Nouvelles séquences binaires et quaternaires pour l'étalement de spectre par séquence directe obtenues via les méthodes de Recuit Simulé et de Recherche Taboue

C. Boulanger*, J.R. Lequepeys*, L. Hérault* et G. Loubet**

* CEA-LETI (CEA/ Technologies Avancées) F 38054 Grenoble Cedex 9 - Service Capteurs et Systèmes pour la Magnétométrie et l'Electromagnétisme - Département Systèmes
** CEPHAG (INPG-ENSIEG) BP 46 Domaine Universitaire 38402 Saint-Martin d'Hères

Résumé

Cet article présente l'application de méthodes combinatoires à l'optimisation de séquences pseudo-aléatoires pour l'étalement de spectre par séquence directe. Cette approche permet pour la première fois la prise en compte des corrélations impaires. Les familles de séquences obtenues, dans les cas binaire et quaternaire, sont comparées à celles de la littérature.

Abstract

This article focuses on the application of combinatorial methods to the optimization of pseudo-random sequences for spread spectrum communications. This approach enables us to take into account for the first time odd correlations. The families of obtained sequences, in the binary and quaternary cases, are compared with those of the litterature.

1 Introduction

Cet article est consacré à la présentation de nouvelles séquences d'étalement binaires (dont les éléments appartiennent à {1; -1}) et quaternaires (dont les éléments appartiennent à {1; -1; j; -j}) optimisées via des méthodes dérivées de l'optimisation combinatoire. Ces séquences sont utilisées dans des systèmes radio utilisant l'étalement de spectre par séquence directe, comme ceux mis au point au LETI [1,2]. Dans un tel système, les séquences sont soit gravées sur un Filtre à Ondes Acoustiques de Surface ou soit chargées dans un ASIC (ce qui permet notamment plus de souplesse d'utilisation).

Deux types de modulation y sont utilisés : la modulation de type BPSK (pour Binary Phase Shift Keying) induit deux sauts de phase qui peuvent être modélisés par les deux transitions (1,1) et (1,-1) dans un espace réel, et la modulation de type QPSK (pour Quaternary Phase Shift Keying) qui induit quatre sauts de phase qui peuvent être modélisés par quatre transitions (1,1), (1,-1), (1,j) et (1,-j) dans un espace complexe.

1.1 Cas mono-utilisateur : une séquence

Dans le cas du BPSK, la séquence d'étalement de longueur N peut être vue comme une suite N-périodique de N entiers 1 ou -1 : $S=(x_0,x_1,...,x_{N-1})$. Deux fonctions d'autocorrélation peuvent être définies, paire et impaire [3]. De même, dans le cas du QPSK, où les x_i sont les racines 4-ièmes de l'unité, quatre fonctions d'autocorrélation (fonctions du décalage u) peuvent être définies de la même manière que précédemment, ce sont les deux précédentes auxquelles on rajoute $\sum_{i=0}^{N-1-u} x_i x_{i+u} + j \sum_{i=N-u}^{N-1} x_i x_{i+u}$, fonction « étendue » d'autocorrélation j-paire de S, et $\sum_{i=0}^{N-1-u} x_i x_{i+u} - j \sum_{i=N-u}^{N-1} x_i x_{i+u}$, fonction « étendue » d'autocorrélation j-impaire de S.

1.2 Cas multi-utilisateurs

Pour un système à Accès Multiple à Répartition par les Codes (ou CDMA en anglais), chaque canal radio possède sa propre séquence d'étalement, mais les utilisateurs émettent sur la même fréquence centrale. Dans le cas du BPSK, l'interférence entre deux canaux décroît lorsque les deux fonctions d'intercorrélation sont faibles, quel que soit le décalage entre les séquences. Les deux fonctions d'intercorrélation entre deux séquences $S_1=(x_0,x_1,...,x_{N-1})$ et $S_2=(y_0,y_1,...,y_{N-1})$ sont appelées intercorrélations paires et impaires [3]. De même, dans le cas du QPSK, les fonctions d'intercorrélation (fonctions du décalage u) entre deux séquences sont les deux précédentes auxquelles on rajoute $\sum_{i=0}^{N-1-u} x_i y_{i+u} + j \sum_{i=N-u}^{N-1} x_i y_{i+u}$, fonction « étendue » d'intercorrélation j-paire et $\sum_{i=0}^{N-1-u} x_i y_{i+u} - j \sum_{i=N-u}^{N-1} x_i y_{i+u}$, fonction « étendue » d'intercorrélation j-impaire.

