

Προηγμένα Θέματα Αλγορίθμων

Γρήγορος Μετασχηματισμός Fourier και συνελίξεις I

Βασίλειος Νάκος

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Ένα πολυώνυμο $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ με πραγματικούς συντελεστές αναπαρίσταται στον υπολογιστή ως μία λίστα αριθμών $[a_0, a_1, \dots, a_{n-1}]$.

Ένα πολυώνυμο $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ με πραγματικούς συντελεστές αναπαρίσταται στον υπολογιστή ως μία λίστα αριθμών $[a_0, a_1, \dots, a_{n-1}]$.

word Ram. Στο μοντέλο word RAM υποθέτουμε μέγεθος λέξης του υπολογιστή $w = \Omega(\log n)$,

Ένα πολυώνυμο $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ με πραγματικούς συντελεστές αναπαρίσταται στον υπολογιστή ως μία λίστα αριθμών $[a_0, a_1, \dots, a_{n-1}]$.

word Ram. Στο μοντέλο word RAM υποθέτουμε μέγεθος λέξης του υπολογιστή $w = \Omega(\log n)$, και ότι οι πράξεις μεταξύ δύο αριθμών στην είσοδο γίνονται σε σταθερό χρόνο.

Πολυώνυμα και word RAM.

Ένα πολυώνυμο $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ με πραγματικούς συντελεστές αναπαρίσταται στον υπολογιστή ως μία λίστα αριθμών $[a_0, a_1, \dots, a_{n-1}]$.

word Ram. Στο μοντέλο word RAM υποθέτουμε μέγεθος λέξης του υπολογιστή $w = \Omega(\log n)$, και ότι οι πράξεις μεταξύ δύο αριθμών στην είσοδο γίνονται σε σταθερό χρόνο.

- Μπορούμε να αποθηκεύσουμε έτσι το $p(x)$ με n λέξεις σε αυτό το μοντέλο.

Πολυώνυμα και word RAM.

Ένα πολυώνυμο $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ με πραγματικούς συντελεστές αναπαρίσταται στον υπολογιστή ως μία λίστα αριθμών $[a_0, a_1, \dots, a_{n-1}]$.

word Ram. Στο μοντέλο word RAM υποθέτουμε μέγεθος λέξης του υπολογιστή $w = \Omega(\log n)$, και ότι οι πράξεις μεταξύ δύο αριθμών στην είσοδο γίνονται σε σταθερό χρόνο.

- Μπορούμε να αποθηκεύσουμε έτσι το $p(x)$ με n λέξεις σε αυτό το μοντέλο.
- Μπορούμε να προσθέσουμε δύο πολυώνυμα σε γραμμικό χρόνο.

Πράξεις με πολυώνυμα.

Δοθέντων πολυωνύμου p και q βαθμού n να υπολογιστεί το $p(x) \cdot q(x)$.

Η απάντηση είναι μια λίστα μήκους $2n - 1$ (το πολύ).

Πράξεις με πολυώνυμα.

Δοθέντων πολυωνύμου p και q βαθμού n να υπολογιστεί το $p(x) \cdot q(x)$.

Η απάντηση είναι μια λίστα μήκους $2n - 1$ (το πολύ).

Δοθέντων πολυωνύμου p και αριθμών $x_1, x_2, \dots, x_n$ να υπολογιστούν τα $p(x_1), p(x_2), \dots, p(x_n)$.

Πόσο χρόνο χρειάζομαι για να βρω το $p(x)$;

Πράξεις με πολυώνυμα.

Δοθέντων πολυωνύμου p και q βαθμού n να υπολογιστεί το $p(x) \cdot q(x)$.

Η απάντηση είναι μια λίστα μήκους $2n - 1$ (το πολύ).

Δοθέντων πολυωνύμου p και αριθμών $x_1, x_2, \dots, x_n$ να υπολογιστούν τα $p(x_1), p(x_2), \dots, p(x_n)$.

Πόσο χρόνο χρειάζομαι για να βρω το $p(x)$; Απάντηση: Μπορεί και μόνο να το γράψω κάτω να χρειάζομαι $\approx \frac{n^2}{w}$ λέξεις, διότι τα νούμερα γίνονται πολύ μεγάλα και θέλω πολλές λέξεις για το καθένα.

