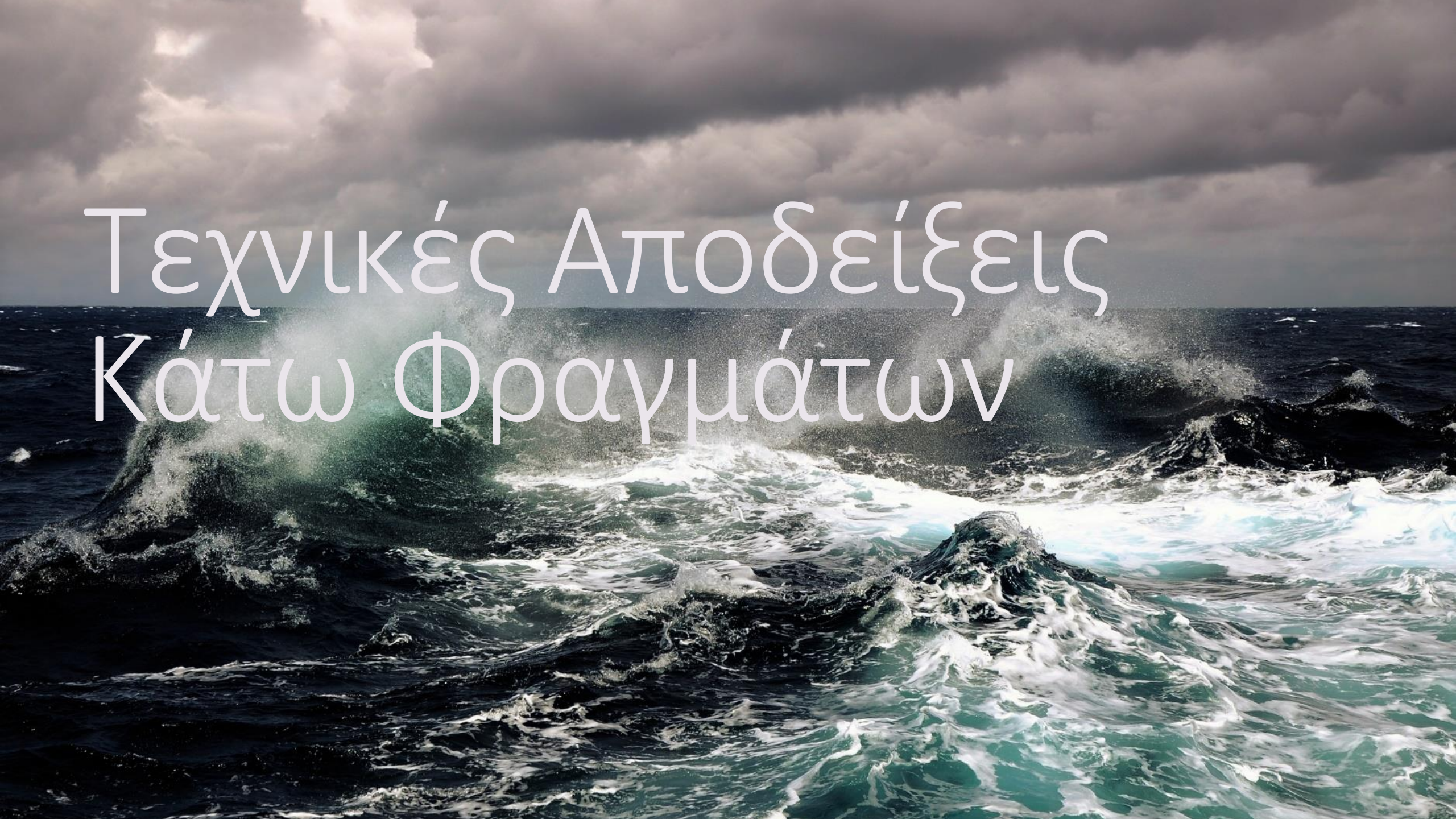


Τεχνικές Αποδείξεις Κάτω Φραγμάτων

Θέλουμε να δείξουμε κυκλωματικά κάτω φράγματα για ομοιόμορφες κλάσεις επειδή:

Δίνουν μεγάλη πληροφορία για τις κλάσεις αυτές: π.χ. αν $EXP \subseteq P_{/poly}$ σημαίνει

- Ότι παρότι δε λύνεται σε πολυωνυμικό χρόνο, το EXP μπορεί να συμπυκνωθεί σε πολυωνυμικό χώρο.
- Ότι για κάθε n, υπάρχει ένα πρόγραμμα μεγέθους και χρόνου $poly(n)$ που λύνει σωστά κάθε EXP στιγμιότυπο μήκους n.

