DIXIEME COLLOQUE SUR LE TRAITEMENT DU
SIGNAL ET SES APPLICATIONS

NICE du 20 au 24 MAI 1985

Séquences complexes à p^m moments ayants de bonnes propriétés de corrélation

P. Godlewski et P. Solé

ENST, dép. SYC, 46 rue Barrault 75013 PARIS

RESUME

On étudie, en liaison avec les modulations numériques, des familles de séquences à $q=p^m$ moments ayant de bonnes propriétés de corrélation.

Nous envisageons deux types de constructions : l'une utilise les corps finis, l'autre l'anneau des entiers modulo q. Nous exhibons à partir de la seconde des familles de séquences ayant des paramètres comparables à ceux des petits ensembles de Kasami.

SUMMARY

We consider sets of sequences with good correlation properties. We study the case where the sequence symbols take their values in a set of $q=p^m$ complex numbers.

Two types of constructions are discussed : one uses finite fields, the other one, integers modulo q. From the second we exhibit sets of sequences with parameters close to those of Kasami small sets.

Séquences complexes à p^m moments ayants de bonnes propriétés de corrélation

Introduction

Considérons le problème suivant : trouver un ensemble S de K séquences de longueur N telles que :

- chacune ait une autocorrélation en forme de pic,
- les différentes intercorrélations soient plates.

On s'intéressent aux séquences qui prennent leurs valeurs dans un ensemble fini (appelé constellation) de q nombres complexes (ou moments).

La corrélation peut être périodique, ce qui facilite les calculs théoriques, ou non périodique ; elle représente alors la sortie d'un filtre adapté à une certaine séquence, lorsque le signal en entrée provient d'une séquence non répétée.

L'utilisation d'un tel ensemble de séquences permet :

- la diminution des interférences inter-usagers dans un système de communications avec accès multiple par codage ;
- la discrimination d'échos multiples successifs en radar ou en sondage ionosphérique.

Le problème de la construction de familles de séquences ayant de bonnes propriétés de corrélation est étudié depuis plus de trente ans. La référence /1/ représente une bonne synthèse du domaine. Dans le cas binaire (q=2), les séquences sont trés souvent obtenues d'une manière algébrique (M-sequences, séquences de Gold, Kasami, ...) ; elles correspondent alors à des codes cycliques ayant une distance de Hamming minimale élevée. Ces constructions algébriques se généralisent facilement au cas ou q est un nombre premier p.

Lorsque $q=p^m$, m>1, les résultats sont plus rares dès que K>1. On considère ici plus particulièrement le cas p=2 d'intéret pratique puisqu'il correspond à des modulations de phase (MDP-4, MDP-8) ou d'amplitudes en quadrature (MAQ-16,...). Les constructions algébriques envisageables utilisent alors soit le corps fini (dit de Galois) à q éléments soit l'anneau Z_q des entiers modulo q. C'est dans ce cadre que s'inscrit notre travail. Nous étudions particulièrement ici le problème de la représentation des structures algébriques finies dans le plan complexe. Nous nous limiterons aux familles ayant des propriétés de corrélations périodiques, le cas non périodique se déduisant souvent du précédent par optimisation de la phase initiale (du décalage circulaire) de chaque séquence.

Notations

Soient u et v deux séquences complexes de longueur N, on appelle **corrélation périodique** la fonction définie pour tout entier k de Z :

$$\theta_{uv}(k) = \sum_{j=0}^{N-1} u_j [v_{j+k}]^*,$$ les indices étant pris modulo N,

et **corrélation non periodique** :

$$C_{uv}(k) = \sum_{j} u_j [v_{j+k}]^*,$$

Dans cette dernière expression, les indices ne sont plus pris modulo N, on suppose alors $u_j = v_j = 0$ si $j \notin [0:N-1] := \{0,1,\ldots,N-1\}$.