Πράξεις με πολυώνυμα.

Δοθέντων πολυωνύμου p και q βαθμού n να υπολογιστεί το $p(x) \cdot q(x)$.

Η απάντηση είναι μια λίστα μήκους $2n - 1$ (το πολύ).

Δοθέντων πολυωνύμου p και αριθμών $x_1, x_2, \dots, x_n$ να υπολογιστούν τα $p(x_1), p(x_2), \dots, p(x_n)$.

Πόσο χρόνο χρειάζομαι για να βρω το $p(x)$; Απάντηση: Μπορεί και μόνο να το γράψω κάτω να χρειάζομαι $\approx \frac{n^2}{w}$ λέξεις, διότι τα νούμερα γίνονται πολύ μεγάλα και θέλω πολλές λέξεις για το καθένα.

Για παράδειγμα $p(3)$ για $p(x) = 1 + x + x^2 + \dots + x^{n-1}$.

Ένας απλός αλγόριθμος για τον πολλαπλασιασμό.

Αλγόριθμος Λυκείου για πολ/σμό πολυωνύμων.

- 1: Έστω t πίνακας με $2n - 1$ θέσεις, αρχικοποιημένος σε όλα 0.
- 2: Για κάθε $i \in [n]$ //διατρέχουμε το p
- 3: Για κάθε $j \in [n]$ //διατρέχουμε το q
- 4: $t[i + j] = t[i + j] + p[i] \cdot q[j]$
- 5: Επέστρεψε το t

👉 Χρόνος εκτέλεσης $O(n^2)$. Μπορούμε καλύτερα;

Αλγόριθμος Λυκείου για πολ/σμό πολυωνύμων.

- 1: Έστω t πίνακας με $2n - 1$ θέσεις, αρχικοποιημένος σε όλα 0.
- 2: Για κάθε $i \in [n]$ //διατρέχουμε το p
- 3: Για κάθε $j \in [n]$ //διατρέχουμε το q
- 4: $t[i + j] = t[i + j] + p[i] \cdot p[j]$
- 5: Επέστρεψε το t

Μας θυμίζει κάτι η **κύρια πράξη** του ψευδοκώδικα;

Αλγόριθμος Λυκείου για πολ/σμό πολυωνύμων.

- 1: Έστω t πίνακας με $2n - 1$ θέσεις, αρχικοποιημένος σε όλα 0.
- 2: Για κάθε $i \in [n]$ //διατρέχουμε το p
- 3: Για κάθε $j \in [n]$ //διατρέχουμε το q
- 4: $t[i + j] = t[i + j] + p[i] \cdot q[j]$
- 5: Επέστρεψε το t

Μας θυμίζει κάτι η **κύρια πράξη** του ψευδοκώδικα;

Αν ορίσω τα διανύσματα p, q, t μήκους $n, n, 2n - 1$ αντίστοιχα τότε

Αλγόριθμος Λυκείου για πολ/σμό πολυωνύμων.

- 1: Έστω t πίνακας με $2n - 1$ θέσεις, αρχικοποιημένος σε όλα 0.
- 2: Για κάθε $i \in [n]$ //διατρέχουμε το p
- 3: Για κάθε $j \in [n]$ //διατρέχουμε το q
- 4: $t[i + j] = t[i + j] + p[i] \cdot q[j]$
- 5: Επέστρεψε το t

Μας θυμίζει κάτι η **κύρια πράξη** του ψευδοκώδικα;

Αν ορίσω τα διανύσματα p, q, t μήκους $n, n, 2n - 1$ αντίστοιχα τότε

$$t[k] = \sum_{i+j=k} p[i] \cdot q[j]$$

Αλγόριθμος Λυκείου για πολ/σμό πολυωνύμων.

- 1: Έστω t πίνακας με $2n - 1$ θέσεις, αρχικοποιημένος σε όλα 0.
- 2: Για κάθε $i \in [n]$ //διατρέχουμε το p
- 3: Για κάθε $j \in [n]$ //διατρέχουμε το q
- 4: $t[i + j] = t[i + j] + p[i] \cdot q[j]$
- 5: Επέστρεψε το t

Μας θυμίζει κάτι η **κύρια πράξη** του ψευδοκώδικα;

Αν ορίσω τα διανύσματα p, q, t μήκους $n, n, 2n - 1$ αντίστοιχα τότε

$$t[k] = \sum_{i+j=k} p[i] \cdot q[j]$$

👉 το t είναι η συνέλιξη του p με το q και γράφουμε $t = p \star q$.

