

Προηγμένα Θέματα Αλγορίθμων

Γρήγορος Μετασχηματισμός Fourier και συνελίξεις II

Βασίλειος Νάκος

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Αλγόριθμος FFT

- 1: $\text{FFT}(p, N)$
- 2: Αν $N = 1$ επέστρεψε a_0
- 3: Έστω $p_{\text{even}} = \sum_{0 \leq k < N/2} a_{2k} x^k$.
- 4: Έστω $p_{\text{odd}} = \sum_{0 \leq k < N/2} a_{2k+1} x^k$.
- 5: $\text{FFT}(p_{\text{even}}, N/2)$
- 6: $\text{FFT}(p_{\text{odd}}, N/2)$
- 7: Για $i = 0$ ως $N - 1$
- 8: $p(\omega^i) = p_{\text{even}}(\omega^{2i}) + \omega^i \cdot p_{\text{odd}}(\omega^{2i})$
- 9: Επέστρεψε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{N-1})$

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}$

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το
 $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Ο τετριμμένος αλγόριθμος σε χρόνο: $O(|A| \cdot |B|)$.

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Ο τετριμμένος αλγόριθμος σε χρόνο: $O(|A| \cdot |B|)$.

👁 Μπορούμε να βρούμε το $A + B$ σε χρόνο $O(u \log u)$:

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Ο τετριμμένος αλγόριθμος σε χρόνο: $O(|A| \cdot |B|)$.

👁 Μπορούμε να βρούμε το $A + B$ σε χρόνο $O(u \log u)$:

★ Ορίζουμε $p(x) = \sum_{a \in A} x^a, q(x) = \sum_{x \in B} x^B$

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Ο τετριμμένος αλγόριθμος σε χρόνο: $O(|A| \cdot |B|)$.

👁 Μπορούμε να βρούμε το $A + B$ σε χρόνο $O(u \log u)$:

★ Ορίζουμε $p(x) = \sum_{a \in A} x^a, q(x) = \sum_{x \in B} x^B$

και υπολογίζουμε το $p(x) \cdot q(x)$ σε χρόνο $O(u \log u)$:

Μία χρήση του FFT.

Δίνονται δύο σύνολο $A, B \subseteq [u]$. Να βρεθεί το $A + B := \{a + b \mid a \in A, b \in B\} \subseteq [2u]$.

Παράδειγμα: $A = \{1, 2\}, B = \{3, 4, 5\}, A + B = \{4, 5, 6, 7\}$.

Ο τετριμμένος αλγόριθμος σε χρόνο: $O(|A| \cdot |B|)$.

👁 Μπορούμε να βρούμε το $A + B$ σε χρόνο $O(u \log u)$:

★ Ορίζουμε $p(x) = \sum_{a \in A} x^a, q(x) = \sum_{x \in B} x^B$

και υπολογίζουμε το $p(x) \cdot q(x)$ σε χρόνο $O(u \log u)$:

👉 από τους μη μηδενικούς συντελεστές του διαβάζουμε το $A + B$.

Πρόβλημα Αθροίσματος Υποσυνόλου.

Δοθέντων n αριθμών $x_1, x_2, \dots, x_n, t$ να βρεθεί αν υπάρχει υποσύνολο των αριθμών S ώστε $\sum_{i \in S} x_i = t$.

Μέσω δυναμικού προγραμματισμού σε $O(n \cdot t)$ (αλγόριθμος Bellman):
★ Έστω $A[i][u]$ ο πίνακας που δηλώνει αν μπορώ να φτιάξω το u χρησιμοποιώντας μόνο τους i πρώτους αριθμούς.

Πρόβλημα Αθροίσματος Υποσυνόλου.

Δοθέντων n αριθμών $x_1, x_2, \dots, x_n, t$ να βρεθεί αν υπάρχει υποσύνολο των αριθμών S ώστε $\sum_{i \in S} x_i = t$.

Μέσω δυναμικού προγραμματισμού σε $O(n \cdot t)$ (αλγόριθμος Bellman):
★ Έστω $A[i][u]$ ο πίνακας που δηλώνει αν μπορώ να φτιάξω το u χρησιμοποιώντας μόνο τους i πρώτους αριθμούς.

- $A[0][0] = T$
- $A[0][u] = F$, για $u \in [t]$
- $A[i][u] = A[i-1][u] \vee A[i-1][u - x_i]$ για $x_i \leq u$.

