

# CONVERSIÓ DE TFD's I CONVOLUCIONS CIRCULARS BIDIMENSIONALS EN UNIDIMENSIONALS \*

per

CARME TORRAS I GENÍS

Institut de Cibernètica (U.P.C. – C.S.I.C.)

## SUMMARY

The paper describes an indexing scheme that allows the error-free computation of some two-dimensional operations as one-dimensional ones. In particular, the conditions which must be satisfied to compute DFT's and circular convolutions in this way are derived, together with the computational effort required. This makes it possible to take full advantage of some very fast linear devices, such as CCD's and SAW's. A CCD implementation of circular convolutions which, by using the proposed indexing scheme, allows to save up to 50% shifts is given. Finally, the reordering of elements underlying each two-dimensional operation is characterized by studying the results of composing a direct and an inverse 2D-1D mapping.

## 1. INTRODUCCIÓ

### 1.1. *Motivació i objectius*

Les imatges són modelitzades habitualment mitjançant funcions reals bidimensionals. Per a processar-les digitalment cal, en primer lloc, discretitzar aquestes funcions i aplicar, seguidament, algorismes que sovint comporten l'avaluació numèrica d'operacions, tals com convolucions i transformades, en dues dimensions. Aquestes operacions són extremament costoses en temps de computació, fet que restringeix, i en certs casos fins i tot impossibilita, la seva implementació en sistemes

\* Aquest treball és un resum de la tesi de llicenciatura presentada per l'autora a la Facultat de Matemàtiques de la Universitat de Barcelona, el gener de 1983.

industrials de visió, sotmesos a unes restriccions considerables quant a temps de resposta.

No és estrany, doncs, que hagin proliferat darrerament els intents d'accelerar el càlcul d'aquestes operacions, tant des del punt de vista algorímic (Kim i Strintzis, 1980; Feather *et al.*, 1980; Mueller *et al.*, 1980; Jenq, 1981; Johnson i Jain, 1981), com des del punt de vista de la seva implementació electrònica (Gilbert *et al.*, 1976; Winston, 1978; Reddy i Hon, 1979; Duff i Levialdi, 1981).

D'altra banda, recentment han començat a ésser utilitzades per al Processament Digital d'imatges tecnologies Charge-Coupled (CCD's) i Surface Acoustic Wave (SAW), que són intrínsecament unidimensionals, ja que funcionen per desplaçaments de càrregues (Miller i Zimmerman, 1975; Nudd, 1977; Willett i Bluzzer, 1977; Barbe *et al.*, 1978, 1980; Gersho, 1979).

Motivats, doncs, d'una banda per la necessitat d'accelerar el càlcul d'operacions bidimensionals tals com la TFD i la convolució circular, i d'altra, pel recent desenvolupament de dispositius CCD's i SAW's encarats al tractament de dades unidimensionals, ens fixarem com a objectiu l'estudi de possibles transformacions de dades bidimensionals en unidimensionals, de manera que el resultat d'efectuar una operació sobre aquestes dades unidimensionals aproximés, dins un cert interval de precisió, el que s'obtidria en efectuar la mateixa operació sobre les dades bidimensionals.

La troballa d'un tipus de transformacions (que anomenarem correspondències 2D-1D i denotarem  $\varphi_{ab}$ ) que permet, no solament "aproximar", sinó també calcular d'una manera exacta operacions bidimensionals mitjançant una única aplicació de l'algorisme unidimensional corresponent, ens impulsà a centrar el nostre estudi en aquest tipus concret de transformacions.

## 1.2. Antecedents històrics

El present treball se situa en el terreny de l'aplicació de resultats de la Teoria Elemental de Nombres al desenvolupament d'algorismes de Processament Digital de Senyals (McClellan i Rader, 1979). Hom pot distingir, en principi, dos tipus d'algorismes: els que resulten d'aplicar els resultats esmentats als valors numèrics de les dades i els que deriven d'aplicar-los a les posicions ocupades per les dades. Els primers exploten les propietats de les transformades definides sobre cossos finits, tals com la transformada numèrica de Fermat o la de Mersenne. El treball realitzat s'enquadra en el marc del segon tipus d'algorismes, entre els quals és obligat d'esmentar l'algorisme de Good (1968, 1971) i el de Winograd (1978). El primer guarda una relació directa amb el contingut

d'aquesta tesina, ja que és basat en les correspondències Sino i Ruritarian, que són un cas particular de les correspondències 2D-1D i 1D-2D estudiades.

Un precedent d'origen considerablement diferent, però que també pretén d'accelerar el càlcul de convolucions bidimensionals, bé que en aquest cas contínues i periòdiques, és la tècnica desenvolupada per Bucy *et al.* (1977) en el context de la desmodulació òptima de fase, i consisteix a aproximar la convolució bidimensional per una d'unidimensional. No solament és aquesta idea subjacent igual a la nostra, sinó que el procediment que utilitza per a construir la funció unidimensional a partir de les dades bidimensionals ens suggerí precisament la definició de les correspondències 2D-1D, prèvia introducció —és clar— de les modificacions pertinents quant a discretització i condicions a complir per les longituds de les dimensions.

## 2. CORRESPONDÈNCIA 2D-1D

### 2.1. Definició i propietats

Donats  $N_1, N_2 \in \mathbb{N}$  i  $a, b \in \mathbb{Z}$ , definirem l'aplicació:

$$\begin{aligned} \varphi_{ab}: \mathbb{Z}_{N_1 N_2} &\longrightarrow \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \\ n &\longrightarrow (n_1, n_2) = (\langle an \rangle_{N_1}, \langle bn \rangle_{N_2}) \end{aligned}$$

*Proposició 1.*  $\varphi_{ab} = \varphi_{a'b'}$  si i només si  $\langle a - a' \rangle_{N_1} = 0$  i  $\langle b - b' \rangle_{N_2} = 0$ .

*Corol·lari 1.1.* El nombre d'aplicacions  $\varphi_{ab}$  és  $(N_1 N_2)$ .

Quan la periodicitat de  $\mathbb{Z}_{N_1}$  i  $\mathbb{Z}_{N_2}$  és representada espacialment per mitjà de la repetició, els punts imatge per a qualsevol aplicació  $\varphi_{ab}$  defineixen una recta de pendent  $\langle a \rangle_{N_1} / \langle b \rangle_{N_2}$  (figura 1).

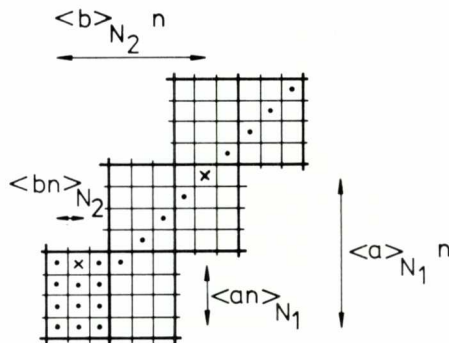


Fig. 1. Representació estesa de l'aplicació  $\varphi_{ab}$ .

*Proposició 2.* El període  $T$  de l'aplicació  $\varphi_{ab}$  tal com ha estat definit és:

$$T = \frac{N_1 N_2}{(a, N_1) (b, N_2) \left( \frac{N_1}{(a, N_1)}, \frac{N_2}{(b, N_2)} \right)}$$

Demostració. El període serà donat pel mínim  $n \in \mathbb{Z}_{N_1 N_2}$  no nul, que satisfaci l'equació:

$$\varphi_{ab}(n) = 0$$

és a dir, el sistema:

$$\left. \begin{aligned} \langle an \rangle_{N_1} &= 0 \\ \langle bn \rangle_{N_2} &= 0 \end{aligned} \right\}$$

S'ha de verificar, doncs, que:

$$\left. \begin{aligned} \frac{a}{(a, N_1)} \cdot n &= \frac{N_1}{(a, N_1)} \cdot q_1 \\ \frac{b}{(b, N_2)} \cdot n &= \frac{N_2}{(b, N_2)} \cdot q_2 \end{aligned} \right\}$$

Com que:

$$\left( \frac{a}{(a, N_1)}, \frac{N_1}{(a, N_1)} \right) = \left( \frac{b}{(b, N_2)}, \frac{N_2}{(b, N_2)} \right) = 1$$

resulta que:

$$\left( n, \frac{N_1}{(a, N_1)} \right) = \frac{N_1}{(a, N_1)}$$

$$\left( n, \frac{N_2}{(b, N_2)} \right) = \frac{N_2}{(b, N_2)}$$

El mínim  $n$  que verifica és doncs el mínim comú múltiple de

$$\frac{N_1}{(a, N_1)} \quad \text{i} \quad \frac{N_2}{(b, N_2)}$$

que és precisament:

$$T = \frac{N_1 N_2}{(a, N_1) (b, N_2) \left( \frac{N_1}{(a, N_1)}, \frac{N_2}{(b, N_2)} \right)} \quad \blacksquare$$

*Corol·lari 2.1.* L'aplicació  $\varphi_{ab}$  és bijectiva si i només si

$$(N_1, N_2) = (a, N_1) = (b, N_2) = 1$$

*Corol·lari 2.2.* Només podran ésser definides aplicacions  $\varphi_{ab}$  bijectives quan  $(N_1, N_2) = 1$ , i, en aquest cas, el nombre total d'aquestes serà  $\phi(N_1) \phi(N_2)$ .

*Proposició 3.* La inversa d'una aplicació bijectiva del tipus considerat  $\varphi_{ab}$ , és donada per:

$$\begin{aligned} \varphi_{ab}^{-1}: \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} &\longrightarrow \mathbb{Z}_{N_1 N_2} \\ (n_1, n_2) &\longrightarrow (n) = \langle n_1 U_1 N_2 + n_2 U_2 N_1 \rangle_{N_1 N_2} \end{aligned}$$

on  $U_1$  i  $U_2$  són les solucions del sistema d'equacions:

$$\left. \begin{aligned} \langle a U_1 N_2 \rangle_{N_1} &= 1 \\ \langle b U_2 N_1 \rangle_{N_2} &= 1 \end{aligned} \right\}$$

*Demostració.* En primer lloc,  $\varphi_{ab}^{-1}$  és una aplicació ben definida, ja que, en virtut del Corol·lari A.2.1(\*), el sistema d'equacions té sempre una solució:

$$\begin{aligned} U_1 &= \langle (aN_2)^{\phi(N_1)-1} \rangle_{N_1} \\ U_2 &= \langle (bN_1)^{\phi(N_2)-1} \rangle_{N_2} \end{aligned}$$

que, segons el Corol·lari A.2.2, és única. A més, es verifica que:

$$\begin{aligned} \varphi_{ab} \circ \varphi_{ab}^{-1} &= \text{Id}_{\mathbb{Z}_{N_1 N_2}} \\ \varphi_{ab}^{-1} \circ \varphi_{ab} &= \text{Id}_{\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}} \end{aligned}$$

on  $\text{Id}_X$  és l'aplicació identitat en el conjunt  $X$ .

