Fast Fourier Transform

Ελπίδα Χαρά Εμμανουηλίδη

Οκτώβριος 2023

Αναδρομή στο Παρελθόν

"The most important numerical algorithm of our lifetime"

-Gilbert Strang

Αναδρομή στο Παρελθόν

Αναδρομή στο Παρελθόν

- C.F Gauss, 1805
- Cooley-Tukey, 1965

Στόχος

- Πολλαπλασιασμός πολυωνύμων

$$A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_d \cdot x^d$$

$$B(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \ldots + b_d \cdot x^d$$

$$C(x) = A(x) \cdot B(x)$$

Βασικές Ιδέες

- Οποιοδήποτε πολυώνυμο βαθμού d μπορεί να αναπαρασταθεί με μοναδικό τρόπο από $d+1$ σημεία στο επίπεδο.

Βασικές Ιδέες

- Αναπαράσταση πολυωνύμων :

$$P(x) = p_0 + p_1 \cdot x + p_2 \cdot x^2 + ... + p_d \cdot x^d$$

-Αναπαράσταση με συντελεστές:

$[p_0, p_1, ..., p_d]$

$\Rightarrow$πολλαπλασιασμός πολυωνύμων σε χρόνο $O(d^2)$.

-Αναπαράσταση με τιμές:

$\{(x_0, P(x_0)), (x_1, P(x_1)), ..., (x_d, P(x_d))\}$

$\Rightarrow$πολλαπλασιασμός πολυωνύμων σε $O(d)$.

Βασικές Ιδέες

Παράδειγμα

$$A(x) = x^2 + 2x + 1 \; , \quad [(-2,1),(-1,0),(0,1),(1,4),(2,9)]$$

$$B(x) = x^2 - 2x + 1 \; , \quad [(-2,9),(-1,4),(0,1),(1,0),(2,1)]$$

$$C(x) = ?$$

Πλάνο

- Δίνονται πολυώνυμα $A(x)$ και $B(x)$ βαθμού d σε αναπαράσταση συντελεστών.
- Βρίσκω την αναπαράσταση τιμών για τα $A(x)$ και $B(x)$ σε $2d + 1$ σημεία.
- Πολλαπλασιάζουμε κατά σημείο ανά ζεύγη ώστε να πάρουμε την αναπαράσταση τιμών για το $C(x) = A(x) \cdot B(x)$.
- Θα μετατρέψουμε την αναπαράσταση τιμών του $C(x)$ σε αναπαράσταση συντλεστών.

Evaluation

- Αναπαράσταση με συντελεστές → Αναπαράσταση με τιμές

$$P(x) = p_0 + p_1 \cdot x + p_2 \cdot x^2 + \ldots + p_d \cdot x^d$$

$$(1, P(1)) \longrightarrow (1, p_0 + p_1 \cdot 1 + p_2 \cdot 1^2 + \ldots + p^d \cdot 1^d)$$

$$(2, P(2)) \longrightarrow (2, p_0 + p_1 \cdot 2 + p_2 \cdot 2^2 + \ldots + p^d \cdot 2^d)$$

$$\vdots \qquad\qquad \vdots$$

$$(n, P(n)) \longrightarrow (n, p_0 + p_1 \cdot n + p_2 \cdot n^2 + \ldots + p^d \cdot n^d)\ , \quad n \geq d + 1$$

Evaluation

ΧΡΟΝΟΣ : $\mathbf{O(d^2)}$

Επιλογή Σημείων

- Για πολυώνυμο βαθμού $n-1$, το οποίο θέλουμε να αποτιμήσουμε για $(n-1)+1=n$ σημεία επιλέγουμε τα ζεύγη αριθμών:

$$\pm \mathrm{x}_1,\ \pm \mathrm{x}_2,\ \ldots,\ \pm \mathrm{x}_{\frac{n}{2}}$$

- $P(-x) = P(x)$
- $P(-x) = -P(x)$

Επιλογή Σημείων

- Επεκτείνουμε την ιδέα :

$$P(x) = P_e(x^2) + x \cdot P_o(x^2) \ ,$$

όπου $P_e(x^2)$, $P_o(x^2)$ είναι βαθμού $\frac{n}{2} - 1$.

- Γενικότερα :

$$P(x_i) = P_e(x_i^2) + x_i \cdot P_o(x_i^2)$$

$$P(-x_i) = P_e(x_i^2) - x_i \cdot P_o(x_i^2)$$

Επιλογή Σημείων

- Συμπέρασμα: ο υπολογισμός του $P(x)$ σε n ζεύγη σημείων $\pm x_1$, $\pm x_2$, ..., $\pm x_{\frac{n}{2}}$, ανάγεται στον υπολογισμό των $P_e(x^2)$, $P_o(x^2)$ στα $n/2$ σημεία $x_1^2, x_2^2, \ldots, x_{\frac{n}{2}}^2$.