Διακριτός Μετασχηματισμός Fourier.

Ο Διακριτός Μετασχηματισμός Fourier είναι ένας μετασχηματισμός ο οποίος παίρνει ένα διάνυσμα $x \in \mathbb{C}^n$ και το μετατρέπει σε $\hat{x} \in \mathbb{C}^n$ με τον εξής τρόπο ($\omega = e^{-2\pi\sqrt{-1}/n}$):

Διακριτός Μετασχηματισμός Fourier.

Ο Διακριτός Μετασχηματισμός Fourier είναι ένας μετασχηματισμός ο οποίος παίρνει ένα διάνυσμα $x \in \mathbb{C}^n$ και το μετατρέπει σε $\hat{x} \in \mathbb{C}^n$ με τον εξής τρόπο ($\omega = e^{-2\pi\sqrt{-1}/n}$):

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{\textcolor{red}{j}=0}^{n-1} x_j \cdot \omega^{i \cdot \textcolor{red}{j}}.$$

Διακριτός Μετασχηματισμός Fourier.

Ο Διακριτός Μετασχηματισμός Fourier είναι ένας μετασχηματισμός ο οποίος παίρνει ένα διάνυσμα $x \in \mathbb{C}^n$ και το μετατρέπει σε $\hat{x} \in \mathbb{C}^n$ με τον εξής τρόπο ($\omega = e^{-2\pi\sqrt{-1}/n}$):

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{\textcolor{red}{j}=0}^{n-1} x_j \cdot \omega^{i \cdot \textcolor{red}{j}}.$$

Ο αντίστροφος Διακριτός Μετασχηματισμός Fourier παίρνει $\hat{x}$ και επιστρέφει $x \in \mathbb{C}^n$ ως

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{\textcolor{red}{j}=0}^{n-1} x_j \cdot \omega^{-i \cdot \textcolor{red}{j}}.$$

Διακριτός Μετασχηματισμός Fourier.

Ο Διακριτός Μετασχηματισμός Fourier είναι ένας μετασχηματισμός ο οποίος παίρνει ένα διάνυσμα $x \in \mathbb{C}^n$ και το μετατρέπει σε $\hat{x} \in \mathbb{C}^n$ με τον εξής τρόπο ($\omega = e^{-2\pi\sqrt{-1}/n}$):

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{\textcolor{red}{j}=0}^{n-1} x_j \cdot \omega^{i \cdot \textcolor{red}{j}}.$$

Ο αντίστροφος Διακριτός Μετασχηματισμός Fourier παίρνει $\hat{x}$ και επιστρέφει $x \in \mathbb{C}^n$ ως

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{\textcolor{red}{j}=0}^{n-1} x_j \cdot \omega^{-i \cdot \textcolor{red}{j}}.$$

Ιδιότητες Μετασχηματισμού Fourier.

Έστω $F \in \mathbb{C}^n$ με $F_{ij} = \frac{1}{\sqrt{N}} \omega^{ij}$.

- ① (ορθοκανονικός μετασχηματισμός) $FF^T = I$.
- ② (αντίστροφος Fourier) $F^{-1} = F^T$.

Ιδιότητες Μετασχηματισμού Fourier.

Έστω $F \in \mathbb{C}^n$ με $F_{ij} = \frac{1}{\sqrt{N}} \omega^{ij}$.

- ❶ (ορθοκανονικός μετασχηματισμός) $FF^T = I$.
- ❷ (αντίστροφος Fourier) $F^{-1} = F^T$.
- ❸ Κάθε γραμμή και κάθε στήλη του πίνακα πλην των πρώτων (με αριθμηση 0) αθροίζουν στο 0.

👉 $\hat{x} = Fx$ και $x = F^T \hat{x}$.

Ιδιότητες Μετασχηματισμού Fourier.

