VNIVERSITAS —SCIENTIARIUM—

Volumen 2 Nº1 JUL. - DIC. 1994

REVISTA DE LA FACULTAD DE CIENCIAS

PONTIFICIA UNIVERSIDAD JAVERIANA

SEMINARIO DE INVESTIGACION EN TRANSFORMADA RAPIDA DE FOURIER

IVÁN CASTRO-CHADID; FABIO MOLINA-FOCAZZIO; YOLIMA UMAÑA-HERNÁNDEZ; ALVARO DUQUE-HOYOS, S.J.; DIONISIO VILLALBA-ALDANA & PATRICIA HERNANDEZ-ROMERO

Seminario de investigación en transformada Rápida de Fourier, Facultad de Ciencias, Departamento de Matemáticas, Pontificia Universidad Javeriana, Santafé de Bogotá, Colombia, Cra. 7 # 43 - 82.

DEDUCCION MATEMATICA DE LAS PROPIEDADES DEL PRODUCTO DE KRONECKER

Resumen

Se presenta una deducción rigurosa de las propiedades relevantes del producto de Kronecker para matrices.

Abstract

A rigorous deduction of some of the main properties of the product of Kronecker for matrices is presented.

INTRODUCCION

El producto de Kronecker es una de las herramientas más importantes en el moderno tratamiento de la transformada rápida. Sus propiedades aritméticas permiten agilizar los procesos de cálculo y síntesis y a la vez facilitan la comprensión de procedimientos que serían muy dispendiosos sin el apoyo de este «producto matricial»; de ahí la necesidad de analizarlas y deducirlas.

DEFINICION :

Sean $A=(a_{ij}) \in \mathcal{M}_{n\times m}$ y $B=(b_{ij}) \in \mathcal{M}_{s\times t}$ matrices sobre un cuerpo $\mathbb{K}$ se define el producto de Kronecker de A y B como

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix}$$

LEMA 1:

$$[i/s] = \begin{cases} [(i-1)/s] & \text{si } s\nmid i \\ [(i-1)/s]+1 & \text{si } s \mid i \end{cases}$$

DEMOSTRACION :

1º Si $s\nmid i$ entonces $i=qs+r$ con $q,r \in \mathbb{Z}$ y $0<r<s$.
Es claro que $q=[i/s]$;restando 1 obtenemos $i-1=qs+r-1$ con $0 \leq r-1<s$ y, por la unicidad en la representación del algoritmo de la división,

tenemos que $q=\lfloor (i-1)/s \rfloor$, luego $\lfloor i/s \rfloor = \lfloor (i-1)/s \rfloor$.

2º Si $s|i$ entonces $i=\alpha s$ con $\alpha \in \mathbb{Z}$, luego

$$\lfloor (i-1)/s \rfloor = \lfloor \alpha - 1/s \rfloor = \alpha - 1 = \frac{i}{s} - 1 = \lfloor i/s \rfloor - 1$$

OBSERVACION :

Si

$$\mu(i,s) = \begin{cases} \lfloor i/s \rfloor + 1 & \text{si } s \nmid i \\ i/s & \text{si } s|i \end{cases}$$

entonces por el lema 1 tenemos que $\mu(i,s) = \lfloor (i-1)/s \rfloor + 1$.

TEOREMA 1:

Sean $A=(a_{ij}) \in \mathcal{M}_{n\times m}$ y $B=(b_{ij}) \in \mathcal{M}_{s\times t}$ matrices sobre un cuerpo $\mathbb{K}$. Si $A \otimes B = (d_{ij}) \in \mathcal{M}_{ns\times mt}$ entonces

$$d_{ij} = a_{\lfloor (i-1)/s \rfloor + 1 \; \lfloor (j-1)/t \rfloor + 1} \; b_{i-\lfloor (i-1)/s \rfloor s \; j-\lfloor (j-1)/t \rfloor t}.$$

DEMOSTRACION :

De la definición de producto de Kronecker se infiere que :

$$d_{ij} = \begin{cases} a_{\lfloor i/s \rfloor + 1 \; \lfloor j/t \rfloor + 1} \; b_{i-\lfloor i/s \rfloor s \; j-\lfloor j/t \rfloor t} & \text{si } s \nmid i \text{ y } t \nmid j \\ a_{\frac{i}{s} \; \lfloor j/t \rfloor + 1} \; b_{s \; j-\lfloor j/t \rfloor t} & \text{si } s|i \text{ y } t \nmid j \\ a_{\lfloor i/s \rfloor + 1 \; \frac{j}{t}} \; b_{i-\lfloor i/s \rfloor s \; t} & \text{si } s \nmid i \text{ y } t|j \\ a_{\frac{i}{s} \; \frac{j}{t}} \; b_{s \; t} & \text{si } s|i \text{ y } t|j \end{cases}$$

entonces aplicando lo visto en la observación anterior tenemos que

$$d_{ij} = {}^{a}\lfloor (i-1)/s \rfloor + 1 \ \lfloor (j-1)/t \rfloor + 1 \quad {}^{b}i - \lfloor (i-1)/s \rfloor s \ j - \lfloor (j-1)/t \rfloor t .$$

LEMA 2:

Si $x \in \mathbb{R}$ y $m \in \mathbb{Z}$ entonces $\lfloor x+m \rfloor = \lfloor x \rfloor + m$.

DEMOSTRACION :

$x+m = \lfloor x+m \rfloor + \mu$ con $0 \leq \mu < 1$. Por otra parte $x = \lfloor x \rfloor + \rho$ con $0 \leq \rho < 1$ de donde $x+m = \lfloor x \rfloor + m + \rho$,por consiguiente

$$\lfloor x+m \rfloor + \mu = \lfloor x \rfloor + m + \rho$$

de donde

$$\left| \lfloor x+m \rfloor - (\lfloor x \rfloor + m) \right| = | \rho - \mu |$$

como $0 \leq |\rho-\mu| < 1$ y $\left| \lfloor x+m \rfloor - (\lfloor x \rfloor + m) \right| \in \mathbb{Z}$ entonces $|\rho-\mu| = 0$;por lo tanto $\left| \lfloor x+m \rfloor - (\lfloor x \rfloor + m) \right| = 0$ lo cual implica que $\lfloor x+m \rfloor = \lfloor x \rfloor + m$.

LEMA 3:

Si $x \in \mathbb{R}$ y $m \in \mathbb{Z}_+$ entonces $\lfloor \lfloor x \rfloor / m \rfloor = \lfloor x/m \rfloor$.

DEMOSTRACION :

Si m=1 el lema se tiene. Si $m \neq 1$ como $x = \lfloor x \rfloor + v$ con $0 \leq v < 1$,entonces por el algoritmo de la división tenemos que existen p y q enteros tales que $\lfloor x \rfloor = p\,m + q$ con $0 \leq q \leq m-1$ entonces

$\frac{x}{m} = p + \frac{q+v}{m}$ luego $[x/m] = p$ ya que $0 \leq q+v<m$. Por otra parte $[[x]/m] = [(pm+q)/m] = p$. De donde $[[x]/m] = [x/m]$.

TEOREMA 2:

Sean $A=(a_{ij}) \in \mathcal{M}_{n \times m}$, $B=(b_{ij}) \in \mathcal{M}_{s \times t}$ y $C=(c_{ij}) \in \mathcal{M}_{p \times q}$ matrices sobre un cuerpo $\mathbb{K}$ entonces $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.

