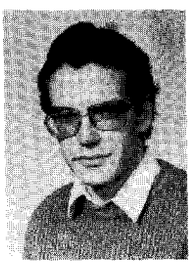
Séquences à faible corrélation

Low correlation sequences



Patrick SOLÉ

ENST, 46, rue Barrault, 75013 PARIS

Ingénieur ENST, 1984; DEA de Mathématiques pures Paris-VI, 1984-1985 (graphes et matroïdes, Berge-Las Vergnias; codage algébrique, Deza-Cohen); Conférence au congrès AAECC « Construction of sequences over Z_q » (Récurrences linéaires sur les entiers modulo q, $q=p^r$, $r>1$); envisage une thèse de docteur-ingénieur (1985) sur un thème de codage algébrique.

RÉSUMÉ

Dans de nombreuses applications (radar, sondage ionosphérique, communications à spectre étalé), se pose le problème suivant : trouver un ensemble de séquences (codes de phase) dont l'intercorrélation soit faible, et l'autocorrélation en forme de pic.

Les cas des séquences binaires et p-aires (p un nombre premier) ont été abondamment traitées dans la littérature. Cet article présente une construction de séquences q-aires (q, une puissance de 2), où les q valeurs prises sont des nombres complexes quelconques. On utilise la Transformation de Hadamard, et les propriétés des formes F_2 bilinéaires sur F_q.

MOTS CLÉS

Séquences q-aires, corrélation périodique, m-séquences, codes sur F_q (radar, spectre étalé).

SUMMARY

In many applications (radar, ionospheric studies, spread spectrum communications), arise the following problem: how to find a set of sequences (phases codes) with low crosscorrelation and peak-shaped autocorrelation.

The binary and p-ary cases (p, a prime integer) have been extensively studied in the literature. This paper presents an algebraic construction of q-ary sequences (q a power of 2), where the q values taken are arbitrary complex numbers. Hadamard Transform, and bilinear forms over GF_q properties are used.

KEY WORDS

q-ary sequences, periodic correlation, m-sequences, codes over F_q (radar, spread spectrum).

TABLE DES MATIÈRES

Introduction

1. Représentation des injections de F_q dans C^q.
1.1. L'algèbre de groupe
1.2. Les caractères du groupe additif $(F_q, +)$
1.3. La transformation de Hadamard

2. Étude de la forme trace
2.1. Définition
2.2. Non-dégénérescence de la forme trace
2.3. Existence d'une base trace-orthogonale
2.4. Conclusions

3. Codes sur F_q
3.1. Définitions
3.2. Représentation d'une m-séquence
3.3. Transitivité de la trace

4. Autocorrélation périodique projetée
4.1. Définitions
4.2. Calcul de la corrélation projetée
4.3. Génération des séquences

5. Corrélation périodique totale
5.1. Hypothèse
5.2. Propriétés de aq
5.3. Calcul de la corrélation
5.4. Calcul de S_v

6. Bornes et exemples
6.1. Généralisation
6.2. Bornes sur l'intercorrélation périodique
6.3. Borne sur l'autocorrélation apériodique.
6.4. Conclusions
6.5. Exemples numériques.

Conclusion

Bibliographie

Remerciements

Introduction

Considérons le problème suivant : trouver un ensemble de séquences (codes de phase) dont :

– les maximums secondaires de l'autocorrélation de chacune d'elles soient les plus faibles possibles;

– les maximums absolus de l'intercorrélation de l'une quelconque avec toute autre soient les plus faibles possibles.

Les principales applications viennent de :

– la diminution des interférences inter-usagers en communications à spectre étalé;

– la discrimination d'échos multiples successifs en radar ou en sondage ionosphérique.

Les principales recherches dans le domaine concernent les m-séquences binaires et leurs propriétés de corrélation périodique [1]. On s'est intéressé également au cas des longueurs non primitives [2]. Les principaux résultats dans le cas des séquences p-aires (p, un nombre premier) sont dans [3].

