UNE MÉTHODE SIMPLE POUR LE CALCUL DE LA DENSITÉ SPECTRALE DE PUISSANCE DE SIGNAUX CODÉS LINÉAIREMENT EN BLOCS

Christophe LE MARTRET *
Georges VEZZOSI **

* CESTA, 37 avenue du Général de Gaulle, 35170 BRUZ
** Laboratoire LTSI, Université de Rennes I, Campus de Beaulieu, 35042 Rennes Cedex

RÉSUMÉ

Le problème du calcul de la Densité Spectrale de Puissance (DSP) d'un signal modulé numériquement par une suite de symboles {b(k)} est souvent rencontré en télécommunications. Il nécessite l'évaluation de la fonction d'autocorrélation de la suite {b(k)}. Dans la plupart des systèmes modernes, ces symboles sont issus d'un codage correcteur d'erreurs. Nous nous intéressons ici au cas du codage linéaire en blocs. Nous montrons que dans le cas binaire sous l'hypothèse d'indépendance des symboles avant codage on aboutit à une méthode très simple pour le calcul des corrélations.

ABSTRACT

The Power Spectral Density computation of digitally modulated signals by a sequence of symbols {b(k)} is often encountered in telecommunications. It requires the evaluation of the autocorrelation function of the sequence {b(k)}. In most of modern telecommunication systems these symbols are coming out from an error correcting coder. In this paper our work is focused on linear block error correcting codes. We show that in the binary case, assuming the independence of the sequence before coding, we achieve a very simple method for computing the correlations.

1 - INTRODUCTION

Le calcul de la Densité Spectrale de Puissance (DSP) de signaux numériques passe par l'évaluation de la fonction de corrélation. Celle-ci dépend de la statistique du train binaire ayant servi à construire le signal. Dans la plupart des systèmes de télécommunications, le train binaire modulant est issu d'un codage. Par exemple, on trouve fréquemment un codage linéaire par blocs. Le calcul de la corrélation dans le cas général (codage non binaire et statistique des bits avant codage quelconque) est complexe [1]. Nous montrons que dans le cas binaire lorsque l'on suppose l'indépendance de la séquence binaire avant codage, il existe une solution simple. Nous décrivons la méthode permettant de calculer les corrélations puis nous l'appliquons au cas d'un Hamming (8,4).

Étude financée par le Centre d'Électronique de l'Armement, 35170 BRUZ.

2 - POSITION DU PROBLÈME

Soit {a(i)} la suite des bits à coder et {b(i)} la suite des bits codés. On définit le codage en blocs (N,K) de matrice génératrice $\underline{G}$ par la relation suivante :

$$\underline{b}_n = \underline{G} \cdot \underline{a}_n \tag{1}$$

avec

$$\begin{aligned} \underline{a}_n &= [a((n-1)K+1), \ \dots \ , a(nK)]^T, \\ \underline{b}_n &= [b((n-1)N+1), \ \dots \ , b(nN)]^T, \\ \underline{G} &= [g(i,j)], \quad 1 \le i \le N, \quad 1 \le j \le K, \end{aligned} \tag{2}$$

les coefficients a(i), b(i) et g(i,j) étant à valeurs dans le corps de Galois GF(2).

Soit l'application φ définie par :

$$\begin{aligned} GF(2) &\xrightarrow{\varphi} \mathbb{R} \\ 0 &\longrightarrow -1 \\ 1 &\longrightarrow 1 \end{aligned} \qquad (3)$$

Le problème posé est celui du calcul des matrices de corrélations

$$\underline{R}(n) = \mathbb{E}\left[\varphi(\underline{b}_k) \cdot \varphi(\underline{b}_{k-n}^T)\right]. \qquad (4)$$

On va supposer maintenant que les symboles a(i) sont indépendants. La statistique de la suite {a(i)} est alors entièrement définie par la probabilité $p_0 = \Pr\{a(i)=0\}$. On pose $p_1 = \Pr\{a(i)=1\}$. On en déduit directement que $\Pr\{\varphi(a(i))=-1\} = p_0$ et que $\Pr\{\varphi(a(i))=1\} = p_1$. La moyenne des v.a. $\varphi(a(i))$ vaut :

$$\mathbb{E}[\varphi(a(i))] = p_1 - p_0. \qquad (5)$$

L'indépendance des a(i) entraîne que les matrices (4) sont toutes identiques pour |n|>0. On posera par la suite :

$$\underline{R} = \underline{R}(n), \quad |n| > 0. \qquad (6)$$

Dans le cas où les a(i) sont indépendants on est alors ramené à calculer $\underline{R}(0)$ et $\underline{R}$.

