

Επαγωγή

Διάλεξη 4: Θεωρία Υπολογισμού · ΗΥ-280

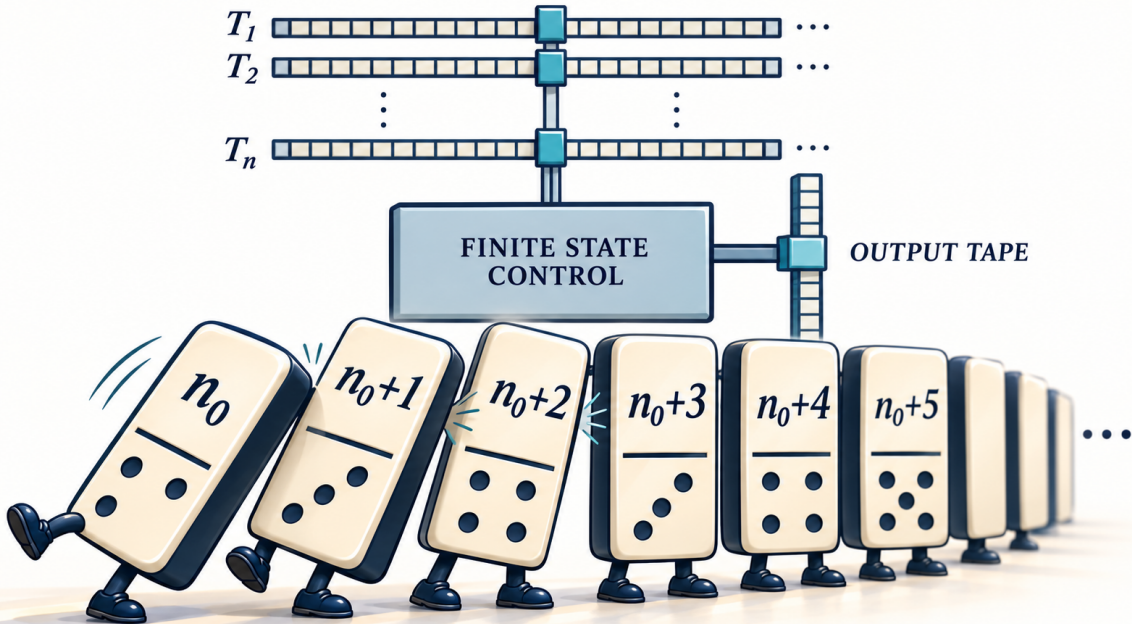
Χαράλαμπος Ε. Τσουρακάκης

Επαγωγή

Η επαγωγή είναι θεμελιώδης στην Πληροφορική: μας επιτρέπει να αποδεικνύουμε ότι ένας ισχυρισμός ισχύει για **κάθε μέγεθος εισόδου** ή **κάθε βήμα υπολογισμού**.

- **Στους αλγορίθμους:** αποδεικνύουμε ορθότητα και αναλύουμε τον χρόνο εκτέλεσης, ιδιαίτερα σε αναδρομικούς αλγορίθμους.
- **Στις δομές δεδομένων:** αποδεικνύουμε ιδιότητες λιστών, δέντρων και άλλων αναδρομικά ορισμένων δομών.
- **Στη Θεωρία Υπολογισμού:** αποδεικνύουμε ιδιότητες λέξεων και γλωσσών, καθώς και τη συμπεριφορά αυτομάτων και μηχανών Turing.

Η βασική σύνδεση: οι αναδρομικοί ορισμοί και οι επαναληπτικοί υπολογισμοί οδηγούν φυσικά σε επαγωγικές αποδείξεις.



Μαθηματική επαγωγή: η βασική αρχή

Στόχος: να αποδείξουμε $P(n)$ για **κάθε** ακέραιο $n \geq n_0$.

1. **Βάση:** αποδεικνύουμε την $P(n_0)$.
2. **Επαγωγικό βήμα:** για αυθαίρετο $k \geq n_0$, υποθέτουμε την $P(k)$ και αποδεικνύουμε την $P(k+1)$.

$$\left[P(n_0) \wedge \forall k \geq n_0 (P(k) \Rightarrow P(k+1)) \right] \Rightarrow \forall n \geq n_0 P(n).$$

Η βάση ξεκινά την αλυσίδα και το βήμα τη συνεχίζει σε κάθε θέση.