Le but de cet article est de donner la représentation la plus générale d'une séquence à valeurs dans F_q par une séquence à q valeurs complexes distinctes (q, une puissance de 2) en vue d'une représentation dans le plan complexe par des modulations du type MDP2, MDP4, et ou même, plus généralement du type MAQ. Puis l'on montrera, dans le cas particulier d'une m-séquence à valeurs dans F_q, comment calculer l'autocorrélation périodique, grâce aux propriétés des codes sur F_q.

1. Représentation des injections de F_q dans C^q

Dans toute la suite $q=2^n$. Pour plus de détails sur l'algèbre de groupe, *voir* [4].

1.1. L'algèbre de groupe

C'est l'ensemble des polynômes formels :

$$\sum_{g \in F_q} a_g X^g,$$

où $a_g \in \mathbb{C}$, corps des complexes.

La somme est définie par :

$$A(X)+B(X)=\sum_{g \in F_q} (a_g+b_g) X^g$$

et le produit par :

$$A(X) * B(X) = \sum_{g \in F_q} \Big(\sum_{h \in F_q} a_{(g-h)} b_h \Big) X^g.$$

1.2. Les caractères du groupe additif $(F_q, +)$

A tout scalaire u dans F_q, on associe un caractère dans F_q, groupe dual de F_q, pris comme groupe additif par :

$$\mathcal{X}_u(v)=(-1)^{B(u, v)},$$

où B (u, v) est une forme F_2 bilinéaire, à valeurs dans F_2, *non dégénérée.*
On vérifie aisément que $\mathscr{X}_u$ est bien un caractère i. e. :

$$\forall g, h \in F_q,$$
$$\mathscr{X}_u(g+h) = \mathscr{X}_u(g)\,\mathscr{X}_u(h).$$

B (u, v) sera choisie au paragraphe 2, et définie indépendamment de la base de projection, ce qui facilitera les calculs.

1.3. La transformation de Hadamard

A tout élément de $\mathbb{C}F_q$, on associe une bijection de F_q sur une partie (quelconque) de $\mathbb{C}$ à q éléments :

$$\sum_{g \in F_q} a_g X^g \overset{\mathscr{F}}{\mapsto} (\mathscr{F}_u)_{u \in F_q},$$
$$\mathscr{F}_u = \sum_{g \in F_q} a_g \mathscr{X}_u(g).$$

Les propriétés de cette transformation sont :
– bijectivité (utilise : B non dégénérée);
– transforme le produit de polynômes en produit « composantes à composantes » (produit de Hadamard).

2. Étude de la forme trace

2.1. Définitions

On appelle *trace de* F_q *sur* F_2 la forme F_2-linéaire suivante :

$$\forall \alpha \in F_q, \quad T_{q/2}(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}.$$

J'appelle forme trace la forme F_2-bilinéaire suivante :

$$(u, v) \mapsto T_{q/2}(u, v).$$

2.2. Non-dégénérescence de la forme trace

On rappelle qu'une forme B est dite non dégénérée si :

$$\forall v \in F_q, \qquad B(u, v) = 0 \quad \Rightarrow \quad u = 0.$$

Supposons :

$$\forall v, \quad T_{q/2}(uv) = 0,$$

et montrons $u = 0$.
Il existe w dans F_q tel que $T_{q/2}(w) = 1$, sinon la trace serait un polynôme de degré $q/2$ avec q racines !
Si $u \neq 0$, en posant $v = w/u$, on obtient $T_{q/2}(w) = 0$!

2.3. Existence d'une base trace orthogonale

Une base (α_i) de F_q sur F_2 telle que :

$$\forall i, j \in [1, 11], \quad T_{q/2}(\alpha_i \alpha_j) = \delta_{ij},$$

(δ_{ij} = symbole de Kronecker) est dite *trace orthogonale.*
Soit (α_i) une base quelconque de F_q sur F_2, et A la matrice de la forme trace sur cette base : A est symétrique. A est régulière car la forme trace est non dégénérée. A n'a pas sa grande diagonale nulle, à cause de w du paragraphe précédent (supposer $\alpha_1 = w$).
Alors, d'après [6], A se factorise : $A = B.\,B'$, B binaire n par n, B' = transposée de B. En posant C = inverse B', on a : $I_n = C'AC$, où I_n est l'identité. Si C est la matrice de changement de base de (α_i) à (β_i), alors (β_i) est trace orthogonale.

