Εισαγωγή στο μοντέλο επικοινωνίας

(Communication complexity)

Ορισμός του μοντέλου.

Έστω πεπερασμένα σύνολα X, Y, Z και συνάρτηση $f : X \times Y \to Z$. Έχουμε δύο παίκτες Alice (A) και Bob (B) που θέλουν να υπολογίσουν την τιμή $f(x, y)$ για $x \in X$ και $y \in Y$. Η δυσκολία έγκειται στο ότι η A γνωρίζει μόνο το x και αντίστοιχα ο B μόνο το y. Είναι λοιπόν απαραίτητο να επικοινωνήσουν για να υπολογίσουν σωστά το $f(x, y)$. Τα μηνύματα που θα ανταλλάξουν καθορίζονται από ένα πρωτόκολλο P. Το P πρέπει σε κάθε *γύρο* να καθορίζει τα παρακάτω.

- Αν η εκτέλεση έχει τελειώσει και, αν ναι, ποια είναι η έξοδος (η τιμή $f(x, y)$).
- Αν όχι, ποιος παίκτης στέλνει μήνυμα. (Αυτό πρέπει να εξαρτάται μόνο από τα μηνύματα που έχουν ανταλλαχθεί μέχρι εκείνη την στιγμή, γιατί αυτή είναι η μόνη κοινή πληροφορία.)
- Ποιο είναι το μήνυμα που πρέπει να στείλει ο επόμενος παίκτης. (Αυτό μπορεί να εξαρτάται εκτός από την επικοινωνία μέχρι εκείνη τη στιγμή και από την είσοδο του παίκτη που στέλνει το μήνυμα.)

Παρατηρήστε ότι δεν γίνεται καθόλου λόγος για τους υπολογισμούς που μπορεί να χρειάζεται να κάνουν οι A και B για να «τρέξουν» το πρωτόκολλο. Έτσι, επιτρέπουμε στους παίκτες να έχουν απεριόριστη υπολογιστική ισχύ.

Ορισμός. *Το κόστος ενός πρωτοκόλλου P σε είσοδο (x, y) είναι τα bits που οι παίκτες στέλνουν. Η πολυπλοκότητα ενός πρωτοκόλλου P είναι το μεγαλύτερο κόστος μεταξύ όλων των $(x, y) \in X \times Y$. Η πολυπλοκότητα της $f : X \times Y \to Z$ είναι η μικρότερη πολυπλοκότητα μεταξύ όλων του πρωτοκόλλων που υπολογίζουν σωστά την f και συμβολίζεται με $D(f)$.*

Δώσαμε τον παραπάνω ορισμό χωρίς να έχουμε ορίσει αυστηρά τι είναι πρωτόκολλο. Ο τυπικός ορισμός μπορεί να αναπαριστά κάθε πρωτόκολλο από ένα δυαδικό δένδρο, όπου κάθε εσωτερικός κόμβος καθορίζει ποιος στέλνει μήνυμα και ποιος παίκτης είναι αυτός, ενώ κάθε φύλλο αντιστοιχεί σε ένα $z \in Z$. Τότε, κάθε (x, y) θα αντιστοιχεί σε ένα μονοπάτι από την ρίζα σε ένα φύλλο και το κόστος σε αυτή την είσοδο είναι το μήκος του μονοπατιού. Το κόστος του πρωτοκόλλου είναι το ύψος του δένδρου. Σε αυτές τις σημειώσεις θα αρκεστούμε στα παραπάνω.

Η ιδιότητα των τετραγώνων.

Κάθε πρωτόκολλο P ορίζει μία διαμέριση $\mathcal{R}_P$ του $X \times Y$, όπου κάθε μέρος αντιστοιχεί σε ένα φύλλο του δένδρου του πρωτοκόλλου. Με άλλα λόγια, αν $R \in \mathcal{R}_P$, τότε τα μηνύματα που ανταλλάσσονται κατά την εκτέλεση του P σε κάθε $(x, y) \in R$ είναι ακριβώς τα ίδια. Θα δείξουμε ότι κάθε τέτοιο R δεν είναι ένα οποιοδήποτε υποσύνολο του $X \times Y$, αλλά έχει πολύ συγκεκριμένη δομή.

Ορισμός. *Ένα ορθογώνιο στο $X \times Y$ είναι ένα υποσύνολο $R \subseteq X \times Y$ τέτοιο που $R = A \times B$ για κάποια $A \subseteq X$ και $B \subseteq Y$.*

Το παρακάτω δίνει έναν ισοδύναμο ορισμό.

Πρόταση 1. *$R \subseteq X \times Y$ είναι ορθογώνιο αν και μόνο αν*

$$(x, y) \in R \text{ και } (x', y') \in R \implies (x, y') \in R.$$

Απόδειξη. Άσκηση. □

Η σημασία των ορθογωνίων εκφράζεται στη παρακάτω πρόταση.

