



Open Archive TOULOUSE Archive Ouverte (OATAO)

OATAO is an open access repository that collects the work of Toulouse researchers and makes it freely available over the web where possible.

This is an author-deposited version published in : <http://oatao.univ-toulouse.fr/>
Eprints ID : 17195

The contribution was presented at GRETSI 2015:
<http://gretsi.fr/colloque2015/>

To cite this version : Benaddi, Tarik and Poulliat, Charly and Boucheret, Marie-Laure and Gadat, Benjamin and Lesthievant, Guy *Récepteur Exact pour la Décomposition de Laurent pour les CPM*. (2015) In: 25eme Edition du Colloque Groupe de Recherche et d'Etudes du Traitement du Signal et des Images (GRETSI 2015), 8 September 2015 - 11 September 2015 (Lyon, France).

Any correspondence concerning this service should be sent to the repository administrator: staff-oatao@listes-diff.inp-toulouse.fr

Récepteur exact pour la décomposition de Laurent pour les CPM

Tarik BENADDI^{1 2 3}, Charly POUILLIAT^{2 3}, Marie-Laure BOUCHERET^{2 3}, Benjamin GADAT⁴, Guy LESTHIEVENT¹

¹Centre National d'Études Spatiales (CNES) - Toulouse

²Université de Toulouse, ENSEEIHT/IRIT

³TéSA - Toulouse

⁴Thales Alenia Space - Toulouse

{tarik.benaddi, charly.poulliat, marie-laure.boucheret}@enseeiht.fr,
benjamin.gadat@thalesaleniaspace.com, guy.lesthievent@cnes.fr

Résumé – Dans ce papier, on propose un récepteur exact pour les modulations à phase continue (CPM) basé sur la décomposition/représentation de Laurent. L'approche proposée permet de remédier aux problèmes des interférences inter-symboles et inter-composantes induites par les composantes de Laurent sans introduire un étage supplémentaire dans le récepteur de type filtre blanchissant. Puis, en se basant sur la décomposition de Rimoldi, on proposera une méthode analytique pour construire le nouveau banc de filtre de réception.

Abstract – In this paper, we derive an exact receiver for continuous phase modulations based on Laurent decomposition. The proposed method allows to cancel the inter-symbol and inter-component interference induced by the Laurent components, without the use of an additional processing stage at the receiver side such as whitening filters. Furthermore, based on Rimoldi decomposition, we will propose an analytical method to derive the new receiver filter bank.

1 Introduction

La modulation à phase continue (CPM) est une famille de modulation de phase où les transitions de la phase entre les différents symboles modulés sont continues. Grâce à leur phase continue et à leur enveloppe constante, les signaux CPM ont une meilleure efficacité spectrale et résistent mieux aux non linéarités induites par les amplificateurs embarqués ou les canaux non linéaires. Ces propriétés intéressantes font que les CPM sont un bon choix dans plusieurs systèmes de communication (DVB-RCS2, Stanag 4660 (TCS-5GHz), GSM, Bluetooth...).

Après l'invention des turbo-codes [1], les CPM codées ont beaucoup bénéficié des schémas de turbo décodage. En effet, on a montré dans [2] que la CPM peut être décomposée comme la somme d'un encodeur de phase continue (CPE) concaténé en série avec un modulateur sans mémoire (MM). De manière indépendante, [3] a dérivé une autre décomposition de la CPM binaire qui représente un signal donné comme la somme de plusieurs signaux modulés en amplitude. L'intérêt majeur de cette représentation est que la quasi totalité de l'énergie du signal est concentrée dans les premières composantes seulement, même pour les ordres de modulations élevées. Ceci permet d'implémenter des récepteurs à faible complexité. L'extension de la décomposition de Laurent au cas M-aire est décrite dans [4]. Dans ce papier, et sans perte de généralités, on se limitera au cas binaire.

Dans [5, 6], les auteurs ont développé le treillis sous-jacent

de la décomposition de Laurent et ont décrit par ce fait les récepteurs Viterbi et BCJR [7] correspondants. Toutefois, dans leur métrique de branches, ils négligent l'interférence inter-composantes (composantes non orthogonales) et l'interférence inter-symboles (les filtres de mises en forme ont une durée supérieure au temps symbole) devant le bruit du canal. Dans le cas d'un récepteur exact et optimal, il faudrait également introduire un filtre blanchissant. Ce filtre devient encore plus important dans les cas de detections non cohérentes [8], d'égalisation [9] ou de multi-porteuses [10]. Dans ce papier, on dérivera dans un premier temps un récepteur basé sur le treillis de Laurent qui prend en compte les interférences inter-composantes et inter-symboles, puis on montrera comment calculer le banc de filtres correspondant et on exprimera la relation entre la décomposition de Rimoldi et la décomposition de Laurent.

