Π01Β. Παραλληλοι Αλγοριθμοι και Πολυπλοκοτητα

Ο Γρηγορος Μετασχηματισμος Fourier

Παπανικολάου Κωνσταντῖνος

μΠλ∀

Ὁ Συνεχὴς Μετασχηματισμὸς Fourier

Μία σειρὰ Fourier εἶναι τὸ ἀνάπτυγμα μιᾶς περιοδικῆς συναρτήσεως $f(x)$ σὰν ἄπειρο ἄθροισμα ἡμιτόνων καὶ συνημιτόνων:

$$f(x) = \frac{1}{2}\alpha_0 + \sum_{n=1}^{\infty} \alpha_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx)$$

ὅπου γιὰ $n > 0$ ἔχουμε:

$$\begin{aligned} \alpha_0 &= \tfrac{1}{\pi}\textstyle\int_{-\pi}^{\pi} f(x)\,dx \\ \alpha_n &= \tfrac{1}{\pi}\textstyle\int_{-\pi}^{\pi} f(x)\cos(nx)\,dx \\ b_n &= \tfrac{1}{\pi}\textstyle\int_{-\pi}^{\pi} f(x)\sin(nx)\,dx \end{aligned}$$

Ὁ μετασχηματισμὸς Fourier εἶναι μία γενίκευση τῆς μιγαδικῆς σειρᾶς Fourier καὶ εἶναι:

$$F(\nu) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i\nu x} dx$$

καὶ ὁ ἀντίστροφος

$$f(x) = \int_{-\infty}^{\infty} F(\nu)\, e^{2\pi i\nu x} d\nu$$

ἂν καὶ θέτοντας $\omega = 2\pi\nu$ μερικοὶ τὸν γράφουν:

$$H(\omega) = \int_{-\infty}^{\infty} h(t)\, e^{-i\omega t} dt$$

καὶ ὁ ἀντίστροφος

$$h(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} H(\omega)\, e^{i\omega t} d\omega$$

Ὁ Διακριτὸς Μετασχηματισμὸς Fourier

Ἔστω τὸ ἄνυσμα $\vec{x} = (x_0, \ldots, x_{N-1})$ μὲ N μιγαδικὲς συνιστῶσες, τότε ὁ διακριτὸς μετασχηματισμὸς Fourier τοῦ $\vec{x}$ εἶναι τὸ ἄνυσμα $\vec{y} = (y_0, \ldots, y_{N-1})$ ὅπου:

$$y_j = \sum_{k=0}^{N-1} x_k \cdot \omega_N^{k \cdot j}, \qquad j = 0, \ldots, N-1$$

ὅπου $\omega_N = e^{\frac{2\pi i}{N}}$ εἶναι ἡ N-οστὴ πρωταρχικὴ μιγαδικὴ ρίζα τῆς μονάδος δηλαδὴ $\omega_N^N = 1$ καὶ γιὰ κάθε $0 < j < N$ ἔχουμε $\omega_N^j \neq 1$. Δηλαδὴ $\vec{y} = \vec{x} \cdot F_N$ ἢ $\vec{y}^T = F_N \cdot \vec{x}^T$, ὅπου F_N εἶναι ἕνας $N \times N$ πίνακας μὲ $F_{N\ k+1, j+1} = \omega_N^{k \cdot j}$ μὲ $0 \leq k, j < N$. Παρατηρῶ ὅτι λόγω κατασκευῆς τοῦ πίνακα αὐτοῦ ἰσχύει $F_N = F_N^T$.
Χρειαζόμαστε συνολικὰ N^2 πολλαπλασιασμοὺς (βήματα) καὶ $N^2 - N$ προσθέσεις στοὺς μιγαδικοὺς ἀριθμούς.

Ὑπολογισμὸς τοῦ πίνακα F_N: Γνωρίζοντας ὅτι ἡ μονάδα ἔχει N πρωταρχικὲς ρίζες παρατηρῶ ὅτι ἀπὸ τὸν ὁρισμὸ τῆς διαιρέσεως ἀκεραίων ἰσχύει γιὰ κάποια $0 \leq m$ καὶ $0 \leq l < N$ ὅτι $k \cdot j = m \cdot N + l$ ἔτσι γιὰ ἐκθέτη στὸ ω_N βάζω τὸ $\mod(k \cdot j, N)$, ἀφοῦ $\omega_N^{m \cdot N + l} = \omega_N^{m \cdot N} \cdot \omega_N^l = \left(\omega_N^N\right)^m \cdot \omega_N^l = 1 \cdot \omega_N^l = \omega_N^l$ δηλαδή:

$$F_{N\ k+1,j+1} = \omega_N^{k \cdot j} = \omega_N^{\mod(k \cdot j, N)}$$

Ἐπειδὴ ὁ πίνακας F_N εἶναι συμμετρικὸς ὡς πρὸς τὴν κύρια διαγώνιο, δηλαδὴ $F_{N\ k+1,j+1} = F_{N\ j+1,k+1}$, ὑπολογίζω μόνο τὰ στοιχεῖα γιὰ τὰ ὁποῖα ἰσχύει $j \leq k$, δηλαδὴ τὴν κύρια διαγώνιο καὶ ὅτι ἔχει ἀπὸ κάτω.