Επιλογή Σημείων

- Χρόνος : Το αρχικό πρόβλημα μεγέθους n χωρίζεται σε δύο υποπροβλήματα ίδιου τύπου, μεγέθους $n/2$ και γραμμικού χρόνου. Συνεπώς προκύπτει η αναδρομική σχέση :

$$T(n) = 2 \cdot T(\tfrac{n}{2}) + O(n).$$

Άρα,

$$O(nlogn).$$

Επιλογή Σημείων

ΠΡΟΒΛΗΜΑ ?!

Πρόβλημα

- Το πρόβλημα υπάρχει στο βήμα της αναδρομής. Όλη η ιδέα βασίζεται στο γεγονός ότι για την αποτίμηση του πολυωνύμου θα χρησιμοποιήσουμε θετικά και αρνητικά ζεύγη σημείων

$$\pm x_1,\ \pm x_2,\ \ldots,\ \pm x_{\frac{n}{2}}.$$

Η κατασκευή αυτή δουλεύει για το πρώτο επίπεδο της αναδρομής όμως στο επόμενο βήμα υπολογίζουμε $n/2$ σημεία καθένα εκ των οποίων είναι υψωμένα στο τετράγωνο.

- Η αναδρομή ≪σπάει≫.

Ερώτημα

- Μπορούμε να κάνουμε το σύνολο των $x_1^2, x_2^2, \ldots, x_{\frac{n}{2}}^2$ να είναι ζεύγη αριθμών με τους αντίθετους τους;

Ερώτημα-Λύση

- Μπορούμε να κάνουμε το σύνολο των $x_1^2, x_2^2, \ldots, x_{\frac{n}{2}}^2$ να είναι ζεύγη αριθμών με τους αντίθετους τους;
- Λύση: Μιγαδικοί αριθμοί $\Rightarrow$ Ρίζες της μονάδας.

Ρίζες της μονάδας

Παράδειγμα

$$P(x) = x^3 + x^2 - x - 1$$

Ρίζες της μονάδας

- Γενίκευση: Για πολυώνυμο

$$P(x) = p_0 + p_1 \cdot x + p_2 \cdot x^2 + \ldots + p_d \cdot x^d$$

χρειαζόμαστε $n \geq (d+1)$ σημεία όπου $n = 2^k$. Τα σημεία που θα διαλέξουμε θα είναι n-οστες ρίζες της μονάδας.

Ρίζες της μονάδας

- Τι είναι όμως οι ρίζες της μονάδας;

→ n μιγαδικές ρίζες της εξίσωσης $z^n = 1$.

→ σημεία που ισαπέχουν πάνω στον μοναδιαίο κύκλο.

→ ορίζουμε τις ρίζες της μονάδας μέσω του όρου $\omega = e^{\frac{2\pi i}{n}}$.

→ όταν θέλουμε να υπολογίσουμε ένα πολυώνυμο για τις n-οστες ρίζες της μονάδας θα το υπολογίζουμε για

$$[\omega^0, \omega^1, ..., \omega^{n-1}].$$

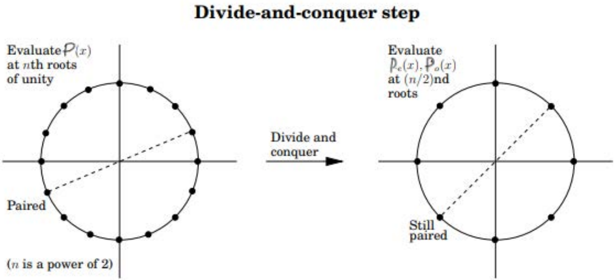
Ρίζες της μονάδας

- Γιατί ο αναδρομικός αλγόριθμος θα λειτουργήσει;

→ Οι n-οστές ρίζες είναι ζεύγη θετικών-αρνητικών αριθμών διότι $\omega^{j+n/2} = -\omega^{j}$.

→ Τετραγωνίζοντας αυτές έχουμε τις $n/2$ ρίζες του $z^{n/2} = 1$.

Ρίζες της μονάδας



Ρίζες της μονάδας

- Συμπέρασμα : Για n δύναμη του 2, σε κάθε επόμενο βήμα της αναδρομής έχουμε τις $(n/2k)$ ρίζες του $z^{n/2^k} = 1$, για $k = 0, 1, 2, ...$ κάθε σετ εκ΄των οποίων είναι ζεύγη θετικών-αρνητικών αριθμών. Άρα αυτό το μοτίβο λειτουργεί σε κάθε επίπεδο της αναδρομής έως ότου καταλήξουμε σε ένα σημείο.

