SEPTIEME COLLOQUE SUR LE TRAITEMENT DU SIGNAL ET SES APPLICATIONS

NICE du 28 MAI au 2 JUIN 1979

CORRELATION ET CONVOLUTION PAR TRANSFORMEES ENTIERES.

Y. GRANDCLAUDE et J.Y. RANCHIN.

Conservatoire National des Arts et Métiers. 292, rue Saint Martin 75003 PARIS.

RESUME

La corrélation et la convolution de données en quantité demande des temps rapidement prohibitifs par calcul direct. L'emploi de la transformation de Fourier rapide (TFR) réduit ces temps, mais insuffisamment encore dans certains cas. Pour cette raison, nous avons essayé d'employer des transformées discrètes modulo un nombre entier.

Les caractéristiques des signaux à traiter nous ont conduit à utiliser une transformation bidimensionnelle modulo $2^{S.2^t}+1$ où S est entier impair.

Les algorithmes ont été installés sur un microprocesseur MC 6 800. La corrélation est réalisée 2,4 à 3 fois plus rapidement que par la TFR.

L'emploi de la microprogrammation sur une machine(mots de 16 bits)rend l'exécution 100 fois plus rapide.

La fabrication d'un opérateur microprogrammé est en cours d'étude.

SUMMARY

Correlation and convolution of large sample data are performed in a too long time by direct algorithm. The use of FFT allows better results but insufficient for real time purpose in several cases. For this reason, we tried to implement discrete transforms modulo an integer.

The caracteristics of the signals to be processed lead to bidimensionnal transform modulo $2^{S.2^t}+1$, S being odd integer.

The correlation has been implemented on MC 6 800 microprocessor. It is performed 2.4 to 3 times faster than FFT.

With the use of microprogramming on a 16 bits computer it is possible to run 100 times faster.

We are planning to build a specialized micro programmed operator.

CORRELATION ET CONVOLUTION PAR TRANSFORMEES ENTIERES.

INTRODUCTION.

Il est toujours souhaitable de réaliser des prétraitements du signal sur le site d'acquisition des données. Il est indispensable de le faire lorsque leur quantité est considérable, - devenant prohibitive pour leur transmission - et qu'il existe un moyen de la réduire. Il en est de même lorsque des décisions doivent être prises dans l'instant.

Dans ces deux cas deux traitements de nature voisine sont parfois employés : convolution ou corrélation entre un signal émis et un signal reçu.

La réalisation numérique de la convolution ou de la corrélation peut être faite par calcul direct :

Si x et h sont les deux signaux

$$C_k = \sum_n x_n \cdot h_{n-k} \quad \text{ou} \quad C_k = \sum_n x_n \cdot h_{n+k}$$

Le nombre d'opérations est proportionnel au produit des bornes de k et n.

D'autres techniques permettent de réduire le nombre d'opérations :

- en utilisant la transformée de Walsh-Hadamard (D.A. PITASSI (1) elle s'applique pour un nombre d'entrées petit.
- en utilisant la propriété de convolution : Si, $*$ l'opération de convolution, $\mathcal{T}$ est une transformation, elle possède cette propriété par :

$$\mathcal{T}(V * R) = \mathcal{T}(V) . \mathcal{T}(R).$$

Parmi ces transformations, la plus utilisée est celle de Fourier dans sa version discrète par algorithme rapide (E.O. BRIGHAM (2)).

Nous étudions ici l'apport des transformées opérant dans un anneau d'entiers, modulo un entier donné et le comparons à la T.F.R. (transformée de Fourier Rapide) et au calcul direct.

1. DEFINITIONS ET PROPRIETES.

1.1. Structure des transformations ayant la propriété de convolution.

Soit une transformation discrète, représentée par la matrice T d'élément courant $t_{k,m}$

k et m = 0,1,2,... N-1.

R. AGARWAL et C. BURRUS (3) notamment, ont établi que la propriété de convolution est équivalente à $t_{k,m} = t_{k,1}^{\ m}$ donc $t_{k,m}^{\ N} = 1$ c'est-à-dire que $t_{k,m}$ est racine nième de l'unité.

Prenant $t_{1,1} = \alpha$ racine d'ordre N, $t_{k,m} = \alpha^{km}$.