Πρόταση 2. *Για κάθε πρωτόκολλο P και φύλλο ℓ του δένδρου του P, το σύνολο*

$$R_\ell = \{(x, y) : \text{η εκτέλεση του } P \text{ στο } (x, y) \text{ οδηγεί στο } \ell\}$$

είναι ορθογώνιο.

Απόδειξη. Έστω ότι για $(x, y) \in R_\ell$ και $(x', y') \in R_\ell$ παίκτες ανταλλάσσουν bits $b = (b_1, b_2, \ldots, b_m)$. Από την προηγούμενη πρόταση, αρκεί να δείξουμε ότι σε είσοδο (x, y') η επικοινωνία είναι b.

Η απόδειξη είναι με επαγωγή στο m. Έστω ότι είναι σειρά της Α μετά την ανταλλαγή των bits $b' = (b_1, b_2, \ldots, b_{k-1})$. Επειδή $(x, y) \in R_\ell$, όταν η Α βλέπει x και επικοινωνία b', ξέρουμε ότι το επόμενο bit είναι b_k. Ομοίως, επειδή $(x, y) \in R_\ell$, όταν ο Β βλέπει y' και επικοινωνία b', ξέρουμε ότι το επόμενο bit είναι b_k. □

Γενικότερα, κάθε υποσύνολο εισόδων που αντιστοιχεί σε οποιοδήποτε κόμβο ενός δένδρου πρωτοκόλλου, είναι ορθογώνιο.

Τέλος, ένα πρωτόκολλο P υπολογίζει σωστά συνάρτηση f, αν για κάθε φύλλο ℓ του δένδρου του P, η f είναι σταθερή στο R_ℓ (δηλαδή, για κάποιο $z \in Z$, $f(x, y) = z$ για κάθε $(x, y) \in R_\ell$).

Ορισμός. *Ένα υποσύνολο $R \subseteq X \times Y$ λέγεται f-μονοχρωματικό αν η f είναι σταθερή στο R.*

Όλα τα παραπάνω μας οδηγούν στο παρακάτω σημαντικό λήμμα.

Λήμμα 3. *Κάθε πρωτόκολλο P για συνάρτηση f καθορίζει διαμέριση του $X \times Y$ σε f-μονοχρωματικά ορθογώνια. Ο αριθμός των ορθογωνίων είναι ο αριθμός των φύλλων του δένδρου του P.*

Το παρακάτω συμπέρασμα προκύπτει από το ότι ένα δυαδικό δένδρο με t φύλλα έχει ύψος τουλάχιστον $\log_2 t$.

Συμπέρασμα 4. *Αν κάθε διαμέριση του $X \times Y$ σε f-μονοχρωματικά ορθογώνια απαιτεί τουλάχιστον t ορθογώνια, τότε $D(f) \geq \log_2 t$.*

Fooling sets.

Μία απλή τεχνική για κάτω φράγματα είναι το λεγόμενο «fooling set». Αυτό είναι ένα σύνολο $S \subseteq X \times Y$ με την ιδιότητα ότι οποιεσδήποτε δύο είσοδοι ανήκουν σε αυτό δεν μπορεί να ανήκουν σε ένα μονοχρωματικό ορθογώνιο. Προκύπτει ότι κάθε διαμέριση του $X \times Y$ σε μονοχρωματικά ορθογώνια πρέπει να έχει μέγεθος τουλάχιστον $|S|$ (αφού κάθε στοιχείο του S πρέπει να ανήκει σε διαφορετικό). Το Συμπέρασμα 4 στο τέλος της προηγούμενης ενότητας δίνει πολυπλοκότητα τουλάχιστον $\log_2 |S|$.

Ορισμός. *Έστω $f : X \times Y \to \{0, 1\}$. Ένα σύνολο $S \subseteq X \times Y$ είναι fooling set για την f αν για κάποιο $z \in \{0, 1\}$ ισχύουν τα παρακάτω.*

- *Για κάθε $(x, y) \in S$, $f(x, y) = z$.*
- *Για κάθε $(x, y) \in S$ και $(x', y') \in S$, $f(x, y') \neq z$ ή $f(x', y) \neq z$.*

Λήμμα 5. *Αν το S είναι fooling set για την f, τότε $D(f) \geq \log_2 |S|$.*

Απόδειξη. Αρκεί να δείξουμε ότι κανένα μονοχρωματικό ορθογώνιο R δεν μπορεί να περιέχει δύο στοιχεία του S. Έστω δύο διαφορετικά στοιχεία (x, y) και (x', y') του S. Έστω, προς άτοπο, ότι $(x, y) \in R$ και $(x', y') \in R$. Από την Πρόταση 1, $(x, y') \in R$ και $(x', y) \in R$. Αφού $f(x, y') \neq z$ ή $f(x', y) \neq z$, το R δεν είναι μονοχρωματικό. Το φράγμα προκύπτει από το Συμπέρασμα 4. □