Ἀντίστροφος τοῦ πίνακα F_N: Ὁ ἀντίστροφος πίνακας F_N^{-1} ὑπολογίζεται πολὺ εὔκολα ἀπὸ τὸν F_N βάζοντας

${F_N^{-1}}_{m+1,n+1} = \frac{1}{N}\omega_N^{-m\cdot n}$ μὲ $0 \leq m, n < N$. Ἔτσι γιὰ τὸ γινόμενο $F_N \cdot F_N^{-1}$ ἔχω γιὰ τὸ $m+1, n+1$ στοιχεῖο τοῦ γινομένου ὅτι ἰσοῦται μὲ τὸ

$$\sum_{k=0}^{N-1} \frac{\omega_N^{k\cdot m} \cdot \omega_N^{-k\cdot n}}{N} = \frac{1}{N}\sum_{k=0}^{N-1} \omega_N^{k(m-n)}$$

Ἐὰν $m = n$ δηλαδὴ τὸ στοιχεῖο βρίσκεται στὴν κύρια διαγώνιο τότε $\frac{1}{N}\sum_{k=0}^{N-1} \omega_N^{k(m-n)} = \frac{1}{N}\sum_{k=0}^{N-1} \omega_N^{k\cdot 0} = 1$, ἀλλιῶς γιὰ κάθε ἄλλο στοιχεῖο ἐκτὸς κυρίας διαγωνίου ἰσχύει $m \neq n$ τότε θέτω $p = m - n$ προφανῶς $p < N$ καὶ συνεπῶς $\omega_N^p \neq 1$ ἔτσι ἔχω $\frac{1}{N}\sum_{k=0}^{N-1} \omega_N^{k\cdot p} = \frac{1}{N}\left(\frac{1-\omega_N^{p\cdot N}}{1-\omega_N^p}\right) = 0$.

Εἶναι προφανὲς ὅτι τὸ ἴδιο ἰσχύει καὶ γιὰ τὸ γινόμενο $F_N^{-1} \cdot F_N$.

Λῆμμα 1: (Θὰ χρησιμοποιηθῆ μόνο ὅταν N ἄρτιος) $\omega_{N/2} = \omega_N^2$.

Ἀπόδειξη: Προφανῶς $\omega_N = e^{\frac{2\pi i}{N}}$ καὶ $\omega_N^2 = \left(e^{\frac{2\pi i}{N}}\right)^2 = e^{\frac{2\cdot 2\pi i}{N}}$.

Ἰσχύει ὅμως $\frac{2\cdot 2\pi i}{N} = \frac{2\pi i}{\frac{N}{2}}$ καὶ ἀπὸ τὸν ὁρισμὸ ἔχουμε $\omega_{N/2} = e^{\frac{2\pi i}{\frac{N}{2}}}$.

Ἄρα $\omega_{N/2} = \omega_N^2$.

Λῆμμα 2: $\omega_{d\cdot N}^{d\cdot k} = \omega_N^k$.

Ἀπόδειξη: $\omega_{d\cdot N}^{d\cdot k} = \left(e^{\frac{2\pi i}{d\cdot N}}\right)^{d\cdot k} = \left(e^{\frac{2\pi i}{d\cdot N}\cdot d}\right)^k = \left(e^{\frac{2\pi i}{N}}\right)^k = \omega_N^k$.

Λῆμμα 3: (Θὰ χρησιμοποιηθῆ μόνο ὅταν N ζυγός) $\omega_N^{\frac{N}{2}} = -1$.

Ἀπόδειξη: $\omega_N^{\frac{N}{2}} = \left(e^{\frac{2\pi i}{N}}\right)^{\frac{N}{2}} = e^{\frac{2\pi i}{N}\cdot\frac{N}{2}} = e^{\pi i} = \cos\pi + i\cdot\sin\pi = -1$.

Ἔστω $\vec{z}$ διάνυσμα μὲ M συνιστῶσες ὅπου M ζυγός, τότε μὲ $\vec{z}_{[0]}$ καὶ $\vec{z}_{[1]}$ συμβολίζω τὰ ἑξῆς ὑποδιανύσματα τοῦ $\vec{z}$:

$$\vec{z}_{[0]} = (z_0, z_2, \ldots, z_{M-2}), \quad \vec{z}_{[1]} = (z_1, z_3, \ldots, z_{M-1})$$

Δηλαδὴ μὲ $\vec{z}_{[0]}$ συμβολίζω τὸ ὑποδιάνυσμα τοῦ $\vec{z}$ ποὺ περιέχει ὅλες τὶς ζυγὲς συνιστῶσες καὶ μὲ $\vec{z}_{[1]}$ αὐτὸ ποὺ περιέχει ὅλες τὶς μονὲς συνιστῶσες τοῦ $\vec{z}$.

Ὁ FFT βασίζεται στὴν ἑξῆς ἰδιότητα: Ἐὰν N εἶναι ἄρτιος καὶ γνωρίζω τοὺς μετασχηματισμοὺς Fourier τῶν $\vec{x}_{[0]}$ καὶ $\vec{x}_{[1]}$ δηλαδὴ $\vec{u} = F_{N/2} \cdot \vec{x}_{[0]}^{T}$ καὶ $\vec{v} = F_{N/2} \cdot \vec{x}_{[1]}^{T}$ τότε βρίσκω τὸν μετασχηματισμὸ Fourier τοῦ $\vec{x}$ ἀπὸ τὸν τύπο:

$$y_j = \begin{cases} u_j + \omega_N^j \cdot v_j & \text{ἐάν } 0 \leq j < N/2 \\ u_{j-N/2} + \omega_N^j \cdot v_{j-N/2} & \text{ἐάν } N/2 \leq j < N \end{cases}$$