Une telle transformation est orthogonale et les éléments $t'_{k,m}$ de T^{-1} sont donnés par :

$$t'_{k,m} = N^{-1} . \alpha^{-km}.$$

La transformée d'une suite $(x)_k$ s'écrit :

$$\mathcal{T}(x) = X \ , \ X_k = \sum_{n=o}^{N-1} x_n \alpha^{nk}$$

$$\mathcal{T}^{-1}(X) = x \quad x_n = \frac{1}{N} . \sum_{k=o}^{N-1} X_k \alpha^{-nk}.$$

Dans le corps des complexes $= e^{-\frac{2j\pi}{N}}$ est la seule racine ayant cette propriété, elle conduit à la transformation de Fourier.

Dans un ensemble fini et plus précisément un anneau on peut trouver d'autres racines .

1.2. Transformations dans un anneau d'entiers modulo un entier donné.

Pour calculer une convolution dans un domaine discret, les opérations faites pour un domaine continu dans le corps des complexes peuvent l'être dans un anneau d'entiers muni d'une somme et d'un produit modulo un entier F.

Un entier α remplace alors $e^{\frac{-2j\pi}{N}}$

La suite résultant du calcul sera congrue à la convolution des suites de départ modulo F.

Le résultat sera non ambigu si elles ont une dynamique telle que $|y| \leq \frac{F}{2}$.

Soit $F = p_1^{r}1 . p_2^{r}2 \ldots p_1^{r}1$ la décomposition de F en facteurs premiers. On trouve dans (3) la démonstration du théorème suivant :

Une transformation $\mathcal{T}$ ayant la propriété de convolution dans l'anneau des entiers existe si et seulement si N est diviseur de $(p_1-1),(p_2-1),\ldots(p_1-1)$.

1.3. Conditions d'efficacité.

Pour que de telles transformations soient pratiquement efficaces, il faut que :

- N soit une puissance de 2 ou de 3 pour pouvoir accélérer l'exécution par un algorithme rapide,
- les multiplications par les puissances de soient simples à réaliser,
- F ait une représentation à petit nombre de bits c'est-à-dire un mot court pour faciliter les opérations modulo F.

2. LES CHOIX POSSIBLES.

2.1. $F = 2^k$. N est alors limité à 1. par le théorème précédent.

2.2. $F = 2^k-1$. nombre de Mersenne.

RADER (4) a démontré l'existence d'une transformation si k est premier. D'après le théorème de Fermat : pour k premier et a entier, k divise a^k-a,

La longueur de la transformée est k pour $\alpha = 2$.

Elle est de 2 k pour $\alpha = -2$.

Elle impose des mots très longs.

2.3. $F = 2^k+1$

Cas où $k = 2^t$ il s'agit des nombres de Fermat.

2 est racine d'ordre $2k = 2^{t+1}$

Les facteurs premiers sont la forme $K.2^{t+2} + 1$. ainsi 2^{t+2} est diviseur de $(p_1-1)\ (p_2-1)\ldots(p_1-1)$.

La longueur de la transformée est $4k = 2^{t+2}$.

La racine $\alpha' = 2^{2^{t-2}} . (2^{2^{t-1}} -1)$. notée $\alpha^{\frac{1}{2}}$ ou $\sqrt{2}$ car $\alpha^2 = 2$ mod. F.

Le nombre de bits de représentation grandit rapidement comme on le voit dans le tableau suivant :

t	F	k	N pour α=2.	N pour $\alpha = \sqrt{2}$.
3	$2^8 + 1$	8	16	32
4	$2^{16}+ 1$	16	32	64
5	$2^{32}+ 1$	32	64	128
6	$2^{64}+ 1$	64	128	256

Agarwal et Burrus (3) proposent alors d'utiliser des nombres $F = 2^{S.2^t+1}$ où S est impair.

Cas où $k = S.2^t$.

On trouve $N = 2^{t+1}$ pour $\alpha = 2^S$

et $N = 2^{t+2}$ pour $\alpha^{\frac{1}{2}} = (2^S)^{\frac{1}{2}}$.