2.4. Conclusions

Dans toute la suite B (u, v) = forme trace.
Sur une base trace orthogonale :

$$B(u, v) = \sum_{i=1}^{n} u_i v_i.$$

3. Codes sur F_q

3.1. Définitions

On appelle *trace de* F_{q^m} *sur* F_q, l'application F_2-linéaire suivante :

$$T_{q^m|q}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i}, \qquad \forall \alpha \in F_{q^m}$$

On appelle *m-séquence* à valeurs dans F_q une séquence q-naire engendrée par récurrence linéaire à polynôme caractéristique primitif à coefficients dans F_q.

3.2. Représentation d'une m-séquence

Soit u_i m-séquence à valeurs dans F_q, de longueur $q^m - 1$, il existe α primitive, et φ dans F_{q^m}, tels que :

$$\forall i \in [1, n], \quad u_i = T_{q^m|q}(\varphi \alpha^i).$$

preuve : Soit α une racine du polynôme caractéristique de la récurrence linéaire associée. α est donc primitive sur F_{q^m}. $i \mapsto \alpha^i$ vérifie la récurrence linéaire sur F_{q^m}. Par linéarité de la trace de F_{q^m} sur F_q, $T_{q^m|q}(\varphi\alpha^i)$ aussi. En faisant $\varphi = \alpha^k$, on a bien tous les décalés circulaires de u_i.

3.3. TRANSITIVITÉ DE LA TRACE

« La projection sur F_2 d'un projeté sur F_q d'un vecteur de F_{q^m} est le projeté sur F_2 du même vecteur de F_{q^m} » :

$$\forall \gamma \in F_{q^m},$$
$$T_{q/2}[T_{q^m/q}(\gamma)] = T_{q^m/2}(\gamma).$$

Preuve :

$$\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}\gamma^{2^{nj}}\right)^{2^i} = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\gamma^{2^{nj+i}} = \sum_{k=0}^{nm-1}\gamma^{2^k}$$
$$(k = nj + i).$$

4. Autocorrélation périodique projetée

4.1. DÉFINITIONS

Soit x une séquence à valeurs complexes de longueur N. Sa fonction d'autocorrélation périodique est alors :

$$\forall l \in \mathbb{Z},$$
$$\theta_{xx}(l) = \sum_{l=0}^{N-1} x_i x_{i+l}^*$$

(indices pris modulo N).
Soit u une séquence à valeurs dans F_q, de longueur N. Par abus de notation, je pose :

$$\theta_{uu}(l) = \theta_{\mathscr{F}_u \mathscr{F}_u}(l) = \sum_{i=0}^{N-1} \mathscr{F}_{u_i} \mathscr{F}_{u_{i+1}}^*.$$

Par interversion de Σ : $\theta_{uu}(l) = \sum_{gh} ag\, a_h^* \theta^{gh}(l)$ où θ_{un}^{gh} *corrélation projetée sur q et h* s'écrit :

$$\theta_{uu}^{gh}(l) = \sum_{l=0}^{N-1} \mathscr{X}_{u_i}(g).\mathscr{X}_{u_{i+l}}(h).$$

4.2. CALCUL DE LA CORRÉLATION PROJETÉE

Exprimant les caractères par la forme trace :

$$\theta_{uu}^{gh}(l) = \sum_{i=0}^{N-1} (-1)^{T_{q/2}(u_i g + u_{i+l}.h)}.$$

Comme u est une m-séquence :

$$u_i g + u_{i+l}.h = T_{q^m/q}[\varphi\, \alpha^i (g + \alpha^l h)].$$

Utilisons alors la transitivité de la trace :

