Μαθημα Δευτερο

'Αρης Παγουρτζης, Βασιλης Νακος ΑΛΜΑ

Προηγούμενο Μάθημα

Περιγραφή κλάδου Λεπτομερούς Πολυπλοκλότητας.
Αρχικές Υποθέσεις Δυσκολίας:

- Πρόβλημα Συντομότερων Μονοπατιών.
- 3-SUM.
- Ορθογώνια Διανύσματα.
- k-SAT.

Προηγούμενο Μάθημα

Περιγραφή κλάδου Λεπτομερούς Πολυπλοκλότητας.
Αρχικές Υποθέσεις Δυσκολίας:

- Πρόβλημα Συντομότερων Μονοπατιών.
- 3-SUM.
- Ορθογώνια Διανύσματα.
- k-SAT.

Αυτό το μάθημα: Μια πιο προσεκτική ματιά στο πρόβλημα των Ορθογώνιων Διανυσμάτων.

Ορθογώνια Διανύσματα και k-SAT

Ορθογώνια Διανύσματα. Δίνονται δύο σύνολα $A, B \subseteq \{0,1\}^d$. Να βρεθεί αν υπάρχει ζέυγος $a \in A, b \in B$ ώστε a, b κάθετα.

Ορθογώνια Διανύσματα και k-SAT

Ορθογώνια Διανύσματα. Δίνονται δύο σύνολα $A, B \subseteq \{0,1\}^d$. Να βρεθεί αν υπάρχει ζεύγος $a \in A, b \in B$ ώστε a, b κάθετα.

k-SAT. Δίνεται μία φόρμουλα ϕ σε κανονική μορφή, πχ

$$\phi := (x_1 \vee x_2 \vee x_N) \wedge \ldots \wedge (x_4 \vee x_7 \vee x_9),$$

με N μεταβλητές και M clauses. Να βρεθεί αν υπάρχει αποτίμηση τιμών αληθείας που ικανοποιεί τη ϕ.

Ορθογώνια Διανύσματα και k-SAT

- Δεν υπάρχει αυστηρά υποτετραγωνικός αλγόριθμος για το πρόβλημα των Ορθογώνιων Διανυσμάτων.
- Εναλλακτικά: Δεν υπάρχει αλγόριθμος $n^{2-\epsilon} \cdot \mathrm{poly}(d)$ για το πρόβλημα των Ορθογώνιων Διανύσματων.
- Ισχυρή Υπόθεση Υποεκθετικού Χρόνου: $\forall \epsilon > 0, \exists k$, έτσι ώστε το k-SAT να μη μπορεί να λυθεί σε $2^{(1-\epsilon)N} \cdot \mathrm{poly}(M)$ χρόνο.

Συσχέτιση Ορθογωνίων Διανυσμάτων και k-SAT

Θεώρημα:Η υπόθεση Ισχυρού Υποεκθετικού Χρόνου υποννοεί την υπόθεση Ορθογώνιων Διανυσμάτων.

Συσχέτιση Ορθογωνίων Διανυσμάτων και k-SAT

Θεώρημα:Η υπόθεση Ισχυρού Υποεκθετικού Χρόνου υποννοεί την υπόθεση Ορθογώνιων Διανυσμάτων.

Ισοδύναμα:

Θεώρημα: Έστω ότι υπάρχει $\epsilon >$ 0 και ένας $n^{2-\epsilon} \cdot \mathrm{poly}(d)$ αλγόριθμος για το πρόβλημα των Ορθογωνίων διανυσμάτων. Τότε υπάρχει $\epsilon' := \epsilon'(\epsilon) >$ 0 και ένας αλγόριθμος χρόνου $2^{(1-\epsilon')N} \cdot \mathrm{poly}(M)$ για το k-SAT.

Χωρίζουμε τις μεταβλητές στη μέση: $x_1, x_2, \ldots, x_{N/2}$, και $x_{N/2+1}, \ldots, x_N$.