$(2^S)^{\frac{1}{2}} = 2^{(S-1)/2 + S.2^{t-2}} . (2^{S.2^{t-1}} -1)$.

Le tableau récapitulatif est alors :

t	S	F	k	N pour $=2^S$	N pour $=(2^S)^{\frac{1}{2}}$
3	3	$2^{24} + 1$	24	16	32
3	5	$2^{40} + 1$	40	16	32
4	3	$2^{48} + 1$	48	32	64

La dimension de la transformée est limitée, mais pour des séquences courtes à grande dynamique elles n'obligent plus à doubler la longueur des mots.

2.4. $F = 2^q \pm 1$. avec q composé.

H. NUSSBAUMER (5) a défini des nombres pseudo Mersenne : $\frac{2^u - 1}{2^{u'} - 1}$

pseudo Fermat : $\frac{2^u + 1}{2^{u'} + 1}$.

Les dimensions ne sont pas des puissances de 2, ce qui ne permet pas d'employer un algorithme très rapide et la complexité des calculs est plus grande que pour les transformations de Fermat.

2.5. Convolution bidimensionnelle.

Dans le meilleur des cas la dimension de la transformée est 4 k pour $F = 2^{k+1}$ où $k = 2^t$.

R.AGARWAL et C. BURRUS (6) ont étudié une convolution bidimensionnelle qui permet de porter la dimension à $8.k^2$.

Les résultats principaux sont les suivants.

Pour $(x)_n$ et $(h)_n$ n = 0,1,... N-1.

Posons N = LP. et construisons deux suites bidimensionnelles (2 L x P) : h' (i,j) et x' (k,l).

CORRELATION ET CONVOLUTION PAR TRANSFORMEES ENTIERES.

comme suit :

$$h'(i,j) = h(jL + i - L) \quad \begin{matrix} i = 0,1,\dots 2l-1 \\ j = 0,1,\dots P-1. \end{matrix}$$

$$x'(k,l) = \begin{cases} x(lL+k). & k = 0,1,\dots L-1. \\ 0. & k = L, L+1,\dots 2L-1. \end{cases} \quad l = 0,1,\dots P-1.$$

Si y' (i,j) est la convolution bidimensionnelle de x' et y', et y la convolution de x et y.

$$y(jL + i) = y'(i + L, j).$$

Ici P et 2 L doivent être une puissance de 2, $P \leq 4k$, $2l \leq 4k$ d'où $N = PL \leq 8k^2$.

Le tableau récapitulatif est alors pour une transformation de Fermat.

t	k	F	$N(\alpha = 2)$	$N(\alpha = \sqrt{2})$
4	16	$2^{16} + 1$	512	2048
5	32	$2^{32} + 1$	2048	8192
6	64	$2^{64} + 1$	8192	32768

Pour une transformation $F = 2^{S.2^t} + 1$

t	$S.2^t$	F	$N(\alpha = 2^S)$.	$N(\alpha = (2^S)^{\frac{1}{2}}$
3	24	$2^{24} + 1$	128	512
3	40	$2^{40} + 1$	128	512
4	48	$2^{48} + 1$	512	2048

Nous atteignons avec ces transformations des longueurs de suites importantes pour des longueurs de mots relativement réduites tout en conservant les autres propriétés des transformations mono - dimensionnelles d'origine.

3. CHOIX PRATIQUE D'UNE TRANSFORMATION.

Connaissant la longueur N des suites d'entrée et la longueur des mots de ces suites b_1 et b_2, on peut établir que

$$2^{b_1} \cdot 2^{b_2} \cdot N \leq \frac{1}{2} 2^k$$

soit $b_1 + b_2 + \text{Log}_2 N \leq k - 1$.

Dans le cas particulier à l'origine de cette étude les signaux avaient les caractéristiques suivantes :

l'un : amplitude 14 bits gain 3 bits.
soit une dynamique de 20 bits.

l'autre : sur 8 bits.

On voulait faire une corrélation sur N = 13 000 points après sommation de $16 = 2^4$ exemplaires du premier signal.

On a pris $N = 2^{14}$ d'où la relation :

$$2^4(2^{14} \cdot 2^{20} \cdot 2^8) \leq \frac{1}{2} 2^b \quad \text{ou}$$

$4 + 14 + 20 + 8 \leq b - 1$ donc $b \geq 47$.