DEMOSTRACION :

Sea $(A \otimes B) \otimes C = (e_{ij})_{pns \times qmt}$ entonces

$$e_{ij} = {}^{d}[(i-1)/s]+1\ [(j-1)/t]+1\ \ {}^{c}i-[(i-1)/s]s\ j-[(j-1)/t]t$$

siendo

$$d_{ij} = {}^{a}[(i-1)/s]+1\ [(j-1)/t]+1\ \ {}^{b}i-[(i-1)/s]s\ j-[(j-1)/t]t$$

luego

$$e_{ij} = {}^{a}[[(i-1)/p]/s]+1\ [[(j-1)/q]/t]+1$$
$${}^{b}[(i-1)/p]+1-[[(i-1)/p]/s]s\ [(j-1)/q]+1-[[(j-1)/q]/t]t$$
$${}^{c}i-[(i-1)/p]p\ j-[(j-1)/q]q.$$

Por el lema 3,

$$[[(i-1)/p]/s] = [(i-1)/(ps)]$$

de donde

$$e_{ij} = {}^{a}[(i-1)/(ps)]+1\ [(j-1)/(qt)]+1$$
$${}^{b}[(i-1)/p]+1-[(i-1)/(ps)]s\ [(j-1)/q]+1-[(j-1)/(qt)]t$$

$$c_{i-[(i-1)/p]p\ j-[(j-1)/q]q}.$$

Por otra parte

$$B\otimes C=(f_{ij})_{sp\times tq} \quad \text{con}$$

$$f_{ij}= b_{[(i-1)/p]+1\ [(j-1)/q]+1}\ \ c_{i-[(i-1)/p]p\ j-[(j-1)/q]q}.$$

$$A\otimes(B\otimes C)=(g_{ij})_{nsp\times mtq} \quad \text{donde}$$

$$g_{ij}= a_{[(i-1)/(sp)]+1\ [(j-1)/(tq)]+1}\ \ f_{i-[(i-1)/(sp)]sp\ j-[(j-1)/(tq)]tq}$$

$$g_{ij}= a_{[(i-1)/(ps)]+1\ [(j-1)/(qt)]+1}$$
$$b_{[(i-[(i-1)/(sp)]sp-1)/p]+1\ [(j-[(j-1)/(qt)]qt-1)/q]+1}$$
$$c_{i-[(i-1)/(sp)]sp-[(i-[(i-1)/(sp)]sp-1)/p]p\ j-[(j-1)/(tq)]tq-[(j-[(j-1)/(tq)]tq-1)/p]p}.$$

Para tener la igualdad entre $e_{ij}=g_{ij}$ debemos probar que

$$[(i-1)/p]-[(i-1)/(ps)]s = [(i-[(i-1)/(sp)]sp-1)/p].$$

En efecto

$$[(i-[(i-1)/(sp)]sp-1)/p] = [(i-1)/p-[(i-1)/(sp)]s]$$
$$= [(i-1)/p]-[(i-1)/(sp)]s \quad \text{por el lema 2}$$

y por lo tanto $e_{ij}=g_{ij}$, de donde $(A\otimes B)\otimes C = A\otimes(B\otimes C)$.

TEOREMA 3:

Sean $A=(a_{ij})\in \mathcal{M}_{n\times m}$, $B=(b_{ij})\in \mathcal{M}_{s\times t}$ y $C=(c_{ij})\in \mathcal{M}_{s\times t}$ matrices sobre un cuerpo $\mathbb{K}$ entonces $A\otimes(B+C) = (A\otimes B)+(A\otimes C)$.

DEMOSTRACION :

Sea $A \otimes (B+C) = (h_{ij})_{ns \times mt}$ donde

$$h_{ij} = a_{\lfloor (i-1)/s \rfloor + 1 \; \lfloor (j-1)/t \rfloor + 1} \; e_{i-\lfloor (i-1)/s \rfloor s \; j-\lfloor (j-1)/t \rfloor t}$$

siendo

$$e_{ij} = b_{ij} + c_{ij}$$

luego

$$h_{ij} = a_{\lfloor (i-1)/s \rfloor + 1 \; \lfloor (j-1)/t \rfloor + 1} \; b_{i-\lfloor (i-1)/s \rfloor s \; j-\lfloor (j-1)/t \rfloor t} + a_{\lfloor (i-1)/s \rfloor + 1 \; \lfloor (j-1)/t \rfloor + 1} \; c_{i-\lfloor (i-1)/s \rfloor s \; j-\lfloor (j-1)/t \rfloor t}$$

el cual coincide con el término i,j de la matriz $(A \otimes B)+(A \otimes C)$.

TEOREMA 4:

Sean $A=(a_{ij}) \in \mathcal{M}_{n \times m}$, $B=(b_{ij}) \in \mathcal{M}_{s \times t}$ y $C=(c_{ij}) \in \mathcal{M}_{s \times t}$ matrices sobre un cuerpo $\mathbf{K}$ entonces $(B+C) \otimes A = (B \otimes A)+(C \otimes A)$.

DEMOSTRACION :

Similar a la del Teorema 3.

COROLARIO 1:

Sean $A=(a_{ij}) \in \mathcal{M}_{n \times m}$, $B=(b_{ij}) \in \mathcal{M}_{n \times m}$, $C=(c_{ij}) \in \mathcal{M}_{s \times t}$ y $D=(d_{ij}) \in \mathcal{M}_{s \times t}$ matrices sobre un cuerpo $\mathbf{K}$ entonces

$$(A+B) \otimes (C+D) = (A \otimes C)+(A \otimes D)+ (B \otimes C)+(B \otimes D).$$

DEMOSTRACION :

Consecuencia inmediata de los Teoremas 3 y 4.

TEOREMA 5:

Sean $A=(a_{ij}) \in \mathcal{M}_{n\times m}$, $B=(b_{ij}) \in \mathcal{M}_{s\times t}$, $C=(c_{ij}) \in \mathcal{M}_{m\times \beta}$ y $D=(d_{ij}) \in \mathcal{M}_{t\times \delta}$ matrices sobre un cuerpo K entonces

$$(A\otimes B)\ (C\otimes D) = AC\otimes BD.$$

DEMOSTRACION :

Sean $A\otimes B = (h_{ij}) \in \mathcal{M}_{ns\times mt}$ con

$$h_{ij}= a_{[(i-1)/s]+1\ [(j-1)/t]+1}\ \ b_{i-[(i-1)/s]s\ j-[(j-1)/t]t}$$

y $C\otimes D = (g_{ij}) \in \mathcal{M}_{mt\times \beta\delta}$ con

$$g_{ij}= c_{[(i-1)/t]+1\ [(j-1)/\delta]+1}\ \ d_{i-[(i-1)/t]t\ j-[(j-1)/\delta]\delta}.$$

Llamemos

$$(A\otimes B)\ (C\otimes D) =(f_{ij})_{ns\times \beta\delta}$$

en donde

$$f_{ij}=\sum_{k=1}^{mt} h_{ik}\ g_{kj}$$

$$=\sum_{k=1}^{mt} a_{[(i-1)/s]+1\ [(k-1)/t]+1}\ \ b_{i-[(i-1)/s]s\ k-[(k-1)/t]t} c_{[(k-1)/t]+1\ [(j-1)/\delta]+1}\ \ d_{k-[(k-1)/t]t\ j-[(j-1)/\delta]\delta}$$

Por otra parte

$$AC= (l_{ij})_{n\times\beta} \qquad l_{ij}=\sum_{k=1}^{m} a_{ik}c_{kj}$$

$$BD= (\rho_{ij})_{s\times\delta} \qquad \rho_{ij}=\sum_{k=1}^{t} b_{ik}d_{kj}$$

$$AC\otimes BD = (q_{ij})_{ns\times\beta\delta} \qquad q_{ij}= l_{\lceil(i-1)/s\rceil+1\ \lceil(j-1)/\delta\rceil+1}\ \rho_{i-\lceil(i-1)/s\rceil s\ j-\lceil(j-1)/\delta\rceil\delta}$$

luego

$$q_{ij}= \left(\sum_{k=1}^{m} a_{\lceil(i-1)/s\rceil+1\ k}\ c_{k\ \lceil(j-1)/\delta\rceil+1}\right)\left(\sum_{k=1}^{t} b_{i-\lceil(i-1)/s\rceil s\ k}\ d_{k\ j-\lceil(j-1)/\delta\rceil\delta}\right).$$

Se puede ver que tanto en q_{ij} como en f_{ij} hay $m\cdot t$ sumandos y que cada uno de ellos es un producto de $a_{ij}\cdot b_{lr}\cdot c_{vw}\cdot d_{z\sigma}$; además el sumando genérico de f_{ij} se puede obtener en q_{ij} reemplazando en la primera suma k por $\lceil(k-1)/t\rceil+1$, mientras que en la segunda k por $\lceil(k-1)/t\rceil t$.

