Υπολογισιμότητα και Πολυπλοκότητα
Computability and Complexity

Διδάσκων: Στάθης Ζάχος
Επιμέλεια Διαφανειών: Μάκης Αρσένης
CoReLab

ΣΗΜΜΥ - Ε.Μ.Π.

Μάιος 2017

Περιεχόμενα

Τυχαιότητα (Randomness) I

- Χρησιμοποιώντας το μοντέλο **δένδρων υπολογισμού**, θα ορίσουμε κλάσεις πολυπλοκότητας που βασίζονται στις **πιθανότητες**, με βάση τυχαίες επιλογές.
- Αυτή η προσέγγιση είναι πολύ χρήσιμη από πρακτική άποψη, αφού σε πολλές εφαρμογές, είναι ικανοποιητικός ένας αλγόριθμος ο οποίος κάνοντας κάποιες τυχαίες επιλογές, δίνει στις περισσότερες των περιπτώσεων το σωστό αποτέλεσμα.
- Ένας **πιθανοκρατικός αλγόριθμος** είναι συνήθως πιο απλός στην διατύπωσή του και στην πράξη πιο αποδοτικός από έναν αντίστοιχο ντετερμινιστικό που επιλύει το ίδιο πρόβλημα. Για παράδειγμα, απλοί πιθανοκρατικοί αλγόριθμοι για τον έλεγχο αν ένας αριθμός είναι πρώτος υπάρχουν από την δεκαετία του 1970 και χρησιμοποιούνται στην πράξη έναντι πιο περίπλοκων ντετερμινιστικών τύπου AKS.
- Στα πλαίσια του μοντέλου δένδρων υπολογισμού, θα θεωρήσουμε ότι η επιλογή σε κάθε κόμβο του δένδρου γίνεται τυχαία με πιθανότητα $1/2$ για κάθε παιδί του κόμβου. Για να δείξουμε ότι η *«συντριπτική» πλειοψηφία* των υπολογισμών δίνει το σωστό αποτέλεσμα, εισαγάγουμε έναν νέο ποσοδείκτη, τον $\exists^+$.

Τυχαιότητα (Randomness) II

- Με την βοήθεια του $\exists^+$, ορίζουμε την κλάση BPP, από το **Bounded Probabilistic Polynomial**:

Ορισμός ($\mathrm{BPP} = (\exists^+, \exists^+)$)

$$L \in \mathrm{BPP} \iff \exists R \in \mathrm{P}: \begin{cases} x \in L & \implies \exists^+ y R(x,y) \\ x \notin L & \implies \exists^+ y \neg R(x,y) \end{cases}$$

Τυχαιότητα (Randomness) III

- Με άλλα λόγια, σε ένα δέντρο για την κλάση BPP έχουμε την «συντριπτική» πλειοψηφία των φύλλων να δίνει το σωστό αποτέλεσμα. Στον παραπάνω ορισμό, δεν έχει μεγάλη σημασία ο ακριβής ορισμός της «συντριπτικής» πλειοψηφίας, αλλά πρέπει να είναι οπωσδήποτε *φραγμένος* (εξ ου και το 'bounded' του BPP) πάνω από το $1/2$. Το ποσοστό της πλειοψηφίας μπορεί να είναι, ενδεικτικά, μεγαλύτερο από $1/2 + \varepsilon$, $1/2 + 1/p(|x|)$, $2/3$, 99%, $1 - 2^{-p(|x|)}$ (όπου $p(|x|) > 1$). Αυτή η δυνατότητα επιλογής υπάρχει, επειδή με πολυωνυμικές επαναλήψεις του αντίστοιχου αλγορίθμου, είναι δυνατόν να αυξήσουμε την πιθανότητα επιτυχίας, όσο θέλουμε. Αλγόριθμοι BPP ονομάζονται **Monte Carlo** ή αλλιώς two-sided error, επειδή ανεξάρτητα από το αποτέλεσμα (ναι ή όχι), υπάρχει κάποια πιθανότητα λάθους. Είναι προφανές ότι η κλάση BPP είναι κλειστή ως προς συμπλήρωμα.

Τυχαιότητα (Randomness) IV

- Ας θεωρήσουμε τώρα αλγορίθμους οι οποίοι κάνουν λάθος μόνον για την μία απάντηση (one sided error). Έτσι, προκύπτει η κλάση RP (**Randomized Polynomial**):

Ορισμός ($\mathrm{RP} = (\exists^+, \forall)$)

$$L \in \mathrm{RP} \iff \exists R \in \mathrm{P}: \begin{cases} x \in L & \implies \exists^+ y R(x,y) \\ x \notin L & \implies \forall y \neg R(x,y) \end{cases}$$

Σε αυτήν την κλάση, αν ο αντίστοιχος RP αλγόριθμος δώσει απάντηση «ναι» (δηλαδή το κατηγόρημα R υπολογιστεί αληθές), είμαστε σίγουροι ότι $x \in L$. Αντίθετα, η απάντηση «όχι» του RP αλγορίθμου δεν είναι «σίγουρη».

Προφανώς, ισχύουν: $\mathrm{RP} \subseteq \mathrm{BPP}$, $\mathrm{coRP} \subseteq \mathrm{BPP}$, αλλά δεν γνωρίζουμε αν $\mathrm{RP} = \mathrm{coRP}$.

Τυχαιότητα (Randomness) V

- Μία άλλη πολύ χρήσιμη κλάση, είναι αυτή που ορίζεται με τομή των RP και coRP, η $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$. Η ονομασία προέρχεται από το **Zero error Probabilistic Polynomial**, γιατί μπορεί εύκολα να δειχτεί ότι ένα πρόβλημα είναι στο ZPP αν υπάρχει πιθανοκρατικός αλγόριθμος ο οποίος τρέχει σε αναμενόμενο πολυωνυμικό χρόνο και δίνει πάντοτε σωστή απάντηση. Πράγματι, αν ένα πρόβλημα είναι στο ZPP, σημαίνει ότι έχουμε ένα RP και έναν coRP αλγόριθμο για αυτό, οπότε αρκεί να τρέχουμε εναλλακτικά τους δύο αλγορίθμους, μέχρι ο ένας να δώσει την «σίγουρή» του απάντηση. Βέβαια, μπορεί να χρειαστεί να τρέχουμε εναλλακτικά τους δύο αλγορίθμους για πάντα, αλλά με μεγάλη πιθανότητα θα έχουμε μία «σίγουρη» απάντηση, μετά από μερικές επαναλήψεις. Εναλλακτικά, μπορούμε να πούμε ότι ένας ZPP αλγόριθμος έχει τρεις εξόδους: «ναι», «όχι» (για τις «σίγουρες» απαντήσεις), και «δεν ξέρω» (για τις όχι «σίγουρες»).