2 Description d'un signal CPM

On considère dans ce papier une séquence de N symboles d'information $\alpha = \{\alpha_i\} \in \{\pm 1, \dots, \pm(M-1)\}^N$. Le signal CPM à transmettre s'écrit donc :

$$s(t) = \sqrt{\frac{2E_s}{T}} \cos(2\pi f_0 t + \theta(t, \alpha) + \theta_0) = \Re[s_b(t)e^{j2\pi f_0 t}] \quad (1)$$

avec

$$\theta(t, \alpha) = \pi h \sum_{i=0}^{N-1} \alpha_i q(t - iT) \text{ où } q(t) = \begin{cases} \int_0^t g(\tau) d\tau, & t \leq L \\ 1/2, & t > L \end{cases}$$

avec E_s l'énergie par symboles, T le temps d'un symbole, f_0 la fréquence porteuse, θ_0 la phase à l'origine, $\theta(t, \alpha)$ la phase du signal, $g(t)$ la réponse en fréquence, $h = k/p$ l'indice de modulation ($k \wedge p = 1$), L la mémoire et $\Re(\cdot)$ la partie réelle. Quand $L = 1$ ($L \geq 2$), on parle d'une CPM à réponse totale (resp. partielle).

2.1 Récepteur de Rimoldi

Posons $U_i = (\alpha_i + (M - 1))/2 \in \{0, 1, \dots, M - 1\}$. [2] montre que le modulateur CPM s'écrit comme la concaténation en série du CPE, décrit par un treillis invariant dans le temps, et du MM, se présentant sous la forme d'un banc de filtres, chacun de longueur T . Le treillis du CPE est défini par le vecteur d'état $\sigma_n^R = [U_{n-1}, \dots, U_{n-L+1}, V_n = [\sum_{i=0}^{n-L} U_i] \bmod p]$. On suppose que le signal $s(t, \alpha)$ est envoyé dans un canal sans mémoire avec un bruit blanc Gaussien (AWGN) avec une densité spectrale de puissance $N_0/2$. L'enveloppe complexe du signal reçu est donnée par :

$$y(t) = \sqrt{\frac{2E_s}{T}} \exp(j\psi(t, \alpha)) + n(t), \quad t > 0 \quad (2)$$

où $\psi(t, \alpha)$ est la phase modifiée [2]. Les sorties des filtres du MM $\{s_i(t)\}$ sont échantillonnées tous les nT , ce qui permet de calculer la projection du signal reçu, Eq. (2) :

$$\mathbf{y}^n = \left[\int_{nT}^{(n+1)T} y(l) s_i^*(l) dl \right]_{1 \leq i \leq pLM}$$

sur l'espace des signaux du récepteur CPM. En considérant n'importe quelle base orthonormée de cet espace, [11], la probabilité $p(\mathbf{y}^n / X_n)$ est proportionnelle $\exp\{2\Re(\mathbf{y}_i^n) / N_0\}$. On utilisera cette expression comme métrique de branche dans le treillis du CPE quand on déroule l'algorithme BCJR [7]. La Fig. 1a illustre le récepteur de Rimoldi.

2.2 Récepteur de Laurent-Kaleh

Dans le cas binaire, la décomposition de Laurent [3] permet de réécrire l'enveloppe complexe de l'Eq. (1) sous la forme de la somme de $K = 2^{L-1}$ signaux modulés en amplitude par les pseudo-symboles $a_{k,n} = \exp(j\pi h A_{k,n})$ comme suit :

$$s_b(t) = \sqrt{2E_s/T} \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} e^{j\pi h A_{k,n}} C_k(t - nT) \quad (3)$$

$$C_k(t) = s_0(t) \prod_{j=1}^{L-1} s_{j+L\beta_{k,j}}(t), \quad 0 < k \leq K - 1$$

$$A_{k,n} = \sum_{i=0}^n \alpha_i - \sum_{j=1}^{L-1} \alpha_{n-j\beta_{k,j}}, \quad s_j(t) = \frac{\sin(\psi(t + jT))}{\sin(\pi h)}$$

$$\psi(t) = \begin{cases} 2\pi h q(t), & 0 \leq t \leq LT \\ \pi h - 2\pi h q(t - LT), & LT \leq t \leq 2LT \\ 0, & \text{sinon} \end{cases}$$

avec $\beta_{k,j}$ est le $j^{\text{ème}}$ bit de la décomposition binaire de l'indice k . Le signal reçu est toujours $y(t) = s_b(t) + n(t)$.

