Κυκλώματα και βασικές Ιδιότητες

Κύκλωμα C

Κατευθυνόμενος ακυκλικός γράφος με n πηγές (κάθε μία αντιστοιχεί σε ένα bit εισόδου) και μία καταβόθρα (το bit εξόδου).

Οι ενδιάμεσοι κόμβοι αντιστοιχούν σε κάποια βασική πύλη, οι εισερχόμενες ακμές αντιστοιχούν στις εισόδους της πύλης και οι εξερχόμενες στο αποτέλεσμα της πύλης.

Μέγεθος του κυκλώματος S_C είναι το πλήθος των πυλών και βάθος d_C το μεγαλύτερο μονοπάτι από κάποια πηγή στην καταβόθρα.

Οι πύλες είναι απλές συναρτήσεις κάποιας βάσης (π.χ. AND, OR, NOT) πεπερασμένου ή μη φραγμένου fan-in.

Ανομοιόμορφος Υπολογισμός

Κάθε κύκλωμα αντιστοιχεί σε ένα μήκος εισόδου ⇒ Οικογένεια άπειρων κυκλωμάτων για τον υπολογισμό μίας γλώσσας

$$\bigcup_{n=0}^{\infty} C_n$$

Μπορούν να υπολογίσουν **κάθε** γλώσσα με οικογένειες κυκλωμάτων το πολύ εκθετικού μεγέθους (καλύτερο γνωστό φράγμα $\frac{2^n}{n}\left(1+o(1)\right)$), ή αλλιώς $\forall L$:

$$L \in SIZE[\frac{2^n}{n}]$$

Πιο ισχυρά από μηχανές Turing ⇒ μη ρεαλιστικό μοντέλο!

Χρειαζόμαστε μεγάλα κυκλώματα;

Υπάρχουν 2^{2^n} συναρτήσεις n εισόδων.

Υπάρχουν 2^{SlogS} κυκλώματα μεγέθους S.

Οπότε πρέπει να υπάρχει τουλάχιστον ένα με ελάχιστο μέγεθος $\frac{2^n}{n}$ (άρα το προηγούμενο φράγμα δε βελτιώνεται).

Στην πραγματικότητα σχεδόν όλα είναι τόσο μεγάλα καθώς ακόμη και για $S = \frac{2^n}{n} - c$ είναι

$$\frac{2^{SlogS}}{2^{2^n}} \leq \frac{1}{2}$$

Κυκλωματική Ιεραρχία

Με επιχείρημα παραγεμίσματος (padding) προκύπτει ότι για κάθε $\frac{2^n}{\mathrm{n}} > S_1(n) > 16{,}9 * S_2(n) > n$ είναι

$$\mathrm{SIZE}[\mathrm{S}_2(\mathrm{n})] \subsetneq \mathrm{SIZE}[\mathrm{S}_1(\mathrm{n})]$$

Μάλιστα, το $\mathrm{SIZE}[\mathrm{S}_1(\mathrm{n})]$ έχει εκθετικά περισσότερες συναρτήσεις από το $\mathrm{SIZE}[\mathrm{S}_2(\mathrm{n})]$!

Οπότε ας ορίσουμε κλάσεις!

Πιο διάσημη:

$$P_{/poly} = \bigcup_{c>0} SIZE[n^c]$$

«εφικτός ανομοιόμορφος υπολογισμός»

Χρειαζόμαστε κι άλλες παραμέτρους για τον ορισμό περισσότερων κλάσεων (όπου θεωρούμε πάντοτε τη **μη ομοιόμορφη** εκδοχή).

Παραλληλία-Κλάση NC

NC^i: $SIZE[n^c]$ με $d(n) \leq O(\log^i n)$ και πύλες NAND σταθερού fan-in.

$$NC = \bigcup_{i \geq 0} NC^i$$

Αντιστοιχεί στην αποδοτική παράλληλη εκτέλεση χρόνου $\log^i n$.

Η NC^0 είναι τετριμμένα αδύναμη, καθώς μπορεί να εξαρτάται μόνο από $D = 2^{O(1)} = O(1)$ bits εισόδου.