  Οι αλγόριθμοι στο ZPP ονομάζονται **Las Vegas**.

Τυχαιότητα (Randomness) VI

- Δεδομένου ότι υπάρχουν αρκετοί πιθανοκρατικοί αλγόριθμοι ευρείας χρήσης για πρακτικά προβλήματα, πολλοί τοποθετούν τους εφικτούς (feasible) υπολογισμούς πάνω από το P, στις πιθανοτικές κλάσεις BPP, RP, ZPP.

  Πάντως, δεν γνωρίζουμε αν υπάρχουν πλήρη προβλήματα για τις κλάσεις που ορίστηκαν παραπάνω (BPP, RP, ZPP).
- Αν τώρα το ποσοστό λάθους ενός πιθανοκρατικού αλγορίθμου δεν φραχθεί μακριά από το $1/2$, τότε έχουμε απλώς την βεβαιότητα ότι στο μοντέλο δένδρων υπολογισμού παραπάνω από τα μισά υπολογιστικά μονοπάτια δίνουν την σωστή απάντηση. Για να δηλώσουμε το παραπάνω χρησιμοποιούμε τον ποσοδείκτη $\exists_{1/2}$. Για unbounded two-sided error, έχουμε την κλάση PP (Probabilistic Polynomial):

Ορισμός ($\mathrm{PP} = (\exists_{1/2}, \exists_{1/2})$)

$$L \in \mathrm{PP} \iff \exists R \in \mathrm{P}: \begin{cases} x \in L & \implies \exists_{1/2} y R(x,y) \\ x \notin L & \implies \exists_{1/2} y \neg R(x,y) \end{cases}$$

Τυχαιότητα (Randomness) VII

- Λόγω της έλλειψης φράγματος για την πιθανότητα λάθους, δεν μπορούμε να χρησιμοποιήσουμε την τεχνική της επανάληψης για να βελτιώσουμε την πιθανότητα σωστού αποτελέσματος από έναν PP αλγόριθμο. Μία άλλη ένδειξη για το ανέφικτο της κλάσης PP σε σχέση με τις BPP, RP, ZPP, προκύπτει από το παρακάτω αποτέλεσμα:

Πρόταση

$\mathrm{NP} \subseteq \mathrm{PP}$.

- Πρέπει επίσης να σημειώσουμε ότι δεν λάβαμε καθόλου υπ' όψιν μας, ως υπολογιστικό πόρο, των αριθμό των τυχαίων bits που χρησιμοποιεί ένας πιθανοκρατικός αλγόριθμος. Στην πράξη, κάθε «τυχαίο» bit που χρειαζόμαστε δεν είναι χωρίς τίμημα, αφού το λαμβάνουμε από κάποια γεννήτρια *ψευδοτυχαίων* bits.
- Τέλος, αναφέρουμε και την κλάση RL (**Randomized Logspace**) που περιέχει τα προβλήματα που έχουν one-sided error αλγόριθμο που χρησιμοποιεί λογαριθμικό χώρο και πολυωνυμικό ως προς το μήκος της εισόδου αριθμό τυχαίων bits.

Πολυωνυμική Ιεραρχία Ι

Αντίστοιχα με προηγούμενο κεφάλαιο, όπου ορίσαμε μαντεία και την αριθμητική ιεραρχία, θα ορίσουμε την **πολυωνυμική ιεραρχία**, η οποία έχει παρόμοια δομή, αλλά βρίσκεται πολύ χαμηλότερα από άποψη υπολογιστικής πολυπλοκότητας. Υπενθυμίζουμε την έννοια του υπολογισμού με μαντείο: Ένας αλγόριθμος χρησιμοποιεί ένα μαντείο για το πρόβλημα Π, αν έχει την δυνατότητα κατά την διάρκεια του υπολογισμού, να ρωτάει το μαντείο για κάποιο στιγμιότυπο x του προβλήματος Π, αν $x \in \Pi$, και το μαντείο να του απαντά άμεσα με ένα «ναι» ή με ένα «όχι». Όσο δύσκολο και να είναι το πρόβλημα P, ο αλγόριθμος δεν σπαταλά επιπλέον υπολογιστικούς πόρους.

Πολυωνυμική Ιεραρχία II

Ορισμός (Κλάσεις με μαντεία)

- $\mathcal{C}^{\Pi}$: η κλάση των προβλημάτων τα οποία λύνονται με αλγόριθμο στην κλάση $\mathcal{C}$ ο οποίος χρησιμοποιεί μαντείο για το πρόβλημα Π
- $\mathcal{C}^{\mathcal{C}_o} = \bigcup_{\Pi \in \mathcal{C}_o} \mathcal{C}^{\Pi}$

Για παράδειγμα, η κλάση $\mathrm{P}^{\mathrm{SAT}}$ αποτελείται από τα προβλήματα που λύνονται με ντετερμινιστικό πολυωνυμικό αλγόριθμο ο οποίος χρησιμοποιεί μαντείο για το πρόβλημα SAT. Άλλη περιγραφή της ίδιας κλάσης είναι: P^{NP} (αφού το SAT είναι NP-πλήρες).

