Κάτω Φράγματα

από το Descriptive Complexity του Neil Immerman

Νικόλαος Διαμαντής

Αλγόριθμοι, Λογική και Διακριτά Μαθηματικά

12/06/2023

Περιεχόμενα

Το πρόβλημα PARITY

- Είναι αληθές όταν η συμβολοσειρά που δίνεται ως είσοδος περιέχει περιττό πλήθος από '1'.
- Έχουμε δει ότι το πρόβλημα δεν είναι ανήκει στην FO.

Το πρόβλημα PARITY

- Είναι αληθές όταν η συμβολοσειρά που δίνεται ως είσοδος περιέχει περιττό πλήθος από '1'.
- Έχουμε δει ότι το πρόβλημα δεν είναι ανήκει στην FO.

Μπορούμε καλύτερα;

Ανάθεση Τιμών

Έστω συνάρτηση $f \to \{0,1\}^*$ με δυαδικές μεταβλητές $V_n = \{x_1, ..., x_n\}$. Περιορίζουμε το V_n με μια αντιστοίχηση $\rho : V_n \to \{0, 1, \star\}$.

Το αποτέλεσμα της ανάθεσης ρ στην f είναι η $f|_\rho$:

- Οι τιμές $\rho(x_i)$ έχουν αντικαταστήσει τις μεταβλητές x_i στην f, για κάθε x_i τέτοιο ώστε $\rho(x_i) \neq \star$.
- Η $f|_\rho$ είναι μια συνάρτηση των μεταβλητών οι οποίες έχουν πάρει τιμή '$\star$'.
- Ορίζουμε $\mathcal{R}_n^r$ το σύνολο όλων των πιθανών αναθέσεων τιμών στο V_n, τέτοιες ώστε να αντιστοιχίζουν ακριβώς r μεταβλητές στην τιμή '$\star$'.

Δένδρα Απόφασης

Έστω πρόταση F σε κανονική διαζευκτική μορφή (DNF).

Ορίζουμε το δένδρο απόφασης $T(F)$ ως εξής:

- Έστω $C_1 = l_1 \wedge \ldots \wedge l_i$ ο πρώτος όρος της F.
  - $F = C_1 \vee F'$
- Η ρίζα του $T(F)$ είναι ένα πλήρες δυαδικό δένδρο απόφασης για τις μεταβλητές της C_1.
- Κάθε φύλο του δέντρου καθορίζει μια ανάθεση ρ η οποία θέτει την κατάλληλη τιμή στις μεταβλητές της C_1 και την τιμή "$\star$" σε όλες τις υπόλοιπες μεταβλητές.
- Υπάρχει μοναδικό φύλλο που κάνει την C_1 αληθή:
  - Το φύλλο αυτό παίρνει τιμή "1".
  - Για κάθε άλλο φύλλο εφαρμόζουμε την ανάθεση ρ και το επεκτείνουμε με το δένδρο απόφασης $T(F'|_\rho)$.

Ύψος του δένδρου

Έστω $h(T)$ το ύψους του δένδρου T.

- Για κάθε DNF πρόταση F η οποία έχει μόνο μικρούς όρους, μπορούμε να διαλέξουμε τυχαία μια ανάθεση $\rho \in \mathcal{R}_n^r$ και με μεγάλη πιθανότητα, το ύψος $h(T(F|_\rho))$ θα είναι μικρό.

Ύψος του δένδρου

Έστω $h(T)$ το ύψους του δένδρου T.

- Για κάθε DNF πρόταση F η οποία έχει μόνο μικρούς όρους, μπορούμε να διαλέξουμε τυχαία μια ανάθεση $\rho \in \mathcal{R}_n^r$ και με μεγάλη πιθανότητα, το ύψος $h(T(F|_\rho))$ θα είναι μικρό.
- Αντίστοιχα, η άρνηση της $F|_\rho$ μπορεί να γραφεί σε DNF ως η διάζευξη των συζεύξεων κάθε διακλάδωσης που καταλήγει σε "0".
  - Επομένως, μια τυχαία ανάθεση μετατρέπει με μεγάλη πιθανότητα μια DNF πρόταση με μόνο μικρούς όρους σε μια CNF.