Πρόβλημα Αθροίσματος Υποσυνόλου.

Δοθέντων n αριθμών $x_1, x_2, \dots, x_n, t$ να βρεθεί αν υπάρχει υποσύνολο των αριθμών S ώστε $\sum_{i \in S} x_i = t$.

Μέσω δυναμικού προγραμματισμού σε $O(n \cdot t)$ (αλγόριθμος Bellman):
★ Έστω $A[i][u]$ ο πίνακας που δηλώνει αν μπορώ να φτιάξω το u χρησιμοποιώντας μόνο τους i πρώτους αριθμούς.

- $A[0][0] = T$
- $A[0][u] = F$, για $u \in [t]$
- $A[i][u] = A[i-1][u] \vee A[i-1][u - x_i]$ για $x_i \leq u$.

Μπορώ να κάνω καλύτερα από $n \cdot t$;

Μία εναλλακτική λύση.

Ορίζουμε ως $\mathcal{S}(X, t)$ το σύνολο όλων των αριθμών $\leq t$ που μπορούν να φτιαχτούν χρησιμοποιώντας υποσύνολα του X .

Μία εναλλακτική λύση.

Ορίζουμε ως $\mathcal{S}(X, t)$ το σύνολο όλων των αριθμών $\leq t$ που μπορούν να φτιαχτούν χρησιμοποιώντας υποσύνολα του X . Δηλαδή,

$$\mathcal{S}(X, t) := \left\{ z \mid z \leq t \vee \exists S \subseteq X : \sum_{i \in S} x_i = z \right\}.$$

Μία εναλλακτική λύση.

Ορίζουμε ως $\mathcal{S}(X, t)$ το σύνολο όλων των αριθμών $\leq t$ που μπορούν να φτιαχτούν χρησιμοποιώντας υποσύνολα του X . Δηλαδή,

$$\mathcal{S}(X, t) := \left\{ z \mid z \leq t \vee \exists S \subseteq X : \sum_{i \in S} x_i = z \right\}.$$

Η ερώτηση γίνεται “ $t \in \mathcal{S}(X, t)$;

Μία εναλλακτική λύση.

Ορίζουμε ως $\mathcal{S}(X, t)$ το σύνολο όλων των αριθμών $\leq t$ που μπορούν να φτιαχτούν χρησιμοποιώντας υποσύνολα του X . Δηλαδή,

$$\mathcal{S}(X, t) := \left\{ z \mid z \leq t \vee \exists S \subseteq X : \sum_{i \in S} x_i = z \right\}.$$

Η ερώτηση γίνεται “ $t \in \mathcal{S}(X, t)$;

- 1: Αφελές FFT Άθροισμα Υποσυνόλου($x_1, \dots, x_n, t$)
- 2: $Z := \emptyset$
- 3: Για $i = 1$ έως n
- 4: $Z := Z + \{x_i\}$
- 5: //Μέσω FFT σε $O(t \log t)$
- 6: $Z := Z \cap [t]$
- 7: //Τώρα $Z = \mathcal{S}(\{x_1, \dots, x_i\}, t)$
- 8: Επέστρεψε αν $t \in Z$.

Μία εναλλακτική λύση.

```
1: Αφελές FFT Άθροισμα Υποσυνόλου( $x_1, \dots, x_n, t$ )
2:    $Z := \emptyset$ 
3:   Για  $i = 1$  έως  $n$ 
4:      $Z := Z + \{x_i\}$ 
5:     //Μέσω FFT σε  $O(t \log t)$ 
6:      $Z := Z \cap [t]$ 
7:     //Τώρα  $Z = \mathcal{S}(\{x_1, \dots, x_i\}, t)$ 
8:   Επέστρεψε αν  $t \in Z$ .
```

👁 Στο i -οστό βήμα έχουμε υπολογίσει το $\mathcal{S}(\{x_1, \dots, x_i\}, t)$.

Μία εναλλακτική λύση.

```
1: Αφελές FFT Άθροισμα Υποσυνόλου( $x_1, \dots, x_n, t$ )
2:    $Z := \emptyset$ 
3:   Για  $i = 1$  έως  $n$ 
4:      $Z := Z + \{x_i\}$ 
5:     //Μέσω FFT σε  $O(t \log t)$ 
6:      $Z := Z \cap [t]$ 
7:     //Τώρα  $Z = \mathcal{S}(\{x_1, \dots, x_i\}, t)$ 
8:   Επέστρεψε αν  $t \in Z$ .
```

👁 Στο i -οστό βήμα έχουμε υπολογίσει το $\mathcal{S}(\{x_1, \dots, x_i\}, t)$.