Πολυωνυμική Ιεραρχία III

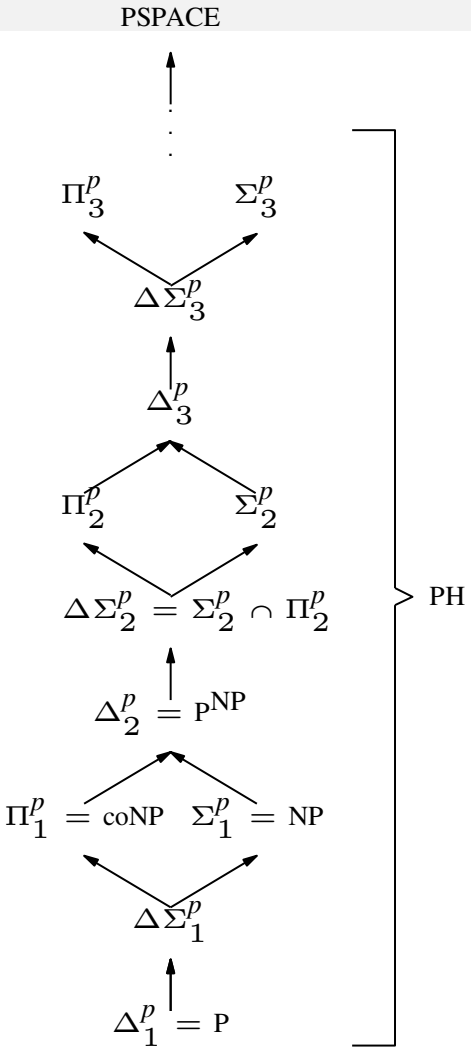
Ορισμός

$(k \geqslant 0)$

- $\Sigma_0^p = \Pi_0^p = \Delta_0^p = \mathrm{P}$
- $\Sigma_{k+1}^p = \mathrm{NP}^{\Sigma_k^p}$, $\Pi_{k+1}^p = \mathrm{co}\Sigma_{k+1}^p$, $\Delta_{k+1}^p = \mathrm{P}^{\Sigma_k^p}$, $\Delta\Sigma_k^p = \Sigma_k^p \cap \Pi_k^p$
- Πολυωνυμική ιεραρχία: $\mathrm{PH} = \bigcup_{k \in \mathbb{N}} \Sigma_k^p$

Ισχύουν τα παρακάτω: $\Sigma_1^p = \mathrm{NP}$, $\Pi_1^p = \mathrm{coNP}$ και για κάθε $k \geqslant 0$: $\Sigma_k^p \subseteq \Sigma_{k+1}^p$ και $\Pi_k^p \subseteq \Sigma_{k+1}^p$. Αν και δεν έχει αποδειχθεί το αυστηρό των παραπάνω εγκλεισμών (όπως στην αριθμητική ιεραρχία), εν τούτοις πιστεύουμε ότι η ιεραρχία είναι *αυστηρή* (strict). Αν η PH δεν είναι αυστηρή, τότε θα υπάρχει κάποιο k για το οποίο $\mathrm{PH} = \Sigma_k^p$, οπότε λέμε ότι *η πολυωνυμική ιεραρχία καταρρέει στο k-οστό επίπεδο* (collapses at the k-th level).

Πολυωνυμική Ιεραρχία IV



Σχήμα: Η πολυωνυμική ιεραρχία PH

Πολυωνυμική Ιεραρχία — Εναλλαγή Ποσοδεικτών Ι

Ένας εναλλακτικός τρόπος ορισμού της πολυωνυμικής ιεραρχίας είναι με την βοήθεια εναλλαγής ποσοδεικτών ($\exists$ και $\forall$). Επισημαίνουμε ότι, σε κάθε περίπτωση, οι ποσοδείκτες αναφέρονται σε αντικείμενα το μέγεθος των οποίων είναι φραγμένο από κάποιο πολυώνυμο p ως προς το μήκος της εισόδου.

Πρόταση

$L \in \Sigma_k^p$ ανν υπάρχει κατηγόρημα R υπολογιζόμενο σε πολυωνυμικό χρόνο και πολυώνυμο p που φράσσει το μέγεθος των αντικειμένων των ποσοδεικτών, τέτοια ώστε:

$$x \in L \iff \exists y_1 \forall y_2 \ldots Q y_k \; R(x, y_1, y_2, \ldots, y_k),$$

όπου $Q = \begin{cases} \exists, & k \text{ περιττό} \\ \forall, & k \text{ άρτιο} \end{cases}$.

Πολυωνυμική Ιεραρχία — Εναλλαγή Ποσοδεικτών II

Παρομοίως, για την κλάση Π_k^p μόνο που τώρα η ακολουθία των ποσοδεικτών αρχίζει από $\forall$:

Πρόταση

$L \in \Pi_k^p$ ανν υπάρχει κατηγόρημα R υπολογιζόμενο σε πολυωνυμικό χρόνο και πολυώνυμο p που φράσσει το μέγεθος των αντικειμένων των ποσοδεικτών, τέτοια ώστε:

$$x \in L \iff \forall y_1 \exists y_2 \ldots Q y_k \; R(x, y_1, y_2, \ldots, y_k),$$

όπου $Q = \begin{cases} \forall, & k \text{ περιττό} \\ \exists, & k \text{ άρτιο} \end{cases}$.

Πολυωνυμική Ιεραρχία — Alternating TM I

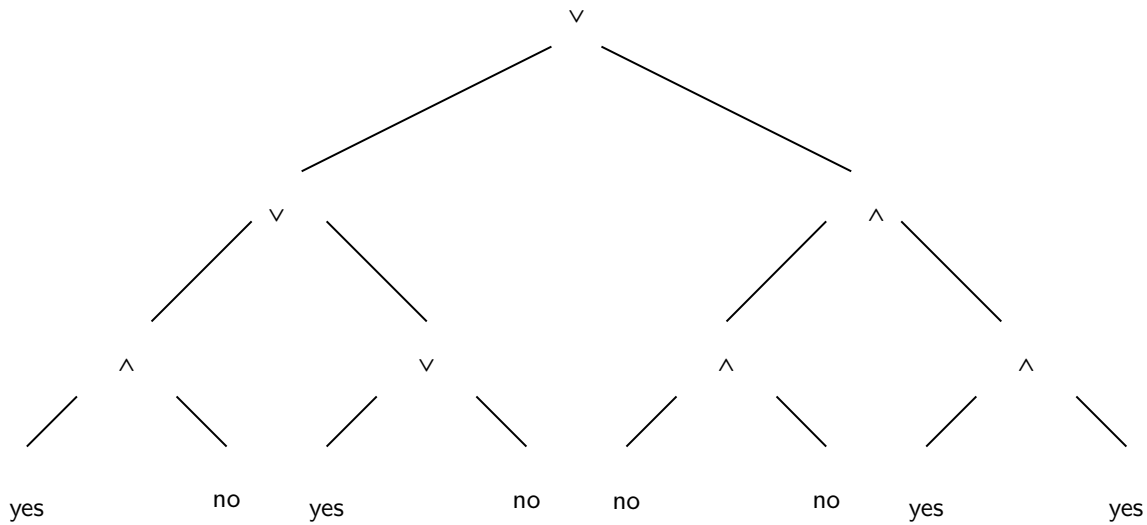
Η εναλλαγή των ποσοδεικτών στην πολυωνυμική ιεραρχία δίνει το έναυσμα για τον ορισμό της μηχανής Turing με εναλλασσόμενη λειτουργία. Αν θεωρήσουμε την δενδρική αναπαράσταση των υπολογισμών μίας NP μηχανής Turing, η μηχανή απαντά ναι, αν υπάρχει ένα τουλάχιστον φύλλο που λέει «ναι». Μπορούμε να θεωρήσουμε ότι κάθε κόμβος στο δένδρο υπολογίζει την διάζευξη ($\vee$) των αποτελεσμάτων από τα παιδιά του και την προωθεί στον γονέα του (τα φύλλα απλώς προωθούν προς τα πάνω), μέχρι το αποτέλεσμα να φτάσει στην ρίζα. Αντίστοιχα, μία coNP μηχανή Turing αποδέχεται όταν στην δενδρική αναπαράσταση όλα τα φύλλα λένε «ναι», οπότε μπορούμε να θεωρήσουμε ότι ο κάθε κόμβος συλλέγει τα αποτέλεσμα των παιδιών του και προωθεί στον γονέα του την σύζευξη ($\wedge$) των αποτελεσμάτων από τα παιδιά του, πάλι μέχρι το σωστό αποτέλεσμα να φτάσει στην ρίζα. Λέμε ότι όλοι οι κόμβοι στο δένδρο μίας NP μηχανής είναι τύπου $\vee$, ή $\exists$, ή υπαρξιακού. Λέμε ότι όλοι οι κόμβοι στο δένδρο μίας coNP μηχανής είναι τύπου $\wedge$, ή $\forall$, ή καθολικού.

