Gyors eljárások a diszkrét Fourier-transzformáció számítására II. rész

DR. KOCSIS FERENC
Budapesti Műszaki Egyetem
Híradástechnikai Elektronika Intézet

ÖSSZEFOGLALÁS

A címben megjelölt témával foglalkozó cikksorozatunk jelen, második része elsőként az egydimenziós DFT többdimenzióssá való átalakításának lehetőségeit vizsgálja. Ezt követi a DFT és a periodikus konvolúció kapcsolatának vizsgálata. Végül gyors eljárást adunk a konvolúció számítására.

DR. KOCSIS FERENC

1975-ben szerzett villamosmérnöki diplomát a BME Villamosmérnöki Karán, majd a Távközlési Kutató Intézetben kezdett dolgozni. Egyetemi doktori értekezését 1978-ban védte meg. 1983 szeptembere óta a BME HEI-ben dolgozik tudományos ösztöndíjasként, ahol a digitális jelfeldolgozás és jelszintézis algoritmikus kérdéseivel foglalkozik. Szakmai érdeklődési köre: rendszertechnika, digitális jelfeldolgozás, számítástechnika, algoritmusok elmélete.

1. Az egydimenziós DFT átalakítása többdimenziós transzformációvá

A dolgozat e folyóirat korábbi számában megjelent első részében a fokozatos részekre bontás eredményének értelmezésénél kiderült, hogy az egydimenziós DFT többdimenziós transzformációvá és egységnyi abszolút értékű komplex számokkal való szorzásokká, úgynevezett forgatásokká alakítható át. A második rész egyrészt a tisztán többdimenziós transzformációvá való alakítás feltételeit vizsgálja, másrészt a DFT számítását ekvivalens módon olyan feladattá próbálja transzformálni, amely megoldására ismert hatékony algoritmus. Az irodalomjegyzéket az 1. rész tartalmazza, a hivatkozások számozása annak megfelelő.

1.1. Az átalakítás feltételei

Tekintsük először az $1-D$ és a $2-D$ DFT közötti kapcsolatot. Induljunk ki ismét az $N=N_1 \cdot P$ felbontásból. Mivel minden egész c-re $e^{-j\left(\frac{2\pi}{N}\right)cN}\equiv 1$, ezért a definíciós egyenletben (1. rész 1-1. összefüggés) szereplő i és k indexek felbontásánál kiindulhatunk a következő alakból ([8]):

$$\begin{aligned} &i=I_1 i_1+I_2 i_2 \bmod N && (I_1 \text{ és } I_2 \text{ egész állandók})\\ &&& 0\le i_1\le N_1-1\\ &&& 0\le i_2\le P-1\\ &k=K_1 k_1+K_2 k_2 \bmod N && (K_1 \text{ és } K_2 \text{ egész állandó})\\ &&& 0\le k_1\le N_1-1\\ &&& 0\le k_2\le P-1 \end{aligned} \tag{1-1}$$

Természetesen sok másféle, a fentiektől eltérő felbontás is elképzelhető (akár nemlineáris is), azonban a gyakorlat szempontjából ezen lineáris kombinációk a legjelentősebbek. Az I_1, I_2, K_1 és K_2 állandókra az első feltétel, hogy az $i\to(i_1, i_2)$ és a $k\to(k_1, k_2)$ leképzések kölcsönösen egyértelműek legyenek. A definíciós összefüggésbe helyettesítve:

$$X(K_1k_1+K_2k_2)=X(k_1,\ k_2)= \tag{1-2}$$
$$=\sum_{i_1=0}^{N_1-1}\sum_{i_2=0}^{P-1} x(I_1i_1+I_2i_2)e^{-j\left(\frac{2\pi}{N}\right)(K_1k_1+K_2k_2)(I_1i_1+I_2i_2)}$$

Beérkezett: 1984. X. 30. (↔)

(1-2) $2-D$ DFT, ha felbontható egy i_2 szerinti belső és egy i_1 szerinti külső összegre. Ez akkor teljesül, ha

$$e^{-j\left(\frac{2\pi}{N}\right)(K_1I_2k_1i_2+K_2I_1k_2i_1)}\equiv 1 \to K_1I_2k_1i_2+ \tag{1-3}$$
$$+K_2I_1i_1k_2\equiv 0 \bmod N.$$

Mivel i_1, i_2, k_1 és k_2 változók, az összefüggés akkor áll, ha

$$\begin{aligned} K_1I_2&\equiv 0 \bmod N,\\ K_2I_1&\equiv 0 \bmod N. \end{aligned} \tag{1-4}$$

Egy lehetséges megoldás:

$$\begin{aligned} K_1&=a_1P & I_1&=b_1P,\\ K_2&=a_2N_1 & I_2&=b_2N_1. \end{aligned} \tag{1-5}$$

P és N értékére nézve eddig semmilyen más feltevést nem tettünk, csupán hogy egészek és $N=N_1\cdot P$. Legyen N_1 és P legnagyobb közös osztója λ, azaz $(N_1, P)=\lambda$:

$$\begin{aligned} K_1&=\lambda a_1p & I_1&=\lambda b_1p\\ K_2&=\lambda a_2n & I_2&=\lambda b_2p \end{aligned} \qquad (n,\ p)=1 \tag{1-6}$$

(1-1)-be helyettesítve és figyelembe véve, hogy $N=\lambda^2np$:

$$\begin{aligned} i&\equiv\lambda(b_1pi_1+b_2ni_2) \bmod \lambda^2np,\\ k&\equiv\lambda(a_1pk_1+a_2nk_2) \bmod \lambda^2np. \end{aligned} \tag{1-7}$$

Mivel i és k a $(0,\ N-1)$ közé eső változók, ezért az (1-2) kongruenciák csak $\lambda=1$ esetben teljesülhetnek, azaz a fenti megoldástípus létezésének szükséges feltétele, hogy N_1 és P relatív prímek legyenek $((N_1,\ P)=1)$.

Hogy (1-2) valóban $N_1\times P$ méretű $2-D$ DFT legyen, annak másik feltétele, hogy a megmaradó expo-

nenciális tagok $e^{-j\left(\frac{2\pi}{N_1}\right)k_1 i_1}$, ill. $e^{-j\left(\frac{2\pi}{P}\right)k_2 i_2}$ alakúak legyenek. Másképpen:

$$\begin{aligned} K_1 I_1 i_1 k_1 &\equiv i_1 k_1 P \bmod N \\ K_2 I_2 i_2 k_2 &\equiv i_2 k_2 N_1 \bmod N. \end{aligned} \tag{1-8}$$

Az összefüggéseknek az i_1, i_2, k_1 és k_2 változók minden értékére teljesülniük kell. A kongruenciákra érvényes alapvető azonosságokat alkalmazva:

$$\begin{aligned} K_1 I_1 &\equiv P \bmod N_1 \qquad K_2 I_2 \equiv 0 \bmod N_1 \\ K_1 I_1 &\equiv 0 \bmod P \qquad K_2 I_2 \equiv N_1 \bmod P. \end{aligned} \tag{1-9}$$

(1-5) helyettesítése után adódik:

$$\begin{aligned} a_1 b_1 P &\equiv 1 \bmod N_1, \\ a_2 b_2 N_1 &\equiv 1 \bmod P. \end{aligned} \tag{1-10}$$

$a_1=1$ és $a_2=1$ választással (2 egyenlet 4 ismeretlennel):

$$\begin{aligned} k_1 P &\equiv 1 \bmod N_1, \\ b_2 N_1 &\equiv 1 \bmod P. \end{aligned} \tag{1-11}$$

Mivel $(N_1, P)=1$, alkalmazható Euler tétele (1. FÜGGELÉK):

$$\begin{aligned} b_1 &= P^{\varphi(N_1)-1} \\ b_2 &= N_1^{\varphi(P)-1}. \end{aligned} \tag{1-12}$$

$\varphi(N)$ az Euler-féle φ függvény, amely az N értéknél kisebb, ahhoz relatív prímek számát adja meg (1. FÜGGELÉK).