En efecte,

$$\begin{aligned} (\varphi_{ab} \circ \varphi_{ab}^{-1})(n) &= \varphi_{ab}^{-1}(\varphi_{ab}(n)) = \varphi_{ab}(\langle an \rangle_{N_1}, \langle bn \rangle_{N_2}) = \\ &= \langle \langle an \rangle_{N_1} U_1 N_2 + \langle bn \rangle_{N_2} U_2 N_1 \rangle_{N_1 N_2} = \\ &= \langle \langle an \rangle_{N_1} \langle (aN_2)^{\phi(N_1)-1} \rangle_{N_1} N_2 + \langle bn \rangle_{N_2} \langle (bN_1)^{\phi(N_2)-1} \rangle_{N_2} N_1 \rangle_{N_1 N_2} \end{aligned}$$

\* Les proposicions i corol·laris assenyalats amb la lletra A es troben a l'apèndix A.

$$\begin{aligned}
 & + \langle bn \rangle_{N_2} \langle (bN_1)^{\phi(N_2)-1} \rangle_{N_2} N_1 \rangle_{N_1 N_2} = \\
 = & \langle \langle n \rangle_{N_1} \langle N_2^{(N_1)-1} \rangle_{N_1} N_2 + \langle n \rangle_{N_2} \langle N_1^{\phi(N_2)-1} \rangle_{N_2} N_1 \rangle_{N_1 N_2}
 \end{aligned}$$

on en el darrer pas ha estat aplicat el Teorema d'Euler:

$$\langle a^{\phi(N_1)} \rangle_{N_1} = \langle b^{\phi(N_2)} \rangle_{N_2} = 1$$

El Teorema del reste xinès ens garanteix que l'expressió obtinguda es igual a  $n$  i, consegüentment,

$$(\varphi_{ab} \circ \varphi_{ab}^{-1})(n) = n, \quad \forall n \in \mathbb{Z}_{N_1 N_2}$$

D'una manera semblant:

$$\begin{aligned}
 (\varphi_{ab}^{-1} \circ \varphi_{ab})(n_1, n_2) & = \varphi_{ab}(\varphi_{ab}^{-1}(n_1, n_2)) = \\
 & = \varphi_{ab}^{-1}(\langle n_1 \langle (aN_2)^{\phi(N_1)-1} \rangle_{N_1} N_2 + \\
 & + n_2 \langle (bN_1)^{\phi(N_2)-1} \rangle_{N_2} N_1 \rangle_{N_1 N_2}) \\
 & = \langle an_1 a^{\phi(N_1)-1} N_2^{\phi(N_1)} \rangle_{N_1}, \\
 & \langle bn_2 b^{\phi(N_1)-1} N_1^{\phi(N_1)-1} N_1^{\phi(N_2)} \rangle_{N_2} = \\
 & = (\langle n_1 \rangle_{N_1}, \langle n_2 \rangle_{N_2}) = \\
 & = (n_1, n_2)
 \end{aligned}$$

on també ha esta aplicat el Teorema d'Euler:

$$\begin{aligned}
 \langle a^{\phi(N_1)} \rangle_{N_1} = \langle b^{\phi(N_2)} \rangle_{N_2} = \langle N_2^{\phi(N_1)} \rangle_{N_1} = \\
 = \langle N_1^{\phi(N_2)} \rangle_{N_2} = 1. \quad \blacksquare
 \end{aligned}$$

A partir d'ara, considerarem només aplicacions  $\varphi_{ab}$  bijectives (figura 2) amb  $a \in \mathbb{Z}_{N_1}$  i  $b \in \mathbb{Z}_{N_2}$ , cada una de les quals permet de repre-

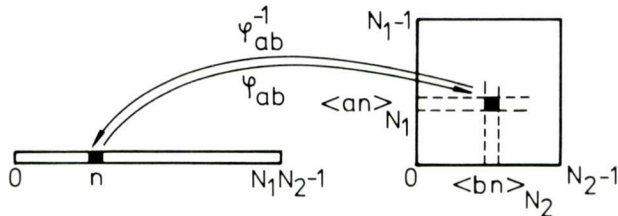


Fig. 2. Aplicació bijectiva  $\varphi_{ab}$  i la seva inversa  $\varphi_{ab}^{-1}$ .

sentar vectors com matrius i matrius com vectors, essent única la correspondència entre les representacions unidimensionals i bidimensionals.

## 2.2. Utilització per al càlcul de la TFD

### 2.2.1. Condicions

*Proposició 4.* Si es verifiquen les següents condicions:

- (1)  $(N_1, N_2) = 1$
- (2)  $f(n_1, n_2)$  és una funció discreta de dimensions  $N_1 \times N_2$
- (3)  $F(w_1, w_2)$  és la seva transformada de Fourier discreta
- (4)  $\tilde{f}(n)$  i  $\tilde{F}(w)$  són les seves corresponents representacions unidimensionals, definides per:

$$\tilde{f}(n) = f(\varphi_{ab}(n)) \text{ i } \tilde{F}(w) = F(\varphi_{a'b'}(w))$$

llavors  $\tilde{F}(w)$  serà la transformada de Fourier discreta de  $\tilde{f}(n)$  si i només si les dues aplicacions bijectives  $\varphi_{ab}$  i  $\varphi_{a'b'}$  satisfan les condicions següents:

$$\langle aa' \rangle_{N_1} = \langle N_2^{\phi(N_1)-1} \rangle_{N_1}$$

$$\langle bb' \rangle_{N_2} = \langle N_1^{\phi(N_2)-1} \rangle_{N_2}$$

*Demostració.* Pel fet d'ésser  $F(w_1, w_2)$  la TFD de  $f(n_1, n_2)$ :

$$F(w_1, w_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) W_{N_1}^{n_1 w_1} W_{N_2}^{n_2 w_2}$$

$$w_1 = 0.1, \dots, N-1$$

$$w_2 = 0.1, \dots, N-1$$

En virtut de la bijectivitat de  $\varphi_{ab}$  i  $\varphi_{a'b'}$ , i segons les definicions de  $\tilde{f}(n)$  i  $\tilde{F}(w)$ , podem rescriure l'anterior equació de la manera següent:

$$\tilde{F}(\varphi_{a'b'}^{-1}(w_1, w_2)) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \tilde{f}(\varphi_{ab}^{-1}(n_1, n_2)) W_{N_1}^{n_1 w_1} W_{N_2}^{n_2 w_2}$$

$$\begin{aligned}w_1 &= 0, 1, \dots, N_1 - 1 \\w_2 &= 0, 1, \dots, N_2 - 1\end{aligned}$$

Substituint ara  $\varphi_{a'b'}^{-1}(w_1, w_2)$  per  $w$  i  $\varphi_{ab}^{-1}(n_1, n_2)$  per  $n$ , i consegüentment,  $n_1$  per  $\langle an \rangle_{N_1}$ ,  $n_2$  per  $\langle bn \rangle_{N_2}$ ,  $w_1$  per  $\langle aw \rangle_{N_1}$  i  $w_2$  per  $\langle bw \rangle_{N_2}$ , obtindrem:

$$\begin{aligned}\tilde{F}(w) &= \sum_{n=0}^{N_1 N_2 - 1} f(n) W_{N_1}^{a n a' w} \cdot W_{N_2}^{b n b' w} \\w &= 0, 1, \dots, N_1 N_2 - 1\end{aligned}$$

on ha estat utilitzada la bijectivitat d'ambdues aplicacions  $\varphi_{ab}$  i  $\varphi_{a'b'}$ , per a reordenar convenientment els termes de què consta el sumatori, així com les equacions.

Perquè  $\tilde{F}(w)$  sigui efectivament la TFD de  $\tilde{f}(n)$  caldrà que es verifiqui que:

$$\begin{aligned}W_{N_1}^{a a' n w} W_{N_2}^{b b' n w} &= W_{N_1 N_2}^{n w} \\n &= 0, 1, \dots, N_1 N_2 - 1 \\w &= 0, 1, \dots, N_1 N_2 - 1\end{aligned}$$

O, duent a terme operacions en el primer membre de l'anterior equació:

$$\begin{aligned}W_{N_1 N_2}^{n w (a a' N_2 + b b' N_1)} &= W_{N_1 N_2}^{n w} \\n &= 0, 1, \dots, N_1 N_2 - 1 \\w &= 0, 1, \dots, N_1 N_2 - 1\end{aligned}$$

La qual cosa es verificarà si i només si:

$$\langle a a' N_2 + b b' N_1 \rangle_{N_1 N_2} = 1$$

que, pel Teorema del reste xinès, equival a que:

$$\begin{aligned}\langle a a' N_2 \rangle_{N_1} &= 1 \\ \langle b b' N_1 \rangle_{N_2} &= 1\end{aligned}$$



I, segons el Corol·lari A.2.1, això és el mateix que:

$$\langle aa' \rangle_{N_1} = \langle N_2^{\phi(N_1)-1} \rangle_{N_1}$$

$$\langle bb' \rangle_{N_2} = \langle N_1^{\phi(N_2)-1} \rangle_{N_2}$$

com volíem demostrar. ■

Per a fer més explícit el significat de la proposició anterior, utilitzarem el diagrama següent (vegeu també la figura 3):

$$\begin{array}{ccc} f(n_1, n_2) & \xrightarrow{2-D \text{ TFD}} & F(w_1, w_2) \\ \varphi_{ab} \downarrow & & \uparrow \varphi_{a'b'} \\ f(n) & \xrightarrow{1-D \text{ TFD}} & F(w) \end{array}$$

en el qual cal interpretar que les aplicacions  $\varphi_{ab}$  i  $\varphi_{a'b'}$  actuen sobre el conjunt d'índexs de les funcions, mentre que les TFD's actuen sobre els valor de les funcions.

La proposició afirma que el diagrama commuta si i només si es verifiquen les condicions enunciades.