Πολυωνυμική Ιεραρχία — Alternating TM II

Μία **εναλλασσόμενη μηχανή Turing** είναι μία μηχανή Turing στην οποία το αντίστοιχο υπολογιστικό δένδρο έχει εσωτερικούς κόμβους τύπου $\vee$ ή $\wedge$. Σημασία έχει το **πλήθος εναλλαγών τύπου**. Το μέγιστο **πλήθος εναλλαγών** (σε ένα μονοπάτι), που πιθανώς να είναι φραγμένο, αποτελεί μέτρο των δυνατοτήτων μίας τέτοιας μηχανής.

Για παράδειγμα, το υπολογιστικό δένδρο του παρακάτω σχήματος έχει πλήθος εναλλαγών τύπου ίσο με 2.

Πολυωνυμική Ιεραρχία — Alternating TM III



Σχήμα: Υπολογιστικό δένδρο με εναλλαγές

Πολυωνυμική Ιεραρχία — Alternating TM IV

Μπορεί να δειχθεί ότι η πολυωνυμική ιεραρχία είναι ακριβώς η κλάση των γλωσσών που γίνεται αποδεκτή από μηχανές Turing που έχουν φραγμένο πλήθος εναλλαγών. Πιο συγκεκριμένα:

- $L \in \Sigma_k^p$ ανν η L γίνεται αποδεκτή από μηχανή Turing που έχει το πολύ k εναλλαγές τύπου και αρχίζει με τύπο $\vee$.
- $L \in \Pi_k^p$ ανν η L γίνεται αποδεκτή από μηχανή Turing που έχει το πολύ k εναλλαγές τύπου και αρχίζει με τύπο $\wedge$.

Παραλληλοποιήσιμα προβλήματα Ι

Για να μελετήσουμε παράλληλους υπολογισμούς θα εισάγουμε ένα νέο μοντέλο υπολογισμού, το **κύκλωμα**.

Ένα κύκλωμα είναι ένας κατευθυνόμενος ακυκλικός γράφος, στον οποίο έχουμε ένα σύνολο κόμβων **εισόδου** και έναν κόμβο που είναι η **έξοδος**. Θεωρούμε ότι οι είσοδοι στο κύκλωμα είναι αληθοτιμές (ή αλλιώς οι τιμές 0 και 1) και κάθε εσωτερικός κόμβος αντιστοιχεί σε μία λογική συνάρτηση (ή αλλιώς πύλη — gate) με πλήθος εισόδων, όσες οι ακμές που καταλήγουν σε αυτόν. Αν ένα κύκλωμα C έχει n εισόδους του ενός bit: x_1, x_2, ..., x_n, τότε για κάθε $x \in \{0,1\}^n$, υπολογίζει μία μοναδική τιμή στην έξοδο, την $C(x)$. Αν $C(x) = 1$, λέμε ότι το κύκλωμα C αποδέχεται την είσοδο των n bit: x.

Παραλληλοποιήσιμα προβλήματα II

Η αναντιστοιχία του παραπάνω ορισμού αποδοχής, σε σχέση με την αποδοχή, ας πούμε, σε μία μηχανή Turing, είναι ότι ένα κύκλωμα, λόγω της αμετάβλητης φύσης του, μπορεί να απαντά για εισόδους μήκους ακριβώς n, ενώ μία μηχανή Turing (ή ένας αλγόριθμος γενικότερα) δέχεται εισόδους οποιουδήποτε μεγέθους. Για τον λόγο αυτό θα θεωρούμε μία οικογένεια κυκλωμάτων $\{C_1, C_2, \dots\}$, όπου κάθε C_n έχει n κόμβους εισόδου. Η **γλώσσα** που αποδέχεται μία οικογένεια κυκλωμάτων είναι η

$$L(C) = \{x \mid C_{|x|}(x) = 1\}.$$

Το πρόβλημα είναι ότι οι οικογένειες κυκλωμάτων (σε αντίθεση με τις μηχανές Turing) δεν είναι αριθμήσιμες.