Αν $NEXP \subseteq P_{/poly}$, τότε οι τυχαιοκρατικοί αλγόριθμοι είναι γνησίως πιο ισχυροί από τους ντετερμινιστικούς (προσεχώς…).

Αν $NP \subseteq P_{/poly}$ η πολυωνυμική ιεραρχία καταρρέει στο δεύτερο επίπεδο (προσεχέστερα…).

Απλές ιδέες

Ψάχνουμε όλα τα κυκλώματα μέχρι μεγέθους $S(n)$ και βρίσκουμε το πρώτο που δεν περιέχεται σε αυτά (υπάρχει πάντα ένα για $\mathrm{n} < S(n) < \frac{2^n}{n}$).

Άρα $DTIME[2^{O(S(n)logS(n))}] \nsubseteq SIZE[S(n)]$.

Επομένως $DTIME[2^{n^{\omega(1)}}] \nsubseteq P_{/poly}$.

Τι γίνεται, αναφορικά με το $P_{/poly}$, για κλάσεις όπως τις $EXP, NEXP, \Sigma_2 EXP$;;

Για αρχή $EXP \nsubseteq SIZE[n^k]$...

$\Sigma_3^P \not\subseteq SIZE[n^k]$

Έστω το ακόλουθο πρόβλημα:

Είσοδος: Ένα μήκος 1^n και ένας δείκτης i.

Έξοδος: **Υπάρχει** μια συμβολοσειρά $x \in \{0,1\}^{n^{2k}}$ που

(α) για **κάθε** $y \in \{0,1\}^{n^{2k}}$ με $y < x$ να ισχύει ότι **υπάρχει** ένα κύκλωμα μεγέθους $< n^{k+1}$ το οποίο να παράγει τη y (στο πίνακα αληθείας της) και

(β) ταυτόχρονα **κάθε** κύκλωμα $< n^{k+1}$ δε παράγει τη x (στο TT της) και

(γ) το i-οστό bit της x είναι 1.

Σε μορφή ποσοδεικτών γράφεται $\exists(\forall\exists \wedge \forall)$, οπότε $\Sigma_3^P \not\subseteq SIZE[n^k]$.

Τρέχουσα κατάσταση

$\Sigma_3^{\mathrm{EXP}} \not\subseteq SIZE\left[2^{n^{o(1)}}\right]$

$EXP^{\Sigma_2^{\mathrm{P}}} \subsetneq SIZE\left[2^{n^{o(1)}}\right]$

$\Sigma_2^{EXP} = NEXP^{NP} \not\subseteq SIZE[f(n)]$ για ημι-εκθετική $f\big(f(n)\big) < 2^n$

$MAEXP \not\subseteq P_{/poly}$

Όλες αυτές οι αποδείξεις (με εξαίρεση τη τελευταία) είναι κατά κάποιο τρόπο μετρητικές και στηρίζονται στο γεγονός ότι **υπάρχει** μία συμβολοσειρά που **κάθε** μικρότερο κύκλωμα δε τη παράγει.

Δε δίνει αποτελέσματα για μικρότερες κλάσεις, π.χ. $EXP, NEXP, EXP^{NP}$.

Γενικό Μοτίβο

Για να αποκλείσουμε μια υπολογιστική κλάση $\mathcal{T}$ από μια κυκλωματική $\mathcal{C}$, υπάρχει μια προφανής φυσική μέθοδος:

1. Βρίσκουμε μια «περιοριστική» ιδιότητα για την οποία δείχνουμε ότι τα κυκλώματα της κλάσης $\mathcal{C}$ δεν μπορούν να την έχουν.