$$T_{q/2}[u_i.g + u_{i+l}.h] = T_{q^m/2}[\varphi\alpha^i(g + \alpha^l h)].$$

Deux cas se présentent :
$q \neq \alpha^l.h$: On reconnait l'expression en fonction de la trace d'une m-séquence binaire de longueur $q^m - 1 = 2^{mn} - 1$, avec 2^{mn-1} « 1 » et $2^{nm-1} - 1$ « 0 » :

$$\theta_{uu}^{gh}(l) = -1.$$

$a = \alpha^l.h$: Comme $T_{q^m/2}(0) = 1$ on a une somme de $q^m - 1$ « 1 » :

$$\theta_{uu}^{gh}(l) = 2^{nm} - 1.$$

Si $(g, h) \neq (0, 0)$, cela se produit pour $\alpha^l = g/h$ dans F_q soit l multiple de $(q^m - 1)/(q - 1) = \lambda$.
En effet si l'on pose $\gamma = \alpha^l$, on a : $\gamma^{q-1} = 1$ donc γ est dans F_q, et, comme α est primitive sur F_{q^m}, α l'est sur F_q.
Pour $1 \neq 0$, cela se produit $q - 2$ fois (0 pour $q = 2$, cas des *m-séquences binaires*).

4.3. GÉNÉRATION DES SÉQUENCES

Rappelons que :

$$\mathscr{F}_u = \sum_{g \in Fq} a_g \mathscr{X}_u(g) = \sum_{g \in F_q} a_g (-1)^{B(u, g)}.$$

En utilisant la transitivité de la trace, il est facile de prouver, que, si le code u est cyclique sur F_q, $B(u, g)$ est cyclique sur F_2.
Par exemple, si u est une m-séquence de polynôme caractéristique h sur F_4, $B(u, g)$ est une m-séquence associée à $h\tilde{h}$ ($\tilde{h}$ = conjugué de h).

5. Corrélation périodique totale

5.1. HYPOTHÈSES

On suppose que les q valeurs prises par les $\mathscr{F}_u$ sont (sans préciser leur ordre) les q racines q-ièmes de l'unité sur C.
On utilise les propriétés de la transformée de Hadamard pour essayer d'évaluer θ_u.

5.2. PROPRIÉTÉS DES a_g

$a_0 = 0$: En utilisant la formule d'inversion :

$$a_0 = \frac{1}{q}\sum_{u \in F_q} {}_u\mathscr{X}_x(0)$$

$$= \frac{1}{q} \sum_{u \in F_q} \mathscr{F}_u = 0.$$

$\sum_{g \in F_q} |a_g|^2 = 1$: La matrice de Hadamard étant orthogonale (à q près) :

$$\sum_g |a_g|^2 = \frac{1}{q} \sum_u |\mathscr{F}_u|^2 = \frac{q}{q} = 1.$$

$\sum_{g \neq h} a_g a_h^* = 0$ Pour $1 = 0$ on a :

$$\theta_{uu}^{gg}(0) = q^m - 1$$

et

$$\theta_{uu}^{gh}(0) = -1 \qquad \text{pour} \quad g \neq h.$$

Or :

$$\theta_{uu}(0) = q^m - 1$$
$$= (q^{m-1}) \times 1 - \sum_{g \neq h} a_g a_h^*.$$

5.3. Calcul de la corrélation

On calcule $\theta_{uu}(l)$ pour $1 \neq 0$.
$\alpha^l \in F_q$:

$$\theta_{uu}(l) = (\sum_g |a_g|^2) \times (-1)$$
$$+ (\sum_{g \neq h} a_g a_h^*) \times (-1),$$
$$\boxed{\theta_{uu}(l) = -1.}$$

$\alpha^l \in F_q$: Comme $a_0 = 0$ on peut supposer $g \neq 0$ et $h \neq 0$. Alors :

$$\exists r \in [1,\ q-2], \quad l = r\lambda.$$

Posons :

$$S_r = \sum_{h \in F_q} a_{\gamma^r h} \cdot a_h^*.$$

On suppose $1 \neq 0$:

$$\boxed{\theta_{uu}(l) = -1 + q^m S_r)}$$

5.4. Calcul de S_r

En utilisant la formule d'inversion de la transformation de Hadamard, il vient :

$$S_r = \frac{1}{q}\left[1 + \sum_{k=0}^{q-1} \mathscr{F}_{\gamma^k} \mathscr{F}_{\gamma^{k+r}}^*\right],$$

où $\gamma = \alpha^\lambda$.