Σημείωση: Στην καθιερωμένη σημειογραφία, το NC, αντιστοιχεί στην ομοιόμορφη εκδοχή της παραπάνω κλάσης, όμως, όπως αναφέραμε, εμείς εννοούμε εδώ πάντοτε τη μη ομοιόμορφη εκδοχή.

Πολλή Παραλληλία – Κλάση AC

AC^i: $SIZE[n^c]$ με $d(n) \leq O(\log^i n)$ και πύλες **μη φραγμένου** fan-in.

$$AC = \bigcup_{i \geq 0} AC^i$$

Η AC^0 δεν είναι τετριμμένη πλέον – Παραλληλία σταθερού βάθους.

$$NC^0 \subsetneq AC^0$$

$NC^i \subseteq AC^i \subseteq NC^{i+1}$ (γνησιότητα γνωρίζουμε μόνο για $i = 0$)

Βέβαια: $NC = AC$

Εξωτικές Πύλες – Κλάσεις ACC, TC

Γενικά επιτρέπουμε οι χρησιμοποιούμενες πύλες απεριόριστου fan-in να είναι συμμετρικές, δηλαδή να είναι μια (απλή) συνάρτηση του πλήθους των εισόδων που είναι 1:

$$\text{sum} = \sum_{i=1}^{n} x_i$$

$ACC(i_1, i_2, \dots i_k)$: Όπως το AC αλλά με ένα C παραπάνω:

$$\text{MOD}_{\text{i}_\text{j}}(\text{x}_1, \dots, \text{x}_\text{n}) = 1 \Leftrightarrow \text{sum} \neq 0 \ (mod\ i_j)$$

TC: Πύλες πλειοψηφίας (νευρωνικά δίκτυα)

$$\text{T}(\text{x}_1, \dots, \text{x}_\text{n}) = 1 \Leftrightarrow sum > \frac{n}{2}$$

Τρέχουσα Ιεραρχία

$NC^i \subseteq AC^i \subseteq ACC^i \subseteq TC^i \subseteq NC^{i+1}$

Γνωρίζουμε μόνο ότι $NC^0 \subsetneq AC^0 \subsetneq ACC^0$.

Όλα τα υπόλοιπα θα μπορούσαν να καταρρέουν σε σταθερό βάθος:

$$ACC^0, TC^0$$

Γνωρίζουμε κάποια ενδιάμεσα αποτελέσματα, όπως π.χ. ότι $TC^0_{d=2} \subsetneq TC^0_{d=3}$, $TC^0_{d=2} \subsetneq AC^0$, κ.ο.κ.

Κυκλώματα για Υπολογιστές

Είναι $DTIME[T(n)] \subseteq SIZE[T^2(n)]$.

Η απόδειξη χρησιμοποιεί παρόμοιες τεχνικές με την απόδειξη ότι το $3 - SAT$ είναι NP-πλήρες

Για κάθε χρονική στιγμή προσομοιώνουμε όλο το configuration της μηχανής με μία στήλη πυλών μήκους $T(n)$ (μία για κάθε κελί της ταινίας και μερικές ακόμη για τη τρέχουσα κατάσταση).

Κάθε επόμενη στήλη εξαρτάται μόνο από τα στοιχεία της προηγούμενης και το τέως τρέχον κελί.

Κάθε κελί εξαρτάται από τα γειτονικά του μόνο.

Τετριμμένο κύκλωμα σταθερού μήκους που ελέγχει αν η κατάσταση στη τελική στήλη είναι κατάσταση αποδοχής.

Κυκλώματα ↔ Φόρμουλες

Για κάθε είσοδο παίρνουμε μία μεταβλητή x_i και για κάθε σύρμα φτιάχνουμε μια νέα μεταβλητή y_i.

Έτσι για μια πύλη $NAND$, αν y_1, y_2 οι είσοδοι και y_o η έξοδος, «αντικαθιστούμε» την πύλη με τον όρο $\left((y_1 \wedge y_2) \leftrightarrow y_0\right)$.

