Μαθημα Τεταρτο

'Αρης Παγουρτζης, Βασιλης Νακος ΑΛΜΑ

Προηγούμενο Μάθημα

Υπόθεση δυσκολίας Συντομότερων Μονοπατιών, (Μιν,+) γινόμενο, προβλήματα τριγώνων σε γραφήματα, και κλάση ισοδυναμίας.

Προηγούμενο Μάθημα

Υπόθεση δυσκολίας Συντομότερων Μονοπατιών, (Μιν,+) γινόμενο, προβλήματα τριγώνων σε γραφήματα, και κλάση ισοδυναμίας.

Σήμερα: Μια πιο αναλυτική ματιά στο πρόβλημα 3SUM.

Προηγούμενο Μάθημα

Υπόθεση δυσκολίας Συντομότερων Μονοπατιών, (Μιν,+) γινόμενο, προβλήματα τριγώνων σε γραφήματα, και κλάση ισοδυναμίας.

Σήμερα: Μια πιο αναλυτική ματιά στο πρόβλημα 3SUM.
Η τελευταία από τις τρεις ‘μεγάλες’ υποθέσεις δυσκολίας.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

- Τετριμμένη λύση: $O(n^3)$.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

- Τετριμμένη λύση: $O(n^3)$.
- Γνωστή: $O(n^2)$.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

- Τετριμμένη λύση: $O(n^3)$.
- Γνωστή: $O(n^2)$.
- Προχωρημένη: $O(n^2 \cdot \left(\frac{\log \log n}{\log n}\right)^2)$.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

- Τετριμμένη λύση: $O(n^3)$.
- Γνωστή: $O(n^2)$.
- Προχωρημένη: $O(n^2 \cdot \left(\frac{\log \log n}{\log n}\right)^2)$.
- Υπόθεση δυσκολίας: Δεν υπάρχει $n^{2-\epsilon}$ αλγόριθμος.

Πρόβλημα 3SUM. Έστω A, B, C σύνολο ακεραίων, πληθικότητας n. Να βρεθεί αν υπάρχουν αριθμοί $a \in A, b \in B, c \in C$ ώστε $a + b + c = 0$.

- Τετριμμένη λύση: $O(n^3)$.
- Γνωστή: $O(n^2)$.
- Προχωρημένη: $O(n^2 \cdot \left(\frac{\log \log n}{\log n}\right)^2)$.
- Υπόθεση δυσκολίας: Δεν υπάρχει $n^{2-\epsilon}$ αλγόριθμος. Η πιο παλιά υπόθεση δυσκολίας, από Gajentaan, Overmars το 95.

Ισοδύναμες Εκδοχές

1. Δίνονται $A, B, C \subseteq \mathbb{Z}$. Να βρεθεί αν υπάρχουν $a \in A, b \in B, c \in C$ ώστε $a + b = c$.

Ισοδύναμες Εκδοχές

1. Δίνονται $A, B, C \subseteq \mathbb{Z}$. Να βρεθεί αν υπάρχουν $a \in A, b \in B, c \in C$ ώστε $a + b = c$.
2. Δίνονται $A, B, C \subseteq \mathbb{Z}$, και στόχος t. Να βρεθεί αν υπάρχουν $a \in A, b \in B, c \in C$ ώστε $a + b + c = t$.

Ισοδύναμες Εκδοχές

1. Δίνονται $A, B, C \subseteq \mathbb{Z}$. Να βρεθεί αν υπάρχουν $a \in A, b \in B, c \in C$ ώστε $a + b = c$.
2. Δίνονται $A, B, C \subseteq \mathbb{Z}$, και στόχος t. Να βρεθεί αν υπάρχουν $a \in A, b \in B, c \in C$ ώστε $a + b + c = t$.
3. Δίνονται $X \subseteq \mathbb{Z}$. Να βρεθεί αν υπάρχουν $a, b, c \in X$ ώστε $a + b + c = 0$.

Αλγόριθμοι για 3SUM

Αλγόριθμος 1. Αν $A, B, C \subseteq \{-U, U\}$, τότε υπάρχει μια $O(U \log U)$ λύση χρησιμοποιώντας πολλαπλασιασμό πολυωνύμων.

Αλγόριθμοι για 3SUM

Αλγόριθμος 1. Αν $A, B, C \subseteq \{-U, U\}$, τότε υπάρχει μια $O(U \log U)$ λύση χρησιμοποιώντας πολλαπλασιασμό πολυωνύμων.

