Darboux egy problémájától a gyors Fourier-transzformációig

Matematika BSc szakdolgozat
Alkalmazott matematikus szakirány

Vályi András

Témavezető: Besenyei Ádám
ELTE TTK Alkalmazott Analízis és Számításmatematikai Tanszék

Budapest
2019

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Besenyei Ádámnak a szakirodalom összegyűjtéséért, a folyamatos konzultációért, és hogy hasznos tanácsaival és kritikáival segített dolgozatom elkészítésében.

Előszó

A dolgozat központi témája a diszkrét Fourier-transzformáció, amely egy széles körben (jelfeldolgozás, adattömörítés, stb.) alkalmazott eljárás.
Az első fejezetben az [5] cikket követve egy Darboux által felvetett problémát és két megoldását mutatjuk be, illetve a későbbi fejezetekben fontos szerepet betöltő komplex egységgyökök alapvető tulajdonságait ismertetjük.
A második fejezetben Darboux problémája által motiválva a klasszikus diszkrét Fourier-transzformációt tárgyaljuk, illetve vizsgáljuk a tulajdonságait.
A harmadik fejezetben a klasszikus diszkrét Fourier-transzformációt általánosítjuk véges Abel-csoportokra.
A negyedik fejezetben pedig a klasszikus diszkrét Fourier-transzformáció hatékony végrehajtására alkalmazott közismert gyors Fourier-transzformációt ismertetjük.
A dolgozat felépítésében az irodalomjegyzékben szereplő [1, 2, 4] művekre támaszkodtunk.

Tartalomjegyzék

1. fejezet

Darboux problémája és két megoldás

Darboux 1878-ban a következő problémát vetette fel. Legyen adott egy kiindulási sokszög a síkon, és végezzünk rajta oldalfelező-iterációt, azaz minden lépésben képezzük az oldalak felezőpontjai mint csúcsok által meghatározott sokszöget. A kérdés: hogyan viselkednek az iteráció során a kapott sokszögek? Darboux a problémát a komplex síkra átfordítva oldotta meg. Hamarosan mi is ismertetjük Darboux gondolatmenetét (az [5] cikkre támaszkodva) és egy másik lehetséges megoldást is. De előtte fogalmazzuk meg a problémát precízen.

1.1. A probléma megfogalmazása

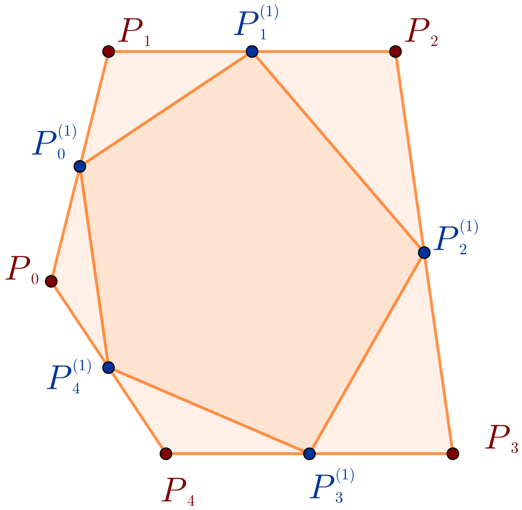
Adott a síkon a $P_0, P_1, \ldots, P_{N-1}$ pontok mint csúcsok által meghatározott Π sokszög (a csúcsokat ebben a sorrendben kötjük össze, és a továbbiakban mindig ezzel a megállapodással élünk). Jelölje $P_j^{(1)}$ a P_jP_{j+1} oldal felezőpontját $j = 0, 1, \ldots, N-2$ esetén, és legyen $P_{N-1}^{(1)}$ a $P_{N-1}P_0$ oldal felezőpontja (lásd az 1.1. ábrát). Jelölje $\Pi^{(1)}$ az így kapott $P_0^{(1)}, P_1^{(1)}, \ldots, P_{N-1}^{(1)}$ csúcsok alkotta sokszöget. Általában, ha már adott a $P_0^{(n)}, P_1^{(n)}, \ldots, P_{N-1}^{(n)}$ pontok által meghatározott $\Pi^{(n)}$ sokszög, akkor $j = 0, 1, \ldots, N-2$ esetén legyen $P_j^{(n+1)}$ a $P_j^{(n)}P_{j+1}^{(n)}$ oldal felezőpontja, és legyen $P_{N-1}^{(n+1)}$ a $P_{N-1}^{(n)}P_0^{(n)}$ oldal felezőpontja. Ismételve az eljárást kapjuk a $\Pi^{(2)}, \Pi^{(3)}, \ldots$ sokszögeket. Kérdés: rögzített $k = 0, 1, \ldots, N-1$ esetén konvergálnak-e a $P_k^{(n)}$ csúcsok, ha n végtelenbe tart, és ha igen, hova? Tegyünk egy kitérőt Darboux megoldásának ismertetése előtt: vizsgáljuk meg a komplex egységgyökök alapvető tulajdonságait.

1.2. A komplex egységgyökök néhány fontos tulajdonsága

Mint ismeretes, adott N pozitív egész szám esetén a $z^N = 1$ egyenlet

$$1, e^{\frac{2\pi i}{N}}, e^{\frac{2\pi i}{N}2}, \ldots, e^{\frac{2\pi i}{N}(N-1)}$$

megoldásait nevezzük komplex N-edik egységgyököknek. Vezessük be az $\omega_N := e^{\frac{2\pi i}{N}}$ jelölést. Ekkor az N-edik egységgyökök ω_N modulo N hatványai. A definícióból az egységgyökök kö-



1.1. ábra. Az oldalfelező-iteráció első lépése.

vetkező tulajdonságai nyilvánvalóak:

$$\omega_N^0 = \omega_N^N = \omega_N^{Nk} = 1 \quad \text{és} \quad \overline{\omega_N^k} = \omega_N^{N-k} \quad (k \in \mathbb{Z}).$$

Az N-edik egységgyököket csoportelméleti szempontból is tekinthetjük. Egyszerűen látható, hogy rögzített N esetén az ω_N^k $(k = 0, 1, \dots, N-1)$ számok csoportot alkotnak a komplex szorzás műveletére nézve. Az egységelem $\omega_N^0 = 1$, az invertálás művelete a komplex konjugálás. Valójában ez a csoport izomorf az egészek modulo N összeadás műveletére vett csoportjával, amelyet $(\mathbb{Z}_N, +)$ jelöl. Az izomorfiát az $\omega_N^k \mapsto k$ leképezés mutatja, amely könnyen beláthatóan műveletartó bijekció. Az N-edik egységgyökök a későbbiekben lényegesnek bizonyuló tulajdonságát fogalmazza meg a következő állítás.

1.1. Állítás (Az egységgyökök ortogonalitása)**.** Legyenek $0 \le k, l \le N-1$ egész számok, ekkor

$$\sum_{n=0}^{N-1} \omega_N^{nk} \overline{\omega_N^{nl}} = \begin{cases} N, & \text{ha } k = l, \\ 0 & \text{különben.} \end{cases} \tag{1.1}$$

Bizonyítás. Ha $k = l$, akkor

$$\sum_{n=0}^{N-1} \omega_N^{nk} \overline{\omega_N^{nl}} = \sum_{n=0}^{N-1} \omega_N^{nk} \omega_N^{-nl} = \sum_{n=0}^{N-1} |\omega_N|^{2kn} = N,$$

hiszen $|\omega_N| = 1$. Ha $k \ne l$, akkor

$$\omega_N^{kn} \overline{\omega_N^{ln}} = \omega_N^{(k-l)n},$$

ahol $-N < k - l < N$ és $k - l \ne 0$ folytán $\omega_N^{k-l} \ne 1$. Ekkor a $q = \omega_N^{k-l}$ jelöléssel

$$\sum_{n=0}^{N-1} \omega_N^{nk} \overline{\omega_N^{nl}} = \sum_{n=0}^{N-1} q^n = \frac{q^N - 1}{q - 1} = 0,$$

mivel $q^N = \omega_N^{N(k-l)} = 1$. $\square$

1.2. Megjegyzés. Az 1.1. Állítás valójában azt jelenti, hogy a $\mathbb{C}^N$-beli

$$\left(\omega_N^0, \omega_N^k, \ldots, \omega_N^{(N-1)k}\right), \quad \left(\omega_N^0, \omega_N^l, \ldots, \omega_N^{(N-1)l}\right)$$

vektorok merőlegesek a szokásos

$$\langle (u_0, u_1, \ldots, u_{N-1}), (v_0, v_1, \ldots, v_{N-1}) \rangle_{\mathbb{C}^N} = \sum_{k=0}^{N-1} u_k \overline{v_k}$$

skalárszorzatra nézve. Így máris világossá válik, hogy az 1.1. Állításban miért neveztük ortogonálisnak az egységgyököket. Célszerű az $(\omega_N^0, \omega_N^k, \omega_N^{2k}, \ldots, \omega_N^{(N-1)k})$ egységgyök hatványok alkotta vektorokat ($k = 0, 1, \ldots, N-1$) egy $(N-1) \times (N-1)$-es mátrix soraiba rendeznünk. Jelölje ezt a mátrixot Ω, azaz

$$\Omega = \begin{pmatrix} 1 & \omega_N^{1\cdot 0} & \omega_N^{2\cdot 0} & \ldots & \omega_N^{(N-1)\cdot 0} \\ 1 & \omega_N^{1\cdot 1} & \omega_N^{2\cdot 1} & \ldots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{1\cdot(N-1)} & \omega_N^{2\cdot(N-1)} & \ldots & \omega_N^{(N-1)\cdot(N-1)} \end{pmatrix}. \tag{1.2}$$