Έστω $F \in \mathbb{C}^n$ με $F_{ij} = \frac{1}{\sqrt{N}} \omega^{ij}$.

- ❶ (ορθοκανονικός μετασχηματισμός) $FF^T = I$.
- ❷ (αντίστροφος Fourier) $F^{-1} = F^T$.
- ❸ Κάθε γραμμή και κάθε στήλη του πίνακα πλην των πρώτων (με αριθμηση 0) αθροίζουν στο 0.

👉 $\hat{x} = Fx$ και $x = F^T \hat{x}$.

Αλλά τι σχέση έχει με πολλαπλασιασμό πολυωνύμων και συνελίξεις;

Μετασχηματισμός Fourier ως αποτίμηση πολυωνύμου.

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot \omega^{i \cdot j}.$$

Μετασχηματισμός Fourier ως αποτίμηση πολυωνύμου.

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot \omega^{i \cdot j}.$$

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot (\omega^i)^j.$$

Μετασχηματισμός Fourier ως αποτίμηση πολυωνύμου.

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot \omega^{i \cdot j}.$$

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot (\omega^i)^j.$$

👁 Αν ορίσουμε το πολυώνυμο

$$p(z) = x_0 + x_1 z + x_2 z^2 + \dots + x_{n-1} z^{n-1}$$

Μετασχηματισμός Fourier ως αποτίμηση πολυωνύμου.

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot \omega^{i \cdot j}.$$

$$\hat{x}_i = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \cdot (\omega^i)^j.$$

👁 Αν ορίσουμε το πολυώνυμο

$$p(z) = x_0 + x_1 z + x_2 z^2 + \dots + x_{n-1} z^{n-1}$$

τότε ο Μετασχηματισμός Fourier είναι ακριβώς το ίδιο με το να αποτιμήσουμε το πολυώνυμο p στα σημεία $\omega^0, \omega^1, \dots, \omega^{n-1}$.

Και τι κάνει ο αντίστροφος;

Ο αντίστροφος Fourier παίρνει τιμές $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$ και

Και τι κάνει ο αντίστροφος;

Ο αντίστροφος Fourier παίρνει τιμές $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$ και υπολογίζει τους άγνωστους συντελεστές του πολυωνύμου p !

Και τι κάνει ο αντίστροφος;

Ο αντίστροφος Fourier παίρνει τιμές $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$ και υπολογίζει τους άγνωστους συντελεστές του πολυωνύμου p !

Άρα,

- **Αποτίμηση** του p σε n ρίζες της μονάδας $\Leftrightarrow$ πολλαπλασιασμός διανύσματος **συντελεστών** με F .

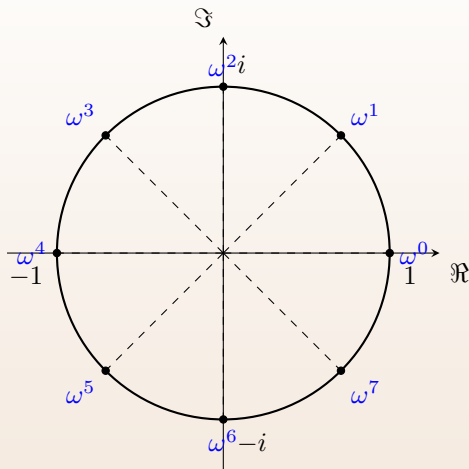
Και τι κάνει ο αντίστροφος;

Ο αντίστροφος Fourier παίρνει τιμές $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$ και υπολογίζει τους άγνωστους συντελεστές του πολυωνύμου p !

Άρα,

- **Αποτίμηση** του p σε n ρίζες της μονάδας $\Leftrightarrow$ πολλαπλασιασμός διανύσματος **συντελεστών** με F .
- Εξαγωγή συντελεστών του p από **αποτιμήσεις** σε n ρίζες της μονάδας $\Leftrightarrow$ πολλαπλασιασμός **διανύσματος αποτιμήσεων** με F^T .