3 - ÉQUIVALENCE DES OPÉRATIONS ÉLÉMENTAIRES DE GF(2) SUR $\mathbb{R}$

Soit l'application *chapeau* définie par :

$$\begin{aligned} GF(2) &\xrightarrow{\wedge} \mathbb{R} \\ 0 &\longrightarrow 0 \\ 1 &\longrightarrow 1 \end{aligned} \qquad (7)$$

Les applications (3) et (7) permettent d'obtenir une équivalence des opérations élémentaires de GF(2) sur le corps des réels.

Soit a et b deux éléments de GF(2). Si $\oplus$ et $\otimes$ désignent respectivement l'addition et la multiplication sur GF(2) alors on a les relations suivantes :

$$\begin{aligned} &\varphi(a \oplus b) = -\varphi(a) \cdot \varphi(b), \\ &\varphi(a \otimes b) = -(-\varphi(a))^{\hat{b}} = -(-\varphi(b))^{\hat{a}}. \end{aligned} \qquad (8)$$

On en déduit l'image de l'application φ sur le produit scalaire de deux vecteurs binaires :

$$\begin{aligned} \varphi\left(\sum_{i=1}^{K} a_i b_i\right) &= (-1)^{K+1} \cdot \prod_{i=1}^{K} \varphi(a_i b_i) \\ &= -\prod_{i=1}^{K} \left[-\varphi(a_i)\right]^{\hat{b}_i}. \end{aligned} \qquad (9)$$

4 - CALCUL DE $\underline{R}(0)$ ET $\underline{R}$

4.1 - Calcul de $\underline{R}$

L'indépendance des a(i) entraîne l'indépendance des vecteurs $\underline{b}_k$ de sorte que la matrice $\underline{R}$ s'exprime simplement par la relation

$$\underline{R} = \underline{m} \cdot \underline{m}^T, \qquad (10)$$

avec $\underline{m} = \left[\mathbb{E}[\varphi(\underline{b}_k(1))], \ \ldots\ , \mathbb{E}[\varphi(\underline{b}_k(N))]\right]^T$.

D'après (1), (9) et compte tenu de l'indépendance des a(i), un élément de $\underline{m}$ s'écrit :

$$\underline{m}(p) = -\prod_{i=1}^{K} \mathbb{E}\left[\left(-\underline{a}_k(i)\right)^{\hat{g}(p,i)}\right]. \qquad (11)$$

D'après l'identité :

$$\mathbb{E}\left[\left(-\varphi(\underline{a}_k(i)\right)^n\right] = \begin{cases} 1 & si \quad n \text{ pair,} \\ p_0 - p_1 & si \quad n \text{ impair,} \end{cases} \qquad (12)$$

les termes du produit (11) peuvent prendre deux valeurs et on en déduit une expression de $\underline{R}(p,q)$ sous la forme :

$$\boxed{\begin{cases} \underline{R}(p,q) = (p_0 - p_1)^{V(p,q)}, \\ V(p,q) = w(\underline{G}_p) + w(\underline{G}_q), \end{cases}} \qquad (13)$$

où $\underline{G}_p$ désigne le vecteur contenant la $p^{\text{ième}}$ ligne de $\underline{G}$ et $w(\underline{G}_p)$ son poids binaire (nombre de 1).

4.2 - Calcul de $\underline{R}(0)$

D'après (1), (9) et compte tenu de l'indépendance des a(i), un élément de $\underline{R}(0)$ s'écrit :

$$\underline{R}^0(p,q) = \mathbb{E}\left[\varphi(\underline{b}_k(p))\cdot\varphi(\underline{b}_k(q))\right]$$
$$= \prod_{i=1}^{K}\mathbb{E}\left[\left(-\varphi(\underline{a}_k(i))\right)^{\hat{g}(p,i)+\hat{g}(q,i)}\right]. \quad (14)$$

D'après l'identité (12) les termes du produit (14) peuvent prendre deux valeurs on en déduit une expression de $\underline{R}^0(p,q)$ sous la forme :

$$\boxed{\begin{cases}\underline{R}^0(p,q) = (p_0 - p_1)^{U(p,q)}, \\ U(p,q) = d_H(\underline{G}_p, \underline{G}_q),\end{cases}} \quad (15)$$

où $d_H(\underline{a},\underline{b})$ désigne la distance de Hamming des mots binaires $\underline{a}$ et $\underline{b}$.