👁 Κοινώς, την πληροφορία που κρατούσε πριν ο $A[i][\cdot]$.

Μία εναλλακτική λύση.

```
1: Αφελές FFT Άθροισμα Υποσυνόλου( $x_1, \dots, x_n, t$ )
2:    $Z := \emptyset$ 
3:   Για  $i = 1$  έως  $n$ 
4:      $Z := Z + \{x_i\}$ 
5:     //Μέσω FFT σε  $O(t \log t)$ 
6:      $Z := Z \cap [t]$ 
7:     //Τώρα  $Z = \mathcal{S}(\{x_1, \dots, x_i\}, t)$ 
8:   Επέστρεψε αν  $t \in Z$ .
```

👁 Στο i -οστό βήμα έχουμε υπολογίσει το $\mathcal{S}(\{x_1, \dots, x_i\}, t)$.

👁 Κοινώς, την πληροφορία που κρατούσε πριν ο $A[i][\cdot]$.

👉 Ο αλγόριθμος είναι ολόιδιος με τον αλγόριθμο του δυναμικού προγραμματισμού με την διαφορά ότι κάθε φορά κάνουμε FFT. Τρέχων χρόνος $O(n \cdot t \log t)$...

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Ας υποθέσουμε ότι υπολογίζω τα $\mathcal{S}(X_1, t)$ και $\mathcal{S}(X_2, t)$.

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Ας υποθέσουμε ότι υπολογίζω τα $\mathcal{S}(X_1, t)$ και $\mathcal{S}(X_2, t)$. Τότε μπορώ να υπολογίσω

$$\mathcal{S}(X, t) = (\mathcal{S}(X_1, t) + \mathcal{S}(X_2, t)) \cap [t].$$

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Ας υποθέσουμε ότι υπολογίζω τα $\mathcal{S}(X_1, t)$ και $\mathcal{S}(X_2, t)$. Τότε μπορώ να υπολογίσω

$$\mathcal{S}(X, t) = (\mathcal{S}(X_1, t) + \mathcal{S}(X_2, t)) \cap [t].$$

σε χρόνο $O(t \log t)$.

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Ας υποθέσουμε ότι υπολογίζω τα $\mathcal{S}(X_1, t)$ και $\mathcal{S}(X_2, t)$. Τότε μπορώ να υπολογίσω

$$\mathcal{S}(X, t) = (\mathcal{S}(X_1, t) + \mathcal{S}(X_2, t)) \cap [t].$$

σε χρόνο $O(t \log t)$.

👁 Συνολικός χρόνος εκτέλεσης: Φτιάχνω ένα δυαδικό δέντρο με n κόμβους και σε κάθε κόμβο πληρώνω $O(t \log t)$.

Υπάρχει κάτι καλύτερο που μπορώ να κάνω;

Ας κόψω τους αριθμούς στη μέση, σε σύνολα X_1, X_2 :

$$\underbrace{x_1, x_2, \dots, x_{n/2}}_{X_1}, \underbrace{x_{n/2+1}, \dots, x_n}_{X_2}.$$

Ας υποθέσουμε ότι υπολογίζω τα $\mathcal{S}(X_1, t)$ και $\mathcal{S}(X_2, t)$. Τότε μπορώ να υπολογίσω

$$\mathcal{S}(X, t) = (\mathcal{S}(X_1, t) + \mathcal{S}(X_2, t)) \cap [t].$$

σε χρόνο $O(t \log t)$.

👁 Συνολικός χρόνος εκτέλεσης: Φτιάχνω ένα δυαδικό δέντρο με n κόμβους και σε κάθε κόμβο πληρώνω $O(t \log t)$. Άρα $O(nt \cdot \log t)$ – πάλι τα ίδια!

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι *δεν μειώνεται* το μήκος των διανυσμάτων.
Πάντα κάνω FFT σε διανύσματα μήκους t .