Ebből világosan látszik, hogy Ω szimmetrikus mátrix, mivel $\Omega_{k,l} = \omega_N^{kl} = \omega_N^{lk} = \Omega_{l,k}$, ahol $\Omega_{k,l}$ az Ω mátrix k-adik sorának l-edik elemét jelöli. Jelölje Ω^* az Ω mátrix adjungáltját, azaz konjugált transzponáltját. Vegyük észre, hogy

$$\Omega\Omega^* = NI_N, \tag{1.3}$$

ahol I_N az $N \times N$-es egységmátrix. Valóban, az Ω mátrix k-adik sora az $(1, \omega_N^k, \ldots, \omega_N^{(N-1)k})$ vektor, az Ω^* mátrix l-edik oszlopa pedig az $(1, \overline{\omega_N^l}, \ldots, \overline{\omega_N^{(N-1)l}})$ vektor, így az (1.1) összefüggés alapján kapjuk, hogy

$$(\Omega\Omega^*)_{k,l} = \begin{cases} N, & \text{ha } k = l, \\ 0, & \text{különben.} \end{cases}$$

1.3. Állítás. Az (1.2) egyenlőség által definiált Ω mátrixra az alábbi tulajdonságok teljesülnek:

$$\left|\mathrm{Det}(\Omega)\right|^2 = N^N \quad \text{és} \quad \Omega^{-1} = \frac{1}{N}\Omega^*.$$

Bizonyítás. Az (1.3) egyenlőség és a determinánsok szorzástétele alapján adódik, hogy:

$$N^N = \mathrm{Det}(NI_N) = \mathrm{Det}(\Omega\Omega^*) = \mathrm{Det}(\Omega)\overline{\mathrm{Det}(\Omega)} = \left|\mathrm{Det}(\Omega)\right|^2.$$

Az (1.3) azonosságból pedig az is következik, hogy

$$\Omega\frac{1}{N}\Omega^* = \frac{1}{N}NI_N = I_N,$$

tehát

$$\Omega^{-1} = \frac{1}{N}\Omega^*.$$

□

1.4. Megjegyzés. Vegyük észre, hogy Ω Vandermonde-típusú mátrix, azaz a következő alakú:

$$\Omega = \begin{pmatrix} 1 & x_0 & \dots & x_0^{N-1} \\ 1 & x_1 & \dots & x_1^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{N-1} & \dots & x_{N-1}^{N-1} \end{pmatrix},$$

ahol $x_k = \omega_N^k$. Ismert, hogy a Vandermonde-mátrix determinánsa

$$\prod_{0 \le k < l \le N-1} (x_l - x_k).$$

Mivel az x_k egységgyökök különbözőek, ezért a determináns nem 0, tehát Ω invertálható.

Ennyi előkészület után rátérhetünk Darboux problémájának első megoldására, mely magától Darboux-tól származik.

1.3. Darboux megoldása

Legyenek a $P_0^{(n)}, P_1^{(n)}, \dots, P_{N-1}^{(n)}$ pontoknak megfelelő komplex számok a komplex síkon:

$$z_0^{(n)}, z_1^{(n)}, \dots, z_{N-1}^{(n)}.$$

Ekkor tekintsük a következő lineáris egyenletrendszert:

$$\underline{z} = \Omega \underline{\zeta}, \tag{1.4}$$

ahol $\underline{z} = (z_0, z_1, \dots, z_{N-1})$ és $\underline{\zeta} = (\zeta_0, \zeta_1, \dots, \zeta_{N-1})$. Az (1.4) egyenletrendszer koordinátánként felírva a következő alakot ölti:

$$z_k = \sum_{n=0}^{N-1} \omega_N^{kn} \zeta_n. \tag{1.5}$$

Az 1.3. Állítás alapján Ω invertálható, $\Omega^{-1} = \frac{1}{N}\Omega^*$, ezért a fenti egyenletrendszernek létezik egyértelmű megoldása, mégpedig

$$\underline{\zeta} = \Omega^{-1}\underline{z} = \frac{1}{N}\Omega^*\underline{z} = \frac{1}{N}\overline{\Omega}\underline{z},$$

ahol utolsó lépésben azt használtuk ki, hogy $\Omega = \Omega^T$. Koordinátánkénti formában a következő eredményt kapjuk:

$$\zeta_k = \frac{1}{N}\sum_{n=0}^{N-1} z_n \overline{\omega_N}^{nk}.$$

Vegyük észre, hogy $k = 0$ esetén

$$\zeta_0 = \frac{z_0 + z_1 + \dots + z_{N-1}}{N}$$

adódik, ami azt jelenti, hogy ζ_0 a Π sokszög súlypontja. Következő lépésként adjuk meg Π oldalfelező pontjait:

$$z_0^{(1)} = \frac{z_0 + z_1}{2}, \quad z_1^{(1)} = \frac{z_1 + z_2}{2}, \quad \dots, \quad z_{N-1}^{(1)} = \frac{z_{N-1} + z_0}{2},$$

azaz

$$z_k^{(1)} = \frac{z_k + z_{k+1}}{2}, \tag{1.6}$$

az alsó indexeket modulo N értve. Általában $\Pi^{(n)}$ oldalfelező pontjai:

$$z_0^{(n+1)} = \frac{z_0^{(n)} + z_1^{(n)}}{2}, \quad \dots, \quad z_{N-1}^{(n+1)} = \frac{z_{N-1}^{(n)} + z_0^{(n)}}{2}.$$

Helyettesítsük most be a $\underline{z}$ vektornak az (1.5) összefüggésbeli előállítását a felezőpontok (1.6) képletéből adódó alakjába:

$$2z_k^{(1)} = z_k + z_{k+1} = \sum_{l=0}^{N-1} \zeta_l \omega_N^{kl} + \sum_{l=0}^{N-1} \zeta_l \omega_N^{(k+1)l}.$$

Mivel $\omega_N^{(k+1)l} = \omega_N^{kl}\omega_N^l$, ezért innen

$$z_k^{(1)} = \sum_{l=0}^{N-1} \zeta_l \omega_N^{kl} \frac{(\omega_N^l + 1)}{2}$$

adódik. Indukcióval könnyen belátható, hogy általában

$$z_k^{(n)} = \sum_{l=0}^{N-1} \zeta_l \omega_N^{kl} \left(\frac{\omega_N^l + 1}{2} \right)^n. \tag{1.7}$$

Vizsgáljuk meg most tüzetesebben $\left(\frac{\omega_N^l+1}{2}\right)^n$ viselkedését. A komplex háromszög-egyenlőtlenséget ω_N^l-re és 1-re felírva kapjuk, hogy

$$\left| \frac{(\omega_N^l + 1)}{2} \right| \le \frac{1+1}{2} = 1,$$

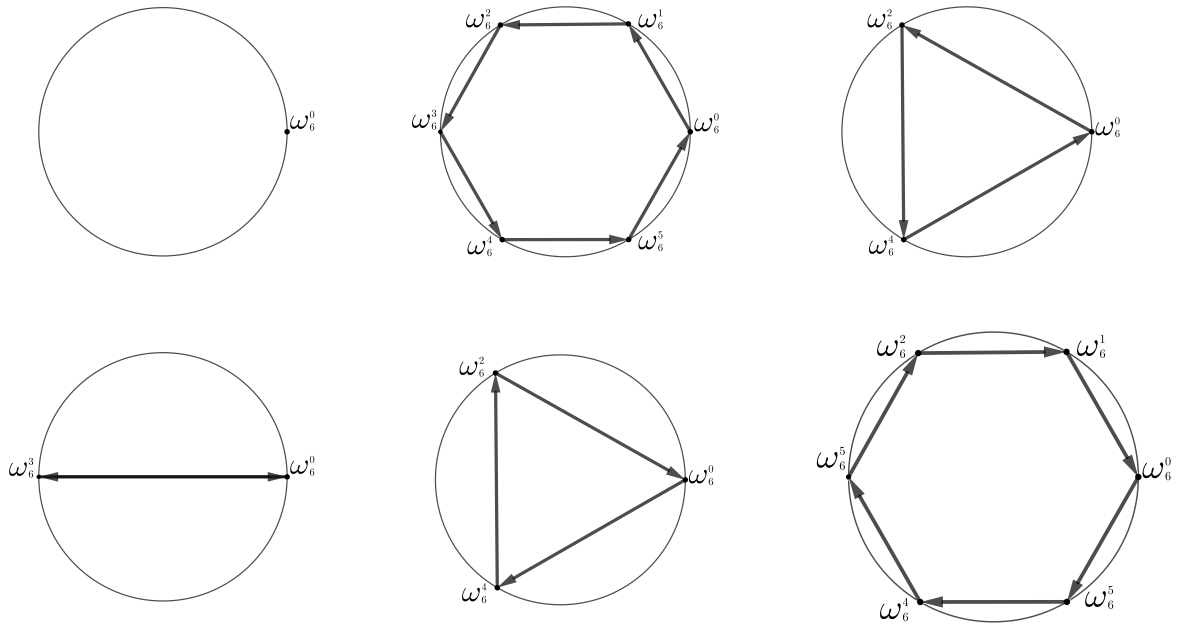
ahol egyenlőség pontosan akkor áll fenn, ha 1 és ω_N^l iránya azonos, vagyis $\omega_N^l = 1$, azaz $l = 0$. Következésképp $l \neq 0$ esetén

$$\lim_{n\to\infty} \left(\frac{\omega_N^l + 1}{2} \right)^n = 0,$$

így az (1.7) összegben az $l = 0$ indexhez tartozón kívül minden tag 0-hoz tart. Emiatt

$$\lim_{n\to\infty} z_k^{(n)} = \zeta_0 \cdot 1 \cdot 1 = \zeta_0,$$

ahol korábbi észrevételünk szerint ζ_0 a Π sokszög súlypontja. Megfogalmazhatjuk tehát a következő tételt:



1.2. ábra. Az egységgyökök hatványai alkotta sokszögek $N = 6$ esetén.

1.5. Tétel. Tetszőleges $\Pi = P_0 P_1 \dots P_{N-1}$ kiindulási sokszög esetén az oldalfelező-iteráció által adódott $\Pi^{(n)}$ sokszögek csúcsai alkotta $P_k^{(n)}$ csúcssorozatok rögzített $k = 0, 1, \dots, N-1$ mellett a kiindulási sokszög súlypontjához konvergálnak $n \to \infty$ esetén.