COROLARIO 2:

Sean $A_\mu\in\mathcal{M}_{r_\mu\times m_\mu}$ y $B_\kappa\in\mathcal{M}_{m_\kappa\times t_\kappa}$ matrices sobre un cuerpo K entonces

$$(A_1\otimes A_2\otimes\cdots\otimes A_n)\ (B_1\otimes B_2\otimes\cdots\otimes B_n) = (A_1B_1)\otimes(A_2B_2)\otimes\cdots\otimes(A_nB_n).$$

DEMOSTRACION : *(Inducción)*

i) Para n=2 es el teorema anterior.

ii) Supongamos que se tiene para n-1; veámoslo para n

$$(A_1 \otimes A_2 \otimes \cdots \otimes A_n)(B_1 \otimes B_2 \otimes \cdots \otimes B_n) = ((A_1 \otimes A_2 \otimes \cdots \otimes A_{n-1}) \otimes A_n)((B_1 \otimes B_2 \otimes \cdots \otimes B_{n-1}) \otimes B_n)$$
$$= (A_1 \otimes A_2 \otimes \cdots \otimes A_{n-1})(B_1 \otimes B_2 \otimes \cdots \otimes B_{n-1}) \otimes A_n B_n$$
$$= ((A_1 B_1) \otimes (A_2 B_2) \otimes \cdots \otimes (A_{n-1} B_{n-1})) \otimes (A_n B_n).$$

NOTACION :

Notaremos $A^{[k]} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{k \text{ - veces}}$.

Del teorema anterior se obtiene $(AB)^{[k]} = A^{[k]} B^{[k]}$.

TEOREMA 6:

Sean $A=(a_{ij}) \in \mathcal{M}_{n \times n}$, $B=(b_{ij}) \in \mathcal{M}_{m \times m}$ entonces $Tra(A \otimes B) = Tra(A)\ Tra(B)$.

DEMOSTRACION :

Sea $A \otimes B = (d_{ij}) \in \mathcal{M}_{nm \times nm}$ entonces

$$Tra(A \otimes B) = \sum_{i=1}^{nm} d_{ii}$$
$$= \sum_{i=1}^{nm} a_{\lfloor (i-1)/m \rfloor + 1 \ \lfloor (i-1)/m \rfloor + 1} \ b_{i-\lfloor (i-1)/m \rfloor m \ j-\lfloor (j-1)/m \rfloor m}.$$

Sea $k = \lfloor (i-1)/m \rfloor + 1$ entonces los sumandos de la expresión anterior son de la forma

$$a_{kk}\ b_{i-(k-1)m \ \ i-(k-1)m}$$

si $1 \leq i \leq m$, entonces $k=1$, $a_{11}\ b_{ii}$

si $m+1 \leq i \leq 2m$, entonces $k=2$, $a_{22}\ b_{i-m \ i-m}$

si $2m+1 \leq i \leq 3m$, entonces $k=3$, $a_{33}\ b_{i-2m\ i-2m}$

si $(n-1)m+1 \leq i \leq nm$, entonces $k=n$ $a_{nn}\ b_{i-(n-1)m\ i-(n-1)m}$

por lo tanto

$$Tra(A \otimes B)=\sum_{i=1i=1}^{n}\sum^{m} a_{ii}\ b_{jj} = Tra(A)\ Tra(B).$$

TEOREMA 7:

Sean $A=(a_{ij}) \in \mathcal{M}_{n \times m}$ y $B=(b_{ij}) \in \mathcal{M}_{s \times t}$ matrices sobre un cuerpo $\mathbf{K}$ entonces $(A \otimes B)^T = A^T \otimes B^T$.

DEMOSTRACION :

Si $(A \otimes B)=(d_{ij})_{ns \times mt}$ entonces $(A \otimes B)^T =(d'_{ij})_{mt \times ns}$ siendo

$d'_{ij} = d_{ji}$, esto es,

$$d'_{ij} = a_{[(j-1)/s]+1\ [(i-1)/t]+1}\ b_{j-[(j-1)/s]s\ i-[(i-1)/t]t}.$$

Por otra parte, si $A^T=(a'_{ij})_{m \times n}$ donde $a'_{ij}=a_{ji}$ y $B^T=(b'_{ij})_{t \times s}$ donde

$b'_{ij}=b_{ji}$, entonces $A^T \otimes B^T =(l_{ij})_{mt \times ns}$ siendo

$$l_{ij} = a'_{[(i-1)/t]+1\ [(j-1)/s]+1}\ b'_{i-[(i-1)/t]t\ j-[(j-1)/s]s}$$

$$= a_{[(j-1)/s]+1\ [(i-1)/t]+1}\ b_{j-[(j-1)/s]s\ i-[(i-1)/t]t}$$

luego $l_{ij}=d'_{ij}$ y $(A\otimes B)^T = A^T\otimes B^T$.

TEOREMA 8:

Si A y B son matrices invertibles de orden n y m respectivamente, entonces $A\otimes B$ es invertible y además $(A\otimes B)^{-1}=A^{-1}\otimes B^{-1}$.

DEMOSTRACION :

$$\begin{aligned}(A\otimes B)(A^{-1}\otimes B^{-1}) &= AA^{-1}\otimes BB^{-1}\\ &= I_n\otimes I_m\\ &= I_{nm};\end{aligned}$$

de la misma forma se tiene que $(A^{-1}\otimes B^{-1})(A\otimes B)=I_{mn}$ y como la inversa es única entonces $(A\otimes B)^{-1}=A^{-1}\otimes B^{-1}$.

LEMA 4:

Sea A una matriz cuadrada, entonces:

A es invertible , si y solo si, AX=0 implica X=0.

DEMOSTRACION :

⇒) Evidente.

⇐) Sea σ_A la transformación lineal asociada a la matríz A mediante la base canónica.

$X\in Ker(\sigma_A)$ implica $\sigma_A(X)=0$ y por lo tanto como AX=0, entonces X=0. De donde $Ker(\sigma_A)=\{0\}$, luego σ_A es inyectiva y por ser una aplicación lineal de espacios vectoriales de la misma dimensión entonces es

biyectiva, por consiguiente σ_A es invertible lo cual demuestra que A es invertible.

LEMA 5:

Sean $X,Y \in \mathcal{M}_{n\times 1}$ tales que $X \otimes Y=0$ entonces X=0 o Y=0.

DEMOSTRACION :

Sean

$$X=\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \quad y \quad Y=\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

entonces

$$X \otimes Y = (d_i)_{nmx1} \quad \text{con } d_i = a_{[(i-1)/m]+1}\ b_{i-[(i-1)/m]m}$$

Como $d_i=0 \quad \forall\ i=1,\ldots,nm$ entonces $a_1Y=0$, $a_2Y=0,\ldots,a_nY=0$;

si alguno de los $b_i \neq 0$, entonces Y=0. Luego X=0 o Y=0.

TEOREMA 9:

Si A y B son matrices cuadradas tales que $A \otimes B$ es invertible, entonces A es invertible y B es invertible.

DEMOSTRACION :

Si B=0 entonces $A \otimes B = 0$ lo cual es una contradicción. Luego $B \neq 0$.
Tomemos $Y \in C^n$ tal que $BY \neq 0$ entonces $Y \neq 0$.
Sea X tal que AX=0, entonces, $AX \otimes BY=0$
Luego $(A \otimes B)(X \otimes Y)=0$, pero como $A \otimes B$ es invertible, entonces $X \otimes Y=0$.
De donde X=0, o, Y=0. Luego X=0 por lo tanto A es invertible. De la misma forma se ve que B es invertible.

BIBLIOGRAFIA

ραχξ ξλλ ωναλδ ν *The Fourier Transform and Its Applications*. χΓρα Θιλλ ωωκ ωμπανψ ξ Ψωρκ

λιωτ Δωυγλασ Φ αω αμαμωθαν *Fast Transforms. Academic Press, New York, 1982.*

λαθυτ ιχθαρδ *Fast Algorithms For Digital Signal Processing.* δδισων ξσλξψ Πυβλισθινγ ωμπανψ

ALGORITMO DE WINOGRAD PARA CALCULAR CONVOLUCIONES

Resumen

En este artículo se presenta el algoritmo de Winograd para calcular convoluciones de algunos polinomios, reduciendo aún más el número de multiplicaciones al contrastarlo con el cálculo directo de convoluciones.

Abstract

The Winograd algorithm to calculate some polynomial convolutions by redicing much more the number of multiplications, when contrasting it to the direct calculation of convolutions is presented in this article.

INTRODUCCION

El algoritmo de Winograd es uno de los más importantes de la familia de algoritmos conocida como «**Transformada rápida**». Se caracteriza por la reducción del número de multiplicaciones en los procesos en que participa.

En 1975 y 1976 el Dr. Shmuel Winograd del Instituto Thomas J. Watson de la I.B.M. publicó sendos artículos en la revista IEEE en donde presentó sus algoritmos. En 1978 dió un método general de construcción y probó importantes teoremas acerca de la no existencia de mejores algoritmos de convolución para los cuerpos de los números reales y complejos. A diferencia de los algoritmos precedentes el de Winograd se caracteriza por su generalidad.