5 - CAS DU HAMMING (8,4)

Nous considérons ici le cas d'un codage de Hamming (7,4) par multiplication, de polynôme générateur $g(x) = x^3 + x + 1$, étendu à un Hamming (8,4) en ajoutant le bit de parité du mot à coder. Sa matrice génératrice est donnée par :

$$\underline{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}^T \quad (16)$$

D'après les expressions (13) et (15) et la matrice (16), on en déduit les valeurs des coefficients U(p,q) et V(p,q) sous forme matricielle :

$$\underline{U} = \begin{bmatrix} 0 & 2 & 1 & 2 & 3 & 3 & 2 & 3 \\ 2 & 0 & 3 & 2 & 1 & 3 & 2 & 3 \\ 1 & 3 & 0 & 3 & 2 & 2 & 3 & 2 \\ 2 & 2 & 3 & 0 & 3 & 3 & 2 & 1 \\ 3 & 1 & 2 & 3 & 0 & 2 & 3 & 2 \\ 3 & 3 & 2 & 3 & 2 & 0 & 1 & 2 \\ 2 & 2 & 3 & 2 & 3 & 1 & 0 & 3 \\ 3 & 3 & 2 & 1 & 2 & 2 & 3 & 0 \end{bmatrix}, \quad (17)$$

$$\underline{V} = \begin{bmatrix} 2 & 2 & 3 & 4 & 3 & 3 & 2 & 5 \\ 2 & 2 & 3 & 4 & 3 & 3 & 2 & 5 \\ 3 & 3 & 4 & 5 & 4 & 4 & 3 & 6 \\ 4 & 4 & 5 & 6 & 5 & 5 & 4 & 7 \\ 3 & 3 & 4 & 5 & 4 & 4 & 3 & 6 \\ 3 & 3 & 4 & 5 & 4 & 4 & 3 & 6 \\ 2 & 2 & 3 & 4 & 3 & 3 & 2 & 5 \\ 5 & 5 & 6 & 7 & 6 & 6 & 5 & 8 \end{bmatrix}. \quad (18)$$

Connaissant la probabilité *a priori* p_0 de la suite $\{\varphi(a(k))\}$ et les matrices $\underline{U}$ et $\underline{V}$, on en déduit directement $\underline{R}(0)$ et $\underline{R}$ par application de (13) et (15).

6 - APPLICATION AU CALCUL DE LA DSP D'UN SIGNAL NUMÉRIQUE CODÉ EN BLOCS

6.1 - Cas général

Soit le signal numérique

$$x(t) = \sum_k c(k)\cdot h(t - kT), \quad (19)$$

dont on cherche à calculer la DSP.

Les $c(k)$ sont à valeurs réelles dans $\{-1,1\}$ et h(t) est une forme d'onde à support borné sur l'intervalle [0,T]. On suppose que la suite $\{c(k)\}$ est déduite de la suite $\{b(k)\}$ par la relation $c(k)=\varphi(b(k))$.

On montre que dans ce cas [2], la DSP s'écrit comme la somme d'une densité continue $\gamma_c(f)$ et d'une densité discrète $\gamma_d(f)$:

$$\begin{cases}\gamma_c(f) = |H(f)|^2 \cdot F_c(f), \\ \gamma_d(f) = |H(f)|^2 \cdot F_d(f),\end{cases} \quad (20)$$

où

$$\begin{cases}F_c(f) = \dfrac{1}{NT}\cdot\sum_k \underline{d}^*(f)(\underline{R}(k) - \underline{R}(\infty))\underline{d}(f), \\ F_d(f) = \dfrac{1}{N^2T^2}\cdot\underline{d}^*(f)\underline{R}(\infty)\underline{d}(f)\cdot\sum_k \delta(f - \dfrac{k}{NT}).\end{cases} \quad (21)$$

avec $\underline{d}(f) = \left[1, e^{2i\pi fT}, \ldots, e^{2i\pi f(N-1)T}\right]^T$.