Ἢ λόγω λήμματος 3 ἐὰν βάλλω $k = j$ ὅταν $0 \leq j < N/2$ καὶ $k = j - \frac{N}{2}$ ὅταν $N/2 \leq j < N$ ἔχουμε:

$$\begin{aligned} y_k &= u_k + \omega_N^k \cdot v_k && \text{ἐάν } 0 \leq k < N/2 \\ y_{k+N/2} &= u_{k+N/2-N/2} + \omega_N^{k+N/2} \cdot v_{k+N/2-N/2} && \text{ἐάν } 0 \leq k < N/2 \\ &= u_k + \omega_N^{k+N/2} \cdot v_k = u_k - \omega_N^k \cdot v_k && \text{ἐάν } 0 \leq k < N/2 \end{aligned}$$

Δεδομένου ὅτι ἀπὸ τὸ λῆμμα 1 ἔχω $\omega_{N/2} = \omega_N^2$ γιὰ τὸν ἀναδρομικὸ ὑπολογισμὸ τοῦ $F_{N/2}$ ἀπὸ τὸν F_N, ἐὰν $0 \leq k, j < N/2$ ἔχω:

$$F_{N/2\ k+1,j+1} = \omega_{N/2}^{k \cdot j} = \left(\omega_N^2\right)^{k \cdot j} = \left(\omega_N^{k \cdot j}\right)^2 = \left(F_{N\ k+1,j+1}\right)^2$$

Ἰσχύει $\left(\omega_N^2\right)^{k \cdot j} = \omega_N^{2 \cdot k \cdot j} = \omega_N^{\bmod (2 \cdot k \cdot j, N)}$, γιὰ $0 \leq k, j < N/2$.

Ἑπομένως $F_{N/2\ k+1,j+1} = \omega_N^{\bmod (2 \cdot k \cdot j, N)}$ ἄρα

$$F_{N/2\ k+1,j+1} = F_{N\ 2k+1,j+1} = F_{N\ k+1,2j+1}$$

Παράδειγμα γιὰ $N = 8$ ἔχουμε $\omega_8 = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$ καὶ γιὰ ἁπλοποίηση στὸ συμβολισμὸ βάζω $\omega = \omega_8$ καθῶς καὶ ἀπὸ τὸ λῆμμα 1 ἔχω $\omega^4 = -1$ καὶ ὁ πίνακας F_8 εἶναι ὁ

$$F_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & -1 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & -1 & \omega^6 & 1 & \omega^2 & -1 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & -1 & \omega^7 & \omega^2 & \omega^5 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega^5 & \omega^2 & \omega^7 & -1 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & -1 & \omega^2 & 1 & \omega^6 & -1 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & -1 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

ἔτσι γιὰ κάθε ἄνυσμα $\vec{x} = (x_0, \ldots, x_7)$ μὲ 8 συνιστῶσες ἔχω ὅτι ὁ FFT εἶναι τὸ $\vec{y} = \vec{x} \cdot F_8$ ἢ $\vec{y}^T = F_8 \cdot \vec{x}^T$.
Ἐδῶ ἐπίτηδες διαλέχθηκε τὸ 8, γιατὶ εἶναι δύναμις τοῦ 2 καὶ θὰ χρησιμεύση ὡς παράδειγμα παρακάτω.

Γιὰ τὸν F_4 ἔχουμε $\omega_4 = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}}$ καὶ γιὰ ἁπλοποίηση στὸ συμβολισμὸ βάζω $\omega' = \omega_4$ καὶ ὁ πίνακας F_4 εἶναι ὁ

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega' & \omega'^2 & \omega'^3 \\ 1 & \omega'^2 & 1 & \omega'^2 \\ 1 & \omega'^3 & \omega'^2 & \omega' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^2 & -1 & \omega^6 \\ 1 & -1 & 1 & -1 \\ 1 & \omega^6 & -1 & \omega^2 \end{pmatrix}$$

δεδομένου ὅτι $\omega' = \omega_4 = \omega_8^2 = \omega^2$.

Γιὰ τὸν F_2 ἔχουμε $\omega_2 = e^{\frac{2\pi i}{2}} = e^{\pi i}$ καὶ γιὰ ἁπλοποίηση στὸ συμβολισμὸ βάζω $\omega'' = \omega_2$ καὶ ὁ πίνακας F_2 εἶναι ὁ

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & \omega'' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & \omega'^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

δεδομένου ὅτι $\omega'' = \omega_2 = \omega_4^2 = \omega'^2 = \omega^4 = -1$.

Οὐσιαστικὰ χρησιμοποιῶ γιὰ νὰ βρῶ τὸν $F_{N/2}$ ἀπὸ τὸν F_N τὸ πάνω ἀριστερὰ τέταρτο τοῦ F_N. Δηλαδὴ τὸ βάθος τῶν πινάκων εἶναι $\log N$. Σὲ αὐτὸ τὸ παράδειγμα φαίνεται ὅτι μὲ ἕνα μόνο ὑπολογισμὸ τοῦ F_N ἔχω ὅλους τοὺς ὑπολοίπους πίνακες.

Ἔτσι ἐὰν τὸ N εἶναι δύναμις τοῦ 2, ἔχω τὸν ἑξῆς ἀλγόριθμο ὁ ὁποῖος πιὸ κάτω θὰ γίνη παράλληλος σὲ N ἐπεξεργαστές.