A részeredményeket összefoglalva: ha N felbontásának a két tagja egymáshoz relatív prím, akkor az eredeti $1-D$ DFT valódi $2-D$ DFT-be alakítható át. A szükséges indexelést meghatározó összefüggések:

$$\begin{aligned} i &\equiv i_1 P^{\varphi(N_1)} + i_2 N_1^{\varphi(P)} \bmod N \qquad & 0 \le i_1 \le N_1 - 1 \\ & & 0 \le i_2 \le P-1 \\ k &\equiv k_1 P + k_2 N_1 \bmod N \qquad & 0 \le k_1 \le N_1 - 1 \\ & & 0 \le k_2 \le P-1 \end{aligned} \tag{1-13}$$

Mivel $(P, N_1)=1$, teljesülnek a kínai maradéktétel ([17]) feltételei, így az (1-1) és az (1-3) összefüggések valóban kölcsönösen egyértelmű leképezést jelentenek $i \to (i_1, i_2)$ és $k \to (k_1, k_2)$ között. A fokozatos részekre bontás azután tovább folytatható, amíg csak P egymáshoz relatív prímek szorzatára bontható, vagyis az N-pontos $1-D$ DFT számítása valóban visszavezethető $N_1 \cdot N_2 \cdot \ldots \cdot N_n$ méretű $n-D$ DFT számítására ($N = \prod_{j=1}^{n} N_j$, és az N_j számok egymással relatív prímek). Az indexek értékeit meghatározó kifejezések:

$$\begin{aligned} i &\equiv i_j \bmod N_j \\ k &\equiv \sum_{j=1}^{n} \frac{N k_j}{N_j} \bmod N_j \end{aligned} \tag{1-14}$$

Mivel az összes (N_i, N_j) párok relatív prímek, így i és k meghatározása ismét történhet az egészekre vonatkozó kínai maradéktétel alapján, ami egyúttal biztosítja az $i \to (i_1, \ldots, i_n)$ és a $k \to (k_1, \ldots, k_n)$ leképezések kölcsönösen egyértelmű voltát is.

1.2. Az együtthatómátrixok közti kapcsolat

Vizsgáljuk meg, mi az összefüggés a kiindulásul szolgáló $1-D$ DFT 1. rész (1-2) szerinti $\mathbf{W}_N$ együtthatómátrixa, valamint az abból ekvivalens átalakításokkal előállított $n-D$ DFT egyes dimenzióbeli együtthatómátrixai között. Először ismét a kétdimenziós esetből kiindulva [$N=N_1 \cdot P$ és $(N_1, P)=1$] az (1-1) összefüggéseket felhasználva kapjuk, hogy az együtthatómátrix elemei:

$$\begin{aligned} w_N^{ik \bmod N} &= e^{-j\left(\frac{2\pi}{N}\right) ik \bmod N} = \\ &= e^{-j\left(\frac{2\pi}{N}\right) K_1 I_1 i_1 k_1 \bmod N} \cdot e^{-j\left(\frac{2\pi}{N}\right) K_2 I_2 i_2 k_2 \bmod N} \end{aligned} \tag{1-15}$$

Az (1-8) szerinti feltételeket behelyettesítve és elvégezve a lehetséges egyszerűsítéseket:

$$\begin{aligned} w_N^{ik \bmod N} &= e^{-j\left(\frac{2\pi}{N}\right) i_1 k_1 P_1 \bmod N} \cdot e^{-j\left(\frac{2\pi}{N}\right) \cdot i_2 k_2 N_1 \bmod N} = \\ &= e^{-j\left(\frac{2\pi}{N}\right) K_1 I_1 i_1 k_1 \bmod N} \cdot e^{-j\left(\frac{2\pi}{N}\right) K_2 I_2 i_2 k_2 \bmod N}. \end{aligned} \tag{1-16}$$

A w mennyiségek alsó indexelése a végrehajtandó DFT pontszámát jelzi. A szorzatot az (i_1, k_1) és az (i_2, k_2) számpárok minden szóba jöhető értékére képezni kell. $w_P^{i_2 k_2 \bmod P}$ értékei viszont ($0 \le i_2 \le P-1$, $0 \le k_2 \le P-1$) éppen a P-pontos, $1-D$ DFT együtthatómátrixát határozzák meg:

$$\{w_P^{i_2 k_2 \bmod P}\} = \mathbf{W}_P. \tag{1-17}$$

Azaz az (1-16) alatti szorzat értéke:

$$\mathbf{W}_N = \{w_N^{ik \bmod N}\} = \{w_{N_1}^{i_1 k_1 \bmod N_1}\} \cdot \mathbf{W}_P. \tag{1-18}$$

A kifejezés jobb oldalán álló érték viszont éppen két mátrix ($\mathbf{W}_N$ és $\mathbf{W}_P$) Kronecker-szorzata. Mátrixok Kronecker szorzatának definícióját és annak néhány fontosabb tulajdonságát a 2. FÜGGELÉK tartalmazza. A Kronecker-szorzatot az „$\otimes$” szimbólummal jelölve az együtthatómátrixok közti kapcsolat:

$$\mathbf{W}_N = \mathbf{W}_N \otimes \mathbf{W}_P. \tag{1-19}$$

A Kronecker-szorzat asszociativitását felhasználva (2. FÜGGELÉK), P további páronként relatív prím tényezőkre való bontásával ($P = N_2 \cdot N_3 \cdot \ldots \cdot N_N$) kimutatható, hogy az ekvivalens $n-D$ DFT egyes dimenzióbeli együtthatómátrixai és az eredeti N-pontos $1-D$ DFT együtthatómátrixa között az összefüggés:

$$\mathbf{W}_N = \mathbf{W}_{N1} \otimes \mathbf{W}_{N2} \otimes \ldots \otimes \mathbf{W}_{Nn}. \tag{1-20}$$

A felbontás gyakorlati kivitelezésével kapcsolatban emlékeztetni kell arra a korábban már említett tényre, hogy a fokozatos részekre osztás együttal a kiindulási adatok átrendezését is jelentheti, amelynek következtében az eredeti $\mathbf{W}_N$ mátrix egyes sorai és oszlopai még a felbontás előtt felcserélődnek.

1.3. A fokozatos részekre osztással elérhető jelfeldolgozási frekvencia

Az $1-D \to n-D$ átalakítás és a fokozatos részekre osztás eredményeinek felhasználásával kimutatható, hogy ily módon a szükséges szorzások száma $f(N) = O(N \log N)$ rendig csökkenthető, ami jelentős

javulás (különösen nagyobb N-értékeknél) a közvetlen kiértékelés $O(N^2)$ műveletszámához képest.

