Πιθανοθεωρητικές Μέθοδοι στην Ανάλυση Κυκλωμάτων

Μεταπτυχιακή Εργασία

Δημήτρης Καλοψικάκης

15 Σεπτεμβρίου 2020

Μπορούν τα λογικά κυκλώματα μικρής πολυπλοκότητας να εκφράσουν συναρτήσεις ισοτιμίας;

Μπορούν τα λογικά κυκλώματα μικρής πολυπλοκότητας να εκφράσουν συναρτήσεις ισοτιμίας;

Μπορούν τα λογικά κυκλώματα μικρής πολυπλοκότητας να εκφράσουν συναρτήσεις ισοτιμίας;

Μπορούν τα λογικά κυκλώματα μικρής πολυπλοκότητας να εκφράσουν συναρτήσεις ισοτιμίας;

Λογική Συνάρτηση:

$$\{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}^n \rightarrow \{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}\,, n \in \mathbb{N}$$

Λογική Συνάρτηση:

$$\{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}^n \to \{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}\,, n \in \mathbb{N}$$

$$\mathbb{R}^n \supset \{0,1\}^n \to \{0,1\} \subset \mathbb{R} \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto 1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto 0 \end{cases}$$

Λογική Συνάρτηση:

$$\{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}^n \to \{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}, n \in \mathbb{N}$$

$$\mathbb{R}^n \supset \{0,1\}^n \to \{0,1\} \subset \mathbb{R} \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto 1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto 0 \end{cases}$$

$$\mathbb{F}_2^n \to \mathbb{F}_2 \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto 1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto 0 \end{cases}$$

Λογική Συνάρτηση:

$$\{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}^n \to \{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}, n \in \mathbb{N}$$

$$\mathbb{R}^n \supset \{0,1\}^n \to \{0,1\} \subset \mathbb{R} \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto 1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto 0 \end{cases}$$

$$\mathbb{F}_2^n \to \mathbb{F}_2 \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto 1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto 0 \end{cases}$$

$$\mathbb{R}^n \supset \{\pm 1\}^n \to \{\pm 1\} \subset \mathbb{R} \quad \begin{cases} \alpha\lambda\eta\theta\acute{\varepsilon}\varsigma \mapsto -1 \\ \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma \mapsto +1 \end{cases}$$

Λογική Συνάρτηση:

$$\{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}^n \rightarrow \{\alpha\lambda\eta\theta\acute{\varepsilon}\varsigma, \psi\varepsilon\upsilon\delta\acute{\varepsilon}\varsigma\}, n \in \mathbb{N}$$

Κανόνες De Morgan:

$$\neg (P \wedge Q) = (\neg P) \vee (\neg Q)$$
$$\neg (P \vee Q) = (\neg P) \wedge (\neg Q)$$
$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

Μια Λογική Συνάρτηση είναι Πολυγραμμικό Πολυώνυμο.

Μια Λογική Συνάρτηση είναι Πολυγραμμικό Πολυώνυμο.

Π.χ.

$$AND_2 : \{\pm 1\}^2 \to \{\pm 1\},$$

$$AND_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1 x_2$$

$$AND_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

Συνάρτηση ισοτιμίας (parity):

$\pi_n =$«*αλήθεια*» <u>*ανν*</u> περιττό πλήθος μεταβλητών «*αλήθειας*».

$$AND_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

Συνάρτηση ισοτιμίας (parity):

π_n =«*αλήθεια*» <u>*ανν*</u> περιττό πλήθος μεταβλητών «*αλήθειας*».

$$\pi_n(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$$

$$AND_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

Συνάρτηση ισοτιμίας (parity):

π_n =«*αλήθεια*» ανν περιττό πλήθος μεταβλητών «*αλήθειας*».

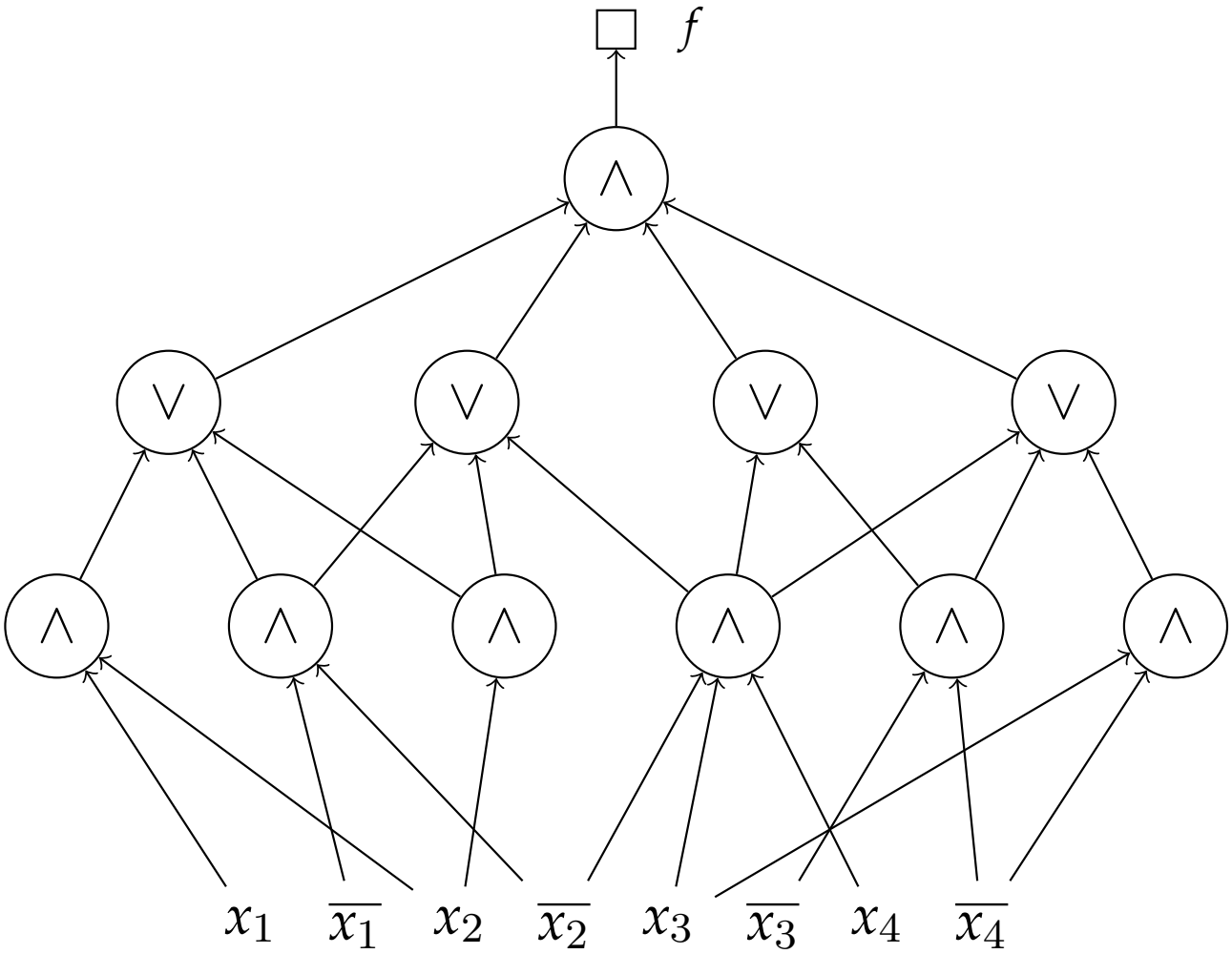
$$\pi_n(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$$

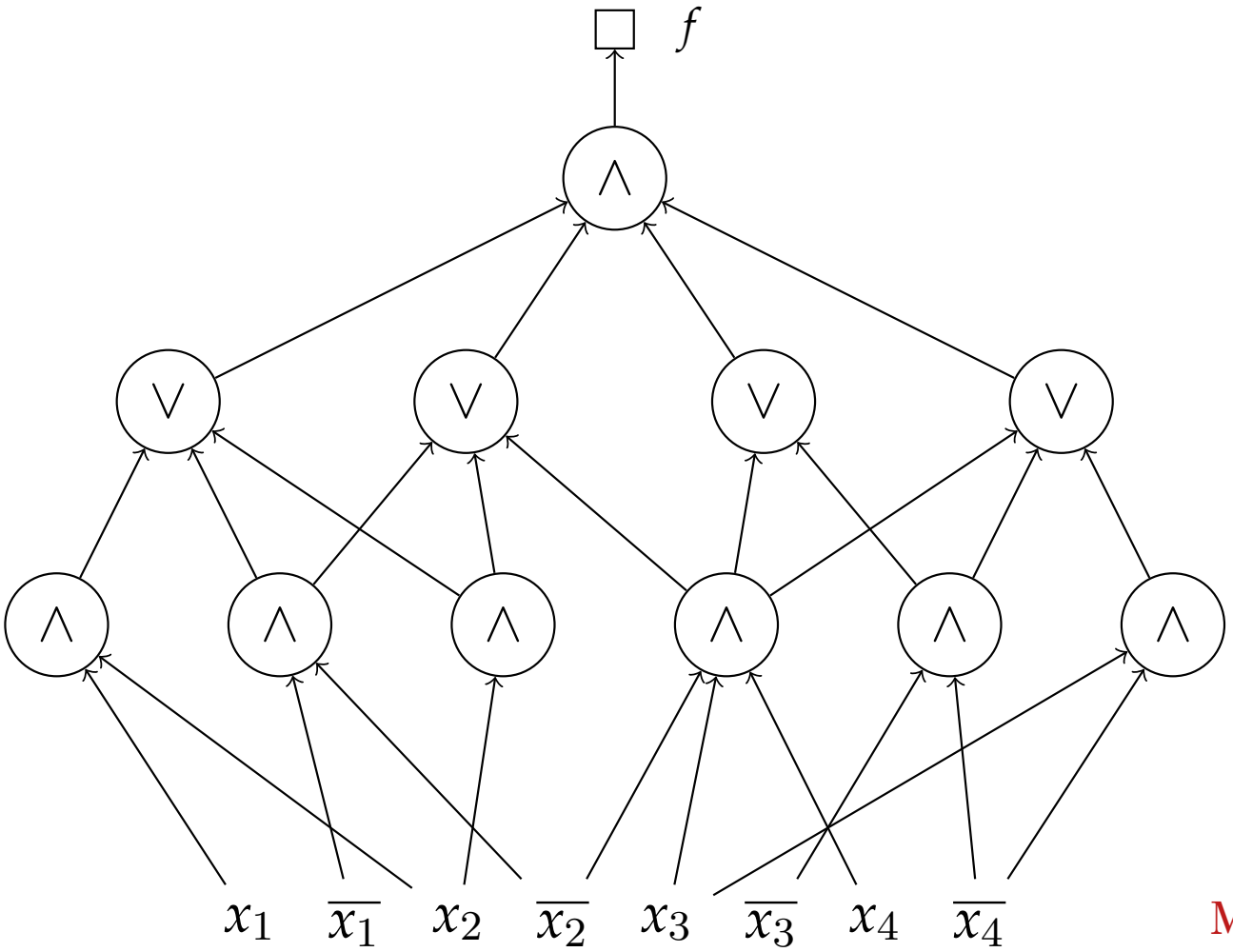
Βάση του χώρου των λογικών συναρτήσεων n μεταβλητών.

Τα λογικά κυκλώματα είναι μια αφαιρετική αναπαράσταση λογικών συναρτήσεων.

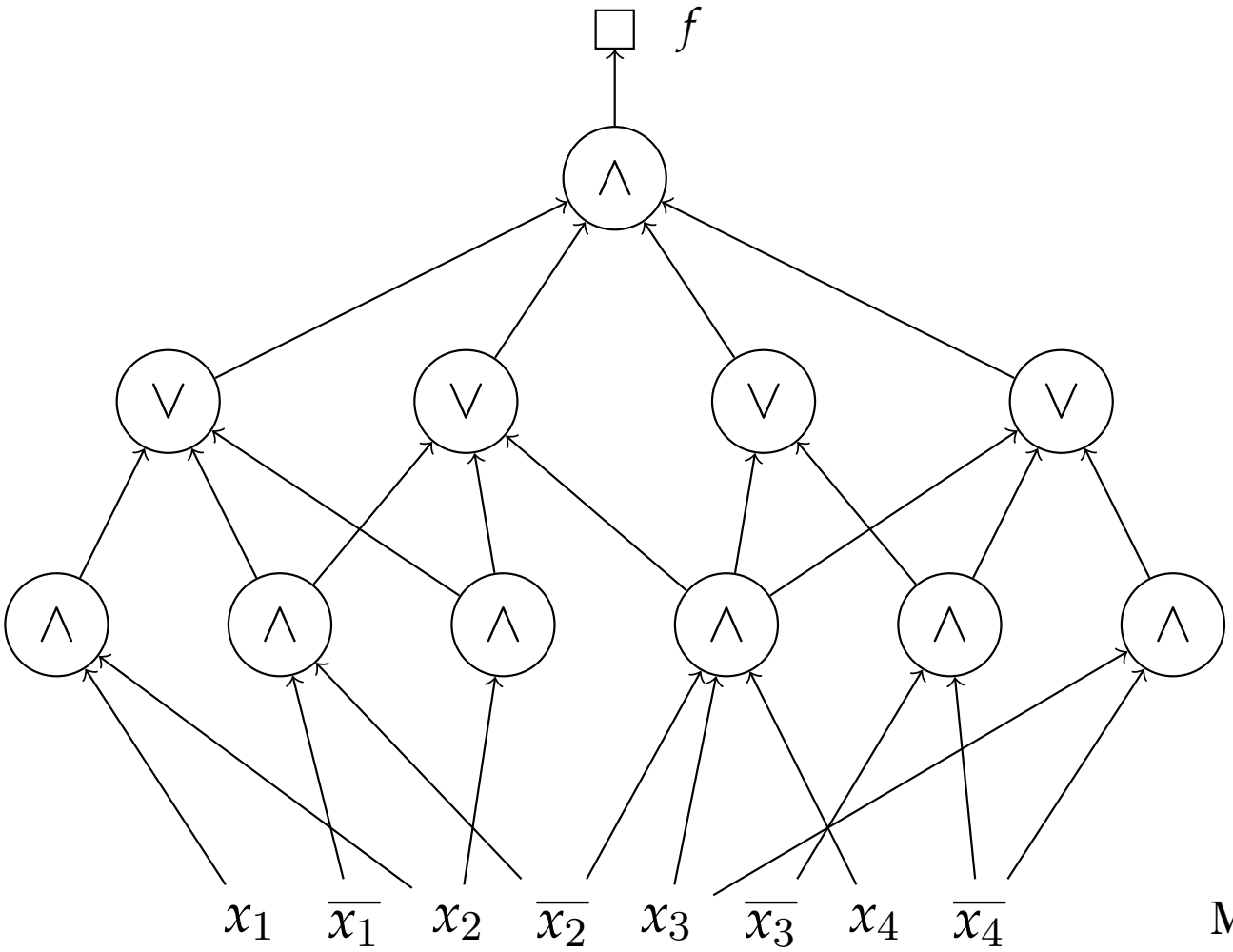
Τα λογικά κυκλώματα είναι μια αφαιρετική αναπαράσταση λογικών συναρτήσεων.

Τα λογικά κυκλώματα είναι μια αφαιρετική αναπαράσταση λογικών συναρτήσεων.