Παραλληλοποιήσιμα προβλήματα III

Για να ξεπεράσουμε την παραπάνω δυσκολία, θα περιοριστούμε σε **ομοιόμορφες οικογένειες κυκλωμάτων** (uniform circuit families). Για αυτές υπάρχει αλγόριθμος και μάλιστα αποδοτικός ο οποίος δεδομένου n κατασκευάζει την αναπαράσταση του κυκλώματος C_n της οικογένειας. Μία επιλογή είναι οι P-ομοιόμορφες οικογένειες, που χρησιμοποιούν πολυωνυμικό αλγόριθμο κατασκευής. Επειδή όμως τα κυκλώματα χρησιμοποιούνται συνήθως για ορισμό κλάσεων χαμηλότερα από το P, θα χρησιμοποιήσουμε μία άλλη πιο περιορισμένη έννοια ομοιομορφίας:

Ορισμός

Μία οικογένεια κυκλωμάτων είναι DLOGTIME-ομοιόμορφη αν υπάρχει μηχανή Turing (με δυνατότητα τυχαίας προσπέλασης στην ταινία εισόδου) που απαντά τις παρακάτω ερωτήσεις σε χρόνο $O(\log n)$:

- Υπάρχει σύνδεση από τον κόμβο u στον κόμβο v στο C_n;
- Τι είδους πύλη έχει ο κόμβος u;

Παραλληλοποιήσιμα προβλήματα IV

Το *μέγεθος* (size) ενός κυκλώματος είναι το πλήθος των κόμβων που περιέχει ο αντίστοιχος γράφος. Το μέγεθος αποτελεί μέτρο του κόστους κατασκευής του κυκλώματος και συνήθως δεν θεωρείται περισσότερο από πολυωνυμικό ως προς το μήκος της εισόδου. Το μέγεθος, όμως, δεν αποτελεί και πολύ καλό μέτρο του χρόνου υπολογισμού σε ένα κύκλωμα, επειδή εν γένει πολλές λογικές πύλες λειτουργούν παράλληλα. Οι πύλες που πρέπει να περιμένουν διαδοχικά ενδιάμεσα αποτελέσματα είναι αυτές που βρίσκονται σε κάθε μονοπάτι από μία είσοδο στην έξοδο. Για τον λόγο αυτό, πιο σημαντικό είναι το *βάθος* (depth) ενός κυκλώματος, που ορίζεται ως το μήκος του μακρύτερου μονοπατιού από είσοδο στην έξοδο.

Παραλληλοποιήσιμα προβλήματα V

Επίσης, σημαντικό είναι το είδος των λογικών πυλών που χρησιμοποιούνται σε κάθε κύκλωμα. Πιο συγκεκριμένα, θεωρούμε τα παρακάτω είδη λογικών πυλών:

1. Λογικές πύλες με περιορισμένο αριθμό εισόδων (bounded fan-in), καθώς και εναδικές πύλες $\neg$. Αρκεί να θεωρήσουμε δυαδικές πύλες $\wedge$ και $\vee$ (μαζί με τις εναδικές πύλες $\neg$).
2. Λογικές πύλες $\wedge$ και $\vee$ με απεριόριστο αριθμό εισόδων (unbounded fan-in), καθώς και εναδικές πύλες $\neg$.
3. Πύλες κατωφλίου (threshold) με απεριόριστο αριθμό εισόδων, καθώς και εναδικές πύλες $\neg$. Αρκεί, αντί για γενικές πύλες κατωφλίου, να χρησιμοποιήσουμε την πύλη πλειοψηφίας (majority gate), που δίνει στην έξοδο 1 αν και μόνον αν τουλάχιστον $r/2$ από τις r εισόδους της είναι 1.

Παραλληλοποιήσιμα προβλήματα VI

Με βάση τα παραπάνω μπορούμε να ορίσουμε τις παρακάτω κλάσεις:

Ορισμός

$(k \geqslant 0)$:

1. NC^k: η κλάση των γλωσσών που γίνονται αποδεκτές από DLOGTIME-ομοιόμορφες οικογένειες κυκλωμάτων πολυωνυμικού μεγέθους και βάθους $O(\log^k n)$, με χρήση πυλών του 1ου είδους (bounded fan-in).
2. AC^k: η κλάση των γλωσσών που γίνονται αποδεκτές από DLOGTIME-ομοιόμορφες οικογένειες κυκλωμάτων πολυωνυμικού μεγέθους και βάθους $O(\log^k n)$, με χρήση πυλών του 2ου είδους (unbounded fan-in).
3. TC^k: η κλάση των γλωσσών που γίνονται αποδεκτές από DLOGTIME-ομοιόμορφες οικογένειες κυκλωμάτων πολυωνυμικού μεγέθους και βάθους $O(\log^k n)$, με χρήση πυλών του 3ου είδους (threshold gates).
4. SC^k: η κλάση των γλωσσών που γίνονται αποδεκτές από DTM σε πολυωνυμικό χρόνο και σε $O(\log^k n)$ χώρο.

Παραλληλοποιήσιμα προβλήματα VII

Επίσης, ορίζεται $\mathrm{NC} = \bigcup_{k \in \mathbb{N}} \mathrm{NC}^k$. Η τελευταία κλάση λέγεται και Nick's Class, από τον Nicholas Pippenger, που ήταν από τους πρώτους που μελέτησε τέτοια κυκλώματα. Στην πραγματικότητα, πολλά άλλα μοντέλα παράλληλου υπολογισμού (π.χ. CRAM), εκτός από τα κυκλώματα, μπορούν να χρησιμοποιηθούν για τον ορισμό της κλάσης NC, κάτι που αποτελεί ένδειξη για την ευρωστία της κλάσης και την στενή σχέση της με τα παραλληλοποιήσιμα προβλήματα.

Το «A» στην AC^k οφείλεται στην εναλλαγή (alternation), αφού αποδεικνύεται ότι η κλάση AC^k, για $k \geqslant 1$, είναι ακριβώς οι γλώσσες που γίνονται αποδεκτές από εναλλασσόμενη μηχανή Turing που χρησιμοποιεί $O(\log n)$ χώρο και κάνει το πολύ $O(\log^k n)$ εναλλαγές. Το «T» στην TC^k προέρχεται από το threshold. Η ονομασία SC, "Steve's Class", προέρχεται από τον Steve Cook.

Παραλληλοποιήσιμα προβλήματα VIII

Πιο συγκεκριμένα οι κλάσεις σχετίζονται μεταξύ τους ως εξής:

Θεώρημα

Για κάθε $k \geqslant 0$, $\mathrm{NC}^k \subseteq \mathrm{AC}^k \subseteq \mathrm{TC}^k \subseteq \mathrm{NC}^{k+1}$.

Σε σχέση με άλλες γνωστές κλάσεις, ισχύει:

Θεώρημα

$\mathrm{Regular} \subseteq \mathrm{NC}^1 \subseteq \mathrm{L} = \mathrm{SC}^1 \subseteq \mathrm{NL} \subseteq \mathrm{AC}^1$.
$\mathrm{Regular} \subset \mathrm{CF} \subset \mathrm{AC}^1$.

Δηλαδή το πρόβλημα του ελέγχου αν μία συμβολοσειρά παράγεται από δεδομένη γλώσσα χωρίς συμφραζόμενα (context free) ανήκει στην κλάση NC^2.