Se pose ainsi le problème de trouver la (ou les) permutations des racines q-ième de l'unité sur $\mathbb{C}$ qui donne (nt) S_r le plus gaible possible. Exemple : $n = 2 = > q = 4$, au mieux on a $s_1 = 1/2$.

6. Bornes et exemple

6.1. Généralisation

Dans le paragraphe 5.1 on a supposé que les $\mathscr{F}_u$ étaient à enveloppe constante; calculs et résultats demeurent inchangés, si l'on suppose seulement :

$$\sum_u \mathscr{F}_u = 0 \qquad \text{et} \qquad \sum_u |\mathscr{F}_u|^2 = q.$$

Ce qui est vérifié par de nombreuses modulations MAQ.

6.2. Bornes sur l'intercorrélation périodique

Rappel

Rappelons que pour deux séquences u et v :

$$\theta_{uv}(l) = \sum_{i=0}^{N-1} \mathscr{F}_{u_i} \mathscr{F}_{o_{i+l}}^*$$
$$= \sum_{qh \in F_q} a_g \bar{a}_h \theta_{uv}^{gh}(l),$$

avec :

$$\theta_{uv}^{gh}(l) = \sum_{i=0}^{N-1} \mathscr{X}_{u_i}(g) \mathscr{X}_{v_{i+l}}(h).$$

Supposons, que la corrélation projetée soit bornée :

$$\forall l, \quad |\theta_{uv}^{gh}(l)| \leqq M.$$

Par exemple, si les projections sur F_2 de u et v sont des paires préférées, on a : $M = t(k)$ (*voir* [1]).
La corrélation totale est alors bornée par :

$$|\theta_{uv}(l)| \leqq M \sum_{g,\ h} |a_g|$$
$$\times |a_h| = M(\sum_g |a_g|)^2,$$

appliquons l'inégalité de Schwarz dans $\mathbb{R}^q$:

$$(\sum_g |a_g|)^2 \leqq q \sum_g |a_g|^2.$$

Or :

$$\sum_g |a_g|^2 = 1,$$

donc :

$$|\theta_{uv}(l)| \leqq q\,M.$$

6.3. Bornes sur l'autocorrélation apériodique

De même que dans le cas périodique, on peut poser :

$$C_{uu}^{gh}(l) = \sum^{N-1-l} \mathscr{X}_u(g)\,\mathscr{X}_u(h).$$

Les mêmes majorations suivent :

$$|C_{uv}^{gh}(l)| \leqq M,$$
$$\forall l, \quad \forall g, h \Rightarrow |C_{uv}(l)| \leqq q\,M.$$

En particulier la borne de McEliece appliquée à la corrélation apériodique projetée donne :

$$|C_{uv}^{gh}(l)| \leqq 2^{k/2}(1+\mathrm{Log\,N})$$
$$\Rightarrow |C_{uu}(l)| \leqq 2^n \sqrt{N+1}(1+\mathrm{Log\,N}).$$

6.4. Conclusion

Ces bornes sont peu fines, en effet, pour $n=2 => q=4$, on a :

$$a_g = 0,\ 0,\ \frac{1+i}{2},\ \frac{1-i}{2}$$
$$\Rightarrow \left(\sum_g |a_g|\right)^2 = 2 \qquad (\mathrm{MDP}2^n).$$

Cependant, elles indiquent que, asymptotiquement, les séquences q-naires ont des propriétés analogues à celles des séquences binaires.

D'autre part, elles suggèrent de prendre, des séquences sur F_q, telles que leur projection sur F_2 donnent de « bonnes » séquences binaires.

Il semble intéressant, mais assez difficile d'établir un lien entre la borne sur la corrélation d'une famille et la distance minimale du code associé.