Έστω

$$p(x) = \left(\sum_{a \in A} x^a\right) \cdot \left(\sum_{b \in B} x^b\right) \cdot \left(\sum_{c \in C} x^c\right)$$

Αλγόριθμοι για 3SUM

Αλγόριθμος 1. Αν $A, B, C \subseteq \{-U, U\}$, τότε υπάρχει μια $O(U \log U)$ λύση χρησιμοποιώντας πολλαπλασιασμό πολυωνύμων.

Έστω

$$p(x) = \left(\sum_{a \in A} x^a\right) \cdot \left(\sum_{b \in B} x^b\right) \cdot \left(\sum_{c \in C} x^c\right)$$

Ο συντελεστής x^t στο $p(x)$ τι δείχνει, οέο;

Ο τετραγωνικός αλγόριθμος

Ας επικεντρωθούμε στην περίπτωση $A = B = C$.
Ταξινομούμε το A: $A = \{a_1, \ldots, a_n\}$.

Θα κοιτάξουμε για κάθε $c \in A$ αν υπάρχουν $a, b \in A$ ώστε $a + b = -c$.
$\star i = n, j = 1$
Όσο $i > 0$ και $j \leq n$:

- Αν $a_i + a_j = -c$ επέστρεψε ΝΑΙ
- Αν $a_i + a_j > -c$ $i := i - 1$.
- Αν $a_i + a_j < -c$ $j := j + 1$.

Επέστρεψε ΟΧΙ

Δέντρα Πολυπλοκότητας

Θεώρημα. Το πρόβλημα 3SUM επιδέχεται δέντρο απόφασης βάθους $O(n^{\frac{3}{2}} \log n)$.

Υπενθύμιση: Δέντρο απόφασης ενός προβλήματος P με είσοδο $x_1, x_2, \ldots, x_n$ είναι ένα δέντρο, όπου κάθε κόμβος περιέχει μία σύγκριση της μορφής $x_i \leq x_j$ (ή γραμμικό συνδυασμό $\sum_i \alpha_i x_i \geq 0$). Οι ακμές είναι $0/1$, και ακολουθούνται ανάλογα το αποτέλεσμα της σύγκρισης.

Δέντρα Πολυπλοκότητας

Θεώρημα. Το πρόβλημα 3SUM επιδέχεται δέντρο απόφασης βάθους $O(n^{\frac{3}{2}} \log n)$.

Υπενθύμιση: Δέντρο απόφασης ενός προβλήματος P με είσοδο $x_1, x_2, \ldots, x_n$ είναι ένα δέντρο, όπου κάθε κόμβος περιέχει μία σύγκριση της μορφής $x_i \leq x_j$ (ή γραμμικό συνδυασμό $\sum_i \alpha_i x_i \geq 0$). Οι ακμές είναι $0/1$, και ακολουθούνται ανάλογα το αποτέλεσμα της σύγκρισης.

Τι μας λένε τα δέντρα πολυπλοκότητας;
Επίσης, που τα έχουμε ξαναδει;

1. Τι μας λένε τα δέντρα πολυπλοκότητας;

1. Τι μας λένε τα δέντρα πολυπλοκότητας;
   Κάτω φράγματα σε δέντρα πολυπλοκότητας $\Rightarrow$ κάτω φράγματα σε μοντέλα υπολογισμού.

1. Τι μας λένε τα δέντρα πολυπλοκότητας;
   Κάτω φράγματα σε δέντρα πολυπλοκότητας $\Rightarrow$ κάτω φράγματα σε μοντέλα υπολογισμού.
2. Επίσης, που τα έχουμε ξαναδει;

1. Τι μας λένε τα δέντρα πολυπλοκότητας;
   Κάτω φράγματα σε δέντρα πολυπλοκότητας $\Rightarrow$ κάτω φράγματα σε μοντέλα υπολογισμού.
2. Επίσης, που τα έχουμε ξαναδει;
   Απόδειξη ότι οποιοσδήποτε αλγόριθμος ταξινόμησης που βασίζεται σε συγκρίσεις απαιτεί $\Omega(n \log n)$ χρόνο.