1.6. Megjegyzés. A bizonyítás során felhasznált

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ \vdots \\ z_{N-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N^1 & \omega_N^2 & \omega_N^3 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^{2\cdot 2} & \omega_N^{3\cdot 2} & \dots & \omega_2^{2\cdot(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2\cdot(N-1)} & \omega_N^{3\cdot(N-1)} & \dots & \omega_N^{(N-1)\cdot(N-1)} \end{pmatrix} \cdot \begin{pmatrix} \zeta_0 \\ \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_{N-1} \end{pmatrix}$$

egyenletrendszernek a következő geometriai jelentés tulajdonítható: a z_0 , $z_1, \dots, z_{N-1}$ pontok a kiindulási Π sokszög csúcsai, az Ω mátrix oszlopai pedig az N-edik egységgyökök hatványainak megfelelő pontok által meghatározott sokszöggel azonosíthatók (lásd 1.2. ábra). Azt mondhatjuk tehát, hogy a Π sokszöget az egységgyökök hatványainak megfelelő sokszögek bázisában állítottuk elő.

1.7. Megjegyzés. Az (1.4) egyenletrendszer felírható polinom alakban is. Valóban, legyen p a következő komplex együtthatós polinom:

$$p(x) = \zeta_0 + \zeta_1 x + \dots + \zeta_{N-1} x^{N-1}.$$

Ekkor a ζ_k együtthatókat ($k = 0, 1, \dots, N-1$) keressük oly módon, hogy a polinom ω_N^k helyen felvett helyettesítési értéke z_k legyen. Ismeretes, hogy a Lagrange-interpoláció alkalmazásával ez a p polinom egyértelműen meghatározható a z_k értékek ismeretében.

1.4. Egy alternatív bizonyítás

Az alábbiakban egy másik lehetséges okoskodást ismertetünk Darboux problémájának megoldására, továbbra is komplex számokat alkalmazva (ez a megoldás a [3] cikkben szerepel). Jelölje Π a kiindulási sokszöget, z_k a csúcsainak megfelelő komplex számokat ($k = 0, 1, \ldots, N-1$), valamint jelölje az iteráció n-edik lépése során kapott sokszöget $\Pi^{(n)}$, és legyenek a $\Pi^{(n)}$ csúcsainak megfelelő komplex számok $z_k^{(n)}$ ($k = 0, 1, \ldots, N-1$). Helyezzük el a Π sokszöget a komplex számsíkra úgy, hogy a csúcsok súlypontja a 0 pontba essen, ekkor

$$\frac{z_1 + z_2 + \cdots + z_{N-1}}{N} = 0. \tag{1.8}$$

Vegyük észre, hogy az iteráció során a súlypont nem változik, ugyanis a $\Pi^{(1)}$ sokszög súlypontja

$$\frac{1}{N}\left(\frac{z_0 + z_1}{2} + \frac{z_1 + z_2}{2} + \cdots + \frac{z_{N-1} + z_0}{2}\right) = \frac{z_1 + z_2 + \cdots + z_{N-1}}{N} = 0. \tag{1.9}$$

Vezessük be a

$$\rho := \max\{|z_k| : k = 0, 1, \ldots, N-1\}$$

konstanst. Ekkor $\Pi^{(N-1)}$ minden $z_k^{(N-1)}$ csúcsára (az indexeket mod N értve)

$$z_k^{(N-1)} = \frac{1}{2}\left(z_k^{(N-2)} + z_{k+1}^{(N-2)}\right) = \frac{1}{4}\left(z_k^{(N-3)} + 2z_{k+1}^{(N-3)} + z_{k+2}^{(N-3)}\right).$$

Ezt rekurzív módon folytatva kapjuk, hogy

$$z_k^{(N-1)} = \frac{c_0 z_0 + c_1 z_1 + \cdots + c_{N-1} z_{N-1}}{2^{N-1}},$$

ahol a c_j együtthatók alkalmas pozitív egészek, amelyekre

$$c_0 + c_1 + \cdots + c_{N-1} = 2^{N-1}.$$

Tehát az (1.8) összefüggés felhasználásával

$$\left|z_k^{(N-1)}\right| = \left|\frac{c_0 z_0 + c_1 z_1 + \cdots + c_{N-1} z_{N-1}}{2^{N-1}}\right| = \left|\frac{(c_0 - 1)z_0 + \cdots + (c_{N-1} - 1)z_{N-1}}{2^{N-1}}\right|.$$

Alkalmazzuk a komplex háromszög-egyenlőtlenséget az iménti összegben szereplő tagokra:

$$\left|\frac{(c_0 - 1)z_0 + \cdots + (c_{N-1} - 1)z_{N-1}}{2^{N-1}}\right| \leq \sum_{k=0}^{N-1}\left|\frac{(c_k - 1)z_k}{2^{N-1}}\right|.$$

Mivel $|z_k| \leq \rho$ és $|c_k - 1| = c_k - 1$, ezért

$$\sum_{k=0}^{N-1}\left|\frac{(c_k - 1)z_k}{2^{N-1}}\right| \leq \frac{1}{2^{N-1}}\rho\sum_{k=0}^{N-1}(c_k - 1) = 2^{-(N-1)}(2^{N-1} - N)\rho = K\rho,$$

ahol $K = 2^{-(N-1)}(2^{N-1} - N)$. Teljes indukcióval egyszerűen belátható, hogy $N \geq 3$ esetén $2^{N-1} > N$, így $K < 1$. Azt kapjuk tehát, hogy

$$\left| z_k^{(N-1)} \right| \leq K\rho,$$

vagyis a $\Pi^{(N-1)}$ sokszög minden csúcsa benne van a $\overline{B(0, K\rho)}$ zárt körlapban. Az (1.9) összefüggés szerint az iteráció során kapott sokszögek súlypontja mindvégig az origó, így természetesen $\Pi^{(N-1)}$ súlypontja is az. Ekkor a $\Pi^{(N-1)}$ sokszögre is $(N-1)$-szer alkalmazva az iterációt adódik, hogy a $\Pi^{2(N-1)}$ sokszög benne van a $\overline{B(0, K^2\rho)}$ zárt körlapban, illetve tetszőleges m pozitív egész esetén a $\Pi^{m(N-1)}$ sokszög benne van a $\overline{B(0, K^m\rho)}$ zárt körlapban. Másrészt vegyük észre, hogy ha egy $n \in \mathbb{N}$ számra a $\Pi^{(n)}$ sokszöget tartalmazza egy rögzített $\overline{B(0, r)}$ zárt körlap, akkor a $\Pi^{(n+1)}$ sokszöget is tartalmazza, mert a zárt körlap konvex. Ezért, ha az iteráció során kapott sokszögek egy részsorozata tart 0-hoz (azaz a csúcsok konvergálnak 0-hoz), akkor a sokszögek sorozata maga is konvergál 0-hoz. Tartsunk m-el a végtelenhez, ekkor $\lim_{m\to\infty} K^m\rho = 0$, így az iménti okoskodás alapján kapjuk, hogy $\lim_{n\to\infty} z_k^{(n)} = 0$ $(k = 0, 1, \ldots, N-1)$. $\square$

2. fejezet

A diszkrét Fourier-transzformáció (DFT)

Ebben a fejezetben arra adunk választ, hogy milyen általánosabb matematikai elmélet húzódik meg Darboux módszere mögött. A kulcsfogalom a diszkrét Fourier-transzformáció lesz.

2.1. A diszkrét Fourier-transzformáció fogalma

Legyen N pozitív egész szám és jelölje $(\mathbb{Z}_N, +)$ az egészek modulo N összeadásra vett csoportját (a továbbiakban csak $\mathbb{Z}_N$). Vegyük észre, hogy egy $\underline{z} = (z_0, z_1, \ldots, z_{N-1})$ komplex vektor tekinthető úgy is, mint egy $f\colon \mathbb{Z}_N \to \mathbb{C}$, $f(k) = z_k$ függvény.

2.1. Definíció. Legyen $L^2(\mathbb{Z}_N)$ a $\mathbb{Z}_N \to \mathbb{C}$ függvények $\mathbb{C}$ feletti vektortere a szokásos

$$\langle f, g \rangle_{L^2(\mathbb{Z}_N)} = \sum_{n=0}^{N-1} f(n)\overline{g(n)}$$

skalárszorzattal ellátva. A skalárszorzat a következő normát indukálja:

$$\|f\|_{L^2(\mathbb{Z}_N)} = \sqrt{\langle f, f \rangle_{L^2(\mathbb{Z}_N)}} = \sqrt{\sum_{n=0}^{N-1} \left|f(n)\right|^2}.$$

A fejezet további részeiben skalárszorzat, illetve norma alatt mindig ezeket fogjuk érteni.

2.2. Megjegyzés. Vegyük észre, hogy az $L^2(\mathbb{Z}_N)$ térben bázist alkotnak a

$$\delta_n(k) = \begin{cases} 1, & \text{ha } k = n, \\ 0 & \text{különben} \end{cases}$$

függvények ($n = 0, 1, \ldots, N-1$). Valóban, minden $f \in L^2(\mathbb{Z}_N), f(k) = z_k$ hozzárendelési szabályú függvény ($k = 0, 1, \ldots, N-1$) egyértelműen előáll $f = \sum_{k=0}^{N-1} z_k \delta_k$ alakban, következésképp $L^2(\mathbb{Z}_N)$ dimenziója N.

A (δ_n) bázis helyett vizsgáljunk meg egy számunkra fontosabb függvénycsaládot az $L^2(\mathbb{Z}_N)$ térben. Tekintsük a következő függvényeket:

$$e_n(k) = \exp\left(\frac{2\pi ikn}{N}\right) \quad (n = 0, 1, \ldots, N-1).$$

2.3. Állítás. Az (e_n) függvények bázist alkotnak $L^2(\mathbb{Z}_N)$-ben.