En escencia, el método introducido por Winograd permite reducir el número de multiplicaciones al calcular el produto de dos polinomios módulo un tercer polinomio, y a partir de esta operación, describe la forma general de cualquier algoritmo destinado al cálculo del polinomio resultante. Apoyándose en la convolución, este resultado le permite obtener la Transformada Discreta de Fourier de longitud N, para valores pequeños de N.

DESCRIPCION DEL ALGORITMO

Queremos calcular la convolución de $g(x)$ y $d(x)$; para ésto, tomamos j polinomios $m^{(i)}(x)$ primos relativos dos a dos tales que

$$m(x)=m^{(1)}(x) \cdots m^{(j)}(x)$$

tenga grado mayor que el de $s(x)=g(x)d(x)$.

Llamemos

$$g^{(k)}(x) \equiv g(x) \bmod m^{(k)}(x) \quad \text{en donde } \partial g^{(k)}<\partial m^{(k)} \ \forall k=1,\cdots,j.$$

De la misma forma

$$d^{(k)}(x) \equiv d(x) \bmod m^{(k)}(x) \text{ en donde } \partial d^{(k)}<\partial m^{(k)} \ \forall k=1,\cdots,j$$

y

$$s^{(k)}(x) \equiv d^{(k)}(x)\ g^{(k)}(x) \mod m^{(k)}(x) \quad \text{en donde } \partial s^{(k)}<\partial m^{(k)} \ \forall k=1,\cdots,j.$$

Aplicando el teorema Chino de los restos se tiene que

$$s(x) \equiv \left(\sum_{k=1}^{j} a^{(k)}(x)\ s^{(k)}(x) \right) \bmod (m^{(1)}(x) \cdots m^{(j)}(x))$$

esto es,

$$s(x) \equiv \left(\sum_{k=1}^{j} a^{(k)}(x)\ s^{(k)}(x) \right) \bmod m(x)$$

en donde los $a^{(k)}(x)$ se encuentran de la siguiente forma:

como $\left(m^{(k)}(x)\ , \frac{m(x)}{m^{(k)}(x)}\right) = 1$, existen polinomios $t^{(k)}(x)$ y $h^{(k)}(x)$ tales que

$$t^{(k)}(x)\ m^{(k)}(x) + h^{(k)}(x)\ \frac{m(x)}{m^{(k)}(x)} = 1,$$

entonces

$$a^{(k)}(x) = h^{(k)}(x)\ \frac{m(x)}{m^{(k)}(x)}\ .$$

El objetivo es expresar los coeficientes de s(x) en función de los coeficientes de

$$\left(\sum_{k=1}^{j} a^{(k)}(x)\ s^{(k)}(x) \right) \bmod m(x)$$

y comparar la complejidad algorítmica en relación con la forma directa.

APLICACION DEL ALGORITMO

Sean

$g(x)=g_1x+g_0$ y $d(x)=d_2x^2+d_1x+d_0$;

tomemos

$m(x)=x(x-1)(x^2+1)$

como $\partial m=4$ entonces

$s(x) \equiv g(x)d(x) \bmod m(x)$ implica que $s(x) = g(x)d(x)$.

Llamemos $m^{(0)}(x) = x$, $m^{(1)}(x) = x-1$ y $m^{(2)}(x) = x^2+1$ entonces tenemos :

$d^{(0)}(x) \equiv (d_2x^2+d_1x+d_0) \bmod x$ de donde $d^{(0)}(x) = d_0$

$d^{(1)}(x) \equiv (d_2x^2+d_1x+d_0) \bmod (x-1)$

$d^{(1)}(x) \equiv (d_2(x^2-1)+d_1(x-1)+d_0+d_1+d_2) \bmod (x-1)$ entonces

$d^{(1)}(x) \equiv (d_0+d_1+d_2) \bmod (x-1)$ y por lo tanto $d^{(1)}(x) = d_0+d_1+d_2$

$d^{(2)}(x) \equiv (d_2x^2+d_1x+d_0) \bmod (x^2+1)$ luego

$d^{(2)}(x) \equiv (d_2(x^2+1)+d_1x+d_0-d_2) \bmod (x^2+1)$ y por lo tanto

$d^{(2)}(x) \equiv (d_1x+d_0-d_2) \bmod (x^2+1)$ lo cual implica que

$d^{(2)}(x) = d_1x+(d_0-d_2)$.

Resumiendo :

$$\begin{cases} d^{(0)}(x) = d_0 = d_0^{(0)} \\ d^{(1)}(x) = d_0+d_1+d_2 = d_0^{(1)} \\ d^{(2)}(x) = d_1x+(d_0-d_2) = d_1^{(2)}\, x + d_0^{(2)} \end{cases}$$

Por otra parte

$$\begin{aligned} g^{(0)}(x) &\equiv (g_1x+g_0) \bmod x \qquad \text{de donde } g^{(0)}(x) = g_0 \\ g^{(1)}(x) &\equiv (g_1x+g_0) \bmod (x-1) \\ g^{(1)}(x) &\equiv (g_1(x-1)+g_0+g_1) \bmod (x-1) \quad \text{entonces } g^{(1)}(x) = g_0+g_1 \\ g^{(2)}(x) &\equiv (g_1x+g_0) \bmod (x^2+1) \quad \text{entonces } g^{(2)}(x) = g_0+g_1x \ . \end{aligned}$$

Resumiendo :

$$\begin{cases} g^{(0)}(x) = g_0 = g_0^{(0)} \\ g^{(1)}(x) = g_0+g_1 = g_0^{(1)} \\ g^{(2)}(x) = g_1x+g_0 = g_1^{(2)}x+g_0^{(2)} \end{cases}$$

entonces

$$\begin{aligned} s^{(0)}(x) &= d^{(0)}(x)\, g^{(0)}(x) \equiv (d_0g_0) \bmod x \quad \text{así} \quad s^{(0)}(x) = d_0g_0 \\ s^{(1)}(x) &= d^{(1)}(x)g^{(1)}(x) \equiv (g_0+g_1)(d_0+d_1+d_2) \bmod x \quad \text{por lo tanto} \\ s^{(1)}(x) &= (g_0+g_1)(d_0+d_1+d_2) \\ s^{(2)}(x) &= d^{(2)}(x)g^{(2)}(x) \equiv (((d_0-d_2)+d_1x)\ (g_1x+g_0)) \bmod (x^2+1) \end{aligned}$$

de donde

$$s^{(2)}(x) \equiv (((d_0-d_2)g_0+(d_1g_0+g_1(d_0-d_2))x+d_1g_1(x^2+1)-d_1g_1) \bmod (x^2+1)$$

luego

$$s^{(2)}(x) \equiv (((d_0-d_2)g_0-d_1g_1)+(d_1g_0+g_1(d_0-d_2))x) \bmod (x^2+1)$$

Resumiendo :

$$\begin{cases} s^{(0)}(x) = d_0 g_0 = s_0^{(0)} \\ s^{(1)}(x) = (g_0+g_1)(d_0+d_1+d_2) = s_0^{(1)} \\ s^{(2)}(x) = ((d_0-d_2)g_0-d_1g_1) + (d_1g_0+g_1(d_0-d_2))x \\ \qquad = s_0^{(2)} + s_1^{(2)}\, x \end{cases}$$

como $$d^{(2)}(x) = \underbrace{(d_0-d_2)} + \underbrace{d_1}\, x$$

$$= d_0^{(2)} + d_1^{(2)}\, x$$

y $$g^{(2)}(x) = \underbrace{g_0} + \underbrace{g_1}\, x$$

$$= g_0^{(2)} + g_1^{(2)}$$

entonces

$$\begin{cases} s_0^{(2)} = d_0^{(2)}\, g_0^{(2)} - d_1^{(2)}\, g_1^{(2)} \\ s_1^{(2)} = d_0^{(2)}\, g_1^{(2)} + d_1^{(2)}\, g_0^{(2)} \end{cases}.$$

Como este resultado es idéntico al que se tiene al multiplicar números complejos, podemos utilizar el algoritmo de optimización de multiplicación de complejos.

Una representación matricial de este algoritmo es :

$$\begin{bmatrix} s_0^{(2)} \\ s_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} g_0^{(2)} & & \\ & g_1^{(2)} - g_0^{(2)} & \\ & & g_1^{(2)} + g_0^{(2)} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d_0^{(2)} \\ d_1^{(2)} \end{bmatrix} \quad (1)$$

de donde se tienen que hacer tan solo tres multiplicaciones.