Αλλά τι μας ενδιαφέρουν οι αλγόριθμοι (άνω φράγματα) για τα δέντρα αποφάσεων;;

1. Τι μας λένε τα δέντρα πολυπλοκότητας;
   Κάτω φράγματα σε δέντρα πολυπλοκότητας $\Rightarrow$ κάτω φράγματα σε μοντέλα υπολογισμού.
2. Επίσης, που τα έχουμε ξαναδει;
   Απόδειξη ότι οποιοσδήποτε αλγόριθμος ταξινόμησης που βασίζεται σε συγκρίσεις απαιτεί $\Omega(n \log n)$ χρόνο.

Αλλά τι μας ενδιαφέρουν οι αλγόριθμοι (άνω φράγματα) για τα δέντρα αποφάσεων;;

Μας λένε πότε ένα κάτω φράγμα **δεν** μπορεί να αποδειχθεί χρησιμοποιώντας τη συγκεκριμένη μέθοδο.

1. Τι μας λένε τα δέντρα πολυπλοκότητας;
   Κάτω φράγματα σε δέντρα πολυπλοκότητας $\Rightarrow$ κάτω φράγματα σε μοντέλα υπολογισμού.
2. Επίσης, που τα έχουμε ξαναδει;
   Απόδειξη ότι οποιοσδήποτε αλγόριθμος ταξινόμησης που βασίζεται σε συγκρίσεις απαιτεί $\Omega(n \log n)$ χρόνο.

Αλλά τι μας ενδιαφέρουν οι αλγόριθμοι (άνω φράγματα) για τα δέντρα αποφάσεων;;

Μας λένε πότε ένα κάτω φράγμα **δεν** μπορεί να αποδειχθεί χρησιμοποιώντας τη συγκεκριμένη μέθοδο.

Ή μπορούν να λειτουργήσουν σαν ενδιάμεσος σταθμός προς έναν αλγόριθμο.

Μικρά Δέντρα αποφάσεων για το 3SUM

Βήμα 1. Ταξινομούμε το A σε αύξουσα σειρα: $O(n \log n)$ συγκρίσεις.

Μικρά Δέντρα αποφάσεων για το 3SUM

Βήμα 1. Ταξινομούμε το A σε αύξουσα σειρα: $O(n \log n)$ συγκρίσεις.

Βήμα 2. Σπάμε το A σε n/g διαδοχικές ομάδες $A_1, A_2, \ldots, A_{n/g}$.

Μικρά Δέντρα αποφάσεων για το 3SUM

Βήμα 1. Ταξινομούμε το A σε αύξουσα σειρα: $O(n \log n)$ συγκρίσεις.

Βήμα 2. Σπάμε το A σε n/g διαδοχικές ομάδες $A_1, A_2, \ldots, A_{n/g}$.

Βήμα 3. Ταξινομούμε το πολυσύνολο

$$D = \cup_{i=1}^{n/g} (A_i - A_i) = \cup_{i=1}^{n/g} \{a - b | a, b \in A_i\},$$

σε αύξουσα σειρά. Απαιτούνται $O(ng \log n)$ συγκρίσεις, και έχουμε μία λίστα L η οποία περιέχει τριάδες i, j, k με $i \in [n/g], j, k \in [g]$ κατά αύξοντα $a_{i,j} - a_{i,k}$.

Βήμα 4. Ταξινομούμε τα $A_{i,j} := A_i + A_j = \{a + b | a \in A_i, b \in A_j\}$, με ο συγκρίσεις, λόγω του βήματος 3!

Βήμα 3. Ταξινομούμε το πολυσύνολο

$$D = \cup_{i=1}^{n/g} A_i - A_i = \cup_{i=1}^{n/g} \{a - b | a, b \in A_i\},$$

σε αύξουσα σειρά. Απαιτούνται $O(ng \log n)$ συγκρίσεις, και έχουμε μία λίστα L η οποία περιέχει τριάδες i, j, k με $i \in [n/g], j, k \in [g]$ κατά αύξοντα $a_{i,j} - a_{i,k}$.

Βήμα 4. Ταξινομούμε τα $A_{i,j} := A_i + A_j = \{a + b | a \in A_i, b \in A_j\}$, με ο συγκρίσεις, λόγω του βήματος 3!

Εφόσον

$$a_{i,j} + a_{i',j'} \leq a_{i,k} + a_{i',k'} \iff a_{i',j'} - a_{i',k} \leq a_{i,k} - a_{i,j},$$

αρκεί να ελέγξουμε αν το (i', j', k') εμφανίζεται πριν από το (i, j, k) στη λίστα L.