Τι είδους περίεργα σημεία είναι αυτά;



$$\omega = e^{\sqrt{-1}\pi/4}, \quad \text{ρίζες του } \omega^8 = 1$$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{n-1}) \cdot q(\omega^{n-1})$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{n-1}) \cdot q(\omega^{n-1})$.
- ★ Από τα n σημεία βρίσκουμε τους συντελεστές $p \cdot q$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{n-1}) \cdot q(\omega^{n-1})$.
- ★ Από τα n σημεία βρίσκουμε τους συντελεστές $p \cdot q$.

Πού είναι το λάθος;

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{n-1}) \cdot q(\omega^{n-1})$.
- ★ Από τα n σημεία βρίσκουμε τους συντελεστές $p \cdot q$.

Πού είναι το λάθος;

👉 Η τελευταία γραμμή επιστρέφει ένα πολώνυμο βαθμού $\leq n$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Στρατηγική. Έστω ότι θέλουμε να υπολογίσουμε το γινόμενο $p \cdot q$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{n-1}) \cdot q(\omega^{n-1})$.
- ★ Από τα n σημεία βρίσκουμε τους συντελεστές $p \cdot q$.

Πού είναι το λάθος;

👉 Η τελευταία γραμμή επιστρέφει ένα πολυώνυμο βαθμού $\leq n$ αλλά το $p \cdot q$ μπορεί να είναι μέχρι βαθμού $2n - 1$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{2n-1})$

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{2n-1}) \cdot q(\omega^{2n-1})$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{2n-1}) \cdot q(\omega^{2n-1})$.
- ★ Από τις $2n - 1$ αποτιμήσεις βρίσκουμε το $p \cdot q$.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{2n-1}) \cdot q(\omega^{2n-1})$.
- ★ Από τις $2n - 1$ αποτιμήσεις βρίσκουμε το $p \cdot q$.

👁 Στην πραγματικότητα, αρκεί να πάρουμε $N \geq 2n - 1$ και μία N -οστή ρίζα της μονάδας ω και να τρέξουμε τον αποπάνω αλγόριθμο.

Μετασχηματισμός Fourier και πολλαπλασιασμός πολυωνύμων.

Έστω ω μία $2n - 1$ -οστή ρίζα της μοναδας, δηλαδή $\omega^{2n-1} = 1$.

- ★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^{2n-1})$
- ★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^{2n-1}) \cdot q(\omega^{2n-1})$.
- ★ Από τις $2n - 1$ αποτιμήσεις βρίσκουμε το $p \cdot q$.

👁 Στην πραγματικότητα, αρκεί να πάρουμε $N \geq 2n - 1$ και μία N -οστή ρίζα της μονάδας ω και να τρέξουμε τον αποπάνω αλγόριθμο. Θα πάρουμε N δύναμη του 2 για διευκόλυνση.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

Αντιστοίχιση με συνελίξεις.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^N)$.

👉 Μετασχηματισμός Fourier του u

Αντιστοίχιση με συνελίξεις.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^N)$.

👉 Μετασχηματισμός Fourier του u

★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^N)$.

👉 Μετασχηματισμός Fourier του v

Αντιστοίχιση με συνελίξεις.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^N)$.

👉 Μετασχηματισμός Fourier του u

★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^N)$.

👉 Μετασχηματισμός Fourier του v

★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^N) \cdot q(\omega^N)$.

👉 Πολλαπλασιασμός $\hat{u}$ με $\hat{v}$

Αντιστοίχιση με συνελίξεις.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^N)$.

👉 Μετασχηματισμός Fourier του u

★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^N)$.

👉 Μετασχηματισμός Fourier του v

★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^N) \cdot q(\omega^N)$.

👉 Πολλαπλασιασμός $\hat{u}$ με $\hat{v}$

★ Από τις $2n - 1$ αποτιμήσεις βρίσκουμε το $p \cdot q$.

👉 Αντίστροφος Μετασχηματισμός Fourier του $u \odot v$

Αντιστοίχιση με συνελίξεις.

Έστω ότι είχα τα διανύσματα $u, v \in \mathbb{R}^N$ (έχω γεμίσει τις τελευταίες $N - n$ θέσεις με μηδενικά.)

★ Υπολογίζουμε τα $p(\omega^0), p(\omega^1), \dots, p(\omega^N)$.

👉 Μετασχηματισμός Fourier του u

★ Υπολογίζουμε τα $q(\omega^0), q(\omega^1), \dots, q(\omega^N)$.