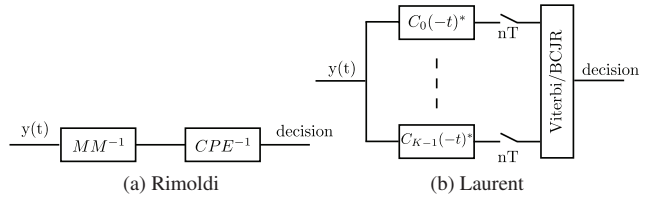


FIGURE 1: Schéma de la décomposition de Rimoldi et de Laurent

Dans le contexte d'un récepteur maximum de vraisemblance (ML), [5] montre que l'on peut former le signal Eq. (3) à partir d'un treillis. En effet, à chaque instant nT , sachant le symbole d'entrée α_n , on peut calculer tous les pseudo-symboles $a_{k,n}$ à partir de l'état courant de la phase, définie par $\sigma_n^L = [a_{0,n-L}, \alpha_{n-L+1}, \dots, \alpha_{n-1}]$, selon la récursion :

$$A_{k,n} = A_{0,n-L} + \alpha_n + \sum_{i=1}^{L-1} \alpha_{n-i} \cdot (1 - \beta_{k,i}) \quad (4)$$

Ainsi, pour chaque transition correspond un signal $\bar{s}_i(t) = \sqrt{2E_s/T} \sum_{k=0}^{K-1} a_{k,n} C_k(t - nT)$. La métrique de branche pour un bruit blanc Gaussien est donc donnée par :

$$\exp\left(\frac{-1}{N_0} \int_{-\infty}^{+\infty} |y(t) - \bar{s}_i(t)|^2\right) \quad (5)$$

La Fig. 1b schématise ce récepteur. En se basant sur cette représentation, [6] développe le récepteur maximum *a posteriori* (MAP) correspondant basé sur l'algorithme BCJR. Les 2^{L-2} premières composantes $\{C_k(t)\}$ sont des filtres de mises en formes de tailles supérieures à T [3] et qui ne respectent pas le critère de Nyquist. Par conséquent, la séquence de bruit échantillonné à la sortie des filtres de réception est corrélée. Pour se ramener à un bruit blanc, il faudra introduire un filtre blanchissant [12] après les $C_k^*(-t)$ concernés. D'autre part, comme les composantes $\{C_k(t)\}$ ne sont pas orthogonales, on aura de l'interférence inter-symboles (ISI).

Afin de simplifier l'Eq. (5), les différents auteurs assument un bruit échantillonné blanc et négligent l'ISI devant le bruit du canal. Ce qui équivaut, après simplification de l'Eq. (5), à filtrer $y(t)$ par les $C_k^*(-t)$ et échantillonner les sorties tous les nT [5, 6] comme le montre le schéma Fig. 1b.

3 Récepteur exact de Laurent

L'expression de $\bar{s}_i(t)$ ne prend en compte que les K pseudo-symboles $\{A_{k,n}\}_k$ et néglige l'effet des $(L - 1)K$ précédents symboles relatifs aux composantes $C_k(t)$ de support $> T$. Soit L_k la longueur de $C_k(t)$ ($C_k(t) = 0, \forall t > L_k T$), [3]. Le nouveau signal à l'instant $\bar{s}_i(t)$ s'écrit :

$$\bar{s}_i(t) = \sqrt{2E_s/T} \sum_{k=0}^{K-1} a_{k,n} C_k(t - nT) + \underbrace{\sqrt{2E_s/T} \sum_{k=0}^{K/2} \left(\sum_{\ell=1}^{L_k-1} a_{k,n-\ell} C_k(t - (n-\ell)T) \right)}_{\text{terme correctif}}$$