Ὁ FFT Ἀλγόριθμος

Recursive-FFT($\vec{x}$)

1. $N =$ μῆκος τοῦ $\vec{x}$ (δύναμις τοῦ 2)

2. Ἐὰν $N = 1$ γύρισε $\vec{x}$

3. $\vec{x}_{[0]} = (x_0, x_2, \ldots, x_{N-2})$ καὶ $\vec{x}_{[1]} = (x_1, x_3, \ldots, x_{N-1})$

4. $\vec{u} =$ Recursive-FFT($\vec{x}_{[0]}$)

5. $\vec{v} =$ Recursive-FFT($\vec{x}_{[1]}$)

6. $\omega_N = e^{\frac{2\pi i}{N}}$ καὶ $\omega = 1$

7. **for** $k = 0$ **to** $N/2 - 1$

   (α′) $y_k = \vec{u}_k + \omega \cdot \vec{v}_k$

   (β′) $y_{k+\frac{N}{2}} = \vec{u}_k - \omega \cdot \vec{v}_k$

   (γ′) $\omega = \omega \cdot \omega_N$

8. Γύρισε $\vec{y}$

Ὁ Ἐπαναληπτικὸς (Μὴ Ἀναδρομικὸς) FFT Ἀλγόριθμος

Rev(k) (τὸ k εἶναι ἀκέραιος στὸ δυαδικὸ σύστημα)

1. l εἶναι τὸ μῆκος τοῦ k σὲ bits

2. **for** $r = 1$ **to** $\left\lceil \frac{l}{2} \right\rceil$

   (α΄) Ἀντάλλαξε τὸ $r-1$ bit μὲ τὸ $l-r$ bit στὴν δυαδικὴ ἀναπαράσταση τοῦ k

3. γύρισε k

Bit-Reverse-Copy($\vec{X}, \vec{Y}$)

1. $N =$ μῆκος τοῦ $\vec{X}$

2. **for** $k = 0$ **to** N

   (α′) $Y_{\mathrm{Rev}(k)} = \vec{X}_k$

Iterative-FFT($\vec{x}$)

1. Bit-Reverse-Copy($\vec{x}, \vec{y}$)

2. $N =$ μῆκος τοῦ $\vec{x}$ (δύναμις τοῦ 2)

3. **for** $s = 1$ **to** $\lg N$ (τὸ $\lg N$ εἶναι πάντα ἀκέραιος)

   (α′) $m = 2^s$ (Τὸ m εἶναι πάντα ἄρτιος)

   (β′) $\omega_m = e^{\frac{2\pi i}{m}}$

   (γ′) **for** $k = 0$ **to** $N - 1$ μὲ βῆμα m (N/m ἐπαναλήψεις)

      i. $\omega = 1$

      ii. **for** $j = 0$ **to** $\frac{m}{2} - 1$ ($m/2$ ἐπαναλήψεις)

         Α′. $u = y_{k+j}$ καὶ $t = \omega \cdot y_{k+j+\frac{m}{2}}$

         Β′. $y_{k+j} = u + t$ καὶ $y_{k+j+\frac{m}{2}} = u - t =$ (ἤ) $u + \omega_m^{m/2} \cdot t$

         Γ′. $\omega = \omega \cdot \omega_m$

Ὁ Παράλληλος FFT Ἀλγόριθμος

Ὁ ἐπαναληπτικὸς (μὴ ἀναδρομικὸς) FFT ἀλγόριθμος Iterative-FFT μπορεῖ νὰ γίνη παράλληλος ἐκτελούμενος ἀπὸ τὸ βῆμα 2 σὲ ἕναν ὑπερκῦβο μὲ N ἐπεξεργαστὲς ἢ σὲ μία πεταλοὺδα μὲ $N \log N$ ἐπεξεργαστές, ἔχοντας ὅμως σὰν εἴσοδο ὄχι τὸ $\vec{x} = (x_0, \ldots, x_{N-1})$ ἀλλὰ τὸ $\vec{y} = \left(x_{\mathsf{Rev}(0)}, \ldots, x_{\mathsf{Rev}(N-1)}\right)$ προερχόμενο ἀπὸ τὴν Bit-Reverse-Copy$(\vec{x}, \vec{y})$. Π.χ. γιὰ $N = 8$ ἔχουμε τὸ γνωστὸ παράδειγμα τοῦ βιβλίου.

Ἐφαρμογὴ στὸν Πολλαπλασιαμὸ Πολυωνύμων καὶ τὴν Συνέλιξη

Ἕνα πολυώνυμο βαθμοῦ $n-1$ $A(x) = \sum_{j=0}^{n-1} \alpha_j x^j$ ἀναπαρίσταται μὲ δύο τρόπους:

1. Σὰν ἕνα διάνυσμα μήκους n τῶν συντελεστῶν τῶν μονωνύμων του $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$

2. Σὰν ἀναπαράσταση σημείων - τιμῶν δηλαδὴ σὰν ἕνα σύνολο n διατεταγμένων ζευγῶν $\{(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})\}$ τέτοια ὥστε γιὰ κάθε ζεῦγος νὰ ἰσχύη $y_k = A(x_k)$.
   Παρατήρηση: Γιὰ νὰ ἔχη τὸ παραπάνω σύνολο n στοιχεῖα (διατεταγμένα ζεύγη) θὰ πρέπει γιὰ κάθε x_j, x_k μὲ $j \neq k$ ποὺ ἀνῆκουν στὸ $\{x_0, x_1, \cdots, x_{n-1}\}$ νὰ ἰσχύη $x_j \neq x_k$