Pour un ensemble S de K séquences on introduit les paramètres suivants :

- Le plus grand pic secondaire de l'autocorrélation (autocorrélation maximum hors pic principal) :

$$\theta_a := \max(|\theta_{uu}(k)| \; ; \; u\in S, \; k\in[1:N-1]),$$

- Le maximum de l'intercorrélation

$$\theta_c := \max(|\theta_{uv}(k)| \; ; \; u,v\in S, \; u\neq v, \; k\in[0:N-1]).$$

On définit de même les paramètres C_a et C_c pour les corrélations non périodiques.

Pour K et N fixés, il s'agit de minimiser ces paramètres θ_a et θ_c (ou C_a et C_c) qui conditionnent les performances d'un systèmes de communication utilisant l'ensemble S.

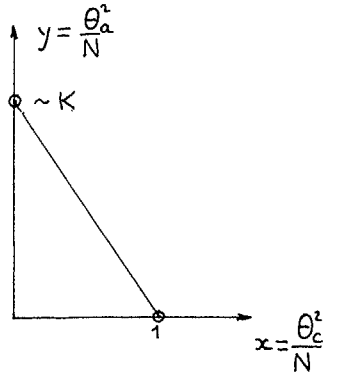
Borne de Welch, Pursley et Sarwate (/2/)

Cette borne exprime d'une part la difficulté de minimiser simultanément θ_a et θ_c et d'autre part que ces paramètres ne peuvent être simultanément inférieurs à $\lambda\sqrt{N}$ dès que K>1. Elle s'écrit :

$$\theta_c^2/N + (\theta_a^2/N).(N-1)/[N(K-1)] \geq 1$$

Ce qui s'interprète graphiquement en disant que les points sous la droite traçée sur la figure sont interdits. Si on impose les mêmes contraintes sur θ_a et θ_c on obtient (en faisant $\theta_a = \theta_c = \theta_m$ dans l'expression précédente) :

$$\theta_m^2 \geq N^2 (K-1) / (NK-1) .$$



De même, dans le cas non périodique on a :

$$(C_c^2/N).(2N-1)/N + (C_a^2/N).(2(N-1)/[N(K-1)] \geq 1$$

avec une interprétation graphique analogue.

Exemple : Le petit ensemble de Kasami possède les parametres suivants : $N=2^{2n}-1$, $K=2^n$, $\theta_a=\theta_c=K+1$; les séquences sont binaires. Pour n=2, on obtient ainsi un ensemble de K=4 séquences de longueur 15 avec $\theta_c=5$, la borne imposant $\theta_m \geq \lceil 3,38 \rceil = 4$. Cet ensemble est considéré comme asymptotiquement optimal puisque la borne signifie

$\theta_m \geq \sqrt{N}.[1-1/K+\epsilon(N)]^{1/2}$ et l'on a effectivement $\theta_m = \sqrt{N}+\epsilon'$. Notons cependant que cette optimalité ne concerne que le paramètre θ_m, la borne ne donnant que peu d'indications sur le nombre K des séquences.

Remarques

- Cette borne semble fine : les points extrêmes peuvent être atteints (/2/).
- La borne ne fait pas intervenir le nombre q de moments. On peut alors se poser la question suivante : Quelles sont les gains de performances que l'on peut espérer obtenir en passant d'une modulation binaire à une modulation q-aire ?

Problèmes de représentation

Considérons tout d'abord le cas binaire : pour représenter un élément x de $F_2=\{0,1\}$ dans le plan complexe, on utilise la correspondance

$$x \longrightarrow (-1)^x$$

qui représente une modulation du type antipodale dont l'archétype est la modulation MDP-2, PSK en anglais (remarquons qu'ici la droite réelle suffit, puisqu'on n'utilise que les deux phase 0 et π). Cette application est un homomorphisme (appelé habituellement **caractère**) du groupe $(F_2,+)$ dans $(\mathbb{C},\times)$. Cette qualité est importante : elle permet de déduire certaines propriétés de corrélation des séquences construites algébriquement à partir de la structure finie (ici F_2, plus généralement un corps ou un anneau).