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι *δεν μειώνεται* το μήκος των διανυσμάτων.
Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι δεν μειώνεται το μήκος των διανυσμάτων. Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

👉 Έστω $b \leq t$. Σπάω τους αρχικούς αριθμούς σε b ομάδες:

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι δεν μειώνεται το μήκος των διανυσμάτων. Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

👉 Εστω $b \leq t$. Σπάω τους αρχικούς αριθμούς σε b ομάδες:

- 1 G_0 έχει όσους είναι πολλαπλασιά του b

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι δεν μειώνεται το μήκος των διανυσμάτων. Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

👉 Έστω $b \leq t$. Σπάω τους αρχικούς αριθμούς σε b ομάδες:

- 1 G_0 έχει όσους είναι πολλαπλασιά του b
- 2 G_1 έχει όσους αφήνουν υπόλοιπο 1 με το b

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι δεν μειώνεται το μήκος των διανυσμάτων. Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

👉 Εστω $b \leq t$. Σπάω τους αρχικούς αριθμούς σε b ομάδες:

- 1 G_0 έχει όσους είναι πολλαπλασιά του b
- 2 G_1 έχει όσους αφήνουν υπόλοιπο 1 με το b
- 3 ...
- 4 G_{b-1} έχει όσους αφήνουν υπόλοιπο $b - 1$ με το b .

Ποιό ήταν το πρόβλημα;

Το βασικό πρόβλημα ήταν ότι δεν μειώνεται το μήκος των διανυσμάτων. Πάντα κάνω FFT σε διανύσματα μήκους t .

Μπορώ να κάνω ένα πιο δημιουργικό 'κόψιμο' αντί να κόβω στη μέση;

👉 Έστω $b \leq t$. Σπάω τους αρχικούς αριθμούς σε b ομάδες:

- 1 G_0 έχει όσους είναι πολλαπλασιά του b
- 2 G_1 έχει όσους αφήνουν υπόλοιπο 1 με το b
- 3 ...
- 4 G_{b-1} έχει όσους αφήνουν υπόλοιπο $b - 1$ με το b .

👁 Προσοχή, οι αριθμοί δεν ισοκατανέμονται στις ομάδες. Μπορεί μια ομάδα να έχει ακόμη και όλους τους αριθμούς.

Επόμενη ιδέα.

Έστω ότι υπολογίζαμε τα $\mathcal{S}(G_0, t), \mathcal{S}(G_1, t), \dots, \mathcal{S}(G_{b-1}, t)$.

Επόμενη ιδέα.

Έστω ότι υπολογίζαμε τα $\mathcal{S}(G_0, t), \mathcal{S}(G_1, t), \dots, \mathcal{S}(G_{b-1}, t)$.

Τότε μπορούμε να υπολογίσουμε το

$$\mathcal{S}(\{x_1, \dots, x_n\}, t) = (\mathcal{S}(G_0, t) + \mathcal{S}(G_1, t) + \dots + \mathcal{S}(G_{b-1}, t)) \cap [t].$$

Επόμενη ιδέα.

Έστω ότι υπολογίζαμε τα $\mathcal{S}(G_0, t), \mathcal{S}(G_1, t), \dots, \mathcal{S}(G_{b-1}, t)$.

Τότε μπορούμε να υπολογίσουμε το

$$\mathcal{S}(\{x_1, \dots, x_n\}, t) = (\mathcal{S}(G_0, t) + \mathcal{S}(G_1, t) + \dots + \mathcal{S}(G_{b-1}, t)) \cap [t].$$

σε χρόνο $O(bt \cdot \log t)$ με τον εξής ψευδοκώδικα.

```
1:    $Z = \emptyset$ 
2:   Για  $i = 1$  έως  $b$ 
3:        $Z := Z + \mathcal{S}(G_i, t)$ 
4:       Χρόνος  $O(\log t)$ 
5:        $Z := Z \cap [t]$ 
6:   Επέστρεψε το  $Z$ .
```

Στην ℓ -οστή ομάδα ισχύει για κάθε x_i είναι της μορφής $x_i = b \cdot y_i + \ell$.

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

Στην ℓ -οστή ομάδα ισχύει για κάθε x_i είναι της μορφής $x_i = b \cdot y_i + \ell$.

Αν στην G_9 ανήκουν οι αριθμοί x_7, x_8, x_{10}, x_{17} τότε μηπώς μπορώ να κοιτάξω τους αριθμούς:

$$\frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

Στην ℓ -οστή ομάδα ισχύει για κάθε x_i είναι της μορφής $x_i = b \cdot y_i + \ell$.