Για τις σταθερές εισόδους θέτουμε αντίστοιχους όρους (π.χ. $(x_1 = 1)(x_2 = 0)$ και για το πιστοποιητικό τίποτα).

Κι αν y_{output} το σύρμα εξόδου προσθέτουμε τον όρο $\left(y_{output} = 1\right)$.

Όλα τα παραπάνω θρισατοποιούνται ομοιομορφότατα σε μια τελική έκφραση μήκους $O(SIZE_{OF_{CIRCUIT}})$…

$T(n)logT(n)$

Στα κυκλώματα είναι αναμενόμενο να υπάρχει ένα υπερκέφαλο (overhead) καθώς όλη η ιστορία της μηχανής είναι γραμμένη και παρέχεται όλη μαζί σε μορφή πυλών (οι οποίες παίρνουν μια μοναδική τιμή και δε μπορούν να επαναχρησιμοποιηθούν).

Από την άλλη, σε όλες αυτές τις προσομοιώσεις, παίρνουμε $T^2(n)$ συνολικές επαναλήψεις, ενώ συμβαίνουν μόνο $T(n)$ αλλαγές κι άρα το μεγαλύτερο ποσοστό των στοιχείων παραμένει τον περισσότερο χρόνο αναλλοίωτο.

Θα δούμε πώς μπορούμε να προσομοιώσουμε τις ολισθήσεις μιας μηχανής χρησιμοποιώντας $O\big(T(n)logT(n)\big)$ βήματα.

$T(n)logT(n)$

Χωρίζουμε την ταινία σε εκατέρωθεν ζώνες διπλασιαζόμενου μεγέθους (άρα συνολικά $O(logT)$ ζώνες).

$$|L_i| = |R_i| = 2 * 2^i$$

Εισάγουμε ένα νέο σύμβολο ⊠ για να συμβολίσουμε το άδειο στοιχείο (διαφορετικό από το σύμβολο κενού ⊔).

Φροντίζουμε κάθε στιγμή:

- Κάθε ζώνη να είναι είτε άδεια, είτε μισή, είτε ολόκληρη.
- Κάθε ζώνη μαζί με την αντίπερα της να έχουν άθροισμα μια ολόκληρη.
- Στο κέντρο να υπάρχει το τρέχον κελί (πάντα γεμάτο).

$T(n)logT(n)$

Κάθε φορά που κάνουμε ολίσθηση αριστερά, βρίσκουμε το πρώτο μη κενό R_j και κουβαλάμε τα 2^j αριστερότερα στοιχεία του στα $R_0, R_1, \dots, R_{j-1}$ έτσι ώστε να είναι όλα μισά (και φέρνουμε το αριστερότερο στο κέντρο).

Όμοια λόγω της συμπληρωματικότητας, όλα τα $L_0, L_1, \dots, L_{j-1}$ ήταν γεμάτα, οπότε τα σπρώχνουμε όλα, ώστε να γίνουν όλα μισά και το L_{j} (που δεν ήταν γεμάτο) να πάρει 2^j επιπλέον στοιχεία.

Όλες οι αναλλοίωτες διατηρούνται και χρειαστήκαμε $O(2^j)$ πράξεις για την ολίσθηση (αντί για $O(T)$).

$T(n)logT(n)$

Για να ξαναδιαλεχθεί το j ως η πρώτη μη κενή ζώνη θα πρέπει να γίνουν μετά από μια τέτοια ολίσθηση τουλάχιστον άλλες

$$\frac{1}{2}\left(|R_0| + |R_1| + \cdots + \left|R_{j-1}\right|\right) \geq 2^{j-1}$$

Άρα για κάθε δείκτη j η αντίστοιχη ζώνη επιλέγεται για το πολύ $T/2^{j-1}$ φορές, οπότε το συνολικό κόστος είναι το πολύ

$$K * \sum_{j=0}^{logT} \frac{T}{2^{j-1}} * 2^j = O(TlogT)$$

Η προσομοίωση μπορεί επίσης να εκφραστεί με ομοιόμορφη φόρμουλα και κύκλωμα ίδιου μήκους.