To Switching Lemma

Håstad's Switching Lemma

Έστω F μια DNF πρόταση με n μεταβλητές, τέτοια ώστε κάθε όρος της να έχει μέγεθος το πολύ k. Έστω $p \leq 1/10, r = pn$ και $s \geq 0$. Τότε:

$$\frac{|\{\rho \in \mathcal{R}_n^r | h(T(F|_\rho)) \geq s\}|}{|\mathcal{R}_n^r|} \leq (10pk)^s.$$

Εναλλακτικά:

$$\Pr[h(T(F|_\rho)) \geq s] \leq (10pk)^s, r \in \mathcal{R}_n^r.$$

Έστω:

- $F = (x_1 \wedge \overline{x_2} \wedge x_4) \vee (x_2 \wedge x_5 \wedge \overline{x_6}) \vee (x_3 \wedge \overline{x_5} \wedge x_7)$
- ρ :

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
ρ	$\star$	1	$\star$	1	$\star$	0	$\star$

Στην πράξη

Έστω:

- $F = (x_1 \wedge \overline{x_2} \wedge x_4) \vee (x_2 \wedge x_5 \wedge \overline{x_6}) \vee (x_3 \wedge \overline{x_5} \wedge x_7)$
- ρ :

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
ρ	$\star$	1	$\star$	1	$\star$	0	$\star$

Έπειτα από την ανάθεση έχουμε:

- $F|_\rho = x_5 \vee (x_3 \wedge \overline{x_5} \wedge x_7)$

Μια πρώτη προσέγγιση

DumbTF(F, ρ):

1. Αν η $F|_\rho$ είναι σταθερή, τότε φτιάξε φύλλο.
2. Βρες τον αριστερότερο όρο που παραμένει μεταβλητή.
3. Τρέξε όλες τις μεταβλητές κάτω από αυτόν.
4. Επανέλαβε μέχρι να ολοκληρωθεί το δένδρο.

Κακές Αναθέσεις

Έστω $\mathcal{B}$ το σύνολο με όλες τις αναθέσεις ρ, τέτοιες ώστε το $\textbf{DumbTF}(F, \rho)$ να έχει ύψος $\geq s$.

Α.ν.δ.ό. $\Pr[\mathcal{B}] \leq (7pk)^s$.

Κακές Αναθέσεις

Έστω $\mathcal{B}$ το σύνολο με όλες τις αναθέσεις ρ, τέτοιες ώστε το **DumbTF**(F, ρ) να έχει ύψος $\geq s$.

Α.ν.δ.ό. $\Pr[\mathcal{B}] \leq (7pk)^s$.

- Παίρνουμε το αριστερότερο μονοπάτι του δένδρου με μήκος $\geq s$.
- Το μονοπάτι αυτό προέκυψε από μια επέκταση της ρ, η οποία σταθεροποίησε επιπλέον s μεταβλητές.
- Αυτή η ανάθεση είναι η Devil(ρ).

Devils and Angels

Devil(ρ): σταθεροποιεί s επιπλέον μεταβλητές από την ρ.

	x_1	x_2	x_3	x_4	x_5	$\dots$
ρ	1	$\star$	0	$\star$	$\star$	$\dots$
Devil(ρ)	1	**0**	0	**0**	**0**	$\dots$
Angel(ρ)	1	**1**	0	**0**	**1**	$\dots$

Angel(ρ): σταθεροποιεί ένα σύνολο από s επιπλέον μεταβλητές $V = V_1 \cup V_2 \cup V_3 \cup \dots$, από την Devil$(\rho)$.

Ποια η πιθανότητα;

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	...
ρ	1	$\star$	0	$\star$	$\star$	1	1	0	$\star$	...
Angel(ρ)	1	**1**	0	**0**	**1**	1	1	0	$\star$	...

