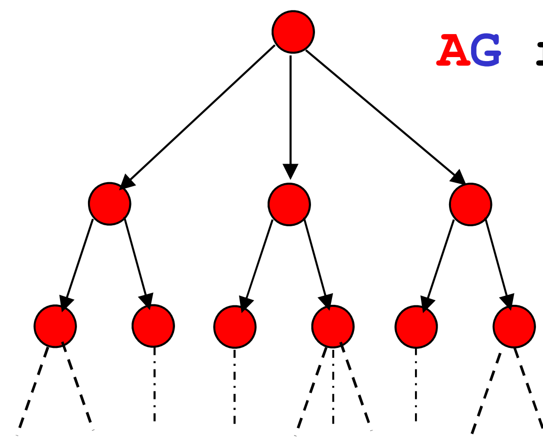
EG red



AF red



AG red



Παραδείγματα

- Έστω ΑΠ οι ατομικές προτάσεις που αφορούν τη μεταβλητή x, τους τελεστές <, ≥ , ≤ και =, και η συνάρτηση x+c

- Οι πιο κάτω ιδιότητες είναι νόμιμες CTL ιδιότητες
  - $\neg\ (x + 7 < 21) \vee (x = 32)$
  - $\mathbf{AF}\ (x + 12 < 30)$
  - $\mathbf{EG}\ (x \geq 0 \wedge x < 20)$
  - $x = 10 \rightarrow \mathbf{AX}\ \mathbf{E}(x \geq 11\ \mathbf{U}\ x = 0)$

- Οι πιο κάτω ιδιότητες δεν είναι νόμιμες
  - $\mathbf{E}\ (\mathbf{F}\ (\mathbf{G}\ x < 10) \wedge (\mathbf{G}\ (x + 12 > y)))$
  - $\mathbf{E}\ (x < 21) \vee \mathbf{X}\ (x = 32)$

Ερμηνεία της CTL

- Η τυπική ερμηνεία της CTL δίνεται (και πάλι) σε σχέση με τις δομές Kripke.
- Μια *δομή Kripke* ορίζεται ως μια πλειάδα $M = (S, R, I, Label)$ 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'
  - $Label : S \to 2^{AP}$ είναι μια συνάρτηση η οποία συνδέει κάθε κατάσταση με τις ατομικές προτάσεις τις οποίες ικανοποιεί.
- Έστω μια κατάσταση $s \in S$. Τότε, Label(s) είναι το σύνολο των ατομικών προτάσεων που ισχύουν στην κατάσταση s.
- Ονομάζουμε μια ακολουθία από καταστάσεις $s_0\, s_1\, s_2 \ldots$ *μονοπάτι* αν s_0 είναι μια αρχική κατάσταση και $(s_i, s_{i+1}) \in R$ για κάθε $i \geq 0$.

Σημασιολογία της CTL: *ιδιότητες κατάστασης*

- Ορίζουμε τη σχέση |= όπου

> *M*, s |= Φ αν και μόνο αν η ιδιότητα Φ ικανοποιείται στην κατάσταση s της δομής M ως εξής:

M, s |= p	αν και μόνο αν	p ∈Label(s)
M, s |= ¬Φ	αν και μόνο αν	δεν ισχύει ότι M,s |= Φ
M, s |= Φ∨Ψ	αν και μόνο αν	(M, s |= Φ) ή (M, s |= Ψ)
M, s |= **E** φ	αν και μόνο αν	M,w |≡ φ για κάποιο μονοπάτι w που ξεκινά από την s
M, s |= **A** φ	αν και μόνο αν	M,w |≡ φ για κάθε μονοπάτι w που ξεκινά από την s

Σημασιολογία της CTL: *ιδιότητες εκτέλεσης*

- Έστω μονοπάτι $w = s_0\, s_1\, s_2\ldots$ της δομής Kripke M και ιδιότητα φ. Ορίζουμε τη σχέση |≡ όπου

M, w |≡ φ   αν και μόνο αν η ιδιότητα φ ικανοποιείται στο μονοπάτι w της δομής M

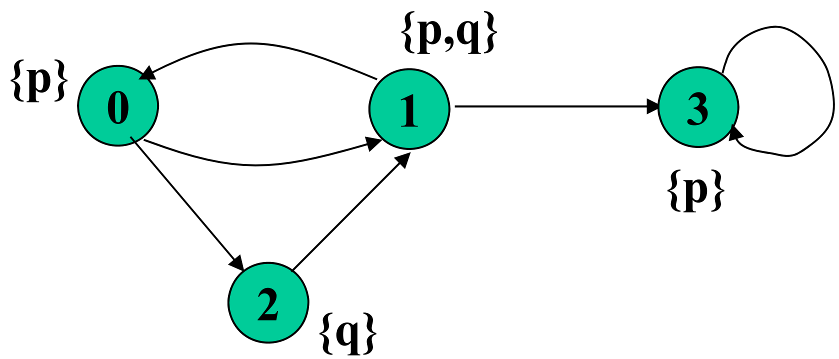
ως εξής:

M, w |≡ **X** Φ αν και μόνο αν M, w[1] |= Φ

M, w |≡ Φ **U** Ψ αν και μόνο αν υπάρχει $j \geq 0$ τέτοιο ώστε M,w[j] |= Ψ και για κάθε $0 \leq k < j$, M,w[k] |= Φ

όπου αν $w = s_0\, s_1\, s_2\ldots$, w[k] είναι η κατάσταση s_k .

Παράδειγμα



Ποιες από τις πιο κάτω ιδιότητες ισχύουν;

M, 0 |= **E X** p √

M, 0 |= **A**(p **U** q) √

M, 0 |= **A X** p ×

M, 0 |= **A G** p ×

M, 0 |= **EF EG** p √

M, 0 |= **AX EG** p ×

Ταυτολογίες της CTL

PLTL κανόνες ανάπτυξης

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

$$\mathbf{F}\,\Phi \equiv \mathtt{true}\;\mathbf{U}\;\Phi$$

$$\mathbf{G}\,\Phi \equiv \mathtt{false}\;\mathbf{R}\;\Phi$$

CTL κανόνες ανάπτυξης

$$\mathbf{E}(\Phi \;\mathbf{U}\; \Psi) \equiv \Psi \lor (\Phi \land \mathbf{EX}\;\mathbf{E}(\Phi\mathbf{U}\Psi))$$

$$\mathbf{A}(\Phi \;\mathbf{U}\; \Psi) \equiv \Psi \lor (\Phi \land \mathbf{AX}\;\mathbf{A}(\Phi\mathbf{U}\Psi))$$

$$\mathbf{EF}\,\Phi \equiv \Phi \lor \mathbf{EX}\;\mathbf{EF}\,\Phi$$

$$\mathbf{AF}\,\Phi \equiv \Phi \lor \mathbf{AX}\;\mathbf{AF}\,\Phi$$

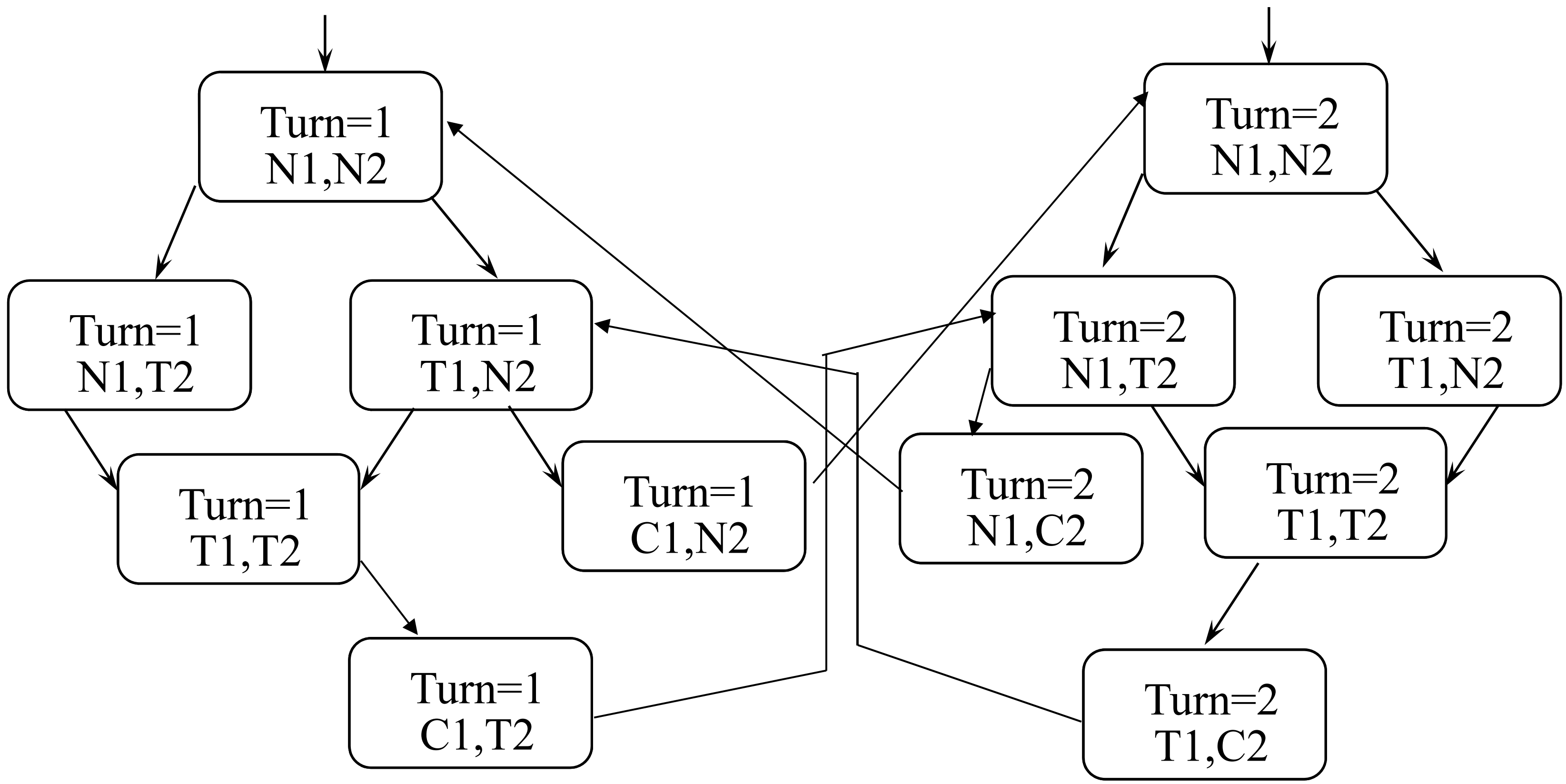
$$\mathbf{EG}\,\Phi \equiv \Phi \land \mathbf{EX}\;\mathbf{EG}\,\Phi$$