f
∧
∨
∨
∨
∨
∧
∧
∧
∧
∧
∧
x1
x1
x2
x2
x3
x3
x4
x4

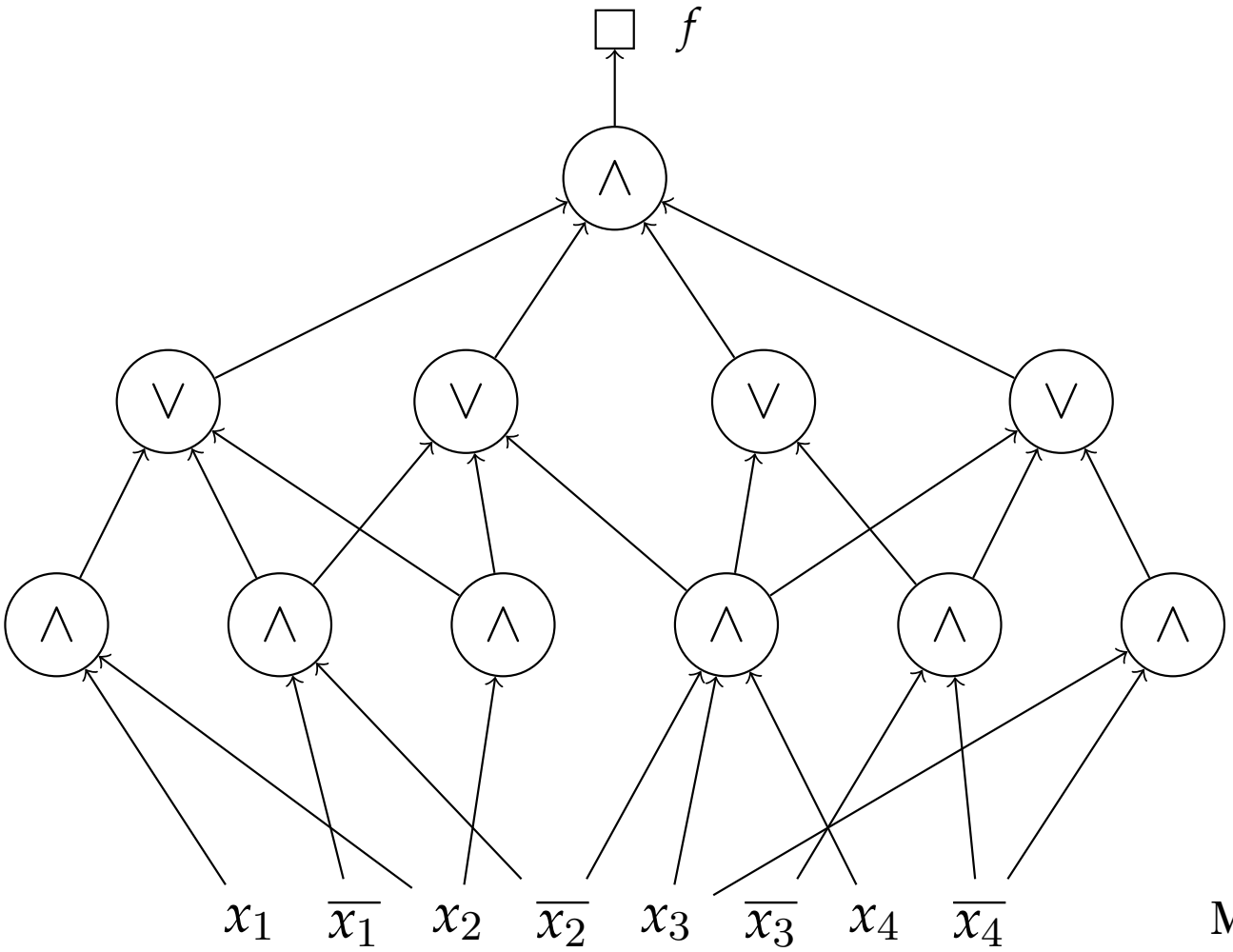


Μεταβλητές Εισόδου



Επίπεδο 1

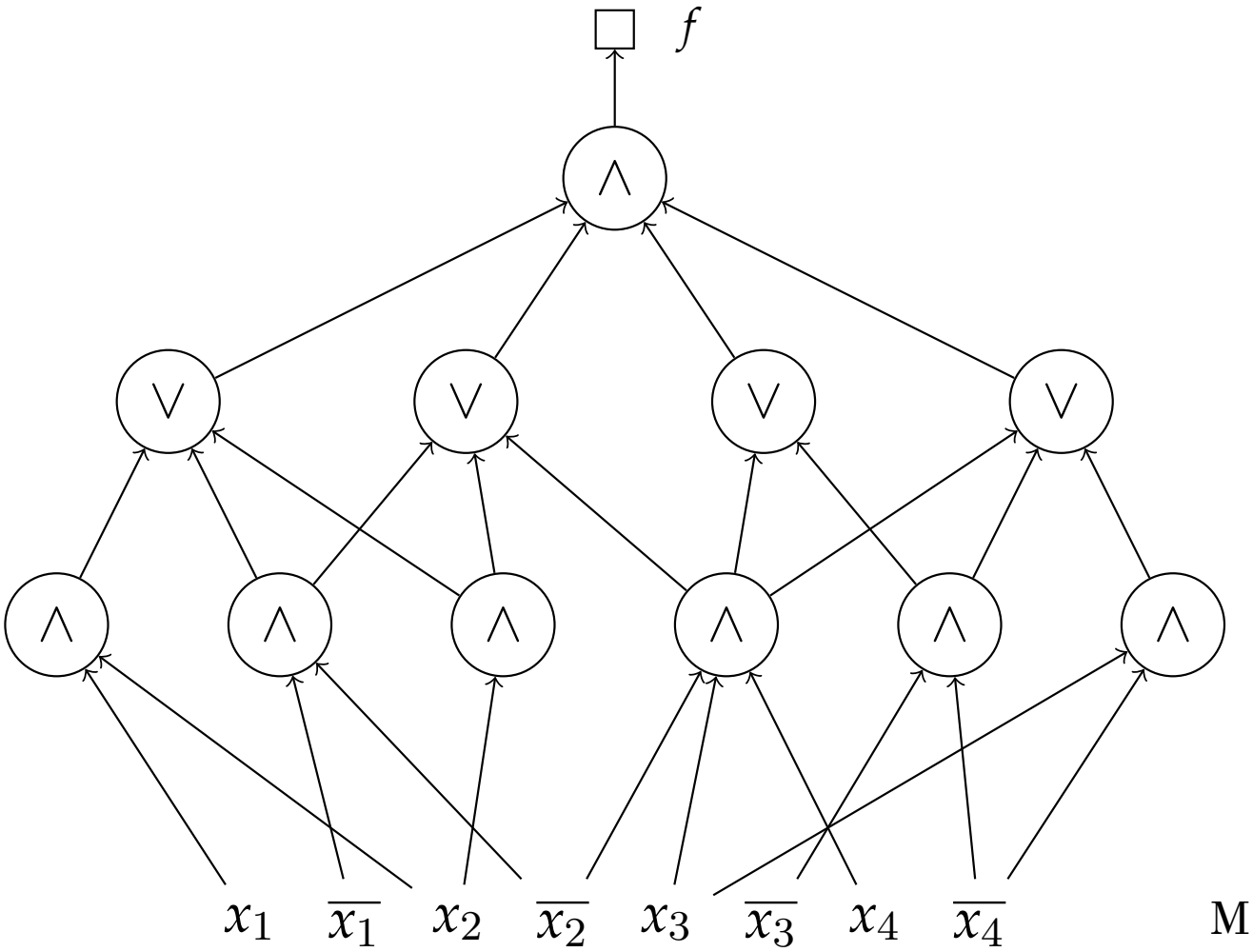
Μεταβλητές Εισόδου



Επίπεδο 2

Επίπεδο 1

Μεταβλητές Εισόδου

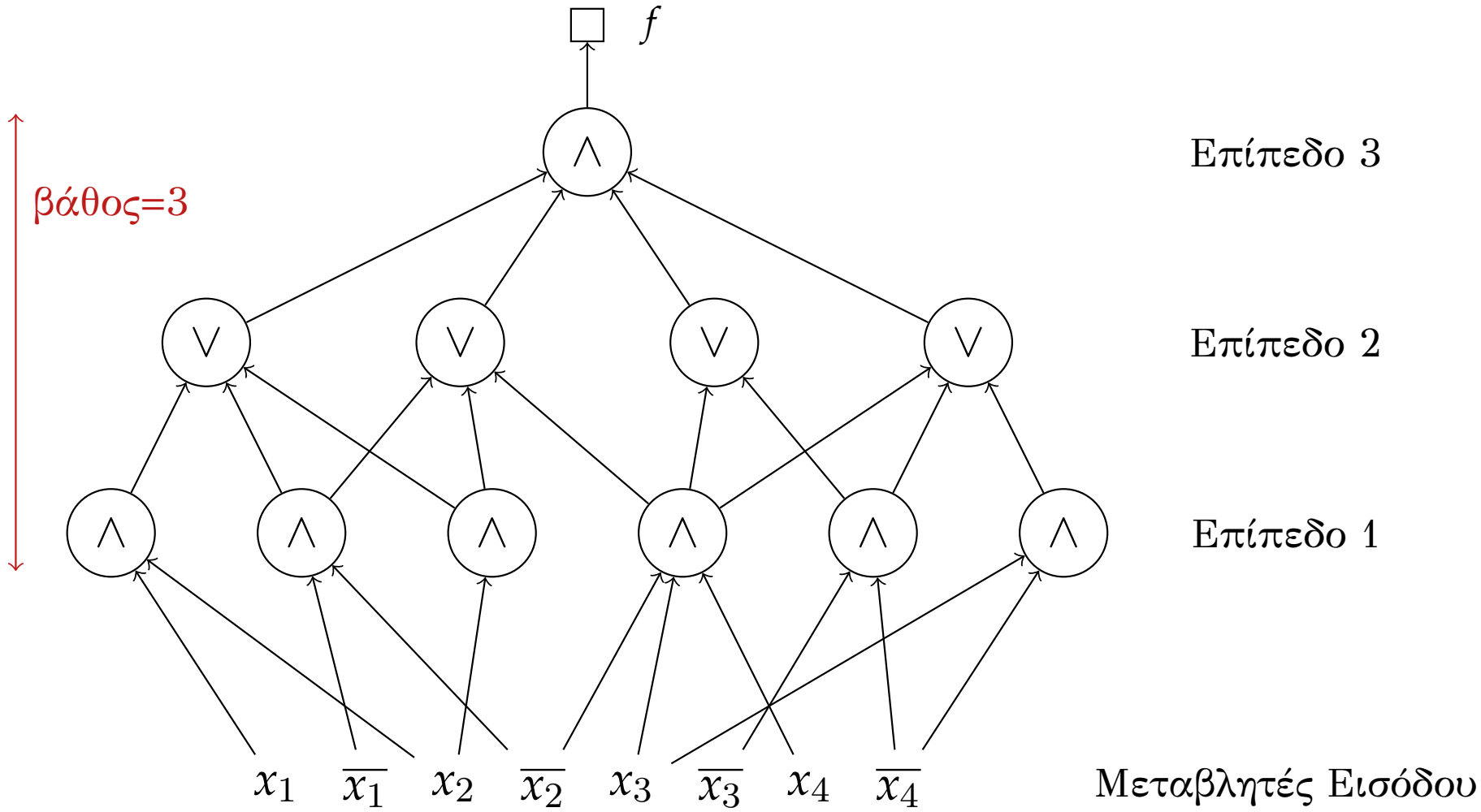


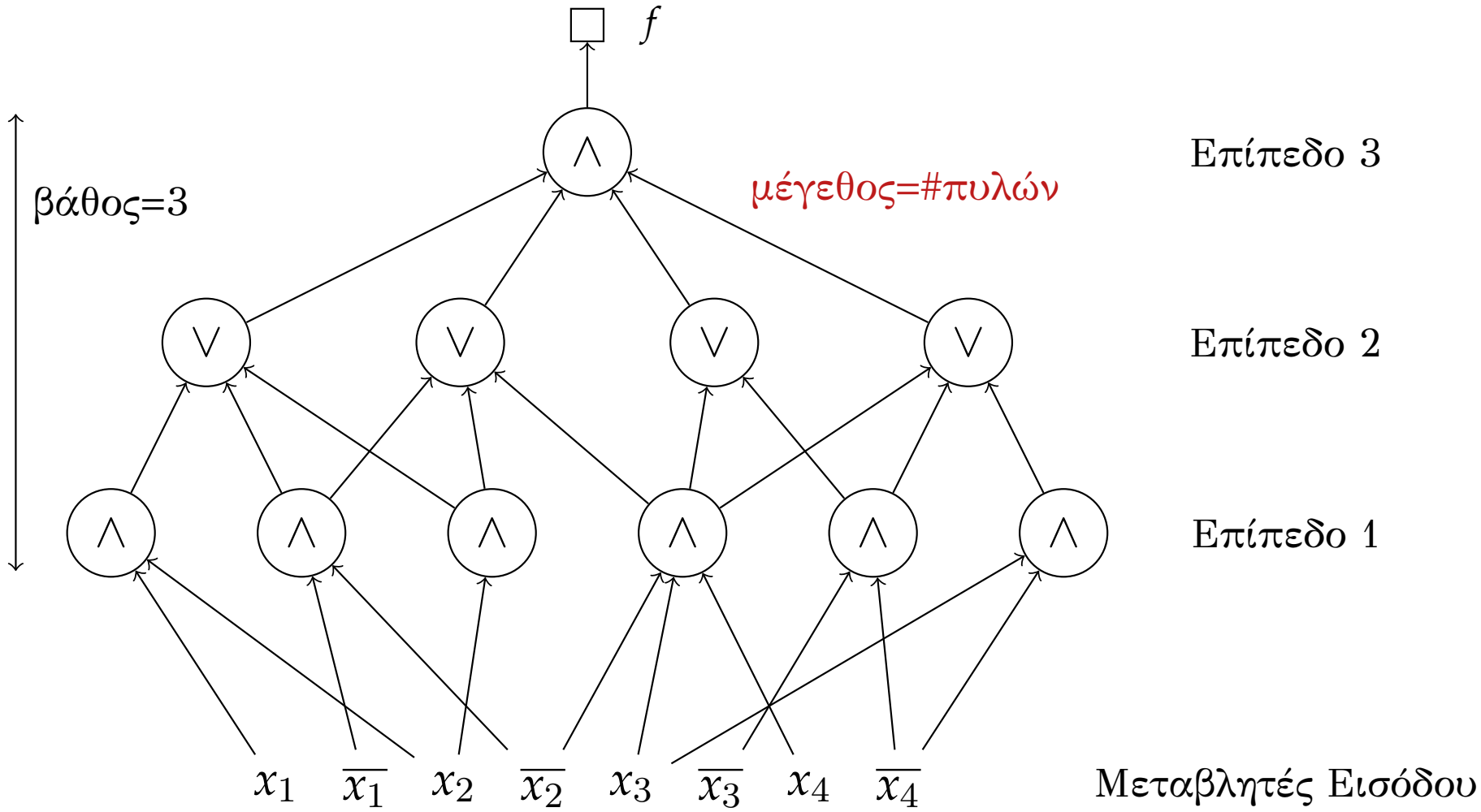
Επίπεδο 3

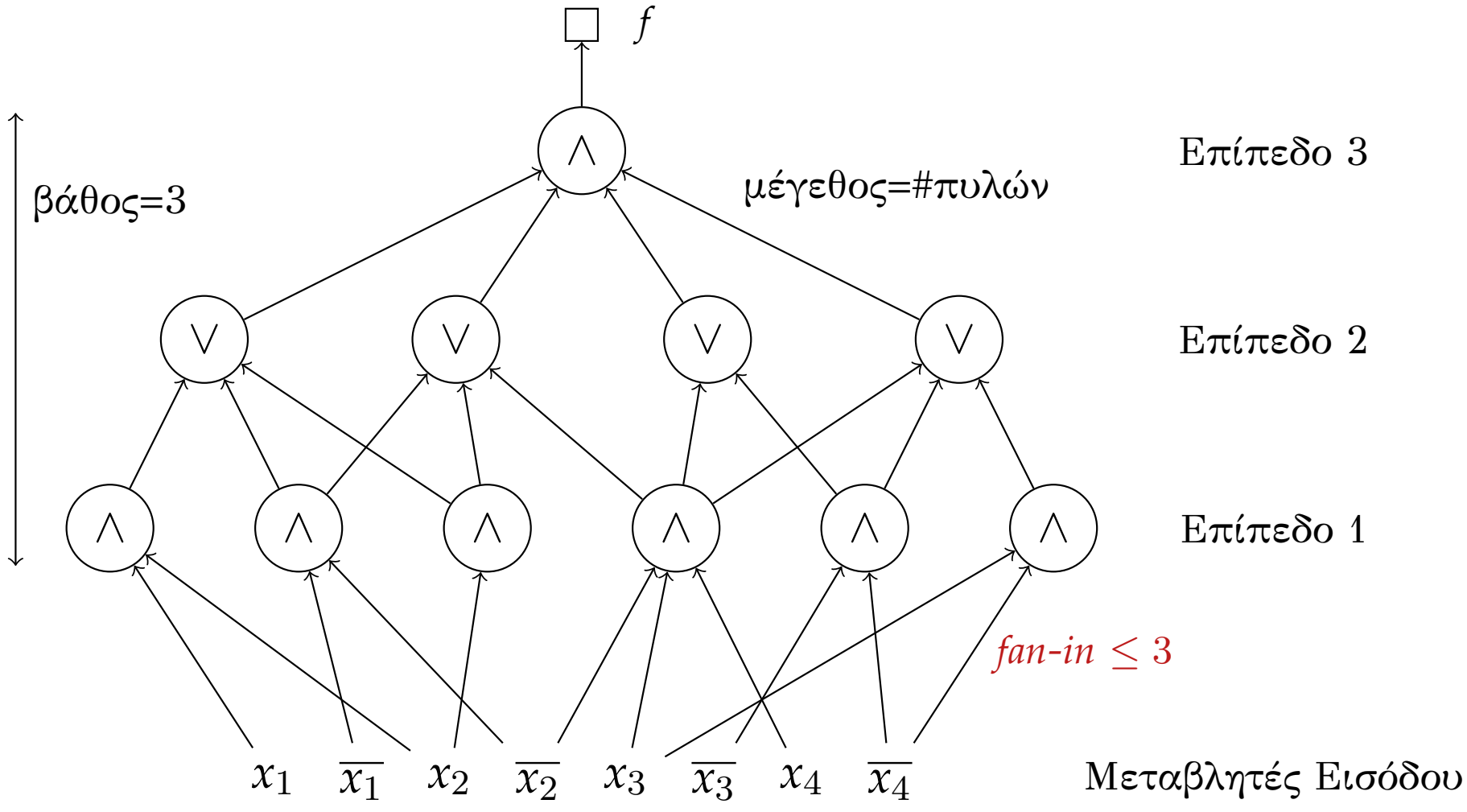
Επίπεδο 2

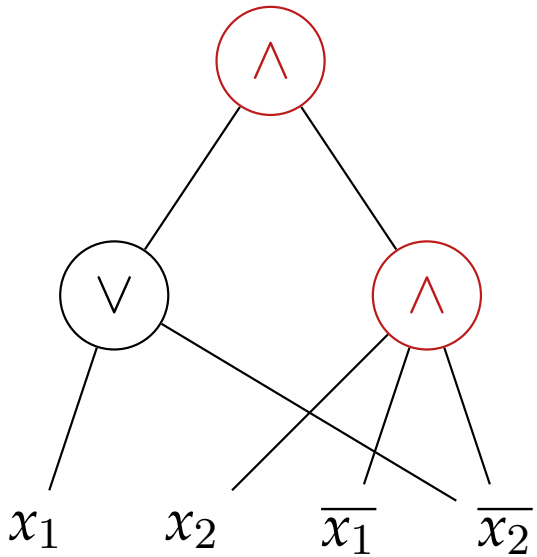
Επίπεδο 1

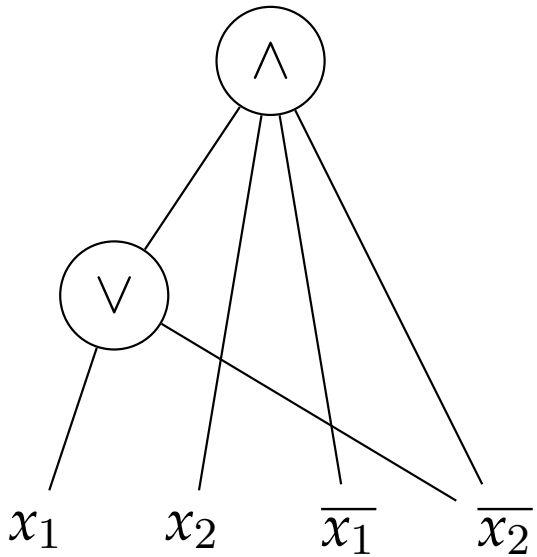
Μεταβλητές Εισόδου

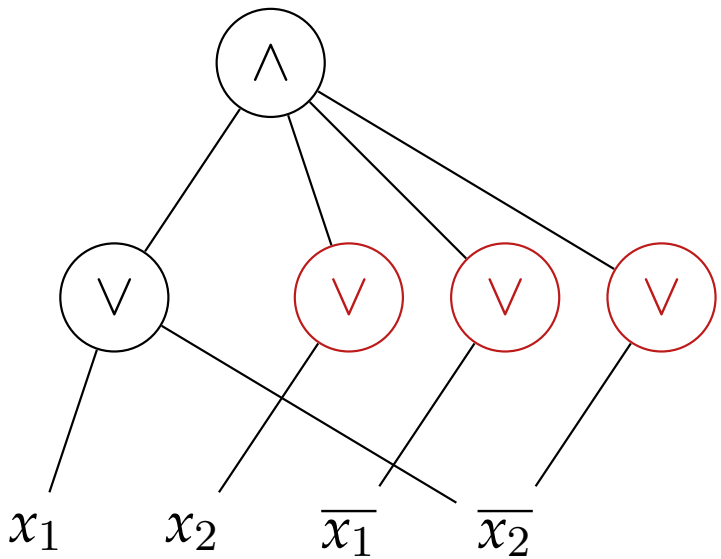

f
βάθος=3
Επίπεδο 3
Επίπεδο 2
Επίπεδο 1
x_1 $\overline{x_1}$ x_2 $\overline{x_2}$ x_3 $\overline{x_3}$ x_4 $\overline{x_4}$
Μεταβλητές Εισόδου