Ποια η πιθανότητα;

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	...
ρ	1	$\star$	0	$\star$	$\star$	1	1	0	$\star$	...
Angel(ρ)	1	**1**	0	**0**	**1**	1	1	0	$\star$	...

$$\Pr[\rho] = \left(\frac{1-p}{2}\right)(p)\left(\frac{1-p}{2}\right)(p)(p)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)(p)...$$

$$\Pr[\text{Angel}(\rho)] = \left(\frac{1-p}{2}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{1-p}{2}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{1-p}{2}\right)\left(\frac{1-k}{2}\right)\left(\frac{1-p}{2}\right)(p)...$$

Ποια η πιθανότητα;

$$\Pr[\rho] = \left(\frac{1-p}{2}\right)(p)\left(\frac{1-p}{2}\right)(p)(p)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)(p)\ldots$$

$$\Pr[\text{Angel}(\rho)] = \left(\frac{1-p}{2}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{1-p}{2}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{\mathbf{1-p}}{\mathbf{2}}\right)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)\left(\frac{1-p}{2}\right)(p)\ldots$$

- Παρατηρούμε ότι $\left(\frac{p}{(\frac{\mathbf{1-p}}{\mathbf{2}})}\right)^s \simeq (2p)^s \leq (2.5k)^s$.
  - p πολύ μικρό $\Rightarrow (1-p) \simeq 1$.

Ποια η πιθανότητα;

$$\Pr[\rho] \leq (2.5p)^s \cdot \Pr[\mathrm{Angel}(\rho)]$$

Ποια η πιθανότητα;

$$\Pr[\rho] \leq (2.5p)^s \cdot \Pr[\mathrm{Angel}(\rho)]$$

$$\sum_{\rho \in \mathcal{B}} \Pr[\rho] \leq (2.5p)^s \cdot \sum_{\rho \in \mathcal{B}} \Pr[\mathrm{Angel}(\rho)]$$

Ποια η πιθανότητα;

$$\Pr[\rho] \leq (2.5p)^s \cdot \Pr[\text{Angel}(\rho)]$$

$$\sum_{\rho \in \mathcal{B}} \Pr[\rho] \leq (2.5p)^s \cdot \sum_{\rho \in \mathcal{B}} \Pr[\text{Angel}(\rho)]$$

$$\Rightarrow \sum_{\rho \in \mathcal{B}} \Pr[\rho] \leq (2.5p)^s \cdot (4k)^s \cdot \sum_{\sigma} \Pr[\sigma] = (10pk)^s$$

Ποια η πιθανότητα;

$$\Pr[\rho] \leq (2.5p)^s \cdot \Pr[\mathrm{Angel}(\rho)]$$

$$\sum_{\rho \in \mathcal{B}} \Pr[\rho] \leq (2.5p)^s \cdot \sum_{\rho \in \mathcal{B}} \Pr[\mathrm{Angel}(\rho)]$$

$$\Rightarrow \sum_{\rho \in \mathcal{B}} \Pr[\rho] \leq (2.5p)^s \cdot (4k)^s \cdot \sum_{\sigma} \Pr[\sigma] = (10pk)^s$$

Οποιαδήποτε ανάθεση σ είναι η $\mathrm{Angel}(\cdot)$ από $\leq (4k)^s$ $\rho \in \mathcal{B}$.

Απόδειξη

- Έστω ανάθεση $\sigma = \text{Angel}(\rho)$ και ένα στοιχείο που μοιάζει σαν:

2	3,	2,	3	4,	k,	1	6,	...,	2	5
0	0	0	1	0	1	0	0	...	1	0

  - Μήκος στοιχείου $= s$.
- Θ.δ.ό. ένας πράκτορας μπορεί να ανακτήσει την ρ.

Πιθανές Τιμές

2	3,	2,	3	4,	k,	1	6,	...,	2	5
0	0	0	1	0	1	0	0	...	1	0

Πλήθος πιθανών τιμών για:

- Αριθμούς του σ στο $[1, s]$: k^s
- Bits του στοιχείου: 2^s
- Ύπαρξη ή μη διαχωριστών (",") στο σ: 2^{s-1}

Όλα μαζί: $\leq (4k)^s$ πιθανές τιμές.