Les critères pour l'optimisation de familles de séquences sont la minimisation, pour tout décalage u non nul, du module des fonctions d'autocorrélation et la minimisation, pour tout décalage u, du module des fonctions d'intercorrélation.

1.3 Précédentes approches

Dans le cas de l'optimisation d'une seule séquence, quelques auteurs ont proposé des constructions de séquences binaires basées sur l'optimisation des propriétés de corrélation paire (voir [3], [4] et les références

associées). En ce qui concerne les familles de séquences, les propriétés des corrélations paires de séquences générées par différents registres à décalage modifiés ont été étudiées. Dans quelques cas, des familles de séquences binaires et quadriphases présentant des propriétés optimales en terme de corrélation paire ont été trouvées.
Comme il n'existe pas de méthodes mathématiques pour construire des séquences avec des propriétés de corrélation impaire optimales, les séquences obtenues précédemment présentent souvent de mauvaises propriétés de corrélation à la fois paire, impaire, j-paire et j-impaire ; de plus, ces séquences existent seulement pour un nombre limité de longueurs, par exemple 2^k-1 pour les familles de séquences dérivées de la théorie des Corps de Galois (la taille de ces familles est également limitée telles les m-séquences ou les familles de Gold ou de Kasami) ou pour des longueurs égales aux nombres premiers dans le cas des séquences de Legendre.
Ce sont pour ces raisons que l'on a développé des méthodes informatiques et qui permettent de prendre en compte tous les critères d'optimisation voulus. L'un de leur plus grand intérêt réside dans leur souplesse d'utilisation (un nombre et une longueur de séquences à la carte).

2 Algorithmes proposés

Au début des années 80, des algorithmes d'optimisation très puissants sont apparus - on les appelle métaheuristiques - tels le Recuit Simulé et la Recherche Taboue (pour un descriptif des algorithmes, se reporter à [4]). Leur mise en œuvre est décrite dans le brevet [5].

2.1 Recuit simulé

Le Recuit Simulé, proposé par Kirkpatrick et Cerny de manière indépendante [6, 7] dans le cas de la résolution de problèmes combinatoires, a été utilisé avec succès dans de nombreux problèmes [8]. Pour implémenter cette méthode, nous avons besoin de reformuler le problème en terme d'optimisation d'une certaine fonction coût. Dans le cas de l'optimisation de séquences d'étalement, ces fonctions coûts sont les suivantes : pour une séquence, c'est le maximum en valeur absolue de toutes les fonctions d'autocorrélation pour tous les décalages u non nuls. Dans le cas de l'optimisation de familles de séquences, c'est le maximum à la fois de toutes les fonctions d'autocorrélation, pour tout décalage u autre que nul, et d'intercorrélation, pour tous les décalages u, que l'on va chercher à diminuer. On appelera la valeur minimale obtenue « **bruit résiduel** ».
De manière classique, un algorithme de recherche de minimum local (ou « descente locale ») a pour point de départ une solution initiale aléatoire et évolue de manière descendante sur une hypersurface de la fonction coût, en procédant à des petits changements sur la solution courante, jusqu'à ce qu'aucune amélioration en terme de fonction coût ne puisse être envisagée. Les transformations élémentaires choisies définissent l'espace de recherche. Nous avons sélectionné les transformations suivantes : une transformation associée à un bit aléatoire de la séquence ou des séquences concernées ($1\leftrightarrow$-1 ou $1\leftrightarrow$j ou $1\leftrightarrow$-j) ou ces mêmes transformations pour un ensemble aléatoire de bits de la ou des séquences considerées. Le principal désavantage de cette méthode est que l'on a tendance à rester piéger dans un minimum local sans avoir la possibilité de s'en extraire et des simulations permettent de montrer que les minima trouvés sont de médiocre qualité.
L'idée maîtresse de la méthode de Recuit Simulé est d'éviter d'être pièger dans un minimum local en acceptant des transformations défavorables avec une probabilité de type Boltzmann $e^{-\frac{\Delta C}{kT}}$, où ΔC est le changement de la fonction coût en valeur algébrique induit par une transformation élémentaire sur la configuration courante et T est le facteur température. Cet algorithme est une « trempe » thermodynamique. A hautes températures, beaucoup de transformations défavorables sont acceptées, alors qu'à basses températures, on est très exigeant.
Les simulations débutent à une température initiale T_i définie de telle manière que le système consideré puisse facilement évoluer d'un minimum local vers un autre. Après un nombre de transformations acceptées ou non,
N_{TR}, la température est décrémentée géométriquement, via une loi de type $T\rightarrow\alpha T$, avec $0<\alpha<1$ mais très proche de 1, jusqu'à ce que le système soit effectivement « gelé » dans un état final c'est-à-dire qu'une descente locale sur la meilleure configuration trouvée ne permette pas d'obtenir un meilleure résultat. Ainsi, au début de l'optimisation par le Recuit Simulé, on accepte beaucoup de transformations favorables ou non. Au-fur-et-à-mesure, on va accepter de moins en moins de transformations défavorables, jusqu'à se retrouver à une très faible température où le système consideré n'évolue plus parce qu'on ne trouve plus de « bonnes » transformation. Ce processus d'optimisation imite les processus d'équilibres thermodynamiques. On trouvera des précisions sur de telles méthodes dans la référence [9].