f
βάθος=3
μέγεθος=#πυλών
Επίπεδο 3
Επίπεδο 2
Επίπεδο 1
x_1 $\overline{x_1}$ x_2 $\overline{x_2}$ x_3 $\overline{x_3}$ x_4 $\overline{x_4}$
Μεταβλητές Εισόδου


f
βάθος=3
μέγεθος=#πυλών
Επίπεδο 3
Επίπεδο 2
Επίπεδο 1
fan-in ≤ 3
x1 x̄1 x2 x̄2 x3 x̄3 x4 x̄4
Μεταβλητές Εισόδου


∧
∨
∧
x_1
x_2
$\overline{x_1}$
$\overline{x_2}$


∧
∨
x_1
x_2
$\overline{x_1}$
$\overline{x_2}$


∧
∨
∨
∨
∨
x_1
x_2
$\overline{x_1}$
$\overline{x_2}$

Ανάλυση Κυκλωμάτων

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.
- Πολυπλοκότητα κυκλώματος: **μέγεθος**, **βάθος**.

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.
- Πολυπλοκότητα κυκλώματος: **μέγεθος**, **βάθος**.
- «Μικρό», «Μεγάλο»: ασυμπτωτικά συναρτήσει του πλήθους των μεταβλητών εισόδου.

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.
- Πολυπλοκότητα κυκλώματος: **μέγεθος**, **βάθος**.
- «Μικρό», «Μεγάλο»: ασυμπτωτικά συναρτήσει του πλήθους των μεταβλητών εισόδου.
- Τάξεις μεγέθους:

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.
- Πολυπλοκότητα κυκλώματος: **μέγεθος**, **βάθος**.
- «Μικρό», «Μεγάλο»: ασυμπτωτικά συναρτήσει του πλήθους των μεταβλητών εισόδου.
- Τάξεις μεγέθους:
  - Σταθερή, λογαριθμική, πολυωνυμική, εκθετική.

Ανάλυση Κυκλωμάτων:

- Θέλουμε κυκλώματα με όσο γίνεται μικρότερη πολυπλοκότητα.
- Πολυπλοκότητα κυκλώματος: **μέγεθος**, **βάθος**.
- «Μικρό», «Μεγάλο»: ασυμπτωτικά συναρτήσει του πλήθους των μεταβλητών εισόδου.
- Τάξεις μεγέθους:
  - Σταθερή, λογαριθμική, πολυωνυμική, εκθετική.
- Οριοθέτηση υπολογιστικής ικανότητας.

AC^k: συναρτήσεις n μεταβλητών, που εκφράζονται από κυκλώματα με πύλες AND, OR, πολυωνυμικού μεγέθους, πολυλογαριθμικού βάθους, $\mathcal{O}\left(\log^k n\right)$,
και μη φραγμένου «*fan-in*».

AC^k: συναρτήσεις n μεταβλητών, που εκφράζονται από κυκλώματα με πύλες AND, OR, πολυωνυμικού μεγέθους, πολυλογαριθμικού βάθους, $\mathcal{O}\left(\log^k n\right)$, και μη φραγμένου «*fan-in*».

AC^k: συναρτήσεις n μεταβλητών, που εκφράζονται από κυκλώματα με πύλες AND, OR, πολυωνυμικού μεγέθους, πολυλογαριθμικού βάθους, $\mathcal{O}\left(\log^k n\right)$, και μη φραγμένου «*fan-in*».

AC^0: συναρτήσεις n μεταβλητών, που εκφράζονται από κυκλώματα με πύλες AND, OR, πολυωνυμικού μεγέθους, σταθερού βάθους, $\mathcal{O}(1)$,
και μη φραγμένου «*fan-in*».

AC^0: συναρτήσεις n μεταβλητών, που εκφράζονται από κυκλώματα με πύλες AND, OR, πολυωνυμικού μεγέθους, σταθερού βάθους, $\mathcal{O}(1)$,
και μη φραγμένου «*fan-in*».

AC: Alternating Class

«Big-Oh» Συμβολισμός

«Big-Oh» Συμβολισμός:

- $f = \mathcal{O}(g)$ αν τελικά $f(n) \leq cg(n)$ για κάποια σταθερά c.

«Big-Oh» Συμβολισμός:

- $f = \mathcal{O}(g)$ αν τελικά $f(n) \leq cg(n)$ για κάποια σταθερά c.
- $f = \Omega(g)$ όταν $g = \mathcal{O}(f)$.

Μπορούν τα λογικά κυκλώματα μικρής πολυπλοκότητας να εκφράσουν συναρτήσεις ισοτιμίας;

Η Βασική Πιθανοθεωρητική Μέθοδος

Η Βασική Πιθανοθεωρητική Μέθοδος:

1. Ορισμός τυχαίου πειράματος.

Η Βασική Πιθανοθεωρητική Μέθοδος:

1. Ορισμός τυχαίου πειράματος.
2. Καθορισμός μέτρων πιθανοτήτων.

Η Βασική Πιθανοθεωρητική Μέθοδος:

1. Ορισμός τυχαίου πειράματος.
2. Καθορισμός μέτρων πιθανοτήτων.
3. Εκτίμηση πιθανοτήτων ενδεχομένων.

Η Βασική Πιθανοθεωρητική Μέθοδος:

1. Ορισμός τυχαίου πειράματος.
2. Καθορισμός μέτρων πιθανοτήτων.
3. Εκτίμηση πιθανοτήτων ενδεχομένων.

$\Rightarrow$ Αν ένα αντικείμενο έχει θετική πιθανότητα, τότε υπάρχει.

Άλλες Τεχνικές

Άλλες Τεχνικές:

- Γραμμικότητα της Μέσης Τιμής

Άλλες Τεχνικές:

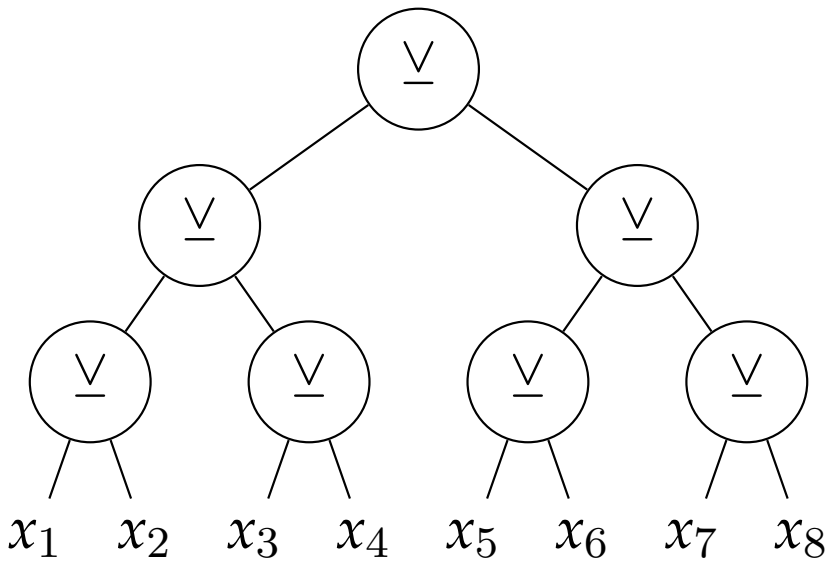
- Γραμμικότητα της Μέσης Τιμής
- Μέθοδος Δεύτερης Ροπής

Άλλες Τεχνικές:

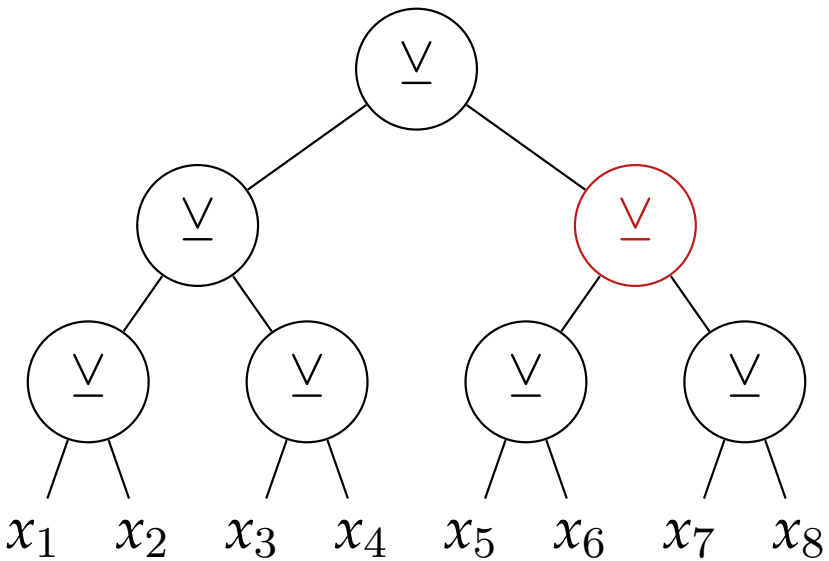
- Γραμμικότητα της Μέσης Τιμής
- Μέθοδος Δεύτερης Ροπής
- Τροποποιήσεις

Μία συνάρτηση ισοτιμίας n μεταβλητών, μπορεί να υπολογιστεί από κυκλώματα πολυωνυμικού μεγέθους και βάθους $\mathcal{O}(\log n)$.

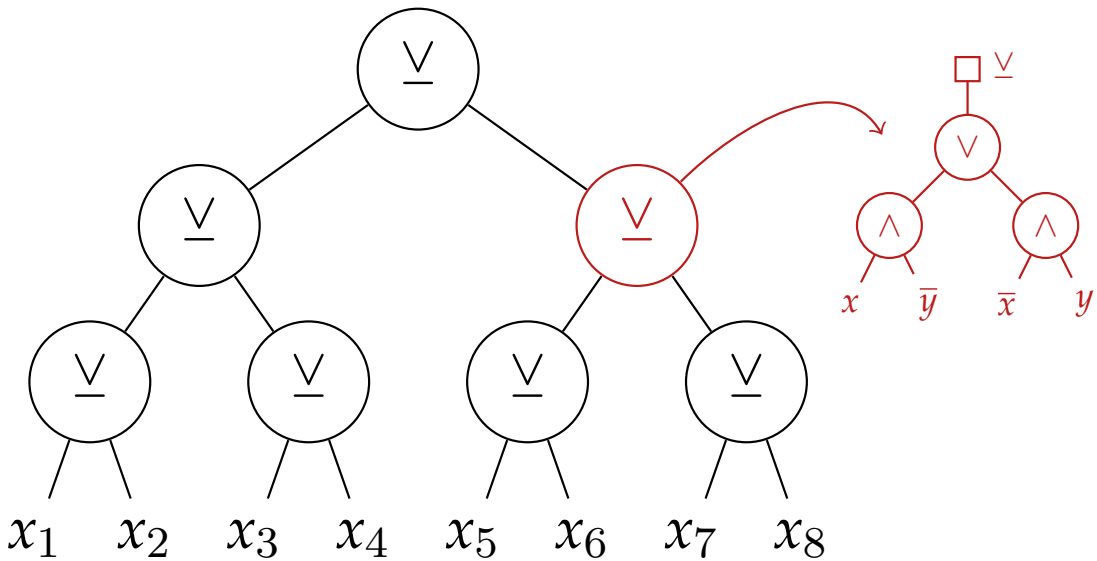
Parity: ποια κυκλώματα μπορούν να την υπολογίσουν



Parity: ποια κυκλώματα μπορούν να την υπολογίσουν



Parity: ποια κυκλώματα μπορούν να την υπολογίσουν



Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Αρκεί να το δείξουνμε για σταθερό «*fan-in*»

Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Αρκεί να το δείξουνμε για σταθερό «*fan-in*»:

- Αν ισχύει, έστω $\pi_n \in AC^0$.

Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Αρκεί να το δείξουνμε για σταθερό «*fan-in*»:

- Αν ισχύει, έστω $\pi_n \in AC^0$.
- Τότε υπάρχει κύκλωμα σταθερού βάθους, t, που υπολογίζει την π_n.

Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Αρκεί να το δείξουνμε για σταθερό «*fan-in*»:

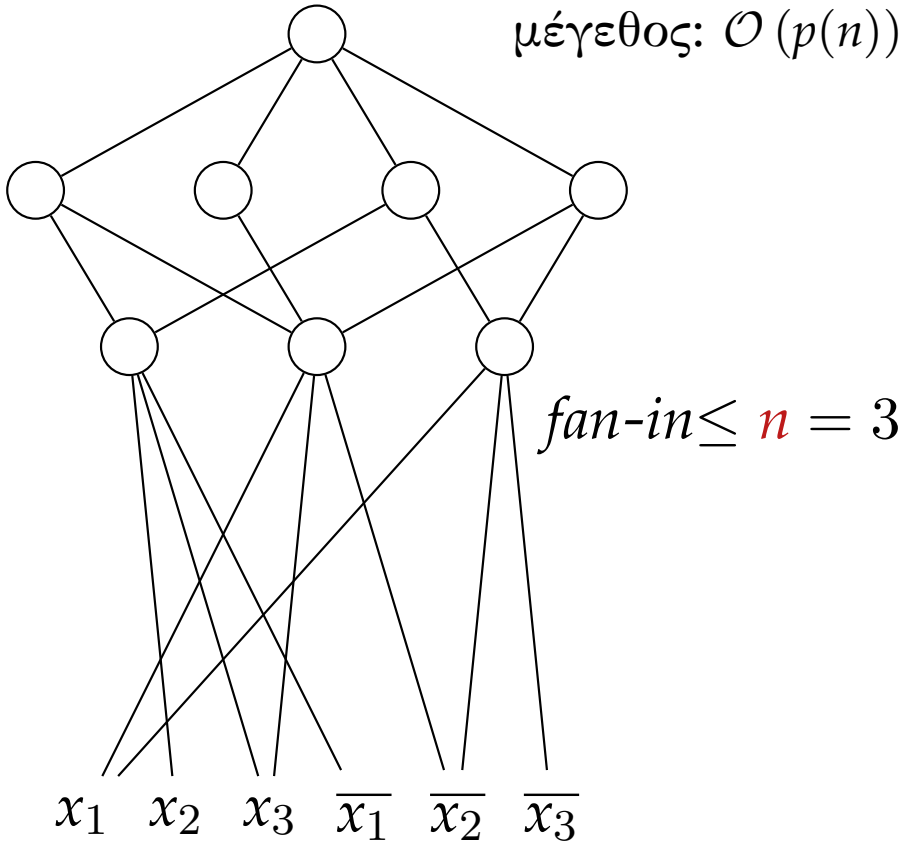
- Αν ισχύει, έστω $\pi_n \in AC^0$.
- Τότε υπάρχει κύκλωμα σταθερού βάθους, t, που υπολογίζει την π_n.
- Προσθέτουμε καταχρηστικά πύλες κάτω από το 1ο επίπεδο με «*fan-in*» 1.