Bizonyítás. Vegyük észre, hogy az 1.1. Állítás éppen azt jelenti, hogy $k, l = 0, 1, \ldots, N-1$ esetén

$$\langle e_k, e_l\rangle = \sum_{n=0}^{N-1} e_k(n)\overline{e_l(n)} = \begin{cases} N, & \text{ha } k = l, \\ 0 & \text{különben.} \end{cases} \tag{2.1}$$

Eszerint (e_n) ortogonális rendszer, tehát lineárisan független, és mivel N elemű, így szükségképpen bázist alkot az N dimenziós térben. Ezek után készen állunk a diszkrét Fourier-transzformáció bevezetésére. □

2.4. Definíció. Adott $f \in L^2(\mathbb{Z}_N)$ függvény *diszkrét Fourier-transzformáltja* azon $\hat{f} \in L^2(\mathbb{Z}_N)$ függvény, amelyre minden $k \in \mathbb{Z}_N$ esetén

$$\hat{f}(k) = \langle f, e_k\rangle = \sum_{n=0}^{N-1} f(n)\overline{e_k(n)} = \sum_{n=0}^{N-1} f(n)e^{\frac{-2\pi ikn}{N}}.$$

2.5. Megjegyzés. Az előbbi definíció alapján világos, hogy a diszkrét Fourier-transzformáció egy lineáris $L^2(\mathbb{Z}_n) \to L^2(\mathbb{Z}_N)$ leképezés. Ha egy $f \in L^2(\mathbb{Z}_N)$ függvényre mint oszlopvektorra tekintünk, akkor a leképezés mátrixa éppen $\overline{\Omega}$, azaz

$$\hat{f} = \overline{\Omega}f.$$

Mivel az (e_n) rendszer bázis, ezért tetszőleges $f \in L^2(\mathbb{Z}_N)$ egyértelműen felírható benne alkalmas c_n komplex együtthatókkal vett lineáris kombinációként:

$$f = \sum_{n=0}^{N-1} c_n e_n.$$

Használjuk ki, hogy (e_n) ortogonális rendszer, így mindkét oldalt az e_k bázisfüggvénnyel skalárisan szorozva a (2.1) összefüggés alapján

$$\langle f, e_k\rangle = \left\langle \sum_{n=0}^{N-1} c_n e_n, e_k \right\rangle = c_k\langle e_k, e_k\rangle = c_k N.$$

Tehát

$$f = \frac{1}{N}\sum_{n=0}^{N-1}\langle f, e_n\rangle e_n = \frac{1}{N}\sum_{n=0}^{N-1}\hat{f}(n)e_n. \tag{2.2}$$

2.6. Definíció. Legyen$f \in L^2(\mathbb{Z}_N)$. Ekkor az f függvénynek a (2.2) képlet szerinti előállítását f *diszkrét Fourier-sorfejtésének* nevezzük.

2.7. Megjegyzés. Vegyük észre, hogy Darboux megoldásában az (1.5) összefüggés éppen diszkrét Fourier-sorfejtést jelent.

2.2. A diszkrét Fourier-transzformáció inverze

Az 1.4. Megjegyzésben láttuk, hogy Ω invertálható és $\Omega^{-1} = \frac{1}{N}\Omega^*$, ebből adódik, hogy a diszkrét Fourier-transzformáció mátrixának inverze:

$$\overline{\Omega}^{-1} = \frac{1}{N}\overline{\Omega}^* = \frac{1}{N}\Omega^T = \frac{1}{N}\Omega.$$

Az inverz transzformáció tehát mátrix alakban felírva a következőképpen néz ki:

$$\frac{1}{N}\begin{pmatrix} 1 & \omega_N^{1\cdot 0} & \omega_N^{2\cdot 0} & \dots & \omega_N^{(N-1)\cdot 0} \\ 1 & \omega_N^{1\cdot 1} & \omega_N^{2\cdot 1} & \dots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \omega_N^{1\cdot (N-1)} & \omega_N^{2\cdot (N-1)} & \dots & \omega_N^{(N-1)\cdot (N-1)} \end{pmatrix} \cdot \begin{bmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \vdots \\ \hat{f}(N-1) \end{bmatrix} = \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix}.$$

Ennek alaján felírhatjuk az inverz diszkrét Fourier-transzformáció pontonkénti képletet is:

$$f(k) = \frac{1}{N}\sum_{n=0}^{N-1} \hat{f}(n)\omega_N^{kn} = \frac{1}{N}\sum_{n=0}^{N-1} \hat{f}(n)e^{2\pi ikn}.$$

2.3. A diszkrét Fourier-transzformáció azonosságai

A következőkben a diszkrét Fourier-transzformáció néhány fontos tulajdonságát igazoljuk. Az első összefüggés kapcsolatot teremt a kiindulási függvény normanégyzete és a transzformáltjának normanégyzete között.

2.8. Tétel (Parseval-azonosság)**.** Legyen $f \in L^2(\mathbb{Z}_N)$ függvény,

$$f = \sum_{n=0}^{N-1} c_n e_n$$

ekkor teljesül a következő azonosság:

$$\sum_{n=0}^{N-1} \left|f(n)\right|^2 = N\sum_{n=0}^{N-1} |c_n|^2 = \frac{1}{N}\sum_{n=0}^{N-1} \left|\hat{f}(n)\right|^2.$$

Bizonyítás. A skalárszorzat definíciója szerint

$$\sum_{n=0}^{N-1} \left|f(n)\right|^2 = \sum_{n=0}^{N-1} f(n)\overline{f(n)} = \|f\|^2 = \langle f, f\rangle.$$

Most az f függvény diszkrét Fourier-sorfejtését használva:

$$\langle f, f\rangle = \left\langle \frac{1}{N}\sum_{n=0}^{N-1} \hat{f}(n)e_n, \frac{1}{N}\sum_{n=0}^{N-1} \hat{f}(n)e_n \right\rangle = \frac{1}{N^2}\sum_{n=0}^{N-1} \left|\hat{f}(n)\right|^2 \langle e_n, e_n\rangle = \frac{1}{N}\sum_{n=0}^{N-1} \left|\hat{f}(n)\right|^2.$$

Tehát

$$\sum_{n=0}^{N-1} \left|f(n)\right|^2 = N \sum_{n=0}^{N-1} |c_n|^2 = \frac{1}{N} \sum_{n=0}^{N-1} \left|\hat{f}(n)\right|^2.$$

□

A 2.8. Tételt általánosíthatjuk a normanégyzetről skalárszorzatra:

2.9. Tétel (Plancherel tétele)**.** Legyenek $f_k \in L^2(\mathbb{Z}_N)$ $(k = 1, 2)$ függvények, ekkor:

$$\langle f_1, f_2 \rangle = \frac{1}{N} \langle \hat{f}_1, \hat{f}_2 \rangle.$$

Bizonyítás. Írjuk fel az f_1, f_2 függvényeket diszkrét Fourier-sor alakban:

$$f_1 = \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}_1(n) e_n, \quad f_2 = \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}_2(n) e_n.$$

Ezen előállítás segítségével a (2.1) összefüggésre támaszkodva könnyen számolható a skalárszorzat:

$$\langle f_1, f_2 \rangle = \left\langle \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}_1(n) e_n, \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}_2(n) e_n \right\rangle = \frac{1}{N^2} N \sum_{n=0}^{N-1} \hat{f}_1(n) \hat{f}_2(n) = \frac{1}{N} \langle f_1, f_2 \rangle.$$

□

A diszkrét Fourier-transzformáció kapcsán fontos szerephez jut egy speciális függvényművelet, a konvolúció.

2.10. Definíció. Legyenek $f, g \in L^2(\mathbb{Z}_N)$ függvények. Ezen függvények *konvolúciója* azon $f * g \in L^2(\mathbb{Z}_N)$ függvény, amelyre

$$(f * g)(k) = \sum_{n=0}^{N-1} f(n) g(k - n) \quad (k = 0, 1, \ldots, N - 1).$$

A következő tételben megadjuk a konvolúció diszkrét Fourier-transzformáltját.

2.11. Tétel. Legyenek $f, g \in L^2(\mathbb{Z}_N)$ függvények. Ekkor teljesül a következő azonosság:

$$\widehat{f * g} = \hat{f} \cdot \hat{g},$$

ahol $f \cdot g$ a pontonkénti (koordinátánkénti) szorzás művelete, azaz $(f \cdot g)(k) = f(k)g(k)$.

Bizonyítás. Induljunk ki a konvolúció definíciójából:

$$(f * g)(k) = \sum_{n=0}^{N-1} f(n) g(k - n).$$

Következő lépésben írjuk fel az f és g függvényeket diszkrét Fourier-sor alakban:

$$\sum_{n=0}^{N-1} f(n)g(k-n) = \sum_{n=0}^{N-1}\left[\frac{1}{N}\left(\sum_{m=0}^{N-1}\hat{f}(m)\omega_N^{mn}\right)\frac{1}{N}\left(\sum_{l=0}^{N-1}\hat{g}(l)\omega_N^{l(k-n)}\right)\right].$$

Gyűjtsük egy tagba ω_N azonos kitevőjű hatványait:

$$\sum_{n=0}^{N-1}\left[\frac{1}{N}\left(\sum_{m=0}^{N-1}\hat{f}(n)\omega_N^{mn}\right)\frac{1}{N}\left(\sum_{l=0}^{N-1}\hat{g}(l)\omega_N^{l(k-n)}\right)\right] =$$
$$= \frac{1}{N}\sum_{m=0}^{N-1}\hat{f}(m)\sum_{l=0}^{N-1}\hat{g}(l)\frac{1}{N}\sum_{n=0}^{N-1}\left(\omega_N^{mn}\omega_N^{l(k-n)}\right).$$

Vegyük észre, hogy

$$\sum_{n=0}^{N-1}\left(\omega_N^{mn}\omega_N^{l(k-n)}\right) = \omega_N^{lk}\sum_{n=0}^{N-1}\omega_N^{n(m-l)} = \begin{cases} N\omega_N^{km}, & \text{ha } l=m,\\ 0 & \text{különben.}\end{cases}$$

Így kapjuk, hogy

$$\sum_{n=0}^{N-1} f(n)g(k-n) = \frac{1}{N}\sum_{m=0}^{N-1}\hat{f}(m)\hat{g}(m)\omega_N^{km} = \frac{1}{N}\sum_{m=0}^{N-1}(\hat{f}\cdot\hat{g})(m)\omega_N^{km}.$$

Vegyük észre, hogy a jobb oldalon egy diszkrét Fourier-sorfejtés áll, mégpedig az $\hat{f}\cdot\hat{g}$ függvényé. Ebből adódik, hogy a konvolúció diszkrét Fourier-transzformáltja:

$$\widehat{(f*g)}(k) = \hat{f}(k)\hat{g}(k) = (\hat{f}\cdot\hat{g})(k).$$

□

2.4. Példák

Vizsgáljuk meg most néhány egyszerű példán keresztül, hogy miként is működik a diszkrét Fourier-transzformáció

2.12. Példa. Legyen $N=2$, ekkor az egységgyökök 1 és -1, így a bázisfüggvényeink a következők:

$$e_0(k) = e^{\frac{2\pi i 0k}{N}} = 1 \quad (k=0,1),$$
$$e_1(k) = e^{\frac{2\pi i 1k}{N}} = \begin{cases} 1, & \text{ha } k=0,\\ -1, & \text{ha } k=1.\end{cases}$$

Válasszuk transzformálandó függvénynek az $f \in L^2(\mathbb{Z}_N)$, $f(0) = 0$, $f(1) = 1$ függvényt. A definícióból adódik, hogy

$$\hat{f}(0) = f(0) + f(1) = 0, \quad \hat{f}(1) = f(0) - f(1) = 2.$$

Ennek megfelelően a diszkrét Fourier-sorfejtés:

$$f = \frac{1}{2}\left(\hat{f}(0)e_0 + \hat{f}(1)e_1\right) = e_1.$$

Ebből nyerjük, hogy $f(k) = e^{ki\pi}$, ezáltal az f függvénynek az egész számokra vett periodikus kiterjesztését nyerjük.