👉 Μετασχηματισμός Fourier του v

★ Υπολογίζουμε τα $p(\omega^0) \cdot q(\omega^0), p(\omega^1) \cdot q(\omega^1), \dots, p(\omega^N) \cdot q(\omega^N)$.

👉 Πολλαπλασιασμός $\hat{u}$ με $\hat{v}$

★ Από τις $2n - 1$ αποτιμήσεις βρίσκουμε το $p \cdot q$.

👉 Αντίστροφος Μετασχηματισμός Fourier του $u \odot v$

👁 Ουσιαστικά χρησιμοποιώ την ιδιότητα $u \star v \leftrightarrow \hat{u} \odot \hat{v}$.

Ιδέα γρήγορου Μετασχηματισμού Fourier.

Έστω ω_N μία N -οστή ρίζα της μονάδας με N δύναμη του δύο¹.

¹Για λόγους αναγνωσιμότητας θα γράφω ως επί το πλείστον ω αντί για ω_N εκτός από ένα σημείο.

Ιδέα γρήγορου Μετασχηματισμού Fourier.

Έστω ω_N μία N -οστή ρίζα της μονάδας με N δύναμη του δύο¹.

$$p(\omega^j) = \sum_{i=0}^{N-1} a_i \omega_N^{i \cdot j} =$$

¹Για λόγους αναγνωσιμότητας θα γράφω ως επί το πλείστον ω αντί για ω_N εκτός από ένα σημείο.

Ιδέα γρήγορου Μετασχηματισμού Fourier.

Έστω ω_N μία N -οστή ρίζα της μονάδας με N δύναμη του δύο¹.

$$p(\omega^j) = \sum_{i=0}^{N-1} a_i \omega_N^{i \cdot j} = \sum_{k: 0 \leq \textcolor{red}{2}k < N} a_{\textcolor{red}{2}k} \omega^{\textcolor{red}{2}k \cdot j} + \sum_{k: 0 \leq \textcolor{blue}{2}k+1 < N} a_{\textcolor{blue}{2}k+1} \omega^{(\textcolor{blue}{2}k+1) \cdot j}$$

¹Για λόγους αναγνωσιμότητας θα γράφω ως επί το πλείστον ω αντί για ω_N εκτός από ένα σημείο.

Ιδέα γρήγορου Μετασχηματισμού Fourier.

Έστω ω_N μία N -οστή ρίζα της μονάδας με N δύναμη του δύο¹.

$$p(\omega^j) = \sum_{i=0}^{N-1} a_i \omega_N^{i \cdot j} = \sum_{k: 0 \leq \textcolor{red}{2k} < N} a_{\textcolor{red}{2k}} \omega_N^{\textcolor{red}{2k} \cdot j} + \sum_{k: 0 \leq \textcolor{blue}{2k+1} < N} a_{\textcolor{blue}{2k+1}} \omega_N^{(\textcolor{blue}{2k+1}) \cdot j}$$

$$p(\omega^j) = \underbrace{\sum_{k: 0 \leq \textcolor{red}{k} < N/2} a_{\textcolor{red}{2k}} \omega_N^{\textcolor{red}{k} \cdot (2j)}}_{p_{\text{even}}(\omega^{2j})} + \omega_N^j \underbrace{\sum_{k: 0 \leq \textcolor{blue}{k} < N/2} a_{\textcolor{blue}{2k+1}} \omega_N^{\textcolor{blue}{k} \cdot (2j)}}_{p_{\text{odd}}(\omega^{2j})}$$

¹Για λόγους αναγνωσιμότητας θα γράφω ως επί το πλείστον ω αντί για ω_N εκτός από ένα σημείο.

Ιδέα γρήγορου Μετασχηματισμού Fourier.