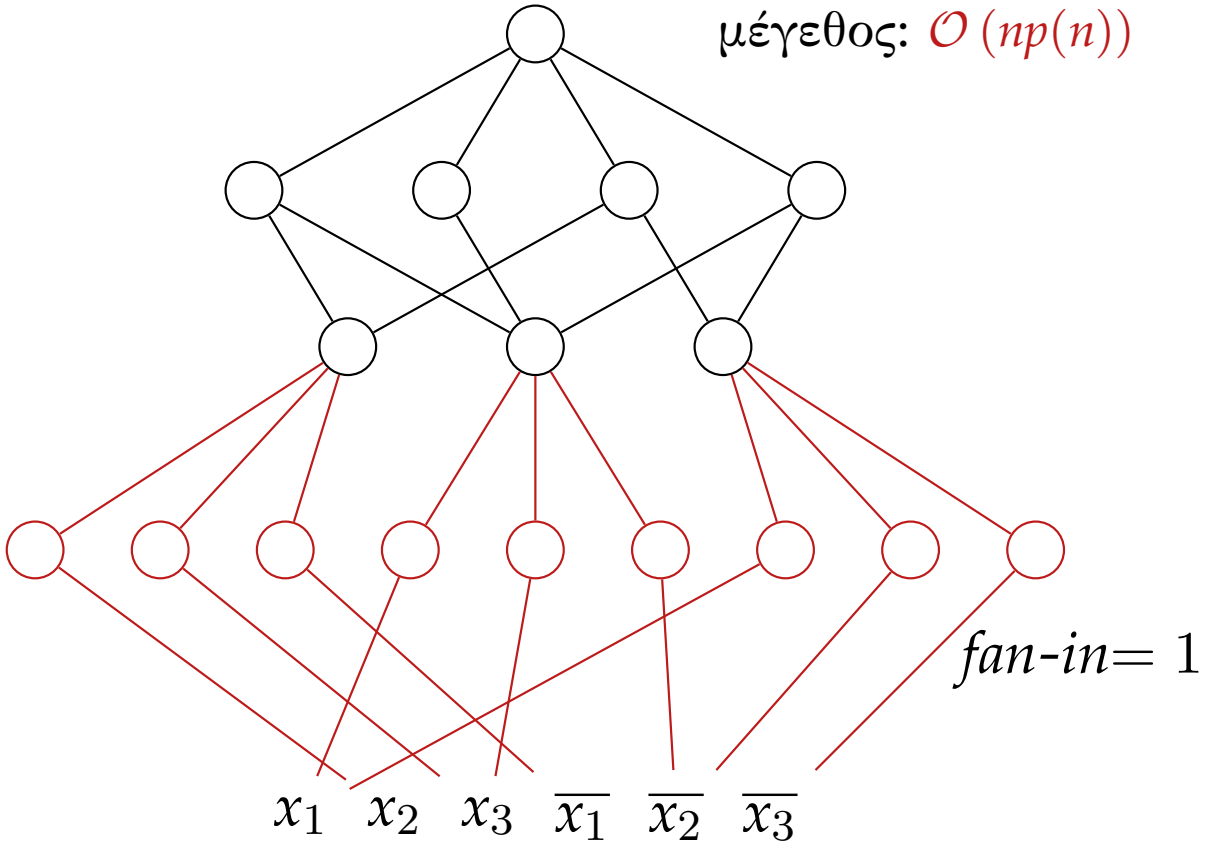
Merrick Furst, James Saxe, Michael Sipser, 1984
Miklós Ajtai, 1983:

Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, συνάρτηση ισοτιμίας.
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Αρκεί να το δείξουνμε για σταθερό «*fan-in*»:

- Αν ισχύει, έστω $\pi_n \in AC^0$.
- Τότε υπάρχει κύκλωμα σταθερού βάθους, t, που υπολογίζει την π_n.
- Προσθέτουμε καταχρηστικά πύλες κάτω από το 1ο επίπεδο με «*fan-in*» 1.
- Άτοπο· άρα $\pi_n \notin AC^0$.


μέγεθος: $\mathcal{O}(p(n))$
$fan\text{-}in \leq n = 3$
x_1 x_2 x_3 $\overline{x_1}$ $\overline{x_2}$ $\overline{x_3}$


μέγεθος: $\mathcal{O}\left(np(n)\right)$
$fan\text{-}in = 1$
x_1 x_2 x_3 $\overline{x_1}$ $\overline{x_2}$ $\overline{x_3}$

Ισχυρισμός 1.
Για οποιαδήποτε $t, c \in \mathbb{N}$ και για οποιοδήποτε πολυώνυμο p, καμία συνάρτηση ισοτιμίας n μεταβλητών δεν μπορεί να υπολογιστεί από κύκλωμα με φράγμα εισόδου c, βάθος t και μέγεθος $p(n)$.

Ισχυρισμός 1.
Για οποιαδήποτε $t, c \in \mathbb{N}$ και για οποιοδήποτε πολυώνυμο p, καμία συνάρτηση ισοτιμίας n μεταβλητών δεν μπορεί να υπολογιστεί από κύκλωμα με φράγμα εισόδου c, βάθος t και μέγεθος $p(n)$.

- Απόδειξη: επαγωγή ως προς το βάθος του κυκλώματος.

Η βάση της επαγωγής για βάθος, $t = 2$ (*Oleg Lupanov, 1961*):

Οι συναρτήσεις ισοτιμίας δεν μπορούν να υπολογιστούν από κύκλωματα πολυωνυμικού μεγέθους, βάθους 2.

Η βάση της επαγωγής για βάθος, $t = 2$ (*Oleg Lupanov, 1961*):

Οι συναρτήσεις ισοτιμίας δεν μπορούν να υπολογιστούν από κύκλωματα πολυωνυμικού μεγέθους, βάθους 2.

- Κάθε πύλη *AND* του πρώτου επιπέδου έχει αναγκαστικά n εισόδους.

Η βάση της επαγωγής για βάθος, $t = 2$ (*Oleg Lupanov, 1961*):

Οι συναρτήσεις ισοτιμίας δεν μπορούν να υπολογιστούν από κύκλωματα πολυωνυμικού μεγέθους, βάθους 2.

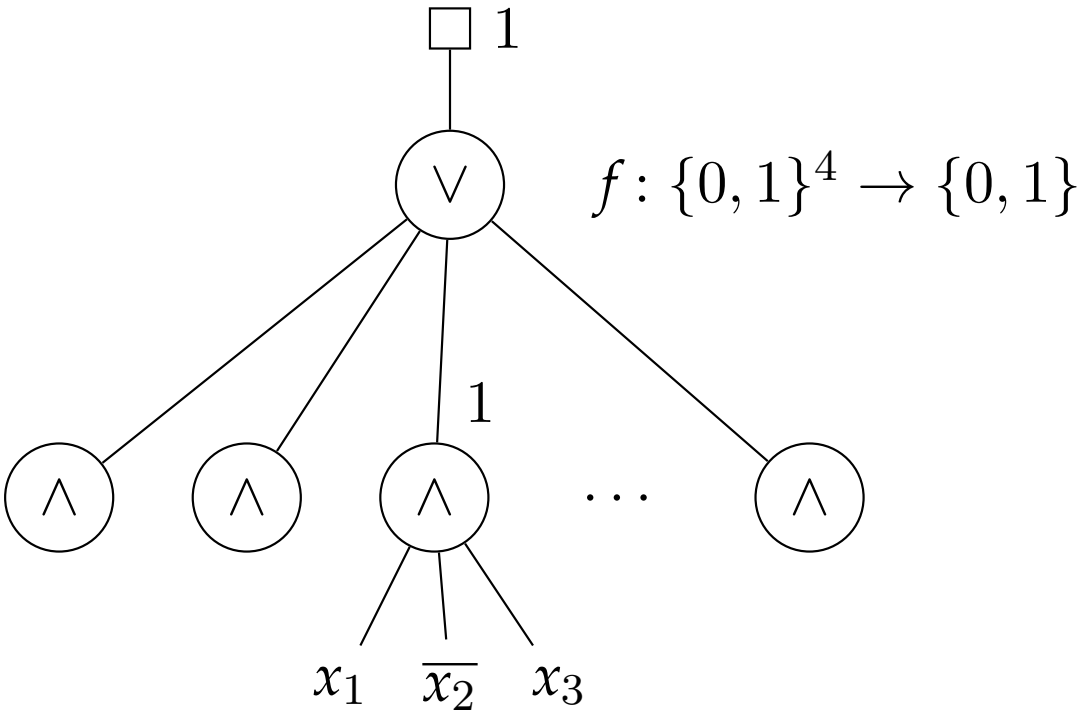
- Κάθε πύλη *AND* του πρώτου επιπέδου έχει αναγκαστικά n εισόδους.
- Κάθε πύλη *AND* του πρώτου επιπέδου αντιστοιχεί σε ένα διάνυσμα για το οποίο η συνάρτηση ισοτιμίας έχει τιμή 1.

Η βάση της επαγωγής για βάθος, $t = 2$ (*Oleg Lupanov, 1961*):

Οι συναρτήσεις ισοτιμίας δεν μπορούν να υπολογιστούν από κύκλωματα πολυωνυμικού μεγέθους, βάθους 2.

- Κάθε πύλη *AND* του πρώτου επιπέδου έχει αναγκαστικά n εισόδους.
- Κάθε πύλη *AND* του πρώτου επιπέδου αντιστοιχεί σε ένα διάνυσμα για το οποίο η συνάρτηση ισοτιμίας έχει τιμή 1.

$\Rightarrow$ Μέγεθος κυκλώματος, τουλάχιστον 2^{n-1}.



$$f(1,0,1,\cdot) \equiv 1 \Rightarrow f \not\equiv \pi_4.$$

x_1	x_2	x_3	x_4	π_4
0	0	0	0	0
0	0	1	0	1
⋮	⋮	⋮	⋮	⋮
1	**0**	**1**	**0**	**0**
⋮	⋮	⋮	⋮	⋮
1	**0**	**1**	**1**	**1**
⋮	⋮	⋮	⋮	⋮
1	1	1	1	0

Βασική Ιδέα:

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.
- Δεν ξέρουμε καν αν υπάρχει κάποιο.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.
- Δεν ξέρουμε καν αν υπάρχει κάποιο.

Αλλά:

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.
- Δεν ξέρουμε καν αν υπάρχει κάποιο.

Αλλά:

- Δε μας ενδιαφέρει να τον βρούμε, ρητά.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.
- Δεν ξέρουμε καν αν υπάρχει κάποιο.

Αλλά:

- Δε μας ενδιαφέρει να τον βρούμε, ρητά.
- Αρκεί να δείξουμε ότι υπάρχει.

Βασική Ιδέα:

- Να δεχθούμε ότι οι π_n υπολογίζονται από κυκλώματα κάποιου ελάχιστου βάθους.
- Να τα μετασχηματίσουμε κατάλληλα ώστε να έχουν βάθος μικρότερο του ελάχιστου

$\Rightarrow$ Άτοπο.

Όμως:

- Πώς θα βρούμε τα κατάλληλα νέα κυκλώματα;
- Δεν έχουμε κάποιον καλό τρόπο.
- Δεν ξέρουμε καν αν υπάρχει κάποιο.

Αλλά:

- Δε μας ενδιαφέρει να τον βρούμε, ρητά.
- Αρκεί να δείξουμε ότι υπάρχει.

$\Rightarrow$ Πιθανοθεωρητική Μέθοδος.

- Έστω ότι υπάρχει ένα ελάχιστο $t > 2$, ώστε η π_n να υπολογίζεται από κύκλωμα βάθους t.

- Έστω ότι υπάρχει ένα ελάχιστο $t > 2$, ώστε η π_n να υπολογίζεται από κύκλωμα βάθους t.
- Έστω ακολουθία, $\{S_n\}_{n\in\mathbb{N}}$, κυκλωμάτων βάθους t.

- Έστω ότι υπάρχει ένα ελάχιστο $t > 2$, ώστε η π_n να υπολογίζεται από κύκλωμα βάθους t.
- Έστω ακολουθία, $\{S_n\}_{n\in\mathbb{N}}$, κυκλωμάτων βάθους t.
- Εφαρμόζουμε την πιθανοθεωρητική μέθοδο των τροποποιήσεων, ώστε να προκύψει η ύπαρξη ακολουθίας κυκλωμάτων $\{S'_n\}_{n\in\mathbb{N}}$ βάθους $t-1$ η οποία να μπορεί να υπολογίσει συνάρτηση ισοτιμίας.

- Έστω ότι υπάρχει ένα ελάχιστο $t > 2$, ώστε η π_n να υπολογίζεται από κύκλωμα βάθους t.
- Έστω ακολουθία, $\{S_n\}_{n\in\mathbb{N}}$, κυκλωμάτων βάθους t.
- Εφαρμόζουμε την πιθανοθεωρητική μέθοδο των τροποποιήσεων, ώστε να προκύψει η ύπαρξη ακολουθίας κυκλωμάτων $\{S'_n\}_{n\in\mathbb{N}}$ βάθους $t-1$ η οποία να μπορεί να υπολογίσει συνάρτηση ισοτιμίας.

$\Rightarrow$ Άτοπο· άρα η π_n δεν υπολογίζεται από κυκλώματα σταθερού βάθους.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

3. Συγχόνευση επιπέδων 2 και 3

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

3. Συγχόνευση επιπέδων 2 και 3

$\Rightarrow$ Νέο κύκλωμα βάθους $t-1$.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

3. Συγχόνευση επιπέδων 2 και 3

$\Rightarrow$ Νέο κύκλωμα βάθους $t-1$.

- Αρκεί να **υπάρχει** τέτοιο κύκλωμα που να υπολογίζει συνάρτηση ισοτιμίας.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

3. Συγχόνευση επιπέδων 2 και 3

$\Rightarrow$ Νέο κύκλωμα βάθους $t-1$.

   - Αρκεί να **υπάρχει** τέτοιο κύκλωμα που να υπολογίζει συνάρτηση ισοτιμίας.

Τυχαίος περιορισμός: η συνάρτηση που προκύπτει αν σταθεροποιήσουμε τυχαία επιλεγμένες μεταβλητές σε τυχαία επιλεγμένες τιμές.

1. Εφαρμογή τροποποίησης: Τυχαίοι Περιορισμοί.
   - Bella Subbotovskaya, 1961.
2. «Αντιστροφή» επιπέδων 1 και 2.

$\Rightarrow$ Επίπεδα 2 και 3: ίδιου τύπου πύλες.

3. Συγχόνευση επιπέδων 2 και 3

$\Rightarrow$ Νέο κύκλωμα βάθους $t-1$.

   - Αρκεί να **υπάρχει** τέτοιο κύκλωμα που να υπολογίζει συνάρτηση ισοτιμίας.

Τυχαίος περιορισμός: *η συνάρτηση που προκύπτει αν σταθεροποιήσουμε τυχαία επιλεγμένες μεταβλητές σε τυχαία επιλεγμένες τιμές.*

Κλειδί: η κατάλληλη επιλογή «τυχαιότητας».

Ερώτημα:

Ερώτημα:

- Μετά τον τυχαίο περιορισμό, το νέο κύκλωμα τι είδους συνάρτηση εκφράζει;

Ερώτημα:

- Μετά τον τυχαίο περιορισμό, το νέο κύκλωμα τι είδους συνάρτηση εκφράζει;

Απάντηση:

Ερώτημα:

- Μετά τον τυχαίο περιορισμό, το νέο κύκλωμα τι είδους συνάρτηση εκφράζει;

Απάντηση:

- Συνάρτηση ισοτιμίας ή το συμπλήρωμά της.

Ερώτημα:

- Μετά τον τυχαίο περιορισμό, το νέο κύκλωμα τι είδους συνάρτηση εκφράζει;

Απάντηση:

- Συνάρτηση ισοτιμίας ή το συμπλήρωμά της.

Γιατί:

Ερώτημα:

- Μετά τον τυχαίο περιορισμό, το νέο κύκλωμα τι είδους συνάρτηση εκφράζει;

Απάντηση:

- Συνάρτηση ισοτιμίας ή το συμπλήρωμά της.

Γιατί:

$$\pi_n(0, x_2, \ldots, x_n) = \pi_{n-1}(x_2, \ldots, x_n)$$
$$\pi_n(1, x_2, \ldots, x_n) = \overline{\pi_{n-1}}(x_2, \ldots, x_n)$$

Παρατήρηση: Ένα κύκλωμα που υπολογίζει την $\overline{\pi_n}$ έχει ακριβώς τα ίδια δομικά χαρακτηριστικά με αυτό που υπολογίζει την π_n.