Ανακτώντας την ρ

Έστω $\rho \in \mathcal{B}$ και $\sigma = \mathrm{Angel}(\rho)$.
Μπορεί ο πράκτορας να ανακτήσει την ρ από την $\mathrm{Angel}(\rho)$;

Ανακτώντας την ρ

Έστω $\rho \in \mathcal{B}$ και $\sigma = \mathrm{Angel}(\rho)$.
Μπορεί ο πράκτορας να ανακτήσει την ρ από την $\mathrm{Angel}(\rho)$;

Ο πράκτορας αρκεί να ανακτήσει το:

$$V = V_1 \cup V_2 \cup V_3 \cup \ldots$$

Ανακτώντας την ρ

Έστω $\rho \in \mathcal{B}$ και $\sigma = \mathrm{Angel}(\rho)$.
Μπορεί ο πράκτορας να ανακτήσει την ρ από την $\mathrm{Angel}(\rho)$;

Ο πράκτορας αρκεί να ανακτήσει το:

$$V = V_1 \cup V_2 \cup V_3 \cup \dots$$

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \dots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ	0	0	1	1	1	0	1	1	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

Αναζητώντας τον πρώτο όρο

Εφαρμόζουμε τον **DumbTF**(F, ρ):

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ	0	0	1	1	1	0	1	1	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ

Αναζητώντας τον πρώτο όρο

Εφαρμόζουμε τον **DumbTF**(F, ρ):

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$\ldots$
σ	0	0	1	1	1	0	1	1	$\ldots$
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	$\ldots$

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ
- $(\overline{x_1} \wedge \overline{x_2} \wedge x_8)$: παραμένει ουδέτερος από την ρ και ικανοποιείται από την σ

Αναζητώντας τον πρώτο όρο

Εφαρμόζουμε τον $\mathbf{DumbTF}(F, \rho)$:

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ	0	0	1	1	1	0	1	1	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ
- $(\overline{x_1} \wedge \overline{x_2} \wedge x_8)$: παραμένει ουδέτερος από την ρ και ικανοποιείται από την σ
  - Είναι ο αριστερότερος όρος που ικανοποιείται
  - Περιέχει το $V_1 = \{x_2, x_8\}$

Διακρίνοντας τις μεταβλητές

- Από το σ, ο πράκτορας γνωρίζει ότι $V_1 \subseteq \{x_1, x_2, x_8\}$.
- Το στοιχείο θα ξεκαθαρίσει ποιο είναι το V_1, εμφανίζοντας τις θέσεις των μεταβλητών του σε κάθε όρο.

Διακρίνοντας τις μεταβλητές

- Από το σ, ο πράκτορας γνωρίζει ότι $V_1 \subseteq \{x_1, x_2, x_8\}$.
- Το στοιχείο θα ξεκαθαρίσει ποιο είναι το V_1, εμφανίζοντας τις θέσεις των μεταβλητών του σε κάθε όρο.

Στοιχείο:

2	3,	...
0	0	...

- Η πρώτη σειρά αναφέρει τις θέσεις (k) και όχι τα ονόματα των μεταβλητών (n).
- Η δεύτερη αναφέρει τις τιμές που δίνει η ανάθεση Devil(ρ).

Αναζητώντας τον επόμενο όρο

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1
- επαναλαμβάνει και αλλάζει σταδιακά τις τιμές του σ με αυτές του Devil(ρ)

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	1	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

Αναζητώντας τον επόμενο όρο

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1
- επαναλαμβάνει και αλλάζει σταδιακά τις τιμές του σ με αυτές του Devil(ρ)

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	1	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ'

Αναζητώντας τον επόμενο όρο

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1
- επαναλαμβάνει και αλλάζει σταδιακά τις τιμές του σ με αυτές του Devil(ρ)

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	1	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ'
- $(\overline{x_1} \wedge \overline{x_2} \wedge x_8)$: παραμένει ουδέτερος από την ρ, δεν ικανοποιείται από την Devil(ρ), άρα και από την σ'

Αναζητώντας τον επόμενο όρο

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1
- επαναλαμβάνει και αλλάζει σταδιακά τις τιμές του σ με αυτές του Devil(ρ)

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	1	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ'
- $(\overline{x_1} \wedge \overline{x_2} \wedge x_8)$: παραμένει ουδέτερος από την ρ, δεν ικανοποιείται από την Devil(ρ), άρα και από την σ'
- $(\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6})$: ικανοποιείται από την σ'

Αναζητώντας τον επόμενο όρο

Ο πράκτορας:

- γνωρίζει μέχρι στιγμής τα V_1 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για το V_1
- επαναλαμβάνει και αλλάζει σταδιακά τις τιμές του σ με αυτές του Devil(ρ)

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \dots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	1	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