Έστω ω_N μία N -οστή ρίζα της μονάδας με N δύναμη του δύο¹.

$$p(\omega^j) = \sum_{i=0}^{N-1} a_i \omega_N^{i \cdot j} = \sum_{k: 0 \leq \textcolor{red}{2}k < N} a_{\textcolor{red}{2}k} \omega_N^{\textcolor{red}{2}k \cdot j} + \sum_{k: 0 \leq \textcolor{blue}{2}k+1 < N} a_{\textcolor{blue}{2}k+1} \omega_N^{(\textcolor{blue}{2}k+1) \cdot j}$$

$$p(\omega^j) = \underbrace{\sum_{k: 0 \leq \textcolor{red}{k} < N/2} a_{\textcolor{red}{2}k} \omega_N^{\textcolor{red}{k} \cdot (2j)}}_{p_{\text{even}}(\omega^{2j})} + \omega_N^j \underbrace{\sum_{k: 0 \leq \textcolor{blue}{k} < N/2} a_{\textcolor{blue}{2}k+1} \omega_N^{\textcolor{blue}{k} \cdot (2j)}}_{p_{\text{odd}}(\omega^{2j})}$$

¹Για λόγους αναγνωσιμότητας θα γράφω ως επί το πλείστον ω αντί για ω_N εκτός από ένα σημείο.

Τι μας ζητείται να υπολογίσουμε.

☞ Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:

Τι μας ζητείται να υπολογίσουμε.

👉 Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_0, a_2, a_4, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

Τι μας ζητείται να υπολογίσουμε.

☞ Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_0, a_2, a_4, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

☞ Το να υπολογίσω τα $p_{\text{odd}}(\omega^j)$ μου λέει:

Τι μας ζητείται να υπολογίσουμε.

👉 Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_0, a_2, a_4, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

👉 Το να υπολογίσω τα $p_{\text{odd}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_1, a_3, a_5, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

Τι μας ζητείται να υπολογίσουμε.

👉 Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_0, a_2, a_4, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

👉 Το να υπολογίσω τα $p_{\text{odd}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_1, a_3, a_5, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

👁 Έχω μειώσει τον βαθμό του πολυωνύμου αλλά όχι το πλήθος των σημείων αποτίμησης.

Τι μας ζητείται να υπολογίσουμε.

👉 Το να υπολογίσω τα $p_{\text{even}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_0, a_2, a_4, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

👉 Το να υπολογίσω τα $p_{\text{odd}}(\omega^j)$ μου λέει:
αποτίμησε το πολυώνυμο βαθμού $< N/2$ με συντελεστές $[a_1, a_3, a_5, \dots]$
σε N ισαπέχοντα σημεία στον μιγαδικό κύκλο.

👁 Έχω μειώσει τον βαθμό του πολυωνύμου αλλά όχι το πλήθος των σημείων αποτίμησης. Δεν μπορώ να κάνω αναδρομή ακόμη.

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} =$

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

Πριν αποτιμούσα στα σημεία $\omega^0, \omega^1, \dots$, και τώρα

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

Πριν αποτιμούσα στα σημεία $\omega^0, \omega^1, \dots$, και τώρα

θέλω να αποτιμήσω στα σημεία $(\omega^0)^2, (\omega^1)^2, \dots, (\omega^N)^2$.

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

Πριν αποτιμούσα στα σημεία $\omega^0, \omega^1, \dots$, και τώρα

θέλω να αποτιμήσω στα σημεία $(\omega^0)^2, (\omega^1)^2, \dots, (\omega^N)^2$.

Μήπως δεν είναι όλα τόσο διαφορετικά εν τέλει;

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

Πριν αποτιμούσα στα σημεία $\omega^0, \omega^1, \dots$, και τώρα

θέλω να αποτιμήσω στα σημεία $(\omega^0)^2, (\omega^1)^2, \dots, (\omega^N)^2$.

Μήπως δεν είναι όλα τόσο διαφορετικά εν τέλει;

👁 $\omega^{2(k+N/2)} =$

Ή μήπως όχι;

Έχω να υπολογίσω το

$$p_{\text{even}}(\omega^j) = \sum_{k: 0 \leq k < N/2} a_{2k} \omega^{2k \cdot j}$$

για $\omega^0, \omega^1, \dots, \omega^{N-1}$.

👁 Για να παρατηρήσω: $\omega^{2k} = (\omega^k)^2$.