Αυτό γιατί:

Αυτό γιατί:

$$\pi_n : \mathbb{F}_2^n \to \mathbb{F}_2, \pi_n = \sum_{i=1}^{n} x_i$$

Αυτό γιατί:

$$\pi_n : \mathbb{F}_2^n \to \mathbb{F}_2, \pi_n = \sum_{i=1}^{n} x_i,$$

$$\overline{\pi_n}\left(x_1, \ldots, x_n\right)$$

Αυτό γιατί:

$$\pi_n : \mathbb{F}_2^n \to \mathbb{F}_2, \pi_n = \sum_{i=1}^{n} x_i,$$

$$\overline{\pi_n}\left(x_1, \ldots, x_n\right) = \left(1 + \sum_{i=1}^{n} x_i\right)$$

Αυτό γιατί:

$$\pi_n : \mathbb{F}_2^n \to \mathbb{F}_2, \pi_n = \sum_{i=1}^{n} x_i,$$

$$\overline{\pi_n}\left(x_1, \ldots, x_n\right) = \left(1 + \sum_{i=1}^{n} x_i\right) = \left(1 + x_k + \sum_{\substack{i=1 \\ i \neq k}}^{n} x_i\right)$$

Αυτό γιατί:

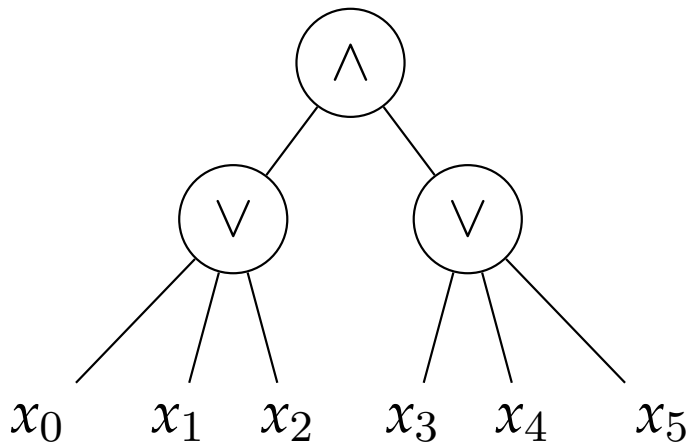
$$\pi_n : \mathbb{F}_2^n \to \mathbb{F}_2, \pi_n = \sum_{i=1}^{n} x_i,$$

$$\overline{\pi_n}\left(x_1, \ldots, x_n\right) = \left(1 + \sum_{i=1}^{n} x_i\right) = \left(1 + x_k + \sum_{\substack{i=1 \\ i \neq k}}^{n} x_i\right) =$$

$$\left(\overline{x_k} + \sum_{\substack{i=1 \\ i \neq k}}^{n} x_i\right) = \pi_n\left(x_1, \ldots, \overline{x_k}, \ldots, x_n\right)$$

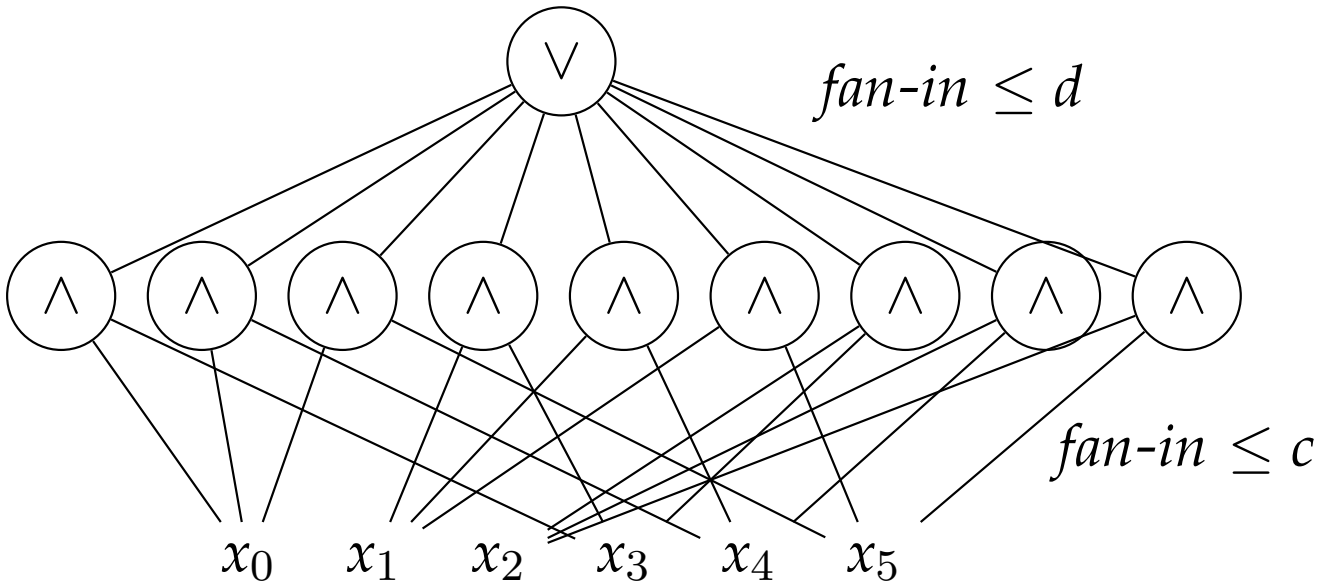
Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.



$$(x_0 + x_1 + x_2) \cdot (x_3 + x_4 + x_5)$$

Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.



$$x_0x_3 + x_0x_4 + x_0x_5 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5$$

Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

$$\overbrace{\left(\sum \dots\right) \times \underbrace{\left(\sum \dots\right)}_{c \text{ όροι στο επίπεδο } 1} \times \cdots \times \left(\sum \dots\right)}^{d \text{ παράγοντες στο επίπεδο } 2}$$

Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

$$\overbrace{\left(\sum \dots\right) \times \underbrace{\left(\sum \dots\right)}_{c \text{ όροι στο επίπεδο } 1} \times \cdots \times \left(\sum \dots\right)}^{d \text{ παράγοντες στο επίπεδο } 2}$$

- Μέγεθος: c^d

Παρατήρηση: Η αντιστροφή διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

$$\overbrace{\left(\sum \dots\right) \times \underbrace{\left(\sum \dots\right)}_{c \text{ όροι στο επίπεδο } 1} \times \cdots \times \left(\sum \dots\right)}^{d \text{ παράγοντες στο επίπεδο } 2}$$

- Μέγεθος: c^d

$\Rightarrow$ Θέλουμε το d να μην εξαρτάται από το n.

Απαιτήσεις από τον τυχαίο περιορισμό:

Απαιτήσεις από τον τυχαίο περιορισμό:

(1) Η αντιστροφή των επιπέδων 1 και 2 να μην αυξάνει εκθετικά το μέγεθος.

Απαιτήσεις από τον τυχαίο περιορισμό:

(1) Η αντιστροφή των επιπέδων 1 και 2 να μην αυξάνει εκθετικά το μέγεθος.

(2) Η μείωση των μεταβλητών να μην καθιστά το μέγεθος εκθετικό ως προς n.

Απαιτήσεις από τον τυχαίο περιορισμό:

(1) Η αντιστροφή των επιπέδων 1 και 2 να μην αυξάνει εκθετικά το μέγεθος.

(2) Η μείωση των μεταβλητών να μην καθιστά το μέγεθος εκθετικό ως προς n.

(3) Η ακολουθία των περιορισμένων κυκλωμάτων να είναι πλήρης, χωρίς κενά.

Συμβολίζουμε:

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.
- $x_i^r \in \{0, 1, x_i\}$ το αποτέλεσμα της δράσης του r στη x_i.

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.
- $x_i^r \in \{0, 1, x_i\}$ το αποτέλεσμα της δράσης του r στη x_i.
- S^r το κύκλωμα από τον περιορισμό του κυκλώματος S.

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.
- $x_i^r \in \{0, 1, x_i\}$ το αποτέλεσμα της δράσης του r στη x_i.
- S^r το κύκλωμα από τον περιορισμό του κυκλώματος S.

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.
- $x_i^r \in \{0, 1, x_i\}$ το αποτέλεσμα της δράσης του r στη x_i.
- S^r το κύκλωμα από τον περιορισμό του κυκλώματος S.

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

- $\mathbb{P}\left[x_i^r = x_i\right] = \frac{1}{\sqrt{n}}$

Συμβολίζουμε:

- r έναν τυχαίο περιορισμό.
- $x_i^r \in \{0, 1, x_i\}$ το αποτέλεσμα της δράσης του r στη x_i.
- S^r το κύκλωμα από τον περιορισμό του κυκλώματος S.

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

- $\mathbb{P}\left[x_i^r = x_i\right] = \frac{1}{\sqrt{n}}$
- $\mathbb{P}\left[x_i^r = 1\right] = \mathbb{P}\left[x_i^r = 0\right] = \frac{1-1/\sqrt{n}}{2}$

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

- $\mathbb{P}\left[x_i^r = x_i\right] = \frac{1}{\sqrt{n}}$
- $\mathbb{P}\left[x_i^r = 1\right] = \mathbb{P}\left[x_i^r = 0\right] = \frac{1-1/\sqrt{n}}{2}$

Αν $X :=$ *#μεταβλητών στο* S^r, τότε:

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

- $\mathbb{P}\left[x_i^r = x_i\right] = \frac{1}{\sqrt{n}}$
- $\mathbb{P}\left[x_i^r = 1\right] = \mathbb{P}\left[x_i^r = 0\right] = \frac{1-1/\sqrt{n}}{2}$

Αν $X :=$ *#μεταβλητών στο* S^r, τότε:

- $\mathbb{E}\left[X\right] = n \cdot \frac{1}{\sqrt{n}} = \sqrt{n}$

Για κάθε μεταβλητή εισόδου, x_i, ενός κυκλώματος ορίζουμε:

- $\mathbb{P}\left[x_i^r = x_i\right] = \frac{1}{\sqrt{n}}$
- $\mathbb{P}\left[x_i^r = 1\right] = \mathbb{P}\left[x_i^r = 0\right] = \frac{1-1/\sqrt{n}}{2}$

Αν $X :=$ *#μεταβλητών στο* S^r, τότε:

- $\mathbb{E}\left[X\right] = n \cdot \frac{1}{\sqrt{n}} = \sqrt{n}$
- $\mathrm{Var}\left[X\right] = n \cdot \frac{1}{\sqrt{n}} \cdot \left(1 - \frac{1}{\sqrt{n}}\right) = \sqrt{n} - 1$

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.
- Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n μεταβλητές.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.
- Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n μεταβλητές.

  $\Rightarrow$ $\exists S^r_m$ με $n \leq m \leq 4n^2$.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.
- Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n μεταβλητές.
  - $\Rightarrow \exists S^r_m$ με $n \leq m \leq 4n^2$.
- Το μέγεθος του S^r_m είναι πολυωνυμικό, αφού το m είναι το πολύ πολυωνυμικά μικρότερο του $4n^2$.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.
- Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n μεταβλητές.
  - $\Rightarrow \exists S^r_m$ με $n \leq m \leq 4n^2$.
- Το μέγεθος του S^r_m είναι πολυωνυμικό, αφού το m είναι το πολύ πολυωνυμικά μικρότερο του $4n^2$.
- Σταθεροποιούμε επιπλέον $m - n$ μεταβλητές στο S^r_m.

Απαίτηση (3): Μετά την εφαρμογή του τυχαίου περιορισμού, για κάθε $n \in \mathbb{N}$ υπάρχει περιορισμένο κύκλωμα S'_n.

- Έστω S_{4n^2} και n σταθεροποιημένο.
- Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n μεταβλητές.
  $\Rightarrow$ $\exists S^r_m$ με $n \leq m \leq 4n^2$.
- Το μέγεθος του S^r_m είναι πολυωνυμικό, αφού το m είναι το πολύ πολυωνυμικά μικρότερο του $4n^2$.
- Σταθεροποιούμε επιπλέον $m - n$ μεταβλητές στο S^r_m.

$\Rightarrow$ Για κάθε κύκλωμα S_{4n^2} υπάρχει S'_n. Άρα η ακολουθία των περιορισμένων κυκλωμάτων είναι πλήρης.

Απαίτηση (2):

Μετά την εφαρμογή του τυχαίου περιορισμού στο S_n να υπάρχει κύκλωμα που να έχει το πολύ πολυωνυμικά λιγότερες μεταβλητές από το αρχικό.

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[|X - \mathbb{E}[X]| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{\mathrm{Var}[X]}{\left(\sqrt{n}/2\right)^2}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[|X - \mathbb{E}[X]| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{\sqrt{n}-1}{\left(\sqrt{n}/2\right)^2}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[|X - \mathbb{E}[X]| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{\sqrt{n}}{\left(\sqrt{n}/2\right)^2}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[|X - \mathbb{E}[X]| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{4}{\sqrt{n}}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[|X - \sqrt{n}| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{4}{\sqrt{n}}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[X \geq \frac{3\sqrt{n}}{2} \text{ ή } X \leq \frac{\sqrt{n}}{2}\right] \leq \frac{4}{\sqrt{n}}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] \leq \frac{4}{\sqrt{n}}$$

Πρόταση: Αν X το πλήθος των μεταβλητών στο S_n^r, τότε

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Chebyshev:

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

Θέλουμε η αντιστροφή (switching) των επιπέδων 1 και 2 να μην οδηγήσει σε κυκλώματα μεγέθους εκθετικής τάξης.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Τότε:

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Τότε:

- Έστω G μια πύλη του δεύτερου επιπέδου.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Τότε:

- Έστω G μια πύλη του δεύτερου επιπέδου.
- Θα δείξουμε ότι το κακό ενδεχόμενο εμφανίζεται στην G με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Τότε:

- Έστω G μια πύλη του δεύτερου επιπέδου.
- Θα δείξουμε ότι το κακό ενδεχόμενο εμφανίζεται στην G με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

$\Rightarrow$ Η πιθανότητα να συμβεί το «κακό» σε *κάποια* πύλη του 2ου επιπέδου είναι $\mathcal{O}\left(\frac{1}{n^k} \cdot n^{k-1}\right) = \mathcal{O}\left(\frac{1}{n}\right)$.

Απαίτηση (1): *ο πυρήνας του προβλήματος.*

- Έστω ότι το μέγεθος του κυκλώματος είναι $\mathcal{O}\left(n^{k-1}\right)$.
- Το ανεπιθύμητο ενδεχόμενο είναι μια πύλη του επιπέδου 2 να εξαρτάται από «πολλές» μεταβλητές.

Τότε:

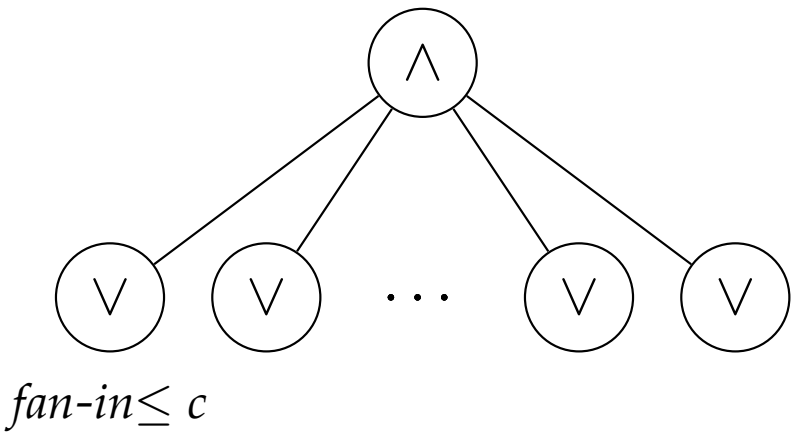
- Έστω G μια πύλη του δεύτερου επιπέδου.
- Θα δείξουμε ότι το κακό ενδεχόμενο εμφανίζεται στην G με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

$\Rightarrow$ Η πιθανότητα να συμβεί το «κακό» σε *κάποια* πύλη του 2ου επιπέδου είναι $\mathcal{O}\left(\frac{1}{n^k} \cdot n^{k-1}\right) = \mathcal{O}\left(\frac{1}{n}\right)$.

$\Rightarrow$ Με μεγάλη πιθανότητα καμιά πύλη στο επίπεδο 2 δεν έχει την κακή ιδιότητα.

Επικεντρωνόμαστε σε ένα υποκύκλωμα *AND-OR* δύο επιπέδων:

Επικεντρωνόμαστε σε ένα υποκύκλωμα *AND-OR* δύο επιπέδων:



Ισχυρισμός 2:

Για κάθε *AND-OR* κύκλωμα με *fan-in*$\leq c$, υπάρχει σταθερά $e = e_c$ ώστε, μετά την εφαρμογή του περιορισμού, η τιμή της πύλης *AND* εξαρτάται από περισσότερες από e_c μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Ισχυρισμός 2:

Για κάθε *AND-OR* κύκλωμα με *fan-in*$\leq c$, υπάρχει σταθερά $e = e_c$ ώστε, μετά την εφαρμογή του περιορισμού, η τιμή της πύλης *AND* εξαρτάται από περισσότερες από e_c μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Απόδειξη:

Ισχυρισμός 2:

Για κάθε *AND-OR* κύκλωμα με *fan-in*$\leq c$, υπάρχει σταθερά $e = e_c$ ώστε, μετά την εφαρμογή του περιορισμού, η τιμή της πύλης *AND* εξαρτάται από περισσότερες από e_c μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Απόδειξη:

- Επαγωγή ως προς c.

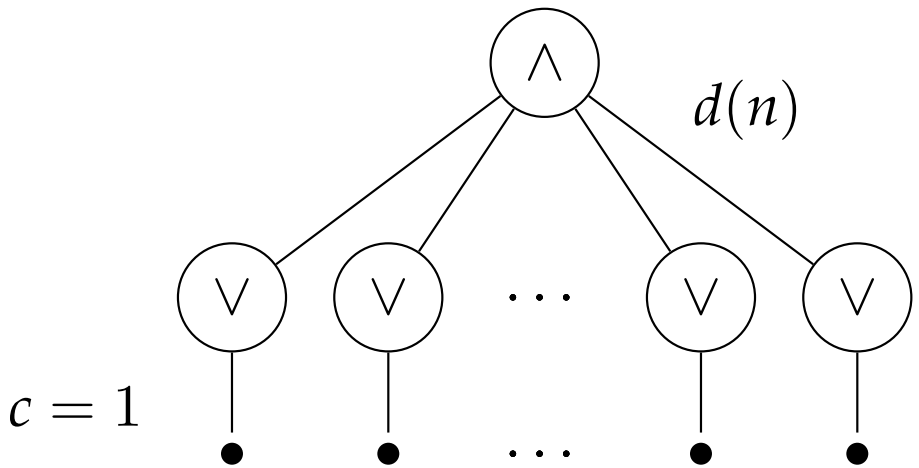
Ισχυρισμός 2:

Για κάθε *AND-OR* κύκλωμα με *fan-in*$\leq c$, υπάρχει σταθερά $e = e_c$ ώστε, μετά την εφαρμογή του περιορισμού, η τιμή της πύλης *AND* εξαρτάται από περισσότερες από e_c μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

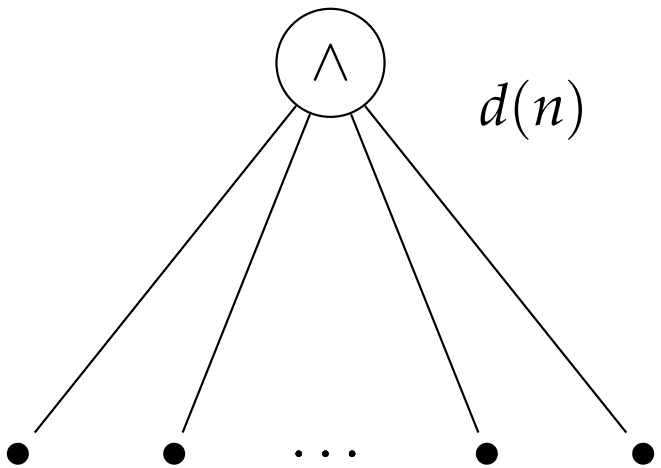
Απόδειξη:

- Επαγωγή ως προς c.
- Διαχωρισμός σε περιπτώσεις «μικρού» και «μεγάλου» φράγματος εισόδου.