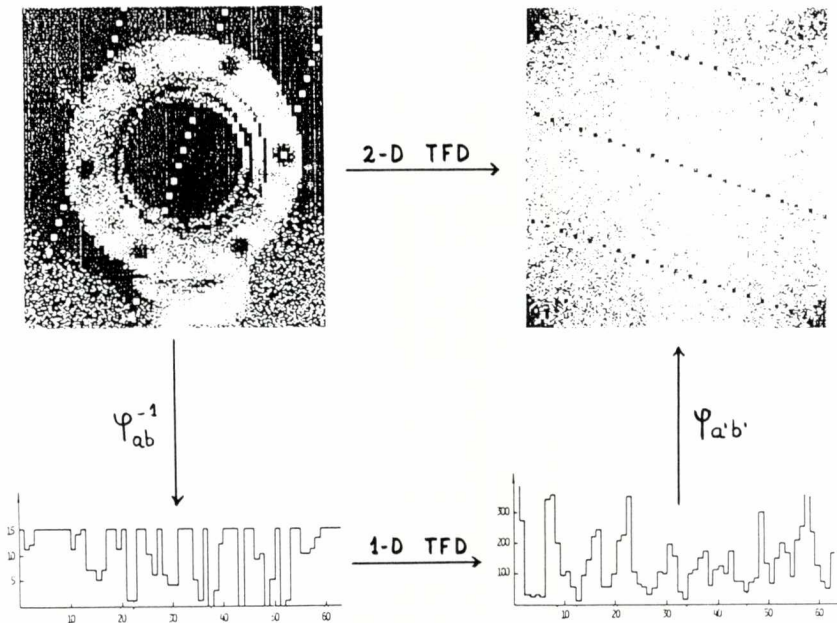


Fig. 3. Procés de càlcul de la TFD d'una imatge de dimensions 64 x 63, mitjançant les aplicacions  $\varphi_{3,1}$  i  $\varphi_{21,1}$ .

*Corol·lari 4.1.* Si  $(N_1, N_2) = 1$ , donada una aplicació  $\varphi_{ab}$  bijectiva, sempre existirà una altra aplicació bijectiva  $\varphi_{a'b'}$  que, juntament amb la primera, permetrà de calcular qualsevol TFD bidimensional d'una funció discreta de dimensions  $N_1 \times N_2$  mitjançant l'avaluació d'una única TFD unidimensional de longitud  $N_1 N_2$ .

Així, doncs, una de les dues aplicacions necessàries per a calcular una TFD bidimensional com si fos unidimensional podrà ésser escollida a voluntat, i l'altra quedarà llavors determinada per les condicions enunciades a la Proposició 4.

Cal observar que si la parella d'aplicacions  $\varphi_{ab}$  i  $\varphi_{a'b'}$  —de les quals la primera actua sobre els índexs de les funcions i la segona sobre els índexs de les seves transformades de Fourier discretes— permet de convertir una TFD bidimensional en una TFD unidimensional, la parella d'aplicacions  $\varphi_{a'b'}$  i  $\varphi_{ab}$  —els dominis d'aplicació de les quals han estat intercanviats— també permet de dur a terme la conversió.

*Corol·lari 4.2.* Si  $(N_1, N_2) = 1$ , la parella d'aplicacions

$$\varphi_{1,1} \text{ i } \varphi_{\langle N_2^{\phi(N_1)-1} \rangle_{N_1}, \langle N_1^{\phi(N_2)-1} \rangle_{N_2}}$$

permet de convertir la TFD bidimensional de qualsevol funció discreta de dimensions  $N_1 \times N_2$ , en una TFD unidimensional.

Mencionem que aquesta parella fou la utilitzada per Good (1971).

*Corol·lari 4.3.* Si  $(N_1, N_2) = 1$ , el nombre de parelles d'aplicacions  $\varphi_{ab}$  i  $\varphi_{a'b'}$  que permeten de convertir una TFD bidimensional d'una funció discreta de dimensions  $N_1 \times N_2$  en una TFD unidimensional és  $\phi(N_1) \phi(N_2)$ .

Dues condicions finals. Primera, la Proposició 4 permet tant de calcular TFD's bidimensionals convertint-les en unidimensionals com a la inversa, és a dir, calcular TFD's unidimensionals descomposant-les en bidimensionals. L'únic requeriment és que la longitud de la TFD unidimensional sigui descomponible en el producte de dos nombres primers entre si. Segona, això que hom ha fet per al cas bidimensional pot ésser estès al cas multidimensional.

### 2.2.2. Esforç computacional

Prenent l'algorisme FFT com a base, podem comparar l'esforç computacional derivat d'utilitzar les aplicacions  $\varphi_{ab}$  per al càlcul de la TFD, amb el requerit pel procediment bidimensional habitual, consistent en l'avaluació de les TFD's unidimensionals de les files seguida de la de les columnes.

Tenint en compte els resultats de l'apèndix B, calcularem, en primer

lloc, l'esforç requerit per a avaluar la TFD d'una matriu quadrada de  $2^n \times 2^n$  valors complexos.

$$\begin{aligned} \# MC_C (2-D) &= 2 N \left[ \left( \frac{n}{2} - 1 \right) N + 1 \right] = \\ &= n N^2 - 2 N^2 + 2 N \end{aligned}$$

$$\# SC_C (2-D) = 2 n N^2$$

que, traduït a operacions reals, és:

$$\begin{aligned} \# MR_C (2-D) &= 2 N \left[ 4 \left[ \left( \frac{n}{2} - 1 \right) N + 1 \right] \right] = \\ &= 4 n N^2 - 8 N^2 + 8 N \end{aligned}$$

$$\begin{aligned} \# SR_C (2-D) &= 2 N \left[ 2 n N + 2 \left[ \left( \frac{n}{2} - 1 \right) N + 1 \right] \right] = \\ &= 4 n N^2 + 2 n N^2 - 4 N^2 + 4 N = \\ &= 6 n N^2 - 4 N^2 + 4 N \end{aligned}$$

Si ara suposem que la funció original de partida és real, llavors les TFD's de les files actuaran sobre valors reals, mentre que les de les columnes ho faran sobre valors complexos. A més, cal tenir en compte que les TFD's de les files seran simètriques respecte a llur part real i antisimètriques respecte a llur part imaginària. Pel fet que si  $\tilde{F}(w)$  és la TFD de  $\tilde{f}(k)$ , llavors  $\tilde{F}^*(w)$  és la TFD de  $\tilde{f}^*(k)$ , serà suficient de calcular la TFD de les  $(N/2 + 1)$  primeres columnes i dur a terme a continuació les assignacions següents:

$$f(w_1, w_2) = f^*(w_1, N_2 - w_2),$$

$$w_2 = \frac{N_2}{2} + 1, \frac{N_2}{2} + 2, \dots, N_2 - 1$$

$$w_1 = 0, 1, \dots, N_1 - 1$$

que ens proporcionaran els valors de les columnes restants. L'esforç computacional requerit en aquest cas serà doncs:

$$\begin{aligned}
 \# \text{MR}_R(2\text{-D}) &= N \left[ (2n - 3) \frac{N}{2} - 2 \right] + \left( \frac{N}{2} + 1 \right) [(2n - 4) N + 4] = \\
 &= (2n - 3) \frac{N^2}{2} - 2N + (2n - 4) \frac{N^2}{2} + 2N + (2n - 4) N + 4 = \\
 &= (4n - 7) \frac{N^2}{2} + (2n - 4) N + 4
 \end{aligned}$$

$$\begin{aligned}
 \# \text{SR}_R(2\text{-D}) &= N \left[ (3n + 1) \frac{N}{2} - 8 \right] + \left( \frac{N}{2} + 1 \right) [(3n - 2) N + 2] = \\
 &= (3n + 1) \frac{N^2}{2} - 8n + (3n - 2) \frac{N^2}{2} + N + (3n - 2) N + 2 = \\
 &= (6n - 1) \frac{N^2}{2} + (3n - 9) N + 2
 \end{aligned}$$

A fi d'establir la comparació que constitueix l'objectiu d'aquest apartat, procedirem ara a calcular l'esforç computacional que comporta l'avaluació de TFD's bidimensionals fent ús de les aplicacions  $\varphi_{ab}$ . Com que l'escombratge de la imatge seguint una línia de pendent adient pot ésser fet per mitjans electrònics, l'esforç computacional quedarà reduït al còmput d'una TFD unidimensional de longitud  $N^2 = 2^{2n}$ .

$$\# \text{MC}_C(1\text{-D}) = nN^2 - N^2 + 1$$

$$\# \text{SC}_C(1\text{-D}) = 2nN^2$$

I, traduint'ho a operacions reals:

$$\# \text{MR}_C(1\text{-D}) = 4nN^2 - 4N^2 + 4$$

$$\# \text{SR}_C(1\text{-D}) = 4nN^2 + 2nN^2 - 2N^2 + 2 = 6nN^2 - 2N^2 + 2$$

Si, a més, imposem que tots els valors sobre els quals hom calcularà la TFD siguin reals, resultarà:

$$\# \text{MR}_C(1\text{-D}) = [2(2n) - 3] \frac{N^2}{2} - 2 = (4n - 3) \frac{N^2}{2} - 2$$

$$\# \text{SR}_R (1\text{-D}) = [3(2n) + 1] \frac{N^2}{2} - 8 = (6n + 1) \frac{N^2}{2} - 8$$

Observem, doncs, que l'esforç computacional requerit és lleugerament més gran si hom utilitza les aplicacions  $\varphi_{ab}$ , tendint a ésser el mateix quan N tendeix a infinit.

### 2.3. Utilització per al càlcul de convolucions circulars

#### 2.3.1. Condicions

*Proposició 5.* Si es verifiquen les següents condicions:

- (1)  $(N_1, N_2) = 1$
- (2)  $\hat{f}(n_1, n_2)$  i  $g(n_1, n_2)$  són funcions discretes de dimensions  $N_1 \times N_2$
- (3)  $(\hat{f} * g)(k_1, k_2)$  és la seva convolució circular bidimensional
- (4)  $\tilde{f}(n)$ ,  $\tilde{g}(n)$  i  $(\tilde{f} * \tilde{g})(k)$  són les seves respectives representacions unidimensionals, definides per:

$$\tilde{f}(n) = f(\varphi_{ab}(n))$$

$$\tilde{g}(n) = g(\varphi_{ab}(n))$$

$$(\tilde{f} * \tilde{g})(k) = (\hat{f} * \hat{g})(\varphi_{a'b'}(k))$$

llavors  $(\tilde{f} * \tilde{g})(k)$  serà la convolució circular unidimensional de  $\tilde{f}(n)$  i  $\tilde{g}(n)$  si i només si les dues aplicacions bijectives  $\varphi_{ab}$  i  $\varphi_{a'b'}$  satisfan les condicions següents:

$$\left\{ \begin{array}{l} a' = a \\ b' = b \end{array} \right\}$$

*Demostració.* Pel fet que  $(\hat{f} * \hat{g})(k_1, k_2)$  és la convolució circular bidimensional de  $\hat{f}(n_1, n_2)$  i  $g(n_1, n_2)$ , tenim que:

$$(\hat{f} * \hat{g})(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \hat{f}(n_1, n_2) g(\langle k_1 - n_1 \rangle_{N_1}, \langle k_2 - n_2 \rangle_{N_2})$$