2.13. Példa. Legyen most $N = 4$, ekkor a negyedik egységgyökök: 1, i ,-1 , $-i$. Válasszuk példánknak az $f = (1, 1, -1, 1)$ függvényt. A diszkrét Fourier-transzformáció kiszámításához használjuk a kényelmes mátrix alakot:

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \quad \overline{\Omega} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & \text{-1} & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

Tehát $\hat{f} = \overline{\Omega} f = (2, 2, -2, 2)$. Ennek megfelelően a diszkrét Fourier-sorfejtés:

$$f = \frac{1}{4}\left(2e_0 + 2e_1 - 2e_2 + 2e_3\right) = \frac{1}{2}\left(e_0 + e_1 - e_2 + e_3\right).$$

Következésképp

$$f(k) = \frac{1}{2}\left(1 + i^k - (-1)^k + (-i)^k\right) = \frac{1}{2}\left(1 - (-1)^k\right) + \cos\frac{k\pi}{2},$$

és ezzel ismét a szóban forgó f függvény periodikus kiterjesztését nyertük az egész számokra.

2.14. Példa. Legyen most N tetszőleges pozitív egész és válasszuk transzformálandó függvénynek a 2.2. Megjegyzésben bevezetett δ_n függvényt ($n = 0, 1, , \ldots, N - 1$). Ez esetben

$$\hat{\delta_n} = \overline{\Omega}\delta_n = \left(\omega_N^{-0\cdot n}, \omega_N^{-1\cdot n}, \ldots, \omega_N^{-(N-1)n}\right) = \overline{e_n},$$

tehát a transzformált éppen az $\overline{\Omega}$ mátrix n-edik oszlopa. Eszerint a diszkrét Fourier-sorfejtés:

$$\delta_n = \frac{1}{N}\sum_{k=0}^{N-1} \omega_N^{-kn} e_k.$$

2.5. Gauss problémája

Az alábbi szakaszban a következő, Gauss által vizsgált problémát tárgyaljuk. Egy kisbolygó pályájáról 12 mérési eredmény állt rendelkezésre (Θ, X) alakban, ahol Θ a hosszúság (fokban mérve), X a szélesség (ívpercben mérve), és feltehető, hogy X függ Θ-tól, azaz $X = f(\Theta)$:

Θ	0	30	60	90	120	150	180	210	240	270	300	330
X	408	89	-66	10	338	807	1238	1511	1583	1462	1183	804

Az adatokból arra lehet következtetni, hogy X periodikusan függ Θ-tól, így célszerű X-et Θ trigonometrikus polinomjaként felírni. Gauss a következő összeggel dolgozott:

$$X = f(\Theta) = a_0 + \sum_{k=1}^{5} \left[a_k \cos\left(\frac{2\pi k\Theta}{360}\right) + b_k \sin\left(\frac{2\pi k\Theta}{360}\right)\right] + a_6 \cos\left(\frac{2\pi 6\Theta}{360}\right). \qquad (2.3)$$

A feladat eszerint az $a_k, b_k \in \mathbb{R}$ ($k = 0, 1, \ldots, 6$) együtthatók meghatározása. Ehhez legyen $N = 12$, $\Theta = k \cdot 30$ ($k = 0, 1, \ldots, 11$). Vegyük észre, hogy

$$a_n \cos\left(\frac{2\pi kn}{N}\right) = \frac{1}{2} a_n \left(e^{\frac{2\pi ikn}{N}} + e^{\frac{-2\pi ikn}{N}}\right) \quad \text{és} \quad b_n \sin\left(\frac{2\pi kn}{N}\right) = \frac{1}{2i} b_n \left(e^{\frac{2\pi ikn}{N}} - e^{\frac{-2\pi ikn}{N}}\right)$$

folytán

$$a_n \cos\left(\frac{2\pi kn}{N}\right) + b_n \sin\left(\frac{2\pi kn}{N}\right) = \frac{a_n - ib_n}{2} e^{\frac{2\pi ikn}{N}} + \frac{a_n + ib_n}{2} e^{\frac{-2\pi ikn}{N}}.$$

Eszerint

$$f(k) = a_0 + \sum_{n=1}^{\frac{N}{2}} \left[\frac{a_n - ib_n}{2} e^{\frac{2\pi ikn}{N}} + \frac{a_n + ib_n}{2} e^{\frac{-2\pi ikn}{N}}\right]. \qquad (2.4)$$

Vezessük be az $A_n = \frac{a_n - ib_n}{2}$ jelölést, ekkor $\overline{A_n} = \frac{a_n + ib_n}{2}$, és így a (2.5) összeg a következő alakban írható:

$$f(k) = a_0 + \sum_{n=1}^{\frac{N}{2}} \left[A_n \omega_N^{kn} + \overline{A_n}\,\overline{\omega_N}^{kn}\right].$$

Ha $\overline{A_n} = A_{N-n}$ teljesülne, akkor ez éppen f diszkrét Fourier-sorfejtése lenne, és a diszkrét Fourier-transzformációval meghatározhatók lennének az együtthatók. Mivel f valós értékű, ezért ez valóban teljesülni fog. Fogalmazzuk meg ezt állításként.

2.15. Állítás. Legyen $f \in L^2(\mathbb{Z}_N)$ valós értékű függvény. Ekkor $\hat{f}(0)$ valós és $\hat{f}(N-k) = \overline{\hat{f}(k)}$ ($k = 0, 1, \ldots, N-1$) esetén.

Bizonyítás. Világos, hogy

$$\hat{f}(0) = \sum_{n=0}^{N-1} f(n) \cdot 1$$

valós, ugyanis feltételünk szerint $f(n) \in \mathbb{R}$. Vizsgáljuk meg állításunk második részét. Definíció szerint

$$\hat{f}(N-k) = \sum_{n=0}^{N-1} f(n)\overline{\omega_N}^{(N-k)n} = \sum_{n=0}^{N-1} f(n)(\overline{\omega_N})^{-kn} = \sum_{n=0}^{N-1} f(n)\omega_N^{kn}.$$

Mivel $f(n)$ valós, így szintén definíció szerint

$$\overline{\hat{f}(k)} = \overline{\sum_{n=0}^{N-1} f(n)\overline{\omega_N^{kn}}} = \sum_{n=0}^{N-1} \overline{f(n)}\omega_N^{kn} = \sum_{n=0}^{N-1} f(n)\omega_N^{kn}.$$

□

Ennek alapján beszélhetünk valós értékű $f \in L^2(\mathbb{Z}_N)$ függvény valós Fourier-soráról:

$$Nf = \hat{f}(0) + (\hat{f}(1)e_1 + \hat{f}(N-1)e_{N-1}) + (\hat{f}(2)e_2 + \hat{f}(N-2)e_{N-2}) + \dots,$$

ahol az utolsó tag N paritásától függően vagy $\hat{f}(\frac{N}{2})$, vagy $\hat{f}(\frac{N-1}{2})e_{\frac{N-1}{2}} + \hat{f}(\frac{N+1}{2})e_{\frac{N+1}{2}}$. Mivel

$$\begin{aligned} &\hat{f}(n)e_n(k) + \overline{\hat{f}(n)}e_{N-n}(k) = 2\mathrm{Re}(\hat{f}(n)e_n(k)) = \\ &= \left(\hat{f}(n) + \overline{\hat{f}(n)}\right)\cos\left(\frac{2\pi ink}{N}\right) + \left(\hat{f}(n) - \overline{\hat{f}(n)}\right)\sin\left(\frac{2\pi ink}{N}\right), \end{aligned}$$

ezért

$$\begin{aligned} &Nf(k) = \hat{f}(0) + \\ &+ \left(\hat{f}(1) + \overline{\hat{f}(1)}\right)\cos\left(\frac{2\pi ik}{N}\right) + \left(\hat{f}(1) - \overline{\hat{f}(1)}\right)\sin\left(\frac{2\pi ik}{N}\right) + \\ &+ \left(\hat{f}(2) + \overline{\hat{f}(2)}\right)\cos\left(\frac{2\pi i2k}{N}\right) + \left(\hat{f}(2) - \overline{\hat{f}(2)}\right)\sin\left(\frac{2\pi i2k}{N}\right) + \dots. \end{aligned}$$

Eszerint Gauss problémájában a (2.3) felírásban szereplő a_k, b_k együtthatók tényleg meghatározhatók diszkrét Fourier-transzformációval, mégpedig:

k	0	1	2	3	4	5	6
a_k	780.6	-411.0	43.4	-4.3	-1.1	0.3	0.1
b_k		-720.2	-2.2	5.5	-1.0	-0.3	

3. fejezet

Diszkrét Fourier-transzformáció véges Abel-csoporton

Ebben a fejezetben a [2, 4] jegyzetekre támaszkodva $\mathbb{Z}_N$-ről általános véges Abel-csoportra általánosítjuk a diszkrét Fourier-transzformációt. A következőkben legyen tehát $(G, +)$ egy N-rendű Abel-csoport, ahol N tetszőleges pozitív egész. A szokásos módon $|G|$ jelöli a G csoport rendjét, azaz elemszámát.