2. Βρίσκουμε μια συνάρτηση της $\mathcal{T}$ που να έχει αυτή την ιδιότητα.

3. ???

4. Profit

$PARITY \notin AC^0$

Περιοριστική Ιδιότητα: Υπάρχουν κάποια bits εισόδου, τα οποία όταν σταθεροποιηθούν σε μια τιμή, η συνάρτηση σταθεροποιείται (δεν εξαρτάται πλέον από τα υπόλοιπα bits)

Τετριμμένη περίπτωση: $k - CNF$ (ή $k - DNF$)

Αρκεί, σταθεροποιώντας κάποια bits, να μετατρέψουμε κάθε AC^0 κύκλωμα σε μία $k - CNF$ και τελειώσαμε.

Θεωρούμε αρχικά AC^0 κύκλωμα σε μορφή δέντρου, πύλες μόνο AND, OR (συμπληρώματα μόνο στην είσοδο), όπου κάθε στρώμα έχει μόνο ένα είδος πυλών και ότι τα στρώματα των AND, OR εναλλάσσονται (εν συντομία μορφή δέντρου).

Λήμμα Εναλλαγής (Χόσταντ)

Μέγεθος: n^b, Βάθος: d, **Μορφή Δέντρου**

Αν σταθεροποιήσουμε $n - n^{\varepsilon}$ τυχαία bits εισόδου (σε μια τυχαία τιμή) από μία $k - CNF$, τότε η πιθανότητα να μπορεί να γραφτεί ως $s - DNF$ είναι τουλάχιστον

$$\Pr[\text{H } k - CNF \ \gamma\rho\alpha\varphi\varepsilon\tau\alpha\iota \ \omega\varsigma \ s - DNF] \geq 1 - \left(\frac{k^{10}}{n^{1-\varepsilon}}\right)^{\frac{s}{2}}$$

Αρχικά $k_0 = 1$ και θέτουμε $k_i = 10b * 2^i$ και $\varepsilon = \frac{1}{2}$.

Μείωση βάθους…

Σταθεροποιώντας κάθε φορά $n - \sqrt{n}$ προκύπτει ότι μπορούμε να φράξουμε τη παραπάνω πιθανότητα από $1 - c_1 * n^{-5b}$ (για τη μία πύλη του 2ου στρώματος).

Επομένως μπορούμε σε κάθε στάδιο με πιθανότητα $1 - c_1 n^{-5}$ να μετατρέπουμε τη $k_i - CNF$ του 2ου στρώματος σε $k_{i+1} - DNF$ (ή αντίθετα $k_i - DNF$ σε $k_{i+1} - CNF$) και συμπτύσσοντας την με τη παραπάνω να μειώσουμε το βάθος κατά 1.

Στο τέλος θα έχουμε μια $k_d - CNF$ με $n^{2^{-d}}$ ελεύθερες μεταβλητές.

Άρα με πιθανότητα τουλάχιστον $(1 - c_2 n^{-5})^d > 0$ υπάρχει μια σταθεροποίηση $< n$ bits εισόδου του AC^0 κυκλώματος για την οποία η εναπομείνουσα συνάρτηση είναι σταθερά 1 ή 0.

Κλάση $\mathcal{T}$

Αρκεί να βρούμε μια κλάση, που να έχει μια συνάρτηση, η οποία να μην έχει τη παραπάνω ιδιότητα (να μη σταθεροποιείται όσα bits και να σταθεροποιήσουμε).

Υποψήφιες συναρτήσεις (οτιδήποτε αφορά το $sum = \sum_{i=1}^{n} x_i$ και επαναλαμβάνεται συχνά· το πολύ κάθε n^d φορές (με $d < 1$)):

$PARITY$: $sum \equiv 0 \ (mod\ 2)$

MOD_k: $sum \equiv 0 \ (mod\ k)$

$PRIME\_SUM$ (με κατάλληλη αλλαγή παραμέτρων και επειδή $g_n = p_n - p_{n-1} \leq n^{0.525}$): $sum \in \mathbb{P}$

Z_INTRP: Το sum είναι αύξων αριθμός διαφάνειας που θα διακόψει ο κος Ζάχος.