$$k_1 = 0, 1, \dots, N_1 - 1$$

$$k_2 = 0, 1, \dots, N_2 - 1$$

Prenent  $\varphi_{ab}(n) = (n_1, n_2)$  i  $\varphi_{a'b'}(k) = (k_1, k_2)$ , i consegüentment,  $n_1 = \langle an \rangle_{N_1}$ ,  $n_2 = \langle bn \rangle_{N_2}$ ,  $k_1 = \langle a'k \rangle_{N_1}$  i  $k_2 = \langle b'k \rangle_{N_2}$ , la bijectivitat de  $\varphi_{ab}$  i  $\varphi_{a'b'}$  implica:

$$(f * g)(\varphi_{a'b'}(k)) = \sum_{n=0}^{N_1 N_2 - 1} f(\varphi_{ab}(n)) g(\langle a'k - an \rangle_{N_1}, \langle b'k - bn \rangle_{N_2})$$

$$k = 0, 1, \dots, N_1 N_2 - 1$$

Per definició de  $\tilde{f}(n)$  i  $\tilde{g}(n)$ :

$$(f * g)(\varphi_{a'b'}(k)) = \sum_{n=0}^{N_1 N_2 - 1} \tilde{f}(n) \tilde{g}(\varphi_{ab}^{-1}(\langle a'k - an \rangle_{N_1}, \langle b'k - bn \rangle_{N_2}))$$

$$k = 0, 1, \dots, N_1 N_2 - 1$$

El segon membre d'aquesta equació serà la convolució unidimensional de  $\tilde{f}(n)$  i  $\tilde{g}(n)$  si i només si:

$$\varphi_{ab}^{-1}(\langle a'k - an \rangle_{N_1}, \langle b'k - bn \rangle_{N_2}) = \langle k - n \rangle_{N_1 N_2}$$

$$k = 0, 1, \dots, N_1 N_2 - 1$$

$$n = 0, 1, \dots, N_1 N_2 - 1$$

O, allò que és la mateixa cosa:

$$\langle a'k - an \rangle_{N_1} = \langle a \langle k - n \rangle_{N_1 N_2} \rangle_{N_1}$$

$$\langle b'k - bn \rangle_{N_2} = \langle b \langle k - n \rangle_{N_1 N_2} \rangle_{N_2}$$

Com que  $\langle \langle x \rangle_{N_1 N_2} \rangle_{N_1} = \langle x \rangle_{N_1}$ , podem rescriure:

$$\langle a'k - an \rangle_{N_1} = \langle a (k - n) \rangle_{N_1}$$

$$\langle b'k - bn \rangle_{N_2} = \langle b (k - n) \rangle_{N_2}$$

I, efectuant operacions amb les aritmètriques mòdul  $N_1$  i  $N_2$ , obtindrem:

$$\begin{aligned} \langle (a' - a) k \rangle_{N_1} &= 0 \\ \langle (b' - b) k \rangle_{N_2} &= 0 \end{aligned} \quad k = 0, 1, \dots, N_1 N_2 - 1$$

Per tant,

$$\begin{aligned} a' &= a \\ b' &= b \end{aligned}$$

que és precisament allò que volíem demostrar. ■

Anàlogament a allò que hem fet amb la Proposició 4, referirem la 5 al diagrama següent:

$$\begin{array}{ccc} f(n_1, n_2), g(n_1, n_2) & \xrightarrow{* 2 - D} & (f * g)(n_1, n_2) \\ \downarrow \varphi_{ab}^{-1} \quad \downarrow \varphi_{ab}^{-1} & & \uparrow \varphi_{ab} \\ \tilde{f}(n), \tilde{g}(n) & \xrightarrow{* 1 - D} & \tilde{(f * g)}(n) \end{array}$$

en el qual les convolucions (\*) unidimensionals i bidimensionals actuen sobre els valors de les funcions, mentre que  $\varphi_{ab}$  ho fa sobre el índexs.

La Proposició 5 afirma que aquest diagrama és commutatiu si i només si es compleixen les condicions enunciades. La commutativitat del diagrama equival al fet que convolucions circulars bidimensionals puguin ésser calculades com unidimensionals via aplicacions  $\varphi_{ab}$  bijectives.

*Corol·lari 5.1.* Si  $(N_1, N_2) = 1$ , hi ha  $\phi(N_1) \phi(N_2)$  aplicacions  $\varphi_{ab}$  bijectives que permeten de calcular convolucions circulars bidimensionals de funcions discretes de dimensions  $N_1 \times N_2$ , mitjançant l'avaluació d'una sola convolució circular unidimensional.

També aquí, com en el cas de la TFD, hom pot fer una lectura alternativa de la Proposició 5, en el sentit que, sota certes condicions, garanteix que una convolució circular unidimensional pot ésser calculada com si fos bidimensional. El resultat enunciat per al cas bidimensional és generalitzable al cas multidimensional.

### 2.3.2. Implementació mitjançant CCD's

La implementació de la convolució circular bidimensional fent ús d'aplicacions  $\varphi_{ab}$  pot fer més eficient el procés de càlcul (disminuir la

seva duració) en certs casos que explicitem al llarg d'aquest apartat.

Diguem, en primer lloc, que un CCD és un dispositiu que permet d'enmagatzemar senyals analògics mostrejats, en forma de paquets de càrrega aïllats de valor proporcional a l'amplitud del senyal en els diferents instants de mostreig. Aquests paquets de càrrega poden ésser desplaçats d'una posició a una altra induint un potencial suficientment gran en la direcció i el sentit desitjats dins el pla del dispositiu. El ritme de desplaçament pot ésser controlat digitalment, la qual cosa proporciona una gran flexibilitat de disseny, especialment adient per al processament de senyals.

Per motius econòmics i tecnològics, la disposició més comunament adoptada és la unidimensional. Els CCD's d'aquesta mena funcionen com a *shift registers*. Amb l'actual tecnologia del silici, han estat assolides velocitats de desplaçament de paquets de càrrega fins de 200 MHz. i sembla probable que en un futur no molt llunyà hom arribi als 900 MHz.

Suposem que disposem d'un únic dispositiu de longitud  $N_2$  i volem calcular la convolució de dues matrius  $f$  i  $g$  de dimensions  $N_1 \times N_2$ . Utilitzant el procediment bidimensional habitual, introduiríem la primera fila de  $f$  en el dispositiu ( $N_2$  *shifts*), carregaríem la primera fila de  $g$  en els  $N_2$  multiplicadors associats i obtindríem una porció de  $(f * g) (0,0)$ , tal com mostra la figura 4 (a). Seguidament desplaçaríem  $N_2 - 1$  vegades els valors en el dispositiu lineal ( $N_2 - 1$  *shifts*) i obtindríem les porcions corresponents de tots els elements de la primera fila de  $(f * g)$ .

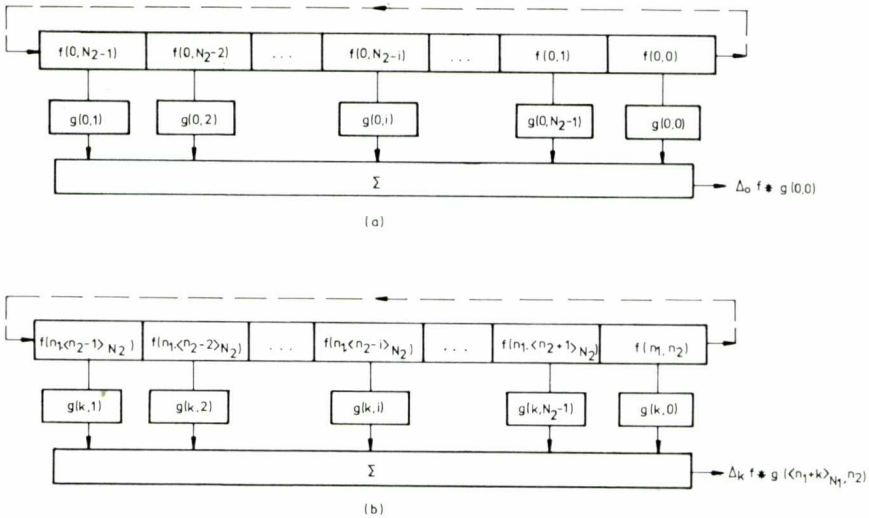


Fig. 4. Implementació mitjançant CCD's del càlcul de la convolució circular bidimensional.



Fet això, i sense modificar els valors dels multiplicadors, procediríem a introduir els valors de la segona fila de  $f$  en el dispositiu unidimensional ( $N_2$  shifts) i desplaçaríem  $N_2-1$  vegades els valors ( $N_2-1$  shifts), obtenint les porcions corresponents a la segona fila de  $f * g$ , i així successivament fins a la fila  $N_1$ . Llavors, carregariem els multiplicadors amb els valors de la segona fila de  $g$  i duríem a terme de nou tot el procés anterior, llevat que començaríem per la fila  $N_1$  de  $f$ , estalviant-nos  $N_2-1$  shifts. La figura 4 (b) mostra una representació genèrica del procés. El nombre total de shifts necessaris seria:

$$\begin{aligned} \# SH_1(2-D) &= (2N_2 - 1) N_1 N_2 - N_2 (N_1 - 1) = \\ &= 2N_2 N_1^2 - N_1^2 - N_2 N_1 + N_2 \end{aligned}$$

Si, en lloc de disposar d'un únic CCD de longitud  $N_2$ , en disposésim de  $N_1$ , podríem dur a terme el procés en paral·lel per a tots els valors de  $k$  en la figura 4 (b), és a dir, ompliríem cada conjunt de  $N_2$  multiplicadors amb una fila de  $g$ . El nombre total de shifts en aquest cas seria:

$$\# SH_{N_1}(2-D) = (2N_2 - 1) N_1$$

En cas d'implementar la convolució circular bidimensional fent ús d'aplicacions  $\varphi_{ab}$ , introduiríem els  $N_2$  primers valors de  $f$  en el dispositiu CCD ( $N_2$  shifts), carregariem els  $N_2$  de  $\tilde{g}$  en els multiplicadors i obtindríem una part de  $(f * g)(0,0)$ , tal com podem veure la figura 5 (a).

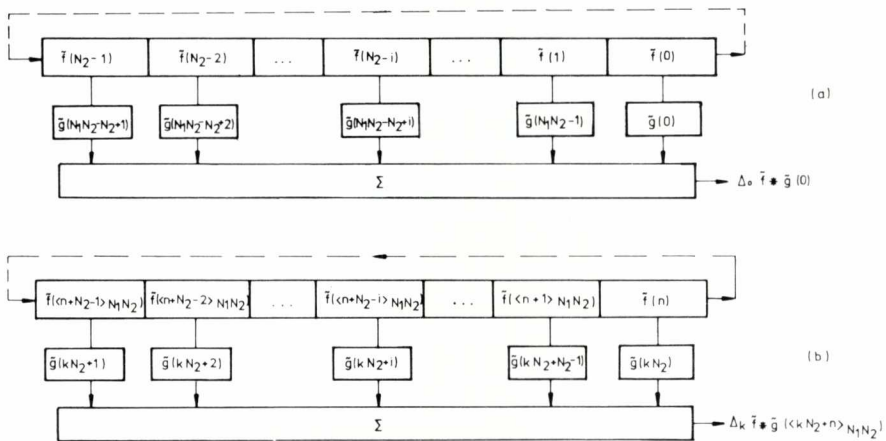


Fig. 5. Implementació mitjançant CCD's del càlcul de la convolució circular unidimensional.