Az elérhető f_{maxjel} jelfeldolgozási frekvencia az 1. rész (1-4) szerint $N=2^{10}\sim 10^3$ pontszámnál az 1. rész (3-14) összefüggés alapján:

$$(1\text{-}21)\qquad f_{maxjel}=\frac{N}{2\cdot t_{szorzás}\cdot f(N)}=237{,}96\ \text{kHz},$$

ami jelentős ugrást jelent a közvetlen kiértékeléssel elérhető frekvenciákhoz képest.

A fokozatos részekre osztás lehetőségeinek a kimerítésével felmerül a kérdés, vajon léteznek-e más, a gyakorlatban is alkalmazható algoritmusok, amelyek a fentieknél gyorsabbak (kisebb a szorzásigényük). Másik fontos kérdés, hogy a DFT számításának bonyolultságát a már ismert módon definiálva létezik-e alsó korlát általános esetben a szorzások számára nézve, s ha igen, az hogyan érhető el. A feladat nehézsége miatt a továbbiakban megelégszünk az első kérdésben felvetett probléma vizsgálatával. Megmutatható, hogy az algebra és a számelmélet eszközeinek a felhasználásával valóban származtathatók az előbbieknél hatékonyabb algoritmusok.

A következőkben a DFT számítását olyan ekvivalens feladattá transzformáljuk, amely megoldására ismert hatékony eljárás, vagy viszonylag könnyen készíthető ilyen. Ezen elvet követve vizsgáljuk a konvolúció és a DFT meghatározása közti kapcsolatot.

2. A DFT és a periodikus konvolúció kapcsolata

Legyen $\{x(i)\}$ és $\{h(i)\}$ két véges, általános esetben komplex $(0\leq i\leq N-1)$ sorozat. Lineáris konvolúciójukon a

$$(2\text{-}1)\qquad y(i)=\sum_{k=\max(0,\,1-N+1)}^{\min(N-1,\,i)} h(i-k)\cdot x(k)$$
$$0\leq i\leq 2N-2$$

sorozatot értjük. A két sorozat periodikus konvolúcióját definiáló összefüggés:

$$(2\text{-}2)\qquad y(i)=\sum_{k=0}^{N-1} h(i-k)\cdot x(k)\qquad 0\leq i\leq N-1.$$

A DFT-t mátrix alakban definiáló 1. rész (1-2) összefüggésben a $\mathbf{W}_N$ együtthatómátrix

$$\{w_N^{k,i}\}=\left\{e^{-j\left(\frac{2\pi}{N}\right)ki}\right\}$$

elemei helyett a minden egész c-reérvényes

$$e^{-j\left(\frac{2\Pi}{N}\right)cN}\equiv 1$$

azonosság miatt elegendő az

$e^{-j\left(\frac{2\pi}{N}\right)(ki \bmod N)}$ értékekkel számolni. A mod N művelet alkalmazásával előállított, úgynevezett redukált kitevőmátrix:

(2-3)

k \ i	0	1	2	3	...	$(N-3)$	$(N-2)$	$(N-1)$
0	0	0	0	0	...	0	0	0
1	0	1	2	3	...	$(N-3)$	$(N-2)$	$(N-1)$
2	0	2	4	6	...	$(N-6)$	$(N-4)$	$(N-2)$
3	0	3	6	9	...	$(N-9)$	$(N-6)$	$(N-3)$
.	.	.	.	.		.	.	.
.	.	.	.	.		.	.	.
.	.	.	.	.		.	.	.
$(N-3)$	0	$(N-3)$	$(N-6)$	$(N-9)$	...	9	6	3
$(N-2)$	0	$(N-2)$	$(N-4)$	$(N-6)$	...	6	4	2
$(N-1)$	0	$(N-1)$	$(N-2)$	$(N-3)$	...	3	2	1

Az első sorral és az első oszloppal nincs mit tenni. Jelentése: $X(0)$ igen egyszerűen számítható, csupán komplex összeadásokat felhasználva

$$\left(X(0)=\sum_{i=0}^{N-1} x(i)\right).$$

A többi transzformált felírható a következő alakban:

$$X(k)=x(0)+\sum_{i=1}^{N-1} x(i)e^{-j\left(\frac{2\pi}{N}\right)ki}\qquad (1\leq k\leq N-1).$$

A zérusokat tartalmazó első sor és az első oszlop elhagyása után a redukált transzformáció mátrixalakban:

$$(2\text{-}4)\qquad X'=\mathbf{W}'_{N-1}\cdot X'\begin{bmatrix}X(1)\\ \vdots\\ X(N-1)\end{bmatrix}=$$
$$=\left[\{w'^{ki}_{N-1}\}=w_N^{ki \bmod N}\right]\begin{bmatrix}X(1)\\ \vdots\\ X(N-1)\end{bmatrix}$$
$$1\leq k\leq N-1$$
$$1\leq i\leq N-1.$$

A $\mathbf{W}_{N-1}$ mátrix elemeinek kitevői a mod N maradékosztályba esnek. Mérete $(N-1)\times(N-1)$. A transzformált sorozat (X') egyrészt nem tartalmazza $X(0)$ értékét, másrészt $X'(k)=X(k)-x(0)$ $(1\leq k\leq N-1)$.

Az $(N-1)$ pontra vett periodikus konvolúció mátrixalakban:

$$(2\text{-}5)\qquad y=\mathbf{H}\cdot x \begin{bmatrix} y(0) \\ y(1) \\ \vdots \\ y(N-3) \\ y(N-2) \end{bmatrix} = \begin{bmatrix} h(0) & h(1) & \dots & h(N-2) \\ h(1) & h(2) & \dots & h(0) \\ \vdots & \vdots & & \\ h(N-3) & h(N-2) & \dots & h(N-4) \\ h(N-2) & h(0) & \dots & h(N-3) \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ \vdots \\ x(N-3) \\ x(N-2) \end{bmatrix}$$

A $\mathbf{H}$ mátrix elemeinek egy lehetséges előállítása az indexek közti összefüggés alapján:

$$(2\text{-}6)\qquad \{h^{ki}\}=\{h((k+i) \bmod N-1)\}.$$

Összehasonlítással látható, hogy a DFT akkor tekinthető periodikus konvolúciónak, ha a $\mathbf{W}'_{N-1}$ együtthatómátrix indexelése is megfelel a periodikus konvolúció indexelésének. A megfelelő indexsorrendek a sorok és az oszlopok ekvivalens felcserélésével esetlegesen is kialakíthatók. Célszerűbbnek látszik azonban szisztematikus eljárást keresni a megfelelő átrendezésre. Az első felmerülő kérdés: létezik-e egyáltalán ilyen átrendezés, és ha igen, milyen feltételek mellett.

Az átrendezés definiálható leképzésként is. Eszerint keresünk olyan leképzés(eke)t, amely(ek) az indexek modulo N vett szorzatát az indexek modulo $(N-1)$ szerint vett összegébe képezik le.

Tekintsük az $a^i \bmod N$ (a pozitív egész) alaku sorozatot, ahol i zérustól kezdve végigfut a természetes számokon. A sorozatban nyilván csak véges számú különböző elem szerepel (a lehetséges maradékosztályok száma N). A sorozat egyetlen elemmel (a) generálható. Euler tételének (1. FÜGGELÉK) felhasználásával kimutatható, hogy a sorozat periodikus. Tekintsük az $(a, N)=1$ esetet [az $(a, N)>1$ eset erre visszavezethető]. Ha a sorozat P értékkel periodikus, akkor:

$$(2\text{-}7)\qquad (a^i \bmod N)=(a^{l+P} \bmod N)=((a^i \bmod N)\cdot (a^P \bmod N) \bmod N).$$

Összehasonlítással adódik, hogy $a^P \bmod N=1$. Euler tétele értelmében ilyen P biztosan létezik. $P=\varphi(N)$, ahol φ az Euler-féle számelméleti függvény. Legyen d a legkisebb periódus. Mivel $(a^0 \bmod N)=1$, ezért $(a^d \bmod N), \dots, (a^{kd} \bmod N)=1$. Nyilván $(a^i \bmod N)\neq 1$, ha $d\nmid i$, mivel egyébként létezne d értéknél kisebb periódus. Ezért $d|\varphi(N)$.