Υπολογιστές για Κυκλώματα;;

Δε γνωρίζουμε την ακριβή σχέση μεταξύ $P_{/poly}$ και οποιασδήποτε ομοιόμορφης κλάσης $DTIME[n^{\omega(1)}]$.

Ακόμη περισσότερο δε γνωρίζουμε καν τη σχέση του με το NP.

Γνωρίζουμε μόνο ότι υπάρχει μια συνάρτηση στο NP που θέλει κυκλώματα μεγέθους τουλάχιστον $5n$.

Εικασία Kolmogorov: $P \subseteq SIZE[O(n)]$

Μέχρι στιγμής:

Τα κυκλώματα δεν αντιστοιχούν σε ρεαλιστικό μοντέλο, λόγω ανομοιομορφίας...

Προσομοιώνουν με έστω μικρό υπέρβαρο κλάσεις για τις οποίες έχουμε ήδη ρεαλιστικό μοντέλο...

Δε γνωρίζουμε αν μπορούν να προσομοιώσουν αποδοτικά πιο μεγάλες κλάσεις (και πιστεύεται πως δεν μπορούν)...

Έχουν καμιά επιπλέον χρησιμότητα;

Λόγω ανομοιομορφίας…

$BPP \subseteq P_{/poly}$

Για $r(n)$ τυχαία bits έχουμε ότι υπάρχουν $2^{r(n)}$ δυνατές τιμές τους.

Κάνουμε το σφάλμα 2^{-n^2} κι έχουμε ότι για κάθε ξεχωριστή είσοδο, μόνο $2^{r(n)-n^2}$ από τις τυχαίες τιμές δίνουν λάθος αποτέλεσμα.

Επομένως υπάρχουν συνολικά $2^{r(n)-n^2} * 2^n \ll 2^{r(n)}$ λάθος τυχαίες τιμές για ένα μήκος εισόδου n. Διαλέγουμε μία που να είναι ορθή για όλες τις εισόδους αυτού του μήκους.

Δε γνωρίζουμε αν $BPP = P$, αλλά μπορούμε να δείξουμε ότι υπάρχει ένας καλός αντιπρόσωπος για κάθε είσοδο ενός δεδομένου μήκους, άρα υπάρχει και μια οικογένεια κυκλωμάτων (προφανώς μη ομοιόμορφα κατασκευάσιμη (μέχρι στιγμής)).

Με μικρό υπέρβαρο...

Τα κυκλώματα θα προέκυπταν συγκλονιστικά εκφραστικά αν είχαμε αποτελέσματα της μορφής:

$$NP \subseteq P_{/poly}$$
$$PSPACE \subseteq P_{/poly}$$
$$EXP \subseteq P_{/poly}$$

Ένα τέτοιο αποτέλεσμα θα σήμαινε ότι πληροφορία που δε μπορεί να παραχθεί ομοιόμορφα για κάθε μήκος εισόδου, έχει υπολογιστική ομοιομορφία (συμπύκνωση για το TT) για κάθε μήκος ξεχωριστά.

Συμπύκνωση

Η παραδοσιακή συμπίεση βρίσκει σε μια συμβολοσειρά επαναλήψεις.

$$01010101101010100101010110101010$$

$$\alpha = 01, \beta = 10, \gamma = \alpha^4, \delta = \beta^4, \varepsilon = (\gamma\delta)^2$$

Η κυκλωματική συμπύκνωση βρίσκει σε μια συμβολοσειρά υπολογιστικές επαναλήψεις

$$11101100101010000110010000010000$$

Πιο ισχυρή από τη συμπίεση.

$NEXP$

$x \in L$ αν και μόνο αν $\exists y: |y| < 2^{n^{O(1)}} \wedge M(x, y) = 1$ όπου M ντετερμινιστική μηχανή πολυωνυμικού χρόνου.

Το x καλείται στιγμιότυπο του προβλήματος και το y πιστοποιητικό του (σαν το NP μόνο που το πιστοποιητικό είναι εκθετικού μήκους).