Seguidament, desplaçaríem  $N_1 N_2 - 1$  vegades els valors en el dispositiu unidimensional ( $N_1 N_2 - 1$  “shifts”) i obtindríem les porcions corresponents a tots els elements de  $f * g$ . Fet això, carregariem els multiplicadors amb els valors  $\tilde{g}(N_2), \tilde{g}(N_2 + 1), \dots, \tilde{g}(2N_2 - 1)$  i duríem a terme de nou el procés anterior, estalviant d'aquesta manera els  $N_2$  shifts necessaris per a omplir el dispositiu unidimensional, perquè ja fóra ple. La figura 5 (b) mostra una representació genèrica del procés. El nombre total de shifts necessaris seria:

$$\begin{aligned} \# SH_1(1-D) &= N_2 + (N_1 N_2 - 1) N_1 = \\ &= N_1^2 N_2 - N_1 + N_2 \end{aligned}$$

Si en lloc de disposar d'un únic CCD de longitud  $N_2$ , en disposessim de  $N_1$ , podríem dur a terme el procés en paral·lel per a tots els valors de  $k$  en la figura 5 (b), és a dir, carregariem tots els multiplicadors disponibles amb seqüències de  $N_2$  valors consecutius de  $\tilde{g}$ . El nombre total de shifts en aquest cas seria:

$$\# SH_{N_1}(1-D) = N_2 + N_1 N_2 - 1$$

Comparant ara els casos bidimensional i unidimensional, observem que la utilització d'aplicacions  $\varphi_{ab}$  comporta un estalvi considerable en termes de nombre de shifts. Aquest estalvi tendeix al 50% quan  $N_1$  tendeix a infinit, tant en el cas de disposar d'un únic CCD de longitud  $N_2$  com en el cas de disposar-ne de  $N_1$ .

### 3. COMPOSICIÓ DE CORRESPONDÈNCIES 2D-1D i 1D-2D

En aquest apartat estudiarem les autoaplicacions de  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  obtingudes en compondre una aplicació inversa  $\varphi_{ab}^{-1}$  amb una aplicació directa  $\varphi_{a'b'}$ , (figura 6). Aquest tipus d'autoaplicacions permet de des-

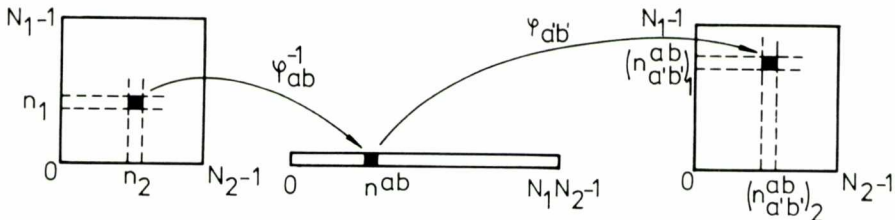


Fig. 6. Autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$ .

criure la reordenació d'elements subjacent al procés de càlcul de la TFD i la convolució circular, quan hom utilitza les aplicacions  $\varphi_{ab}$ .

3.1. *Caracterització de les autoaplicacions* ( $\varphi_{ab}^{-1} \circ \varphi_{a'b'}$ )

Establirem, en primer lloc, unes convencions de notació:

$$\begin{aligned} \varphi_{ab}^{-1}(n_1, n_2) &= n^{ab} \\ \varphi_{a'b'}(n^{ab}) &= \left( (n_{a'b'}^{ab})_1, (n_{a'b'}^{ab})_2 \right) \end{aligned}$$

on  $n, n^{ab} \in \mathbb{Z}_{N_1 N_2}$ ,  $n_1, (n_{a'b'}^{ab})_1 \in \mathbb{Z}_{N_1}$  i  $n_2, (n_{a'b'}^{ab})_2 \in \mathbb{Z}_{N_2}$ .

Quan els dos superíndexs o els dos subíndexs siguin iguals a la unitat, els suprimirem:

$$\begin{aligned} \varphi_{1,1}^{-1}(n_1, n_2) &= \varphi^{-1}(n_1, n_2) = n^{1,1} = n \\ \varphi_{1,1}(n^{ab}) &= \varphi(n^{ab}) = ((n_{1,1}^{ab})_1, (n_{1,1}^{ab})_2) = ((n^{ab})_1, (n^{ab})_2) \end{aligned}$$

Hom dedueix d'aquestes convencions que:

$$\varphi_{ab}(n^{ab}) = ((n_{ab}^{ab})_1, (n_{ab}^{ab})_2) = (n_1, n_2)$$

L'aplicació  $\varphi_{1,1}$  ens permetrà de rescriure cadascuna de les proposicions que es verifiquen a  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ , en termes d'elements de  $\mathbb{Z}_{N_1 N_2}$  i viceversa, d'acord amb les correspondències següents:

$$\begin{aligned} \varphi_{1,1}(n_{a'b'}^{ab}) &= ((n_{a'b'}^{ab})_1, (n_{a'b'}^{ab})_2) \\ \varphi_{1,1}^{-1}((n_{a'b'}^{ab})_1, (n_{a'b'}^{ab})_2) &= n_{a'b'}^{ab}, \quad \bullet \end{aligned}$$

ja que, en virtut del Corol·lari A.1.1, les sumes i productes a l'espai  $\mathbb{Z}_{N_1 N_2}$  poden ésser rescrits com sumes i productes component a component a l'espai  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ .

*Proposició 6.*  $n_{a'b'}^{ab} = \langle 1_{a'b'}^{ab}, \bullet n \rangle_{N_1 N_2}$ .

Demostració. Per definició de  $n_{a'b'}^{ab}$ , i de les aplicacions  $\varphi_{ab}$ :

$$\begin{aligned} n_{a'b'}^{ab} &= (\varphi_{a'b'} \circ \varphi_{ab}^{-1})(n) = \varphi_{ab}^{-1}[\varphi_{a'b'}(n)] = \varphi_{ab}^{-1}(\langle a'n \rangle_{N_1}, \langle b'n \rangle_{N_2}) \\ &= \langle \langle a'n \rangle_{N_1} \langle aN_2 \rangle^{\phi(N_1)-1} \rangle_{N_1 N_2} + \end{aligned}$$

$$\begin{aligned}
 & + \langle b'n \rangle_{N_2} \langle (bN_1)^{\phi(N_2)-1} \rangle_{N_2} N_1 \rangle_{N_1 N_2} = \\
 & = \langle na'a^{\phi(N_1)-1} N_2 \phi(N_1) + nb'b^{\phi(N_2)-1} N_1 \phi(N_2) \rangle_{N_1 N_2} = \\
 & = \langle \langle a'a^{\phi(N_1)-1} N_2 \phi(N_1) + b'b^{\phi(N_2)-1} N_1 \phi(N_2) \rangle_{N_1 N_2} n \rangle_{N_1 N_2}
 \end{aligned}$$

Fent  $n = 1$ :

$$1_{a,b}^{ab} = \langle a'a^{\phi(N_1)-1} N_2 \phi(N_1) + b'b^{\phi(N_2)-1} N_1 \phi(N_2) \rangle_{N_1 N_2}$$

I, en conseqüència:

$$n_{a,b}^{ab} = \langle 1_{a,b}^{ab} \cdot n \rangle_{N_1 N_2}$$

que és allò que preteníem demostrar. ■

Així, la imatge d'un element  $(n_1, n_2)$  de l'anell  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  per l'autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a,b})$  és el resultat de multiplicar-lo component a component per la imatge de l'element unitat  $(1,1)$ .

*Corol·lari 6.1.* Qualsevol autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a,b})$  és determinada unívocament per la imatge de qualsevol element  $(m_1, m_2) \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  tal que  $(m_1, N_1) = (m_2, N_2) = 1$ .

*Corol·lari 6.2.* Una autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a,b})$  és un automorfisme si i només si la imatge de l'element unitat  $(1,1)$  és idempotent.

*Proposició 7.*  $(1_{a,b}^{ab}, N) = 1$ , on  $N$  prendrà els valors  $N_1 N_2, N_1 \circ N_2$ , segons que hom interpreti l'enunciat a  $\mathbb{Z}_{N_1 N_2}, \mathbb{Z}_{N_1} \circ \mathbb{Z}_{N_2}$ .

*Proposició 8.* Si  $(n, N_1 N_2) = 1$ , llavors  $\exists ! a, a' \in \mathbb{P}_{N_1}$  i  $\exists ! b, b' \in \mathbb{P}_{N_2}$  tals que  $1^{ab} = 1_{a,b} = n$ .

Definirem ara l'operació interna  $\odot$  dins el conjunt

$$\{\psi \in \text{Autoaplicacions } (\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}): \psi(n_1, n_2) = (n_1, n_2) \cdot \psi(1,1)\}$$

Donats dos elements  $\psi_1, \psi_2$  del conjunt esmentat:

$$(\psi_1 \odot \psi_2)(1,1) = (\psi_1 \circ \psi_2)(1,1) = \psi_2(\psi_1(1,1))$$

I per la Proposició 6:

$$(\psi_1 \odot \psi_2)(1,1) = \psi_1(1,1) \cdot \psi_2(1,1)$$

Observeu que, en general,  $\psi_1 \odot \psi_2 \neq \psi_1 \circ \psi_2$ , encara que coincideixin per a  $(1,1)$ .