Αν στην G_9 ανήκουν οι αριθμοί x_7, x_8, x_{10}, x_{17} τότε μηπώς μπορώ να κοιτάξω τους αριθμούς:

$$\frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

και βρω όλους τους αριθμούς που φτιάχνονται πλέον ως αθροίσματα υποσυνόλων από αυτούς,

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

Στην ℓ -οστή ομάδα ισχύει για κάθε x_i είναι της μορφής $x_i = b \cdot y_i + \ell$.

Αν στην G_9 ανήκουν οι αριθμοί x_7, x_8, x_{10}, x_{17} τότε μηπώς μπορώ να κοιτάξω τους αριθμούς:

$$\frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

και βρω όλους τους αριθμούς που φτιάχνονται πλέον ως αθροίσματα υποσυνόλων από αυτούς, αλλά πλέον $\leq \frac{t-9}{b}$;

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

$$\star x_i = b \cdot y_i + \ell.$$

$$x_7, x_8, x_{10}, x_{17} \Rightarrow \frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

$$\star x_i = b \cdot y_i + \ell.$$

$$x_7, x_8, x_{10}, x_{17} \Rightarrow \frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

Όχι ακριβώς... Αν $y_7 + y_8 + y_{10}$ δίνουν τον ίδιο άθροισμα με το y_{17} , τότε όταν πάμε να μεταφέρουμε τον αριθμό πίσω, κάτι χάνουμε...

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

$$\star x_i = b \cdot y_i + \ell.$$

$$x_7, x_8, x_{10}, x_{17} \Rightarrow \frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

Όχι ακριβώς... Αν $y_7 + y_8 + y_{10}$ δίνουν τον ίδιο άθροισμα με το y_{17} , τότε όταν πάμε να μεταφέρουμε τον αριθμό πίσω, κάτι χάνουμε...

$$s = y_7 + y_8 + y_{10} \Rightarrow b \cdot s + 3 \cdot 9 = b \cdot s + 27$$

Υπολογισμός ενός $\mathcal{S}(G_\ell, t)$

$$\star x_i = b \cdot y_i + \ell.$$

$$x_7, x_8, x_{10}, x_{17} \Rightarrow \frac{x_7 - 9}{b}, \frac{x_8 - 9}{b}, \frac{x_{10} - 9}{b}, \frac{x_{17} - 9}{b},$$

Όχι ακριβώς... Αν $y_7 + y_8 + y_{10}$ δίνουν τον ίδιο άθροισμα με το y_{17} , τότε όταν πάμε να μεταφέρουμε τον αριθμό πίσω, κάτι χάνουμε...

$$s = y_7 + y_8 + y_{10} \Rightarrow b \cdot s + 3 \cdot 9 = b \cdot s + 27$$

$$s = y_{17} \Rightarrow b \cdot s + 1 \cdot 9 = b \cdot s + 9.$$

Τι ακριβώς θέλουμε;

Πρέπει να υπολογίσουμε όχι μόνο ποιοι αριθμοί φτιάχνονται από τα αντίστοιχα y_i της ομάδας G_ℓ , αλλά και από τι μεγέθους υποσύνολα μπορούμε να το πετύχουμε αυτό.

Τι ακριβώς θέλουμε;

Πρέπει να υπολογίσουμε όχι μόνο ποιοι αριθμοί φτιάχνονται από τα αντίστοιχα y_i της ομάδας G_ℓ , αλλά και από τι μεγέθους υποσύνολα μπορούμε να το πετύχουμε αυτό.

Έστω $y_i = \frac{x_i - \ell}{b}$ για $i \in G_\ell$ [κανονικοποίηση].

Τι ακριβώς θέλουμε;

Πρέπει να υπολογίσουμε όχι μόνο ποιοι αριθμοί φτιάχνονται από τα αντίστοιχα y_i της ομάδας G_ℓ , αλλά και από τι μεγέθους υποσύνολα μπορούμε να το πετύχουμε αυτό.

Έστω $y_i = \frac{x_i - \ell}{b}$ για $i \in G_\ell$ [κανονικοποίηση].

👉 Τότε πρέπει να βρω όλα τα ζεύγη (s, κ) με $s \leq \underbrace{(t - \ell)/b}_{\bar{t}}$ ώστε

ανάμεσα στα κανονικοποιημένα στοιχεία να υπάρχει υποσύνολο μεγέθους κ που να αθροίζει στο s .