De acuerdo con el algoritmo de Winograd tenemos que

$$s(x) \equiv \left(a^{(0)}(x)s^{(0)}(x) + a^{(1)}(x)s^{(1)}(x) + a^{(2)}(x)s^{(2)}(x)\right) \bmod \left(x(x-1)(x^2+1)\right)$$

en donde $a^{(0)}(x)$, $a^{(1)}(x)$ y $a^{(2)}(x)$ se calculan de la siguiente manera :

1•) $\left(x, \frac{m(x)}{x} \right) = 1$ esto es $\left(x, (x-1)(x^2+1) \right) = 1$. Por lo tanto existen polinomios $m^{(0)}(x)$ y $h^{(0)}(x)$ en $\mathbb{Q}[x]$ tales que

$$m^{(0)}(x)\, x + h^{(0)}(x)\, (x^3-x^2+x-1) = 1$$

por lo tanto

$$(x^2-x+1)\, x + (-1)\, (x^3-x^2+x-1) = 1$$

luego

$$a^{(0)}(x) = -x^3+x^2-x+1$$

2•) $\left(x-1, \frac{m(x)}{x-1} \right) = 1$ esto es $\left(x-1, x^3+x \right) = 1$. Por lo tanto existen polinomios $m^{(1)}(x)$ y $h^{(1)}(x)$ en $\mathbb{Q}[x]$ tales que

$$m^{(1)}(x)\ (x-1) + h^{(1)}(x)\ (x^3+x) = 1$$

pero

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

luego

$$\tfrac{1}{2}(x^3+x) + (-\tfrac{1}{2})\ (x^2+x+2)\ (x-1) = 1$$

de donde

$$a^{(1)}(x) = \tfrac{1}{2}\ (x^3+x)$$

3•) $\left(x^2+1,\ \frac{m(x)}{x^2+1} \right) = 1$ esto es $\left(x^2+1,\ x^2-x \right) = 1$. Por lo tanto existen polinomios $m^{(2)}(x)$ y $h^{(2)}(x)$ en $Q[x]$ tales que

$$m^{(2)}(x)\ (x^2+1) + h^{(2)}(x)\ (x^2-x) = 1$$

pero

$$(-\tfrac{1}{2})(x-2)\ (x^2+1) + (\tfrac{1}{2})\ (x^2-x)\ (x-1) = 1$$

de donde

$$a^{(2)}(x) = \tfrac{1}{2}\ (x^2-x)(x-1) = \tfrac{1}{2}\ (x^3-2x^2+x)\ .$$

De lo anterior se desprende que

$$s(x) \equiv \left((-x^3+x^2-x+1)s^{(0)}(x) + \tfrac{1}{2}(x^3+x)s^{(1)}(x) + \tfrac{1}{2}(x^3-2x^2+x)\ s^{(2)}(x)\right) \bmod \left(x(x-1)\ (x^2+1)\right)$$

esto es,

$$s(x) \equiv \left((-x^3+x^2-x+1)s_0^{(0)} + \tfrac{1}{2}(x^3+x)s_0^{(1)} + \tfrac{1}{2}(x^3-2x^2+x)\ (s_0^{(2)}+s_1^{(2)}x)\right) \bmod m(x)$$

como $x^4 = m(x) + x^3 - x^2 + x$ entonces reemplazando obtenemos

$$\left(s_3x^3+s_2x^2+s_1x+s_0\right) \equiv \left(\left(-s_0^{(0)}+\frac{1}{2}s_0^{(1)}+\frac{1}{2}s_0^{(2)}-\frac{1}{2}s_1^{(2)}\right)x^3 + \left(s_0^{(0)}-s_0^{(2)}\right)x^2 + \left(-s_0^{(0)}+\frac{1}{2}s_0^{(1)}+\frac{1}{2}s_0^{(2)}+\frac{1}{2}s_1^{(2)}\right)x + s_0^{(0)} \right) \bmod m(x) .$$

Como ambos polinomios de la congruencia son de grado menor o igual a 3 y el grado de m(x) es cuatro, entonces la congruencia se convierte en una igualdad y por lo tanto :

$$\begin{cases} s_0 = s_0^{(0)} \\ s_1 = -s_0^{(0)}+\frac{1}{2}s_0^{(1)}+\frac{1}{2}s_0^{(2)}+\frac{1}{2}s_1^{(2)} \\ s_2 = s_0^{(0)}-2\frac{1}{2}s_0^{(2)} \\ s_3 = -s_0^{(0)}+\frac{1}{2}s_0^{(1)}+\frac{1}{2}s_0^{(2)}-\frac{1}{2}s_1^{(2)} \end{cases}$$

siendo

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 1 \\ 1 & 0 & -2 & 0 \\ -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} s_0^{(0)} \\ \frac{1}{2}s_0^{(1)} \\ \frac{1}{2}s_0^{(2)} \\ \frac{1}{2}s_1^{(2)} \end{bmatrix} \qquad (2)$$

la representación matricial de estas ecuaciones.

Por otra parte como

$$\begin{cases} d_0 = d_0^{(0)} \\ d_0+d_1+d_2 = d_0^{(1)} \\ d_1x+(d_0-d_2) = d_1^{(2)}\ x + d_0^{(2)} \end{cases}$$

entonces

$$\begin{bmatrix} d_0^{(0)} \\ d_0^{(1)} \\ d_0^{(2)} \\ d_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix} \qquad (3)$$

a partir de lo anterior definimos un vector columna integrado por los elementos D_0, D_1, D_2, D_3 y D_4 en donde :

$$\begin{bmatrix} D_0 \\ D_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d_0^{(0)} \\ d_0^{(1)} \end{bmatrix}$$

y de acuerdo con (1)

$$\begin{bmatrix} D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d_0^{(2)} \\ d_1^{(2)} \end{bmatrix}$$

de modo que la representación matricial del vector es :

$$\begin{bmatrix} D_0 \\ D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} \begin{bmatrix} d_0^{(0)} \\ d_0^{(1)} \\ d_0^{(2)} \\ d_1^{(2)} \end{bmatrix}$$

y aplicando (3) tenemos:

$$\begin{bmatrix} D_0 \\ D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

que una vez efectuando la multiplicación, queda

$$\begin{bmatrix} D_0 \\ D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix} \qquad (4)$$

y de la misma manera al considerar

$$\begin{cases} g^{(0)}(x) = g_0 = g_0^{(0)} \\ g^{(1)}(x) = g_0+g_1 = g_0^{(1)} \\ g^{(2)}(x) = g_1x+g_0 = g_1^{(2)}\ x + g_0^{(2)} \end{cases}$$

se llega a

$$\begin{bmatrix} g_0^{(0)} \\ g_0^{(1)} \\ g_0^{(2)} \\ g_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \end{bmatrix} \qquad (5)$$

pero como

$$\begin{bmatrix} g_0^{(0)} \\ g_0^{(1)} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} g_0^{(0)} \\ g_0^{(1)} \end{bmatrix}$$

y de (1) podemos deducir

$$\begin{bmatrix} g_0^{(2)} \\ g_1^{(2)} - g_0^{(2)} \\ g_1^{(2)} + g_0^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} g_0{}^{(2)} \\ g_1{}^{(2)} \end{bmatrix}$$

entonces

$$\begin{bmatrix} g_0^{(0)} \\ g_0^{(1)} \\ g_0^{(2)} \\ g_1^{(2)}-g_0^{(2)} \\ g_1^{(2)}+g_0^{(2)} \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 1 & 1 \end{bmatrix} \end{bmatrix} \begin{bmatrix} g_0^{(0)} \\ g_0^{(1)} \\ g_0^{(2)} \\ g_1^{(2)} \end{bmatrix} \qquad (6).$$