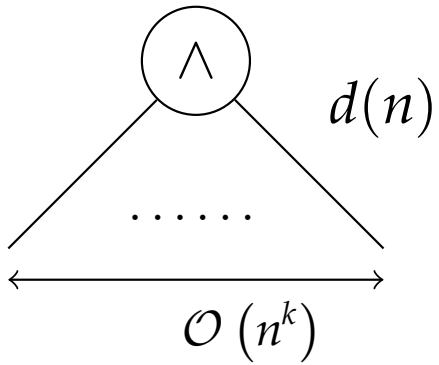
Για $c = 1$ το κύκλωμα εκφυλίζεται σε κύκλωμα μίας πύλης *AND*.



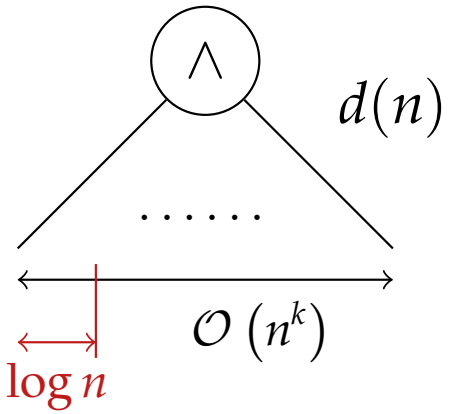
Για $c = 1$ το κύκλωμα εκφυλίζεται σε κύκλωμα μίας πύλης *AND*.

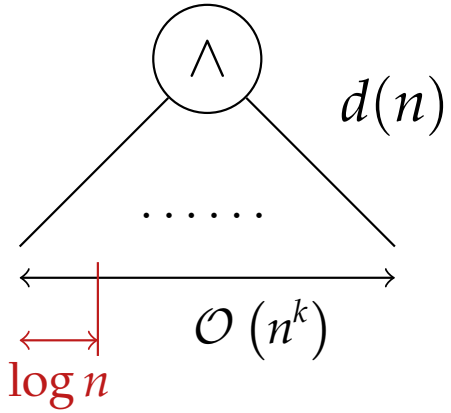


Parity$\notin AC^0$: Ισχυρισμός 2, βάση της επαγωγής.

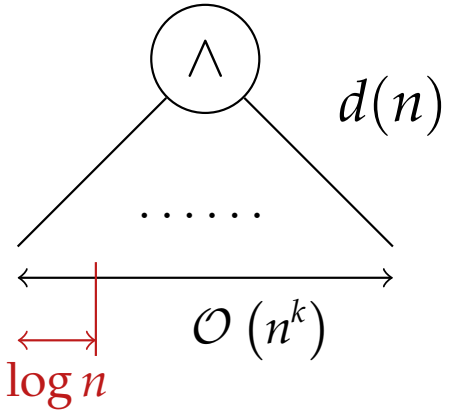


Parity$\notin AC^0$: Ισχυρισμός 2, βάση της επαγωγής.



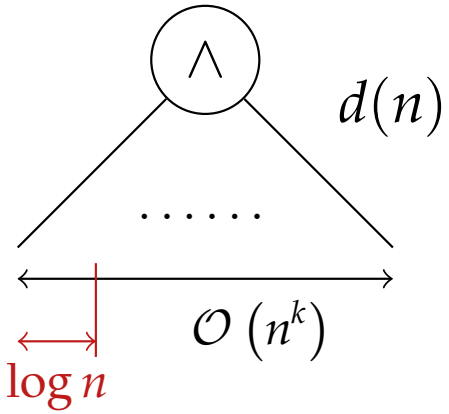


(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.



(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.

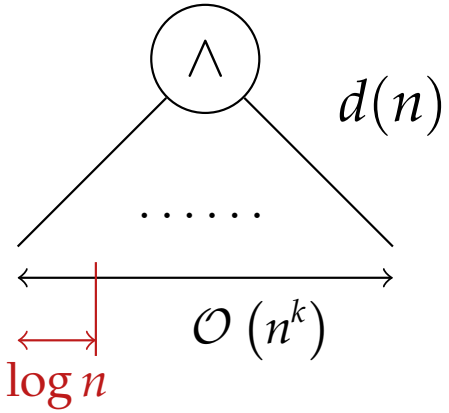
- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθεί στο 0 κάποια είσοδος.



(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθεί στο 0 κάποια είσοδος.

  $\Rightarrow$ πύλη *AND* ανεξάρτητη από μεταβλητές.

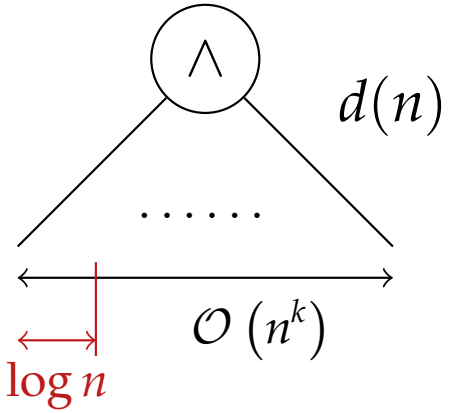


(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθεί στο 0 κάποια είσοδος.

  $\Rightarrow$ πύλη *AND* ανεξάρτητη από μεταβλητές.

(B) Μικρό φράγμα εισόδου: $d(n) \leq 4k \log_2 n$



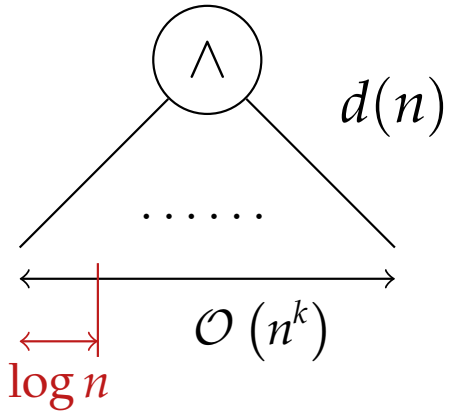
(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθεί στο 0 κάποια είσοδος.

  $\Rightarrow$ πύλη *AND* ανεξάρτητη από μεταβλητές.

(B) Μικρό φράγμα εισόδου: $d(n) \leq 4k \log_2 n$

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθούν όλες οι είσοδοι, πλην ίσως σταθερού πλήθους.



(A) Μεγάλο φράγμα εισόδου: $d(n) \geq 4k \log_2 n$.

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθεί στο 0 κάποια είσοδος.

  $\Rightarrow$ πύλη *AND* ανεξάρτητη από μεταβλητές.

(B) Μικρό φράγμα εισόδου: $d(n) \leq 4k \log_2 n$

- Ελπίζουμε ότι είναι «πολύ πιθανό» να σταθεροποιηθούν όλες οι είσοδοι, πλην ίσως σταθερού πλήθους.

  $\Rightarrow$ πύλη *AND* εξαρτάται το πολύ από σταθερού πλήθους μεταβλητές. (που είναι το ζητούμενο)

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND.
Τότε,

Περίπτωση (A): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND.
Τότε,

$$\mathbb{P}\left[\wedge \not\equiv 0\right] \leq \mathbb{P}\left[e \neq 0, \forall e \in E\right]$$

Περίπτωση (A): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND. Τότε,

$$\mathbb{P}[\wedge \not\equiv 0] \leq \mathbb{P}[e \neq 0, \forall e \in E]$$

$$\mathbb{P}[e \neq 0, \forall e \in E] \leq (1 - \mathbb{P}[e = 0])^{|E|}$$

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND. Τότε,

$$\mathbb{P}[\wedge \not\equiv 0] \leq \mathbb{P}[e \neq 0, \forall e \in E]$$

$$\mathbb{P}[e \neq 0, \forall e \in E] \leq \left(\frac{\sqrt{n}+1}{2\sqrt{n}}\right)^{4k \log_2 n}$$

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND. Τότε,

$$\mathbb{P}[\wedge \not\equiv 0] \leq \mathbb{P}[e \neq 0, \forall e \in E]$$

$$\mathbb{P}[e \neq 0, \forall e \in E] \leq \left(\frac{3}{4}\right)^{4k \log_2 n}$$

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND. Τότε,

$$\mathbb{P}[\wedge \not\equiv 0] \leq \mathbb{P}[e \neq 0, \forall e \in E]$$

$$\mathbb{P}[e \neq 0, \forall e \in E] \leq \frac{1}{n^k}$$

Περίπτωση (Α): Μεγάλο φράγμα εισόδου, $d(n) \geq 4k \log_2 n$.

Έστω $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ οι είσοδοι της πύλης AND. Τότε,

$$\mathbb{P}[\wedge \not\equiv 0] \leq \mathbb{P}[e \neq 0, \forall e \in E]$$

$$\mathbb{P}[e \neq 0, \forall e \in E] \leq \frac{1}{n^k}$$

$$\Rightarrow$$

$$\mathbb{P}[\wedge \not\equiv 0] = \mathcal{O}\left(\frac{1}{n^k}\right)$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

- Παρατήρηση: $\mathbb{E}[X] = \left(4k \log_2 n\right) \frac{1}{\sqrt{n}} \to 0$, καθώς $n \to +\infty$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1]$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] = \sum_{i=e_1}^{d(n)} \binom{d(n)}{i} \left(\frac{1}{\sqrt{n}}\right)^i \left(1 - \frac{1}{\sqrt{n}}\right)^{d(n)-i}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] = \sum_{i=e_1}^{d(n)} \binom{d(n)}{i} \left(\frac{1}{\sqrt{n}}\right)^i \left(1 - \frac{1}{\sqrt{n}}\right)^{d(n)-i}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \sum_{i=e_1}^{d(n)} \binom{d(n)}{i} \left(\frac{1}{\sqrt{n}}\right)^i$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \sum_{i=e_1}^{d(n)} \binom{d(n)}{i} \left(\frac{1}{\sqrt{n}}\right)^{e_1}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \left(\frac{1}{\sqrt{n}}\right)^{e_1} \sum_{i=e_1}^{d(n)} \binom{d(n)}{i}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \left(\frac{1}{\sqrt{n}}\right)^{e_1} \sum_{i=0}^{d(n)} \binom{d(n)}{i}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \left(\frac{1}{\sqrt{n}}\right)^{e_1} 2^{d(n)}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq \left(\frac{1}{\sqrt{n}}\right)^{e_1} 2^{4k \log_2 n}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq n^{4k - \frac{e_1}{2}}$$

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq n^{4k - \frac{e_1}{2}}$$

Για $e_1 = 10k$:

Περίπτωση (Β): Μικρό φράγμα εισόδου, $d(n) \leq 4k \log_2 n$.

Έστω X το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, και $e_1 > 0$ μια σταθερά. Τότε,

$$\mathbb{P}[X \geq e_1] \leq n^{4k - \frac{e_1}{2}}$$

Για $e_1 = 10k$:

$$\mathbb{P}[X \geq 10k = e_1] = \mathcal{O}\left(\frac{1}{n^k}\right)$$

Σε κάθε περίπτωση, όταν $c = 1$, μετά την εφαρμογή του περιορισμού, με μεγάλη πιθανότητα η πύλη AND εξαρτάται από το πολύ σταθερού πλήθους μεταβλητές.

$\Rightarrow$ Ισχυρισμός 2, ισχύει για τη βάση της επαγωγής.

Έστω ότι ισχύει το ζητούμενο για μια σταθερα $e_{c-1} > 0$.

Έστω N το πλήθος των πυλών OR που συνδέονται με την AND και έχουν, ανά δύο, ξένα σύνολα μεταλβητών εισόδου.

Διαχωρίζουμε δύο περιπτώσεις:

(A) $N \geq k2^c \log_2 n$.

(B) $N \leq k2^c \log_2 n$.

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right]$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] = 1 - \mathbb{P}\left[OR \equiv 0 \text{ ή } OR \not\equiv \text{σταθ.}\right]$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \mathbb{P}\left[OR \equiv 0\right]$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \left(\frac{1 - 1/\sqrt{n}}{2}\right)^c$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right]$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$
$$\mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \not\equiv 0\right]$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$

$$\mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \not\equiv 0\right] \leq$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$
$$\mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \not\equiv 0\right] \leq$$
$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^N$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$
$$\mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \not\equiv 0\right] \leq$$
$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$
$$\mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \not\equiv 0\right] \leq$$
$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n} \leq$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.

  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$

$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n} \leq$$

$$\left(1 - \frac{1}{2^c}\right)^{k2^c \log_2 n}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$

$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n} \leq$$

$$n^{k2^c \log_2 \left(1-2^{-c}\right)}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$
$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n} \leq$$
$$n^{k2^c\left(-2^{-c}\right)}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq$$

$$\left(\mathbb{P}\left[\text{μία πύλη } OR \not\equiv 0\right]\right)^{k2^c \log_2 n} \leq$$

$$\frac{1}{n^k}$$

(A) $N \geq k2^c \log_2 n$. /* Χωρίς επαγωγή */

- «Πολύ πιθανό», κάποια πύλη OR να σταθ. στο 0.
  $\Rightarrow$ $AND \equiv 0$.

Έστω μία συγκεκριμένη πύλη OR:

$$\mathbb{P}\left[OR \equiv 1\right] \leq 1 - \frac{1}{2^c}$$

Επομένως,

$$\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] = \mathcal{O}\left(\frac{1}{n^k}\right)$$

(B) $N \leq k2^c \log_2 n$.

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c - 1$.

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c - 1$.

Θεώρημα επέκτασης του Boole:

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c - 1$.

Θεώρημα επέκτασης του Boole:
Αν f λογική συνάρτηση, τότε

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

Θεώρημα επέκτασης του Boole:
Αν f λογική συνάρτηση, τότε

$$f(x) = f(1) \cdot x + f(0) \cdot \overline{x}$$

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

Θεώρημα επέκτασης του Boole:
Αν f λογική συνάρτηση, τότε

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

Θεώρημα επέκτασης του Boole:
Αν f λογική συνάρτηση, τότε

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

όπου, $x^i := \begin{cases} x, \text{ όταν } i=0 \\ \bar{x}, \text{ όταν } i=1 \end{cases}$

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

- Κάθε υποκύκλωμα να περιλαμβάνει όλες τις πύλες *OR* του επιπέδου 1.

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

- Κάθε υποκύκλωμα να περιλαμβάνει όλες τις πύλες OR του επιπέδου 1.
- Θέλουμε όσο γίνεται λιγότερους όρους.

(B) $N \leq k2^c \log_2 n$.

- Ανάλυση σε υποκυκλώματα με *fan-in* $\leq c-1$.

$$f(x_1,\ldots,x_n) = \sum_{i_1=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} \ldots x_k^{i_k} f\left(1^{i_1},\ldots,1^{i_k},x_{k+1},\cdots,x_n\right)$$

- Κάθε υποκύκλωμα να περιλαμβάνει όλες τις πύλες *OR* του επιπέδου 1.
- Θέλουμε όσο γίνεται λιγότερους όρους.
- Μετά τον περιορισμό, η πιθανότητα εξάρτησης της *AND* από μεταβλητές να παραμείνει της τάξεως $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

- Αν όχι, έστω g πύλη χωρίς μεταβλητή στο H.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

- Αν όχι, έστω g πύλη χωρίς μεταβλητή στο H.
- Τότε, $M \cup \{g\}$ πύλες με ανά δύο ξένα σύνολα εισόδων.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

- Αν όχι, έστω g πύλη χωρίς μεταβλητή στο H.
- Τότε, $M \cup \{g\}$ πύλες με ανά δύο ξένα σύνολα εισόδων.
- M μεγιστικό $\Rightarrow$ άτοπο.

Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

- Πλήθος αναθέσεων τιμών στις μεταβλητές του H: $l = 2^{|H|}$.

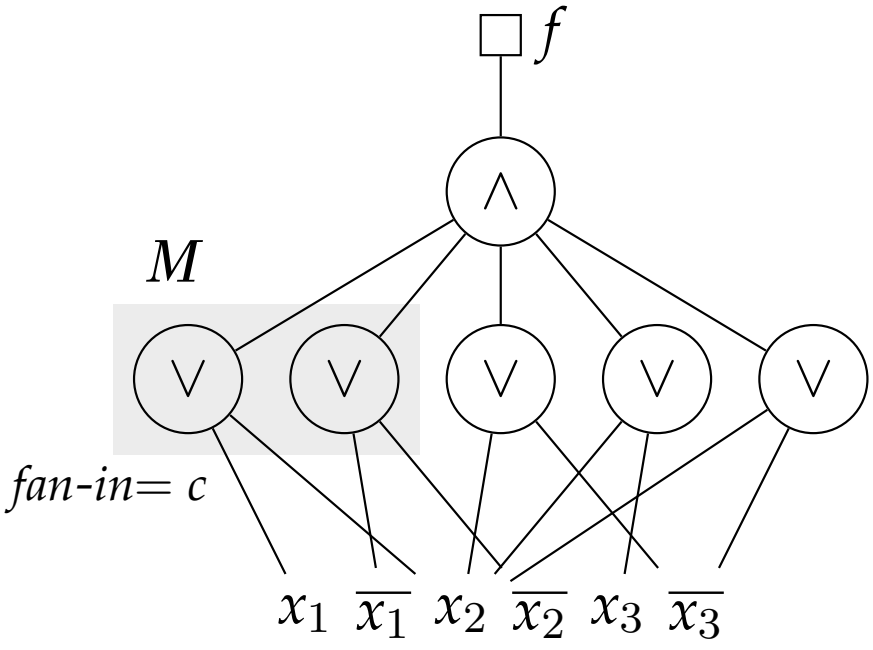
Κατασκευή της ανάλυσης σε υποκυκλώματα:

- Έστω f η λογική συνάρτηση που εκφράζεται από το κύκλωμα που εξετάζουμε.
- Θεωρούμε πύλες OR με ξένα, ανά δύο, σύνολα μεταβλητών εισόδου.
- Έστω M ένα μεγιστικό σύνολο από τέτοιες πύλες.
- Έστω H το σύνολο των μεταβλητών στις εισόδος τους.

