# Διαλογικά Συστήματα Αποδείξεων

Αντώνης Αντωνόπουλος

*Κρυπτογραφία & Πολυπλοκότητα*

17/2/2012

- Επέκταση του **NP** συστήματος αποδείξεων εισάγωντας αλληλεπίδραση!
- Ένα άτομο προσπαθεί να πείσει ένα άλλο για το ότι μία συμβολοσειρά ανήκει σε μία γλώσσα.

## Ορισμός

Μία γλώσσα $L \subseteq \{0,1\}^*$ ανήκει στην κλάση $\mathbf{IP}[k]$ αν υπάρχει $k$ (το οποίο μπορεί να εξαρτάται από το μήκος της εισόδου), και μία Πιθανοτική Μηχανή Turing $V$ που μπορεί να έχει μία διαλογική διαδικασία $k$ γύρων με κάποια **NP**-Μηχανή Turing $P$, που να ικανοποιεί τις εξής συνθήκες:

- (*Completeness*) Αν $x \in L$: **υπάρχει** $P$ τέτοιος ώστε $\mathbf{Pr}\left[\langle P, V\rangle(x) = 1\right] \geq \frac{2}{3}$
- (*Soundness*) Αν $x \notin L$: **για κάθε** $P$ ισχύει ότι $\mathbf{Pr}\left[\langle P, V\rangle(x) = 1\right] \leq \frac{1}{3}$

- Αν ο verifier είναι μία ντετερμινιστική μηχανή Turing, τότε έχουμε ακριβώς την περιγραφή της κλάσης **NP**, που είδαμε παραπάνω. Αν όμως επιτρέψουμε στον verifier την χρήση τυχαιότητας, μπορούμε να υπολογίσουμε πολύ περισσότερες γλώσσες.
- $\mathbf{NP} \subseteq \mathbf{IP}$
- $\mathbf{BPP} \subseteq \mathbf{IP}$
- Οι πιθανότητες αποδοχής και απόρριψης βασίζονται μόνο στα τυχαία bits που χρησιμοποιεί ο Verifier και δεν μπορεί να τις επηρεάσει ο Prover.
- Τα bits του Verifier κρατώνται 'μυστικά' από τον Prover.

## Ορισμός

Δύο γράφοι $G_1$ και $G_2$ είναι *ισομορφικοί*, αν υπάρχει μια μετάθεση $\pi$ των ονομάτων των κόμβων του $G_1$, τέτοιος ώστε $\pi(G_1) = G_2$. Αν $G_1$ και $G_2$ είναι ισομορφικοί, το συμβολίζουμε με $G_1 \cong G_2$.

Με βάση τα παραπάνω, ορίζουμε τα προβλήματα:

- `GI` (Graph Isomorphism): Δίνονται δύο γράφοι $G_1, G_2$, είναι ισομορφικοί;
- `GNI` (Graph Non-Isomorphism):: Δίνονται δύο γράφοι $G_1, G_2$, είναι *μη*-ισομορφικοί;

- `GI` $\in$ **NP**, αφού ένα συνοπτικό πιστοποιητικό για τον ισομορφισμό είναι η μετάθεση $\pi$.
- Ομοίως, **GNI** ανήκει στο *co***NP**, ως το συμπλήρωμα του `GI`.

Verifier: Διαλέγει τυχαία ένα $i \in \{1, 2\}$, και μεταθέτει τυχαία τις κορυφές του $G_i$ και παίρνει έναν νέο γράφο $H$.
Στέλνει τον $H$ στον Prover.
Prover: Διακρίνει ποιός από τους $G_1$, $G_2$ χρησιμοποιήθηκε για να παράγει τον $H$.
Έστω $G_j$ αυτός ο γράφος.
Στέλνει το $j$ στον $V$.
Verifier: Αποδέχεται αν $i = j$. Απορρίπτει αλλιώς.

- Αν $G_1 \ncong G_2$, τότε ο Prover μπορεί να μαντέψει ποιός από τους δύο γράφους είναι ισομορφικός με τον $H$, και έτσι ο Verifier αποδέχεται με πιθανότητα 1.
- Αν $G_1 \cong G_2$, ο Prover δεν μπορεί να ξεχωρίσει τους δύο γράφους. Έτσι, το καλύτερο που μπορεί να κάνει είναι να διαλέξει στην τύχη έναν γράφο, και ο Verifier αποδέχεται με πιθανότητα $1/2$.