En forma similar a como lo hicimos con los D_k y apoyándonos en (5) y (6) vamos a definir un vector columna integrado por los elementos G_0, G_1, G_2, G_3 y G_4 de la siguiente manera:

$$\begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \\ G_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \end{bmatrix}$$

por lo tanto :

$$\begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \\ G_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \end{bmatrix}$$

finalmente definamos :

$$\begin{cases} S_0 = G_0D_0 = g_0^{(0)}d_0^{(0)} \\ S_1 = G_1D_1 = \frac{1}{2}\, g_0^{(1)}d_0^{(1)} \\ S_2 = G_2D_2 = \frac{1}{2}\, g_0^{(2)}(d_0^{(2)}+d_1^{(2)}) \\ S_3 = G_3D_3 = \frac{1}{2}(g_1^{(2)} - g_0^{(2)})d_0^{(2)} \\ S_4 = G_4D_4 = \frac{1}{2}(g_1^{(2)}+g_0^{(2)})d_1^{(2)} \end{cases}$$

luego

$$\begin{bmatrix} 2S_2 \\ 2S_3 \\ 2S_4 \end{bmatrix} = \begin{bmatrix} g_0^{(2)} & & \\ & g_1^{(2)} - g_0^{(2)} & \\ & & g_1^{(2)} + g_0^{(2)} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d_0^{(2)} \\ d_1^{(2)} \end{bmatrix}$$

pero de acuerdo con lo visto en (1) tenemos :

$$\begin{bmatrix} s_0^{(2)} \\ s_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2S_2 \\ 2S_3 \\ 2S_4 \end{bmatrix} \qquad (7)$$

por otra parte

$$\begin{cases} s_0^{(0)} = g_0^{(0)} d_0^{(0)} = S_0 \\ s_0^{(1)} = g_0^{(1)} d_0^{(1)} = 2S_1 \end{cases} \tag{8}$$

de (7) y (8) se desprende que :

$$\begin{bmatrix} s_0^{(0)} \\ s_0^{(1)} \\ s_0^{(2)} \\ s_1^{(2)} \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix} \end{bmatrix} \begin{bmatrix} S_0 \\ 2S_1 \\ 2S_2 \\ 2S_3 \\ 2S_4 \end{bmatrix}$$

como

$$\begin{bmatrix} s_0^{(0)} \\ \frac{1}{2}s_0^{(1)} \\ \frac{1}{2}s_0^{(2)} \\ \frac{1}{2}s_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} s_0^{(0)} \\ s_0^{(1)} \\ s_0^{(2)} \\ s_1^{(2)} \end{bmatrix}$$

y

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

entonces

$$\begin{bmatrix} s_0^{(0)} \\ \frac{1}{2}s_0^{(1)} \\ \frac{1}{2}s_0^{(2)} \\ \frac{1}{2}s_1^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$$

reemplazando en (2) obtenemos :

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 1 \\ 1 & 0 & -2 & 0 \\ -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & -1 \\ 1 & 0 & -2 & 0 & 2 \\ -1 & 1 & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & -1 \\ 1 & 0 & -2 & 0 & 2 \\ -1 & 1 & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} G_0D_0 \\ G_1D_1 \\ G_2D_2 \\ G_3D_3 \\ G_2D_4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & -1 \\ 1 & 0 & -2 & 0 & 2 \\ -1 & 1 & 0 & -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} G_0 & 0 & 0 & 0 & 0 \\ 0 & G_1 & 0 & 0 & 0 \\ 0 & 0 & G_2 & 0 & 0 \\ 0 & 0 & 0 & G_3 & 0 \\ 0 & 0 & 0 & 0 & G_4 \end{bmatrix} \begin{bmatrix} D_0 \\ D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix}$$

pero, de acuerdo con lo visto en (4), podemos reemplazar el vector de las D_i para obtener la representación matricial del algoritmo de Winograd para este ejemplo particular.

En el siguiente cuadro vamos a presentar en forma sintética todo el procedimiento que hemos logrado desarrollar :

ALGORITMO DE WINOGRAD PARA CALCULAR LA CONVOLUCION

$s(x)= s_3x^3+s_2x^2+s_1x+s_0$ DE $g(x)=g_1x+g_0$ Y $d(x)=d_2x^2+d_1x+d_0$

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & -1 \\ 1 & 0 & -2 & 0 & 2 \\ -1 & 1 & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} G_0 & 0 & 0 & 0 & 0 \\ 0 & G_1 & 0 & 0 & 0 \\ 0 & 0 & G_2 & 0 & 0 \\ 0 & 0 & 0 & G_3 & 0 \\ 0 & 0 & 0 & 0 & G_4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

en donde

$$\begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \\ G_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \end{bmatrix} .$$

Por otra parte, como

$$\begin{cases} s_0 = S_0 \\ s_1 = -S_0+S_1+2S_2+S_3-S_4 \\ s_2 = S_0-2S_2+2S_4 \\ s_3 = -S_0+S_1-S_3-S_4 \end{cases} \tag{9}$$

entonces haciendo

$$c_1=S_4-S_2 \quad y \quad c_3=S_3+S_4$$

se tiene que

$$\begin{cases} s_0 = S_0 \\ s_2 = S_4-S_2+S_4-S_2+S_0 = c_1+c_1+s_0 \\ s_1 = S_1+S_3+S_4-S_0+2S_2-2S_4=S_1+c_3-s_2 \\ s_3 = -(S_3+S_4)-S_0+S_1=-c_3-S_0+S_1 \end{cases} \tag{10}$$

donde podemos observar que el número de adiciones pasa de ser 12 en (9) a 8 en (10).

Como el producto matricial

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

genera 4 adiciones (ya que d_0+d_1 aparece dos veces) entonces el algoritmo de Winograd requiere exactamente de:

5 multiplicaciones
12 adiciones .

VARIACIONES DEL ALGORITMO

Al emplear el algoritmo de Winograd para calcular la convolución se elige un polinomio m(x) con ∂m>∂s. Es posible en algunos casos seleccionar el polinomio m(x) de tal forma que el ∂m=∂s y apoyándose en procedimientos similares (aunque no iguales), a los empleados en el algoritmo de Winograd obtener nuevos algoritmos que sean más eficientes. Veamos dos ejemplos.

EJEMPLO 1:

Sean

$$g(x)=g_1x+g_0 \quad y \quad d(x)=d_2x^2+d_1x+d_0;$$

calcular la convolución $s(x)= s_3x^3+s_2x^2+s_1x+s_0$ de $g(x)$ y $f(x)$.

DESARROLLO :

Tomemos $m(x)=x(x-1)(x+1)$, llamemos $m^{(0)}(x) = x$, $m^{(1)}(x) = x-1$ y

$m^{(2)}(x) = x+1$ entonces :

1•) $\left(x, \frac{m(x)}{x} \right) = 1$, esto es $\left(x, (x-1)(x+1) \right) = 1$. Por lo tanto

$$x\, x + (-1)(x-1)(x+1) = 1$$

luego

$$a^{(0)}(x) = -(x^2-1).$$

2•) $\left(x-1, \frac{m(x)}{x-1} \right) = 1$, esto es $\left(x-1, x(x+1) \right) = 1$. Por lo tanto

$$\left(-\frac{1}{2} \right) (x+2)\ (x-1) + \left(\frac{1}{2} \right) x\ (x+1) = 1$$

luego

$$a^{(1)}(x) = \frac{1}{2}\ x\ (x+1).$$

3•) $\left(x+1,\ \frac{m(x)}{x+1} \right) = 1$ esto es $\left(x+1,\ x\ (x-1) \right) = 1.$

$$\left(-\frac{1}{2} \right) (x-2)\ (x+1) + \left(\frac{1}{2} \right) x\ (x-1) = 1$$

luego

$$a^{(2)}(x) = \frac{1}{2}\ x\ (x-1).$$

Ahora introducimos cuatro constantes S_0, S_1, S_2 y S_3 tales que

$$s(x) = a^{(0)}(x)\ S_0 + a^{(1)}(x)\ S_1 + a^{(2)}(x)\ S_2 + m(x)\ S_3 \quad \text{entonces}$$

$$s_3x^3+s_2x^2+s_1x+s_0 = (-x^2+1)\ S_0 + (x^2+x)\ \frac{S_1}{2} + (x^2-x)\ \frac{S_2}{2} + (x^3-x)\ S_3 \quad (1)$$

luego

$$\begin{cases} s_0 = S_0 \\ s_1 = \dfrac{S_1}{2} - \dfrac{S_2}{2} - S_3 \\ s_2 = -S_0 + \dfrac{S_1}{2} + \dfrac{S_2}{2} \\ s_3 = S_3 \end{cases}$$

que en forma matricial es :

