# ΠΡΟΔΙΑΓΡΑΦΗ ΙΔΙΟΤΗΤΩΝ ΜΕ ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ Ι

- ***Ιδιότητες προσεγγισιμότητας*** (reachability properties): αναφέρονται στο ενδεχόμενο προσέγγισης μιας συγκεκριμένης κατάστασης.
- ***Ιδιότητες ασφαλείας*** (safety properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο δεν πρόκειται να συμβεί ποτέ.
- ***Ιδιότητες βιωσιμότητας*** (liveness properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο εν τέλει θα συμβεί.
- ***Ιδιότητες αμεροληψίας*** (fairness properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο (δεν) θα συμβαίνει άπειρα συχνά.

# ΠΡΟΔΙΑΓΡΑΦΗ ΙΔΙΟΤΗΤΩΝ ΜΕ ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ ΙΙ

Είναι σημαντικός οπ διαχωρισμός των ιδιοτήτων σε κατηγορίες γιατί:

- ***Μεθοδολογία προδιαγραφής***. Όταν το σύνολο των ιδιοτήτων των προδιαγραφών ενός συστήματος καθορισθεί και τυποποιηθεί επιβάλλεται να δώσουμε απαντήσεις στα ερωτήματα «ποιες ιδιότητες ασφαλείας;», «ποιες ιδιότητες βιωσιμότητας;» κ.α. Αυτό βοηθάει στο να εντοπίσουμε τυχόν παραλείψεις και οδηγεί σε προδιαγραφές με βελτιωμένη δομή.
- ***Οικονομία της μελέτης επαλήθευσης***. Οι ιδιότητες προσεγγισιμότητας και οι ιδιότητες ασφαλείας είναι συνήθως οι πιο κρίσιμες για την ορθότητα του συστήματος και γι΄ αυτό απαιτούν μεγαλύτερη επένδυση σε χρόνο, προτεραιότητα, ακρίβεια κ.α. από την πλευρά του μηχανικού της ανάλυσης. Ευτυχώς οι ιδιότητες των συγκεκριμένων κατηγοριών είναι συνήθως ευκολότερο να ελεγχθούν.
- ***Μεθοδολογία επαλήθευσης***. Μερικές τεχνικές εφαρμόζονται μόνο σε συγκεκριμένους τύπους ιδιοτήτων και για αυτό είναι σημαντικό να αναγνωρίσουμε την κατηγορία στην οποία ανήκει μία δοθείσα ιδιότητα.
- ***Μεθοδολογία μοντελοποίησης***. Μπορούμε για παράδειγμα όταν ελέγχουμε ιδιότητες ασφαλείας να κάνουμε διαφορετικές αφαιρέσεις – απλοποιήσεις από στο μοντέλο από ότι όταν ελέγχουμε ιδιότητες βιωσιμότητας.

# ΙΔΙΟΤΗΤΕΣ ΠΡΟΣΕΓΓΙΣΙΜΟΤΗΤΑΣ Ι

- ***Ιδιότητες προσεγγισιμότητας*** (reachability properties): αναφέρονται στο ενδεχόμενο προσέγγισης μιας συγκεκριμένης κατάστασης.

  ΠΑΡΑΔΕΙΓΜΑΤΑ:

  «είναι ενδεχόμενο να έχουμε n < 0» (R1)

  «μπορεί να προσπελασθεί ένα κρίσιμο τμήμα» (R2)

  ή η άρνηση ιδιοτήτων προσεγγισιμότητας όπως

  «δεν μπορεί να έχουμε n < 0» (R3)

  «δεν μπορεί να προσεγγισθεί κατάσταση `crash`» (R4)

  Η προσεγγισιμότητα μπορεί να είναι απλή όπως στα προηγούμενα παραδείγματα ή υπό προϋπόθεση όταν μία συνθήκη περιορίζει τη μορφή των μονοπατιών που προσεγγίσουν την κατάσταση που ενδιαφέρει:

  «μπορούμε να προσπελάσουμε το κρίσιμο τμήμα χωρίς να διέρθουμε από κατάσταση όπου n=0» (R5)»