Γενικά όταν το X είναι NP-πλήρες πρόβλημα, το $succinct\text{-}X$ είναι $NEXP$-πλήρες.

$succinct - SAT$

Η είσοδος δεν είναι πλέον ένα SAT, αλλά η συμπίεση ενός SAT ερωτήματος σε μορφή κυκλώματος (άρα η περιγραφή της συμπύκνωσης του).

Στιγμιότυπο: ένα κύκλωμα n εισόδων, το οποίο για κάθε είσοδο i, επιστρέφει τη περιγραφή του i-οστού όρου (clause) μίας SAT έκφρασης 2^n μήκους (και 2^n μεταβλητών).

Σημείωση: Όταν η είσοδος μας είναι μήκους N, τότε το ποσοστό των $succinct - SAT$ ερωτημάτων μήκους 2^N είναι πάρα πολύ μικρότερο από όλα τα ερωτήματα σχετικού μήκους.

Το $succinct\text{-}SAT$ είναι $NEXP$-πλήρες.

Υπάρχει ισοδύναμη $3\text{-}SAT$ για το $NEXP$ ακριβώς όπως στην απόδειξη για τα NP-πλήρη προβλήματα.

Μένει μόνο να δείξουμε πως είναι συμπυκνώσιμη: Προκύπτει από τοπική και χρονική επαναληψιμότητα μιας μηχανής Turing.

Παράδειγμα:

Για παράδειγμα: $n = 100, |y| = 2^{30}$ και χρόνου $T = 2^{30}$.

Ψάχνουμε τον $\mathrm{i} = 32975321750375893 4$-οστό όρο του αντίστοιχου $3\text{-}SAT$. Ισοδύναμα την $\mathrm{i} = 32975321750375893 4$-οστή πύλη του αντίστοιχου ισοδύναμου κυκλώματος μεγέθους $2^{O(n)}$.

Έχουμε ότι για κάθε στήλη ξοδεύουμε π.χ. 2^{35} μεταβλητές και πύλες, ΟΙ ΟΠΟΙΕΣ ΕΠΑΝΑΛΑΜΒΑΝΟΝΤΑΙ ΑΛΛΑΖΟΝΤΑΣ ΜΟΝΟ ΤΟΥΣ ΔΕΙΚΤΕΣ.

$$32975321750375893 4 \bmod 2^{35} = 25247255126$$

Άρα η πύλη είναι ίδια με το $\mathrm{j} = 25247255126$-ό στοιχείο κάθε στήλης. ΟΜΩΣ ΚΑΙ ΚΆΘΕ ΣΤΗΛΗ ΕΠΑΝΑΛΑΜΒΑΝΕΤΑΙ ΚΆΘΕ $n^2 = 10000$ ΘΕΣΕΙΣ.

$$25247255126 \bmod 10000 = 5126$$

Παράδειγμα (συνέχεια)

Επομένως για να βρούμε την $32975321750375893 4$-οστή πύλη του κυκλώματος:

- Βρίσκουμε ότι ισούται με την $2524725512 6$-οστή πύλη κάθε στήλης
- Η οποία ισούται με την 5126-οστή πύλη ενός σταθερού επαναλαμβανόμενου κυκλώματος μεγέθους 10000 θέσεων
- Όλα σε πολυωνυμικό (ως προς το μήκος εισόδου) χρόνο.

Αν μπορούμε να βρούμε εύκολα την αντίστοιχη πύλη, μπορούμε εύκολα να βρούμε και τις αντίστοιχες μεταβλητές του SAT-όρου.

Επειδή όλα τα παραπάνω είναι ομοιόμορφα (με εξαίρεση το κύκλωμα μεγέθους 10000 θέσεων που εξαρτάται από τη περιγραφή της μηχανής), μπορούμε εύκολα να κατασκευάσουμε ένα κύκλωμα μεγέθους $poly(100)$ που παράγει στο TT της όλη την ισοδύναμη 3-SAT.