6.5. Exemples numériques

Considérons $F_4 = 0,\ 1,\ \alpha,\ \alpha^2\}$ avec $\alpha^2 = 1+\alpha$.

Choisissons les $\mathscr{F}_u$ qui minimisent S_r (*voir* § 5.4) :

$$\mathscr{F}_0 = 1; \qquad \mathscr{F}_1 = -i;$$
$$\mathscr{F}_\alpha = -1; \qquad \mathscr{F}_{\alpha^2} = i.$$

Les A_g et les $\mathscr{F}_u$ sont reliés par une transformation de Hadamard :

$$4\begin{bmatrix} a_0 \\ a_1 \\ a_\alpha \\ a_{\alpha^2} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ -i \\ -1 \\ i \end{bmatrix}$$

ce qui donne :

$$a_0 = 0,$$
$$a_1 = \frac{1-i}{2},$$
$$a_\alpha = \frac{1+i}{2},$$
$$a_{\alpha^2} = 0.$$

La suite q-aire s'exprime alors en fonction des projections binaires :

$$\mathscr{F}_{u_i} = \sum_{g \in F_4} a_g (-1)^{T_{4/2}(u_i g)}$$
$$= \left(\frac{1-i}{2}\right)(-1)^{T_{4/2}(u_i)} + \left(\frac{1+i}{2}\right)(-1)^{T_{4/2}(\alpha u_i)}$$

Supposons maintenant que u_i soit une m-séquence sur F_q, de longueur $4^m - 1$:

$$u_i = T_{4^m/4}(\gamma^i),$$

où $\gamma \in F_{4^m}$, γ primitive.

Utilisons maintenant la transitivité de la trace, pour exprimer les projections :

$$T_{4/2}(u_i) = T_{4^m/2}(\gamma^i)$$

et

$$T_{4/2}(\alpha u_i) = T_{4^m/2}(\alpha\gamma^i).$$

En remarquant que :

$$\alpha = \gamma^{N/3},$$

où $N = 2^{nm} - 1 = 4^m - 1$.

On voit que les projections sur F_2 sont des m-séquences binaires de même polynôme générateur, décalées circulairement de N/3 :

$$T_{4/2}(u_i) = T_{2^{2m}/2}(\gamma^i)$$

et

$$T_{4/2}(\alpha u_i) = T_{2^{2M}/2}(\gamma^{i+(N/3)}).$$

Conclusion

On a montré comment construire des suites complexes a *q valeurs complexes quelconques* en utilisant les propriétés des corps finis F_q pour $q = 2^n$. Cependant ces

séquences se calculent simplement à partir de codes cycliques sur F_2.
On a calculé pour une m-séquence q-aire la corrélation périodique. Le calcul théorique est susceptible de généralisation à d'autres codes cycliques, *via* le polynôme de Mattson-Solomon. Les performances obtenues se rapprochent de celles des m-séquences binaires.
D'autres recherches sont possibles :
Étude de l'intercorrélation périodique (décimation).
Ensemble de séquences à performances garanties (*cf.* Gold, Kasami).
Propriétés de corrélation non périodique.
Généralisation à p^m valeurs, pour p premier.

Remerciements

Nous tenons à remercier ici P. Godlewski, chercheur à l'ENST, dont les conseils et les encouragements nous furent d'une aide précieuse au cours de ce travail.

BIBLIOGRAPHIE

[1] SARWATE et PURSLEY, Crosscorrelations properties of pseudo-random and related sequences, *Proceedings of the IEEE*, May 1980.

[2] MC-ELIECE, Correlation properties of sets of sequences derived from irreducible cyclic codes, *Info. and Control*, n° 45, 1980.

[3] HELLESETH, Some results about the crosscorrelation function between two maximal linear sequences, *Discrete Math.*, 16, 1976.

[4] CAMION, *Difference sets in elementary Abelian groups.*

[5] SLOANE et MC-WILLIAMS, *Error Correcting Codes.*

[6] Référence [814] de la bibliographie [5].