Θα κοιτάξουμε για κάθε $c \in A$ αν υπάρχουν $a, b \in A$ ώστε $a + b = -c$.

Θα κοιτάξουμε για κάθε $c \in A$ αν υπάρχουν $a, b \in A$ ώστε $a + b = -c$.

$\star i = n/g, j = 1$
Όσο $i > 0$ και $j \leq n/g$:

- Αν $-c \in A_{i,j}$ επέστρεψε ΝΑΙ (δυαδική αναζήτηση)
- Αν $\min(A_i) + \max(A_j) > -c$, θέσε $i := i - 1$.
- Αν τίποτε από τα παραπάνω, θέσε $j := j + 1$.

Επέστρεψε ΟΧΙ

Θα κοιτάξουμε για κάθε $c \in A$ αν υπάρχουν $a, b \in A$ ώστε $a + b = -c$.

$\star i = n/g, j = 1$
Όσο $i > 0$ και $j \leq n/g$:

- Αν $-c \in A_{i,j}$ επέστρεψε ΝΑΙ (δυαδική αναζήτηση)
- Αν $\min(A_i) + \max(A_j) > -c$, θέσε $i := i - 1$.
- Αν τίποτε από τα παραπάνω, θέσε $j := j + 1$.

Επέστρεψε ΟΧΙ

Πλήθος συγκρίσεων. $O((ng + n^2/g) \log n) = O(n^{\frac{3}{2}} \log n)$, για $g := \sqrt{n}$.

Ώρα για αναγωγές!

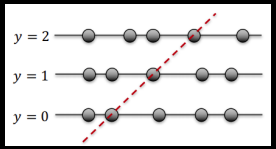
Πρόβλημα GeomBase: Δίνονται n σημεία σε τρεις οριζόντιες γραμμές $y = 0, y = 1, y = 2$. Να βρεθεί αν υπάρχει μία μη οριζόντια γραμμή που περιέχει τρία σημεία.

Ισχυρισμός. Δεν υπάρχει υποτετραγωνικός αλγόριθμος, εκτός αν η υπόθεση 3SUM καταρρέει.

Ώρα για αναγωγές!

Πρόβλημα GeomBase: Δίνονται n σημεία σε τρεις οριζόντιες γραμμές $y = 0, y = 1, y = 2$. Να βρεθεί αν υπάρχει μία μη οριζόντια γραμμή που περιέχει τρία σημεία.

Ισχυρισμός. Δεν υπάρχει υποτετραγωνικός αλγόριθμος, εκτός αν η υπόθεση 3SUM καταρρέει.

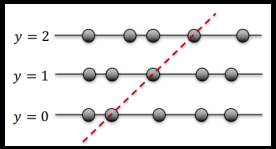


Για ένα (A, B, C) στιγμιότυπο του 3SUM κατασκευάζουμε σημεία $(a, 0)$ για $a \in A$, $(b, 2)$ για $b \in B$, $(c/2, 1)$ για $c \in C$.

Ώρα για αναγωγές!

Πρόβλημα GeomBase: Δίνονται n σημεία σε τρεις οριζόντιες γραμμές $y = 0, y = 1, y = 2$. Να βρεθεί αν υπάρχει μία μη οριζόντια γραμμή που περιέχει τρία σημεία.

Ισχυρισμός. Δεν υπάρχει υποτετραγωνικός αλγόριθμος, εκτός αν η υπόθεση 3SUM καταρρέει.



Για ένα (A, B, C) στιγμιότυπο του 3SUM κατασκευάζουμε σημεία $(a, 0)$ για $a \in A$, $(b, 2)$ για $b \in B$, $(c/2, 1)$ για $c \in C$.
Τρία σημεία είναι συνευθειακά αν $c/2 - a = b - c/2 \iff a + b = c$.

Ένα κλασικό γεωμετρικό πρόβλημα: δοθέντων n σημείων στο επίπεδο, υπάρχει ευθεία με τουλάχιστον 3 σημεία πάνω της·

Ένα κλασικό γεωμετρικό πρόβλημα: δοθέντων n σημείων στο επίπεδο, υπάρχει ευθεία με τουλάχιστον 3 σημεία πάνω της·
Ισχυρισμός. Δεν υπάρχει $n^{2-\epsilon}$ αλγόριθμος, εκτός αν η 3SUM εικασία καταρρέει.