Η επαγωγική υπόθεση είναι προσωρινή υπόθεση για την απόδειξη της συνεπαγωγής. Οι έλεγχοι λίγων τιμών δεν αρκούν.

Παράδειγμα: το άθροισμα των περιττών

Για κάθε $n \geq 0$ θέλουμε να αποδείξουμε

$$P(n) : \sum_{i=1}^n (2i - 1) = n^2.$$

Βάση $n = 0$: το κενό άθροισμα είναι $0 = 0^2$.

Βήμα: έστω $k \geq 0$ και $\sum_{i=1}^k (2i - 1) = k^2$.

$$\begin{aligned} \sum_{i=1}^{k+1} (2i - 1) &= \underbrace{\sum_{i=1}^k (2i - 1)}_{k^2 \text{ από την ΕΥ}} + (2k + 1) \\ &= k^2 + 2k + 1 = (k + 1)^2. \end{aligned}$$

Άρα $P(k + 1)$ και, με επαγωγή, $P(n)$ για κάθε $n \geq 0$.

Ισχυρή επαγωγή

Στο βήμα μπορούμε να χρησιμοποιούμε **όλες τις μικρότερες περιπτώσεις**:

$$\underbrace{P(n_0)}_{\text{βάση}}, \quad \underbrace{(\forall j \in \{n_0, \dots, k\} P(j)) \Rightarrow P(k+1)}_{\text{βήμα για κάθε } k \geq n_0}.$$

Χρήσιμη όταν η νέα περίπτωση εξαρτάται από μικρότερα μεγέθη που δεν είναι απαραίτητα το αμέσως προηγούμενο.

Ίδια αποδεικτική ισχύς με την απλή επαγωγή. Θέτουμε

$$Q(k) := \bigwedge_{j=n_0}^k P(j).$$

Η απλή επαγωγή στην $Q(k)$ δίνει την ισχυρή επαγωγή στην $P(k)$.

Ισχυρή επαγωγή: γινόμενο πρώτων

Πρόταση. Κάθε ακέραιος $n \geq 2$ είναι γινόμενο πρώτων.

Βάση: το 2 είναι πρώτο.

Βήμα: έστω $n \geq 3$. Υποθέτουμε την πρόταση για κάθε j με $2 \leq j < n$.

- Αν το n είναι πρώτο, είναι ήδη γινόμενο ενός πρώτου.
- Διαφορετικά, $n = ab$, όπου $2 \leq a, b < n$. Η επαγωγική υπόθεση δίνει αναλύσεις των a, b σε πρώτους. Το γινόμενό τους δίνει μια ανάλυση του n .

Αποδείξαμε την ύπαρξη της ανάλυσης. Η μοναδικότητα χρειάζεται ξεχωριστή απόδειξη.

Καλή διάταξη και ελάχιστο αντιπαράδειγμα

Αρχή καλής διάταξης: κάθε μη κενό υποσύνολο της $\mathbb{N} = \{0, 1, 2, \dots\}$ έχει ελάχιστο στοιχείο.

Γιατί λειτουργεί η επαγωγή; Αν υπάρχει αντιπαράδειγμα, έστω m το μικρότερο. Η βάση δίνει $m > n_0$. Από την ελαχιστότητα ισχύει $P(m - 1)$, οπότε το επαγωγικό βήμα δίνει $P(m)$: αντίφαση.

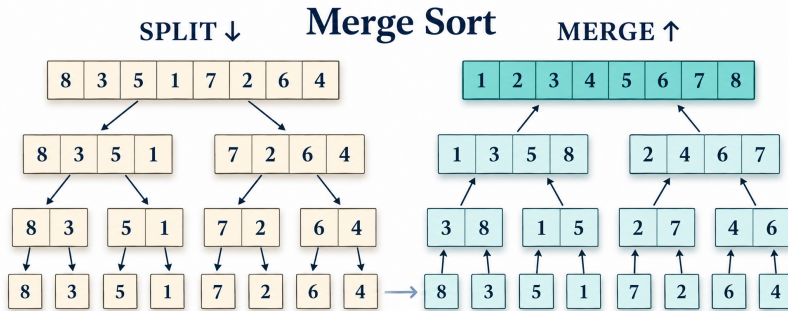
Άπειρη κάθοδος: από κάθε αντιπαράδειγμα κατασκευάζουμε ένα αυστηρά μικρότερο. Αυτό είναι αδύνατο στους φυσικούς.