- Στην παραλλαγή των Διαλογικών Αποδείξεων που ονομάζεται παιχνίδια Arthur-Merlin τα τυχαία bits αποκαλύπτονται στον Prover.
- Ο Merlin δεν μπορεί να προβλέψει τα μελλοντικά τυχαία bits του Βασιλιά Αρθούρου, και ο Αρθούρος δεν έχει τρόπο να κρύψει από τον Merlin τα προηγούμενα τυχαία bits του.
- Ο Merlin παίζει τον ρόλο του Prover ,και ο Αρθούρος τον ρόλο του Verifier, αλλά σε αυτή την περίπτωση, ο Merlin έχει περισσότερη δύναμη από τον κανονικό Prover.
- Η κλάση **AM** είναι η κλάση των γλωσσών $L$ με ένα Διαλογικό Σύστημα Αποδείξεων, στο οποίο ο Verifier στέλνει μια τυχαία συμβολοσειρά, και ο Prover απαντάει με ένα μήνυμα.
- Επίσης, η κλάση **MA** αποτελείται από όλες τις γλώσσες $L$, για τις οποίες υπάρχει ένα Διαλογικό Σύστημα Αποδείξεων στο οποίο ο Prover στέλνει πρώτος ένα μήνυμα.

- Η έξοδος $\langle V, P \rangle(x)$ είναι τυχαία μεταβλητή.
- Κάθε γλώσσα στο **PSPACE** έχει Διαλογικό Σύστημα Αποδείξης.
- Μπορούμε να αντικαταστήσουμε την πιθανότητα $2/3$ με $1 - 2^{-n^s}$ και την πιθανότητα (της ορθότητας) $1/3$ με $2^{-n^s}$, χωρίς να αλλάζει η κλάση, για κάθε σταθερά $s > 0$.
- Μπορούμε επίσης να αλλάξουμε την πιθανότητα (της πληρότητας) $2/3$ με $1$ χωρίς να αλλάζει η κλάση, αλλά το να αλλάξουμε την πιθανότητα (της ορθότητας) $1/3$ με $0$, ισοδυναμεί με έναν μη-πιθανοτικό Verifier, και η κλάση **IP** καταρρέει στην **NP**.
- $\mathbf{MA}[1] = \mathbf{NP}$, $\mathbf{AM}[1] = \mathbf{BPP}$, και ότι η κλάση **AM**
- $\mathbf{AM} = \mathbf{BP} \cdot \mathbf{NP}$
- Για σταθερές $k \geq 2$, $\mathbf{AM}[k] = \mathbf{AM}[2]$.
- $\mathbf{IP}[k] \subseteq \mathbf{AM}[k+2]$
- $\mathtt{GNI} \in \mathbf{AM}$

- Μια απόδειξη μηδενικής γνώσης δεν συνεπάγει τίποτα άλλο πέρα από την εγκυρότητά της.
- Ο όρος 'μηδενική' γνώση οφείλεται στο ότι το παραπάνω μπορεί να μεταφραστεί ως την σωστή επιλογή του prover έναντι στις προσπάθειες του verifier να αποκτήσει πληροφορίες μέσω της αλληλεπίδρασης.
- Πολυωνυμικά μη-διακρίσιμα σύνολα μπορούν να θεωρούνται ίσα για όλους τους πρακτικούς σκοπούς, αφού κάθε πολυωνυμική διαδικασία που χρησιμοποιεί ένα από τα δύο σύνολα παρουσιάζει την ίδια συμπεριφορά.

## Ορισμός

Έστω $L \subseteq \{0,1\}^*$. Οι οικογένειες $\Pi_1 = \{\pi_1(x)\}_{x \in L}$ και $\Pi_2 = \{\pi_2(x)\}_{x \in L}$ λέγονται οικογένειες κατανομών πιθανότητας αν κάθε $\pi_i(x)$ για $i \in \{1,2\}$ και $x \in L$ αποτελεί τυχαία μεταβλητή. Για κάθε αλγόριθμο $A$, έστω $p_i^A$ η πιθανότητα ο $A$ να βγάζει έξοδο 1 με είσοδο $x$ και ένα στοιχείο επιλεγμένο σύμφωνα με την κατανομή $\pi_i(x)$:

$$p_i^A = \sum_{\alpha} \mathbf{Pr}\left[A(x,\alpha) = 1\right] \cdot \mathbf{Pr}\left[\pi_i(x) = \alpha\right]$$