Ένα κλασικό γεωμετρικό πρόβλημα: δοθέντων n σημείων στο επίπεδο, υπάρχει ευθεία με τουλάχιστον 3 σημεία πάνω της·
Ισχυρισμός. Δεν υπάρχει $n^{2-\epsilon}$ αλγόριθμος, εκτός αν η 3SUM εικασία καταρρέει.

Δοθέντος στιγμιοτύπου A του 3SUM, κατασκευάζουμε σημεία $(a, a^3), \forall a \in A$.

Ένα κλασικό γεωμετρικό πρόβλημα: δοθέντων n σημείων στο επίπεδο, υπάρχει ευθεία με τουλάχιστον 3 σημεία πάνω της·
Ισχυρισμός. Δεν υπάρχει $n^{2-\epsilon}$ αλγόριθμος, εκτός αν η 3SUM εικασία καταρρέει.

Δοθέντος στιγμιοτύπου A του 3SUM, κατασκευάζουμε σημεία $(a, a^3), \forall a \in A$.
Τα σημεία $(a, a^3), (b, b^3), (c, c^3)$ είσαι συνευθειακά αν και μόνο αν

$$\frac{a^3 - b^3}{a - b} = \frac{c^3 - b^3}{c - b} \iff a + b + c = 0.$$

Το 3SUM είναι δύσκολο ακόμα και με μικρά στοιχεία

Θεώρημα. Το 3SUM μπορεί να αναχθεί σε γραμμικό χρόνο στην περίπτωση όπου $A, B, C \subseteq [\mathcal{O}(n^3)]$.

Το 3SUM είναι δύσκολο ακόμα και με μικρά στοιχεία

Θεώρημα. Το 3SUM μπορεί να αναχθεί σε γραμμικό χρόνο στην περίπτωση όπου $A, B, C \subseteq [\mathcal{O}(n^3)]$.

Ανοικτά ερωτήματα. Είναι υποτετραγωνικά δύσκολο το 3SUM όταν $A, B, C \subseteq [n^{2+\delta}]$, για $0 \leq \delta < 1$;

Τα εργαλεία μας

Το εργαλείο μας: (Μαγικές) Συναρτήσεις κατακερματισμού κατάλληλες για μία τέτοια αναγωγή..

Τα εργαλεία μας

Το εργαλείο μας: (Μαγικές) Συναρτήσεις κατακερματισμού κατάλληλες για μία τέτοια αναγωγή..

1. $g : [U] \to [p]$, με $g(x) = x \bmod p$, όπου p πρώτος (Ολομορφικός κατακερματισμός).

Τα εργαλεία μας

Το εργαλείο μας: (Μαγικές) Συναρτήσεις κατακερματισμού κατάλληλες για μία τέτοια αναγωγή..

1. $g : [U] \to [p]$, με $g(x) = x \bmod p$, όπου p πρώτος (Ολομορφικός κατακερματισμός).
2. $t : [U] \to [m]$, με
$$h(x) = (\sigma x) \bmod p \bmod m,$$
όπου p πρώτος $\geq 2U$, και $\sigma \in \mathbb{Z}_p^*$ (γραμμικός κατακερματισμός).

Τα εργαλεία μας

Το εργαλείο μας: (Μαγικές) Συναρτήσεις κατακερματισμού κατάλληλες για μία τέτοια αναγωγή..

1. $g : [U] \to [p]$, με $g(x) = x \bmod p$, όπου p πρώτος (Ολομορφικός κατακερματισμός).
2. $t : [U] \to [m]$, με
$$h(x) = (\sigma x) \bmod p \bmod m,$$
όπου p πρώτος $\geq 2U$, και $\sigma \in \mathbb{Z}_p^*$ (γραμμικός κατακερματισμός).
3. $h : [U] \to [m]$ με
$$h(x) = (\sigma x) \bmod N \operatorname{div} m,$$
όπου N, m δυνάμεις του 2, και $\sigma \in \mathbb{Z}_N^*$ (γραμμικός κερματισμός II).

Οι τρεις πιο κλασικές συναρτήσεις κατακερματισμού. Η τυχαιότητα βρίσκεται

1. στην h στην επιλογή του πρώτου p.
2. Στις t, h στην επιλογή του σ.

Οι τρεις πιο κλασικές συναρτήσεις κατακερματισμού. Η τυχαιότητα βρίσκεται

1. στην h στην επιλογή του πρώτου p.
2. Στις t, h στην επιλογή του σ.