(*) Κάθε πύλη OR έχει τουλάχιστον μια μεταβλητή στο H.

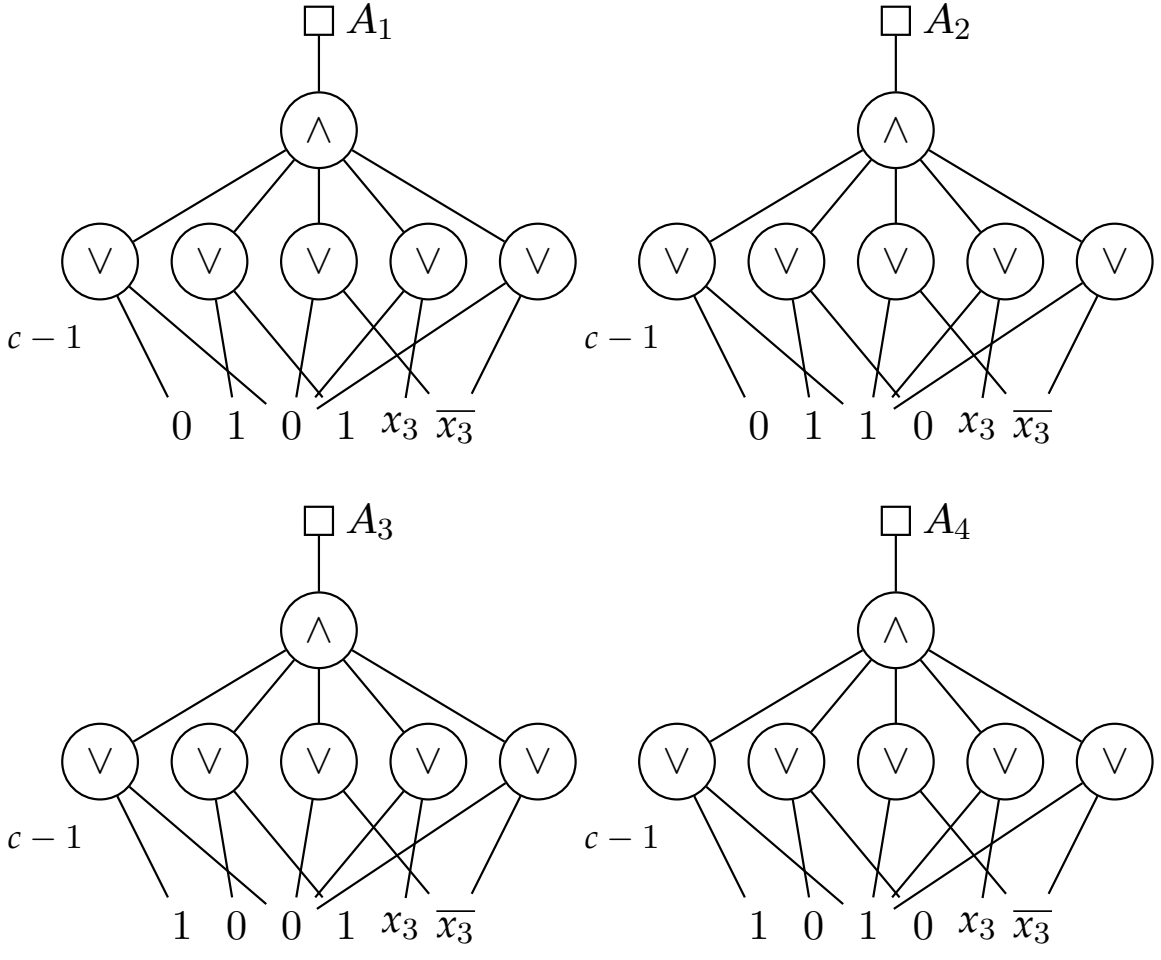
- Πλήθος αναθέσεων τιμών στις μεταβλητές του H: $l = 2^{|H|}$.
- Οι αναθέσεις δημιουργούν υποκυκλώματα $A_1, \ldots, A_l$ με *fan-in* $\leq c - 1$.

Parity$\notin AC^0$: Ισχυρισμός 2, επαγωγικό βήμα, $N \leq k2^c \log_2 n$.



$$H = \{x_1, x_2\}$$

Parity$\notin AC^0$: Ισχυρισμός 2, επαγωγικό βήμα, $N \leq k2^c \log_2 n$.



$$f = (\overline{x_1} \cdot \overline{x_2} \cdot A_1) + (\overline{x_1} \cdot x_2 \cdot A_2) + (x_1 \cdot \overline{x_2} \cdot A_3) + (x_1 \cdot x_2 \cdot A_4)$$

- Έστω

- Έστω
  - r τυχαίος περιορισμός.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.
  - A_i^r οι συνιστώσες της.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.
  - A_i^r οι συνιστώσες της.
  - l^r το πλήθος τους.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.
  - A_i^r οι συνιστώσες της.
  - l^r το πλήθος τους.
- Επαγωγική Υπόθεση: οι πύλες AND στα A_i^r εξαρτώνται από περισσότερες από e_{c-1} μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.
  - A_i^r οι συνιστώσες της.
  - l^r το πλήθος τους.
- Επαγωγική Υπόθεση: οι πύλες AND στα A_i^r εξαρτώνται από περισσότερες από e_{c-1} μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

$\Rightarrow$ Το κύκλωμα, που εκφράζει την f^r, εξαρτάται από περισσότερες από $l^r e_{c-1}$ μεταβλητές με πιθανότητα $l^r\,\mathcal{O}\left(\frac{1}{n^k}\right)$.

- Έστω
  - r τυχαίος περιορισμός.
  - f^r η περιορισμένη συνάρτηση.
  - A_i^r οι συνιστώσες της.
  - l^r το πλήθος τους.
- Επαγωγική Υπόθεση: οι πύλες AND στα A_i^r εξαρτώνται από περισσότερες από e_{c-1} μεταβλητές, με πιθανότητα $\mathcal{O}\left(\frac{1}{n^k}\right)$.

$\Rightarrow$ Το κύκλωμα, που εκφράζει την f^r, εξαρτάται από περισσότερες από $l^r e_{c-1}$ μεταβλητές με πιθανότητα $l^r\,\mathcal{O}\left(\frac{1}{n^k}\right)$.

- Θέλουμε το l^r να είναι ανεξάρτητο του n.

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] = \sum_{i=\alpha}^{|H|} \binom{|H|}{i} \left(\frac{1}{\sqrt{n}}\right)^i \left(1 - \frac{1}{\sqrt{n}}\right)^{|H|-i}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq \sum_{i=\alpha}^{|H|} \binom{|H|}{i} \left(\frac{1}{\sqrt{n}}\right)^i$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq \left(\frac{1}{\sqrt{n}}\right)^{\alpha} \sum_{i=\alpha}^{|H|} \binom{|H|}{i}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών OR: $\leq k2^c \log_2 n$.

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών *OR*: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης *OR*: $\leq c$.

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών *OR*: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης *OR*: $\leq c$.

$\Rightarrow$ $|H| \leq ck2^c \log_2 n$.

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών OR: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης OR: $\leq c$.

$\Rightarrow$ $|H| \leq ck2^c \log_2 n$.

Επομένως,

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών *OR*: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης *OR*: $\leq c$.

$\Rightarrow |H| \leq ck2^c \log_2 n$.

Επομένως,

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{ck2^c \log_2 n}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών OR: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης OR: $\leq c$.

$\Rightarrow$ $|H| \leq ck2^c \log_2 n$.

Επομένως,

$$\mathbb{P}[h > \alpha] \leq n^{-\frac{\alpha}{2} + ck2^c \log_2 n}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

- Πλήθος πυλών OR: $\leq k2^c \log_2 n$.
- *fan-in* κάθε πύλης OR: $\leq c$.

$\Rightarrow |H| \leq ck2^c \log_2 n$.

Για $\alpha = 2(k + ck2^c)$,

$$\mathbb{P}[h > \alpha] \leq \frac{1}{n^k}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

Για $\alpha = 2(k + ck2^c)$,

$$\mathbb{P}[h > \alpha] \leq \frac{1}{n^k}$$

- Έστω h το πλήθος των στοιχείων του H που παρέμειναν μεταβλητές, και $\alpha > 0$ σταθερά.

$$\mathbb{P}[h > \alpha] \leq n^{-\alpha/2} 2^{|H|}$$

Για $\alpha = 2(k + ck2^c)$,

$$\mathbb{P}[h > \alpha] \leq \frac{1}{n^k}$$

$\Rightarrow$ Με μεγάλη πιθανότητα, η συνάρτηση f^r στην ανάλυσή της σε υποκυκλώματα, εκφράζεται από το πολύ $2^h \leq m := 2^{2(k+ck2^c)}$ όρους.

Θέτουμε $e_c := m \cdot e_{c-1}$,

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{H } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right]$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$
$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right]$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$
$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right]$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$
$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right)$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right)$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{H } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right) + m \cdot \mathcal{O}\left(\frac{1}{n^k}\right)$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{H } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right) + m \cdot \mathcal{O}\left(\frac{1}{n^k}\right)$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right) + m \cdot \mathcal{O}\left(\frac{1}{n^k}\right)$$

$$= \mathcal{O}\left(\frac{1}{n^k}\right)$$

Θέτουμε $e_c := m \cdot e_{c-1}$,

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$

$$\mathbb{P}\left[h > 2(k + ck2^c)\right] +$$

$$\mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$

$$\mathcal{O}\left(\frac{1}{n^k}\right) + m \cdot \mathcal{O}\left(\frac{1}{n^k}\right)$$

$$= \mathcal{O}\left(\frac{1}{n^k}\right)$$

- Δείξαμε ότι Parity$\in AC^1$.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.
  - Εφαρμογή κατάλληλου περιορισμού.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.
  - Εφαρμογή κατάλληλου περιορισμού.

(*) «Αντιστροφή» επιπέδων 1 και 2, συγχόνευση επιπέδων 2 και 3.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.
  - Εφαρμογή κατάλληλου περιορισμού.

  (*) «Αντιστροφή» επιπέδων 1 και 2, συγχόνευση επιπέδων 2 και 3.
    - Η «αντιστροφή» εν γένει αυξάνει το μέγεθος εκθετικά, εκτός αν το «fan-in» στο επίπεδο 2 είναι ανεξάρτητο του n.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.
  - Εφαρμογή κατάλληλου περιορισμού.

  (*) «Αντιστροφή» επιπέδων 1 και 2, συγχόνευση επιπέδων 2 και 3.
    - Η «αντιστροφή» εν γένει αυξάνει το μέγεθος εκθετικά, εκτός αν το «fan-in» στο επίπεδο 2 είναι ανεξάρτητο του n.
    - Ισχυρισμός (2): Υπάρχει (μη τυχαίος) περιορισμός, ώστε οι πύλες στο επίπεδο 2 να μην εξαρτώνται από το n.

- Δείξαμε ότι Parity$\in AC^1$.
- Θεώρημα: Parity$\notin AC^0$. Αρκεί για «*fan-in*»$\leq c$.
- Ισχυρισμός (1): Η Parity δεν υπολογίζεται από κύκλωμα πολυωνυμικού μεγέθους, σταθερού βάθους t και «*fan-in*»$\leq c$.
  - Έστω t το ελάχιστο βάθος τέτοιου κυκλώματος, που υπολογίζει την Parity.
  - Εφαρμογή κατάλληλου περιορισμού.

  (*) «Αντιστροφή» επιπέδων 1 και 2, συγχόνευση επιπέδων 2 και 3.
    - Η «αντιστροφή» εν γένει αυξάνει το μέγεθος εκθετικά, εκτός αν το «fan-in» στο επίπεδο 2 είναι ανεξάρτητο του n.
    - Ισχυρισμός (2): Υπάρχει (μη τυχαίος) περιορισμός, ώστε οι πύλες στο επίπεδο 2 να μην εξαρτώνται από το n.

  $\Rightarrow$ Κύκλωμα βάθους $t-1$ που υπολογίζει Parity: άτοπο.

Συμπέρασμα για την οριοθέτηση της πολυπλοκότητας των συναρτήσεων ισοτιμίας:

- Υπολογίζονται από κυκλώματα βάθους $\mathcal{O}(\log n)$.

Συμπέρασμα για την οριοθέτηση της πολυπλοκότητας των συναρτήσεων ισοτιμίας:

- Υπολογίζονται από κυκλώματα βάθους $\mathcal{O}(\log n)$.
- Δεν υπολογίζονται από κυκλώματα βάθους $\mathcal{O}(1)$.

- Βελτίωση κάτω φράγματος με αλγεβρική οπτική.

- Βελτίωση κάτω φράγματος με αλγεβρική οπτική.
- Alexander Razborov, Roman Smolensky

- Βελτίωση κάτω φράγματος με αλγεβρική οπτική.
- Alexander Razborov, Roman Smolensky
- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο μικρής πολυπλοκότητας το οποίο προσεγγίζει την f.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο μικρής πολυπλοκότητας το οποίο προσεγγίζει την f.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο προσεγγίζει την f.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο προσεγγίζει την f.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f σχεδόν για κάθε σημείο του $\{0,1\}^n$.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f σχεδόν για κάθε σημείο του $\{0,1\}^n$.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

(B) Δεν υπάρχει πολυώνυμο μικρής πολυπλοκότητας το οποίο να προσεγγίζει την π_n.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

(B) Δεν υπάρχει πολυώνυμο μικρής πολυπλοκότητας το οποίο να προσεγγίζει την π_n.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

(B) Δεν υπάρχει πολυώνυμο βαθμού το πολύ $\sqrt{n}/2$ το οποίο να προσεγγίζει την π_n.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

(B) Δεν υπάρχει πολυώνυμο βαθμού το πολύ $\sqrt{n}/2$ το οποίο να προσεγγίζει την π_n.

$\Rightarrow$ Οι συναρτήσεις ισοτιμίας δεν ανήκουν στην κλάση AC^0.

- Βασικό θεώρημα: $\forall n \in \mathbb{N}, \pi_n \notin AC^0$.

(A) Για κάθε $f \in AC^0$ και $\epsilon > 0$, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon) \cdot 2^n$ σημεία του $\{0,1\}^n$.

(B) Δεν υπάρχει πολυώνυμο βαθμού το πολύ $\sqrt{n}/2$ το οποίο να προσεγγίζει την π_n.

$\Rightarrow$ Οι συναρτήσεις ισοτιμίας δεν ανήκουν στην κλάση AC^0.

$\rightarrow$ Παράπλευρο αποτέλεσμα: κάθε κύκλωμα που υπολογίζει τη συνάρτηση ισοτιμίας έχει βάθος

$$\Omega\left(\frac{\log n}{\log\log n}\right)$$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Δεν έχουμε καποιον καλό τρόπο να ψάξουμε να βρούμε –**αν υπάρχει!**– ένα πολυώνυμο που να την προσεγγίζει.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Δεν έχουμε καποιον καλό τρόπο να ψάξουμε να βρούμε –**αν υπάρχει!**– ένα πολυώνυμο που να την προσεγγίζει.
  - Δε χρειάζεται να το βρούμε· αρκεί να δείξουμε ότι υπάρχει.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - Θέλουμε να λιγοστέψουμε τους παράγοντες (και άρα τον βαθμό)

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - Θέλουμε να λιγοστέψουμε τους παράγοντες (και άρα τον βαθμό)
    - και να "πιάσουμε" όσα περισσότερα μονώνυμα γίνεται.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - $S_0 := \{1, \ldots, n\}, S_{i+1} \subset S_i, \mathbb{P}[j \in S_{i+1} | j \in S_i] = 1/2$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - $S_0 := \{1, \ldots, n\}, S_{i+1} \subset S_i, \mathbb{P}[j \in S_{i+1} | j \in S_i] = 1/2$
    - $p := \prod_{i=0}^{\mathcal{O}(\log n)} \left(1 - \sum_{j \in S_i} x_j\right)$, $\deg p = \mathcal{O}(\log n)$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - $S_0 := \{1, \ldots, n\}, S_{i+1} \subset S_i, \mathbb{P}[j \in S_{i+1} | j \in S_i] = 1/2$
    - $p := \prod_{i=0}^{\mathcal{O}(\log n)} \left(1 - \sum_{j \in S_i} x_j\right)$, $\deg p = \mathcal{O}(\log n)$
    - $\mathbb{P}[OR \equiv 1 - p] = 1 - \epsilon > 0$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
  - Πιθανοθεωρητική "προσομοίωση":
    - $S_0 := \{1, \ldots, n\}, S_{i+1} \subset S_i, \mathbb{P}[j \in S_{i+1} | j \in S_i] = 1/2$
    - $p := \prod_{i=0}^{\mathcal{O}(\log n)} \left(1 - \sum_{j \in S_i} x_j\right)$, $\deg p = \mathcal{O}(\log n)$
    - $\mathbb{P}[OR \equiv 1 - p] = 1 - \epsilon > 0$
    - Ομοίως για την συνάρτηση *AND*.

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
- Γενικότερα, αν $f \in AC^0$, τότε
  $\mathbb{P}[f \equiv p] = 1 - \epsilon > 0$, $\deg p = \mathcal{O}\left(\log\left(\frac{s}{\epsilon}\right)\log^d(s)\right)$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
- Γενικότερα, αν $f \in AC^0$, τότε
  $\mathbb{P}[f \equiv p] = 1 - \epsilon > 0$, $\deg p = \mathcal{O}\left(\log\left(\frac{s}{\epsilon}\right)\log^d(s)\right)$

$\Rightarrow$ Αν $S_p = \{x : f(x) = p(x)\}$, τότε $\mathbb{E}\left[|S_p|\right] = (1 - \epsilon) \cdot 2^n$

(A) Κάθε $f \in AC^0$ προσεγγίζεται από κάποιο πολυώνυμο πολυλογαριθμικού βαθμού.