Az Euler-tétel másik fontos következménye, hogy

$$(2\text{-}8)\qquad (a^i \bmod N)=(a^{i \bmod \varphi(N)} \bmod N).$$

Azon elemeket, amelyekre a legkisebb periódus éppen $\varphi(N)$ értékű, primitív gyököknek nevezzük. Ismert számelméleti eredmény (Gauss [1]) szerint primitív gyökök csupán $N=2, 4, p, p^k$ és $2p^k$ értékekre léteznek, ahol p páratlan prím. A primitív gyökök fontosságát számunkra az a tény adja, hogy N prím esetén $\varphi(N)=N-1$, azaz létezik olyan a egész (a primitív gyök), amelyre az $a^i \bmod N$ sorozat egy periódusa az $(1, 2, \dots, N-1)$ számok valamely permutációja, azaz kölcsönösen egyértelmű leképezés létesíthető i és $(a^i \bmod N)$ között. Az

$$(2\text{-}9)\qquad (a^i \bmod N)=(a^{i \bmod \varphi(N)} \bmod N)=(a^{i \bmod (N-1)} \bmod N)$$

összefüggés alapján:

$$(2\text{-}10)\qquad \begin{matrix} k\equiv a^{i_1} \bmod N \\ i\equiv a^{i_2} \bmod N \end{matrix} \quad k\cdot i \bmod N=(a^{i_1+i_2} \bmod N)=(a^{i_1+i_2 \bmod (N-1)} \bmod N),$$

ami pontosan a keresett leképzés.

A primitív gyökök előállítására szisztematikus módszer nem ismert. Ha egy számhoz létezik primitív gyök, akkor ugyanazon értékhez több primitív gyök is tartozhat. Néhány prímszám legkisebb primitív gyökét az 1. FÜGGELÉK tartalmazza. Példaként ugyanott látható az $i\to a^i \bmod N$ leképezés $N=7$, $a=3$ esetre.

A primitív gyökök fogalmának felhasználásával már könnyen megmutatható, hogy N prím volta esetén az N-pontos DFT ekvivalens módon átalakítható periodikus konvolúcióvá. A bizonyítás egyúttal megadja az átalakítás algoritmusát is ([24]). Ismét az 1. rész (1-1) alatti definíciós összefüggésből kiindulva számítsuk $X(0)$ értékét külön, és a többi tagban is kezeljük külön $X(0)$-t, azaz:

$$X(0)=\sum_{i=0}^{N-1} x(i)$$

$$(2\text{-}11)\qquad X(k)=x(0)+\sum_{i=1}^{N-1} x(i)w^{ki} \quad 1\leq k\leq N-1 \text{ és } (k, N)=1.$$

A primitív gyökök létezését kihasználva változócserét végrehajtva:

$$(2\text{-}12)\qquad \begin{matrix} k\to (a^k \bmod N) \\ i\to (a^{-i} \bmod N). \end{matrix}$$

Mivel $(a^{\varphi(N)} \bmod N)=1$ (Euler-tétel), ezért $(a^{-i} \bmod N)=(a^{\varphi(N)-i} \bmod N)$. Az első változócsere ($k$) az egyenletek átszámozását jelenti, míg a másik (i) az összegzésen belül a tagok átrendezését.

$$(2\text{-}13)\qquad X(a^k \bmod N)=$$

$$=x(0)+\sum_{i=1}^{N-1} x(a^{-i} \bmod N)w^{(-i+k) \bmod N}=$$

$$=x(0)+\sum_{i=1}^{N-1} x(a^{-i} \bmod N)w^{(k-i) \bmod N},$$

vagyis $X(a^k \bmod N)$ éppen egy $\varphi(N)=N-1$ hosszúságú (N prím) periodikus konvolúció.

Ha $N=p^k$ (p páratlan prím), az átalakításnál nehézséget okoznak p többszörösei. Az előzőekhez hasonlóan kimutatható, hogy az $N=p^k$ pontszámú DFT számítható 1 db $p^{k-1}(p-1)$ hosszúságú, 2 db $p^{k-2}(p-1)$ hosszúságú, ... és p^{k-1} db $(p-1)$ hosszúságú periodikus konvolúcióként.

A fejezet elején kijelölt célokat elértük: kiderült, hogy a DFT azon esetekben, amikor a transzformáció N pontszáma prím, vagy páratlan prímszám hatványa, visszavezethető periodikus konvolúció számítására.

3. Gyors eljárás a konvolúció számítására

A DFT számításához szükséges szorzások számának ($f(N)$) csökkentésére irányuló algoritmikus módszerek közül a fokozatos részekre osztás lehetőségeinek kimerítése után egy lehetséges stratégia az eredeti feladat visszavezetése ekvivalens módon olyan feladatra, amely számítására már ismert, vagy található hatékony algoritmus. Az előzőek szerint a DFT meghatározása ekvivalens a periodikus konvolúció számításával, ha $N=2$, 4, p, p^k vagy $2p^k$, ahol a p páratlan prím.

3.1. Gyors eljárás a lineáris konvolúció számítására

Legyen $\{x(i)\}$ és $\{h(i)\}$ két időtartománybeli, N pontból álló véges sorozat, amely tagjai akár komplexek is lehetnek. Legyen $H(z)$ és $X(z)$ két $(N-1)-d$ fokú polinom:

$$H(z)=\sum_{i=0}^{N-1} h(i)z^i = h(0)+h(1)z \ldots + h(N-1)z^{N-1}$$

(3-1)

$$X(z)=\sum_{i=0}^{N-1} x(i)z^i = x(0)+x(1)z+\ldots+x(N-1)z^{N-1}.$$

A polinomok együtthatói a sorozatok tagjai (formailag a két polinom megegyezik a két sorozat Laplace-féle z-transzformáltjával). Az időtartománybeli lineáris konvolúciónak megfelel a két polinom szorzása:

$$(3\text{-}2)\quad Z\{y(i)\}=Z\{h(i) * x(i)\}=Y(z)=H(z)\cdot X(z),$$

ahol $Y(z)$ egy $(2N-2)$-edfokú polinom, amely együtthatói az $\{x(i)\}$ és a $\{h(i)\}$ sorozatok konvolúciójának eredményéül adódnak:

$$(3\text{-}3)\quad Y(z)=y\sum_{i=0}^{2N-2} y(i)z^i = y(0)+y(1)z+\ldots+ +y(2N-2)z^{N-2}.$$

Ezek szerint az $y(i)=[y(0), y(1), \ldots, y(2N-2)]$ konvolúciós sorozat meghatározása visszavezethető két $(N-1)$-edfokú polinom szorzatával meghatározott polinom együtthatóinak előállítására.

Toom ([26]) tétele szerint két $(N-1)$-tagú sorozat időtartománybeli lineáris konvolúciója meghatározható $(2N-1)$ db szorzással (a racionális számtestbe tartozó, előre ismert állandókkal való szorzásokat nem számítva).