Για την ακρίβεια, η g (αντίστοιχα h, t) ορίζει μία *οικογένεια* συναρτήσεων, από την οποία επιλέγεται μία συνάρτηση στην τύχη.

Οι τρεις πιο κλασικές συναρτήσεις κατακερματισμού. Η τυχαιότητα βρίσκεται

1. στην h στην επιλογή του πρώτου p.
2. Στις t, h στην επιλογή του σ.

Για την ακρίβεια, η g (αντίστοιχα h, t) ορίζει μία *οικογένεια* συναρτήσεων, από την οποία επιλέγεται μία συνάρτηση στην τύχη.

Ορισμός: Μία τυχαία συνάρτηση κατακερματισμού $f : [U] \to [m]$ λέγεται d-οικουμενική αν

$$\forall x, y \in [U] : \mathbb{P}\{f(x) = f(y)\} \leq \frac{d}{U}.$$

Οι τρεις πιο κλασικές συναρτήσεις κατακερματισμού. Η τυχαιότητα βρίσκεται

1. στην h στην επιλογή του πρώτου p.
2. Στις t, h στην επιλογή του σ.

Για την ακρίβεια, η g (αντίστοιχα h, t) ορίζει μία *οικογένεια* συναρτήσεων, από την οποία επιλέγεται μία συνάρτηση στην τύχη.

Ορισμός: Μία τυχαία συνάρτηση κατακερματισμού $f : [U] \to [m]$ λέγεται d-οικουμενική αν

$$\forall x, y \in [U] : \mathbb{P}\{f(x) = f(y)\} \leq \frac{d}{U}.$$

Ιδανικά, θέλουμε $d = 1$.

1. $g : [U] \to [p]$ είναι αφινική, δηλαδή

$$(g(x+y) = g(x) + g(y)) \bmod p,$$

αλλά

1. $g : [U] \to [p]$ είναι αφινική, δηλαδή

$$(g(x+y) = g(x) + g(y)) \bmod p,$$

   αλλά είναι $O(\log U)$-οικουμενική.
2. $t : [U] \to [m]$ είναι 4-οικουμενική,

1. $g : [U] \to [p]$ είναι αφινική, δηλαδή

$$(g(x+y) = g(x) + g(y)) \bmod p,$$

αλλά είναι $O(\log U)$-οικουμενική.

2. $t : [U] \to [m]$ είναι 4-οικουμενική, αλλά είναι *σχεδόν* αφινική:

$$(t(x+y) - t(x) - t(y)) \bmod m \in \{0, U \bmod m\}.$$

3. $h : [U] \to [p]$ είναι 4-οικουμενική,

1. $g : [U] \to [p]$ είναι αφινική, δηλαδή

$$(g(x+y) = g(x) + g(y)) \bmod p,$$

αλλά είναι $O(\log U)$-οικουμενική.

2. $t : [U] \to [m]$ είναι 4-οικουμενική, αλλά είναι *σχεδόν* αφινική:

$$(t(x+y) - t(x) - t(y)) \bmod m \in \{0, U \bmod m\}.$$

3. $h : [U] \to [p]$ είναι 4-οικουμενική, αλλά *σχεδόν* αφινική:

$$h(x+y) - h(x) - h(y) \in \{-1, 0\} \bmod m.$$

1. Παίρνουμε τυχαία $h : [U] \to [m], m := \Theta(n^3)$.
2. $A' := \{h(a)|a \in A\}, B' := \{h(b), b \in B\}, C' := \{h(c)|c \in C\}$
3. $A'' := \{h(a)|a \in A\}, B'' := \{h(b), b \in B\}, C'' := \{h(c) + 1|c \in C\}$
4. Λύνουμε τα (A', B', C') και (A'', B'', C'') (δουλεύομε μοδ μ).

1. Παίρνουμε τυχαία $h : [U] \to [m], m := \Theta(n^3)$.
2. $A' := \{h(a) | a \in A\}, B' := \{h(b), b \in B\}, C' := \{h(c) | c \in C\}$
3. $A'' := \{h(a) | a \in A\}, B'' := \{h(b), b \in B\}, C'' := \{h(c) + 1 | c \in C\}$
4. Λύνουμε τα (A', B', C') και (A'', B'', C'') (δουλεύομε μοδ μ).
5. Αν τα τελικά στιγμιότυπα δεν έχουν λύση, ανακοινώνουμε ότι δεν υπάρχει λύση.