Χωρίζουμε τις μεταβλητές στη μέση: $x_1, x_2, \ldots, x_{N/2}$, και $x_{N/2+1}, \ldots, x_N$.
Για καθεμία από τις $2^{N/2}$ αποτίμησεις τιμών στις $x_1, x_2, \ldots, x_{N/2}$, φτιάχνουμε ένα διάνυσμα στο A.

- Παραδείγματος χάρην, Για την αποτίμηση $v = \{false, false, true, \ldots, true\}$, φτιάχνουμε το διάνυσμα $a_v \in \{0, 1\}^M$ το το οποίο έχει 0 στη j-οστή θέση, αν η v ικανοποιεί το j-οστό clause, αλλιώς 1.

Χωρίζουμε τις μεταβλητές στη μέση: $x_1, x_2, \ldots, x_{N/2}$, και $x_{N/2+1}, \ldots, x_N$.
Για καθεμία από τις $2^{N/2}$ αποτίμησεις τιμών στις $x_1, x_2, \ldots, x_{N/2}$, φτιάχνουμε ένα διάνυσμα στο A.

- Παραδείγματος χάρην, Για την αποτίμηση $v = \{false, false, true, \ldots, true\}$, φτιάχνουμε το διάνυσμα $a_v \in \{0, 1\}^M$ το το οποίο έχει 0 στη j-οστή θέση, αν η v ικανοποιεί το j-οστό clause, αλλιώς 1.
- Όμοια φτιάχνουμε διανύσματα στο b_v.

Χωρίζουμε τις μεταβλητές στη μέση: $x_1, x_2, \ldots, x_{N/2}$, και $x_{N/2+1}, \ldots, x_N$.
Για καθεμία από τις $2^{N/2}$ αποτίμησεις τιμών στις $x_1, x_2, \ldots, x_{N/2}$, φτιάχνουμε ένα διάνυσμα στο A.

- Παραδείγματος χάρην, Για την αποτίμηση $v = \{false, false, true, \ldots, true\}$, φτιάχνουμε το διάνυσμα $a_v \in \{0, 1\}^M$ το το οποίο έχει 0 στη j-οστή θέση, αν η v ικανοποιεί το j-οστό clause, αλλιώς 1.
- Όμοια φτιάχνουμε διανύσματα στο b_v.
- $|A| = |B| = 2^{N/2}$.
- $A, B \subseteq \{0, 1\}^M$.

Έστω ότι υπάρχει αποτίμηση v που κάνει την ϕ αληθή. Τότε

- Έστω $v = (v_1, v_2), |v|_1 = |v_2| = N/2$.

Έστω ότι υπάρχει αποτίμηση v που κάνει την ϕ αληθή. Τότε

- Έστω $v = (v_1, v_2), |v|_1 = |v_2| = N/2$.
- Ισχυριζόμαστε ότι τα διανύσματα a_{v_1}, b_{v_2} είναι κάθετα.

Έστω ότι υπάρχει αποτίμηση v που κάνει την ϕ αληθή. Τότε

- Έστω $v = (v_1, v_2), |v|_1 = |v_2| = N/2$.
- Ισχυριζόμαστε ότι τα διανύσματα a_{v_1}, b_{v_2} είναι κάθετα.
- Κάθε clause ικανοποιείται από τη v. Άρα, για κάθε $j \in [M]$, το j-οστό clause θα ικανοποιείται είτε μέσω του v_1 είτε μέσω του v_2.

Έστω ότι υπάρχει αποτίμηση v που κάνει την ϕ αληθή. Τότε

- Έστω $v = (v_1, v_2), |v|_1 = |v_2| = N/2$.
- Ισχυριζόμαστε ότι τα διανύσματα a_{v_1}, b_{v_2} είναι κάθετα.
- Κάθε clause ικανοποιείται από τη v. Άρα, για κάθε $j \in [M]$, το j-οστό clause θα ικανοποιείται είτε μέσω του v_1 είτε μέσω του v_2.
- Άρα είτε $a_{v_1}[j] = 0$ είτε $b_{v_2}[j] = 0$, για κάθε j.