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} S_0 \\ \frac{1}{2}S_1 \\ \frac{1}{2}S_2 \\ S_3 \end{bmatrix}$$

pero como $s(x) = (g_1x+g_0)(d_2x^2+d_1x+d_0)$ entonces:

i) $s(0)=g_0d_0$ pero en (1) $s(0)=s_0=S_0$ de donde
$$S_0=g_0d_0.$$

ii) $s(1)=(g_1+g_0)(d_2+d_1+d_0)$ como en (1) $s(1)=S_1$ entonces
$$S_1=(g_1+g_0)(d_2+d_1+d_0).$$

iii) $s(-1)=(-g_1+g_0)(d_2-d_1+d_0)$ puesto que en (1) $s(-1)=S_2$ se obtiene
$$S_2=(g_0-g_1)(d_2-d_1+d_0).$$

Por otra parte, por lo visto en (1) tenemos que $S_3=s_3=g_1d_2$. Resumiendo, finalmente llegamos a que

$$\begin{cases} S_0 = g_0d_0 \\ \frac{1}{2}S_1 = \dfrac{(g_0+g_1)}{2}(d_2+d_1+d_0) \\ \frac{1}{2}S_2 = \dfrac{(g_0-g_1)}{2}(d_2-d_1+d_0) \\ S_3 = g_1d_2 \end{cases}$$

escrito en forma matricial tenemos :

$$\begin{bmatrix} S_0 \\ \frac{1}{2}S_1 \\ \frac{1}{2}S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} g_0 & & & \\ & \frac{g_0+g_1}{2} & & \\ & & \frac{g_0-g_1}{2} & \\ & & & g_1 \end{bmatrix} \begin{bmatrix} d_0 \\ d_0+d_1+d_2 \\ d_0-d_1+d_2 \\ d_2 \end{bmatrix}$$

$$= \begin{bmatrix} g_0 & & & \\ & \frac{g_0+g_1}{2} & & \\ & & \frac{g_0-g_1}{2} & \\ & & & g_1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

por lo tanto

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} g_0 & & & \\ & \frac{g_0+g_1}{2} & & \\ & & \frac{g_0-g_1}{2} & \\ & & & g_1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

y así este algoritmo requiere exactamente de:

4 multiplicaciones
7 adiciones

EJEMPLO 2:

Sean

$$g(x)=g_2x^2+g_1x+g_0 \quad y \quad d(x)=d_2x^2+d_1x+d_0;$$

calcular la convolución $s(x)= s_4x^4+s_3x^3+s_2x^2+s_1x+s_0$ de $g(x)$ y $f(x)$.

DESARROLLO:

Tomemos $m(x)=x(x-1)(x+1)(x-2) = x^4-2x^3-x^2+2x$, llamemos

$m^{(0)}(x) = x$, $m^{(1)}(x) = x-1$, $m^{(2)}(x) = x+1$ y $m^{(3)}(x) = x+2$, entonces :

1•) $\left(x, \frac{m(x)}{x} \right) = 1$, esto es $\left(x, (x-1)(x+1)(x+2) \right) = 1$. Por lo tanto

$$\frac{1}{2}x\ (-x^2+2x+1) + \frac{1}{2}(x-1)(x+1)(x-2) = 1$$

luego

$$a^{(0)}(x) = \frac{1}{2}(x-1)(x+1)(x-2) = \frac{1}{2}(x^3-2x^2-x+2).$$

2•) $\left(x-1, \frac{m(x)}{x-1} \right) = 1$, esto es $\left(x-1, x(x+1)(x-2) \right) = 1$. Por lo tanto

$$\frac{1}{2}\ (x^2-2)\ (x-1) + \left(-\frac{1}{2}\right) x\ (x+1)\ (x-2) = 1$$

luego

$$a^{(1)}(x) = \left(-\frac{1}{2}\right) x\ (x+1)(x-2) = \left(-\frac{1}{2}\right)(x^3-x^2-2x).$$

3•) $\left(x+1, \frac{m(x)}{x+1} \right) = 1$, esto es $\left(x+1, x\,(x-1)(x-2) \right) = 1$. Por lo tanto

$$\left(-\frac{1}{6}\right)(-x^2+4x-6)\,(x+1) + \left(-\frac{1}{6}\right) x\,(x-1)(x-2) = 1$$

luego

$$a^{(2)}(x) = \left(-\frac{1}{6}\right) x\,(x-1)(x-2) = \left(-\frac{1}{6}\right)(x^3-3x^2+2x).$$

4•) $\left(x-2, \frac{m(x)}{x-2} \right) = 1$, esto es $\left(x-2, x\,(x-1)(x+1) \right) = 1$. Por lo tanto

$$\left(-\frac{1}{6}\right)(x^2+2x+3)\,(x-2) + \frac{1}{6} x\,(x-1)(x+1) = 1$$

luego

$$a^{(3)}(x) = \frac{1}{6}(x^2-x)(x+1) = \frac{1}{6}(x^3-x).$$

Ahora introducimos cinco constantes S_0, S_1, S_2, S_3 y S_4 tales que

$$s(x) = a^{(0)}(x)\,S_0 + a^{(1)}(x)\,S_1 + a^{(2)}(x)\,S_2 + a^{(3)}(x)\,S_3 + m(x)\,S_4$$

en consecuencia

$$\begin{aligned} s_4x^4+s_3x^3+s_2x^2+s_1x+s_0 = {} & (x^3-2x^2-x+2)\,\frac{S_0}{2} + (-x^3+x^2+2x)\,\frac{S_1}{2} + \\ & (-x^3+3x^2-2x)\,\frac{S_2}{6} + (x^3-x)\,\frac{S_3}{6} + \\ & S_4\,(x^4-2x^3-x^2+2x) \end{aligned} \qquad (2)$$

luego

$$\begin{cases} s_0 = 2\left(\frac{S_0}{2}\right) \\ s_1 = (-1)\left(\frac{S_0}{2}\right) + 2\left(\frac{S_1}{2}\right) + (-2)\left(\frac{S_2}{6}\right) + (-1)\left(\frac{S_3}{6}\right) + 2\,S_4 \\ s_2 = (-2)\left(\frac{S_0}{2}\right) + 1\left(\frac{S_1}{2}\right) + 3\left(\frac{S_2}{6}\right) + (-1)\,S_4 \\ s_3 = 1\left(\frac{S_0}{2}\right) + (-1)\left(\frac{S_1}{2}\right) + (-1)\left(\frac{S_2}{6}\right) + 1\left(\frac{S_3}{6}\right) + (-2)\,S_4 \\ s_4 = S_4 \end{cases}$$

en forma matricial queda :

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ -1 & 2 & -2 & -1 & 2 \\ -2 & 1 & 3 & 0 & -1 \\ 1 & -1 & -1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2}S_0 \\ \frac{1}{2}S_1 \\ \frac{1}{6}S_2 \\ \frac{1}{6}S_3 \\ S_4 \end{bmatrix} .$$

Pero como $s(x) = (g_2x^2+g_1x+g_0)(d_2x^2+d_1x+d_0)$ entonces:

i) $s(0)=g_0d_0$ pero en (2) $s(0)=s_0=S_0$ de donde

$$S_0=g_0d_0$$

ii) $s(1)=(g_2+g_1+g_0)(d_2+d_1+d_0)$ pero en (2) $s(1)=S_1$ de donde

$$S_1=(g_2+g_1+g_0)(d_2+d_1+d_0)$$

iii) $s(-1)=(g_2-g_1+g_0)(d_2-d_1+d_0)$ pero en (2) $s(-1)=S_2$ de donde

$$S_2=(g_2-g_1+g_0)(d_2-d_1+d_0)$$

iv) $s(2)=(4g_2+2g_1+g_0)(4d_2+2d_1+d_0)$ pero en (2) $s(2)=S_3$ de donde
$S_3=(4g_2+2g_1+g_0)(4d_2+2d_1+d_0)$;

por otra parte, por lo visto en (2) se observa que $S_4=s_4=g_2d_2$. Resumiendo, tenemos finalmente que

$$\begin{cases} \frac{S_0}{2} = \frac{1}{2}g_0d_0 \\ \frac{S_1}{2} = \frac{1}{2}(g_2+g_1+g_0)(d_2+d_1+d_0) \\ \frac{S_2}{6} = \frac{1}{6}(g_2-g_1+g_0)(d_2-d_1+d_0) \\ \frac{S_3}{6} = \frac{1}{6}(4g_2+2g_1+g_0)(4d_2+2d_1+d_0) \\ S_4 = g_2d_2 \end{cases}$$

que escrito en forma matricial nos da:

$$\begin{bmatrix} \frac{1}{2}S_0 \\ \frac{1}{2}S_1 \\ \frac{1}{6}S_2 \\ \frac{1}{6}S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}g_0 & & & & \\ & \frac{g_0+g_1+g_2}{2} & & & \\ & & \frac{g_0-g_1+g_2}{6} & & \\ & & & \frac{g_0+2g_1+4g_2}{6} & \\ & & & & g_2 \end{bmatrix} \begin{bmatrix} d_0 \\ d_0+d_1+d_2 \\ d_0-d_1+d_2 \\ d_0+2d_1+4d_2 \\ d_2 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{2}g_0 & & & & \\ & \frac{g_0+g_1+g_2}{2} & & & \\ & & \frac{g_0-g_1+g_2}{6} & & \\ & & & \frac{g_0+2g_1+4g_2}{6} & \\ & & & & g_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

por lo tanto

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ -1 & 2 & -2 & -1 & 2 \\ -2 & 1 & 3 & 0 & -1 \\ 1 & -1 & -1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2}g_0 & & & & \\ & \frac{g_0+g_1+g_2}{2} & & & \\ & & \frac{g_0-g_1+g_2}{6} & & \\ & & & \frac{g_0+2g_1+4g_2}{6} & \\ & & & & g_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \end{bmatrix}$$