# ΙΔΙΟΤΗΤΕΣ ΠΡΟΣΕΓΓΙΣΙΜΟΤΗΤΑΣ ΙΙ

ΠΑΡΑΔΕΙΓΜΑΤΑ:

ή μπορεί να εφαρμόζεται σε οποιαδήποτε προσεγγίσιμη κατάσταση

«πάντα μπορούμε να επιστρέφουμε στην αρχική κατάσταση» (R6)

«μπορούμε να επιστρέψουμε στην αρχική κατάσταση» (R7)

Η ιδιότητα R6 σημαίνει ότι ισχύει για οποιαδήποτε προσεγγίσιμη κατάσταση, ενώ η ιδιότητα R7 προδιαγράφει ένα ενδεχόμενο που ισχύει μόνο για την τρέχουσα κατάσταση.

# ΙΔΙΟΤΗΤΕΣ ΠΡΟΣΕΓΓΙΣΙΜΟΤΗΤΑΣ & ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ Ι

- Όταν οι ιδιότητες προσεγγισιμότητας διατυπώνονται σε χρονική λογική χρησιμοποιείται ο συνδυασμός τελεστών **EF** και οι ιδιότητες γράφονται τελικά ως **EF**$\varphi$, όπου $\varphi$ είναι ένας προτασιακός τύπος χωρίς χρονικούς τελεστές.

  ΠΑΡΑΔΕΙΓΜΑΤΑ:

  R1: **EF**(n < 0)  R3: ¬**EF**(n<0)

  R2: **EF** `crit_sec`  R4: ¬**EF** `crash`

  Τονίζουμε ότι η πρόταση ¬**EF**$\varphi$ μπορεί επίσης να διατυπωθεί ως **AG**¬$\varphi$ που διαβάζεται ως «κατά μήκος κάθε μονοπατιού και σε κάθε κατάσταση ισχύει η ¬$\varphi$».

- Η προσεγγισιμότητα από οποιαδήποτε κατάσταση απαιτεί το συνδυασμό των τελεστών **AG** και **EF**

  R6: **AG** (**EF** `init`)

# ΙΔΙΟΤΗΤΕΣ ΠΡΟΣΕΓΓΙΣΙΜΟΤΗΤΑΣ & ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ ΙΙ

- Η προσεγγισιμότητα υπό προϋπόθεση χρησιμοποιεί των τελεστή **E**_∪_

  ΠΑΡΑΔΕΙΓΜΑ:
  R5: **E** $(n \neq 0) \cup$ `crit_sec`

- Η λογική PLTL δεν ταιριάζει τόσο καλά για τη διατύπωση ιδιοτήτων προσεγγισιμότητας. Πιο συγκεκριμένα επειδή η PLTL εξυπακούεται ότι ποσοτικοποιεί πάνω σε όλες τις πιθανές εκτελέσεις γι αυτό το λόγο μπορεί να εκφράσει προσεγγισιμότητα μόνο με άρνηση πρότασης: κάτι δεν είναι προσεγγίσιμο.

- Η κατασκευή του χώρου καταστάσεων μπορεί (ανάλογα με το εργαλείο) να γίνεται
  - με ευθεία ακολουθία εκτέλεσης (forward chaining)
  - με ανάστροφη ακολουθία εκτέλεσης (backward chaining)
  - με "on the fly" διερεύνηση (χρήσιμη όταν η απάντηση yes σε ερώτημα προσεγγισιμότητας δεν απαιτεί εξαντλητική διερεύνηση του χώρου καταστάσεων)

# ΙΔΙΟΤΗΤΕΣ ΑΣΦΑΛΕΙΑΣ

- ***Ιδιότητες ασφαλείας*** (safety properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο δεν πρόκειται να συμβεί ποτέ.