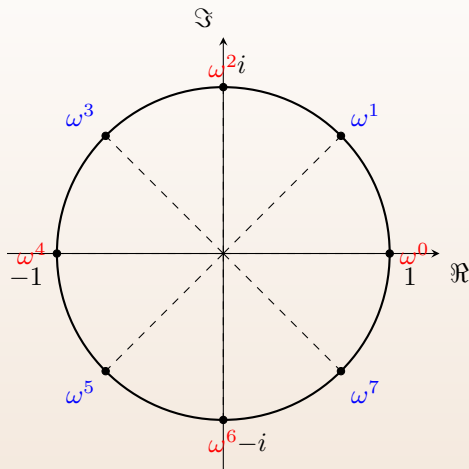
Πριν αποτιμούσα στα σημεία $\omega^0, \omega^1, \dots$, και τώρα

θέλω να αποτιμήσω στα σημεία $(\omega^0)^2, (\omega^1)^2, \dots, (\omega^N)^2$.

Μήπως δεν είναι όλα τόσο διαφορετικά εν τέλει;

👁 $\omega^{2(k+N/2)} = \omega^{2k} \cdot \omega^N = \omega^{2k}$.

Τι είδους περίεργα σημεία είναι αυτά;



👁 Οι αριθμοί $(\omega_N^0)^2, (\omega_N^1)^2, \dots, (\omega_N^N)^2$ είναι μόνο $N/2$ διακριτοί αριθμοί.

Επιστροφή στον Μετασχηματισμό Fourier.

👁 Οι αριθμοί $(\omega_N^0)^2, (\omega_N^1)^2, \dots, (\omega_N^N)^2$ είναι μόνο $N/2$ διακριτοί αριθμοί.

Και για την ακρίβεια ισούνται με $\omega_{N/2}^0, \omega_{N/2}^2, \dots, \omega_{N/2}^{\frac{N}{2}-1}$.

Επιστροφή στον Μετασχηματισμό Fourier.

👁 Οι αριθμοί $(\omega_N^0)^2, (\omega_N^1)^2, \dots, (\omega_N^N)^2$ είναι μόνο $N/2$ διακριτοί αριθμοί.

Και για την ακρίβεια ισούνται με $\omega_{N/2}^0, \omega_{N/2}^2, \dots, \omega_{N/2}^{\frac{N}{2}-1}$.

Άρα, έχουμε να αποτιμήσουμε δύο πολυώνυμα βαθμού $< \frac{N}{2}$ στις $N/2$ -οστές ρίζες της μονάδας.

Επιστροφή στον Μετασχηματισμό Fourier.

👁 Οι αριθμοί $(\omega_N^0)^2, (\omega_N^1)^2, \dots, (\omega_N^N)^2$ είναι μόνο $N/2$ διακριτοί αριθμοί.

Και για την ακρίβεια ισούνται με $\omega_{N/2}^0, \omega_{N/2}^2, \dots, \omega_{N/2}^{\frac{N}{2}-1}$.

Άρα, έχουμε να αποτιμήσουμε δύο πολυώνυμα βαθμού $< \frac{N}{2}$ στις $N/2$ -οστές ρίζες της μονάδας.

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 $p(\omega^0), p(\omega^1), \dots, p(\omega^{N-1})$

★ Χρόνος εκτέλεσης: $T(n) = 2 \cdot T(n/2) + O(n)$

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 $p(\omega^0), p(\omega^1), \dots, p(\omega^{N-1})$

★ Χρόνος εκτέλεσης: $T(n) = 2 \cdot T(n/2) + O(n) = O(n \log n)$

Αλγόριθμος αντίστροφου 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 $p(\omega^0), p(\omega^1), \dots, p(\omega^{N-1})$

Θεώρημα

Μπορούμε να υπολογίσουμε τον Διακριτό Μετασχηματισμό Fourier (ή τον αντίστροφό του) ενός διανύσματος μήκους n σε χρόνο $O(n \log n)$.

Θεώρημα

Δοθέντων των συντελεστών δύο πολυωνύμων βαθμού $< n$ μπορούμε να υπολογίσουμε τους συντελεστές του γινομένου τους σε χρόνο $O(n \log n)$.

👉 (Για να είμαστε ακριβείς, στα παραπάνω αποτελέσματα μπορούμε να αποδείξουμε ότι παίρνουμε το σωστό αποτέλεσμα με πολύ μικρό σφάλμα $\approx 2^{-w}$ ανά αριθμό της εξόδου.)