Κλάσεις: P, L, TC^0, ACC^0

$ACC^0(p) \nsubseteq ACC^0(q)$

Με μια παρόμοιας λογικής (τεχνική-συνδυαστική) απόδειξη προκύπτει ότι για κάθε δύο πρώτους $p \neq q$

υπάρχει ένα σχετικά μικρό πολυώνυμο στο $GF(q)$ που προσομοιώνει καλά το $ACC^0(q)$ και

ότι δεν υπάρχει κανένα (τέτοιου μικρού μεγέθους) που να υπολογίζει τη MOD_p.

Άρα ισχύει $ACC^0(p) \nsubseteq ACC^0(q)$ για οποιουσδήποτε διαφορετικούς p, q.

Δε γνωρίζουμε τι γίνεται όταν έχουμε δύο πρώτους μαζί…

Ακόμη και για $p = 2,\ q = 3$ θα μπορούσε με τη τρέχουσα γνώση να ισχύει ότι $ACC^0 \subseteq ACC^0(6)$ ή κι ότι $NP \subseteq ACC^0(6)$.

Ζητείται ελπίς...

Χρειαζόμαστε μια πιο σύνθετη ιδιότητα για να δείξουμε κάτω φράγματα για το γενικό ACC^0.

Δεδομένου ότι (μέχρι πριν λίγο καιρό) ήταν άγνωστο αν ολόκληρο $NEXP$ μπορούσε να γραφτεί με ACC^0 κυκλώματα, οποιαδήποτε ιδιότητα (που είναι έστω και λίγο περιοριστική) είναι ευπρόσδεκτη – π.χ. ότι είναι υποσύνολο κάποιας σχετικά απλής κλάσης χωρίς modula κλπ.

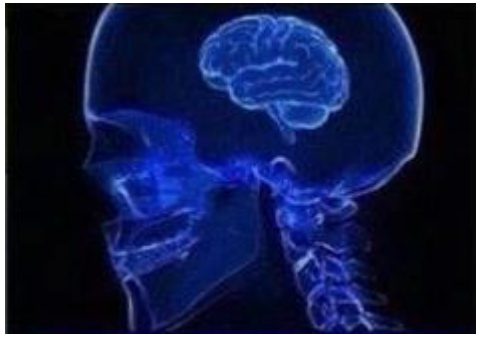
Γνωρίζουμε ότι είναι υποσύνολο του TC^0.

Αλλά δε γνωρίζουμε τίποτα πολύ χρήσιμο για το TC^0, επειδή κι αυτό είναι δύσκολο.

Αρκεί να βρούμε μια πιο εύκολη κλάση από την TC^0, η οποία να είναι αρκετά απλή ώστε να μπορούμε να κάνουμε αποδείξεις με αυτήν και αρκετά σύνθετη ώστε να περιέχει όλο το ACC^0...

Σε κάθε περίπτωση θα της δώσουμε το τυχαίο όνομα SYM+.

SYM+ κυκλώματα (ως κυκλώματα)



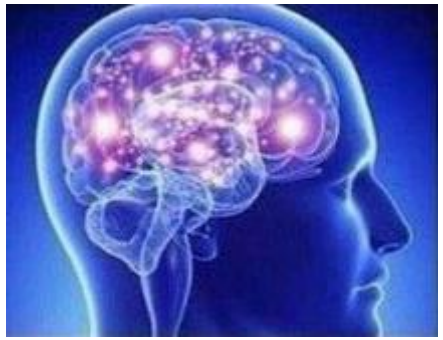
SYM+ λέγεται ένα κύκλωμα που:

Έχει βάθος 2.

Το πρώτο στρώμα αποτελείται μόνο από πύλες AND (με δεδομένα τα συμπληρώματα).

Το δεύτερο στρώμα αποτελείται από μια συμμετρική πύλη (η οποία εξαρτάται μόνο από το $sum = \sum_{i=1}^{n} x_i$).