Έστω ότι υπάρχει ορθογώνιο ζεύγος $(a_{v_1}, b_{v_2}) \in A \times B$.

Έστω ότι υπάρχει ορθογώνιο ζεύγος $(a_{v_1}, b_{v_2}) \in A \times B$.

Έστω η αποτίμηση $v := (v_1, v_2)$. Τότε

- Για κάθε $j \in [m]$ έχουμε $a_{v_1}[j] = 0$ ή $v_{v_2}[j] = 0$.

- Άρα τουλάχιστον μία από τις δύο αποτιμήσεις κάνουν το j-οστό clause αληθές.
- Εφόσον ισχύει για όλες τα clauses, η v ικανοποιεί τη ϕ.

Πρόβλημα Μεταβολής Ακολουθίας (edit distance

Δίνονται δύο συμβολοσειρές $X, Y \in \Sigma^n$. Μπορούμε να κάνουμε τις εξής πράξεις: διαγραφή, αντικατάσταση, αλλαγή συμβόλου, με κόστη c_d, c_r, c_m αντίστοιχα.

Πρόβλημα Μεταβολής Ακολουθίας (edit distance

Δίνονται δύο συμβολοσειρές $X, Y \in \Sigma^n$. Μπορούμε να κάνουμε τις εξής πράξεις: διαγραφή, αντικατάσταση, αλλαγή συμβόλου, με κόστη c_d, c_r, c_m αντίστοιχα.

Να βρεθεί το ελάχιστο κόστος, το οποίο μετατρέπει τη μία ακολουθία στην άλλη.
Κλασική $O(n^2)$ λύση με δυναμικό προγραμματισμό.

Μέγιστη Κοινή Υπακολουθία

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$. Να βρεθεί η μέγιστη κοινή υπακολουθία τους.

Μέγιστη Κοινή Υπακολουθία

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$. Να βρεθεί η μέγιστη κοινή υπακολουθία τους.

$\mathrm{DP}[i, j] :=$ μήκος της μέγιστη κοινής υπακολουθία του $X[1, \ldots, i]$ με $Y[1, \ldots, j]$.

Μέγιστη Κοινή Υπακολουθία

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$. Να βρεθεί η μέγιστη κοινή υπακολουθία τους.

$\text{DP}[i, j] :=$ μήκος της μέγιστη κοινής υπακολουθία του $X[1, \ldots, i]$ με $Y[1, \ldots, j]$.

- $\text{DP}[0, j] = \text{DP}[i, 0] = 0$.
- $\text{DP}[i, j] = \text{DP}[i-1, j-1] + 1$, αν $X[i] = X[j]$.
- $\text{DP}[i, j] = \min\{\text{DP}[i-1, j], \text{DP}[i, j-1]\}$, αλλιώς.

Περιτύλιγμα Δυναμικού Χρόνου

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$, με την κάθε ακολουθία να αντιστοιχεί σε μια χρονοσειρά. Κρατάμε από ένα δείκτη στο πρώτο σημείο κάθε χρονοσειράς.

Περιτύλιγμα Δυναμικού Χρόνου

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$, με την κάθε ακολουθία να αντιστοιχεί σε μια χρονοσειρά. Κρατάμε από ένα δείκτη στο πρώτο σημείο κάθε χρονοσειράς.
Μπορούμε να διασχίσουμε τις χρονοσειρές, προχωρώντας κάθε φορά τουλάχιστον έναν δείκτη κατά 1. Δηλαδή, αν οι δείκτες είναι στην κατάσταση (i, j), μπορούν δυνητικά να πάνε στην κατάσταση $(i + 1, j), (i, j + 1), (i + 1, j + 1)$.