Διαλογική αλληλεπίδραση (interactivity) I

Διαλογικά συστήματα αποδείξεων (IP)

Ας θεωρήσουμε έναν **αποδείκτη (prover)** που προσπαθεί να αποδείξει την αλήθεια μίας πρότασης του τύπου «$x \in L$» σε κάποιον άλλο, που τον ονομάζουμε **επαληθευτή (verifier)**.

Ο αποδείκτης είναι παντοδύναμος, με την έννοια ότι είναι ένας αλγόριθμος χωρίς περιορισμούς στο μέγεθος των αγαθών που χρησιμοποιεί (χρόνος, χώρος). Αντίθετα, ο επαληθευτής είναι απλώς ένας πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου.

Ο επαληθευτής και ο αποδείκτης συμμετέχουν σε ένα πρωτόκολλο επικοινωνίας στέλνοντας μηνύματα. Ανάλογα με τα μηνύματα που λαμβάνει ο V από τον P, ο V αποδέχεται την απόδειξη, αλλιώς την απορρίπτει. Ο αποδείκτης μπορεί να μην είναι έντιμος, και να θέλει να πείσει τον επαληθευτή ότι «$x \in L$», ακόμη και για x για τα οποία «$x \notin L$». Ο επαληθευτής, απέναντι στον παντοδύναμο αποδείκτη, μπορεί να χρησιμοποιήσει εκτός του πολυωνυμικού χρόνου, κυρίως την τυχαιότητα που διαθέτει.

Διαλογική αλληλεπίδραση (interactivity) II

Διαλογικά συστήματα αποδείξεων (IP)

Η κλάση IP ορίστηκε από τους Goldwasser, Micali, Rackoff:

Ορισμός

$L \in \mathrm{IP}$:

- $x \in L \implies$ υπάρχει αποδείκτης (prover) P, ώστε ο επαληθευτής (verifier) V πάντοτε αποδέχεται (δηλαδή έχουμε πιθανότητα αποδοχής ίση με 1)·
- $x \notin L \implies$ για κάθε αποδείκτη (prover) P, ο επαληθευτής V δεν αποδέχεται με συντριπτική πιθανότητα.

Ας θεωρήσουμε το **πρόβλημα μη ισομορφισμού γράφων**: «Δίνονται δύο γράφοι. Είναι μη ισομορφικοί;». Αυτό το πρόβλημα ανήκει στο coNP. Θα δώσουμε ένα πρωτόκολλο για το πρόβλημα μη ισομορφισμού γράφων, που θα δείχνει ότι το πρόβλημα είναι στο IP.

Διαλογική αλληλεπίδραση (interactivity) III

Διαλογικά συστήματα αποδείξεων (IP)

Αρχικά, ο επαληθευτής έχει τους δύο γράφους G_1 και G_2. Επιλέγει τυχαία έναν από τους δύο, έστω των G_i, και υπολογίζει έναν τυχαίο ισομορφικό γράφο του G_i, έστω τον H (αυτό γίνεται διαλέγοντας τυχαία μία μετάθεση των n κορυφών του γράφου G_i). Στέλνει τον γράφο H στον αποδείκτη, ζητώντας ένα j τέτοιο ώστε ο G_j να είναι ισομορφικός του H. Ο αποδείκτης απαντά με ένα $j \in \{1, 2\}$. Ο επαληθευτής αποδέχεται αν όντως $i = j$, αλλιώς απορρίπτει.

Στην περίπτωση που όντως οι G_1, G_2 είναι μη ισομορφικοί, ο P, αφού είναι παντοδύναμος, βρίσκει με ποιον (μοναδικό) γράφο είναι ισομορφικός ο H που του έστειλε ο V και δίνει την σωστή τιμή για να αποδεχθεί ο V. Αν τώρα οι G_1, G_2 είναι ισομορφικοί, ο P αδυνατεί να συμπεράνει από ποιον γράφο προήλθε ο ισομορφικός H, άρα δεν μπορεί να κάνει κάτι καλύτερο από το να στείλει τυχαία ένα από τα $\{1, 2\}$ στον V. Έτσι, αν οι δύο γράφοι είναι μη ισομορφικοί ο V δεν αποδέχεται με πιθανότητα $1/2$.

Τα παραπάνω σκιαγραφούν μία απόδειξη ότι το πρόβλημα μη ισομορφισμού γράφων ανήκει στην IP.

Διαλογική αλληλεπίδραση (interactivity) IV

Διαλογικά συστήματα αποδείξεων (IP)

Στην πραγματικότητα, κάθε γλώσσα στην πολυωνυμική ιεραρχία έχει πρωτόκολλο IP. Μάλιστα, έχει αποδειχθεί το ακόμη ισχυρότερο αποτέλεσμα:

Θεώρημα (Shamir)

$\mathrm{IP} = \mathrm{PSPACE}$

Τι γίνεται όμως στην περίπτωση που ο επαληθευτής μπορεί να διαλέγεται με δύο ή περισσότερους αποδείκτες; Αν οι αποδείκτες επικοινωνούν μεταξύ τους, τότε παραμένουμε στην κλάση IP (πρακτικά, ένας αποδείκτης, ως παντοδύναμος αλγόριθμος, μπορεί να εξομοιώνει οσουσδήποτε άλλους). Αν όμως, οι αποδείκτες δεν έχουν επικοινωνία μεταξύ τους, τότε προκύπτει η ισχυρότερη κλάση MIP (Multi IP). Μάλιστα ισχύει: $\mathrm{MIP} = \mathrm{NEXP}$.

Διαλογική αλληλεπίδραση (interactivity) I

Κλάσεις Arthur-Merlin

Στην κλάση IP ο επαληθευτής κρατά «κρυφά» τα τυχαία bits που χρησιμοποιεί. Μάλιστα, στην απόδειξη ότι το πρόβλημα μη ισομορφισμού γράφων είναι στην IP, αυτό αποτελεί βασικό συστατικό της απόδειξης. Φαίνεται ότι αν ο επαληθευτής είναι υποχρεωμένος να αποκαλύπτει τα bits του, προκύπτει μία μικρότερη κλάση γλωσσών από την IP. Σε αυτήν την κλάση γλωσσών ο αποδείκτης ονομάζεται Merlin και ο επαληθευτής Arthur (αυτή η περιγραφή οφείλεται στον Babai). Μάλιστα, μπορούμε να θεωρήσουμε ότι τα μηνύματα του Arthur είναι ακόμα πιο περιορισμένα: απλώς στέλνει τα τυχαία bits στον Merlin. Ανάλογα με τις απαντήσεις του Merlin, ο Arthur αποφασίζει αν θα αποδεχθεί.