Τι ακριβώς θέλουμε;

Πρέπει να υπολογίσουμε όχι μόνο ποιοι αριθμοί φτιάχνονται από τα αντίστοιχα y_i της ομάδας G_ℓ , αλλά και από τι μεγέθους υποσύνολα μπορούμε να το πετύχουμε αυτό.

Έστω $y_i = \frac{x_i - \ell}{b}$ για $i \in G_\ell$ [κανονικοποίηση].

👉 Τότε πρέπει να βρω όλα τα ζεύγη (s, κ) με $s \leq \underbrace{(t - \ell)/b}_{\bar{t}}$ ώστε

ανάμεσα στα κανονικοποιημένα στοιχεία να υπάρχει υποσύνολο μεγέθους κ που να αθροίζει στο s .

👁 Με αυτή την πληροφορία μπορούμε να βρούμε πλήρως το $\mathcal{S}(G_\ell, t)$.

Τι ακριβώς θέλουμε;

Πρέπει να υπολογίσουμε όχι μόνο ποιοι αριθμοί φτιάχνονται από τα αντίστοιχα y_i της ομάδας G_ℓ , αλλά και από τι μεγέθους υποσύνολα μπορούμε να το πετύχουμε αυτό.

Έστω $y_i = \frac{x_i - \ell}{b}$ για $i \in G_\ell$ [κανονικοποίηση].

☛ Τότε πρέπει να βρω όλα τα ζεύγη (s, κ) με $s \leq \underbrace{(t - \ell)/b}_{\bar{t}}$ ώστε

ανάμεσα στα κανονικοποιημένα στοιχεία να υπάρχει υποσύνολο μεγέθους κ που να αθροίζει στο s .

- 👁 Με αυτή την πληροφορία μπορούμε να βρούμε πλήρως το $\mathcal{S}(G_\ell, t)$.
- ★ Μήπως ζητάμε πολλά ή όχι; Θέλουμε μέχρι $\frac{t}{b} \cdot |G_\ell|$ ζεύγη.

Ας σπάσουμε τα κανονικοποιημένα στοιχεία στην μέση.

$$\underbrace{y_1, y_2, \dots, y_{m/2}}_{Y_1}, \underbrace{y_{m/2+1}, \dots, y_m}_{Y_2}.$$

Ας σπάσουμε τα κανονικοποιημένα στοιχεία στην μέση.

$$\underbrace{y_1, y_2, \dots, y_{m/2}}_{Y_1}, \underbrace{y_{m/2+1}, \dots, y_m}_{Y_2}.$$

Υπολογίζω αναδρομικά δύο σύνολα:

- 1 $\overline{S}(Y_1, \bar{t})$ που έχει όλα **ζεύγη** (s, κ) που φτιάχνονται από το Y_1 .
- 2 $\overline{S}(Y_2, \bar{t})$ που έχει όλα **ζεύγη** (s, κ) που φτιάχνονται από το Y_2 .

Ας σπάσουμε τα κανονικοποιημένα στοιχεία στην μέση.

$$\underbrace{y_1, y_2, \dots, y_{m/2}}_{Y_1}, \underbrace{y_{m/2+1}, \dots, y_m}_{Y_2}.$$

Υπολογίζω αναδρομικά δύο σύνολα:

- 1 $\overline{S}(Y_1, \bar{t})$ που έχει όλα **ζεύγη** (s, κ) που φτιάχνονται από το Y_1 .
- 2 $\overline{S}(Y_2, \bar{t})$ που έχει όλα **ζεύγη** (s, κ) που φτιάχνονται από το Y_2 .

Μετά πρέπει να συνδυάσω τις λύσεις:

$$\overline{S}(Y_1, \bar{t}) + \overline{S}(Y_2, \bar{t}).$$

Πόσο γρήγορα μπορώ να το κάνω;

Πάμε προσεκτικά.

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{\left(|Y_1| + |Y_2| \right)}_m$.

Πάμε προσεκτικά.

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{(|Y_1| + |Y_2|)}_m$.

👉 Ας υποθέσουμε ότι μπορούμε να το υπολογίσουμε στον ίδιο χρόνο.
Τότε η αναδρομή δημιουργεί ένα δυαδικό δέντρο

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{\left(|Y_1| + |Y_2|\right)}_m$.