La matrice $\underline{R}(\infty)$ quand elle existe est définie par :

$$\underline{R}(\infty) = \lim_{n \to \infty} \underline{R}(n).$$

Lorsque l'on suppose la séquence avant codage indépendante, les expressions (21) se réduisent à :

$$\begin{cases} F_c(f) = \dfrac{1}{NT} \cdot \underline{d}^*(f)(\underline{R}(0) - \underline{R})\underline{d}(f), \\ F_d(f) = \dfrac{1}{N^2T^2} \cdot \underline{d}^*(f)\underline{R}\underline{d}(f) \cdot \sum_k \delta(f - \dfrac{k}{NT}). \end{cases} \quad (22)$$

6.2 - Exemple numérique

Nous montrons la validité de la méthode proposée dans cet article sur un exemple numérique. Nous reprenons le cas du code de Hamming (8,4) de matrice génératrice (16) du paragraphe 5.

Pour $p_0 = 0{,}1$ et $p_0 = 0{,}9$ nous avons représenté (FFT de 512 pts) :

- *a)* Fig.1.a et Fig.2.a, les spectres simulés par un tirage aléatoire de 1280 mots de code,

- *b)* Fig.1.b et Fig.2.b, les spectres théoriques (20), (22) où les matrices $\underline{R}(0)$ et $\underline{R}$ ont été calculées par (13) et (15) à partir des matrices (17) et (18).

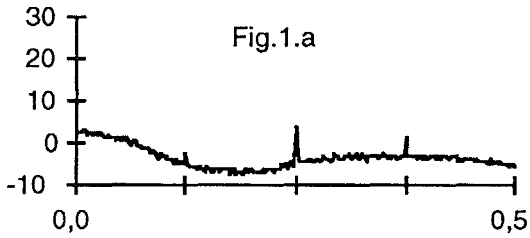

Fig.1.a

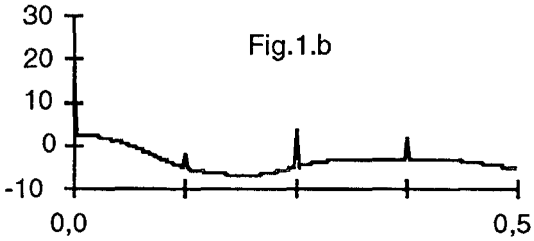

Fig.1.b

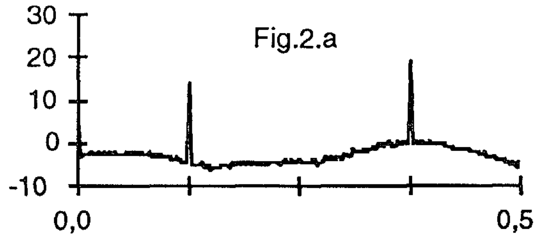

Fig.2.a

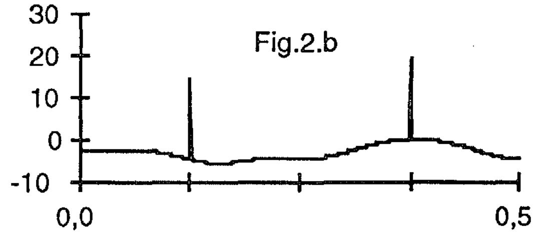

Fig.2.b

CONCLUSION

Nous avons présenté une méthode simple permettant de calculer les matrices de corrélation d'une séquence de bits codés linéairement en blocs quand la séquence avant codage est indépendante. Il semble que l'on puisse étendre ce travail dans le cas où la séquence codée est bruitée par un canal binaire symétrique. Toutefois cette approche ne permet pas de traiter le cas d'une séquence d'entrée non indépendante car l'on ne sait pas calculer de manière explicite l'espérance d'un produit de n variables corrélées.

BIBLIOGRAPHIE

[1] J.H. GILCHRIST, J.B. THOMAS, "Power Spectral Densities of Modulated Error Correcting Coded Sequences", IEEE Trans. on Communications, vol COM-23, n°11, November 1975.

[2] G.L. CARIOLARO, G.P. TRONCA, "Spectra of Block Coded Digital Signals", IEEE Trans. on Communications, COM-22, n°10, October 1974.