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

$L \in \text{IP}$:

- $x \in L \implies$ 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.

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

Διαλογική αλληλεπίδραση (interactivity) III

Διαλογικά συστήματα αποδείξεων (IP)

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.

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

Διαλογική αλληλεπίδραση (interactivity) IV

Διαλογικά συστήματα αποδείξεων (IP)

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 $x \in L$.

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

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

Διαλογική αλληλεπίδραση (interactivity) III

Κλάσεις Arthur-Merlin

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:

Πρόταση

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

Διαλογική αλληλεπίδραση (interactivity) IV

Κλάσεις Arthur-Merlin

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

$L \in \mathrm{PCP}$:

- $x \in L \implies$ 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.

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

Διαλογική αλληλεπίδραση (interactivity) II

Probabilistic Checable Proofs — PCP

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).

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:

Διαλογική αλληλεπίδραση (interactivity) III

Probabilistic Checable Proofs — PCP

Θεώρημα (PCP)

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

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).