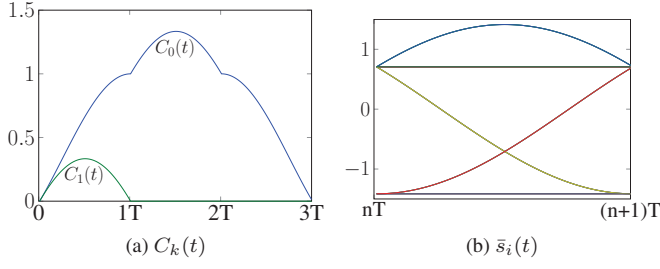


FIGURE 2: Composantes et banc de filtres exact pour une $L=2$, REC, $h=2/3$

Le terme correctif représente l'interférence des symboles passés. A l'instar de l'Eq. (4), on peut retrouver tous les pseudo-symboles passés à partir de σ_n^L . Posons :

$$\underline{\alpha}_n = [\alpha_{n-L+1}, \dots, \alpha_n], \quad \mathbf{B}_k = \begin{pmatrix} (K-1-k)_2^T \\ 1 \end{pmatrix}_{[L \times 1]}$$

$$\mathbf{J} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix}_{[L \times L]}$$

où $(K-1-k)_2$ est la décomposition binaire de $K-1-k$ sur $L-1$ bits et T l'opérateur transposition. Les pseudo-symboles $A_{k,n-\ell}$ peuvent être calculés par la récursion :

$$A_{k,n-\ell} = A_{0,n-L} + \underline{\alpha}_n \mathbf{J}^\ell \mathbf{B}_k, \quad 0 \leq \ell \leq L \quad (6)$$

Exemple : pour $L=4$ ($K=8$), on a :

$$\underline{\alpha}_n^T = \begin{pmatrix} \alpha_{n-3} \\ \dots \\ \alpha_n \end{pmatrix}, \quad \mathbf{B}_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{J} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Ainsi, la métrique de branche dans l'Eq. (5) est plus exacte ici puisqu'on prend en compte les interférences. Désormais, au lieu de filtrer avec les $C_k^*(-t)$ à la réception, on filtre avec un banc de filtres constitué des pM^L différentes valeurs de $\bar{s}_i(t)$ tronquées sur $[nT, (n+1)T]$. Afin de trouver les différents $\bar{s}_i(t)$ pour un schéma CPM donné, il suffit de simuler en amont et une seule fois $\{\bar{s}_i(t) \cdot \pi_n(t)\}$ pour tous les pM^{L-1} états σ_n^L , $\pi_n(t)$ est la fonction porte unitaire de support $[nT, (n+1)T]$. La Fig. 2 donne un exemple du banc de filtres pour une configuration CPM.

3.1 Expression analytique du banc de filtres

Pour trouver l'expression analytique du banc de filtres $\{\bar{s}_i\}_i$, on peut utiliser la décomposition de Rimoldi. En effet, à partir d'un état σ_n^R du CPE et du symbole d'entrée U_n , la forme d'onde

$s_i(t)$ correspondante, $t = \tau + nT$, $0 \leq \tau < T$, est [2] :

$$s_i(t) = \exp(j\bar{\psi}(\tau, X_n))$$

$$X_n = [U_n, \sigma_n^R] = [U_n, U_{n-1}, \dots, U_{n-L+1}, V_n]$$

$$\bar{\psi}(\tau, X_n) = \left[2\pi h V_n + 4\pi h \sum_{k=0}^{L-1} U_{n-k} q(\tau + kT) + W(\tau) \right]$$

$$W(\tau) = \pi h (M-1) \tau / T - 2\pi h (M-1) \sum_{i=0}^{L-1} q(\tau + iT) + (L-1)(M-1)\pi h$$

Finalement, pour former le signal CPM final, il faut revenir à la fréquence non modifiée, pour cela, il suffit de multiplier, à n'importe quelle section du treillis n , les $\{s_i(t)\}_i$ par $\exp(j2\pi(f_1 - f_0)t)$ avec $f_1 = f_0 - h(M-1)/2T$. On trouve :

$$\exp(j2\pi(f_1 - f_0)t) = \exp\left(-j\pi \frac{(M-1)h}{T} t\right)$$

$$= \exp\left(-j\pi \frac{(M-1)h}{T} \tau\right) \exp(-j\pi(M-1)hn)$$

$$= \exp\left(-j\pi h \frac{\tau}{T}\right) \exp(-j\pi hn) \quad (\text{cas binaire}) \quad (7)$$

A l'instant suivant, c'est-à-dire $n+1$:

- si k dans h est pair (et donc p impair), le facteur exponentiel à gauche dans Eq. (7) devient :

$$\exp(-j\pi h(n+1)) = \exp(-j\pi hn) \exp(-j\pi h)$$

$$= \exp(-j\pi hn) \exp(-j\pi h + j2\pi hp) \quad (\pi hp \equiv 0[2\pi])$$

$$= \exp(-j\pi hn) \exp(j\pi(p-1)h)$$

Or $p-1$ est pair, $\exists \beta \in \mathbb{N}/p-1 = 2\beta$, donc quand on multiplie Eq. (7) avec $s_i(t)$, on obtient en argument :

$$\bar{\psi}(\tau, X_n) + \pi(p-1)h$$

$$= 2\pi h V_n + 4\pi h \sum_{k=0}^{L-1} U_{n-k} q(\tau + kT) + W(\tau) + 2\pi h \beta$$

$$= 2\pi h (V_n + \beta) + 4\pi h \sum_{k=0}^{L-1} U_{n-k} q(\tau + kT) + W(\tau)$$

$$= \bar{\psi}(\tau, X'_n) \quad (\text{où } X'_n = [U_n, \dots, U_{n-L+1}, V_n + \beta])$$

Or, $\bar{\psi}(\tau, X'_n)$ a déjà été calculé à l'instant n . On retrouve donc entièrement le banc de filtres en évaluant en une seule section n , $\forall n \geq 0$. La Fig. 2b trace les différents filtres obtenus pour une $L=2$, REC et $h=2/3$ à un instant n .

- En revanche, si k est impair, alors :

$$\exp(-j\pi h(n+1)) = \exp(-j\pi hn) \exp(-j\pi h)$$

$$= \exp(-j\pi hn) \exp(-j\pi h + j2\pi hp) \quad (2\pi hp = 0[2\pi])$$

$$= \exp(-j\pi hn) \exp(j\pi 2(p-1)h) \exp(j\pi h)$$

Or $2(p-1)$ est pair. Comme dans le cas précédent, on peut montrer que le banc de filtres de l'instant $n+1$, peut être calculés en multipliant les filtres du banc précédent par $\exp(j\pi h)$.

De la même manière, on peut montrer que le banc de filtres à l'instant $n+\ell$, $\forall \ell \in \mathbb{N}$ est le même que celui de $n+(\ell \text{ modulo } 2)$. Par conséquent, pour retrouver tous les filtres de réception, on

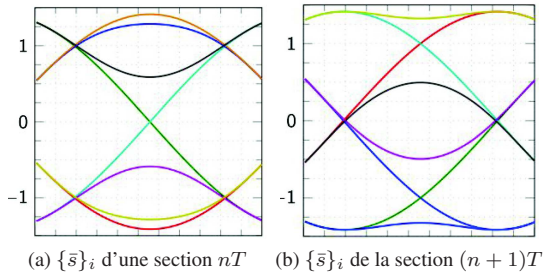


FIGURE 3: Banc de filtres exact pour une $L=2$, REC, $h=3/4$

	λ_1	λ_2	λ_4	λ_9	λ_{10}	ρ_4	ρ_5	E_s/N_0 seuil
exact	0.12	0.59	-	0.009	0.28	0.4	0.6	-1.87dB
classique	0.11	0.48	0.12	-	0.29	0.2	0.8	-0.5dB

TABLE 1: Codes LDPC optimisés pour le récepteur exact et classique

commence par calculer les $\{\bar{s}_i(t)\}_i$ correspondant à un instant $n, \forall n \geq 0$, puis à l'instant suivant $n+1$ pour trouver les filtres manquants, ce qui est équivalent à multiplier le banc précédent par $\exp(j\pi h)$. La Fig. 3 trace les différents filtres obtenus pour une $L=2$, REC, $h=3/4$ dans deux sections du treillis consécutives.

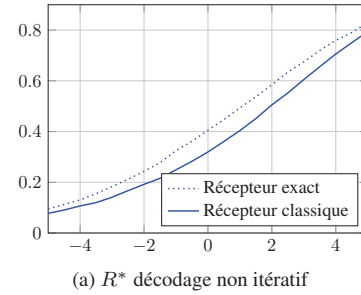
N.B. : dans le cas de modulation M-aire, il faut distinguer les cas selon la parité de : $1 - M \bmod p$.