Ἐὰν ἔχω ἕνα πολυώνυμο $p(x) = \sum_{j=0}^{n-1} p_j x^j$ βαθμοῦ $n-1$ καὶ πάρω τὶς n μιγαδικὲς ρίζες τῆς μονάδος γιὰ τὴν ἀναπαράσταση σημείων τιμῶν τότε ἔχω τὸ ἐξῆς σύνολο:

$$\left\{\left(\omega_n^0, p\left(\omega_n^0\right)\right), \left(\omega_n^1, p\left(\omega_n^1\right)\right), \cdots, \left(\omega_n^{n-1}, p\left(\omega_n^{n-1}\right)\right)\right\}$$

Παρατηρῶ ὅμως ὅτι :

$$p\left(\omega_n^j\right) = \sum_{k=0}^{n-1} p_k \left(\omega_n^j\right)^k = \sum_{k=0}^{n-1} p_k \omega_n^{jk}$$

Ἄρα γίνεται προφανὲς ὅτι:

$$\begin{pmatrix} p\left(\omega_n^0\right) \\ p\left(\omega_n^1\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right) \end{pmatrix} = F_n \cdot \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{pmatrix}$$

Οὐσιαστικὰ ἐφαρμόζεται ὁ μετασχηματισμὸς Fourier γιὰ τὸ διάνυσμα $(p_0, p_0, \cdots, p_{n-1})$ καὶ τὸ πολυώνυμο p ἀλλάζει τρόπο ἀναπαραστάσεως.

Ἐφόσον ὁ F_n ἀντιστέφεται ἔχω

$$\begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{pmatrix} = F_n^{-1} \cdot \begin{pmatrix} p\left(\omega_n^0\right) \\ p\left(\omega_n^1\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right) \end{pmatrix}$$

Ἐδῶ χρησιμοποιεῖται ὁ ἀντίστροφος μετασχηματισμός Fourier ποὺ εἶναι ὅμως ὁ ἴδιος ἀλγόριθμος τοῦ FFT ἀλλὰ μὲ ἄλλο πίνακα, γιατὶ ἡ ω_n^{-1} ἀνῆκει καὶ αὐτὴ στὶς n μιγαδικὲς ρίζες τῆς μονάδος.

Ἔτσι ἐὰν θέλουμε νὰ πολλαπλασιάσουμε δύο πολυώνυμα A καὶ B βαθμοῦ $n_A - 1$ καὶ $n_B - 1$ ἀντιστοίχως καὶ ὡς ἀποτέλεσμα ἔχουμε ἕνα πολυώνυμο H βαθμοῦ $n_H - 1$ ὅπου τὸ n_H εἶναι δύναμις τοῦ 2 ἔχουμε τὸν ἑξῆς ἀλγόριθμο:

1. Βρὲς τὶς n_H μιγαδικὲς ρίζες τῆς μονάδος καὶ ὑπολόγισε τὶς τιμὲς τῶν A καὶ B χρησιμοποιώντας τὸν μετασχηματισμὸ Fourier.

2. Ὑπολόγισε τὸ H στὶς n_H μιγαδικὲς ρίζες τῆς μονάδος ἀπὸ τὸν τύπο $H\left(\omega_{n_H}^{j}\right) = A\left(\omega_{n_H}^{j}\right) B\left(\omega_{n_H}^{j}\right)$.

3. Βρὲς τοὺς συντελεστὲς τῶν μονωνύμων τοῦ H ἀπὸ τὶς τιμές του στὶς n_H μιγαδικὲς ρίζες τῆς μονάδος, χρησιμοποιώντας τὸν ἀντίστροφο μετασχηματισμὸ Fourier.

Προσοχή: Στὰ πολυώνυμα A καὶ B θεωρῶ ὅτι ἔχουν μηδενικοὺς συντελεστὲς σὲ ὅλα τὰ μονώνυμα ἀπὸ βαθμὸ n_A καὶ n_B ἀντιστοίχως μὲχρι καὶ βαθμοῦ n_{H-1}. Αὐτὸ κάνει δυνατὸ τὸν μετασχηματισμὸ Fourier ἀφοῦ πουθενὰ δὲν ὑφίσταται περιορισμὸς στοὺς συντελεστὲς τῶν πολυωνύμων, πόσοι εἶναι ἢ τί τιμὲς ἔχουν.
Τὸ πρῶτο βῆμα θέλει παράλληλο χρόνο $O(\log n_H)$, τὸ δεύτερο βῆμα θέλει παράλληλο χρόνο $O(1)$ καὶ τὸ τρίτο βῆμα θέλει πάλι παράλληλο χρόνο $O(\log n_H)$. ἄρα ὁ πολλαπλασιασμὸς πολυωνύμων γίνεται σὲ χρόνο $O(\log n_H)$.

Ἡ συνέλιξη πάλι εἶναι οὐσιαστικὰ ἕνας πολλαπλασιασμὸς πολυωνύμων καὶ τὰ A καὶ B εἶναι διανύσματα.