Le problème de la représentation d'un élément de la structure finie par des points du plan complexe trouve donc, dans le cas binaire, une solution harmonieuse. De même si p est un nombre premier l'application :

$$x \xrightarrow{\chi_k} \chi_k(x)=(\omega^k)^x \quad \text{où } \omega = e^{2i\pi/p} \text{ et } k\in[0:p-1],$$

définit un morphisme de $(F_p,+)$ dans $(\mathbb{C},\times)$. La constellation obtenue est celle de la modulation MDP-p.

Se pose alors le problème plus général de représenter un corps fini F à q éléments dans le plan complexe lorsque $q=p^m$. On montre qu'un caractère s'écrit nécéssairement :

$$\chi_y(x) = (\omega)^{\langle x,y\rangle}$$

où $y\in F$ et $\langle x,y\rangle$ désigne le produit scalaire des éléments x et y de F_q considéré comme espace vectoriel de dimension m sur F_p. Cette quantité $\langle x,y\rangle$ est ainsi assimilable à un nombre entier compris entre 0 et p-1. Notons aussi que les p points obtenus en image restent sur le cercle unité. Pour une constellation quelconque de q points, il est utile de considérer l'algèbre de groupe $\mathbb{C}G$ où $G=(F_q,+)$ et la transformation de Fourier $\mathcal{F}$ définie sur cette algèbre par :

$$x \xrightarrow{\mathcal{F}} \mathcal{F}u = \sum_{y\in F_q} a_y \chi_y(x)$$

où les a_y sont des nombres complexes dépendant de la constellation.

Exemple : q=4 ; $F_4=\{0,1,\alpha,\alpha^2\}$ avec $\alpha^2=\alpha+1$. Choisissons la constellation : $\mathcal{F}o=1$; $\mathcal{F}1=i$; $\mathcal{F}\alpha=-i$; $\mathcal{F}\alpha^2=-1$. ou i désigne la racine de -1 dans $\mathbb{C}$. La transformation de Fourier s'écrit matriciellement :

$$\begin{bmatrix} 1 \\ i \\ -i \\ -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_\alpha \\ a_{\alpha^2} \end{bmatrix}$$

On reconnait une matrice d'Hadamard, elle vérifie bien $H.H^T=4I$. Ce qui permet de déterminer simplement les valeurs de a_y : $a_0=a_{\alpha^2}=0$; $a_1=(1-i)/2$; $a_\alpha=(1+i)/2$.

Construction à partir des corps finis

Soit (x_j) une séquence d'éléments d'un corps fini F à 2^m éléments. Pour caractériser sa représentation complexe $(\mathcal{F}x_j)$, il suffit, d'après ce qui précède, de connaître les "projections" binaires $\chi_y(x_j)$ pour tout y de F.

Lorsque (x_j) est un mot d'un code cyclique, on montre (/4/) que $(\chi_y(x_j))$ représente un mot d'un code cyclique binaire dont le polynome générateur ne dépend pas de y.

Classiquement on exprime le produit scalaire à partir d'un opérateur "trace" :

$\langle x,y\rangle = T_{q/2}(xy)$ avec

$$T_{q/2}(x) = \sum_{k=0}^{m-1} x^{2^k}$$

Prenons le cas d'une séquence de longueur maximale $N=q^n-1$ (ou M-séquence). Elle peut s'écrire :

$$x_j = T_{q^n/q}(\beta \gamma^j)$$

où β,γ appartiennent au surcorps $F'=F_{q^n}$ de F, γ étant un élément primitif de F'. On a de nouveau considéré un opérateur trace :

$$T_{q^n/q}(z) = \sum_{k=0}^{n-1} x^{q^k}$$

De cette manière en utilisant la transitivité des traces on obtient

$$\chi_y(x_j) = (-1)^{T_{q^n/2}(y\,\beta\,\gamma^j)}$$

C'est une M-séquence binaire dont le polynome caractéristique est le polynome minimal de γ dans F_2. Le raisonnement précédent peut s'étendre à un code cyclique quelconque en exprimant l'élément générique u_i comme une somme de traces.