4 Comparaison de performance

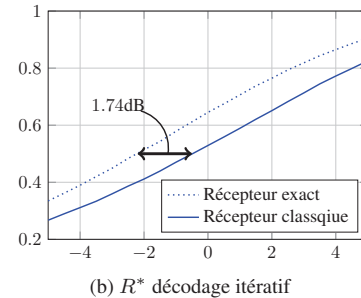
La Fig. 4b trace le rendement maximal R^* possible d'un code externe en concaténation série. R^* est approximé ici par l'aire sous la courbe de la fonction EXIT chart [13] associée à un décodage MAP [6] basé sur les deux récepteurs de la GMSK $h = 1/3, L = 3, BT = 0.3$ dans un schéma itératif. La Fig. 4a illustre R^* dans un schéma non itératif (Le point correspondant à une information mutuelle a priori nulle dans l'EXIT chart). Dans le cas non itératif, le récepteur introduit dans ce papier permet une légère amélioration par rapport au récepteur classique. En revanche, dans le cas itératif, notre récepteur présente une amélioration considérable. Ainsi, pour un rendement de code externe de $1/2$, on peut observer un gain allant jusqu'à 1.74 dB rien qu'en changeant le banc de filtres de réception. En utilisant les méthodes introduites dans [14], le tableau Table 1 résume le profil des codes LDPC (Low Parity Check Code [15]) optimisés et le seuil correspondant.

5 Conclusion

Dans ce papier, nous avons dérivé un récepteur optimal exact basé sur la décomposition de Laurent qui permet d'une part, de supprimer les interférences induites par les composantes de Laurent, et d'autre part, de former un banc de filtres de réception à temps symbole. Dans un deuxième temps, nous avons dérivé deux méthodes pour calculer ce banc de filtres, l'une à partir du treillis de Kaleh [5] et l'autre à partir du treillis de Rimoldi [2]. Les futurs travaux porteront sur les performances de



(a) R^* décodage non itératif



(b) R^* décodage itératif

FIGURE 4: Comparaison R^* pour la GMSK $h = 1/3, L = 3, BT = 0.3$ notre récepteur dans des schémas plus sensibles à l'interférence (multi-trajet, multi-porteuses, égalisation, ...).

Références

- [1] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding : Turbo-codes," *IEEE Trans. Commun.*, vol. 44, no. 10, pp. 1261–1271, 1996.
- [2] B. E. Rimoldi, "A decomposition approach to cpm," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 260–270, 1988.
- [3] P. Laurent, "Exact and approximate construction of digital phase modulations by superposition of amplitude modulated pulses (amp)," *IEEE Trans. Commun.*, vol. 34, no. 2, pp. 150–160, 1986.
- [4] U. Mengali and M. Morelli, "Decomposition of m-ary cpm signals into pam waveforms," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1265–1275, 1995.
- [5] G. K. Kaleh, "Simple coherent receivers for partial response continuous phase modulation," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 9, pp. 1427–1436, 1989.
- [6] P. A. Murphy, G. E. Ford, and M. Golanbari, "Map symbol detection of cpm bursts," *Kluwer International Series in Engineering and Computer Science*, pp. 199–210, 1997.
- [7] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate (corresp.)," *IEEE Trans. Inf. Theory*, vol. 20, pp. 284–287, 1974.
- [8] L.-J. Lampe, R. Tzschoppe, J. B. Huber, and R. Schober, "Noncoherent continuous-phase modulation for ds-cdma," in *IEEE International Conference on Communications, 2003. ICC'03*, vol. 5, 2003, pp. 3282–3286.
- [9] J. Tan and G. L. Stuber, "Frequency-domain equalization for continuous phase modulation," in *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, 2005, pp. 2479–2490.
- [10] A. Montazeri and J. Haddadnia, "Mcm and cpm combination as compared to the use of fde for cpm." Citeseer.
- [11] P. Moqvist and T. M. Aulin, "Serially concatenated continuous phase modulation with iterative decoding," in *IEEE Trans. Commun.*, vol. 49, no. 11, 2001, pp. 1901–1915.
- [12] N. Ibrahim, "Bluetooth receiver design based on laurent's decomposition," Master's thesis, The American University of Beirut, 2005.
- [13] J. Hagenauer, "The exit chart-introduction to extrinsic information transfer in iterative processing," in *Proc. 12th European Signal Processing Conference (EUSIPCO)*, 2004, pp. 1541–1548.
- [14] T. Benaddi, C. Poulliat, M.-L. Boucheret, B. Gadat, and G. Lesthievant, "Design of unstructured and protograph-based ldpc coded continuous phase modulation," in *2014 IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 1982–1986.
- [15] R. G. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.