Ἀκρίβεια Ὑπολογισμῶν τοῦ FFT Ἀλγορίθμου

Ἡ N-οστὴ ρίζα τῆς μονάδος δὲν μπορεῖ νὰ ὑπολογισθῆ ἀκριβῶς ἀφοῦ μπορεῖ νὰ εἶναι ἄρρητος ἀριθμός. Γι᾽ αὐτό, ὅταν τὸ πρόβλημα (εἴσοδος) ἔχει ρητοὺς ἀριθμούς, (κατ᾽ οὐσίαν ἀκεραίους) τότε ἔχει νόημα νὰ γίνουν οἱ ὑπολογισμοὶ ὡς πρὸς modulo m, ὅπου m κάποιος καταλλήλως ἐπιλεγμένος ἀκέραιος. Γιὰ ἕναν ἀλγόριθμο FFT ποὺ ἡ εἴσοδός του θὰ εἶναι ἀκέραιοι ἡ ἐπιλογὴ τοῦ m θὰ πρέπη νὰ ἱκανοποιῆ ἀρκετὲς συνθῆκες.

Θὰ πρέπη τὸ m νὰ εἶναι ἀρκετὰ μεγάλο ὥστε ἡ πραγματικὴ ἔξοδος τοῦ προβλήματος νὰ μπορῆ νὰ ἐξαχθῆ ἀπὸ τὴν ἔξοδο ὡς πρὸς modulo m. Δηλαδὴ ἔστω $\vec{\alpha} = \left(\alpha_0, \alpha_1, \cdots, \alpha_{N/2-1}\right)$ καὶ $\vec{b} = \left(b_0, b_1, \cdots, b_{N/2-1}\right)$ καὶ $\vec{c} = (c_0, c_1, \cdots, c_{N-2})$ ἡ ἔξοδος, τότε

$$m > N \cdot \left(\max_{0 \le j < N/2} \left|\alpha_j\right|\right) \cdot \left(\max_{0 \le j < N/2} \left|b_j\right|\right)$$

ποὺ σημαίνει ὅτι κάνοντας τὶς πράξεις στὸν ἀλγόριθμο ἔχουμε

$$m > 2 \cdot \left(\max_{0 \le j < N-1} \left| c_j \right| \right) \Longleftrightarrow \frac{m}{2} > \left(\max_{0 \le j < N-1} \left| c_j \right| \right)$$

ποὺ σημαίνει ὅτι τὸ $c_j = \text{if } \left(\left| c'_j \right| < \left| c'_j - m \right| \right) \text{ then } c'_j \text{ else } \left(c'_j - m \right)$ ὅπου c'_j εἶναι ἡ ἔξοδος modulo m.

Πρὲπει νὰ βρεθῆ ἕνα m ὡς πρὸς τὸ ὁποῖο τὸ N νὰ εἶναι ἀντιστρέψιμο, ἀφοῦ τὸ $1/N$ χρειάζεται στὸν ὑπολογισμὸ τοῦ F_N^{-1} καθῶς καὶ ἕνα ω_N ποὺ νὰ εἶναι ἡ N-οστὴ πρωταρχικὴ ρίζα τῆς μονάδος. Αὐτὸ δὲν εἶναι δύσκολο ὅταν τὸ N καὶ τὸ $\omega_N > 1$ εἶναι δυνάμεις τοῦ 2. Ἔτσι θέτω $m = \omega_N^{N/2} + 1$ ποὺ εἶναι περιττὸς καὶ τὸ N ἄρτιος ἄρα τὸ N εἶναι ἀντιστρέψιμο ὡς πρὸς modulo m.

Παρατηρῶ ὅτι $\omega_N^{N/2} = m - 1 \equiv -1 \mod m$ καὶ συνεπῶς $\omega_N^N \equiv (-1)^2 \equiv 1 \mod m$. Ἐπιπλέον μὲ κατάλληλη ἐπιλογὴ τοῦ $\omega_N = 2^a$ (ποὺ εἶναι ἀντιστρέψιμο ὡς πρὸς modulo m) ἐξασφαλίζουμε ὅτι $1 < \omega_N^p < m - 1$ γιὰ κάθε $0 < p < N/2$ ἄρα $\omega_N^p \neq \pm 1 \mod m$, ἐὰν $N/2 < p < N$ τότε $\omega_N^p \equiv -\omega_N^{p-N/2} \mod m$ ἀφοῦ $1 \equiv \omega_N^{N/2} \cdot \omega_N^{-N/2} \equiv -1 \cdot \omega_N^{-N/2} \mod m$ ἄρα $\omega_N^p \neq 1 \mod m$. Τὸ ω_N εἶναι N -οστὴ πρωταρικὴ ρίζα τῆς μονάδος modulo m.

Τὸ τελευταίο ποὺ ὑπολείπεται εἶναι νὰ δειχθῆ ὅτι

$$\frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{k \cdot p} = 0 \mod m$$

γιὰ κάθε p μὲ $0 < p < N$ (ἰσχύει σὲ σώματα καὶ σὲ δακτυλίους ἀλλὰ παραλείπεται ἡ ἀπὸδειξη).