De les tres anteriors proposicions es desprèn la següent caracterització de les autoaplicacions  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$ :

*Proposició 9.* Els quatre grups multiplicatius següents són isomorfs:

- (a)  $( \{ (\varphi_{ab}^{-1} \circ \varphi_{a'b'}) \} , \cdot ) =$   
 $( \{ \psi \in \text{Autoaplicacions } (\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}): \psi (n_1, n_2) = (n_1, n_2) \cdot \psi (1,1) \} ,$   
 $( \{ \psi \in \text{Endoaplicacions } (\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}): \psi (n_1, n_2) = (n_1, n_2) \cdot \psi (1,1)$   
 $i ((\psi (1,1))_1, N_1) = ((\psi (1,1))_2, N_2) = 1 \} , \odot )$
- (b)  $( \{ 1_{a'b'}^{ab} \} , \cdot ) = ( \{ 1^{ab} \} , \cdot ) = ( \{ 1_{a'b'} \} , \cdot ) = (\mathbb{P}_{N_1 N_2} , \cdot )$
- (c)  $( \{ (\psi_1, \psi_2) \in \text{Endoapl. } (\mathbb{Z}_{N_1}) \times \text{Endoapl. } (\mathbb{Z}_{N_2}): \psi_i (n_i) = n_i \cdot \psi_i (1)$   
 $i (\psi_i (1), N_i) = 1, i = 1, 2 \} , \odot )$
- (d)  $( \{ (1_{a'b'}^{ab})_1 \} \times \{ (1_{a'b'}^{ab})_2 \} , \cdot ) = (\mathbb{P}_{N_1} \times \mathbb{P}_{N_2}, \cdot )$

Demostració. De la Proposició 6 se segueix que:

$$\{ (\varphi_{ab}^{-1} \circ \varphi_{a'b'}) \} \subseteq \{ \psi \in \text{Autoaplicacions } (\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}):$$

$$: \psi (n_1, n_2) = (n_1, n_2) \cdot \psi (1,1) \}$$

I, per la Proposició 7 i el Corol·lari A.2.2, les autoaplicacions considerades són totes bijectives.

D'altra banda, segons el Corol·lari A.2.2, condició necessària i suficient perquè qualsevol endoaplicació  $\psi$ , que verifiqui  $\psi (n_1, n_2) = (n_1, n_2) \cdot \psi (1,1)$ , sigui bijectiva és que  $((\psi (1,1))_1, N_1) = ((\psi (1,1))_2, N_2) = 1$ .

La Proposició 8 garanteix finalment que qualsevol endoaplicació  $\psi$  d'aquest tipus pot ésser escrita  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$ .

Queda així demostrada la igualtat dels tres primers conjunts esmentats a l'apartat (a) de l'enunciat.

El fet que aquests conjunts, juntament amb l'operació  $\odot$ , constitueixin un grup multiplicatiu és conseqüència immediata de la definició de  $\odot$  i de la Proposició 6.

Les igualtats dels conjunts de l'apartat (b) deriven directament de les Proposicions 7 i 8.

Finalment, en virtut del Corol·lari 6.1, l'isomorfisme entre els grups multiplicatius (a) i (b) pot ésser definit de la manera següent:

$$\begin{aligned} \{ (\varphi_{ab} \circ \varphi_{a'b'}) \} &\longrightarrow \mathbb{P}_{N_1 N_2} \\ \psi &\longrightarrow \psi (1,1) \\ \psi \odot \eta &\longrightarrow \psi (1,1) \cdot \eta (1,1) \end{aligned}$$

D'altra banda, interpretant les Proposicions 6, 7 i 8 a  $\mathbb{Z}_{N_i}$ , i seguint un raonament anàleg a l'anterior, hom obté un isomorfisme entre els grups multiplicatius (c) i (d).

L'isomorfisme entre els grups (b) i (d) és assegurat pel Corol·lari A.1.2. ■

Conseqüència immediata de l'apartat (b) de l'anterior proposició és que qualsevol autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  pot ésser pensada com a composició d'una aplicació inversa  $\varphi_{c'd}^{-1}$  i l'aplicació unitària directa  $\psi_{1,1}$ ; o bé, com a composició de l'aplicació unitària inversa  $\psi_{1,1}^{-1}$  i una aplicació directa  $\varphi_{c'd}$ .

Una altra conseqüència d'interès pràctic és que cada autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  de  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  pot ésser descomposta en una autoaplicació de  $\mathbb{Z}_{N_1}$  i una autoaplicació de  $\mathbb{Z}_{N_2}$ . És a dir, la reordenació d'elements subjacent a una operació bidimensional, com per exemple la TFD o la convolució circular, efectuada via les aplicacions  $\varphi_{ab}$ , pot ésser descomposta en una reordenació de files i una reordenació de columnes.

*Corol·lari 9.1.*  $1_{a'b}^{ab} = 1_{c'd}^{cd}$ , si i només si:

$$\langle a'a\phi^{(N_1)-1} \rangle_{N_1} = \langle c'c\phi^{(N_1)-1} \rangle_{N_1}$$

$$\langle b'b\phi^{(N_2)-1} \rangle_{N_2} = \langle d'd\phi^{(N_2)-1} \rangle_{N_2}$$

*Corol·lari 9.2.* El nombre d'autoaplicacions de  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  del tipus  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  és  $\varphi(N_1) \cdot \varphi(N_2)$ .

Gràcies a la caracterització de les autoaplicacions  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  donada per la Proposició 9, aquestes hereten totes les propietats dels nombres pertanyents a  $\mathbb{P}_{N_1 N_2}$ ; en particular, l'existència d'elements inversos respecte a  $\odot$  i  $+$ . Caracteritzarem a continuació la forma que prendran aquests elements invers i oposat, mitjançant un parell de proposicions.

*Proposició 10.*  $1_{a'b}^{ab} = 1_{a^*b^*}^{ab} \cdot 1_{a'b}^{a^*b^*}$

*Corol·lari 10.1.*  $(1_{a'b}^{ab})^{-1} = 1_{ab}^{a'b'}$

*Corol·lari 10.2.*  $1_{a'b}^{ab} = 1_{ab}^{a'b'}$  si i només si  $(1_{a'b}^{ab})^2 = 1$

*Corol·lari 10.3.* La relació definida dins el conjunt  $\{1_{ab}\}$  de la manera següent:

$$1_{ab} R 1_{cd} \iff 1_{ab}^{cd} = 1_{cd}^{ab}$$

és d'equivalència.

*Proposició 11.*  $1_{a'b'}^{ab} + 1_{(N_1-a')(N_2-b')}^{ab} = 0$

*Corol·lari 11.1.*  $1_{(N_1-a)(N_2-b)}^{ab} = 1_{ab}^{(N_1-a)(N_2-b)} = N-1$  on  $N$  pot prendre els valors  $N_1N_2, N_1 \circ N_2$ , segons que hom interpreti l'enunciar a  $\mathbb{Z}_{N_1N_2}, \mathbb{Z}_{N_1} \circ \mathbb{Z}_{N_2}$ .

### 3.2. Invariants per les autoaplicacions $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$

Caracteritzarem a continuació els elements de  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$  que romanen invariants per les autoaplicacions  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$ . Ens restringirem, en primer lloc, als elements invariants per una sola autoaplicació, i estudiarem seguidament els comuns a més d'una autoaplicació.

*Proposició 12.* Els únics elements  $n \in \mathbb{Z}_N$  invariants per l'autoaplicació  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  són els següents:

$$n = \frac{k N}{((1_{a'b'}^{ab}, -1), N)}, \quad k = 0, 1, \dots, ((1_{a'b'}^{ab}, -1), N) - 1$$

on  $N$  pot ésser reemplaçat per  $N_1N_2, N_1 \circ N_2$ .

*Demostració.*  $n \in \mathbb{Z}_N$  és invariant per  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  només si:

$$n_{a'b'}^{ab} = n$$

O, per la Proposició 6:

$$\langle 1_{a'b'}^{ab}, \cdot n \rangle_N = n$$

Per tant,

$$\langle (1_{a'b'}^{ab}, -1) \cdot n \rangle_N = 0$$

I, consegüentment:

$$n = \frac{k N}{((1_{a'b'}^{ab}, -1), N)}, \quad k = 0, 1, \dots, ((1_{a'b'}^{ab}, -1), N) - 1. \quad \blacksquare$$

Definim ara el conjunt d'invariants per una autoaplicació  $(\varphi_{a'b'}^{-1} \circ \varphi_{a'b'})$  com:

$$I_{a'b'}^{ab} = \left\{ n \in \mathbb{Z}_N : n = \frac{kN}{((1_{a'b'}^{ab} - 1), N)}, k = 0, 1, \dots, ((1_{a'b'}^{ab} - 1), N) \right\}$$

*Corol·lari 12.1.* La inclusió de conjunts "C" estableix una relació d'ordre parcial dins el cojunt  $\{ I_{a'b'}^{ab} \} \subseteq$

$$\subseteq \left\{ \left\{ n \in \mathbb{Z}_N : n = k \cdot d, k = 0, 1, \dots, \frac{N}{d} - 1 \right\} : d \in \mathbb{Z}_N \wedge (d, N) = d \right\}$$

$$\subseteq \mathcal{P}(\mathbb{Z}_N)$$

essent  $\mathcal{P}(\mathbb{Z}_N)$  el conjunt de parts de  $\mathbb{Z}_N$ .

*Corol·lari 12.2.*  $I_{a'b'}^{ab} = I_{c'd}^{cd}$ , si i només si:

$$((1_{a'b'}^{ab} - 1), N) = ((1_{c'd}^{cd} - 1), N).$$

*Corol·lari 12.3.* Si  $(N, 2) = 1$ , llavors l'únic invariant global, és a dir, l'únic invariant per totes les autoaplicacions  $(\varphi_{a'b'}^{-1} \circ \varphi_{a'b'})$  és  $n = 0$ .

Si  $(N, 2) = 2$ , els únics invariants globals són  $n = 0$  i  $n = N/2$ .

El fet que, en els enunciats de la proposició i corol·laris anteriors,  $N$  pugui ésser substituïda per  $N_1 N_2$ ,  $N_1$  o  $N_2$ , té una implicació interessant: els invariants de  $\mathbb{Z}_{N_1}$  o  $\mathbb{Z}_{N_2}$  han d'ésser interpretats com invariants "relatius", en el sentit que canvien de posició però sense moure's d'una determinada fila o columna. Així, per exemple, els elements de la fila 0 canvien de posició però mantenint-se sempre dins la fila 0.

Observeu que aquesta interpretació no afecta en absolut el nombre d'invariants globals, que segueix essent 1 (l'element  $(0,0)$ ) en el cas que  $(N_1 N_2, 2) = 1$ , i 2 en el cas  $(N_1 N_2, 2) = 2$ . En aquest darrer cas, i a causa de la restricció inicial segons la qual  $(N_1, N_2) = 1$ , es verifica que o bé  $(N_1, 2) = 1$ , o bé  $(N_2, 2) = 1$ , però no es poden donar ambdós casos. Així, doncs, els elements invariants seran el  $(0,0)$ , i el  $(N_1/2, 0)$  o bé el  $(0, N_2/2)$ .



3.3. Autoaplicacions  $(\varphi_{ab}^{-1} \circ \varphi_{a'b'})$  subjacents a la TFD i a la convolució circular

Estudiarem a continuació el nombre i tipus de reordenacions d'elements que es poden donar en avaluar TFD's i convolucions circulars utilitzant les aplicacions  $\varphi_{ab}$ .