Παράδειγμα: EQ. Οι Α και Β λαμβάνουν $x, y \in \{0, 1\}^n$ και ορίζουμε

$$\text{EQ}(x, y) = 1 \iff x = y.$$

Είναι ξεκάθαρο ότι $D(\text{EQ}) \leq n + 1$, αφού μπορεί η Α να στείλει το x στον Β (n bits) και ο Β να της δώσει την απάντηση (1 bit). Χρησιμοποιώντας το συμπέρασμα στο τέλος της προηγούμενης ενότητας, θα δείξουμε ότι $D(\text{EQ}) \geq n + 1$ και άρα $D(\text{EQ}) = n + 1$.

Το παρακάτω σύνολο S είναι fooling set μεγέθους 2^n.

$$S = \{(x, x) : x \in \{0, 1\}^n\}$$

Από το Λήμμα 5 προκύπτει $D(\text{EQ}) \geq n$. Επειδή όμως υπάρχουν και 0-ορθογώνια, προκύπτει το ζητούμενο $D(\text{EQ}) \geq n + 1$.

Παράδειγμα: DISJ. Οι Α και Β λαμβάνουν $x, y \subseteq \{1, 2, \ldots, n\}$ και ορίζουμε

$$\text{DISJ}(x, y) = 1 \iff x \cap y = \emptyset.$$

Το παρακάτω σύνολο S είναι fooling set μεγέθους 2^n.

$$S = \{(x, \bar{x}) : x \subseteq \{1, 2, \ldots, n\}\}$$

Όπως για την EQ προκύπτει $D(\text{DISJ}) \geq n + 1$.

Άσκηση. *Δείξτε ότι* $D(\text{GT}) = n + 1$*, όπου η συνάρτηση* GT *σε είσοδο ακεραίους* $0 \leq x, y < 2^n$ *είναι 1 αν και μόνο αν* $x > y$*.*

Μηχανές Turing και Communication Complexity.

Το μοντέλο υπολογισμού που περιγράψαμε είναι πολύ χρήσιμο για την μελέτη χρονικής και χωρικής πολυπλοκότητας σε άλλα μοντέλα υπολογισμού. Εδώ θα απαντήσουμε σε ερωτήματα που αφορούν σε μηχανές Turing (TM). Ο λόγος είναι ότι μπορούμε να φανταστούμε έναν μερικό υπολογισμό να αφήνει την TM σε μία *κατάσταση* και η συνέχεια αυτού το υπολογισμού να συνεχίζει από αυτήν. Το μέγεθος της *επικοινωνίας* που απαιτείται σχετίζεται λοιπόν με το μέγεθος της κατάστασης (χωρική πολυπλοκότητα) και το πλήθος των φορών που γίνεται αυτό σχετίζεται με τον χρόνο.

Στο παράδειγμα που θα δούμε αφορά σε TM με μία ταινία εισόδου (read only) και k ταινίες εργασίας (read/write). Η χρονική πολυπλοκότητα μίας μηχανής είναι $T(n)$ αν σε κάθε είσοδο με μήκος n σταματάει (το πολύ) σε $T(n)$ βήματα. Η χωρική πολυπλοκότητα μίας μηχανής είναι $S(n)$ αν σε κάθε είσοδο με μήκος n η TM χρησιμοποιεί το πολύ $S(n)$ κελιά των ταινιών εργασίας.

Το παρακάτω λήμμα δείχνει πως η πολυπλοκότητα μίας συνάρτησης στο μοντέλο επικοινωνίας σχετίζεται με την χωρική και χρονική πολυπλοκότητα μίας σχετικής γλώσσας στο μοντέλο των μηχανών Turing.

Λήμμα 6. *Έστω συνάρτηση* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$*. Αν υπάρχει μηχανή Turing που αποδέχεται όλες τις εισόδους του συνόλου*

$$\{x0^n y : |x| = |y| = n \text{ και } f(x,y) = 1\},$$

απορρίπτει όλες τις εισόδους του συνόλου

$$\{x0^n y : |x| = |y| = n \text{ και } f(x,y) = 0\},$$

και σε κάθε είσοδο μήκους $3n$ *σταματάει το πολύ σε* $T(n)$ *βήματα και χρησιμοποιεί το πολύ* $S(n)$ *χώρο, τότε*