Παράδειγμα: αν $n = ab$ δεν έχει ανάλυση σε πρώτους, τότε τουλάχιστον ένα από τα $a, b < n$ επίσης δεν έχει.

Από έναν αναδρομικό αλγόριθμο στην επαγωγή

Παράδειγμα: MergeSort. Για να ταξινομήσουμε $n = 2^r$ στοιχεία:

1. Τα χωρίζουμε σε δύο μισά.
2. Ταξινομούμε κάθε μισό αναδρομικά.
3. Συγχωνεύουμε τις ταξινομημένες ακολουθίες με το πολύ n συγκρίσεις.



Από έναν αναδρομικό αλγόριθμο στην επαγωγή

Ένα **άνω φράγμα** στο πλήθος συγκρίσεων ορίζεται από

$$T(1) = 0, \quad T(n) = \underbrace{2T(n/2)}_{\text{δύο αναδρομικές κλήσεις}} + \underbrace{n}_{\text{συγχώνευση}}.$$

Ισχυρισμός: $T(2^r) = r 2^r$, δηλαδή $T(n) = n \log_2 n$.

Βάση: $r = 0$: $T(1) = 0 = 0 \cdot 1$.

Βήμα: Υποθέτουμε ότι $T(2^r) = r 2^r$. Τότε

$$T(2^{r+1}) = 2T(2^r) + 2^{r+1} = 2r 2^r + 2^{r+1} = (r+1)2^{r+1}.$$

Ο αλγόριθμος δίνει την αναδρομική σχέση· η επαγωγή αποδεικνύει τη λύση της.

Δομική επαγωγή

Σε έναν αναδρομικό ορισμό έχουμε **βασικά αντικείμενα** και **κανόνες κατασκευής** νέων αντικειμένων. Θεωρούμε μόνο όσα προκύπτουν με πεπερασμένες εφαρμογές των κανόνων.

Για να αποδείξουμε την $P(X)$ για όλα τα αντικείμενα:

1. Αποδεικνύουμε την P για κάθε βασικό αντικείμενο.
2. Για **κάθε** κανόνα $X = C(X_1, \dots, X_k)$, υποθέτουμε $P(X_1), \dots, P(X_k)$ και αποδεικνύουμε $P(X)$.

Παραδείγματα: λέξεις, δέντρα, αριθμητικές εκφράσεις.

Η επαγωγή στους φυσικούς είναι η ειδική περίπτωση με βάση το 0 και κανόνα κατασκευής $n \mapsto n + 1$.