A bizonyítás elvégezhető a kiszámítási eljárás megadásával. Az algoritmus s szakirodalomban Toom–Cook-eljárás néven ismeretes (pl. [5]). Az $\{x(i)\}$ és a $\{h(i)\}$ sorozatok (3-2) és (3-3) szerint egyértelműen meghatározzák az $Y(z)$ polinomot. A Lagrange-féle interpolációs tétel állítása viszont kimondja, hogy tetszőleges $(2N-2)$-edfokú polinomot egyértelműen meghatározza $(2N-1)$ pontban felvett értéke. Ha $Y(z)$ a keresett polinom, akkor a z_i $(0\leq i\leq 2N-2)$ pontokban felvett $Y(z_i)$ értékek ismeretében $Y(z)$ előállítása:

$$(3\text{-}4)\quad Y(z)=\sum_{i=0}^{2N-2} Y(z_i)\prod_{i\neq k}\frac{(z-z_k)}{(z_i-z_k)}.$$

Az összefüggés jobb oldala az ismert Lagrange-féle interpolációs polinom. (3-2) szerint $Y(z_i)=H(z_i)\cdot X(z_i)$ $(0\leq i\leq 2N-2)$, azaz $Y(z)$ valóban előállítható $(2N-1)$ db $H(z_i)\cdot X(z_i)$ szorzat ismeretében (az összegben álló szorzattag kifejtése után $Y(z)$ keresett együtthatói az $Y(z_i)$ értékek lineáris kombinációiként adódnak). A számítás egyszerűsíthető a z_i értékek ügyes választásával.

Az eljárás leírható mátrixos jelölésmóddal is. Legyen $x=[x(0), x(1), \ldots, x(N-1)]^T$, $h=[h(0), h(1), \ldots, h(N-1)]^T$. Definiáljuk az **A** együtthatómátrixot a következőképpen:

$$(3\text{-}5)\quad \mathbf{A}=\begin{bmatrix} 1 & z_0 & z_0^2 & \ldots & z_0^{N-1} \\ 1 & z_1 & z_1 & \ldots & z_1 \\ 1 & z_2 & z_2^2 & \ldots & z_2^{N-1} \\ \vdots & & \vdots & & \vdots \\ 1 & z_{2N-2} & & \ldots & z_{2N-2}^{2N-2} \end{bmatrix}.$$

Ekkor:

$$(3\text{-}6)\quad \mathbf{A}x=[X(z_0), X(z_1), \ldots, X(z_{2N-2})]^T \text{ és}$$
$$\mathbf{A}h=[H(z_0), H(z_1), \ldots, H(z_{2N-2})]^T.$$

Bevezetve az $m=[Y(z_0), Y(z_1), \ldots, Y(z_{2N-2})]^T$ segédvektort, $m=(\mathbf{A}h)\bigcirc(\mathbf{A}x)$, ahol a ,$\bigcirc$' szimbólum az elemenkénti szorzást jelenti. Az interpolációs formulából következően $Y(z)$ együtthatói valóban az $\{m(i)\}$ értékek lineáris kombinációi, azaz:

$$(3\text{-}7)\quad \mathbf{y}=\mathbf{C}m,$$

ahol **C** egy $(2N-1)\times(2N-1)$ méretű mátrix. **C** elemei racionálisak, ha a z_i értékek is racionálisak.

3.2. A periodikus konvolúció számítása

Az $\{x(i)\}$ és a $\{h(i)\}$ sorozatok periodikus konvolúcióját leíró $\{y(i)\}$ sorozathoz $(0\leq i\leq N-1)$ a (3-1) és a (3-2) összefüggésekhez hasonlóan hozzárendelt $Y(z)$ polinom fokszáma a definícióból következően $(N-1)$. Előállításának módjából következik a definiáló összefüggés:

$$(3\text{-}8)\quad Y(z)=H(z)\cdot X(z) \bmod (z^N-1).$$

Helyessége egyszerű polinomosztással belátható ($H(z)\cdot X(z) \bmod z^N-1$) éppen a (z^N-1) polinommal valós osztás maradékát jelenti:

$$H(z)\cdot X(z)=\sum_{i=0}^{N-1} z^i \sum_{k=0}^{i} x(i-k)\cdot h(k)+$$
$$+z^N \sum_{i=0}^{N-2}\sum_{k=i+1}^{N-1} x(N-k+i)\cdot h(k)$$

(3-9)

$$H(z)\cdot X(z) \bmod (z^N-1)=z^{N-1}\sum_{k=0}^{N-1} x(N-1-k)\cdot h(k)+$$
$$+\sum_{i=0}^{N-2} z^i \sum_{k=0}^{i} x(i-k)\cdot h(k)+\sum_{k=i+1}^{N-1} x(N-k+i)\cdot h(k).$$

Vegyük észre, hogy a polinom együtthatói valójában az $\{x(i)\}$ és a $\{h(i)\}$, N pontból álló sorozatok periodikus konvolúciójának felelnek meg, azaz a periodikus konvolúció számítását két polinom szorzata egy speciális polinommal való osztási maradékának meghatározására lehet visszavezetni.

Winograd tétele ([27]) kimondja, hogy az $Y(z)=H(z)\cdot X(z) \bmod (z^N-1)$ periodikus konvolúció kiszámításához $2N-K$ db szorzás szükséges, ahol K pontosan N osztóinak száma. A szorzások számának meghatározásánál a racionális számtestbe tartozó, előre ismert állandókkal való szorzásokat nem számítottuk. A bizonyítás (pl. [5]) ismét megad egy lehetséges kiszámítási módot.

A (z^N-1) polinom felbontható egész együtthatós, a racionális számtestben egyébként felbonthatatlan polinomok szorzatára:

(3-10) $$z^N-1=P_{d1}(z)\cdot P_{d2}(z)\ldots P_{dk}(z) \qquad (d_i|N).$$

A $P_{d_i}(z)$ polinomok a számelméletből ismert, úgynevezett ciklotomikus polinomok. Fokszámuk $\varphi(d_i)$, ahol φ az első részben már említett Euler-féle számelméleti függvény.

Mivel $\deg(Y(z))<N$ és a $P_{d_i}(z)$ polinomok egész együtthatójúak, teljesülnek a polinomokra vonatkozó kínai maradéktétel (3. FÜGGELÉK) feltételei, vagyis $Y(z)$ egy lehetséges előállítása:

$$Y(z)=\left[\sum_{d|N} Y_d(z)\cdot B_d(z)\right] \bmod (z^N-1), \text{ ahol}$$

(3-11) $$Y_d(z)=[H(z)\cdot X(z)] \bmod P_d(z) \text{ és}$$

$$B_d(z)=[(z^N-1)/P_d(z)]\cdot\{1/[(z^N-1)/P_d(z)]\} \bmod P_d(z).$$

Az $Y_d(z)=H(z)\cdot X(z) \bmod P_d(z)$ konvolúciók az előzőek szerint legfeljebb $2\varphi(d)-1$ szorzással meghatározhatók [$Y_d(z)$ fokszáma $\varphi(d)$-nél biztosan nem nagyobb]. Mivel az eredeti konvolúció K db ilyen konvolúció összegeként számítható, a szükséges szorzások száma nem több, mint $\sum_{d|N} 2\varphi(d)-1=2N-K$ (felhasználva az ismert $\sum_{l=1}^{K}\varphi(d_l)=N$ azonosságot). Winograd azt is kimutatta, hogy a szükséges szorzások minimális száma valóban $2N-K=O(N)$.