En reprenant les arguments de l'exemple précédent il est alors clair que toute séquence à 4 phases construite à partir d'une M-séquence sur F_4 peut s'écrire :

$$\mathcal{F}x_j = \sum_{y\in F} a_y (-1)^{T_{4/2}(x_j)}$$

$$= [(1-i)/2].(-1)^{T_{4^n/2}(\beta\gamma^j)} + [(1+i)/2].(-1)^{T_{4^n/2}(\alpha\beta\gamma^j)}$$

En notant que $N=4^n-1$, $\gamma^N=1$ et que l'on peut choisir $\alpha=\gamma^{N/3}$ (puisqu'ainsi $\alpha^3=1$), il apparait que les projections binaires d'une M-séquence sur F_4 sont 2 M-séquences binaires de même polynome caractéristique, décalées de N/3.

Exemple : pour fixer les idées considérons le polynome sur F_4 de degré n=2, $X^2+X+\alpha$, qui est primitif. Il lui correspond une M-séquence de longueur N=15 sur F_4, $(x_j)=(0,1,1,\alpha^2,1,0,\alpha,\alpha,\ldots)$
La séquence complexe obtenue est alors
$(\mathcal{F}x_j)=(1,i,i,-1,i,1,-i,-i,i,-i,1,-1,-1,-i,-1)$,
on pourra vérifier la répartition régulière, prévisible pour une M-séquence (3 "1", 4 "i", 4 "-1", 4 "-i"). L'autocorrélation de cette séquence est aisément calculable puisqu'elle est obtenue en combinant une M-séquence et sa décalée circulaire de 5 pas.

$$\theta_{uu}(k) = 15 \text{ si } k=0,$$
$$= -1 \text{ si } k\not\equiv 0 \bmod(15),$$
$$= -1+8i \text{ si } k=5,$$
$$= -1-8i \text{ si } k=10.$$

Ce type de résultat reste valable dans le cas des M-séquences dès que $\sum_x Fx = 0$ (/3/).

Construction à partir des entiers modulo q.

La représentation

$$x \longrightarrow \omega^x$$

d'un élément x de Z_q dans le plan complexe s'impose lorsqu'on utilise une modulation de phase MDP-q, ce que nous supposons dans ce paragraphe. Si u et v sont les images dans le plan complexe de deux séquences x et y sur Z_q : $u_j=\chi(x_j)$ et $v_j=\chi(y_j)$, on a

$$\theta_{uv}(k) = \sum_j \chi(x_j)\,\chi(y_{j+k})^*$$

$$= \sum_j \chi(x_j-y_{j+k}).$$

Pour déterminer cette valeur on considère le N-uplet à composantes dans Z_q défini par $z=x-D^k y$ où D^k représente le décalage circulaire de k pas. Il suffit, en fait, de connaître le nombre de chacun des symboles de Z_q que z contient. De cette manière si z contient n_ℓ symboles "ℓ", $\ell\in Z_q$, on peut écrire

$$\theta_{uv}(k) = \sum_\ell n_\ell\, \omega^\ell .$$

Par exemple si q=4, on a $\theta_{uv}(k) = (n_0-n_2)+i(n_1-n_3)$.

Nous présentons maintenant une construction utilisants des codes cycliques monogènes sur Z_4.
L'anneau des polynomes $Z_4[X]$ n'étant pas euclidien, il existe des codes cycliques sur Z_4 engendrés avec deux générateurs (/5/).
Par souci de simplicité on ne considère ici que les codes cycliques dont les mots peuvent être obtenus à partir d'une récurrence linéaire. Soit $h(X)=\sum_j h_j X^j$, le polynome caractéristique de cette récurrence et $h^{(2)}(X)$, l'image modulo 2 de ce polynome h. On montre alors (/5/) la propriété suivante :
Propriété : Soit h un polynome normalisé de $Z_4[X]$. Si la récurrence sur F_2 de polynome caractéristique $h^{(2)}$ engendre une séquence de période n, alors h engendre, par récurence linéaire sur Z_4, une séquence de période 2n.

Application : "pseudo M-séquences" sur Z_4.