- $(x_1 \wedge \overline{x_2})$: δεν ικανοποιείται ούτε από τη ρ, ούτε από την σ'
- $(\overline{x_1} \wedge \overline{x_2} \wedge x_8)$: παραμένει ουδέτερος από την ρ, δεν ικανοποιείται από την Devil(ρ), άρα και από την σ'
- $(\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6})$: ικανοποιείται από την σ'
  - αφού έχει τα Angel(ρ) bits για το V_2

Διακρίνοντας τις μεταβλητές

$(\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6})$:

- Είναι ο αριστερότερος όρος που ικανοποιείται
- Περιέχει το $V_2 = \{x_4\}$

Διακρίνοντας τις μεταβλητές

$(\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6})$:

- Είναι ο αριστερότερος όρος που ικανοποιείται
- Περιέχει το $V_2 = \{x_4\}$

Ομοίως:

- Ο πράκτορας γνωρίζει από το σ' ότι $V_2 \subseteq \{x_2, x_4, x_5, x_6\}$.
- Το στοιχείο θα ξεκαθαρίσει ποιο είναι το V_2, εμφανίζοντας τις θέσεις των μεταβλητών του σε κάθε όρο.

Διακρίνοντας τις μεταβλητές

$(\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6})$:

- Είναι ο αριστερότερος όρος που ικανοποιείται
- Περιέχει το $V_2 = \{x_4\}$

Ομοίως:

- Ο πράκτορας γνωρίζει από το σ' ότι $V_2 \subseteq \{x_2, x_4, x_5, x_6\}$.
- Το στοιχείο θα ξεκαθαρίσει ποιο είναι το V_2, εμφανίζοντας τις θέσεις των μεταβλητών του σε κάθε όρο.

Στοιχείο:

2	3,	2,	...
0	0	0	...

Η ανάκτηση της ρ

Ο πράκτορας:

- Γνωρίζει μέχρι στιγμής τα V_1, V_2 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για τα V_1, V_2

Η ανάκτηση της ρ

Ο πράκτορας:

- Γνωρίζει μέχρι στιγμής τα V_1, V_2 και σ'
  - σ' : σ αλλά με τα bits της Devil(ρ) για τα V_1, V_2

$$F = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_8) \vee (\overline{x_2} \wedge x_4 \wedge x_5 \wedge \overline{x_6}) \vee \ldots$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	...
σ'	0	**0**	1	**0**	1	0	1	**0**	...
ρ	0	$\star$	1	$\star$	1	0	1	$\star$	...

Η ανάκτηση της ρ

Επαναλαμβάνοντας την διαδικασία για όλους τους όρους, ο πράκτορας:

- Γνωρίζει τα $V_1, V_2, \ldots = V$ και σ'
  - $\sigma' : \sigma = \text{Angel}(\rho)$ αλλά με τα bits της $\text{Devil}(\rho)$ για τα $V_1, V_2, ..., V$

Στοιχείο:

2	3,	2,	3	4,	k,	1	6,	...,	2	5
0	0	0	1	0	1	0	0	...	1	0

Η ανάκτηση της ρ

Επαναλαμβάνοντας την διαδικασία για όλους τους όρους, ο πράκτορας:

- Γνωρίζει τα $V_1, V_2, ... = V$ και σ'
  - $\sigma' : \sigma = \text{Angel}(\rho)$ αλλά με τα bits της $\text{Devil}(\rho)$ για τα $V_1, V_2, ..., V$

Στοιχείο:

2	3,	2,	3	4,	k,	1	6,	...,	2	5
0	0	0	1	0	1	0	0	...	1	0

Ο πράκτορας τελικά ανακτά το ρ θέτοντας $\star$ στις V θέσεις του σ.

Περιεχόμενα

Κάτω φράγματα για το PARITY

Håstad '86

Δένδρα απόφασης για το PARITY με βάθος $d+1$, έχουν μέγεθος $\epsilon^{\Omega(n^{1/d})}$, $\epsilon > 1$.

Αν το PARITY $\in \mathrm{FO}[s(n)]$, τότε $s(n) = \Omega(\log n / \log\log n)$, ακόμα και με την παρουσία αυθαίρετων τιμών (" $\star$ ").