SYM+ κυκλώματα (ως πολυώνυμα)



Ισοδύναμα ένα SYM+ κύκλωμα χαρακτηρίζεται από:

Ένα πολυώνυμο

$$P(x_1, \dots, x_n) = \sum_{y \in \{0,1\}^n} \hat{P}[y] \prod_{i=1}^{n} x_i^{y_i}$$

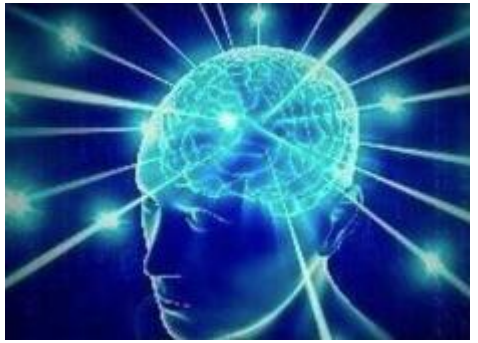
Μία συνάρτηση $\Theta\colon \mathbb{Z} \to \{0,1\}$, τέτοια ώστε $x \in L$ αν και μόνο αν $\Theta\big(P(x_1, \dots, x_n)\big) = 1$.

Ορίζουμε:

ως βαθμό D του SYM+ κυκλώματος τον βαθμό του αντίστοιχου P (ο οποίος αντιστοιχεί στο μέγιστο fan-in των AND πυλών)

ως έκταση s του SYM+ κυκλώματος το μέγιστο συντελεστή $\max|\hat{P}[y]|$ του κυκλώματος

SYM+ κυκλώματα (ως πίνακες)



Ισοδύναμα ένα SYM+ κύκλωμα χαρακτηρίζεται από:

Ένα πολυώνυμο

$$P(x_1, \dots, x_n) = \sum_{y \in \{0,1\}^n} \hat{P}[y] \prod_{i=1}^{n} x_i^{y_i}$$

Μία συνάρτηση $\Theta\colon \mathbb{Z} \to \{0,1\}$, τέτοια ώστε $x \in L$ αν και μόνο αν $\Theta\big(P(x_1, \dots, x_n)\big) = 1$.

Για ένα SYM+ κυκλώματος βαθμού D και έκτασης $s = max\,|\hat{P}[y]|$ έχουμε ότι ο $\hat{P}$ έχει μέγεθος n^D και ότι $max|P(x_1, \dots, x_n)| \leq n^D * s$.

Άρα αρκούν για τη πλήρη περιγραφή του οι πίνακες $\hat{P}$ και Θ μεγέθους $O(n^D)$ και $O(n^D * s)$ αντίστοιχα.

Τα ACC^0 μετατρέπονται σε SYM+ [Yao, Beigel-Tarui]

Μπορούμε να μετατρέψουμε ένα ACC^0 κύκλωμα n εισόδων και μεγέθους S σε ένα SYM+ κύκλωμα βαθμού $\log^a S$ και έκτασης $2^{\log^a S}$.

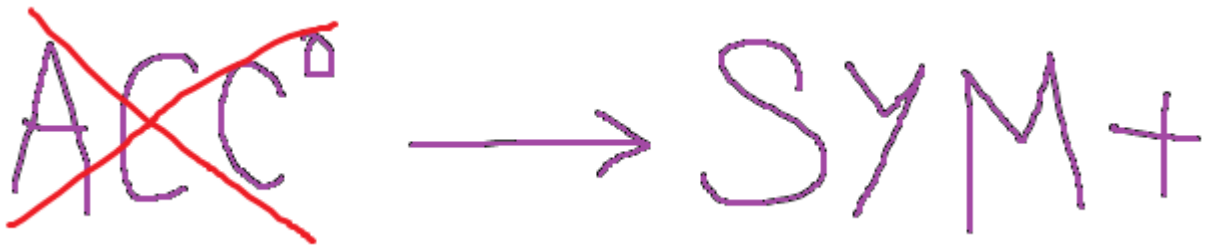
Και μπορούμε να το κάνουμε σε χρόνο $2^{O(\log^a S)}$!

Σημείωση: Το a είναι συνάρτηση **MONO** του d, δηλαδή $a = a(d) > 0$.