ΣΗΜΑΝΤΙΚΗ ΠΑΡΑΤΗΡΗΣΗ (για το μέλλον)

Η παραγόμενη $3-\mathrm{SAT}$ έχει βάσει των προηγούμενων μήκος $T^2(n)$.

Προκύπτει ότι μπορούμε να διατηρήσουμε όλη αυτή την ομοιομορφία ακόμη και για τη περίπτωση του $T(n)logT(n)$!

Έτσι το κύκλωμα που συμπυκνώνει την ισοδύναμη $3-\mathrm{SAT}$ μπορεί να έχει πολυωνυμικό μέγεθος και π.χ. για $T(n)=2^{n^c}$, μόλις $n^c+klogn$ bits εισόδου.

Γιατί να μελετήσουμε τα κυκλώματα;

Παντρευόμαστε ώστε να λύνουμε από κοινού τα προβλήματα που μας έφερε ο γάμος.

Τα κυκλώματα, σε αντίθεση με τις μηχανές, παρέχουν όλες τις πράξεις της εκτέλεσης απέναντι από τον ερευνητή.

Πιο εύκολη εξαγωγή συνδυαστικών/περιοριστικών επιχειρημάτων, από ό,τι σε μια κρυψίνουν αναδρομή.

ΚΑΙ ΠΑΝΩ ΑΠΌ ΌΛΑ…

Τα κυκλώματα δε σχετικοποιούνται!

Βασικό στοιχείο της σχετικοποίησης (ή αλλιώς ρελατιβαϊζέισιον) είναι ότι χρησιμοποιείται ως είσοδος η περιγραφή μιας άλλης μηχανής και το άτοπο προκύπτει όταν η είσοδος είναι η περιγραφή της ίδιας της μηχανής.

Λόγω της ανομοιομορφίας των κυκλωμάτων, δε μπορούμε να δώσουμε ως είσοδο σε ένα κύκλωμα ένα ισοδύναμο μικρότερου μεγέθους (καθώς η περιγραφή του θέλει τουλάχιστον $SlogS$ χώρο).

Ακόμη περισσότερο, η μηχανή που δίνεται ως είσοδος αντιμετωπίζεται ως μαύρο κουτί (επεμβαίνουμε μόνο στις εισόδους και στην έξοδο του).

Τα κυκλώματα είναι κατ' εξοχήν μοντέλα που παρουσιάζεται όλη η λειτουργία και οι λεπτομέρειες του υπολογισμού αυτούσια στον ερευνητή.

$NP\ vs\ P_{/poly}$

Το να δειχθεί ότι $NP \not\subseteq P_{/poly}$ είναι πιο ισχυρό από το $NP \neq P$, αλλά φαίνεται πιο φιλικό στον χρήστη (και πιο ελπιδοφόρο από τις απλές αυτοαναφορικές τεχνικές)...

Άλλωστε, πιστεύεται για παρόμοιους λόγους, ότι $NP \not\subseteq P_{/poly}$ καθώς αλλιώς $PH = \Sigma_2^P$ (περισσότερα επί τούτου αργότερα).

Σε κάθε περίπτωση, δεν είναι χάσιμο χρόνου...

...εκ πρώτης όψεως.

Κρατάμε ότι:

1. Μπορούμε να ορίσουμε διάφορες κυκλωματικές κλάσεις, υποσύνολα του $P_{/poly}$ θέτοντας περιορισμούς στο βάθος, στο fanin ή στο είδος των πυλών.

2. Κάθε $NEXP$ ερώτημα χρόνου $T(n)$ μπορεί να αναχθεί σε ένα στιγμιότυπου του $succinct - SAT$ όπου το αντίστοιχο κύκλωμα έχει $\log\big(T(n)logT(n)\big)$ bits εισόδου.

3. Τα κυκλώματα δε φυσικοποιούνται και άρα αποτελούν δελεαστικούς διάδοχους των διαγώνιων επιχειρημάτων για την αντιμετώπιση μεγάλων ανοιχτών ερωτημάτων της Θεωρίας Πολυπλοκότητας.


To be continued...