Definim, en primer lloc, el conjunt d'autoaplicacions subjacent al càlcul de la TFD via aplicacions  $\varphi_{ab}$ :

$$\mathcal{F} = \{ 1_{a^*b^*}^{ab} : \langle a a^* N_2 \rangle_{N_1} = \langle b b^* N_1 \rangle_{N_2} = 1 \}$$

*Proposició 13.* Si  $1_{a^*b^*}^{ab} \in \mathcal{F}$ ,  $1_{a^*b^*}^{ab} = 1 \langle a^2 N_2 \rangle_{N_1} \langle b^2 N_1 \rangle_{N_2} = 1 \langle a^{*2} N_2 \rangle_{N_1} \langle b^{*2} N_1 \rangle_{N_2}$ .

Demostració. Suposem  $1_{a^*b^*}^{ab} = 1^{cd}$ . Pel Corol·lari 9.1,

$$\langle a^* a \phi(N_1)^{-1} \rangle_{N_1} = \langle c \phi(N_1)^{-1} \rangle_{N_1}$$

$$\langle b^* b \phi(N_2)^{-1} \rangle_{N_2} = \langle d \phi(N_2)^{-1} \rangle_{N_2}$$

Aplicant el Corol·lari A.2.1:

$$c = \langle (a^* a \phi(N_1)^{-1}) \phi(N_1)^{-1} \rangle_{N_1} = \langle a^* \phi(N_1)^{-1} a \rangle_{N_1}$$

$$d = \langle (b^* b \phi(N_2)^{-1}) \phi(N_2)^{-1} \rangle_{N_2} = \langle b^* \phi(N_2)^{-1} b \rangle_{N_2}$$

I tenint en compte que  $\langle aa^* N_2 \rangle_{N_1} = \langle bb^* N_1 \rangle_{N_2} = 1$ ,

$$c = \langle a^2 N_2 \rangle_{N_1}$$

$$d = \langle b^2 N_1 \rangle_{N_2}$$

Amb què queda demostrada la primera igualtat. Quant a la segona, suposem que  $1_{a^*b^*}^{ab} = 1_{c'd'}$ , novament pel Corol·lari 9.1:

$$\langle a^* a \phi(N_1)^{-1} \rangle_{N_1} = c'$$

$$\langle b^* b \phi(N_2)^{-1} \rangle_{N_2} = d'$$

I tenint en compte que  $\langle aa^* N_2 \rangle_{N_1} = \langle bb^* N_1 \rangle_{N_2} = 1$ :

$$c' = \langle a^{*2} N_2 \rangle_{N_1}$$

$$d' = \langle b^{*2} N_1 \rangle_{N_2}$$

Amb què queda demostrada la segona igualtat. ■

*Corol·lari 13.1.* Si  $1_{a^*b^*}^{ab}, 1_{c^*d^*}^{cd} \in \mathcal{F}$ , llavors  $1_{a^*b^*}^{ab} = 1_{c^*d^*}^{cd}$  si i només si:

$$\langle a^2 \rangle_{N_1} = \langle c^2 \rangle_{N_1}$$

$$\langle b^2 \rangle_{N_2} = \langle d^2 \rangle_{N_2}$$

*Corol·lari 13.2.* [ $1_{a^*b^*}^{ab} \in \mathcal{F} \wedge 1_{a^*b^*}^{ab} = 1$ ] si i només si:

$$\langle a^2 \rangle_{N_1} = \langle a^{*2} \rangle_{N_1} = \langle N_2^{\phi(N_1)-1} \rangle_{N_1}$$

$$\langle b^2 \rangle_{N_2} = \langle b^{*2} \rangle_{N_2} = \langle N_1^{\phi(N_2)-1} \rangle_{N_2}$$

*Proposició 14.* Els quatre conjunts següents tenen el mateix cardinal:

(a)  $\mathcal{F}$

(b)  $\{ (n_1, n_2) \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} : n_1 = \langle a^2 \rangle_{N_1}, n_2 = \langle b^2 \rangle_{N_2}, \\ a \in \mathbb{P}_{N_1}, b \in \mathbb{P}_{N_2} \}$

(c)  $\{ n \in \mathbb{Z}_{N_1 N_2} : n = p^2, p \in \mathbb{P}_{N_1 N_2} \}$

(d) el conjunt quocient  $\{ 1_{ab} \} / R$ , essent  $R$  la relació d'equivalència definida al Corol·lari 10.3.

*Demostració.* Que els conjunts dels apartats (a) i (b) tenen el mateix cardinal és conseqüència immediata del Corol·lari 13.1. El Corol·lari A.1.2 assegura la igualtat dels cardinals dels conjunts dels apartats (b) i (c). Finalment, per definició de la relació  $R$ , i en virtut del Corol·lari 10.2:

$$\begin{aligned} 1_{ab} R 1_{cd} &\iff 1_{ab}^{cd} = 1_{cd}^{ab} \iff \\ &\iff (1_{ab}^{cd})^2 = 1 \iff \\ &\iff 1_{a^2 b^2}^{c^2 d^2} = 1 \iff \\ &\iff 1_{a^2 b^2}^{c^2 d^2} \quad 1_{c^2 d^2} = 1_{c^2 d^2} \iff \\ &\iff 1_{a^2 b^2} = 1_{c^2 d^2} \iff \\ &\iff \langle a^2 \rangle_{N_1} = \langle c^2 \rangle_{N_1} \wedge \langle b^2 \rangle_{N_2} = \langle d^2 \rangle_{N_2} \end{aligned}$$

Això demostra que els conjunts dels apartats (b) i (d) tenen el mateix cardinal. ■

*Corol·lari 14.1.* La següent aplicació és bjectiva:

$$\begin{aligned} \mathcal{F} &\longrightarrow \{1_{ab}\}/R \\ 1_{a^*b^*}^{ab} &\longrightarrow [1_{ab}] \end{aligned}$$

*Corol·lari 14.2.*  $[1_{a^*b^*}^{ab} = 1_{c^*d^*}^{cd}, \quad \forall 1_{a^*b^*}^{ab}, 1_{c^*d^*}^{cd} \in \mathcal{F}]$  si i només si  $[1_{cd}^{ab} = 1_{ab}^{cd}, \quad \forall a, c \in \mathbb{P}_{N_1}, \quad \forall b, d \in \mathbb{P}_{N_2}]$

Aquest darrer corol·lari és interessant perquè assegura que hi haurà una única reordenació d'elements subjacent al càlcul de la TFD via aplicacions  $\varphi_{ab}$ , si i només si:

$$\begin{aligned} &\forall a, a' \in \mathbb{P}_{N_1} \\ (\varphi_{ab}^{-1} \circ \varphi_{a'b'}) &= (\varphi_{a'b'}^{-1} \circ \varphi_{ab}), \\ &\forall b, b' \in \mathbb{P}_{N_2} \end{aligned}$$

Passem seguidament a estudiar el cas de la convolució circular. Definim el conjunt de totes les autoaplicacions subjacents a la realització d'aquesta operació via aplicacions  $\varphi_{ab}$ :

$$\mathcal{C} = \{ 1_{a',b}^{ab}, : a = a' \text{ i } b = b' \} = \{ 1 \}$$

Trivialment, doncs, l'única autoaplicació subjacent a l'avaluació de la convolució circular via aplicacions  $\varphi_{ab}$  és la identitat. En altres paraules, no hi ha reordenació d'elements.

#### 4. CONCLUSIONS

L'objectiu del present treball era d'estudiar possibles implementacions unidimensionals de la TFD i la convolució circular bidimensionals, que permetessin d'aprofitar els recents desenvolupaments que s'han produït en el terreny de les tecnologies CCD i SAW, donant lloc a dispositius intrínsecament lineals i extremament ràpids.

En aquesta línia, han estat caracteritzades unes correspondències entre representacions uni- i bidimensionals de les dades, que permeten d'efectuar les operacions en una o dues dimensions indistintament. La implementació d'aquestes correspondències és extremament simple, ja que consisteix a escombrar la imatge, considerant que en lloc d'un rectangle hom té un tor (identificant costats oposats) i usant-hi una recta de pendent adequat perquè puguin passar per tots els punts del reticle obtingut en discretitzar.

En particular, pel que fa a la TFD, ha estat demostrada l'existència de parelles de correspondències tals que l'aplicació d'una d'elles al domini espacial equival a l'aplicació de l'altra al domini freqüencial. Aquest resultat permet de dur a terme TFD's bidimensionals mitjançant una única aplicació de l'algorisme unidimensional, simplement utilitzant una correspondència 2D-1D qualsevol per a transformar la funció bidimensional en unidimensional; i la seva parella, per a dur a terme la transformació inversa una vegada calculada ja la TFD. Anàlogament, una TFD unidimensional pot ésser calculada per mitjans bidimensionals.

Ha estat demostrat que l'esforç computacional és lleugerament inferior en el cas de calcular la TFD per mitjans bidimensionals, que en el cas de fer-ho unidimensionalment, tendint a ésser el mateix quan el nombre de punts s'apropa a l'infinit.

Quant a la convolució circular, ha estat demostrat que la mateixa correspondència existent entre les representacions uni- i bidimensionals de dues funcions és la que es dona entre les representacions uni- i bidimensionals de llur producte de convolució. Això possibilita el càlcul de convolucions circulars bidimensionals com si es tractés de llurs homònimes unidimensionals, simplement utilitzant una correspondència 2D-1D qualsevol per a transformar les funcions bidimensionals en unidimensionals i dur a terme la transformació inversa després d'haver calculat la convolució unidimensional corresponent. És clar que, d'una forma anàloga, una convolució circular unidimensional pot ésser calculada per mitjans bidimensionals.

Ha estat descrita una implementació unidimensional de la convolució circular bidimensional, que fa ús de dispositius lineals (tipus CCD) i suposa una reducció del temps de computació del 50% respecte a la seva implementació bidimensional.

Finalment, les propietats de les autoaplicacions de  $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ , resultants de la composició d'una correspondència 2D-1D amb una altra 1D-2D, han estat estudiades i ha estat demostrat que el seu conjunt, juntament amb un producte adientment definit, formen un grup multiplicatiu isomorf al subgrup de  $(\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}, \cdot)$  format pels parells ordenats d'elements primers amb  $N_1$  i  $N_2$ , respectivament. Conseqüència pràctica d'aquest resultat és que la reordenació d'elements subjacent a la TFD o la convolució circular bidimensionals, calculades via correspondències 2D-1D, pot ésser descomposta en una reordenació de files i una reordenació de columnes. Després de caracteritzar els elements invariants per aquestes autoaplicacions, hem procedit a l'estudi detallat d'aquelles subjacentes a la TFD, i hem demostrat que n'hi ha tantes com elements de  $\mathbb{Z}_{N_1 N_2}$  que són quadrats perfectes d'elements primers amb  $N_1 N_2$ .