Διαλογική αλληλεπίδραση (interactivity) II

Κλάσεις Arthur-Merlin

Λέμε ότι οι Arthur και Merlin παίζουν ένα παιχνίδι k κινήσεων μεταξύ τους (κάθε κίνηση αντιστοιχεί σε ένα μήνυμα): αν ο Arthur κινείται πρώτος το παιχνίδι συμβολίζεται με $\mathrm{AM}(k)$, ενώ αν κινείται πρώτος ο Merlin με $\mathrm{MA}(k)$. Για παράδειγμα, $\mathrm{AM}(1) = \mathrm{A}$, $\mathrm{AM}(2) = \mathrm{AM}$, $\mathrm{AM}(3) = \mathrm{AMA}$, $\mathrm{MA}(1) = \mathrm{M}$, $\mathrm{MA}(2) = \mathrm{MA}$, $\mathrm{MA}(3) = \mathrm{MAM}$. Μία άλλη διαφορά σε σχέση με την κλάση IP είναι ότι χρειάζεται να φράξουμε τις πιθανότητες μακριά από το $1/2$ (πάλι δεν έχει μεγάλη σημασία η ακριβής τιμή). Τυπικά, για την κλάση $\mathrm{AM}(k)$, έχουμε:

Ορισμός

$L \in \mathrm{AM}(k)$ ανν υπάρχει παιχνίδι k κινήσεων όπου παίζει πρώτος ο Arthur και στο οποίο αν:

- $x \in L \implies$ ο Arthur πείθεται με πιθανότητα μεγαλύτερη από $2/3$ ότι $x \in L$.
- $x \notin L \implies$ ο Arthur πείθεται με πιθανότητα μικρότερη από $1/3$ ότι $x \in L$.

Διαλογική αλληλεπίδραση (interactivity) III

Κλάσεις Arthur-Merlin

Με την βοήθεια των γενικευμένων ποσοδεικτών οι κλάσεις μπορούν να γραφτούν ως εξής (Zachos):

$$\mathrm{AM} = \mathrm{AM}(2) = (\exists^{+}\exists, \exists^{+}\forall), \quad \mathrm{MA} = \mathrm{MA}(2) = (\exists\exists^{+}, \forall\exists^{+}),$$

και για άρτιο k, αν $\mathrm{AM}(k) = (\mathbf{Q}_1, \mathbf{Q}_2)$, όπου $\mathbf{Q}_1$, $\mathbf{Q}_2$ ακολουθίες ποσοδεικτών:

$$\mathrm{AM}(k+1) = (\mathbf{Q}_1\exists^{+}, \mathbf{Q}_2\exists^{+}), \quad \mathrm{AM}(k+2) = (\mathbf{Q}_1\exists^{+}\exists, \mathbf{Q}_2\exists^{+}\forall).$$

Η παραπάνω περιγραφή, μπορεί να απλοποιηθεί ως εξής (Zachos):

$$\mathrm{AM} = \mathrm{AM}(2) = (\forall\exists, \exists^{+}\forall), \quad \mathrm{MA} = \mathrm{MA}(2) = (\exists\forall, \forall\exists^{+}),$$

και για άρτιο k, αν $\mathrm{AM}(k) = (\mathbf{Q}_1, \mathbf{Q}_2)$, όπου $\mathbf{Q}_1$, $\mathbf{Q}_2$ ακολουθίες ποσοδεικτών:

$$\mathrm{AM}(k+1) = (\mathbf{Q}_1\forall, \mathbf{Q}_2\exists^{+}), \quad \mathrm{AM}(k+2) = (\mathbf{Q}_1\forall\exists, \mathbf{Q}_2\exists^{+}\forall).$$

Χρησιμοποιώντας ιδιότητες των ποσοδεικτών προκύπτουν τα παρακάτω αποτελέσματα:

Διαλογική αλληλεπίδραση (interactivity) IV

Κλάσεις Arthur-Merlin

Πρόταση

$\mathrm{MA} \subseteq \mathrm{AM}$.

Πρόταση

Η ιεραρχία των παιχνιδιών Arthur-Merlin καταρρέει, δηλαδή:

$$\mathrm{AM} = \mathrm{AM}(k) = \mathrm{MA}(k+1), \quad \textit{για κάθε } k \geqslant 2.$$

Αν και όπως είπαμε, η κλάση Arthur-Merlin με πολυωνυμικό πλήθος μηνυμάτων αλληλεπίδρασης φαίνεται ασθενέστερη (λόγω δημοσιοποίησης των τυχαίων bits) σε σχέση με την IP, εν τούτοις οι Goldwasser, Sipser απέδειξαν ότι είναι ισοδύναμες.

Διαλογική αλληλεπίδραση (interactivity) I

Probabilistic Checable Proofs — PCP

Αν αντικαταστήσουμε στις διαλογικές αποδείξεις, τον αποδείκτη με μία απλή απόδειξη, έχουμε την κλάση PCP. Ας πούμε ότι στην PCP, ο αποδείκτης δεν έχει καμμία άλλη επικοινωνία, εκτός από το να γράψει στην αρχή της αλληλεπίδρασης με τον επαληθευτή V μίαν απόδειξη και να την στείλει στον V. Πρέπει να σημειώσουμε ότι οι αποδείξεις αυτές ελέγχονται πιθανοτικά από τον V. Τυπικά:

Ορισμός

$L \in \text{PCP}$:

- $x \in L \implies$ υπάρχει απόδειξη Π τέτοια ώστε ο επαληθευτής (verifier) V πάντοτε αποδέχεται (δηλαδή έχουμε πιθανότητα αποδοχής ίση με 1)·
- $x \notin L \implies$ για κάθε «απόδειξη» Π, ο επαληθευτής V δεν αποδέχεται με συντριπτική πιθανότητα.