A minimális számú szorzást igénylő algoritmusok származtatását megkönnyíti, hogy az eredeti $Y(z)=H(z)\cdot X(z) \bmod (z^N-1)$ periodikus konvolúció több kisebb pontszámú $Y_d(z)=H(z)\cdot X(z) \bmod P_d(z)=H_d(z)\cdot X_d(z) \bmod P_d(z)$ konvolúcióra vezethető vissza, ahol $H_d(z)=H(z) \bmod P_d(z)$, ill. $X_d(z)=X(z) \bmod P_d(z)$. A $H_d(z)\cdot X_d(z)$ szorzat értéke a Toom—Cook-algoritmussal vagy egyéb szisztematikus eljárással meghatározható. Az A és a **C** mátrixok bonyolultsága következtében azonban még kis N értékekre is érdemes az optimálistól kismértékben eltérő algoritmusokat keresni. Az eltérés eredményeképpen az A és a **C** mátrixok elemei egyszerűsödnek, ami megkönnyíti a gyakorlati megvalósítást. Ára: a szorzások számának kismértékű növekedése.

3.3. Példa a periodikus konvolúció kiszámítására

Példaképp határozzuk meg az optimális számítási eljárást $N=6$ esetére. A keresett periodikus konvolúció:

(3-12) $$y(i)=\sum_{j=0}^{5} h(i-j)\cdot x(j);\ 0\le i\le 5;\ X(z)=\sum_{j=0}^{5} x(j)z^j \text{ és } H(z)=\sum_{j=0}^{5} h(j)z^j.$$

Polinom alakban:

(3-13) $$Y(z)=H(z)\cdot X(z) \bmod (z^6-1)$$

(a keresett $y(i)$ értékek az $Y(z)$ polinom együtthatói). N osztói $d=1$, 2, 3 és 6, így az osztó polinom felbontása:

$$(z^6-1)=P_1(z)\cdot P_2(z)\cdot P_3(z)\cdot P_4(z)=$$
$$=(z-1)(z+1)(z^2-z+1)(z^2+z+1).$$

A szükséges segédmennyiségek:

$$H_1(z)=H(z) \bmod P_1(z)=\sum_{j=0}^{5} h(j)$$

$$H_2(z)=H(z) \bmod P_2(z)=h(0)-h(1)+h(2)-h(3)+h(4)-h(5)$$

$$H_3(z)=H(z) \bmod P_3(z)=\{h(0)-h(2)+h(5)-h(3)\}+z\{h(1)-h(4)+h(2)-h(5)\}$$

$$H_4(z)=H(z) \bmod P_4(z)=\{h(0)-h(2)+h(3)-h(5)\}+z\{h(1)-h(2)+h(4)-h(5)\}.$$

Az $X_i(z)=X(z) \bmod P_i(z)$ $(1\le i\le 4)$ mennyiségek azonos felépítésűek. A kínai maradéktétel segédpolinomjainak meghatározása:

$$B_1(z)=\frac{1}{6}\cdot(z+1)(z^2-z+1)(z^2+z+1)$$

$$B_2(z)=-\frac{1}{6}\cdot(z-1)(z^2-z+1)(z^2+z+1)$$

$$B_3(z)=-\frac{1}{2}\cdot(z-1)(z^2+z+1)$$

$$B_4(z)=\frac{1}{2}\cdot(z+1)(z^2-z+1).$$

A szorzások számának minimálásához az $\{x(i)\}$ és a $\{h(i)\}$ együtthatókból képzett értékek:

$$h_0=[h(0)-h(2)+h(3)-h(5)]/6$$
$$x_0=x(0)-x(2)+x(3)-x(5)$$
$$h_1=[h(1)-h(2)+h(4)-h(5)]/6$$
$$x_1=x(1)-x(2)+x(4)-x(5)$$
$$h_2=h_1-h_0 \qquad x_2=x_0-x_1$$

$$h_3=[h(0)-h(2)+h(5)-h(3)]/6$$
$$x_3=x(0)-x(2)+x(5)-x(3)$$
$$h_4=[h(1)-h(4)+h(2)-h(5)]/6$$
$$x_4=x(1)-x(4)+x(2)-x(5)$$
$$h_5=h_3+h_4 \qquad x_5=x_3+x_4$$
$$h_6=[h(0)-h(1)+h(2)-h(3)+h(4)-h(5)]/6$$
$$x_6=x(0)-x(1)+x(2)-x(3)+x(4)-x(5)$$
$$h_7=\left[\sum_{j=0}^{5} h(j)\right]/6 \qquad x_7=\left[\sum_{j=0}^{5} x(j)\right].$$

Az $Y_i(z)$ segédpolinomok:

$$Y_1(z)=H_1(z)\cdot X_1(z) \bmod P_1(z)=6h_7x_7$$
$$Y_2(z)=H_2(z)\cdot X_2(z) \bmod P_2(z)=6h_6x_6$$
$$Y_3(z)=H_3(z)\cdot X_3(z) \bmod P_3(z)=6(x_5h_5-x_3h_3)z+$$
$$+6(x_3h_3-x_4h_4)$$
$$Y_4(z)=H_4(z)\cdot X_4(z) \bmod P_4(z)=6(x_2h_2-x_0h_0)z+$$
$$+6(x_0h_0-x_1h_1)$$
$$m_i=h_ix_i \qquad 0\leq i\leq 7,$$

végül az $Y(z)$ polinom keresett együtthatói:

$$y(0)=\{(m_0-m_1)-(m_1+m_2)\}+$$
$$+\{(m_3-m_4)-(m_4-m_5)\}+(m_6+m_7)$$
$$y(1)=\{(m_0+m_2)+(m_1+m_2)\}-$$
$$-\{(m_3-m_5)+(m_4-m_5)\}-(m_6-m_7)$$
$$y(2)=-\{(m_0-m_1)+(m_0+m_2)\}-$$
$$-\{(m_3-m_4)+(m_3-m_5)\}+(m_6+m_7)$$
$$y(3)=\{(m_0-m_1)-(m_1+m_2)\}-$$
$$-\{(m_3-m_4)-(m_4-m_5)\}-(m_6-m_7)$$
$$y(4)=\{(m_0+m_2)+(m_1+m_2)\}+$$
$$+\{(m_3-m_5)+(m_4-m_5)\}+(m_6+m_7)$$
$$y(5)=-\{(m_0-m_1)+(m_0+m_2)\}+$$
$$+\{(m_3-m_4)+(m_3-m_5)\}-(m_6-m_7).$$

A szükséges szorzások száma 8 ($2N-K=2\cdot 6-4=8$), az összeadásoké pedig 44.

3.4. A periodikus konvolúció számítására szolgáló gyors eljárások értékelése

A polinomokra vonatkozó kínai maradéktétel felhasználásával kapott eredményeket $N=2$, 3, 4, 5 és 7 pontszámokra a 4. FÜGGELÉK tartalmazza ([5]). Az ott leírt algoritmusokhoz szükséges szorzások és összeadások száma az 1. táblázatban található (az elméleti minimum természetesen $2N-K$).

Az összeadások száma az asszociativitási tulajdonság felhasználásával ügyes csoportosítással esetlegesen csökkenthető. Egyelőre azonban nem ismeretes az összeadások minimális számára vonatkozó tétel, ill. szisztematikus eljárás számuk minimálására.