Τα σύνολα $\Pi_1$ και $\Pi_2$ λέγονται πολυωνυμικά ή υπολογιστικά μη-διακρίσιμα, αν για κάθε πιθανοτικό αλγόριθμο $A$ και $c > 0$ και για κάθε (αρκετά μεγάλο) $n = |x|, x \in L$:

$$|p_1^A(x) - p_2^A(x)| \leq |x|^{-c}$$

Δίνονται δύο γράφοι $G_1$, $G_2$ (κοινή είσοδος):
(Έστω $\phi$ ο ισομορφισμός μεταξύ των γράφων ($G_2 = \phi(G_1)$) )

Prover: Παράγει ένα γράφο $H$, ο οποίος είναι τυχαίος ισομορφισμός του $G_1$. Αυτό γίνεται ως εξής:
Επιλέγει μία μετάθεση $\pi$, και υπολογίζει τον $H = \pi(G_1)$.
Στέλνει τον $H$ στον verifier.
Verifier: Διαλέγει τυχαία ένα $\alpha \in \{1, 2\}$, και το στέλνει στον Prover.
(Διαισθητικά, ο Verifier ζητάει από τον Prover να του αποδείξει ότι οι $H$ και $G_\alpha$ είναι όντως ισομορφικοί.)
Prover: Αν $\alpha = 2$, τότε ο Prover στέλνει το $\pi$ στον Verifier, αλλιώς του στέλνει την μετάθεση $\pi \cdot \phi$.
Verifier: Αν η μετάθεση $\psi$ που έστειλε ο Prover **δεν** είναι ισομορφισμός μεταξύ των $G_\alpha$ και $H$ (δηλ. $H \neq \psi(G_\alpha)$), τότε ο Verifier σταματάει και *απορρίπτει*. Αλλιώς, συνεχίζει.
Αν ο Verifier έχει ολοκληρώσει $m$ επαναλήψεις των παραπάνω βημάτων, τότε *αποδέχεται*.

- Το πρωτόκολλο αυτό συνιστά ένα Διαλογικό Σύστημα Μηδενικής Γνώσης για το GI.

- $view_{P,V}$: εικόνα που έχει ο Verifier κατά την εκτέλεση του πρωτοκόλλου.

**Ορισμός**

Τα σύνολα $\Pi_1$ και $\Pi_2$ λέγονται στατιστικά μη-διακρίσιμα, αν για κάθε $c > 0$ και $n = |x|, x \in L$ αρκετά μεγάλα:

$$|\mathbf{Pr}[\pi_1(x) = \alpha] - \mathbf{Pr}[\pi_2(x) = \alpha]| \leq |x|^{-c}$$

**Ορισμός**

Τα σύνολα $\Pi_1$ και $\Pi_2$ λέγονται τέλεια μη-διακρίσιμα, αν για κάθε $x \in L$ οι κατανομές $\pi_1(x)$ και $\pi_2(x)$ ταυτίζονται.

## Ορισμός

Ένα Διαλογικό Πρωτόκολλο είναι πρωτόκολλο:

- τέλειας μηδενικής γνώσης για μια γλώσσα $L$, αν για κάθε «ανέντιμο» Verifier $V'$ υπάρχει πιθανοτικός αλγόριθμος $A$ πολυωνυμικού χρόνου, τέτοιος ώστε τα σύνολα $\{view_{P,V'}(x)\}_{x\in L}$ και $\{A(x)\}_{x\in L}$ να είναι τέλεια μη-διακρίσιμα.
- στατιστικής μηδενικής γνώσης, αν είναι στατιστικά μη-διακρίσιμα.
- υπολογιστικής μηδενικής γνώσης, αν είναι υπολογιστικά/πολυωνυμικά μη-διακρίσιμα.

$$\mathbf{PZK} \subseteq \mathbf{SZK} \subseteq \mathbf{CZK} \subseteq \mathbf{IP}$$

# Περαιτέρω Μελέτη


- Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 1st edition, April 2009
- Oded Goldreich, Silvio Micali, Avi Wigderson: Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. J. ACM 38(3): 691-729 (1991)
- Shafi Goldwasser, Silvio Micali, Charles Rackoff: The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comput. 18(1): 186-208 (1989)
- Στάθης Ζάχος, Κρυπτογραφία και Πολυπλοκότητα, Ε.Μ.Π., Αθήνα 2007


**Thank You!**