$$D(f) = O(T(n)S(n)/n).$$

Απόδειξη. Έστω M η TM της υπόθεσης του λήμματος. Οι A και B σε είσοδο (x, y) εκτελούν την M σε είσοδο $x0^n y$· σταματούν με έξοδο 1 αν και μόνο αν η M αποδέχεται. Σε κάθε σημείο της εκτέλεσης, η κεφαλή της ταινίας εισόδου διαβάζει είτε ένα bit του x, είτε ένα από τα n μηδενικά, είτε ένα bit του y. Στην 1η περίπτωση, «τρέχει» την M η A, στην 3η ο B, ενώ στην 2η ο τελευταίος παίκτης που έτρεχε την M πριν η κεφαλή μπει στην περιοχή των μηδενικών. Κάθε παίκτης δηλαδή τρέχει την M όσο μπορεί και μετά αναλαμβάνει ο άλλος.

Η πληροφορία που χρειάζεται ένας παίκτης να παραλάβει για να συνεχίσει τον υπολογισμό της M είναι τα περιεχόμενα των (μη κενών κελιών των) ταινιών εργασίας (όπως έχουν διαμορφωθεί εκείνη την στιγμή), την τοποθεσία των κεφαλών των ταινιών εργασίας, και την κατάσταση της M. Το μέγεθος του μηνύματος είναι $O(S(n))$.

Η σημαντική παρατήρηση είναι ότι κάθε φορά που η εκτέλεση «περνάει» από τον έναν παίκτη στον άλλο, η κεφαλή της ταινίας εισόδου έχει διαβάσει n μηδενικά. Επειδή η ταινία διαβάζει ένα κελί τη φορά, αυτό δεν μπορεί να γίνει σε λιγότερο από n βήματα. Προκύπτει ότι η εκτέλεση περνάει από τον έναν στον άλλον το πολύ $T(n)/n$ φορές (αλλιώς η M δεν σταματάει σε $T(n)$ βήματα). Αφού κάθε φορά οι παίκτες ανταλλάσσουν το πολύ $O(S(n))$ bits, η συνολική επικοινωνία είναι το πολύ $O(S(n)T(n)/n)$. □

Έστω M μία TM που αποφασίζει αν μία λέξη μήκους $3n$ είναι καρκινική σε χρόνο $T(n)$ και χώρο $S(n)$. Έστω $f(x, y) = 1$ αν και μόνο αν $x = y^R$ (όπου $y_1 y_2 \cdots y_n^R = y_n y_{n-1} \cdots y_1$. Τότε η M αποδέχεται όλες τις εισόδους του συνόλου

$$\{x0^n y : |x| = |y| = n \text{ και } f(x,y) = 1\}$$

και απορρίπτει όλες τις εισόδους του συνόλου

$$\{x0^n y : |x| = |y| = n \text{ και } f(x,y) = 0\}.$$

Επειδή στο μοντέλο επικοινωνίας η πολυπλοκότητα της f είναι ίση με την πολυπλοκότητα της EQ, έχουμε $D(f) = n + 1$. Από τα παραπάνω και το Λήμμα προκύπτει το εξής συμπέρασμα.

Θεώρημα 7. *Κάθε μηχανή Turing που αποφασίζει την γλώσσα των καρκινικών λέξεων σε χρόνο* $T(n)$ *και χώρο* $S(n)$ *ικανοποιεί* $T(n)S(n) = \Omega(n^2)$.

Το θεώρημα είναι (ουσιαστικά) βέλτιστο, γιατί για την γλώσσα αυτή υπάρχει ΤΜ με $T(n) = O(n)$ και $S(n) = O(n)$ (η Μ αντιγράφει την είσοδο σε ταινία εργασίας και συγκρίνει τα περιεχόμενα των δύο ταινιών διαβάζοντας τη μία από αριστερά προς τα δεξιά και την άλλη από δεξιά προς τα αριστερά), καθώς και ΤΜ με $T(n) = O(n^2)$ και $S(n) = O(\log n)$ (ελέγχει για κάθε i αν το i-οστό bit είναι ίσο με το bit στη θέση $n - i$).

Χρησιμοποιώντας αυτό το tradeoff μεταξύ χρονικής και χωρικής πολυπλοκότητας, μπορεί κανείς να δείξει κάτω φράγμα στην χωρική πολυπλοκότητα.

Συμπέρασμα 8. *Κάθε μηχανή Turing που αποφασίζει την γλώσσα των καρκινικών λέξεων χρειάζεται* $\Omega(\log n)$ *χώρο.*

Απόδειξη. Άσκηση. □

Με παρόμοιες τεχνικές μπορεί να δειχθεί ότι κάθε μηχανή Turing *με μία ταινία* που αποφασίζει την γλώσσα των καρκινικών λέξεων έχει χρονική πολυπλοκότητα $\Omega(n^2)$.