Nagy N értékekre az optimális algoritmus származtatása igen nehézkessé válik. A C mátrix egyes elemei igen nagyok lehetnek, és a szükséges összeadások száma is hirtelen megnő. Ugyanakkor az optimálistól kismértékben eltérő (a minimálisnál valamivel több szorzást tartalmazó) algoritmusok bonyolultsága is lényegében $O(N)$.

1. táblázat

N	K	$2N-K$	M	A_c	$f(N)=3M$	$A_r=2A_c+5M$
2	2	2	2	4	6	28
3	2	4	4	11	12	42
4	3	5	5	15	15	55
5	2	8	10	35	30	120
6	4	8	8	44	24	122
7	2	12	19	72	57	239
8	4	12	14	46	42	162
9	3	15	22	98	66	306

A_c: a komplex összeadások száma, M: a komplex szorzások száma, A_r: a valós összeadások száma.

Másik lehetőség az egydimenziós konvolúciót többdimenzióssá alakítani úgy, hogy az egyes dimenziók méretének szorzata éppen az egydimenziós konvolúció méretét adja. A DFT meghatározása szempontjából azonban elegendő néhány kis (lehetőleg prím, vagy prímhatvány) pontszámra meghatározni a lehetőleg optimális konvolúciós eljárást, mert az $1-D$ DFT biztosan többdimenzióssá alakítható át, ha a pontszám egymáshoz relatív prím tényezők szorzatára bontható. A gyakorlati esetekben fontos pontszámok esetén azonban N általában néhány, viszonylag kicsi, egymáshoz relatív prím szorzatára bontható.

A konvolúciót optimálisan számító algoritmusoknak hasonlóan nagy jelentősége van, mint a DFT eljárásoknak. A szükséges szorzások számának csökkentése ugyanis itt is a kötött idejű jelfeldolgozás maximális frekvenciájának a növekedésére vezet (pl. véges súlyfüggvényű szűrőknél), mint a DFT alkalmazásán alapuló eszközöknél.

(A cikk ugyanezen folyóirat későbbi számában folytatódik.)

1. FÜGGELÉK

Euler-tétel:

Ha $(x, N)=1$, akkor

$$x^{\varphi(N)}=1 \bmod N.$$

$\varphi(N)$ az Euler-féle φ-függvény. Jelentése: azon értékek száma, amelyek N-nél kisebbek és ahhoz relatív prímek. Definíciószerűen $\varphi(1)=1$. Ha N prím, nyilván $\varphi(N)=N-1$. $N=p^\alpha$ (prímhatvány) esetén egyszerű leszámlálással kimutatható, hogy:

$$\varphi(N)=\varphi(p^\alpha)=p^{\alpha-1}(p-1).$$

Bizonyítás nélkül az általános összefüggés $\varphi(N)$-re, ha a törzstényezős felbontásból indulunk ki, azaz

$$N=\prod_{i=1}^{n} p_i^{\alpha i}$$

akkor $$\varphi\left(\prod_{i=1}^{n} p_i^{\alpha_i}\right)=\prod_{i=1}^{n}\varphi(p_i^{\alpha_i}).$$

Példa:

Legyen $x=7$ és $N=6$. Ekkor $(x, N)=1$. Az N értéknél kisebb egészek: 1, 2, 3, 4 és 5. Ezek közül $(1, 6)=1$ és $(5, 6)=1$, azaz $\varphi(N)=2$. Euler tételét felírva:

$$(x^{\varphi(N)} \bmod N)=(7^2 \bmod 6)=(49 \bmod 6)=1.$$

Néhány prímszám legkisebb primitív gyöke:

p	a	p	a	p	a	p	a	p	a	p	a	p	a	p	a
2	1	11	2	23	5	41	6	59	2	73	5	97	5	109	6
3	2	13	2	29	2	43	3	61	2	79	3	101	2	113	3
5	2	17	3	31	3	47	5	67	2	83	2	103	5	127	3
7	2	19	2	37	2	53	2	71	7	89	3	107	2	131	2

Az $i \to a^i \bmod N$ leképzés $N=7$, $a=3$ esetén $(1 \leq i \leq 6)$:

i	1	2	3	4	5	6
$a^i \bmod N$	3	2	6	4	5	1

2. FÜGGELÉK

Mátrixok Kronecker-szorzata:

Definíció: Két mátrix (**A** és **B**) Kronecker-szorzatán (direkt szorzatán) a következő kifejezést értjük:

$$\mathbf{A}\otimes\mathbf{B}=\begin{bmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B}\ldots a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B}\ldots a_{2n}\mathbf{B} \\ \vdots & \\ a_{m1}\mathbf{B} & a_{m2}\mathbf{B}\ldots a_{mn}\mathbf{B} \end{bmatrix}.$$

Az **A** mátrix mérete $m\times n$, a **B** mátrix mérete $k\times l$, míg az $\mathbf{A}\otimes\mathbf{B}$ mátrix $mk\times nl$ nagyságú.

Fontosabb azonosságok (bizonyítás nélkül):

1. $$\mathbf{A}\otimes\mathbf{B}=\begin{bmatrix} b_{11}\mathbf{A} & b_{12}\mathbf{A}\ldots b_{1l}\mathbf{A} \\ b_{21}\mathbf{A} & b_{22}\mathbf{A}\ldots b_{2l}\mathbf{A} \\ \vdots & \\ b_{k1}\mathbf{A} & b_{k2}\mathbf{A}\ldots b_{kl}\mathbf{A} \end{bmatrix}.$$

A definíciós összefüggéssel összehasonlítva látható, hogy a Kronecker-szorzat nem kommutatív.

2. $\mathbf{A}\otimes\mathbf{B}\otimes\mathbf{C}=(\mathbf{A}\otimes\mathbf{B})\otimes\mathbf{C}=\mathbf{A}\otimes(\mathbf{B}\otimes\mathbf{C})$ (asszociativitás)
3. $(\mathbf{A}+\mathbf{B})\otimes(\mathbf{C}+\mathbf{D})=\mathbf{A}\otimes\mathbf{C}+\mathbf{A}\otimes\mathbf{D}+\mathbf{B}\otimes\mathbf{C}+\mathbf{B}\otimes\mathbf{D}$ (disztributivitás)
4. $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})=(\mathbf{AC})\otimes(\mathbf{BD})$
5. $(\mathbf{A}_1\mathbf{B}_1)\otimes(\mathbf{A}_2\mathbf{B}_2)\otimes\ldots\otimes(\mathbf{A}_n\mathbf{B}_n)=$ $=(\mathbf{A}_1\otimes\mathbf{B}_2\otimes\ldots\otimes\mathbf{A}_n)\cdot(\mathbf{B}_1\otimes\mathbf{B}_2\otimes\ldots\otimes\mathbf{B}_n)$
6. $(\mathbf{A}\otimes\mathbf{B})^T=\mathbf{A}^T\otimes\mathbf{B}^T$
7. $(\mathbf{A}\otimes\mathbf{B})^{-1}=\mathbf{A}^{-1}\otimes\mathbf{B}^{-1}$
8. $\mathbf{A}^{(2)}=\mathbf{A}\otimes\mathbf{A}$ (hatvány definíciója)
   $\mathbf{A}^{k+1}=\mathbf{A}\otimes\mathbf{A}^k=\mathbf{A}^k\otimes\mathbf{A}$
   $(\mathbf{AB})^k=\mathbf{A}^k\cdot\mathbf{B}^k$ minden **A** és **B** mátrixra.