3.1. Abel-csoport karakterei

A klasszikus diszkrét Fourier-transzformációnál a kulcsszerepet az N-edik egységgyökök játszották, ezt most az úgynevezett karakterek fogják betölteni.

3.1. Definíció. A G csoport egy χ *karaktere* egy $\chi\colon G \to \mathbb{C}^\times$ homomorfizmus, azaz művelettartó leképezés:

$$\chi(a+b) = \chi(a) \cdot \chi(b) \quad (a, b \in G),$$

ahol $\mathbb{C}^\times$ jelöli $\mathbb{C} \setminus \{0\}$ multiplikatív csoportját.

Nyilvánvaló, hogy

$$(\chi(a))^N = \chi(a + a + \cdots + a) = \chi(Na) = \chi(0) = 1 \quad (a \in G),$$

tehát χ értékei éppen az N-edik egységgyökök. Szintén világos, hogy

$$\chi(-a) = \chi(a)^{-1} = \overline{\chi(a)} \quad (a \in G).$$

Nevezzük triviális karakternek azt a χ karaktert, amelyre minden $a \in G$ esetén $\chi(a) = 1$, a továbbiakban erre az 1_G jelölést használjuk. Az alábbiakban a karakterek fontos tulajdonságait fogalmazzuk meg és látjuk be.

3.2. Állítás. Minden $\chi \neq 1_G$ karakterre

$$\sum_{a \in G} \chi(a) = 0.$$

Bizonyítás. Legyen $b \in G$ olyan, hogy $\chi(b) \neq 1$. Ilyen b létezik, mert $\chi \neq 1_G$. Ha S jelöli a bal oldali összeget, akkor

$$S \cdot \chi(b) = \sum_{a \in G} \chi(a)\chi(b) = \sum_{a \in G} \chi(a+b) = S,$$

tehát $S(\chi(b) - 1) = 0$, azaz szükségképpen $S = 0$. □

3.3. Állítás. Legyenek χ és ψ karakterek G fölött. Ekkor érvényes a következő összefüggés:

$$\sum_{a \in G} \chi(a) \cdot \overline{\psi(a)} = \begin{cases} N, & \text{ha } \chi = \psi, \\ 0 & \text{különben.} \end{cases}$$

Bizonyítás. A $\chi = \psi$ eset következik abból, hogy

$$\overline{\chi(a)} = \frac{1}{\chi(a)},$$

mivel $\chi(a)$ komplex egységgyök. Ha $\chi \neq \psi$, akkor $\chi\overline{\psi}$ nem triviális karakter, tehát a bizonyítandó összefüggés a 3.2. Állításból következik. □

Most nézzünk néhány konkrét példát karakterekre.

3.4. Példa. Legyen $(\langle\gamma\rangle, \cdot)$ egy negyedrendű ciklikus csoport, ahol $\langle\gamma\rangle$ jelöli a γ által generált ciklikus részcsoportot. Ekkor $\gamma^4 = 1$, tehát $(\chi(\gamma))^4 = 1$, így χ helyettesítési értékei a 4-edik egységgyökök. Írjuk fel a karakterek táblázatát:

	γ	γ^2	γ^3	γ^4
1_G	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	i	-1	$-i$
χ_3	1	$-i$	-1	i

Jelölje $\mathbb{Z}_N^*$ az N-hez relatív prím pozitív egészek csoportját a modulo N szorzás műveletére nézve. Ennek a csoportnak a rendje $\phi(N)$, ahol ϕ az Euler-féle ϕ-függvény, ami egy n pozitív egész számhoz az n-nél kisebb, n-hez relatív prím pozitív egész számok számát rendeli. Nézzünk meg néhány ilyen csoportot.

3.5. Példa. $N = 4$ esetén $\mathbb{Z}_4^* = \{1, 3\}$, ez a csoport izomorf a $(\mathbb{Z}_2, +)$ csoporttal, az izomorfiát az

$$1 \to 0, \quad 3 \to 1$$

leképezés mutatja. $N = 5$ esetén $\mathbb{Z}_4^* = \{1, 2, 3, 4\}$, ez a csoport izomorf a $(\mathbb{Z}_4, +)$ csoporttal. Az izomorfiát az

$$1 \to 0, \quad 2 \to 1, \quad 3 \to 3, \quad 4 \to 2$$

leképezés mutatja. $N = 8$ esetén $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, ez a csoport izomorf a $\mathbb{Z}_2 \times \mathbb{Z}_2$ csoporttal. Az izomorfiát most az

$$1 \to (0,0), \quad 3 \to (1,0), \quad 5 \to (0,1), \quad 7 \to (1,1)$$

leképezés mutatja. Vizsgáljuk meg most $\mathbb{Z}_4^*$ karaktereit:

$$\chi_1(1) = 0, \quad \chi_1(3) = 1, \quad \chi_2(1) = 1, \quad \chi_2(3) = -1.$$

Ezek kiterjeszthetők $\mathbb{Z}$-re olyan módon, hogy

$$\chi(m) = \begin{cases} 0, & \text{ha } m \text{ páros}, \\ \chi(1), & \text{ha } m = 4k+1, \\ \chi(3), & \text{ha } m = 4k+3. \end{cases}$$

3.6. Definíció. Ha χ, ψ karakterek, akkor legyen $\chi \cdot \phi$ azon karakter, amelyre

$$\chi \cdot \psi(a) = \chi(a)\psi(a) \quad (a \in G).$$

Legyen $\hat{G}$ a karakterek halmaza G felett. Könnyen látható, hogy az iménti pontonkénti szorzás műveletére nézve $(\hat{G}, \cdot)$ csoportot alkot, ezt nevezzük G *duális csoportjának.*

3.2. A duális csoport

A most következő szakaszban be fogjuk látni, hogy $G \cong \tilde{G}$, azaz egy véges Abel-csoport izomorf a duális csoportjával. Ennek bizonyításához több állításon keresztül vezet az út, most ezeket ismeretjük.

3.7. Állítás. Legyen G véges rendű Abel-csoport és legyen $H \subset G$ valódi részcsoport. Ekkor H bármely karaktere pontosan $|G{:}H|$ különféle módon terjeszthető ki G karakterévé.

Bizonyítás. Teljes indukciót végzünk $G{:}H$ rendje szerint. Legyen $a \in G$, $a \notin H$, tehát $H \subset \subset \langle H, a \rangle \subset G$, ahol $\langle\,\rangle$ jelenti a generált részcsoportot. Legyen χ a H részcsoport egy karaktere. Valamilyen m pozitív egész számra $a + a + \cdots + a = ma \in H$, legyen k a legkisebb ilyen szám, azaz

$$k = \min\{m > 0 \mid ma \in H\}.$$

Ekkor k éppen a rendje a G/H faktorcsoportban, tehát $k = \big|\langle H, a \rangle{:}H\big|$. Ha $\tilde{\chi}$ kiterjesztése χ-nek, akkor a művelettartás miatt:

$$(\tilde{\chi}(a))^k = \tilde{\chi}(ka) = \chi(ka), \tag{3.1}$$

azaz $\chi(a)$ szükségképpen az egyik k-adik gyöke $\chi(ka)$-nak, ebből pontosan k darab van. Illetve, ha már a $\chi(a)$ értéket tudjuk, akkor $h \in H$ és $l \in \mathbb{Z}$ esetén a művelettartás miatt szükségszerűen teljesülnie kell az alábbi összefüggésnek:

$$\tilde{\chi}(h + la) = \chi(h)\tilde{\chi}(a)^l.$$

Még meg kell mutatnunk, hogy ez a kiterjesztés jóldefiniált. Ehhez tekintsük egy $\langle H, a \rangle$ részcsoportbeli elem két különböző előállítását: $h + la = h' + l'a$. Ekkor $a(l - l') \in H$, azaz $l - l' | k$. Eszerint $l' = l + kq$ alakban írható, ahol $q \in \mathbb{Z}$, ekkor

$$h = h' + (l' - l)a = h' + kqa.$$

Az $l' = l + kq$ előállítás miatt

$$\chi(h')\tilde{\chi}(a)^{l'} = \chi(h')\tilde{\chi}(a)^{l}\tilde{\chi}(a)^{kq}.$$

Mivel $\chi(ka) = (\tilde{\chi}(a))^k$, így

$$\chi(h')\tilde{\chi}(a)^{l}\tilde{\chi}(a)^{kq} = \chi(h')\tilde{\chi}(a)^{l}\chi(ka)^{q} = \chi(h' + kqa)\tilde{\chi}(a)^{l} = \chi(h)\tilde{\chi}(a)^{l}.$$

Beláttuk tehát, hogy $\tilde{\chi}(h' + l'a) = \tilde{\chi}(h + la)$, így $\tilde{\chi}$ jóldefiniált, könnyen láthatóan homomorfizmus, és a H részcsoportra való megszorítása éppen χ, így valóban kiterjesztés. Innen az indukciós lépéssel következik az állításunk, hiszen

$$\left|G{:}\langle H, a\rangle\right| < |G{:}H|.$$

□

A 3.7. Állítást az $\langle 1\rangle \subset G$ triviális részcsoportra alkalmazva az alábbi fontos következmény adódik:

3.8. Következmény. Egy véges Abel-csoportnak és duális csoportjának megegyezik az elemszáma, azaz $\left|\hat{G}\right| = |G|$.

3.9. Állítás. Legyen $g \in G$, $g \neq 0$. Ekkor van olyan $\chi \in \hat{G}$ karakter, amire $\chi(g) \neq 1$.

Bizonyítás. Legyen a g által generált $\langle g\rangle$ ciklikus csoport elemszáma n. Mivel $g \neq 0$, ezért $n > 1$. Ekkor $\langle g\rangle$ izomorf az n-edik komplex egységgyökök S^1 ciklikus csoportjával, és ez az izomorfizmus megfelel $\langle g\rangle$ egy karakterének. A 3.7. Állítás szerint ez a karakter kiterjeszthető a G csoportra, és ebben a kiterjesztésben g képe nem az 1. □

3.10. Állítás. Ha G véges Abel-csoport és $g_1 \neq g_2 \in G$, akkor van olyan $\chi \in \hat{G}$ karakter, amelyre $\chi(g_1) \neq \chi(g_2)$.