PM

Περιτύλιγμα Δυναμικού Χρόνου

Δίνονται δύο ακολουθίες $X, Y \in \Sigma^n$, με την κάθε ακολουθία να αντιστοιχεί σε μια χρονοσειρά. Κρατάμε από ένα δείκτη στο πρώτο σημείο κάθε χρονοσειράς.
Μπορούμε να διασχίσουμε τις χρονοσειρές, προχωρώντας κάθε φορά τουλάχιστον έναν δείκτη κατά 1. Δηλαδή, αν οι δείκτες είναι στην κατάσταση (i, j), μπορούν δυνητικά να πάνε στην κατάσταση $(i+1, j), (i, j+1), (i+1, j+1)$.

Θέλουμε να βρούμε τη διάσχιση $\mathcal{D}$ που ελαχιστοποιεί το άθροισμα

$$\sum_{\text{καταστάσεις } (i,j) \in \mathcal{D}} |X[i] - Y[j]| .$$

Τι συμβαίνει;

Όλα τα προαναφερθέντα προβλήματα δεν έχουν *αυστηρά* υποτετραγωνικούς χρόνους. Υπάρχουν μόνο μικρές βελτιώσεις, παραδείγματος χάρην για τη Μέγιστη Κοινή Υπακολουθία γνωρίζουμε αλγόριθμο $\approx \frac{n^2}{\left(\frac{\log n}{\log \log n}\right)^2}$ (Masek και Paterson, 1980).

Τι συμβαίνει;

Όλα τα προαναφερθέντα προβλήματα δεν έχουν *αυστηρά* υποτετραγωνικούς χρόνους. Υπάρχουν μόνο μικρές βελτιώσεις, παραδείγματος χάρην για τη Μέγιστη Κοινή Υπακολουθία γνωρίζουμε αλγόριθμο $\approx \frac{n^2}{\left(\frac{\log n}{\log \log n}\right)^2}$ (Masek και Paterson, 1980).

Μπορούμε να εξηγήσουμε την έλλειψη αυστηρά υποτετραγωνικών αλγορίθμων;

Δυσκολία Μέγιστης Κοινής Υπακολουθίας

Θεώρημα. Αν υπάρχει αλγόριθμος χρόνους $n^{2-\epsilon}$ με $\epsilon > 0$, για το πρόβλημα της Μέγιστης Κοινής Υπακολουθίας, τότε υπάρχει αλγόριθμος χρόνου $n^{2-\epsilon} \cdot \mathrm{poly}(d)$ για το πρόβλημα των Ορθογωνίων διανυσμάτων.

Δυσκολία Μέγιστης Κοινής Υπακολουθίας

Θεώρημα. Αν υπάρχει αλγόριθμος χρόνους $n^{2-\epsilon}$ με $\epsilon > 0$, για το πρόβλημα της Μέγιστης Κοινής Υπακολουθίας, τότε υπάρχει αλγόριθμος χρόνου $n^{2-\epsilon} \cdot \mathrm{poly}(d)$ για το πρόβλημα των Ορθογωνίων διανυσμάτων.

Όμοια για τα άλλα δύο πρόβλημα σε συμβολοσειρές.

Θα μετατρέψουμε ένα στιγμιότυπο του προβλήματος των Ορθογωνίων Διανυσμάτων σε δύο ακολουθίες μήκους $O(nd^2)$. Το μήκος της μέγιστης κοινής ακολουθίας των τελευταίων δείχνει αν υπάρχει ορθογώνιο ζεύγος στ αρχικό στιγμιότυπο.

Θα μετατρέψουμε ένα στιγμιότυπο του προβλήματος των Ορθογωνίων Διανυσμάτων σε δύο ακολουθίες μήκους $O(nd^2)$. Το μήκος της μέγιστης κοινής ακολουθίας των τελευταίων δείχνει αν υπάρχει ορθογώνιο ζεύγος στ αρχικό στιγμιότυπο.

Δεδομένων συμβολοσειρών X, Y μια ακολουθία $(i_1, j_1), \ldots (i_k, j_k)$ ώστε

$$X[i_i] = Y[j_1], \ldots, X[i_k] = Y[j_k],$$

θα λέγεται ευθυγράμμιση.