3. FÜGGELÉK

A polinomokra vonatkozó kínai maradéktétel

Legyen $A(z)$ egy véges tér felett definiált N-edfokú polinom, amely K db egymáshoz relatív prím, ugyanazon tér felett értelmezett polinom szorzatára bontható:

$$A(z)=A_1(z)\cdot A_2(z)\ldots A_k(z).$$

Legyen $\deg A_i(z)=N_i(z)$ az $A_i(z)$ polinom fokszáma, és $N=\prod_{i=1}^{n} N_i$. Akkor adott $B_i(z)$ $(0\leq\deg B_i(z)<N_i$ és $0\leq i\leq K)$ polinomokhoz létezik olyan egyértelmű $B(z)$ polinom, amelyre $\deg[B(Z)]<N$, és $B_i(z)=B(z) \bmod A_i(z)$. A $B(z)$ polinomot meghatározó összefüggés:

$$B(z)=\left[\sum_{i=1}^{k} B_i(z)\cdot C_i(z) \bmod A(z)\right],$$ ahol a $C_i(z)$ segédpolinomokat definiáló egyenlet:

$$C_i(z)=\frac{A(z)}{A_i(z)}\cdot\frac{1}{[A(z)/A_i(z)] \bmod A_i(z)}.$$

4. FÜGGELÉK

A: komplex összeadások száma, *M:* komplex szorzások száma.

Algoritmus 1. $N=2$, $M=2$, $A=4$.

$a_0=(h(0)+h(1))/2$ $b_0=x(0)+x(1)$ $m_0=a_0b_0$
$y(0)=m_0+m_1$

$a_1=(h(0)-h(1))/2$ $b_1=x(0)-x(1)$ $m_1=a_1b_1$
$y(1)=m_0-m_1$

Algoritmus 2. $A=3$, $M=4$, $A=11$

$a_0=(h(0)+h(1)+h(2))/3$ $b_0=x(0)+x(1)+x(2)$
$m_0=a_0b_0$

$a_1=h(0)-h(2)$ $b_1=x(0)-x(2)$ $m_1=a_1b_1$

$a_2=h(1)-h(2)$ $b_2=x(1)-x(2)$ $m_2=a_2b_2$

$a_3=(n_1+a_2)/3$ $b_3=b_1+b_2$ $m_3=a_3b_3$

$y(0)=m_0+(m_1-m_3)$ $y(1)=m_0-(m_1-m_3)-(m_2-m_3)$
$y(2)=m_0+(m_2-m_3)$

Algoritmus 3. $N=4$, $M=5$, $A=15$.

$a_0=\big((h(0)+h(2))+(h(1)+h(3))\big)/4$
$b_0=(x(0)+x(2))+(x(1)+x(3))$
$a_1=\big((h(0)+h(2))-(h(1)+h(3))\big)/4$
$b_1=(x(0)+x(2))-(x(1)+x(3))$
$a_2=(h(0)-h(2))/2$
$h_2=(x(0)-x(2))+x((1)-x(3))$

$$a_3=\big((h(0)-h(2))-(h(1)-h(3))\big)/2$$
$$a_4=\big((h(0)-h(2))+(h(1)-h(3))\big)/2$$
$$b_3=x(0)-x(2)\quad b_4=x(1)-x(3)$$
$$m_i=a_ib_i\qquad 0\le i\le 4$$
$$y(0)=m_0+m_1)+(m_2-m_4)\quad y(2)=(m_0+m_1)-(m_2-m_4)$$
$$y(1)=(m_0-m_1)+(m_2-m_3)\quad y(3)=(m_0-m_1)-(m_2-m_3)$$

Algoritmus 4. $N=5$, $M=10$, $A=35$.

$$a_0=\left(\sum_{i=0}^{4}h(i)\right)\qquad a_1=h(0)-h(4)\qquad a_2=h(1)-h(4)$$
$$a_3=h(2)-h(4)$$
$$a_4=h(3)-h(4)\qquad a_5=a_1+a_2\qquad a_6=a_3+a_4\qquad a_7=a_1+a_3$$
$$a_8=a_2+a_4\qquad a_9=(a_5+a_6)/5.$$

A b_0-b_9 mennyiségek hasonló felépítésűek, elhagyva az állandókkal való osztást.

$$m_i=a_ib_i\qquad 0\le i\le 9$$
$$y(0)=(m_0-m_9)+(m_1-m_4)-m_3+m_6$$
$$y(2)=(m_0-m_9)+(m_2-m_3)-m_1+m_7$$
$$y(1)=(m_0-m_9)-(m_1-m_4)-m_2+m_5$$
$$y(4)=(m_0-m_9)-(m_2-m_3)-m_4+m_8$$
$$y(3)=(m_0+m_0)+(m_0+m_0)+$$
$$+m_0-y(0)-y(1)-y(2)-y(4).$$

Algoritmus 5. $N=6$, $M=10$, $A=35$. Lásd a 2.3-beli példát.

Algoritmus 6. $N=7$, $M=19$, $A=72$.

$$a_1=h(0)-h(6)\quad a_2=h(1)-h(6)\quad a_3=h(2)-h(6)$$
$$a_4=h(3)-h(6)\quad a_5=h(4)-h(6)\quad a_6=h(5)=h(6)$$
$$a_7=a_1+a_4\qquad a_8=a_2+a_5\qquad a_9=a_3+a_6$$
$$a_{10}=a_1+a_2\qquad a_{11}=a_2+a_3\qquad a_{12}=a_1+a_3$$
$$a_{13}=a_4+a_5\qquad a_{14}=a_5+a_6\qquad a_{15}=a_4+a_3$$
$$a_{16}=a_{10}+a_{13}\qquad a_{17}=a_{11}+a_{14}\qquad a_{18}=(a_7+a_{17})/7$$
$$a_0=a_{18}+h(6)\quad b_{18}=b_7+b_{17}$$
$$b_0=b_{18}+x(6)+(x(6)+x(6))+(x(6)+x(6))+$$
$$+(x(6)+x(6)).$$

b_1-b_{17} hasonló felépítésűek, mint a_1-a_{17} csupán a $h(i)$ mennyiségek helyett az $x(i)$ mennyiségeket tartalmazzák.

$$m_i=a_ib_i\qquad 0\le i\le 18$$
$$u_0=m_0-m_{18}\quad u_1=m_1-m_5\quad u_2=m_4+m_6$$
$$u_3=m_1+m_3\quad u_4=m_2-m_6\quad u_5=m_2+m_3+m_4+$$
$$+m_5-m_8\quad u_6=u_0-u_3\quad u_7=u_0+u_5$$
$$y(0)=u_0+u_1-u_2-m_3+m_9+m_{13}$$
$$y(1)=u_0-u_1-u_2-m_2+m_{10}+m_{15}$$
$$y(2)=u_6+u_4-m_5+m_{12}+m_{14}$$
$$y(3)=u_6-u_4-m_4+m_7+m_{11}$$
$$y(4)=u_7+m_1-m_7-m_{10}-m_{13}+m_{16}$$
$$y(6)=u_7+m_6-m_9-m_{11}-m_{14}+m_{17}$$
$$y(5)=(m_0+m_0)+(m_0+m_0)+(m_0+m_0)+$$
$$+m_0-y(0)-y(1)-y(2)-y(3)-y(4)-y(5)-y(6).$$