Έστω s το (πολυωνυμικό) μέγεθος του κυκλώματος που υπολογίζει την f, d το (σταθερό) βάθος του και $\epsilon > 0$.

- Προσέγγιση της συνάρτησης $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$
- Γενικότερα, αν $f \in AC^0$, τότε
  $\mathbb{P}[f \equiv p] = 1 - \epsilon > 0$, $\deg p = \mathcal{O}\left(\log\left(\frac{s}{\epsilon}\right)\log^d(s)\right)$

$\Rightarrow$ Αν $S_p = \{x : f(x) = p(x)\}$, τότε $\mathbb{E}\left[|S_p|\right] = (1-\epsilon)\cdot 2^n$

$\Rightarrow$ Άρα, υπάρχει πολυώνυμο πολυλογαριθμικού βαθμού το οποίο ταυτίζεται με την f σε τουλάχιστον $(1-\epsilon)\cdot 2^n$ σημεία.

(B) Δεν υπάρχρει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

(B) Δεν υπάρχρει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε:
  $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε:
  $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε:
  $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.
  - $\dim \mathcal{POL} = \sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon) \cdot 2^n$

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε: $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.
  - $\dim \mathcal{POL} = \sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon) \cdot 2^n$
- $L(S) :=< S >$

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε: $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.
  - $\dim \mathcal{POL} = \sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon) \cdot 2^n$
- $L(S) :=< S >$
- $L(S) \hookrightarrow \mathcal{POL}$

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε:
  $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.
  - $\dim \mathcal{POL} = \sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon) \cdot 2^n$
- $L(S) :=< S >$
- $L(S) \hookrightarrow \mathcal{POL}$
- $(1-\epsilon) \cdot 2^n \leq \dim L(S) \leq \dim \mathcal{POL} < (1-\epsilon) \cdot 2^n$

(B) Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ τ.ω. $p \approx \pi_n$

- Έστω $\epsilon > 0$.
- Έστω ότι υπάρχει πολυώνυμο p, ώστε:
  $p(x) = \pi_n(x), \forall x \in S \subset \{0,1\}^n$, όπου $|S| \geq (1-\epsilon) \cdot 2^n$
- $\mathcal{POL} := \left\{ p | \deg p \leq \frac{n+\sqrt{n}}{2} \right\}$.
  - $\dim \mathcal{POL} = \sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon) \cdot 2^n$
- $L(S) :=< S >$
- $L(S) \hookrightarrow \mathcal{POL}$
- $(1-\epsilon) \cdot 2^n \leq \dim L(S) \leq \dim \mathcal{POL} < (1-\epsilon) \cdot 2^n$

$\Rightarrow$ Άτοπο.

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$
  - **P vs NP:**

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$
  - **P vs NP**:
    - P: κλάση προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Μηχανή Turing.

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$
  - **P vs NP**:
    - **P**: κλάση προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
    - **NP**: κλάση προβλημάτων που μια δεδομένη απάντηση μπορεί να επαληθευτεί σε πολυωνυμικό χρόνο από μια Μηχανή Turing.

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$
  - **P vs NP**:
    - **P**: κλάση προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
    - **NP**: κλάση προβλημάτων που μια δεδομένη απάντηση μπορεί να επαληθευτεί σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
  - *Η ανάλυση κυκλωμάτων θεωρείται καλό μονοπάτι για την απάντηση $P \neq NP$.*

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}(T(n))$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}(T(n)\log T(n))$
  - **P vs NP**:
    - **P**: κλάση προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
    - **NP**: κλάση προβλημάτων που μια δεδομένη απάντηση μπορεί να επαληθευτεί σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
  - Η ανάλυση κυκλωμάτων θεωρείται καλό μονοπάτι για την απάντηση $P \neq NP$.
    - Αν βρεθεί μια συνάρτηση $f \in NP$ για την οποία η πολυπλοκότητα του C_f έχει κάτω φράγμα τάξεως μεγαλύτερης της πολυωνυμικής, τότε $P \neq NP$

- Ξεκίνημα Ανάλυσης Κυκλωμάτων: 1949, Shannon με στόχο την ελαχιστοποίηση υλικών στοιχείων σε κυκλώματα.
- Από τη δεκαετία 1960, στενή σχέση με Θεωρία Πολυπλοκότητας:
  - Αν f έχει χρονική πολυπλοκότητα $\mathcal{O}\left(T(n)\right)$, τότε το C_f έχει πολυπλοκότητα (μέγεθος) $\mathcal{O}\left(T(n)\log T(n)\right)$
  - **P vs NP**:
    - **P**: κλάση προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
    - **NP**: κλάση προβλημάτων που μια δεδομένη απάντηση μπορεί να επαληθευτεί σε πολυωνυμικό χρόνο από μια Μηχανή Turing.
  - Η ανάλυση κυκλωμάτων θεωρείται καλό μονοπάτι για την απάντηση $P \neq NP$.
    - Αν βρεθεί μια συνάρτηση $f \in NP$ για την οποία η πολυπλοκότητα του C_f έχει κάτω φράγμα τάξεως μεγαλύτερης της πολυωνυμικής, τότε $P \neq NP$
  - **[1M$]**

- Switching Lemma του Johan Håstad, 1987.

- Switching Lemma του Johan Håstad, 1987.
  - *Έστω A είναι ένα AND-OR κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου fan-in.*

- Switching Lemma του Johan Håstad, 1987.
  - Έστω A είναι ένα *AND-OR* κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου *fan-in*.
  - Εφαρμόζεται τυχαίος περιορισμός πιθανότητας p.

- Switching Lemma του Johan Håstad, 1987.
  - Έστω A είναι ένα *AND-OR* κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου *fan-in*.
  - Εφαρμόζεται τυχαίος περιορισμός πιθανότητας p.
  - Αν A' το περιορισμένο κύκλωμα,

- Switching Lemma του Johan Håstad, 1987.
  - Έστω A είναι ένα *AND-OR* κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου *fan-in*.
  - Εφαρμόζεται τυχαίος περιορισμός πιθανότητας p.
  - Αν A' το περιορισμένο κύκλωμα,
  - Τότε η πιθανότητα το A' να μην μπορεί να εκφραστεί ως κύκλωμα *OR-AND* μεγέθους το πολύ $s+1$, φράσσεται άνω από $(5pk)^s$.

- Switching Lemma του Johan Håstad, 1987.
  - Έστω A είναι ένα *AND-OR* κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου *fan-in*.
  - Εφαρμόζεται τυχαίος περιορισμός πιθανότητας p.
  - Αν A' το περιορισμένο κύκλωμα,
  - Τότε η πιθανότητα το A' να μην μπορεί να εκφραστεί ως κύκλωμα *OR-AND* μεγέθους το πολύ $s+1$, φράσσεται άνω από $(5pk)^s$.

(!) Καμία εξάρτηση από το πλήθος των μεταβλητών εισόδου.

- Switching Lemma του Johan Håstad, 1987.
  - Έστω A είναι ένα *AND-OR* κύκλωμα δύο επιπέδων, μεγέθους $k+1$ και μη φραγμένου *fan-in*.
  - Εφαρμόζεται τυχαίος περιορισμός πιθανότητας p.
  - Αν A' το περιορισμένο κύκλωμα,
  - Τότε η πιθανότητα το A' να μην μπορεί να εκφραστεί ως κύκλωμα *OR-AND* μεγέθους το πολύ $s+1$, φράσσεται άνω από $(5pk)^s$.
  - (!) Καμία εξάρτηση από το πλήθος των μεταβλητών εισόδου.
  - Βέλτιστο κάτω φράγμα στο μέγεθος κυκλωμάτων βάθους k για τον υπολογισμό συναρτήσεων ισοτιμίας:

$$\exp\left(\Omega\left(n^{\frac{1}{k-1}}\right)\right)$$

- P vs BPP

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:
  - Αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί (*derandomization*) σε ντετερμινιστικό, με κόστος χρόνου το πολύ πολυωνυμικό.

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:
  - Αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί (*derandomization*) σε ντετερμινιστικό, με κόστος χρόνου το πολύ πολυωνυμικό.

$\Rightarrow P = BPP$

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:
  - Αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί (*derandomization*) σε ντετερμινιστικό, με κόστος χρόνου το πολύ πολυωνυμικό.

$\Rightarrow P = BPP$

- Όμως:

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:
  - Αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί (*derandomization*) σε ντετερμινιστικό, με κόστος χρόνου το πολύ πολυωνυμικό.

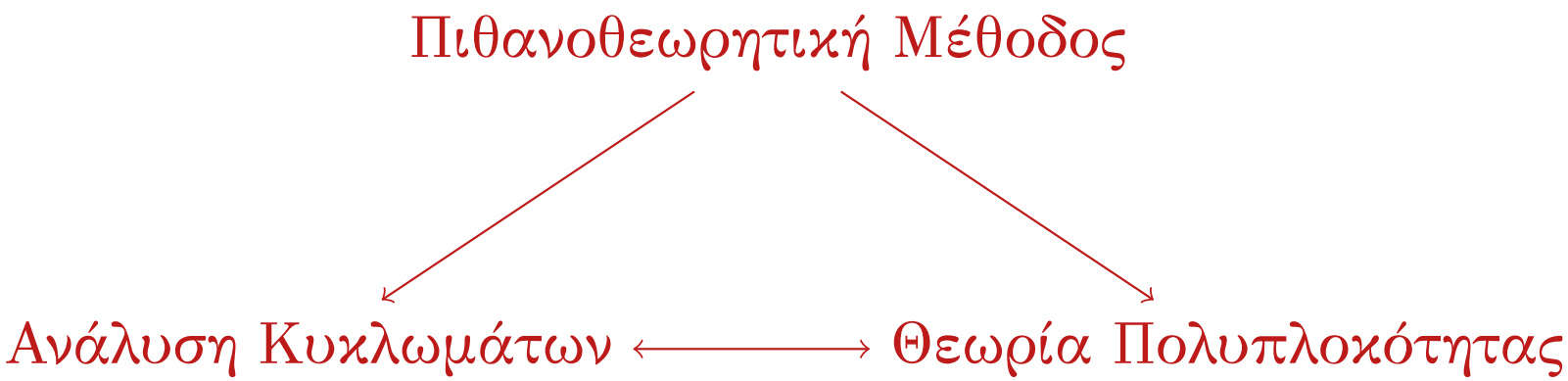
$\Rightarrow P = BPP$

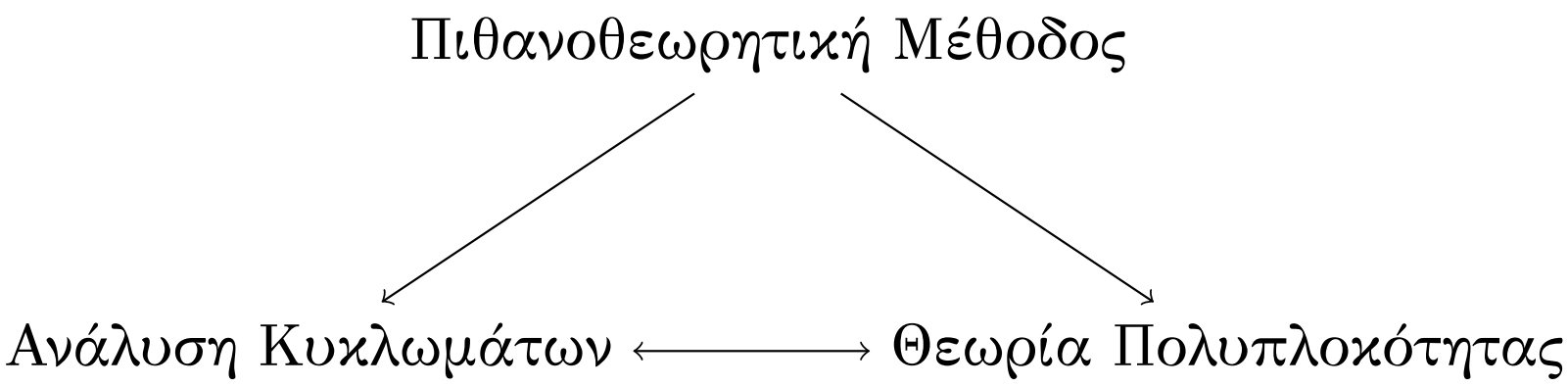
- Όμως:
  - Η διαδικασία της αποτυχαιοποίησης (*derandomization*) αποδεικνύεται ότι απαιτεί κάτω φράγματα λογικών κυκλωμάτων.

- P vs BPP
  - **BPP**: η κλάση των προβλημάτων απόφασης που απαντώνται σε πολυωνυμικό χρόνο από μια Τυχαιοποιημένη Μηχανή Turing.
- Προφανώς $P \subset BPP$.
- Λογική Υπόθεση: $P \neq BPP$.
- Όμως:
  - Αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί (*derandomization*) σε ντετερμινιστικό, με κόστος χρόνου το πολύ πολυωνυμικό.

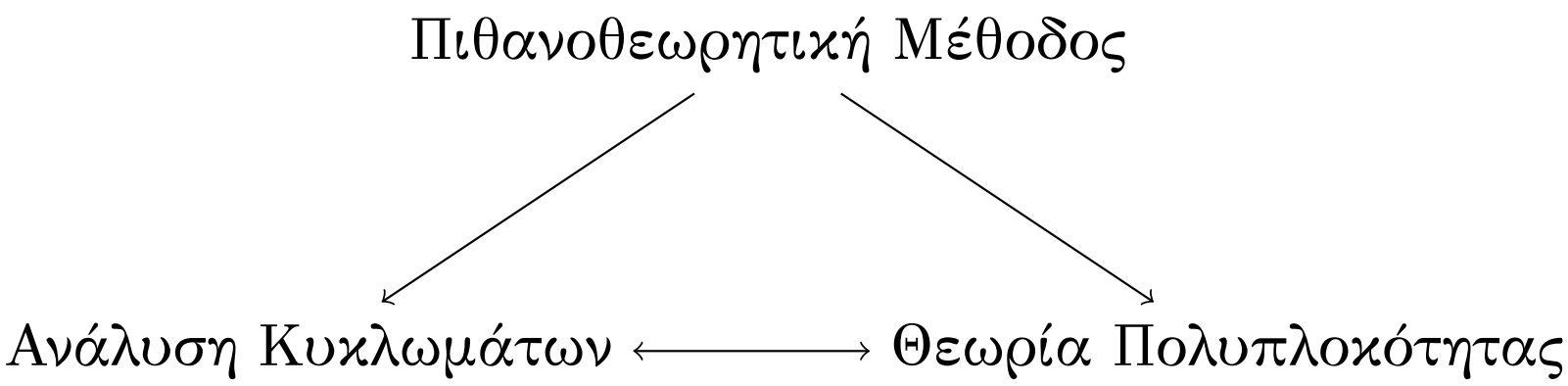
$\Rightarrow$ $P = BPP$: **Εικασία**

- Όμως:
  - Η διαδικασία της αποτυχαιοποίησης (*derandomization*) αποδεικνύεται ότι απαιτεί κάτω φράγματα λογικών κυκλωμάτων.

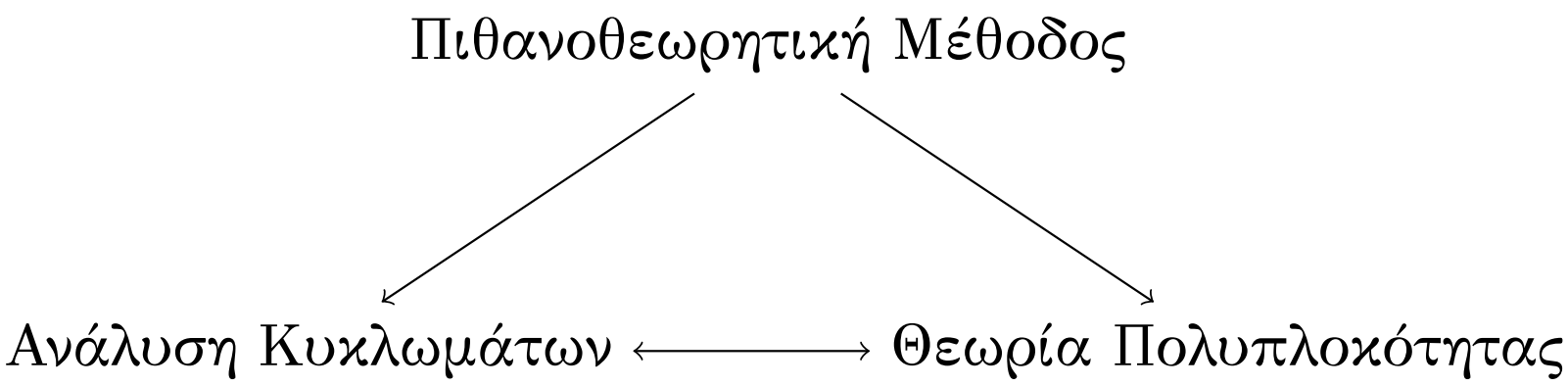

Πιθανοθεωρητική Μέθοδος
Ανάλυση Κυκλωμάτων
Θεωρία Πολυπλοκότητας



- Όχι πανάκεια.



- Όχι πανάκεια.
- Η εισαγωγή τυχαιότητας είναι και εργαλειακού χαρακτήρα.



- Όχι πανάκεια.
- Η εισαγωγή τυχαιότητας είναι και εργαλειακού χαρακτήρα.

(*) Μοιάζει να υπάρχει θεμελιώδης δομική σχέση αυτων των προβλημάτων με την Πιθανοθεωρητική Μέθοδο.