Κωδικοποίηση Γινομένου

Λήμμα. Υπάρχουν συμβολοσειρές $C_A(0), C_A(1), C_B(0), C_B(1) \in \{0,1\}^3$**,** έτσι ώστε για κάθε $s, t \in \{0,1\}$ έχουμε

$$MK(C_A(s), C_B(t)) = 2 \cdot (1 - s \cdot t),$$

όπο $MK(X, Y)$ το μήκος της μέγιστης κοινής υπακολουθία των X, Y.

Κωδικοποίηση Γινομένου

Ορίζουμε

- $C_A(0) := 001$,
- $C_A(1) := 111$,
- $C_B(0) := 011$,
- $C_B(1) := 000$

Κωδικοποίηση *εσωτερικού* γινομένου

Λήμμα. Υπάρχουν $F_A, F_B : \{0,1\}^d \to \{0,1,2\}^{3d^2}$ έτσι ώστε για οποιαδήποτε $a, b \in \{0,1\}^d$ έχουμε

$$MK\left(F_A(a), F_B(b)\right) = (3d^2 - d) - 2\sum_{k=1}^{d} a[k] \cdot b[k].$$

Για $c \in \Sigma$ και θετικό ακέραιο n, έστω $c^n := \underbrace{c\, c \ldots c}_{n \text{ τιμες}}$.

Για $c \in \Sigma$ και θετικό ακέραιο n, έστω $c^n := \underbrace{c\, c \ldots c}_{n \text{ τιμες}}$.

Κατασκευάζουμε τις συμβολοσειρές ως:

- $F_A(a) := C_A(a[1])2^{3d}C_A(a[2])2^{3d} \ldots 2^{3d}C_A(a[d])$.
- $F_B(b) := C_B(b[1])2^{3d}C_B(b[2])2^{3d} \ldots 2^{3d}C_B(b[d])$.

Για $c \in \Sigma$ και θετικό ακέραιο n, έστω $c^n := \underbrace{c\, c \ldots c}_{n \text{ τιμες}}$.

Κατασκευάζουμε τις συμβολοσειρές ως:

- $F_A(a) := C_A(a[1])2^{3d}C_A(a[2])2^{3d} \ldots 2^{3d}C_A(a[d])$.
- $F_B(b) := C_B(b[1])2^{3d}C_B(b[2])2^{3d} \ldots 2^{3d}C_B(b[d])$.

$\star$ Θυμηθείτε ότι

1. $s \cdot t = 0 \leftrightarrow MK(C_A(s), C_B(t)) = 2$.
2. $s \cdot t = 1 \leftrightarrow MK(C_A(s), C_B(t)) = 0$.

Κατασκευή εσωτερικού γινομένου με κατώφλι

Λήμμα. Υπάρχουν $G_X, G_Y : \{0,1\}^d \to \{0,1,2,3\}^{6d^2-d-2}$, υπολογίσιμες σε χρόνο $O(d^2)$, έτσι ώστε για κάθε διάνυσμα $a, b \in \{0,1\}^d$ έχουμε

- $MK(G_X(a), G_Y(b)) = 3d^2 - d$, αν a, b κάθετα.
- $MK(G_X(a), G_Y(b)) = 3d^2 - d - 2$, διαφορετικά.

Κατασκευάζουμε τα $G_A(a), G_B(b)$ ως

- $G_A(a) := F_A(a)3^{3d^2-d-2}$
- $G_B(b) := 3^{3d^2-d-2}F_B(b)$

$\star$ Θυμηθείτε ότι

$$MK\left(F_A(a), F_B(b)\right) = (3d^2 - d) - 2\sum_{k=1}^{d} a[k] \cdot b[k].$$

Προς την τελική αναγωγή

Θεώρημα(Αναγωγή αναλυτικά): Δεδομένων συνόλων $A, B \subseteq \{0,1\}^d$ με $|A| = |B| = n$, μπορούμε σε χρόνο $O(nd^2)$ να κατασκευάσουμε συμβολοσειρές X, Y και έναν ακέραιο τ ώστε $MK(X, Y) \geq \tau$ αν και μόνο αν στα A, B περιέχει ένα ορθογώνιο ζεύγος διανυσμάτων.