Soit h un polynome normalisé tel que $h^{(2)}$ soit primitif sur F_2 et $n=2^d-1$ ou $d=\deg(h^{(2)})=\deg(h)$. Alors h engendre deux types de séquences non nulles de longueur 2n :

- n séquences de période n qui sont des copies de la séquence binaire engendrée par $h^{(2)}$ (on remplace 1 par 2). Elles se déduisent donc l'une de l'autre par décalage circulaire.
- n(n+1) séquences de période 2n, ce qui correspond à (n+1)/2 classes sous le décalage circulaire.

Si on se donne $h^{(2)}$ il existe (n+1) polynomes h possibles. Il y a donc beaucoup plus de séquences que dans le cas binaire.

Exemple : $h^{(2)}=X^3+X+1$ d'où $d=3$, $h=X^3-X-1$, les séquences obtenues par la récurrence $x_{j+3}=x_{j+1}+x_j$, ont comme motif (à un décalage circulaire près) l'un des 5 mots de longueur 2n=14 :

	(n_1,n_2,n_3,n_4)	θ
0 0 2 0 2 2 2 0 0 2 0 2 2 2	(6, 0, 8, 0)	-2
0 0 1 0 1 1 1 2 2 3 0 1 3 1	(4, 6, 2, 2)	2+4i
0 0 3 0 3 3 3 2 2 1 0 3 1 3	(4, 2, 2, 6)	2-4i
1 2 3 3 1 2 0 3 2 3 1 1 0 2	(2, 4, 4, 4)	-2
3 2 1 1 3 2 0 1 2 1 3 3 0 2	(2, 4, 4, 4)	-2

A partir des quatres derniers mots, on obtient (en transformant ℓ en i^ℓ) une famille de séquences quadriphases, dont les différentes corrélations périodiques appartiennent à l'ensemble $\{14,-2,2\pm4i\}$ (corrélations quadri-valuées), en module $|\theta|=\sqrt{20}\approx 4,47$. La borne inférieure évoquée plus haut imposait $\sqrt{10,69}\approx 3,27$. Ces séquences sont donc proches de l'optimum et ont des performances comparables à celles du petit ensemble de Kasami.

Un autre exemple : sur Z_8 on obtient K=4 séquences de longueur 12 ayant un paramètre $\theta_m=4$, la borne imposant $\theta_m\geq 3,03$. Puisque $\lceil 3.03\rceil=4$, cet ensemble a des performances au moins aussi bonnes que tout ensemble binaire.

Conclusion

Nous avons proposé des outils pour représenter, dans le plan complexe, des séquences à 2^m moments, définies à partir de structures algébriques finies.

Deux types de constructions ont été étudiées :

A partir des corps finis, nous obtenons des autocorrélations ayant des pics secondaires périodiques. Elles ne remplissent donc pas les exigences habituelles.

Les techniques de construction utilisant des anneaux finis fournissent des séquence a priori plus intéressantes. Nous avons en particulier exhibé des ensembles dont les paramètres sont comparables à ceux des "petits ensembles" de Kasami. Par rapport au cas binaire on peut espérer deux sortes d'avantages : augmenter la cardinalité $K(N,\theta_m)$ de chaque famille (par exemple d'un facteur multiplicatif constant), un nombre plus important de familles (agilité).

Références :

/1/ D.V. Sarwate et M.B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences", Proceedings of the IEEE, Vol.68, NO5, pp 593-619, Mai 1980.

/2/ D.V. Sarwate, "Bounds on Crosscorrelation and Autocorrelation of Sequences", IEEE Trans. Inform. Theory, vol IT-25, pp.720-724, pp.720-724, Novemb. 1979.

/3/ P.Solé, "Séquences à faible corrélation", à paraître dans la revue française de traitement de signal.

/4/ G. Pasquier, "Projections et images binaires de codes sur F_2^n", Revue du Cethedec, 4ème trimestre 1981, NS81-2, pp45-56.

/5/ P.Solé, "Construction de séquences sur Z_q, $q=p^r$", Colloque AAECC, Toulouse, Septembre 1984, soumis à publication.