Διαλογική αλληλεπίδραση (interactivity) II

Probabilistic Checable Proofs — PCP

Αυτή η κλάση φαίνεται πολύ ισχυρότερη από την IP γιατί πλέον ο επαληθευτής έχει να «αντιμετωπίσει» ένα στατικό αντικείμενο (την απόδειξη) και όχι ένα προσαρμοζόμενο στις ερωτήσεις του (τον αποδείκτη). Και πράγματι αποδεικνύεται ότι $\mathrm{PCP} = \mathrm{MIP}(= \mathrm{NEXP})$. Για τον λόγο αυτό, θα θεωρήσουμε περιορισμούς της κλάσης PCP. Θα θεωρήσουμε δύο είδη αγαθών που δεν μπορεί να χρησιμοποιεί αφειδώς ο επαληθευτής:

- τυχαιότητα (με την μορφή τυχαίων bits)·
- bits της απόδειξης που εξετάζονται (ερωτήσεις, ή αλλιώς queries, στην απόδειξη).

Διαλογική αλληλεπίδραση (interactivity) III

Probabilistic Checable Proofs — PCP

Ορισμός

Η κλάση $\mathrm{PCP}(r(n), q(n))$ αποτελείται από τις γλώσσες $L \in \mathrm{PCP}$ για τις οποίες ο πιθανοτικός πολυωνυμικού χρόνου επαληθευτής V χρησιμοποιεί $O(r(n))$ τυχαία bits και ελέγχει $O(q(n))$ bits στην απόδειξη.

Για παράδειγμα, ήδη γνωστές κλάσεις πολυπλοκότητας μπορούν να οριστούν με την βοήθεια των παραπάνω: $\mathrm{PCP} = \mathrm{PCP}(\mathrm{poly}(n), \mathrm{poly}(n))$, $\mathrm{P} = \mathrm{PCP}(0, 0)$, $\mathrm{NP} = \mathrm{PCP}(0, \mathrm{poly}(n))$, $\mathrm{coRP} = \mathrm{PCP}(\mathrm{poly}(n), 0)$.

Ένα πολύ σημαντικό αποτέλεσμα (Arora, Lund, Motwani, Sudan, Szegedy) είναι το εξής:

Θεώρημα (PCP)

$\mathrm{NP} = \mathrm{PCP}(\log n, 1)$.

Διαλογική αλληλεπίδραση (interactivity) IV

Probabilistic Checable Proofs — PCP

Μία εφαρμογή του θεωρήματος PCP είναι σε αποδείξεις μη προσεγγισιμότητας.

Το βασικό εργαλείο στην απόδειξη του προηγουμένου θεωρήματος είναι μία μέθοδος (PCP encoding) που διαχέει ένα πιθανό λάθος μίας απόδειξης σε όλα τα κομμάτια της απόδειξης, έτσι ώστε ο επαληθευτής να έχει συντριπτική πιθανότητα να διαγνώσει το λάθος. Η μέθοδος αυτή βασίζεται σε τεχνικές κωδίκων διόρθωσης λαθών (error correcting codes).

Μέτρητικές Κλάσεις Ι

Μετρητικές κλάσεις ορίζονται με βάση το πλήθος των λύσεων που έχει κάποιο πρόβλημα. Πρόκειται δηλαδή για κλάσεις συναρτήσεων (όπως η FP). Ενδιαφέρον έχουν οι παρακάτω δύο κλάσεις:

Ορισμός

#P είναι η κλάση των συναρτήσεων f για τις οποίες υπάρχει μη ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου, το υπολογιστικό δέντρο της οποίας έχει ακριβώς $f(x)$ υπολογιστικά μονοπάτια που αποδέχονται (για είσοδο x).

Ορισμός

#L είναι η κλάση των συναρτήσεων f για τις οποίες υπάρχει μη ντετερμινιστική μηχανή Turing λογαριθμικού χώρου, το υπολογιστικό δέντρο της οποίας έχει ακριβώς $f(x)$ υπολογιστικά μονοπάτια που αποδέχονται (για είσοδο x).

Μέτρητικές Κλάσεις II

Σε μετρητικές κλάσεις χρήσιμες είναι αναγωγές που διατηρούν το πλήθος των λύσεων.

Ένα χαρακτηριστικό παράδειγμα πλήρους προβλήματος για την #P είναι το πρόβλημα #SAT: «Δίνεται τύπος σε συζευκτική κανονική μορφή. Πόσες διαφορετικές αναθέσεις υπάρχουν που ικανοποιούν τον τύπο;». Είναι προφανές ότι $\varphi \in \text{SAT}$ ανν $\#\text{SAT}(\varphi) \neq 0$.

Ο *Valiant* έδειξε ότι υπάρχουν προβλήματα απόφασης στο P (π.χ. ύπαρξη τέλειου ταιριάσματος σε γραφήματα) των οποίων το αντίστοιχο μετρητικό πρόβλημα (π.χ. *#PERFECT MATCHINGS*) είναι #P-πλήρες.

Μερικά αποτελέσματα για αυτές τις κλάσεις:

$$\text{FP} \subseteq \#\text{P} \subseteq \text{FPSPACE}, \quad \text{P}^{\text{PP}} = \text{P}^{\#\text{P}}, \quad \text{FL} \subseteq \#\text{L} \subseteq \text{FNC}^2.$$

Μέτρητικές Κλάσεις III

Θεώρημα (*Toda*)

$\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Η απόδειξη αποτελείται από δύο βασικούς εγκλεισμούς, όπως φαίνεται στα παρακάτω λήμματα:

Lemma

$\mathbf{PH} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$.

Απόδειξη:

1. $\oplus\mathbf{P}^{\oplus\mathbf{P}} = \oplus\mathbf{P}$ (Papadimitriou-Zachos)
2. $\mathbf{NP} \subseteq \mathbf{BPP} \Rightarrow \mathbf{PH} \subseteq \mathbf{BPP}$ (Zachos)
3. $\mathbf{NP} \subseteq \mathbf{RP}^{\oplus\mathbf{P}}$ (Valiant-Vazirani) $\subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$

Μέτρητικές Κλάσεις IV

4. $\mathbf{NP}^{\oplus\mathbf{P}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}^{\oplus\mathbf{P}}}$ (3. με μαντείο $\oplus\mathbf{P}$) $\overset{1.}{\Rightarrow} \mathbf{NP}^{\oplus\mathbf{P}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$
5. $\mathbf{NP}^{\oplus\mathbf{P}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}} \Rightarrow \mathbf{PH}^{\oplus\mathbf{P}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$ (2. με μαντείο $\oplus\mathbf{P}$)
6. $\mathbf{PH}^{\oplus\mathbf{P}} = \mathbf{PH} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$

□

Lemma

$\mathbf{BPP}^{\oplus\mathbf{P}} \subseteq \mathbf{P}^{\#\mathbf{P}}$

Χωρίς απόδειξη.

□