Το πρόβλημα REACH$_\alpha$

REACH$_\alpha$

Έστω εναλλασσόμενο κατευθυνόμενο γράφημα $G = (V, E, A, s, t)$ του οποίου οι κορυφές είναι σημαδεμένες με κάποιον ποσοδείκτη $(\forall, \exists)$. Το $a \subseteq V$ είναι το σύνολο των καθολικών κορυφών. Έστω $\tau_{\alpha g} = \langle E^2, A^1, s, t \rangle$ το λεξιλόγιο των εναλλασσόμενων γραφημάτων. Έστω $P_\alpha^G(x, y)$ η μικρότερη σχέση στις κορυφές του G, τέτοια ώστε:

- $P_\alpha^G(x, x)$.
- Αν η x είναι υπαρξιακή και $P_\alpha^G(z, y)$ ισχύει για κάποια ακμή (x, z), τότε $P_\alpha^G(x, y)$.
- Αν η x είναι καθολική, άρα υπάρχει τουλάχιστον μια ακμή που ¨φεύγει' από την x, και επιπλέον αν η $P_\alpha^G(z, y)$ ισχύει για όλες τις ακμές (x, z), τότε $P_\alpha^G(x, y)$.

$$\mathrm{REACH}_\alpha = \{G | P_\alpha^G(s, t)\}$$

Κάτω φράγμα για το REACH_α

Θεώρημα

Το REACH_α δεν μπορεί να εκφραστεί με βαθμό ποσοδεικτών $2^{\sqrt{\log n}-1}$ σε γλώσσα χωρίς διάταξη.

Κάτω φράγμα για το REACH_α

Θεώρημα

Το REACH_α δεν μπορεί να εκφραστεί με βαθμό ποσοδεικτών $2^{\sqrt{\log n}-1}$ σε γλώσσα χωρίς διάταξη.

Αποδεικτική ιδέα:

Κατασκευάζουμε γραφήματα G_m, H_m τέτοια ώστε:

- $||G_m|| = ||H_m|| < m^{1+\log m}$
- $G_m \sim_m H_m$
- $G_m \in \mathrm{REACH}_\alpha$ και $H_m \notin \mathrm{REACH}_\alpha$

Κάτω φράγμα για Fixed Point και Counting

Θεώρημα

Υπάρχει μια ακολουθία από ζεύγη γραφημάτων $\{A_n, A'_n\}, n \in \mathbb{N}$, τα οποία χρωματίζονται από έναν αλγόριθμο γραμμικού χρόνου και έχουν τις ακόλουθες ιδιότητες:

- A_n, A'_n έχουν $O(n)$ κορυφές.
- A_n, A'_n έχουν βαθμό 3 και χρωματικό αριθμό 4.
- $A_n \equiv_{\mathcal{C}^n} A'_n$.
- A_n, A'_n δεν είναι ισομορφικά μεταξύ τους.

Κάτω φράγμα για Fixed Point και Counting

Θεώρημα

Υπάρχει μια ακολουθία από ζεύγη γραφημάτων $\{A_n, A'_n\}, n \in \mathbb{N}$, τα οποία χρωματίζονται από έναν αλγόριθμο γραμμικού χρόνου και έχουν τις ακόλουθες ιδιότητες:

- A_n, A'_n έχουν $O(n)$ κορυφές.
- A_n, A'_n έχουν βαθμό 3 και χρωματικό αριθμό 4.
- $A_n \equiv_{\mathcal{C}^n} A'_n$.
- A_n, A'_n δεν είναι ισομορφικά μεταξύ τους.

Επακόλουθα

Η FO(wo$\leq$)(LFP,COUNT) περιέχεται αυστηρά σε order-inderpendent πολυωνυμικό χρόνο.

Και μια ιεραρχία

Arity Hierarchy Theorem

Για κάθε $k > 1$, υπάρχει μια φόρμουλα $\phi_k(x_1, ..., x_k, x'_1, ..., x'_k)$ η οποία μπορεί να εκφραστεί σε FO(TC(arrity k)) αλλά όχι σε FO(PFP(arrity $k-1$)), και επομένως ούτε σε FO(LFP(arrity $k-1$)) ή FO(TC(arrity $k-1$)).

Επιπλέον Αναφορές

- Ryan O'Donnell - The Switching Lemma

- Benjamin Rossman - A Switching Lemma Tutorial

Σας ευχαριστώ!