Γιὰ νὰ ἰσχύουν τὰ προηγούμενα χρειαζόμαστε ἕνα κατάλληλο $\omega_N = 2^a$ καὶ ἐπιλέγουμε

$$a = \left\lceil \frac{2}{N} \log \left(N \cdot \left(\max_{0 \leq j < N/2} \left| \alpha_j \right| \right) \cdot \left(\max_{0 \leq j < N/2} \left| b_j \right| \right) \right) \right\rceil < \left\lceil \frac{2}{N} \log m \right\rceil$$

Ἐὰν τὰ α_j καὶ b_j ἔχουν τὸ πολὺ $O\left(N^b\right)$ μῆκος τότε τὸ m ἔχει καὶ αὐτὸ $O\left(N^b + \log N\right)$ μῆκος καὶ τὸ ω_N ἔχει a μῆκος δηλαδὴ ἀνάλογο τοῦ $O\left(N^{b-1} + \frac{\log N}{N}\right) \approx O\left(N^{b-1}\right)$. Παρατηρῶ ὅτι τὸ a δὲν εἶναι ἀρκετὰ μεγάλο ἀφοῦ ἔχει μῆκος $O\left((b-1)\log N\right)$.
Ἐὰν ἡ εἴσοδος ἔχει μῆκος $O\left(poly\left(b\right)\right)$ τότε κάθε ὑπολογισμὸς περιέχει ἀκεραίους μὲ $O\left(poly\left(b\right)\right)$ μῆκος.

Ἀφοῦ λοιπὸν μποροῦμε νὰ κάνουμε πράξεις (παράγραφος 1.2, 2.3) σὲ παράλληλο χρόνο $O(\log N)$ χρειαζόμαστε παράλληλο χρόνο $O\left(\log^2 N\right)$ γιὰ τὴν συνέλιξη δύο διανυσμάτων, γίνεται ὅμως καὶ σὲ παράλληλο χρόνο $O(\log N)$ ἐὰν παρατηρήσουμε ὅτι τὸ ω_N εἶναι δύναμις τοῦ 2 καὶ ἐφόσον ἡ ἀναπαράσταση εἶναι στὸ δυαδικό, μποροῦμε νὰ φτιάξουμε ἕναν πολλαπλασιαστὴ (bit ἐπεξεργαστὴ) σὲ κάθε ἐπεξεργαστὴ ποὺ νὰ κάνη κατ΄ εὐθείαν ὀλίσθηση τῶν bit ἀριστερά, μὲ ἀνάλογο τρόπο ἡ πρόσθεση γίνεται σὲ $O(1)$ χρόνο (παράγραφος 1.2.3).

Βεβαίως σὲ κάθε ἐνδιάμεσο στάδιο γίνεται πάντα ἀναγωγὴ ὡς πρὸς modulo m. Αὐτὸ εἶναι εὔκολο νὰ γίνη ἀφοῦ $2^{aN/2} \equiv -1 \pmod{m}$, ὅπου $m = \omega_N^{N/2} + 1$ καὶ $\omega_N = 2^a$. Ἑπομένως κάθε ἀκέραιος μήκους k μπορεῖ νὰ γραφῆ ὡς ἄθροισμα ἢ διαφορὰ $\left\lceil \frac{2k}{aN} \right\rceil$ (ὁ καθένας μήκους $\frac{aN}{2} = \lfloor \log m \rfloor$ modulo m).

Ἔτσι μποροῦμε νὰ ἀνάγουμε τὴν ὑπολογιζομένη τιμὴ σὲ κάθε βῆμα σὲ ἄθροισμα ἢ διαφορὰ δύο ἀκεραίων μήκους $\lfloor \log m \rfloor$ modulo m δηλαδή, σὲ σταθερό χρόνο.

Στὸ τέλος ὁ πολλαπλασιασμὸς μὲ τὸ $1/N$ modulo m εἶναι πάλι εὔκολος ἀφοῦ $\omega_N^N = 2^{aN} \equiv 1 \mod m$ ἄρα $N^{-1} \equiv 2^{aN - \log N} \mod m$, ἄρα ὁ πολλαπλασιασμὸς μὲ $1/N$ modulo m γίνεται μὲ μετακίνηση δεξιὰ $aN - \log N = O(\log m)$ bit.

Πρέπει νὰ γίνουν καὶ κάποιες μετατροπὲς συνολικοῦ χρόνου $O(\log N)$ γιὰ τὴν ἐμφάνιση τῶν ἀποτελεσμάτων. Δηλαδή, ἡ μετατροπὴ τῶν $O(\log m)$ μήκους εἰσόδων χρειάζεται $O(\log N)$ bit βήματα μὲ ἕνα πλῆρες δυϊαδικὸ δένδρο μὲ $O(\log N)$ φύλλα, ἐδῶ κάθε εἴσοδος ἔχει μῆκος $O(m)$ καὶ μποροῦμε νὰ μειώσουμε κάθε τιμὴ ὡς πρὸς modulo m σὲ $O(\log N)$ βήματα προσθέτοντας ἢ ἀφαιρώντας τὸ m τὸ πολὺ $O(1)$ φορές.

Χρειαζόμαστε $\Theta(\log m)$ bit ἐπεξεργαστὲς γιὰ τὶς φάσεις τοῦ ὑπολογισμοῦ στὸ βῆμα 1 καὶ παρεμβολῆς (interpolation) στὸ βῆμα 3 καὶ $\Theta\left(\log^2 m\right)$ bit ἐπεξεργαστὲς γιὰ τὴν φάση τοῦ πολλαπλασιασμοῦ τοῦ βήματος 2. Τὸ τελευταίο ὅριο μπορεῖ νὰ γίνη καὶ σὲ $O(\log m \log\log m)$ ὅπως θὰ φανῇ στὴν ἑπομένη παράγραφο 3.7.4 Ἐφαρμογὴ στὸν Πολλαπλασιασμὸ Ἀκεραίων.