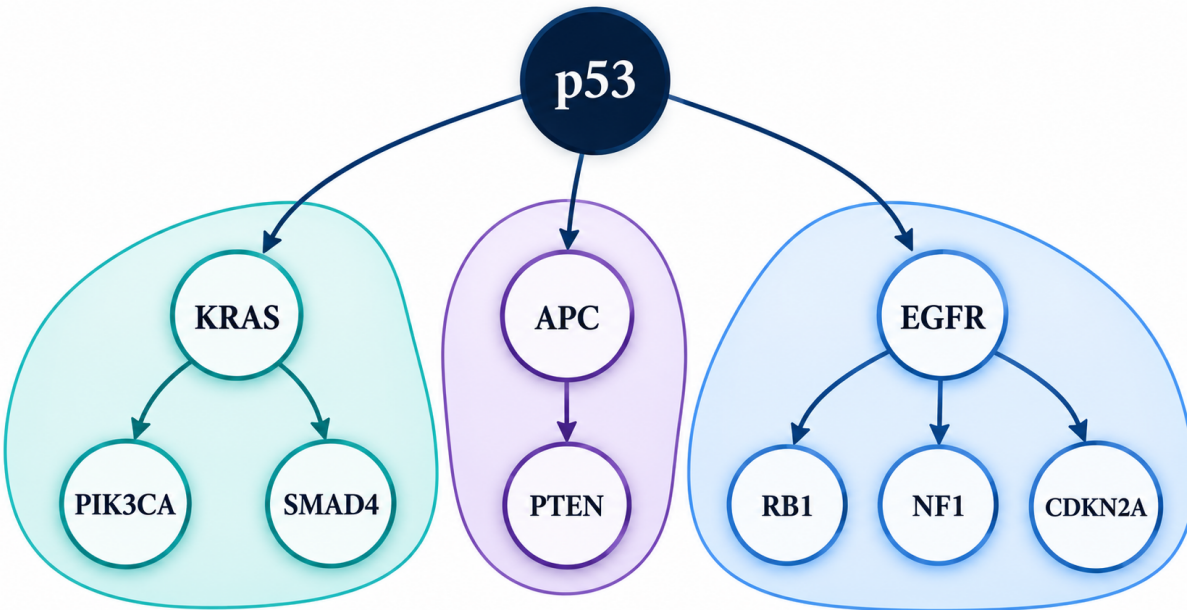
Δέντρα, ρίζες και υποδέντρα

Δέντρο είναι ένα συνεκτικό, μη κατευθυνόμενο γράφημα χωρίς κύκλους. Ισοδύναμα, μεταξύ κάθε δύο κορυφών υπάρχει ακριβώς ένα απλό μονοπάτι.

Σε ένα **ριζωμένο δέντρο** επιλέγουμε μία κορυφή ως **ρίζα**. Κατευθύνουμε τις ακμές από τον **γονέα** προς τα **παιδιά**:

- Η ρίζα δεν έχει γονέα· κάθε άλλη κορυφή έχει ακριβώς έναν γονέα.
- Οι κορυφές χωρίς παιδιά ονομάζονται **φύλλα**.
- Το **υποδέντρο με ρίζα** v αποτελείται από τη v , όλους τους απογόνους της και τις ακμές που τους συνδέουν.

Κάθε παιδί της ρίζας είναι ρίζα ενός μικρότερου δέντρου!



Σχηματικό παράδειγμα μεταλλάξεων

Δομική επαγωγή: ακμές ενός δέντρου

Κατασκευή ριζωμένων δέντρων: ένα μόνο φύλλο, ή νέα ρίζα που συνδέεται με τις ρίζες $k \geq 1$ ξένων δέντρων $T_1, \dots, T_k$.

Πρόταση: κάθε τέτοιο δέντρο έχει $e = v - 1$ ακμές.

Βάση: ένα φύλλο έχει $v = 1, e = 0$.

Βήμα: υποθέτουμε $e_i = v_i - 1$ για κάθε T_i .

$$v = 1 + \sum_{i=1}^k v_i, \quad e = k + \sum_{i=1}^k e_i = k + \sum_{i=1}^k (v_i - 1) = \sum_{i=1}^k v_i = v - 1.$$

Η υπόθεση αφορά τα **άμεσα υποδέντρα** της νέας ρίζας.

Δομική επαγωγή: παρενθέσεις εκφράσεων

Ορισμός: αριθμοί και μεταβλητές είναι εκφράσεις. Αν E, F είναι εκφράσεις, τότε είναι και οι $E + F$, $E \cdot F$, (E) .

Πρόταση: $L(E) = R(E)$, όπου L, R μετρούν τις αριστερές και τις δεξιές παρενθέσεις.

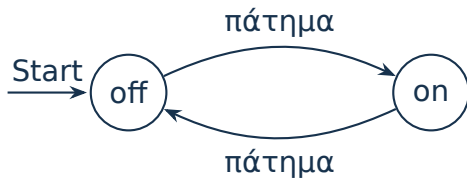
Βάση: για αριθμό ή μεταβλητή, $L = R = 0$.

Βήμα: υποθέτουμε $L(E) = R(E)$ και $L(F) = R(F)$.

- Για $G = E + F$ ή $G = E \cdot F$: $L(G) = L(E) + L(F) = R(E) + R(F) = R(G)$.
- Για $G = (E)$: $L(G) = L(E) + 1 = R(E) + 1 = R(G)$.

Καλύψαμε **όλους τους κανόνες** του αναδρομικού ορισμού.