$$\mathbf{AG}\,\Phi \equiv \Phi \land \mathbf{AX}\;\mathbf{AG}\,\Phi$$

Ιδιότητες στη CTL

- Δυνατότητα προσέγγισης κατάστασης
  - απλή $\quad$ **EF** Φ
  - εξαρτώμενη $\quad$ **E**(Ψ **U** Φ)
  - από κάθε κατάσταση $\quad$ **AG** (**EF** Φ)
- Ασφάλεια (κάτι κακό δεν συμβαίνει ποτέ) $\quad$ **AG** ¬bad
- Ζωτικότητα (Liveness) $\quad$ **AF** good
- Ανταπόκρισης $\quad$ **AG** (Φ → **AF** Ψ)
- Δικαιοσύνη $\quad$ **AG** (**EF** Φ)

Αμοιβαίος αποκλεισμός



N_i : η διεργασία i είναι εκτός της κρίσιμής της περιοχής

T_i : η διεργασία i προσπαθεί να εισέλθει στην κρίσιμη περιοχή

C_i : η διεργασία i είναι εντός της κρίσιμής της περιοχής

Αμοιβαίος Αποκλεισμός

- Ασφάλεια: οι δύο διεργασίες δεν βρίσκονται ποτέ ταυτόχρονα στην κρίσιμή τους περιοχή

  $$\mathbf{AG}(\neg\ (C1 \land C2))$$

- Ζωτικότητα: Κάθε φορά που η διεργασία 1 προσπαθεί να εισέλθει στην κρίσιμή της περιοχή θα το πράξει

  $$\mathbf{AG}(T1 \rightarrow \mathbf{AF}\ C1)$$

- Έλλειψη εμποδίων: Κάθε φορά που η διεργασία 1 βρίσκεται στη μη κρίσιμη της περιοχή, είναι δυνατόν, στην επόμενη χρονική στιγμή να προσπαθήσει να εισέλθει στην κρίσιμή της περιοχή

  $$\mathbf{AG}(N1 \rightarrow \mathbf{EX}\ T1)$$

- Έλλειψη αυστηρής διάταξης: Είναι δυνατόν, η διεργασία 1 να εισέλθει στην κρίσιμή της περιοχή δύο συνεχόμενες φορές χωρίς να παρεμβληθεί η διεργασία 2.

  $$\mathbf{EF}(C1 \land \mathbf{E}(C1\ \mathbf{U}\ (\neg\ C1 \land \mathbf{E}(\neg\ C2\ \mathbf{U}\ C1))))$$