  ΠΑΡΑΔΕΙΓΜΑΤΑ:

  «δεν θα βρεθούν ποτέ ταυτόχρονα οι δύο διεργασίες στο κρίσιμο τμήμα» (S1)

  «δεν θα έχουμε ποτέ υπερχείλιση μνήμης» (S2)

  «η κατάσταση . . . . . είναι μη εφικτή» (S3)

  «όσο το κλειδί του αυτοκινήτου δεν είναι στη θέση ανάφλεξης το αυτοκίνητο δεν πρόκειται να πάρει μπρος» (S4)

- Η άρνηση μιας ιδιότητας προσεγγισιμότητας είναι ιδιότητα ασφαλείας και η άρνηση μιας ιδιότητας ασφαλείας είναι ιδιότητα προσεγγισιμότητας.

# ΙΔΙΟΤΗΤΕΣ ΑΣΦΑΛΕΙΑΣ & ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ

- Στη CTL χρησιμοποιούμε τον τελεστή **AG**
- Στην PLTL χρησιμοποιούμε τον τελεστή **G**

ΠΑΡΑΔΕΙΓΜΑΤΑ:

$\mathbf{AG}\ \neg(\texttt{crit-sec}_1 \wedge \texttt{crit-sec}_2)$ (S1)

$\mathbf{AG}\ \neg\texttt{overflow}$ (S2)

ενώ οι ίδιες ιδιότητες στην PLTL

$\mathbf{G}\ \neg(\texttt{crit-sec}_1 \wedge \texttt{crit-sec}_2)$ (S1)

$\mathbf{G}\ \neg\texttt{overflow}$ (S2)

Ιδιότητες ασφαλείας με προϋποθέσεις μπορούν να εκφραστούν με τον τελεστή **W** ($\varphi_1\ \mathbf{W}\ \varphi_2 \equiv (\varphi_1 \cup \varphi_2) \vee \mathbf{G}\ \varphi_1$):

A $\neg$`starts` **W** `key` (S4)

ενώ στην PLTL

$\neg$`starts` **W** `key` (S4)

Το ισχυρό until ($\cup$) θα σήμαινε απλά ότι κάποια στιγμή θα καταλήξουμε να ισχύει η πρόταση `key` που αυτό δεν είναι ιδιότητα ασφαλείας.

# ΙΔΙΟΤΗΤΕΣ ΒΙΩΣΙΜΟΤΗΤΑΣ Ι

- ***Ιδιότητες βιωσιμότητας*** (liveness properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο εν τέλει θα συμβεί.

  ΠΑΡΑΔΕΙΓΜΑΤΑ:

  «οποιαδήποτε απαίτηση εν τέλει θα ικανοποιηθεί» (L1)
  «με συνεχή προσπάθεια κάποιος τελικά θα πετύχει» (L2)
  «αν καλέσουμε τον ανελκυστήρα τελικά αυτός θα έρθει» (L3)
  «το φανάρι θα γίνει πράσινο» (L4)
  «μετά τη βροχή θα έχει ηλιοφάνεια» (L5)

  Μία ιδιότητα βιωσιμότητας δεν σχετίζεται με προσεγγισιμότητα. Δεν λέμε «είναι δυνατό το φανάρι να γίνει πράσινο» αλλά λέμε ότι «το φανάρι θα γίνει πράσινο» που είναι κάτι περισσότερο από μία απλή ιδιότητα προσεγγισιμότητας.

# ΙΔΙΟΤΗΤΕΣ ΒΙΩΣΙΜΟΤΗΤΑΣ ΙΙ

ΠΑΡΑΔΕΙΓΜΑ:

«το πρόγραμμα θα τερματίσει» (L6)

Αυτό είναι μία ιδιότητα βιωσιμότητας και ταυτόχρονα ένα χαρακτηριστικό παράδειγμα που δείχνει ότι οι ιδιότητες βιωσιμότητας δεν σχετίζονται με την ιδιότητα του να είναι κάτι «εν ζωή». Σε πολλές περιπτώσεις μία ιδιότητα του να είναι κάτι «εν ζωή» σημαίνει ότι κάθε τμήμα του συστήματος παραμένει προσεγγίσιμο.

- Υπάρχουν δύο μεγάλες οικογένειες ιδιοτήτων βιωσιμότητας: η ***απλή βιωσιμότητα*** που επίσης αποκαλείται ***πρόοδος*** και η ***επαναλαμβανόμενη βιωσιμότητα*** που μερικές φορές αποκαλείται ***αμεροληψία***.