1. Παίρνουμε τυχαία $h : [U] \to [m], m := \Theta(n^3)$.
2. $A' := \{h(a) | a \in A\}, B' := \{h(b), b \in B\}, C' := \{h(c) | c \in C\}$
3. $A'' := \{h(a) | a \in A\}, B'' := \{h(b), b \in B\}, C'' := \{h(c) + 1 | c \in C\}$
4. Λύνουμε τα (A', B', C') και (A'', B'', C'') (δουλεύομε μοδ μ).
5. Αν τα τελικά στιγμιότυπα δεν έχουν λύση, ανακοινώνουμε ότι δεν υπάρχει λύση.
6. Αλλιώς, αν λύση (x', y', z') για το (A', B', C'), ελέγχουμε αν $h^{-1}(x') + h^{-1}(y') = h^{-1}(z')$.
7. Αλλιώς, αν λύση (x', y', z') για το (A', B', C'), κοιτάμε αν $h^{-1}(x') + h^{-1}(y') = h^{-1}(z' - 1)$.

Ανάλυση.

Η λύση θα βρεθεί: Αν $x + y = z$ με $(x, y, z) \in A \times B \times C$ τότε $(h(x) + h(y)) \bmod m \in (h(z) + \{0, 1\}) \bmod m$, οπότε είτε στο (A', B', C') είτε στο (A'', B'', C'') θα υπάρχει λύση.

Ανάλυση.

Η λύση θα βρεθεί: Αν $x + y = z$ με $(x, y, z) \in A \times B \times C$ τότε $(h(x) + h(y)) \bmod m \in (h(z) + \{0, 1\}) \bmod m$, οπότε είτε στο (A', B', C') είτε στο (A'', B'', C'') θα υπάρχει λύση.

Δεν υπάρχουν ψευδολύσεις: Έστω $(x, y, z) \in A \times B \times C$. Ποια η πιθανότητα $(h(x) + h(y)) = h(z') \bmod m$;

Ανάλυση.

Η λύση θα βρεθεί: Αν $x + y = z$ με $(x, y, z) \in A \times B \times C$ τότε $(h(x) + h(y)) \bmod m \in (h(z) + \{0, 1\}) \bmod m$, οπότε είτε στο (A', B', C') είτε στο (A'', B'', C'') θα υπάρχει λύση.

Δεν υπάρχουν ψευδολύσεις: Έστω $(x, y, z) \in A \times B \times C$. Ποια η πιθανότητα $(h(x) + h(y)) = h(z') \bmod m$;
Λόγω της περίπου αφινικότητας, πρέπει το $h(x + y - z)$ να πέφτει σε ένα σύνολο μεγέθους 4 (γιατί;). Αυτό συμβαίνει με $O(\frac{1}{n})$ πιθανότητα.

Ανάλυση.

Η λύση θα βρεθεί: Αν $x + y = z$ με $(x, y, z) \in A \times B \times C$ τότε $(h(x) + h(y)) \bmod m \in (h(z) + \{0, 1\}) \bmod m$, οπότε είτε στο (A', B', C') είτε στο (A'', B'', C'') θα υπάρχει λύση.

Δεν υπάρχουν ψευδολύσεις: Έστω $(x, y, z) \in A \times B \times C$. Ποια η πιθανότητα $(h(x) + h(y)) = h(z') \bmod m$;
Λόγω της περίπου αφινικότητας, πρέπει το $h(x + y - z)$ να πέφτει σε ένα σύνολο μεγέθους 4 (γιατί;). Αυτό συμβαίνει με $O(\frac{1}{n})$ πιθανότητα.

Μπορούμε να πάρουμε ένα φράγμα ένωσης (union bound) πάνω σε όλες τις τριάδες, να συμπεράνουμε ότι δεν υπάρχει ψευδολύση.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

- Πιο ‘δομημένο’ πρόβλημα από το 3SUM.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

- Πιο 'δομημένο' πρόβλημα από το 3SUM.
- Αν 3SUM υποτετραγωνικά επιλύσιμο, τότε πρέπει να λύσουμε το Συνελικτικό 3SUM πρώτα.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

- Πιο 'δομημένο' πρόβλημα από το 3SUM.
- Αν 3SUM υποτετραγωνικά επιλύσιμο, τότε πρέπει να λύσουμε το Συνελικτικό 3SUM πρώτα.
- Ωστόσο, 3SUM υποτετραγωνικά *ισοδύναμο* με συνελικτικό 3SUM.