Σχέδιο της Απόδειξης μετατροπής του ACC^0 σε SYM+

Σχέδιο της Απόδειξης μετατροπής του ACC^0 σε SYM+

Σχέδιο της Απόδειξης μετατροπής του ACC^0 σε SYM+



(Επιτρέπουμε μόνο πύλες OR και MOD διατηρώντας πάντα μορφή δέντρου).

1. Παίρνουμε $polylog(n)$ τυχαία bits των πυλών OR (από έναν δειγματικό χώρο μεγέθους $2^{polylog(S)}$) με τρόπο τέτοιο ώστε να υπάρχει καλή πιθανότητα το τελικό αποτέλεσμα να ισούται με το αρχικό.

2. Μετατρέπουμε το κύκλωμα σε αριθμητικό όπου οι πύλες πολλαπλασιασμού έχουν fan-in το πολύ $polylog(n)$
   1. $OR(x_1, \dots, x_k) = 1 - (1 - x_1) * \cdots * (1 - x_k)$ και
   2. $MOD_p(x_1, \dots, x_n) = (\sum_{i=1}^{n} x_i)^{p-1} \ (mod p)$

   Σπρώχνουμε τα πάντα ώστε οι πύλες πολλαπλασιασμού να είναι στο πρώτο στρώμα με fan-in πάλι $polylog(n)$, τα επόμενα στρώματα να είναι μόνο πύλες MOD και στην κορυφή μόνο ο αθροιστής.

3. Διώχνουμε στρώμα-στρώμα τις MOD_p μετατρέποντας τη Θ σε $\Theta'(y) = \Theta(y(\mathrm{mod} p))$ (για πολλές πύλες MOD_p παίρνουμε modulus amplifying polynomials).

Και τώρα το καλό…

Έστω ένα ACC^0 κύκλωμα C με n εισόδους, βάθους d και μεγέθους $S \leq 2^{n^\delta}$ για κάποιο $\delta = \delta(d) > 0$ που θα προσδιορίσουμε προσεχώς.

Τότε το $ACC^0 - SAT$ για το παραπάνω στιγμιότυπο λύνεται σε χρόνο 2^{n-n^δ}.

Απόδειξη

Α. Μετατρέπουμε το κύκλωμα C σε ένα ACC^0 C' με $n' = n - 2n^\delta$ εισόδους.

Β. Χρησιμοποιούμε το προηγούμενο Λήμμα, ώστε να μετατρέψουμε το C' σε ένα ισοδύναμο SYM+ βαθμού $\sqrt{n}$, έκτασης $2^{\sqrt{n}}$ και $n' = n - 2n^\delta$ εισόδων.

Γ. Χρησιμοποιούμε δυναμικό προγραμματισμό για να βρούμε αν ικανοποιείται το παραπάνω SYM+ σε χρόνο $2^{n'} poly(n) \ll 2^{n-n^\delta}$.

Α. Μείωση Εισόδων

Φτιάχνουμε το

$$C'(x_1, \dots, x_{n'}) = \bigvee_{x_{n'+1}, \dots, x_n} C(x_1, \dots, x_{n'}, \quad x_{n'+1} \dots, x_n)$$

Το C' έχει μέγεθος $S' = 2^{2n^\delta} * S \leq 2^{3n^\delta}$ και βάθος $d + 1$ και ισχύει ότι είναι ικανοποιήσιμο αν και μόνο αν το C είναι ικανοποιήσιμο.

Ο τετριμμένος αλγόριθμος κάνει $2^{n'} * O(S') = O(2^{n+n^\delta})$ …

Β. Μετατροπή σε SYM+

Θέτουμε $\delta(d) = \frac{1}{3a(d+1)}$ έτσι ώστε $2^{\log^a S'} \leq 2^{\left(3n^{\delta(d+1)}\right)^{a(d+1)}} \leq 2^{\sqrt{n}}$

Άρα μπορούμε (σε χρόνο $2^{O(\sqrt{n})}$) να μετατρέψουμε το προηγούμενο C' σε ένα SYM+ έκτασης $2^{\sqrt{n}}$, βαθμού $\sqrt{n}$ και $n' = n - 2n^{\delta}$ μεταβλητών, έστω το

$$P(x_1, \dots, x_{n'}) = \sum_{y \in \{0,1\}^{n'}} \hat{P}[y] \prod_{i=1}^{n'} x_i^{y_i}$$

μαζί με ένα Θ μεγέθους $2^{\sqrt{n}} * \mathrm{n}^{\sqrt{n}} \ll 2^{\mathrm{n}}$.