Bizonyítás. Alkalmazzuk a 3.9. Állítást a $g = g_1 - g_2$ elemre. □

3.11. Állítás. Legyen ω egy primitív N-edik egységgyök. Ekkor minden $j \in \mathbb{Z}$ esetén a

$$\chi_j\colon \mathbb{Z}_N \to \mathbb{C}^{\times}, \quad \chi_j(a) = \omega^{aj}$$

leképezés karakter. Továbbá érvényesek a következő tulajdonságok:

(a) $\chi_j = \chi_k$ pontosan akkor, ha $j \equiv k \pmod N$

(b) $\chi_j = \chi_1^j$

(c) $\hat{\mathbb{Z}}_N = \{\chi_0, \chi_1, \ldots, \chi_{N-1}\}$, azaz $\mathbb{Z}_N$ duális csoportja éppen az (e_n) függvényosztály.

(d) $\hat{\mathbb{Z}}_N \cong \mathbb{Z}_N$, azaz $\mathbb{Z}_N$ izomorf a duális csoportjával.

Bizonyítás. (a) és (b) következik χ_j definíciójából. Legyen χ tetszőleges karakter G felett, ekkor $\chi(1) = \omega^j$ valamilyen j-re, hiszen χ helyettesítési értékei N-edik egységgyökök, tehát $\chi = \chi_j$. Ez a bijekció meg is adja a (d) izomorfiát. □

3.12. Állítás. Legyen $G = H_1 \bigoplus H_2$ direkt összeg, ϕ_1 a H_1 csoport karaktere, ϕ_2 a H_2 csoport karaktere. Értelmezzük a $\phi_1 \bigoplus \phi_2 : H_1 \bigoplus H_2 \to \mathbb{C}^\times$ lelépezést a következő módon:

$$(\phi_1 \bigoplus \phi_2)(h_1, h_2) = \phi_1(h_1) \cdot \phi_2(h_2).$$

Ekkor a $\phi_1 \bigoplus \phi_2$ leképezés karakter G-ben. Sőt, G összes karaktere előáll ilyen alakban, következésképpen $\hat{G} \cong \hat{H}_1 \bigoplus \hat{H}_2$.

Bizonyítás. Az egyszerűség kedvéért vezessük be a $\chi := \phi_1 \bigoplus \phi_2$ jelölést. Az, hogy χ karakter, nyilvánvaló, mivel

$$\chi(h_{11} + h_{12}, h_{21} + h_{22}) = \phi_1(h_{11} + h_{12})\phi_2(h_{21} + h_{22}) =$$
$$= \phi_1(h_{11})\phi_1(h_{12})\phi_2(h_{21})\phi_2(h_{22}) = \chi(h_{11}, h_{21})\chi(h_{12}, h_{22}).$$

Most lássuk be, hogy a χ karaktert definiáló $\hat{H}_1 \bigoplus \hat{H}_2 \to \hat{G}$ leképezés injektív, amihez elég azt látni, hogy a magja triviális. Valóban, legyen $\phi_1 \bigoplus \phi_2$ triviális karakter. Ez azt jelenti, hogy minden $h_1 \in H_1, h_2 \in H_2$ esetén

$$(\phi_1 \bigoplus \phi_2)(h_1, h_2) = \phi_1(h_1)\phi_2(h_2) = 1.$$

Rögzítsük le h_1-et úgy, hogy $\phi_1(h_1) = 1$ legyen. Ekkor ϕ_2 szükségképpen triviális karakter. Hasonlóan, h_2 lerögzítésével hasonlóan látható, hogy ϕ_1 is szükségképpen triviális karakter. Mivel $|G| = |H_1||H_2|$ és $\left|\hat{H}_1 \bigoplus \hat{H}_2\right| = \left|\hat{H}_1\right|\left|\hat{H}_2\right|$, továbbá a 3.8. Következmény alapján $\left|\hat{G}\right| = |G|$, $\left|\hat{H}_1\right| = |H_1|$, $\left|\hat{H}_2\right| = |H_2|$, ezért $|\hat{G}| = |\hat{H}_1 \bigoplus \hat{H}_2|$, így G minden karaktere előáll ilyen alakban. □

Most már minden készen áll, hogy belássuk a célul kitűzött tételt.

3.13. Tétel. A G csoport izomorf a duális csoportjával: $G \cong \hat{G}$.

Bizonyítás. Ismert, hogy véges rendű Abel-csoport felbontható prímhatvány rendű ciklikus csoportok direkt összegére, azaz

$$G \cong \mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2} \bigoplus \cdots \bigoplus \mathbb{Z}_{n_k}.$$

Ekkor a 3.11. és a 3.12. Állításokból kapjuk, hogy

$$\hat{G} \cong \hat{\mathbb{Z}}_{n_1} \bigoplus \hat{\mathbb{Z}}_{n_2} \bigoplus \cdots \bigoplus \hat{\mathbb{Z}}_{n_k} \cong \mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2} \bigoplus \cdots \bigoplus \mathbb{Z}_{n_k} \cong G.$$

□

3.14. Tétel. Egy G véges Abel-csoport izomorf a második duális csoportjával, azaz $G \cong \hat{\hat{G}}$, sőt, $a \in G$ esetén legyen $\tilde{a} \in \hat{\hat{G}}$ az az elem, amelyre $\tilde{a}(\chi) = \chi(a)$, ekkor az $a \mapsto \tilde{a}$ leképezés természetes izomorfizmus G és $\hat{\hat{G}}$ között (teljesül az úgynevezett *Pontrjagin-dualitás*).

Bizonyítás. Az, hogy $G \cong \tilde{\tilde{G}}$, nyilvánvaló az izomorfia tranzitivitása miatt. Mivel egy csoportnak és a duális csoportjának az elemszáma megegyezik, elég megmutatnunk, hogy a leképezés injektív. Legyen $g \in G$ ezen leképezés magjában, ekkor minden $\chi \in \hat{G}$ karakterre $\chi(g) = 1$, tehát a 3.9 Állítás alapján $g = 0$, állításunkat beláttuk. $\square$

Tekintsük a G-ből $\mathbb{C}$-be képző függvények N dimenziós vektorterét, amelyet $\mathbb{C}^G$ jelöl. Vezessük be ezen a következő skalárszorzatot:

$$\langle f, g \rangle_{\mathbb{C}^G} = \frac{1}{N} \sum_{a \in G} f(a)\overline{g(a)}.$$

3.15. Állítás. A $\hat{G}$ csoport elemei ortonormált bázist alkotnak a $\mathbb{C}^G$ vektortérben.

Bizonyítás. Az ortonormalitás következik a 3.3. Állításból. Az ortogonalitásból következik a lineáris függetlenség, és mivel $|\hat{G}| = |G| = N$, ezért a $\hat{G}$ csoport egy N elemű lineárisan független rendszer az N dimenziós térben, tehát szükségképpen bázist alkot. $\square$

3.16. Definíció. Legyen $G = \{a_0, a_1, \ldots, a_{N-1}\}$, és legyen $\hat{G} = \{\chi_0, \chi_1, \ldots, \chi_{N-1}\}$. Az alábbi $N \times N$-es C mátrixot G *karaktertáblájának* nevezzük:

$$C = \begin{pmatrix} \chi_0(a_0) & \chi_0(a_1) & \chi_0(a_2) & \ldots & \chi_0(a_{N-1}) \\ \chi_1(a_0) & \chi_1(a_1) & \chi_1(a_2) & \ldots & \chi_1(a_{N-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \chi_{N-1}(a_0) & \chi_{N-1}(a_1) & \chi_{N-1}(a_2) & \ldots & \chi_{N-1}(a_{N-1}) \end{pmatrix},$$

azaz $C_{ij} = (\chi_i(a_j))$.

A 3.3. Állításból kapjuk az alábbi állítást.

3.17. Állítás. A C mátrixra a következő azonosság teljesül:

$$A \cdot A^\star = A^* \cdot A = I_N.$$

3.18. Megjegyzés. Alkalmazzuk az ortogonalitást $\hat{\hat{G}}$-ra:

$$\sum_{\chi \in \hat{G}} \chi(a)\overline{\chi(b)} = \begin{cases} N, & \text{ha } a = b, \\ 0 & \text{különben.} \end{cases}$$

A $b = 0$, $a \neq 0$ speciális esetben eszerint

$$\sum_{\chi \in \hat{G}} \chi(a) = 0,$$

ami a 3.2. Állítás duálisa.

3.3. Fourier-transzformáció véges Abel-csoporton

A most következő szakaszban a klasszikus diszkrét Fourier-transzformációt általánosítjuk véges Abel-csoportra. A 3.15. Állításban láttuk, hogy a $\chi \in \hat{G}$ karakterek ortonormált bázist alkotnak a $\mathbb{C}^G$ térben, tehát minden $f \in \mathbb{C}^G$ függvény egyértelműen előáll a következő alakban:

$$f = \sum_{\chi \in \hat{G}} c_\chi \chi.$$

Ezt az előállítást az f függvény *Fourier-sorának* nevezzük, ahol a c_χ együtthatók az ortonormáltság miatt a következő alakúak:

$$c_\chi = \langle f, \chi \rangle_{\mathbb{C}^G}.$$

3.19. Definíció. Az $f \in \mathbb{C}^G$ függvény *Fourier-transzformáltjának* nevezzük azon $\hat{f} \in \mathbb{C}^{\hat{G}}$ függvényt, amelyre

$$\hat{f}(\chi) = \sum_{a \in G} f(a)\overline{\chi(a)} \quad (\chi \in \hat{G}).$$

A klasszikus diszkrét Fourier-transzformációhoz hasonlóan ez is invertálható:

$$f = \sum_{\chi \in \hat{G}} c_\chi \chi = \sum_{\chi \in \hat{G}} \frac{1}{N} \hat{f}(\chi)\chi,$$

tehát

$$f(a) = \frac{1}{N} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(a).$$

Definiáljunk skalárszorzatot $\mathbb{C}^{\hat{G}}$ felett is a következő módon:

$$\langle f, g \rangle_{\mathbb{C}^{\hat{G}}} = \frac{1}{N} \sum_{\chi \in \hat{G}} f(\chi)\overline{g(\chi)}.$$