Hem efectuat dues aplicacions al Processament Digital d'Imatges, l'una consistent en la segmentació de la imatge d'una peça mecànica, i l'altra, en la localització dels forats continguts en aquesta peça. Per raons d'espai no han estat recollides en el present resum.

En síntesi, les correspondències 2D-1D possibiliten la implementació unidimensional d'operacions bidimensionals tals com la TFD o la convolució circular, permetent així d'aprofitar la rapidesa de dispositius unidimensionals desenvolupats darrerament basats en tecnologies CCD i SAW. Pel fet que els sistemes de visió utilitzats en entorns industrials han de dur a terme el tractament de les imatges en temps real, aquest sembla un camp adient on explorar amb més detall, en el futur, els avantatges i inconvenients derivats de la utilització de les correspondències 2D-1D. El fet que els resultats obtinguts siguin generalitzables al cas n-dimensional, i en particular al cas de correspondències 3D-1D, sembla també d'interès, vista l'actual tendència a l'estudi i desenvolupament de sistemes de visió tridimensional.

### APÈNDIX A. NOCIONS DE TEORIA ELEMENTAL DE NOMBRES

Un tractament detallat dels teoremes enunciats en el present apèndix es troba a Borevitch i Chafarevitch (1967) i Vinogradov (1977).

*Proposició A.1.* (Teorema del reste xinès). Si  $n_1, n_2, \dots, n_k$  són nombres enters primers dos a dos, llavors el sistema d'equacions:

$$\{ \langle x \rangle_{n_i} = r_i, i = 1, 2, \dots, k \}$$

té una solució única en  $\mathbb{Z}_{\prod_{s=1}^k n_s}$ , que és donada per l'expressió:

$$x = \langle r_1 U_1 N_1 + r_2 U_2 N_2 + \dots + r_k U_k N_k \rangle_{\prod_{s=1}^k n_s}$$

on  $N_i = \frac{\prod_{s=1}^k n_s}{n_i}$  i  $U_i$  és la solució de l'equació  $\langle U_i N_i \rangle_{n_i} = 1, A_i = 1, 2, \dots, k$ .

*Corol·lari A.1.1.* Si  $n_1, n_2, \dots, n_k$  són nombres enters primers dos a dos, llavors l'aplicació:

$$\begin{aligned} \mathbb{Z}_{\prod_{s=1}^k n_s} &\longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} \\ x &\longrightarrow (\langle x \rangle_{n_1}, \langle x \rangle_{n_2}, \dots, \langle x \rangle_{n_k}) \end{aligned}$$

és un isomorfisme d'anells, la inversa del qual és donada per:

$$\begin{aligned} \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} &\longrightarrow \mathbb{Z}_{\prod_{s=1}^k n_s} \\ (r_1, r_2, \dots, r_k) &\longrightarrow \langle r_1 U_1 N_1 + r_2 U_2 N_2 + \dots + r_k U_k N_k \rangle_{\prod_{s=1}^k n_s} \end{aligned}$$

on  $N_i$  i  $U_i$  són definides com a la Proposició A.1.

*Corol·lari A.1.2.* Si  $n_1, n_2, \dots, n_k$  són nombres primers dos a dos, llavors l'isomorfisme d'anells:

$$\begin{aligned} \mathbb{Z}_{\prod_{s=1}^k n_s} &\longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} \\ x &\longrightarrow (\langle x \rangle_{n_1}, \langle x \rangle_{n_2}, \dots, \langle x \rangle_{n_k}) \end{aligned}$$

fa correspondre al conjunt  $\mathbb{P}_{\prod_{s=1}^k n_s} \subset \mathbb{Z}_{\prod_{s=1}^k n_s}$ , el conjunt  $\mathbb{P}_{n_1} \times \mathbb{P}_{n_2} \times \dots \times \mathbb{P}_{n_k}$ .

El cardinal dels conjunts  $\mathbb{P}_n$ , expressat en funció de "n", és l'anomenada funció d'Euler  $\phi(n)$ .

*Proposició A.2.* (Teorema d'Euler): Si  $(a, n) = 1$ , llavors

$$\langle a^{\phi(n)} \rangle_n = 1.$$

*Corol·lari A.2.1.* Si  $(a, n) = 1$ , llavors l'equació  $\langle ax \rangle_n = 1$  sempre té solució i aquesta és

$$x = \langle a^{\phi(n)-1} \rangle_n$$

*Corol·lari A.2.2.* Si  $(a, n) = 1$ , llavors l'aplicació:

$$\begin{aligned} \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ x &\longrightarrow \langle ax \rangle_n. \end{aligned}$$

és bijectiva i el subconjunt  $\mathbb{P}_n \subset \mathbb{Z}_n$  és tancat per aquesta aplicació.

## APÈNDIX B. COST COMPUTACIONAL DE L'ALGORISME FFT.

Els resultats exposats en el present apèndix han estat derivats seguint les directrius marcades per Brigham (1974), Knuth (1969) i Savage (1976).

Indicarem per # MC i # SC el nombre de multiplicacions i sumes complexes, respectivament. El subíndex C assenyalarà que el vector al qual hom aplica l'algorisme és complex. Substituint C per R obtindren les significacions anàlogues en el cas real.

Suposant que el vector esmentat és de longitud  $N = 2^n$ , llavors:

$$\# MC_C = \left( \frac{n}{2} - 1 \right) N - 1$$

$$\# SC_C = nN$$

Tenint en compte que la multiplicació complexa requereix el còmput de quatre multiplicacions reals així com dues sumes també reals, i que cada suma complexa requereix dues sumes reals, resulta que:

$$\# MR_C = (2n - 4) N - 4$$

$$\# SR_C = (3n - 2) N - 2$$

Si la funció de la qual hom vol calcular la TFD és real, llavors hom pot aplicar l'algorisme FFT d'una forma més eficient que purament posant a zero la part imaginària. Cal només definir un vector complex que tingui part real igual als elements d'índex parell i part imaginària igual als elements d'índex senar, i tenir en compte que la part real d'una TFD és sempre simètrica (ja que depèn de la funció cosinus), mentre que la part imaginària és sempre antisimètrica (perquè depèn de la funció sinus). La TFD de longitud  $N$  queda així reduïda a una TFD de longitud  $N/2$  més una certa reordenació final de les dades.

$$\# MR_R = (2n - 3) \frac{N}{2} - 2$$

$$\# SR_R = (3n - 1) \frac{N}{2} - 8$$

## BIBLIOGRAFIA

1. D. F. BARBE, W. D. BAKER i K. L. DAVIS. "Signal Processing with CCD". *IEEE Journal of Solid-State Circuits*, vol. SC-13, pp. 34-51 (feb. 1978).
2. D. F. BARBE, W. D. BAKER i K. L. DAVIS. "Signal Processing with Charge-Coupled Devices". Dins "Charge-Coupled Devices", editat per D.F. Barke, *Topics in Applied Physics*, vol. 38, Springer-Verlag, 1980.
3. Z. I. BOREVITCH i I. R. CHAFAREVITCH. "Theorie des Nombres", Gauthier-Villars, 1967.
4. E. O. BRIGHAM. "The Fast Fourier Transform", Prentice-Hall, 1974.
5. R. S. BUCY, A. J. MALLINCKRODT i H. YOUSSEF. "High Speed Convolution of Periodic Functions". *SIAM Journal of Mathematical Analysis*, vol. 8, núm. 4, pp. 619-625 (ago. 1977).
6. M. J. B. DUFF i S. LEVIALDI (eds.). "Languages and Architectures for Image Processing", Academic Press, 1981.
7. A. E. FEATHER, L. J. SIEGEL i H. J. SIEGEL. "Image correlation using parallel processing". *Proc. 5th Int. Conf. on Pattern Recognition* (des. 1980).
8. A. GERSHO. "Charge-Transfer Filtering". *Proceedings IEEE*, vol. 67. núm. 2 (feb. 1979).
9. B. K. GILBERT, C. E. STOKMA, C. E. JAMES, L. W. HOBROC, E. S. YANG, K. C. BALLARD i E. H. WOOD. "A real-time hardware system for digital processing of images". *IEEE Trans. on Computers*, vol. C-25, pp. 1089-1100 (1976).
10. I. J. GOOD. "The interaction algorithm and practical Fourier analysis". *J. Royal Statistics Society*, ser. B, vol. 20, pp. 361-372 (1968).
11. I. J. GOOD. "The relationship between two Fast Fourier Transforms". *IEEE Trans. on Computers*, vol. C-20, núm. 3, pp. 310-317 (mars 1971).
12. Y. C. JENQ. "Digital convolution algorithm for pipelining multiprocessor systems". *IEEE Trans. on Computers*, vol. C-30, núm. 12 (des. 1981).
13. L. R. JOHNSON i A. K. JAIN. "An efficient two-dimensional FFT algorithm". *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. PAMI-2, núm. 2 (nov. 1981).
14. C. E. KIM i M. G. STRINTZIS. "High speed multidimensional convolution". *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. PAMI-2, núm. 3 (maig 1980).
15. D. KNUTH. "The Art of Computer Programming", vol. II: "Seminumerical Algorithms", Addison-Wesley, 1969.
16. J. H. McCLELLAN i Ch. M. RADER. "Number Theory in Digital Signal Processing", Prentice-Hall, 1979.
17. C. S. MILLER i T. A. ZIMMERMAN. "The application of Charge-Coupled Devices to Digital Signal Processing". *Conference Records of the IEEE Int. Conf. on Communications*, pp. 220-234 (1975).
18. P. T. MUELLER, L. J. SIEGEL i H. J. SIEGEL. "Parallel algorithms for the two-dimensional FFT". *Proc. of the 5th Int. Conf. on Pattern Recognition* (des. 1980).



19. G. R. NUDD. "CCDs image processing circuitry". *Proc Image Understanding Workshop*, SAI-78-549-WA, 1977.
20. D. R. REDDY i R. W. HON. "Computer Architectures for Vision". Dins "*Computer Vision and Sensory-Based Robots*", editat per G.G. Dodd i L. Rossol, Plenum Press, 1979.
21. J. E. SAVAGE. "*The Complexity of Computing*", Wiley & Sons, 1976.
22. I. VINOGRADOV. "*Fundamentos de Teoría de Números*", MIR, 1977.
23. T. J. WILLETT i N. BLUZZER. "CCD implementation of an image segmentation algorithm". *Proc. Image Understanding Workshop*, SAI-78-656-WA, 1977.
24. S. WINOGRAD. "On computing the discrete Fourier transform". *Mathematics of Computation*, vol. 32, núm. 141, pp. 175-199 (gen. 1978).
25. P. A. WINSTON. "M.I.T. progress in understanding images". *Proc. Image Understanding Workshop*, SAI-79-749-WA, 1978.