Έστω $A = \{a_0, a_1, \ldots, a_n\}, B = \{b_0, b_1, \ldots, b_n\}$, και $\gamma := 6d^2 - d - 2$.

Ορίζουμε

- $X := G_A(a_0)\ 4^\gamma\ G_A(a_1)\ \ldots 4^\gamma G_A(a_{n-1})\ 4^\gamma\ G_A(a_1)\ 4^\gamma \ldots 4^\gamma\ G_A(a_{n-1})$
- $Y := 4^{n\gamma}\ G_B(b_0)\ 4^\gamma\ G_B(b_1) \ldots 4^\gamma G_B(b_{n-1})\ 4^{n\gamma}$

Έστω $A = \{a_0, a_1, \ldots, a_n\}, B = \{b_0, b_1, \ldots, b_n\}$, και $\gamma := 6d^2 - d - 2$.

Ορίζουμε

- $X := G_A(a_0)\ 4^\gamma\ G_A(a_1)\ \ldots 4^\gamma G_A(a_{n-1})\ 4^\gamma\ G_A(a_1)\ 4^\gamma \ldots 4^\gamma\ G_A(a_{n-1})$
- $Y := 4^{n\gamma}\ G_B(b_0)\ 4^\gamma\ G_B(b_1) \ldots 4^\gamma G_B(b_{n-1})\ 4^{n\gamma}$

Ισχυρισμός.

$$MK(X, Y) \geq (2n-1)\gamma + \max_{\Delta \in \{0,\ldots,n-1\}} \sum_{j=0}^{n-1} MK(G_A(a_{j+D \bmod n}), G_B(b_j)).$$

Έστω $A = \{a_0, a_1, \ldots, a_n\}, B = \{b_0, b_1, \ldots, b_n\}$, και $\gamma := 6d^2 - d - 2$.

Ορίζουμε

- $X := G_A(a_0)\ 4^\gamma\ G_A(a_1)\ \ldots 4^\gamma G_A(a_{n-1})\ 4^\gamma\ G_A(a_1)\ 4^\gamma \ldots 4^\gamma\ G_A(a_{n-1})$
- $Y := 4^{n\gamma}\ G_B(b_0)\ 4^\gamma\ G_B(b_1) \ldots 4^\gamma G_B(b_{n-1})\ 4^{n\gamma}$

Ισχυρισμός.

$$MK(X, Y) \geq (2n-1)\gamma + \max_{\Delta \in \{0,\ldots,n-1\}} \sum_{j=0}^{n-1} MK(G_A(a_{j+D \bmod n}), G_B(b_j)).$$

$\star$ ορθογώνιο ζεύγος υπάρχει
$\rightarrow MK(X, Y) \geq (2n-1) \cdot \gamma + (n-1) \cdot (3d^2 - d - 2) + 3d^- d = \tau.$

- $X := G_A(a_0)\ 4^\gamma\ G_A(a_1)\ \ldots 4^\gamma G_A(a_{n-1})\ 4^\gamma\ G_A(a_1)\ 4^\gamma \ldots 4^\gamma\ G_A(a_{n-1})$
- $Y := 4^{n\gamma}\ G_B(b_0)\ 4^\gamma\ G_B(b_1) \ldots 4^\gamma G_B(b_{n-1})\ 4^{n\gamma}$

$\star MK(X, Y) < \tau \rightarrow$ δεν υπάρχει ορθογώνιο ζεύγος $(a, b) \in A \times B$.

Σύνοψη

- Η Ισχυρή Υπόθεση Υποεκθετικού Χρόνου υποννοεί την Υπόθεση Ορθογώνιων Διανυσμάτων.
- Υπόθεση Ορθογώνιων Διανυσμάτων δίνει τετραγωνική δυσκολία για κλασικά προβλήματα συμβολοσειρών, τα οποία λύνονται με δυναμικό προγραμματισμό.

Ευχαριστούμε!