Ένα ενδιάμεσο πρόβλημα.

Συνελικτικό 3SUM. Δίνεται πίνακας ακεραίων A μήκους n. Να βρεθεί αν υπάρχουν δείκτες i, j με $i + j \leq n$ ώστε $A[i] + A[j] = A[i + j]$.

- Πιο 'δομημένο' πρόβλημα από το 3SUM.
- Αν 3SUM υποτετραγωνικά επιλύσιμο, τότε πρέπει να λύσουμε το Συνελικτικό 3SUM πρώτα.
- Ωστόσο, 3SUM υποτετραγωνικά *ισοδύναμο* με συνελικτικό 3SUM.
- Χρησιμοποιείται ως ενδιάμεσος σταθμός δυσκολίας για άλλα προβλήματα (δες πρώτη σειρά σκήσεων).

Στη σειρά ασκήσεων

Προβλήματα με τρίγωνα (ξανά): Δίνεται γραος G με βάρη στις ακμές. Να βρεθεί αν υπάρχει τρίγωνο v_1, v_2, v_3 **μηδενικού βάρους** στο G, δηλαδή

$$w(v_1, v_2) + w(v_2, v_3) + w(v_3, v_4) = 0.$$

Στη σειρά ασκήσεων

Προβλήματα με τρίγωνα (ξανά): Δίνεται γραος G με βάρη στις ακμές. Να βρεθεί αν υπάρχει τρίγωνο v_1, v_2, v_3 **μηδενικού βάρους** στο G, δηλαδή

$$w(v_1, v_2) + w(v_2, v_3) + w(v_3, v_4) = 0.$$

Στην προηγούμενη διάλεξη είδαμε το πρόβλημα **αρνητικού τριγώνου**, και είπαμε ότι είναι υποκυβικά ισοδύναμο με το Πρόβλημα Συντομότερων Μονοπατιών.

Στη σειρά ασκήσεων

Προβλήματα με τρίγωνα (ξανά): Δίνεται γραος G με βάρη στις ακμές. Να βρεθεί αν υπάρχει τρίγωνο v_1, v_2, v_3 **μηδενικού βάρους** στο G, δηλαδή

$$w(v_1, v_2) + w(v_2, v_3) + w(v_3, v_4) = 0.$$

Στην προηγούμενη διάλεξη είδαμε το πρόβλημα **αρνητικού τριγώνου**, και είπαμε ότι είναι υποκυβικά ισοδύναμο με το Πρόβλημα Συντομότερων Μονοπατιών.

Θα δούμε ότι το 3SUM ανάγεται στο πρόβλημα **μηδενικού** τριγώνου σε $n^{\frac{3}{2}}$ χρόνο.

Λίγη ιστορία ακόμα

Θεώρημα. (Williams and Williams, 2009) Το πρόβλημα αρνητικού τριγώνου ανάγεται στο πρόβλημα αρνητικού τριγώνου, όταν τα βάρη των ακμών είναι πολυωνυμικά μικρά.

Λίγη ιστορία ακόμα

Θεώρημα. (Williams and Williams, 2009) Το πρόβλημα αρνητικού τριγώνου ανάγεται στο πρόβλημα αρνητικού τριγώνου, όταν τα βάρη των ακμών είναι πολυωνυμικά μικρά.

Άρα το πρόβλημα του μηδενικού τριγώνου είναι APSP-δύσκολο.Αλλά είναι και 3SUM-δύσκολο.

Λίγη ιστορία ακόμα

Θεώρημα. (Williams and Williams, 2009) Το πρόβλημα αρνητικού τριγώνου ανάγεται στο πρόβλημα αρνητικού τριγώνου, όταν τα βάρη των ακμών είναι πολυωνυμικά μικρά.

Άρα το πρόβλημα του μηδενικού τριγώνου είναι APSP-δύσκολο.Αλλά είναι και 3SUM-δύσκολο.

Ακόμα και μία από τις δύο εικασίες να καταρρέει, τότε το εν λόγω πρόβλημα μπορεί να είναι δύσκολο λόγω της άλλης. Μάλλον είναι όντως δύσκολο ...

Ευχαριστούμε!