Εκτέλεση του FFT

$$\underline{FFT} \quad P(x) : [p_0, p_1, ..., p_{n-1}]$$

$$\omega = e^{\frac{2\pi i}{n}} : [\omega^0, \omega^1, ..., \omega^{n-1}]$$

$$\swarrow \qquad\qquad\qquad \searrow$$

$$\underline{\text{FFT}} \;\; P_e(x^2) : [p_0, p_2, ..., p_{n-2}] \qquad \underline{\text{FFT}} \;\; P_o(x^2) : [p_1, p_3, ..., p_{n-1}]$$

$$[\omega^0, \omega^2, ..., \omega^{n-2}] \qquad\qquad [\omega^0, \omega^2, ..., \omega^{n-2}]$$

$$\downarrow \qquad\qquad\qquad \downarrow$$

Εκτέλεση του FFT

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$y_e = [P_e(\omega^0), ..., P_e(\omega^{n-2})] \qquad y_o = [P_o(\omega^0), ..., P_o(\omega^{n-2})]$$

$$\searrow \qquad\qquad\qquad\qquad \swarrow$$

$$P(\omega^j) = P_e(\omega^{2j}) + \omega^j \cdot P_e(\omega^{2j})$$

$$P(\omega^{j+n/2}) = P_e(\omega^{2j}) - \omega^j \cdot P_e(\omega^{2j})$$

$$j \in \{0, 1, 2, ..., (n/2 - 1)\}$$

$$\downarrow$$

$$y = [P(\omega^0), P(\omega^1), ..., P(\omega^{n-1})]$$

Interpolation

- Μπορούμε να περιγράψουμε την διαδικασία του Evaluation, δηλαδή την αναπαράσταση τιμών ενός πολυωνύμου, μέσω του πίνακα :

$$\begin{bmatrix} P(x_o) \\ \vdots \\ P(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \cdot \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

Interpolation

- Στον FFT το k-οστό στοιχείο αποτίμησης είναι το $x_k = \omega^k$. Άρα :

$$\underbrace{\begin{bmatrix} P(\omega^0) \\ \\ \vdots \\ \\ P(\omega^{n-1}) \end{bmatrix}}_{Y} = \underbrace{\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2\cdot(n-1)} & \dots & \omega^{(n-1)\cdot(n-1)} \end{bmatrix}}_{V} \cdot \underbrace{\begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{bmatrix}}_{p}$$

Ουσιαστικά:

$$FFT : \mathbb{C}^n \to \mathbb{C}^n,\ FFT(p) = V \cdot p.$$

Interpolation

Πως γυρίζω πίσω ?!

Interpolation

- Στόχος : $p = V^{-1} \cdot Y$
- Αν δείξουμε την ισότητα

$$V^{-1} = \frac{1}{n}\bar{V}$$

θα ισχύει ότι οι συζυγείς ρίζες της μονάδας είναι επίσης ρίζες της μονάδας οπότε μπορούμε να εφαρμόσουμε *FFT* με την διαφορά ότι $\omega = \omega^{-1}$ και ο πίνακας που προκύπτει θα είναι πολλαπλασιασμένος με $\frac{1}{n}$.

Interpolation

- Απόδειξη : Θ.δ.ο $V \cdot \bar{V} = n \cdot I$.

Έστω η k-οστή γραμμή του πίνακα V και η j-οστή στήλη του συζυγούς πίνακα $\bar{V}$. Τότε

$$\begin{pmatrix} 1 & e^{\frac{2\pi \cdot i \cdot k}{n}} & \dots & e^{\frac{2\pi \cdot k \cdot (n-1)}{n}} \end{pmatrix} \cdot \begin{pmatrix} e^{-\frac{2\pi \cdot i \cdot j}{n}} \\ \vdots \\ e^{-\frac{2\pi \cdot i \cdot (n-1) \cdot j}{n}} \end{pmatrix} = \sum_{i=0}^{n-1} e^{\frac{2\pi \cdot i \cdot (k-j)}{n}}$$

$\Rightarrow$Αν $k = j$ τότε το εσωτερικό γινόμενο ισούται με n.

$\Rightarrow$Αν $k \neq j$ προκύπτει η γεωμετρική σειρά με λόγο $e^{\frac{2\pi \cdot (k-j)}{n}}$ και ισούται με 0.

Inversion

• Inverse FFT : Άρα για να βρούμε τους συντελεστές ενός πολυωνύμου χρειάζεται απλώς να τρέξουμε τον *FFT* χρησιμοποιώντας το $\omega^{-1} = e^{-2\pi i/n}$ για τις n-οστές ρίζες της μονάδας και να πολλαπλασιάσουμε με $\frac{1}{n}$ τον πίνακα που προκύπτει.

Ουσιαστικά :

$$IFFT : \mathbb{C}^n \to \mathbb{C}^n,\ IFFT(Y) = V^{-1} \cdot Y.$$

Recap

- Οι τέσσερεις βασικές ιδέες :

i) Πολλαπλασιασμός πολυωνύμων σε αναπαράσταση τιμών.

ii) Evaluation σε $\pm$ ζεύγη τιμών.

iii) Evaluation στις n-οστές ρίζες της μονάδας $\Rightarrow$ *FFT*.

iv) Interpolation λύνεται επίσης με *FFT* αλλά $\omega = \frac{1}{n}\omega^{-1}$ $\Rightarrow$ *IFFT*.

References

Dasgupta, C.H. Papadimitriou, U.V. Vazirani. *Algorithms* (McGraw-Hill), 2008

J.Kleinberg, E.Tardos. *Algorithm Design* (Addison-Wesley), 2006