Αμοιβαία επαγωγή: ο διακόπτης ως αυτόματο



Θεωρούμε τις δύο προτάσεις για το αυτόματο:

$S_1(n)$: Μετά από n πατήματα, είναι σε κατάσταση off $\iff n$ είναι άρτιος.

$S_2(n)$: Μετά από n πατήματα, είναι σε κατάσταση on $\iff n$ είναι περιττός.

Στόχος: να αποδείξουμε ταυτόχρονα τις $S_1(n)$ και $S_2(n)$ για κάθε $n \geq 0$.

Γιατί χρειαζόμαστε αμοιβαία επαγωγή;

Θα μπορούσε κανείς να σκεφτεί ότι οι $S_1(n)$ και $S_2(n)$ είναι ουσιαστικά το ίδιο.

Πράγματι, για τους αριθμούς ξέρουμε ότι ένας αριθμός δεν μπορεί να είναι και άρτιος και περιττός.

Όμως για ένα αυτόματο δεν είναι πάντα αυτονόητο ότι βρίσκεται σε μία και μόνο μία κατάσταση. Στο συγκεκριμένο παράδειγμα αυτό ισχύει, αλλά αυτό πρέπει ουσιαστικά να ενσωματωθεί στην απόδειξη.

Γι' αυτό δεν αποδεικνύουμε μόνο μία πρόταση, αλλά **δύο μαζί**:

$$S_1(n) \quad \text{και} \quad S_2(n).$$

Η απόδειξη θα έχει:

- μία **βάση** για $n = 0$,
- και ένα **επαγωγικό βήμα** από το n στο $n + 1$,

αλλά επειδή κάθε $S_i(n)$ είναι ισοδυναμία, θα εμφανιστούν **τέσσερις επιμέρους περιπτώσεις** στη βάση και **τέσσερις** στο βήμα.

Βάση: $n = 0$

Θέλουμε να δείξουμε τις $S_1(0)$ και $S_2(0)$.

1. $[S_1; \text{If}]$

Αφού το 0 είναι άρτιος, πρέπει να δείξουμε ότι μετά από 0 πατήματα το αυτόματο είναι σε κατάσταση off.

Αυτό είναι άμεσο, γιατί η αρχική κατάσταση είναι η off.

2. $[S_1; \text{Only-if}]$

Υποθέτουμε ότι μετά από 0 πατήματα το αυτόματο είναι σε κατάσταση off.

Τότε πρέπει να δείξουμε ότι το 0 είναι άρτιος.

Αυτό είναι αληθές από τον ορισμό: το 0 είναι άρτιος.

Βάση: οι άλλες δύο περιπτώσεις

3. $[S_2; If]$

Η υπόθεση του ``if'' για την $S_2(0)$ είναι ότι το 0 είναι περιττός.

Αυτή η υπόθεση είναι **ψευδής**. Άρα κάθε πρόταση της μορφής

``αν H τότε C ''

είναι αληθής όταν το H είναι ψευδές.

Επομένως ισχύει και η $S_2(0)$ ως προς το ``if'' μέρος.

4. $[S_2; Only-if]$

Υποθέτουμε ότι μετά από 0 πατήματα το αυτόματο είναι σε κατάσταση on.

Αυτό όμως είναι αδύνατο, γιατί η κατάσταση on επιτυγχάνεται μόνο αν ακολουθήσουμε τόξο με ετικέτα *πάτημα*, δηλαδή μόνο μετά από τουλάχιστον ένα πάτημα.

Άρα η υπόθεση είναι πάλι **ψευδής**, και επομένως το if-then είναι αληθές.

Συμπέρασμα: οι $S_1(0)$ και $S_2(0)$ ισχύουν.

Επαγωγική υπόθεση και στόχος

Επαγωγική υπόθεση: Υποθέτουμε ότι για κάποιο $n \geq 0$ ισχύουν και οι δύο προτάσεις:

$S_1(n)$: off μετά από n πατήματα $\iff n$ άρτιος,

$S_2(n)$: on μετά από n πατήματα $\iff n$ περιττός.

Θέλουμε να δείξουμε:

$S_1(n+1)$ και $S_2(n+1)$.