# ΙΔΙΟΤΗΤΕΣ ΑΠΛΗΣ ΒΙΩΣΙΜΟΤΗΤΑΣ ΣΤΗ ΧΡΟΝΙΚΗ ΛΟΓΙΚΗ

- Χρησιμοποιούμε τον τελεστή **F**

  «οποιαδήποτε απαίτηση εν τέλει θα ικανοποιηθεί» (L1)

  στην CTL: **AG**(`req` → **AF** `sat`)

  στην PLTL: **G**(`req` → **F** `sat`)

  «το σύστημα μπορεί πάντα να επιστρέφει στην αρχική του κατάσταση»

  στην CTL: **AGEF** `init`

  στην PLTL: μπορεί να εκφραστεί μόνο αν έχουμε φανερή περιγραφή του συνόλου των καταστάσεων που ικανοποιούν την **EF** `init`

- Θεωρούμε ότι ο τελεστής $\cup$ εκφράζει ιδιότητα βιωσιμότητας αν και αυτό δεν είναι τελείως σωστό:

$$P \cup Q \equiv \mathbf{F}Q \wedge (P\mathbf{W}Q)$$

- Με την παραπάνω παραδοχή οι προτάσεις $\mathbf{A}P \cup Q$ και $\mathbf{E}P \cup Q$ θεωρούνται ιδιότητες βιωσιμότητας

# ΑΠΟΥΣΙΑ ΑΔΙΕΞΟΔΟΥ

- Η απουσία αδιεξόδου είναι μία ιδιότητα που προδιαγράφει ότι δεν υπάρχει κατάσταση που να καθιστά αδύνατη την ύπαρξη προόδου. Η ιδιότητα αυτή είναι μία ιδιότητα ορθότητας για συστήματα που τρέχουν επάπειρο, αλλά σε μία πιο γενική θεώρηση ένα σύνολο τελικών καταστάσεων (π.χ. σε ένα πρωτόκολλο) απαιτείται να μην περιλαμβάνει κατάσταση αδιεξόδου.
- Στην πιο γενική περίπτωση η απουσία αδιεξόδου γράφεται στην CTL ως **AGEX** `true`
- Από θεωρητική άποψη η απουσία αδιεξόδου δεν είναι ιδιότητα ασφαλείας παρόλο που χρησιμοποιούμε τον τελεστή **AG**.
- Αν δεν είναι εφικτή η απόδειξη της απουσίας αδιεξόδου με μεθόδους ιδιοτήτων ασφαλείας μπορούμε να προσπαθήσουμε να εκφράσουμε την απυσία αδιεξόδου με ένα αυτόματο (βλ. προτεινόμενο βιβλίο)

# ΙΔΙΟΤΗΤΕΣ ΑΜΕΡΟΛΗΨΙΑΣ

- ***Ιδιότητες αμεροληψίας*** (fairness properties): εκφράζουν το ότι κάτω από συγκεκριμένες συνθήκες ένα ενδεχόμενο (δεν) θα συμβαίνει άπειρα συχνά.
- Χρησιμοποιούμε στη CTL* τον τελεστή **GF** $\varphi$

  ΠΑΡΑΔΕΙΓΜΑΤΑ:

  «η πύλη θα ανοίγει άπειρα συχνά» (F1)
  **AGF** `gate_open`
  «αν γίνονται άπειρα συχνές αιτήσεις προσπέλασης στο κρίσιμο τμήμα τότε και η προσπέλαση σε αυτό θα γίνεται άπειρα συχνά» (F2)
  **A** (**GF** `crit_req` $\rightarrow$ **GF** `crit_in`)
- Δεν μπορούν να εκφραστούν σε καθαρή CTL εκτός και αν εκφράσουμε την **AGF** ως **AGAF**, αλλά δεν μπορούμε να κάνουμε κάτι ανάλογο για την **EGF**
- Υπάρχει παραλλαγή της CTL κατάλληλη για έλεγχο αμεροληψίας