Ο τετριμμένος αλγόριθμος θέλει $2^{n'} * n^{\sqrt{n}} * poly(n) \gg 2^n$.

Γ. Δυναμικός Προγραμματισμός

Όμως

$$P(1, x_2, \dots, x_{n'}) = \sum_{y \in \{0,1\}^{n'}} \hat{P}[y] \prod_{i=2}^{n'} x_i^{y_i} = \sum_{y \in \{0,1\}^{n'-1}} \hat{P}[0y] \prod_{i=2}^{n'} x_i^{y_i} + \sum_{y \in \{0,1\}^{n'-1}} \hat{P}[1y] \prod_{i=2}^{n'} x_i^{y_i}$$

Δηλαδή

$$P(1, x_2, \dots, x_{n'}) = P(0, x_2, \dots, x_{n'}) + \check{P}\,(x_2, \dots, x_{n'})$$

για $\check{P}$ το αντίστοιχο πολυώνυμο:

$$\check{P} = \sum_{y \in \{0,1\}^{n'-1}} \hat{P}[1y] \prod_{i=2}^{n'} x_i^{y_i}$$

Γ. Δυναμικός Προγραμματισμός

Έστω $P(\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})$ το διάνυσμα $2^{n'}$ θέσεων που περιλαμβάνει όλες τις τιμές του P.

Επομένως $P(\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}}) = [P(0, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}}), P(1, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})]$

Όπου όμως

$$P(1, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}}) = P(0, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}}) + \check{P}(\boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})$$

Άρα αρκεί να υπολογίσουμε το $P(0, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})$, το $\check{P}(\boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})$ και μετά να κατασκευάσουμε το $P(\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_{n'}})$ σε $O(2^{n'})$ βήματα.

$$T(n') = 2T(n' - 1) + 2^{n'} poly(n)$$

Επομένως τερματίζει σε $2^{n'} * Poly(n)$ βήματα.

Συνολικά:

1. Χρειαστήκαμε $O\left(2^{3n^{\delta}}\right)$ βήματα για την κατασκευή του C' με $n' = n - 2n^{\delta}$ εισόδους.

2. Χρειαστήκαμε $2^{O(\sqrt{n})}$ βήματα για τη μετατροπή του C' σε ένα ισοδύναμο SYM+ (P, Θ).

3. Χρειαστήκαμε $2^{n-2n^{\delta}} poly(n) \ll 2^{n-n^{\delta}}$ βήματα για τον υπολογισμό όλων των τιμών του παραπάνω κυκλώματος (και έλεγχο αν κάποια από αυτές δίνει 1).

Άρα τελειώσαμε σε χρόνο $2^{n-n^{\delta}}$.

Ηθικά διδάγματα:

Αποδεικνύουμε μια τεχνική-συνδυαστική ιδιότητα για τα κυκλώματα της κλάσης $\mathcal{C}$ που δείχνουν ότι δεν έχουν τις ιδιότητες ενός μαύρου κουτιού. Π.χ. σε ένα μαύρο κουτί:

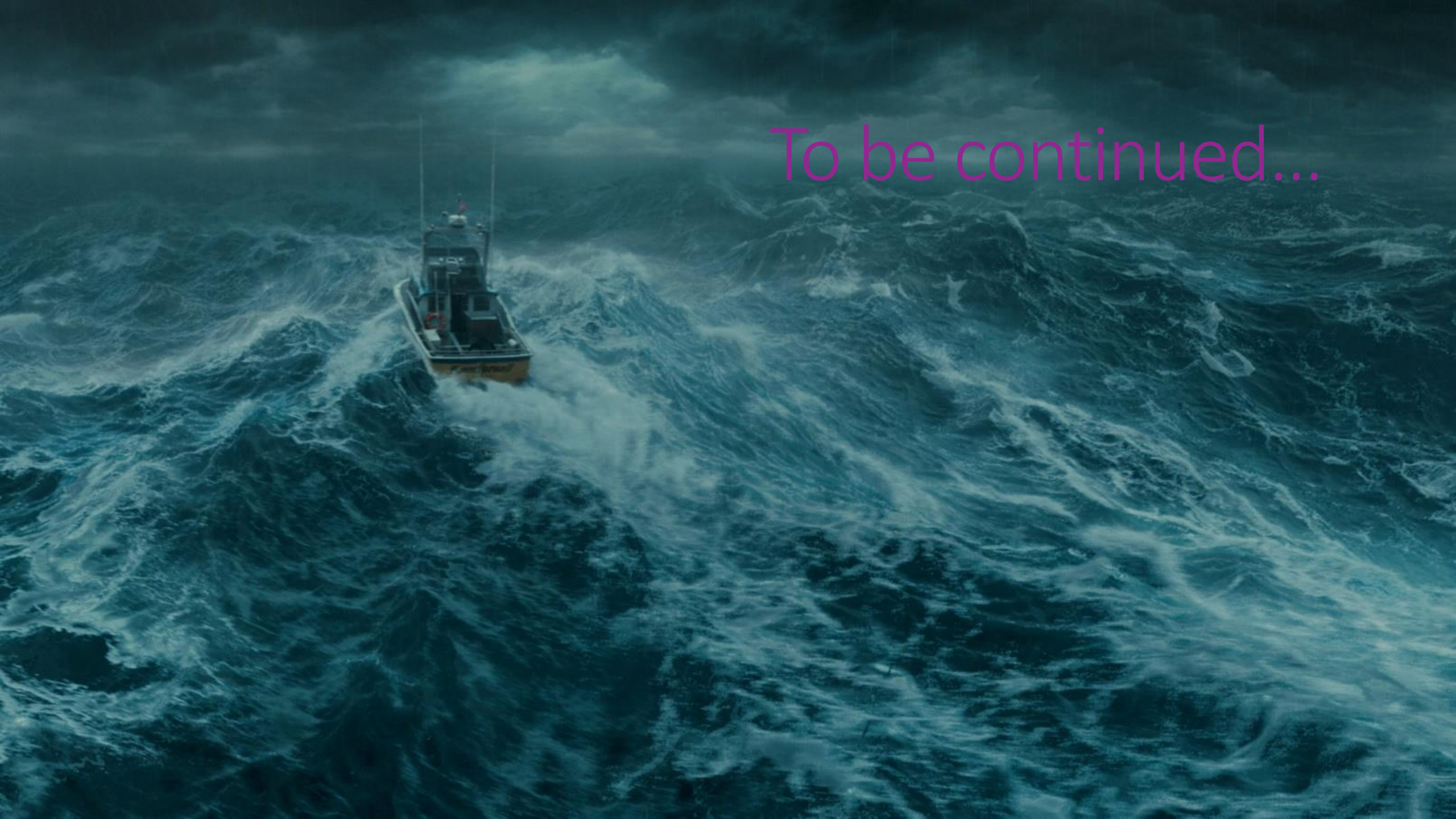
Πρέπει να ψάξουμε όλες τις τιμές του για να δούμε αν υπάρχει κάποια επιλογή bits που σταθεροποιούν την έξοδο του.

Πρέπει να ψάξουμε όλες τις τιμές του για να δούμε αν βγάζει έξοδο 1 *σε κάποια από αυτές.*

Βρίσκουμε μια συνάρτηση μιας ομοιόμορφης κλάσης $\mathcal{T}$ που να μπορεί να υπολογίσει κάτι που αποκλείεται από τη $\mathcal{C}$ (εξαιτίας της παραπάνω ιδιότητας) και καταλήγουμε ότι $\mathcal{T} \nsubseteq \mathcal{C}$.

Αρκεί να βρούμε μια αντίστοιχη τεχνική-συνδυαστική ιδιότητα για το $P_{/poly}$, να δείξουμε ότι το NP (ή όποια άλλη κλάση θέλουμε) την έχει και να καταλήξουμε ότι $NP \nsubseteq P_{/poly}$.

Ή και όχι…


To be continued...