Legyen $\delta \in \mathbb{C}^G$ a következő függvény:

$$\delta(a) = \begin{cases} 1, & \text{ha } a = 0, \\ 0 & \text{különben.} \end{cases}$$

Ekkor

$$\hat{\delta}(\chi) = \sum_{a \in G} \delta(a)\overline{\chi(a)} = \overline{\chi(0)} = 1,$$

így nyerjük δ Fourier-sorfejtését:

$$\delta = \frac{1}{N} \sum_{\chi \in \hat{G}} \chi.$$

Most nézzük meg, hogy a klasszikus diszkrét Fourier-transzformációra vonatkozó Plancherel-tétel igaz-e a G csoport feletti transzformációra:

3.20. Tétel (Plancherel-tétel Abel-csoportra)**.** Minden $f, g \in \mathbb{C}^G$ függvényre

$$\langle f, g\rangle_{\mathbb{C}^G} = \frac{1}{N}\langle \hat{f}, \hat{g}\rangle_{\mathbb{C}^{\hat{G}}}.$$

Bizonyítás. A Fourier-traszformáció lineáris, így ha az azonosságot egy adott bázisra belátjuk, készen vagyunk. Legyen ez a következő (δ_a) bázis ($a \in G$):

$$\delta_a(b) = \delta(b - a) \quad (b \in G).$$

Világos, hogy a (δ_a) rendszer bázist alkot, mivel egy adott $f \in \mathbb{C}^G$, $f(a) = c_a$ függvény egyértelműen előáll

$$f = \sum_{a\in G} c_a\delta_a$$

alakban. Ekkor

$$\hat{\delta_a}(\chi) = \sum_{b\in G} \delta_a(b)\overline{\chi(b)} = \overline{\chi(a)},$$

tehát az ortogonalitás miatt

$$\langle \hat{\delta_a}, \hat{\delta_b}\rangle = \frac{1}{N}\sum_{\chi\in\hat{G}} \overline{\chi(a)}\chi(b) = \begin{cases} 1, & \text{ha } a = b, \\ 0 & \text{különben.} \end{cases}$$

Ezt összevetve azzal, hogy

$$\langle \delta_a, \delta_b\rangle = \begin{cases} \frac{1}{N}, & \text{ha } a = b, \\ 0 & \text{különben,} \end{cases}$$

adódik az állításunk. $\square$

4. fejezet

A gyors Fourier-transzformáció (FFT)

A most következő fejezetben megvizsgáljuk, hogy milyen módszerrel lehet minél kevesebb művelettel végrehajtani a diszkrét Fourier-transzformációt.

4.1. A diszkrét Fourier-transzformáció számításigénye

Emlékeztetőként, egy $f \in L^2(\mathbb{Z}_N)$ függvény diszkrét Fourier-transzformáltja az alábbi függvény:

$$\hat{f}(k) = \sum_{n=0}^{N-1} f(n) e^{\frac{-2\pi ikn}{N}} \quad (k \in \mathbb{Z}_N).$$

Egy $\hat{f}(k)$ érték kiszámításához egy adott k esetén az egységgyökök ismeretében N darab komplex szorzásra és $N-1$ darab komplex összeadásra van szükség, tehát a teljes transzformált kiszámításához $N(N-1)$ komplex összeadás és N^2 komplex szorzás kell. Vizsgáljuk most meg, hogy a komplex műveletek végrehajtásához hány valós műveletre van szükség. Legyenek az $x_1,\ x_2 \in \mathbb{C}$ számok a következő alakúak: $x_1 = a_1 + b_1 i, \quad x_2 = a_2 + b_2 i$. Összegképzésnél a valós és a képzetes részek adódnak össze:

$$x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\, i.$$

A komplex összeadás tehát elvégezhető két valós összeadás segítségével. A szorzás kicsivel bonyolultabb:

$$x_1 x_2 = (a_1 + b_1 i)\,(a_2 + b_2 i) = a_1 a_2 - b_1 b_2 + (a_1 b_2 + a_2 b_1)\, i.$$

A komplex szorzás tehát 4 valós szorzás és 2 valós összeadás segítségével végezhető el. Összegezve: A diszkrét Fourier-transzformáció teljes kiszámításához nyers módszerrel $4N^2$ valós szorzásra és $2N(N-1) + 2N^2$ valós összegadásra van szükség. Numerikus számítások során a szorzás elvégzése jóval költségesebb, mint az összadásé, így most próbáljunk meg a számítási módszerünkön finomítani. Vegyük fel a következő segédváltozókat:

$$\begin{aligned}U &= a_1(a_2 - b_2),\\ V &= b_2(a_1 - b_1),\\ W &= b_1(a_1 + b_1).\end{aligned}$$

Írjuk fel most a komplex szorzást a segédváltozók segítségével:

$$x_1x_2 = (a_1 + b_1 i)\,(a_2 + b_2 i) = a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)\, i = (U + V) + (W - U)\, i.$$

A segédváltozók kiszámításához összesen 3 valós összeadást és 3 valós szorzást végeztünk el, a szorzás végrehajtásához pedig 2 valós összeadást, így egy komplex szorzás műveletigénye 3 valós szorzásra és 5 valós összeadásra változott.

4.2. Az FFT levezetése

Az alábbi szakaszban egy hatékonyabb számítási eljárást ismertetünk. Induljunk ki a diszkrét Fourier-transzformáció képletéből, és az egyszerűség kedvéért tegyük fel, hogy $N = 2^r$ alkalmas r természetes számra. Bontsuk fel a diszkrét Fourier-transzformáció képletében szereplő összeget páros és páratlan indexek szerint:

$$\hat{f}(k) = \sum_{n=0}^{N-1} f(n)e^{\frac{-2\pi ikn}{N}} = \sum_{l=0}^{\frac{N}{2}-1} f(2l)\cdot \overline{\omega_N}^{2lk} + \sum_{l=0}^{\frac{N}{2}-1} f(2l+1)\cdot \overline{\omega_N}^{(2l+1)k}. \tag{4.1}$$

Vezessük be a következő $L^2\left(\mathbb{Z}_{\frac{N}{2}}\right)$-beli függvényeket:

$$f^{(0)} = \big(f(0), f(2), f(4), \ldots, f(N-2)\big)\,, \quad f^{(1)} = \big(f(1), f(3), f(5), \ldots, f(N-1)\big)\,.$$

Vegyük észre, hogy

$$\overline{\omega_N}^{2lk} = \overline{\omega_{\frac{N}{2}}}^{lk} \quad \text{és} \quad \overline{\omega_N}^{(2l+1)k} = \overline{\omega_{\frac{N}{2}}}^{lk}\cdot \overline{\omega_N}^{k}.$$

Ekkor az előbbi jelölésekkel a (4.1) összeg így alakul:

$$\hat{f}(k) = \widehat{f^{(0)}}(k) + \overline{\omega}_N^k \cdot \widehat{f^{(1)}}(k) \tag{4.2}$$

minden $k = 0, 1, 2, \ldots, N-1$ esetén. Sőt, mivel

$$\overline{\omega_N}^{\frac{N}{2}+k} = \overline{\omega_N}^{\frac{N}{2}}\cdot \overline{\omega_N}^{k} = -\overline{\omega_N}^{k}\,,$$

ezért

$$\begin{cases} \widehat{f}(k) = \widehat{f^{(0)}}(k) + \overline{\omega_N}^k \widehat{f^{(1)}}(k), & k = 0, 1, \ldots, \dfrac{N}{2} - 1\\ \widehat{f}\left(\dfrac{N}{2} + k\right) = \widehat{f^{(0)}}(k) - \overline{\omega_N}^k \widehat{f^{(1)}}(k), & k = 0, 1, \ldots, \dfrac{N}{2} - 1. \end{cases}$$

Tehát az eredeti problémát felbontottuk két feleakkora méretű problémára, ezt nyilván iterálhatjuk, amíg 2 méretű problémához nem jutunk (az algoritmuselméletből jól ismert „oszd meg és uralkodj” módszer példája). Ez az úgynevezett gyors Fourier-transzformáció (angolul: Fast Fourier Transform (FFT)).

4.1. Állítás. Az FFT algoritmusban $N = 2^r$ esetén az elvégzendő szorzások száma $M(N) = \mathcal{O}(Nr)$

Bizonyítás. Teljes indukcióval fogjuk belátni r szerint. Tegyük fel, hogy $r = 1$, $N = 2$. Ekkor a szorzások száma $M(N) = M(2) = 1 \leq 1 \cdot 2 = Nr$. Indukciós lépésként tegyük fel, hogy $M(N) \leq N \cdot r$. Ekkor a (4.2) összefüggés alapján:

$$M(2^{r+1}) = M(2N) = 2M(N) + 2N.$$

Az indukciós feltevés szerint:

$$2M(N) + 2N \leq 2N \cdot r + 2N = 2N(r + 1).$$

Tehát az indukciós lépést beláttuk, így a teljes indukció elve alapján készen vagyunk. □

4.2. Megjegyzés. Összevetve a korábbi módszerrel, nagyságrendi javulást értünk el, $\Theta(N^2)$ helyett $\mathcal{O}(N \cdot \log(N))$ szorzást kell elvégezni.

Irodalomjegyzék

[1] Brad G. Osgood, Lectures on the Fourier Transform and Its Applications, American Mathematical Society, 2019, 251–292.

[2] László Babai, Characters of finite Abelian groups
https ://people.cs.uchicago.edu/~laci/reu02/fourier.pdf

[3] M. Rosenman, R. E. Huston, Solution of Problem 3547, The American Mathematical Monthly, Vol. 40, No. 3 (Mar., 1933), 184–185.

[4] Keith Conrad, The Fourier Transform and Equations over Finite Abelian Groups, https ://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf

[5] I. J. Schoenberg, The Finite Fourier Series and Elementary Geometry, The American Mathematical Monthly, Vol. 57, No. 6 (Jun. – Jul., 1950), pp. 390–404.