Ἐφαρμογὴ στὸν Πολλαπλασιασμὸ Ἀκεραίων

Παρατηρώντας πιὸ προσεκτικὰ τὸν πολλαπλασιασμὸ ἀκεραίων καὶ πολυωνύμων μποροῦμε νὰ πολλαπλασιάσουμε 2 ἀκεραίους μήκους N σὲ χρόνο $O\left(N\log^2 N\log\log N\right)$, μὲ χρήση οὐρᾶς ὁ χρόνος μειώνεται σὲ $O\left(N\log N\log\log N\right)$.
Ἔτσι μπορῶ νὰ πολλαπλασιάσω 2 ἀκεραίους μήκους N mondulo 2^N+1 γιὰ κάθε N τοῦ τύπου $N=2^\delta\beta$ ὅπου δ καὶ β εἶναι ἀκεραίοι καὶ $\beta\leq 4\log N+2$ (δηλαδὴ τὸ N εἶναι μικρὸ πολλαπλάσιο μιᾶς δυνάμεως τοῦ 2).
Ἔστω a, b εἶναι 2 ἀκέραιοι μήκους N καὶ θέλουμε νὰ τοὺς πολλαπλασιάσουμε mondulo 2^N+1 ὅπου τὸ N ἱκανοποιεῖ τὰ παραπάνω. Ἔστω λοιπὸν r μὲ $\sqrt{\frac{N}{\log N}}<r\leq 2\sqrt{\frac{N}{\log N}}$ καὶ $s=N/r$.

Ἔτσι χωρίζω τοὺς a, b σὲ r μπλόκ μήκους s ἕκαστο καὶ τοὺς ἀναπαριστῶ μὲ 2 πολυώνυμα:

$$a = a\,(x) = \sum_{j=0}^{r-1} a_j x^j \quad , \qquad b = b\,(x) = \sum_{j=0}^{r-1} b_j x^j$$

ὅπου $x = 2^s$ καὶ τὰ a_j, b_j ἔχουν μῆκος s. Ἔτσι γιὰ τὸν ὑπολογισμὸ τοῦ γινομένου τῶν a, b ὑπολογίζω τὸ

$$ab = c\,(x) = \sum_{j=0}^{2(r-1)} c_j x^j$$

μὲ $x = 2^s$ καὶ

$$c_k = \sum^{k=j_1+j_2} a_{j_1} b_{j_2}$$

μὲ $0 \leq k \leq 2r-2$, καὶ ἀπὸ ἐδῶ καὶ πέρα χρησιμοποιῶ τοὺς προηγουμένους ἀλγορίθμους ἀφοῦ ὁ ὑπολογισμὸς τοῦ $(c_{2r-2}, \cdots, c_0)$

εἶναι ἡ συνέλιξη τῶν $(a_{r-1}, \cdots, a_0)$ καὶ $(b_{r-1}, \cdots, b_0)$.
Ὡστόσο ὁ ἀλγόριθμος θὰ ἦταν πιὸ ἀποτελεσματικός, ἐὰν μπορούσαμε νὰ μειώσουμε τὸν ἐκθέτη κατὰ ἕναν παράγοντα 2. Παρατηροῦμε ὅτι $x_r = 2^{rs} \equiv -1 \left(\mod 2^N + 1 \right)$ ἔτσι λοιπὸν πρὲπει νὰ δειχθῆ ὅτι

$$ab \equiv d(x) = \sum_{j=0}^{r-1} d_j x^j \left(\mod 2^N + 1 \right)$$

ὅπου

$$d_k = c_k - c_{k+r} = \sum^{k=j_1+j_2} a_{j_1} b_{j_2} - \sum^{k+r=j_1+j_2} a_{j_1} b_{j_2}$$

καὶ μὲ προσεκτικὴ ἀλλαγὴ τὼν δεικτῶν ἔχουμε

$$d_k = \sum_{h=0}^{k} a_h b_{k-h} - \sum_{h=k+1}^{r-1} a_h b_{r+k-h}$$

γιὰ $0 \le k \le r-1$.
Τὸ διάνυσμα $(d_{r-1}, \cdots, d_0)$ λέγεται ἀρνητικὴ κεκαλυμμένη συνέλιξη (ἀδόκιμος ὅρος τοῦ negative wrapped convolution) τῶν $(a_{r-1}, \cdots, a_0)$ καὶ $(b_{r-1}, \cdots, b_0)$.
Θὰ ὑπολογισθῆ ἡ ἀρνητικὴ κεκαλυμμένη συνέλιξη τῶν $(a_{r-1}, \cdots, a_0)$ καὶ $(b_{r-1}, \cdots, b_0)$ ὡς πρὸς modulo $2^t + 1$ ὅπου t θὰ εἶναι τὸ μοναδικὸ ἀκέραιο πολλαπλάσιο τοῦ r στὸ διάστημα

$$2s + \log r + 1 < t \le 2s + \log r + 1 + r$$

Τὸ d_k εἶναι τὸ ἄθροισμα ἢ ἡ διαφορὰ γινομένων ἀκεραίων μήκους s-bit καὶ εἶναι ἀρκετὰ μεγάλο γιὰ κατ΄ εὐθείαν ὑπολογισμὸ τῆς τιμῆς του modulo $2^t + 1$ γιὰ κάθε k μὲ $0 \le k < r$.
Τὸ t εἶναι τῆς μορφῆς $2^\sigma \beta$ μὲ $\beta \le 4 \log t + 2$ ἀφοῦ εἶναι ἀκέραιο πολλαπλάσιο τοῦ r.