✚ Ας υποθέσουμε ότι μπορούμε να το υπολογίσουμε στον ίδιο χρόνο. Τότε η αναδρομή δημιουργεί ένα δυαδικό δέντρο και σε κάθε επίπεδο πληρώνουμε $m \cdot \bar{t}$

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{\left(|Y_1| + |Y_2| \right)}_m$.

👉 Ας υποθέσουμε ότι μπορούμε να το υπολογίσουμε στον ίδιο χρόνο. Τότε η αναδρομή δημιουργεί ένα δυαδικό δέντρο και σε κάθε επίπεδο πληρώνουμε $m \cdot \bar{t}$ άρα συνολικά $m \cdot \bar{t} \cdot \log m$.

Πάμε προσεκτικά.

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{\left(|Y_1| + |Y_2| \right)}_m$.

✚ Ας υποθέσουμε ότι μπορούμε να το υπολογίσουμε στον ίδιο χρόνο. Τότε η αναδρομή δημιουργεί ένα δυαδικό δέντρο και σε κάθε επίπεδο πληρώνουμε $m \cdot \bar{t}$ άρα συνολικά $m \cdot \bar{t} \cdot \log m$.

Τι πρόβλημα στην πραγματικότητα έχουμε να λύσουμε για να συνδυάσουμε τα υπο-προβλήματα;

Το $\overline{\mathcal{S}}(Y_1, \bar{t}) + \overline{\mathcal{S}}(Y_2, \bar{t})$ μπορεί να έχει μέγεθος μέχρι $\bar{t} \cdot \underbrace{\left(|Y_1| + |Y_2| \right)}_m$.

✚ Ας υποθέσουμε ότι μπορούμε να το υπολογίσουμε στον ίδιο χρόνο. Τότε η αναδρομή δημιουργεί ένα δυαδικό δέντρο και σε κάθε επίπεδο πληρώνουμε $m \cdot \bar{t}$ άρα συνολικά $m \cdot \bar{t} \cdot \log m$.

Τι πρόβλημα στην πραγματικότητα έχουμε να λύσουμε για να συνδυάσουμε τα υπο-προβλήματα;

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το $A + B = \{a + b \mid a \in A, b \in B\}$.

Πάμε προσεκτικά.

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το
 $A + B = \{a + b \mid a \in A, b \in B\}$.

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το $A + B = \{a + b \mid a \in A, b \in B\}$.

👉 Ορίζουμε τα πολύωνυμα

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa,$$

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το $A + B = \{a + b \mid a \in A, b \in B\}$.

👉 Ορίζουμε τα πολύωνυμα

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa,$$

και βρίσκουμε το $p(x, y) \cdot q(x, y)$.

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το $A + B = \{a + b \mid a \in A, b \in B\}$.

👉 Ορίζουμε τα πολύωνυμα

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa,$$

και βρίσκουμε το $p(x, y) \cdot q(x, y)$. Από εκεί μπορούμε να διαβάσουμε το $A + B$.

Δίνονται δύο σύνολα $A, B \subseteq [u] \times [m]$, βρες το $A + B = \{a + b \mid a \in A, b \in B\}$.

👉 Ορίζουμε τα πολώνυμα

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa,$$

και βρίσκουμε το $p(x, y) \cdot q(x, y)$. Από εκεί μπορούμε να διαβάσουμε το $A + B$.

Αλλά πώς θα υπολογίσουμε γινόμενο πολυωνύμων σε δύο μεταβλητές;

Πολλαπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^{\kappa}, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^{\kappa}.$$

Πολυπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa.$$

Ορίζουμε

$$\tilde{p}(x) = \sum_{(a, \kappa) \in A} x^{\kappa \cdot (u+1) + a},$$

Πολλαπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa.$$

Ορίζουμε

$$\tilde{p}(x) = \sum_{(a, \kappa) \in A} x^{\kappa \cdot (u+1) + a}, \quad \tilde{p}(x) = \sum_{(b, \kappa) \in B} x^{\kappa \cdot (u+1) + b}.$$

Πολυπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa.$$

Ορίζουμε

$$\tilde{p}(x) = \sum_{(a, \kappa) \in A} x^{\kappa \cdot (u+1) + a}, \quad \tilde{q}(x) = \sum_{(b, \kappa) \in B} x^{\kappa \cdot (u+1) + b}.$$

👁 Τα πολυώνυμα είναι βαθμού $O(m \cdot u)$.

Πολυπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa.$$

Ορίζουμε

$$\tilde{p}(x) = \sum_{(a, \kappa) \in A} x^{\kappa \cdot (u+1) + a}, \quad \tilde{q}(x) = \sum_{(b, \kappa) \in B} x^{\kappa \cdot (u+1) + b}.$$

👁 Τα πολυώνυμα είναι βαθμού $O(m \cdot u)$.

👉 Υπολογίζουμε το $\tilde{p}(x) \cdot \tilde{q}(x)$ με FFT σε χρόνο $O(m \cdot u \cdot \log(mu))$.

Πολυπλασιάζοντας πολυώνυμα δύο μεταβλητών.

$$p(x, y) = \sum_{(a, \kappa) \in A} x^a y^\kappa, \quad q(x, y) = \sum_{(b, \kappa) \in B} x^b y^\kappa.$$

Ορίζουμε

$$\tilde{p}(x) = \sum_{(a, \kappa) \in A} x^{\kappa \cdot (u+1) + a}, \quad \tilde{q}(x) = \sum_{(b, \kappa) \in B} x^{\kappa \cdot (u+1) + b}.$$

👁 Τα πολυώνυμα είναι βαθμού $O(m \cdot u)$.

👉 Υπολογίζουμε το $\tilde{p}(x) \cdot \tilde{q}(x)$ με FFT σε χρόνο $O(m \cdot u \cdot \log(mu))$.

Διαβάσουμε το $A + B$ από κάθε μονώνυμο του γινομένου.

Ας τα μαζέψουμε.

★ Για κάθε ομάδα G_ℓ μπορούμε να υπολογίσουμε το $\mathcal{S}(G_\ell, t)$ σε χρόνο $O(|G_\ell| \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Ας τα μαζέψουμε.

★ Για κάθε ομάδα G_ℓ μπορούμε να υπολογίσουμε το $\mathcal{S}(G_\ell, t)$ σε χρόνο $O(|G_\ell| \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Άρα για όλες τις ομάδες $\sum_{\ell=0}^{b-1} O(|G_\ell| \cdot \frac{t}{b} \cdot \log t) = O(n \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Ας τα μαζέψουμε.

★ Για κάθε ομάδα G_ℓ μπορούμε να υπολογίσουμε το $\mathcal{S}(G_\ell, t)$ σε χρόνο $O(|G_\ell| \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Άρα για όλες τις ομάδες $\sum_{\ell=0}^{b-1} O(|G_\ell| \cdot \frac{t}{b} \cdot \log t) = O(n \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Συνολικός χρόνος

$$O\left(n \cdot \frac{t}{b} \cdot \log t + b \cdot t \log t\right).$$

Ας τα μαζέψουμε.

★ Για κάθε ομάδα G_ℓ μπορούμε να υπολογίσουμε το $\mathcal{S}(G_\ell, t)$ σε χρόνο $O(|G_\ell| \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Άρα για όλες τις ομάδες $\sum_{\ell=0}^{b-1} O(|G_\ell| \cdot \frac{t}{b} \cdot \log t) = O(n \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Συνολικός χρόνος

$$O\left(n \cdot \frac{t}{b} \cdot \log t + b \cdot t \log t\right).$$

Διαλέγοντας $b := \sqrt{n/\log n}$ παίρνουμε χρόνο $O(\sqrt{nt} \cdot \log t \cdot \sqrt{\log n})$.

Ας τα μαζέψουμε.

★ Για κάθε ομάδα G_ℓ μπορούμε να υπολογίσουμε το $\mathcal{S}(G_\ell, t)$ σε χρόνο $O(|G_\ell| \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Άρα για όλες τις ομάδες $\sum_{\ell=0}^{b-1} O(|G_\ell| \cdot \frac{t}{b} \cdot \log t) = O(n \cdot \frac{t}{b} \cdot \log t \cdot \log n)$.

Συνολικός χρόνος

$$O\left(n \cdot \frac{t}{b} \cdot \log t + b \cdot t \log t\right).$$

Διαλέγοντας $b := \sqrt{n/\log n}$ παίρνουμε χρόνο $O(\sqrt{nt} \cdot \log t \cdot \sqrt{\log n})$.

Θεώρημα

Το πρόβλημα Αθροίσματος Υποσυνόλου λύνεται σε χρόνο $O(\sqrt{nt} \cdot \log t \cdot \sqrt{\log n})$.