2.2 Recherche taboue

La Recherche Taboue, introduite par Glover [10], est une autre stratégie de recherche locale créée pour pouvoir s'extraire des minima locaux. Même s'il n'y a pas de meilleures solutions que la solution courante à quelques transformations près, on se déplace quand même vers la meilleure ou la moins mauvaise des solutions que l'on peut atteindre dans un voisinage de l'état courant. On a utilisé également des procédés d' intensification : par exemple, la meilleure séquence obtenue lors de la Recherche Taboue est sauvegardée et employée lors de nouvelles mises à jour de cet algorithme. Les mêmes transformations que celles utilisées par le Recuit Simulé ont été employées. Mais, on court le risque de retomber sur des solutions déjà explorées, et par la même de tourner en rond, lorsque l'on décrit l'espace des minima locaux. Afin d'éviter cette situation, l'idée est d'utiliser un procédé à mémoire qui conserve les dernières transformations effectuées dans une liste dite « Taboue ». Une transformation que l'on effectue

souvent est interdite pendant un certain nombre, N_{TA}, d'itérations. On se reportera à la référence [9] pour une description plus complète de cette méthode.

2.3 Optimalité

Comme le nombre d'itérations est fini, on n'a aucune garantie que le Recuit Simulé et la Recherche Taboue trouvent le minimum global de façon certaine. Le facteur de pénalisation N_{TA} a besoin d'être déterminé lors d'essais successifs. Il n'y a, de même, pas de règle absolue pour déterminer N_{TR}. On peut néanmoins remarquer qu'une des particularités de ces algorithmes stochastiques est d'être indépendant de l 'état initial, ce qui n'est clairement pas le cas des algorithmes de recherche locale. De plus, seule la convergence asymptotique du Recuit Simulé a été prouvée, la convergence de la Recherche Taboue est plus empirique, mais il faut remarquer que ce dernier donne de meilleurs résultats dans un temps de simulation donné. Les spécialistes le reconnaissent et lui accordent beaucoup de développements à l'heure actuelle sans bien pouvoir justifier ce meilleur comportement. Les performances obtenues dans le cas des deux algorithmes, on le verra plus loin, sont clairement bien meilleures que celles des méthodes dites « classiques », telles les constructions mathématiques et les algorithmes de descente locale .

3 Résultats

3.1 Séquences binaires

En ce qui concerne les séquences de longueurs comprises entre 1 et 100, et plus spécialement dans le cas des propriétés d'autocorrélation paire, les performances de nos algorithmes (C.O. pour Combinatorial Optimization) sont présentées figure 1. Elles sont comparées à une borne arithmétique optimale.

Jusqu'à la longueur 88, les performances de nos algorithmes sont optimum : un minimum global est trouvé. Au-delà de cette valeur, on perd la borne inférieure d'un pas, principalement parce que les temps de calcul deviennent trop grands (supérieurs à la semaine typiquement). A titre de comparaison, des chercheurs, tels Fourdan [11] et Lindner [12], ont proposé des logiciels de recherche locale ou des hardwares de recherche exhaustive qui n'ont permis d'optimiser des séquences que jusqu'à la longueur 40.