Δηλαδή πάλι θα εξετάσουμε τέσσερις περιπτώσεις:

1. $[S_1(n+1); \text{If}]$
2. $[S_1(n+1); \text{Only-if}]$
3. $[S_2(n+1); \text{If}]$
4. $[S_2(n+1); \text{Only-if}]$

Επαγωγικό βήμα: απόδειξη της $S_1(n + 1)$

1. $[S_1(n + 1); \text{If}]$

Υποθέτουμε ότι το $n + 1$ είναι άρτιος.

Τότε ο n είναι περιττός.

Από την επαγωγική υπόθεση $S_2(n)$ συμπεραίνουμε ότι μετά από n πατήματα το αυτόματο είναι σε κατάσταση on.

Το επόμενο πάτημα το μεταφέρει από on σε off.

Άρα μετά από $n + 1$ πατήματα το αυτόματο είναι σε κατάσταση off.

2. $[S_1(n + 1); \text{Only-if}]$

Υποθέτουμε ότι μετά από $n + 1$ πατήματα το αυτόματο είναι σε κατάσταση off.

Για να βρεθεί στην off μετά από ένα ακόμη πάτημα, θα πρέπει αμέσως πριν, δηλαδή μετά από n πατήματα, να ήταν στην on.

Με την επαγωγική υπόθεση $S_2(n)$ συμπεραίνουμε ότι ο n είναι περιττός.

Άρα το $n + 1$ είναι άρτιος.

Επομένως αποδείχθηκε η $S_1(n + 1)$.

Επαγωγικό βήμα: απόδειξη της $S_2(n + 1)$

3. $[S_2(n + 1); \text{If}]$

Υποθέτουμε ότι το $n + 1$ είναι περιττός.

Τότε ο n είναι άρτιος.

Από την επαγωγική υπόθεση $S_1(n)$ έχουμε ότι μετά από n πατήματα το αυτόματο είναι σε κατάσταση off.

Με ένα ακόμη πάτημα μεταβαίνει στην κατάσταση on.

Άρα μετά από $n + 1$ πατήματα βρίσκεται στην on.

4. $[S_2(n + 1); \text{Only-if}]$

Υποθέτουμε ότι μετά από $n + 1$ πατήματα το αυτόματο είναι σε κατάσταση on.

Τότε αμέσως πριν, δηλαδή μετά από n πατήματα, πρέπει να ήταν στην off.

Από την επαγωγική υπόθεση $S_1(n)$ συμπεραίνουμε ότι ο n είναι άρτιος.

Άρα το $n + 1$ είναι περιττός.

Επομένως αποδείχθηκε και η $S_2(n + 1)$.

Συμπέρασμα

Αποδείξαμε:

- τη **βάση** για $n = 0$,
- και το **επαγωγικό βήμα**:

$$S_1(n) \wedge S_2(n) \implies S_1(n+1) \wedge S_2(n+1).$$

Άρα, με αμοιβαία επαγωγή, για κάθε $n \geq 0$ ισχύουν:

$S_1(n)$: off μετά από n πατήματα $\iff n$ άρτιος,

$S_2(n)$: on μετά από n πατήματα $\iff n$ περιττός.

Κεντρική ιδέα: όταν δύο ιδιότητες εξαρτώνται η μία από την άλλη, συχνά τις αποδεικνύουμε **ταυτόχρονα**.

Σύνοψη επιχειρήματος

Ένας διακόπτης ξεκινά κλειστός και αλλάζει κατάσταση σε κάθε πάτημα.

$S_1(n)$: κλειστός μετά από n πατήματα $\iff n$ άρτιος,

$S_2(n)$: ανοιχτός μετά από n πατήματα $\iff n$ περιττός.

Αποδεικνύουμε με επαγωγή την $Q(n) := S_1(n) \wedge S_2(n)$.

Βάση $n = 0$: κλειστός και άρτιος, μη ανοιχτός και μη περιττός.

Βήμα:

κλειστός στο $n + 1 \iff$ ανοιχτός στο $n \xrightarrow{B(n)} n$ περιττός $\iff n + 1$ άρτιος,

ανοιχτός στο $n + 1 \iff$ κλειστός στο $n \xrightarrow{A(n)} n$ άρτιος $\iff n + 1$ περιττός.

Υποθέτουμε και τις δύο ιδιότητες στο n και αποδεικνύουμε και τις δύο στο $n + 1$.