Al contar detalladamente se puede observar que este algoritmo requiere exactamente de:

5 multiplicaciones
20 adiciones

las 7 preadiciones se obtienen de la siguiente manera:

$$\begin{aligned} d_0+d_1+d_2 &= d_0+(d_1+d_2) \\ d_0-d_1+d_2 &= d_0+(d_2-d_1) \\ d_0+2d_1+4d_2 &= (d_1+d_2)+(d_1+d_2)+(d_2-d_1)+(d_0+d_1+d_2); \end{aligned}$$

para calcular cuantas postadiciones hay, procedemos de la siguiente manera :

Sea

$$\begin{bmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ T_4 \end{bmatrix}$$

el resultado de multiplicar las últimas tres matrices de la expresión matricial final, entonces las postadiciones se obtienen al efectuar el producto siguiente:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ -1 & 2 & -2 & -1 & 2 \\ -2 & 1 & 3 & 0 & -1 \\ 1 & -1 & -1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ T_4 \end{bmatrix}$$

luego

$$
\begin{aligned}
s_0 &= T_0+T_0 \\
s_1 &= (T_1+T_1)-(T_2+T_2)+((T_4+T_4)-T_0-T_3) \\
s_2 &= -(T_0+T_0)+(T_2+T_2)+(T_1+T_2)-T_4 \\
s_3 &= -((T_4+T_4)-T_0-T_3)-(T_1+T_2) \\
s_4 &= T_4
\end{aligned}
$$

por lo tanto hay 13 postadiciones.

REFERENCIAS

BLAHUT, R.E. 1987. Fast algorithms for digital signal processing. Addison-Wesley Publishing Company.

ELIOT, D.F. & RAO, K,R. 1982. Fast transforms algorithms, analyses, applications. Academic Press, New York.

WINOGRAD, S. 1978. «On computing the discrete fast Fourier transform». Math. Comp. 32:175-199.

FUNDAMENTACION MATEMATICA DE LA REVERSION DIGITAL

Resumen

Se presenta una dedución rigurosa de la reversión digital de un entero en cualquier base.

Abstract

A rigorous deduction of the digit reversal of an integer in any base is presented.

INTRODUCCION

En algunos procesos de Transformada Rápida de Fourier los datos se permutan para facilitar los cálculos orientados a la disminución del número de operaciones aritméticas, así como también la reducción del tiempo computacional.

Este tipo de permutación presenta un vector de datos cuyos elementos están ubicados en puestos que corresponden a desarrollos en una base fija del número en cuestión, pero con los coeficientes en el orden inverso. El algoritmo que se desarrolla en el presente artículo, permite restituir de una manera eficiente el orden perdido en el manejo de estos datos. Se adjunta el respectivo programa en BASIC.

DEFINICION 1:

Sea $b \in \mathbb{Z}^+$, $b>1$ y $A \in \mathbb{Z}^+$, si el desarrollo en base b de A es:

$$A=a_{n-1}a_{n-2}\cdots a_1a_0 \qquad 0 \le a_i \le b-1$$

se define el elemento reverso de A en base b como el entero c cuyo desarrollo en base b es:

$$c=a_0a_1\cdots a_{n-2}a_{n-1}\ .$$

OBSERVACION:

Recordemos que $A=a_{n-1}a_{n-2}\cdots a_1a_0$ es la expresión en base b de:

$$A=a_{n-1}b^{n-1}+a_{n-2}b^{n-2}+\cdots+a_1b+a_0 \qquad 0 \le a_i \le b-1\ .$$

LEMISCO:

Sean $A=a_{n-1}a_{n-2}\cdots a_1a_0$ con $0 \le a_i \le b-1$ y $K=a_{n-2}a_{n-3}\cdots a_1a_0a_{n-1}$ entonces

$$K=bA+(1-b^n)\ [A/b^{n-1}]\ .$$

TEOREMA:

Sean A y D los enteros cuyos desarrollos en base b son:

$$A=a_{n-(k+1)}a_{n-(k+2)}\ \cdots\ a_0a_{n-k}a_{n-(k-1)}\ \cdots\ a_{n-1} \qquad y$$

$$D=a_{n-(k+2)}a_{n-(k+3)}\ \cdots\ a_0a_{n-(k+1)}a_{n-k}\ \cdots\ a_{n-1}$$

con $0 \leq a_i \leq b-1$.

Entonces

$$D=(b^{k+1}-b^k)[A/b^k]\ +(b^k-b^n)\ [A/b^{n-1}]+A \qquad \forall k \geq 0$$

DEMOSTRACION :

Sabemos que $[A/b^k] = a_{n-(k+1)}a_{n-(k+2)}\ \cdots\ a_0$. Por el LEMISCO tenemos que

$$b[A/b^k]\ +\ (1-b^{n-k})[[A/b^k]/b^{n-k-1}] = a_{n-(k+2)}a_{n-(k+3)}\ \cdots\ a_0a_{n-(k+1)}$$

pero como

$$[[A/b^k]/b^{n-k-1}]=[A/b^{n-1}]$$

entonces

$$b[A/b^k]\ +\ (1-b^{n-k})[A/b^{n-1}]=a_{n-(k+2)}a_{n-(k+3)}\ \cdots\ a_0a_{n-(k+1)}$$

luego

$$b^k\Big(b[A/b^k]\ +\ (1-b^{n-k})[A/b^{n-1}]\Big)=a_{n-(k+2)}a_{n-(k+3)}\ \cdots\ a_0a_{n-(k+1)}\ \underbrace{0\ \cdots\ 0}_{k\ \text{ceros}};$$

por otra parte se tiene

$$A-b^k\lfloor A/b^k\rfloor = a_{n-k}\ a_{n-(k-1)}\cdots a_{n-1}$$

de donde

$$D = b^{k+1}\lfloor A/b^k\rfloor + (b^k-b^n)\ \lfloor A/b^{n-1}\rfloor + A-b^k\lfloor A/b^k\rfloor$$

esto es

$$D = (b^{k+1}-b^k)\lfloor A/b^k\rfloor + (b^k-b^n)\ \lfloor A/b^{n-1}\rfloor + A\ .$$

PROGRAMA EN BASIC PARA CALCULAR EL ELEMENTO REVERSO DE UN ENTERO EN BASE b

```
CLS
PRINT TAB(10); " CALCULO DEL ELEMENTO REVERSO EN BASE b DE K
PARA
                0 ≤ K ≤ (b^n)-1 "
PRINT
INPUT "      TECLEE LA BASE     b = ", B
INPUT "      TECLEE EL EXPONENTE n = ", N
PRINT
FOR W = 0 TO B ^ N - 1
                A = W
                GOSUB PROCESO
                PRINT TAB(10); "A("; TAB(12); W; TAB(18); ") = ";
```

```
                    TAB(22); D
                NEXT W
END

PROCESO:
FOR K = 0 TO N - 2
                D = (B^(K+1)-B^K)*INT(A/B^K)+(B^K-B^N)*INT(A/B^(N-1)) + A
                A = D
NEXT K
RETURN
```

REFERENCIAS

BLAHUT, R.E. 1987. Fast algorithms for digital signal processing, Addison-Wesley Publishing Company.

BRACEWELL R.N. 1986. The Fourier transform and its applications. McGraw-Hill Book Company. New York.

ELIOT, D.F. & RAO, R. 1982. Fast transforms algorithms, analysis, applications. Academic Press. New York.