En ce qui concerne les propriétés d'intercorrélation et d'autocorrélation, les performances obtenues sont présentées, pour des familles de séquences de tailles variables et de longueur 63, et comparées à celles des séquences classiques (voir [3], [4] et les références associées), en figure 2. Les performances présentées par les familles obtenues via les algorithmes stochastiques sont meilleures et ce pour n'importe quelle taille de familles, mais c'était prévisible parce que les familles de la littérature sont optimisées en terme d'auto- et d'intercorrélations paires seulement. Notamment, les performances sont légèrement meilleures que celles de la famille de Gold, généralement utilisée dans les dispositifs pratiques. Malheureusement, nous n'atteignons pas la borne de Welch [3] (laquelle ne tient compte que des corrélations paires). A la connaissance des auteurs, il n'y a pas eu de tentatives d'optimisation sur des hardwares ou des logiciels de familles de séquences dans la littérature.

3.2 Séquences quaternaires

Nous présentons également les performances de nos algorithmes pour les séquences quaternaires en figure 3. Les performances obtenues sont ici aussi comparées à celles de familles de séquences de la littérature (voir [4] et les références associées). Nos performances sont meilleures et l'écart avec les familles classiques est plus marqué que précédemment.

4 Futures évolutions et conclusion

L'utilisation de métaheuristiques dédiées à l'optimisation combinatoire a permis l'optimisation de nouvelles séquences présentant des propriétés de corrélation qui sont plus favorables que celles déjà publiées (Kasami, Novosad), en particulier parce que ces méthodes permettent de tenir compte de tous les critères d'optimisation, ce que ne permettent pas les constructions mathématiques.

Un autre intérêt est que l'on peut optimiser des séquences de longueur quelconque et des familles de séquences de taille quelconque, binaires ou quaternaires, ce que la théorie ne pouvait pas permettre. Ceci permet une plus grande souplesse dans leur utilisation dans les applications de radiocommunications, notamment pour les performances requises en terme de débit - lié directement à la longueur des séquences - et pour un nombre d'utilisateurs donné - lié au nombre de séquences dans la famille considérée.

Nous allons maintenant nous consacrer à des améliorations : en particulier des efforts de codage informatique pour aller plur vite et obtenir ainsi des résultats de meilleure qualité. Nous allons également aborder d'autres procédés combinatoires.

Remerciements

Cette étude a été effectuée dans le cadre du programme européen ACTS, et plus précisément du projet FRANS ACTS 0083. Elle a permis de déterminer les séquences utilisées dans le cadre de ce projet par le LETI.

Bibliographie

[1] C. Fort et A. Le Roy, "Composant pour récepteur ou émetteur-récepteur différentiel de signaux à étalement de spectre par séquence directe et émetteur-récepteur correspondant", Brevet Français N°9608272 - 06/07/1993.

[2] D. Lattard, J.R. Lequepeys, B. Piaget et N. Danièle, "Circuit numérique pour récepteur différentiel de signaux à étalement de spectre par séquence directe", Brevet Français, N°9514322 - 04/12/1995.

[3] D.W. Sarwate et M.B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences", Proc. IEEE 68, pp. 593-619, 1980.

[4] C. Boulanger, J.R. Lequepeys et L. Hérault, "New spreading binary sequences obtained by Simulated Annealing and Tabu Search", ICPMSC'96, Dec. 3-5, Hong Kong 1996.
[5] C. Boulanger, J.R. Lequepeys et L. Hérault, "Procédé de transmission à étalement de spectre par séquence directe, avec génération et optimisation des séquences", Brevet français N°9614671, 29/11/1996.
[6] S. Kirkpatrick, C.D. Gelatt and M.P. Vecchi, "Optimization by simulated annealing", Science, vol. 220, pp. 671-680, 1983.
[7] V. Cerny, "A thermodynamical approach to the travelling salesman problem : an efficient simulated algorithm", J. Op. Res., 32, pp. 41-51, 1985.
[8] A.A. El Gamal, L.A. Hemachandra, I. Sherpling and V.K. Wei, "Using simulated annealing to design good codes", IEEE Trans. on Inform. Th., vol. IT-33, pp. 119-123, Jan. 1987.
[9] M. Pirlot, "General local search heuristics in Combinatorial Optimization : a tutorial", Belgian Journal of Operations Research, Statistics and Computer Science, vol. 32, no. 1-2, pp. 7-67, 1992.
[10] F. Glover, "Future paths for integer programming and links to artificial intelligence", Compute