D'où le choix

de $F = 2^{S.2^t} + 1$ avec : S = 3, t = 4, $\alpha = 8$,

$\alpha^{\frac{1}{2}} = 2^{37} - 2^{13}$.

Le passage de 2 048 à 13 000 a été fait par addition recouvrement classique.

4. RESULTATS.

Dans cette arithmétique $2^b = -1$, il faut donc b + 1 bits pour la mettre en oeuvre sans tests compliqués.

La réalisation a été faite sur un micro processeur à mots de 8 bits MC 6 800.

Les mémoires de travail et les constantes ont été placées dans la zone à adressage direct. La programmation a été faite sur un système de développement.

Les opérations élémentaires ont les caractéristiques suivantes :

Opération modulo $2^{48}+1$	Nombre d'octets	Temps d'exécution ms
addition	180	0,3
négation	90	0,4
multiplication par $= 2^3$	300	2
multiplication par $= 2^{37} - 2^{13}$ k	80	4 à 7
multiplication 48 x 48	700	25

Les opérations de transformation s'exécutent en :

Nombre N de points	TFR (s)	T.entière	Rapport TFR/T.E.	Matrice 2 L . P
16	0,56	0,085	6,6	-
32	1,5	0,23	6,5	-
64	4,25	0,66	6,4	-
128	10,5	2	5,2	16 x 16
256	25	5	5	32 x 16
512	57	12	4,75	32 x 32
1024	130	30	4,3	64 x 32
2048	290	73	4	64 x 64

Les opérations de corrélation s'exécutent en :

N	Corrélation T. entière(s)	Corrélation TFR(s)	Corrélation $\sum a_i . b_i$
16	0,6	1,2	0,75
32	1,3	3,5	3
64	3	9,2	12
128	10,5	24	48
256	23	53	192
512	51	120	768
1024	114	275	3072
2048	250	600	12288

N	$\frac{\text{TFR}}{\text{T. entière}}$	$\frac{\sum a_i . b_i}{\text{T. entière}}$
16	2	1,25
32	2,7	2,3
64	3	4
128	2,3	4,5
256	2,3	8
512	2,4	15
1024	2,4	27
2048	2,4	49

5. DEVELOPPEMENTS EN COURS ET CONCLUSION.

Les résultats précédents sont étroitement liés au matériel employé. La TFR est longue car il n'y a pas d'opérateur de multiplication cablé. Mais la Transformée entière l'est également à cause de la longueur de mots de 8 bits au lieu des 49 qui seraient nécessaires.

Une évaluation a été faite des durées d'exécution sur un ordinateur à mots de 16 bits micro programmable (l'unité centrale est constituée de 4 tranches AMD 2 900) (6), les opérations élémentaires étant micro programmées comme fonctions.

Pour la Transformée entière le gain de temps est compris entre 95 et 110, ce qui fournirait des temps d'exécution de l'ordre de la seconde.

Un projet en cours d'étude consiste à réaliser un opérateur spécialisé de 48 bits microprogrammé, les temps d'exécutions seraient encore divisés par quatre.

BIBLIOGRAPHIE

(1) D.A. PITASSI : "Fast convolution using Walsh Transform" IEEE Trans on electromagnetic compatibility Vol EMG 13, pp. 130-133.Août 1971

(2) E.O. BRIGHAM : "The Fast Fourier Transform" Prentice Hall Inc. Englewoods Cliffs, New Jersey USA 1974.

(3) R. AGARWAL and C. BURRUS : "Fast convolution using Fermat number transforms with applications to digital filtering". IEEE trans on acoustic, speech, signal processing Vol ASSP - 22 pp. 87-97. Avril 1974

(4) C. RADER : "Discrete convolutions via Mersenne Transforms", IEEE trans on computers, Vol C 21, pp. 1269-1273. Décembre 1972.

(5) H.J. NUSSBAUMER : "Filtrage numérique par transformées discrètes". Thèse de Doctorat, Université de Nice, Janvier 1977.

(6) J.N. BERRE : "Construction d'un ordinateur micro programmable". Mémoire d'Ingénieur CNAM. Paris 1979.