Quelques Résultats sur les Codes LDPC Hybrides

Lucile Sassatelli, David Declercq

ETIS - ENSEA/UCP/CNRS UMR-8051 95014 Cergy, FRANCE
sassatelli@ensea.fr,declercq@ensea.fr

Résumé − Ce papier rassemble quelques résultats sur une nouvelle classe très générale de codes LDPC, nommés codes LDPC hybrides. Les symboles d'un mot de code LDPC hybride appartiennent à des ensembles finis d'ordres différents. On peut ainsi contrôler conjointement le couple (densité de branche, taille des symboles). Le condition de stabilité exposée dans ce papier permet d'identifier un avantage des codes LDPC hybrides sur les codes LDPC classique binaires et non-binaires. Une analyse de l'évolution de l'information mutuelle est menée, sous approximation gaussienne, en vue de concevoir de bons codes LDPC hybrides. Grâce au fait que l'on peut inclure des contraintes de taille finie dans l'optimisation, les simulations à tailles finies montrent que nos codes représentent un compromis intéressant entre bonnes performances en convergence et en plancher d'erreur. En particulier, pour un rendement de 1/6, le code LDPC hybride optimisé bat les meilleurs codes connus.

Abstract − In this paper, some results on a very general class of LDPC codes are gathered. The hybrid LDPC codeword symbols belong to different order finite sets. That is why we can jointly control the couple (edge density,symbol size). Thanks to the stability condition given in this paper, we identify an advantage of hybrid LDPC codes over classical binary and non-binary LDPC codes. Information content evolution is analysed using a Gaussian approximation, in order to efficiently design hybrid LDPC codes. Some finite length constraints can be included in the asymptotic optimization, leading to good trade-off between convergence and error floor. In particular, for code rate 1/6, the optimized hybrid LDPC code is better than the best known codes.

1 Introduction

Comme les Turbo Codes, les codes LDPC sont des codes pseudo-aléatoires approchant la capacité du canal. Les codes LDPC binaires ont été redécouverts par MacKay, et la forme non-binaire ensuite étudiée par Davey [1]. L'intérêt des codes LDPC non-binaires, par rapport aux binaires, apparaît pour des trames courtes ou des modulations d'ordre élevé [2, 3, 4]. Cependant, les bons codes LDPC non-binaires à taille finie sont "ultra-creux", et ont donc des seuils de convergence dégradés par rapport aux codes LDPC binaires. L'intérêt des codes LDPC hybrides repose sur la combinaison des avantages des familles de codes LDPC binaires et non-binaires. Ce compromis est réalisé par le mélange de symboles de différents ordres au sein d'un même mot de code. D'où l'appelation de codes hybrides. Ce papier rassemble les résultats obtenus jusqu'ici, concernant notamment l'étude asymptotique.
La première partie souligne la généralité de la structure de ces nouveaux codes. Dans la deuxième section, le contexte de l'étude est présenté, et les propriétés importantes de symétrie et invariance par application linéaire sont exposées. La troisième section concerne la condition de stabilité et une illustration, et la quatrième l'analyse de type EXIT chart des codes hybrides en vue de leur optimisation, ainsi que les résultats montrant l'intérêt des cette nouvelle famille très générale de codes LDPC.

2 Classe des Codes LDPC Hybrides

Un code LDPC hybride est un code LDPC dont les noeuds de variable appartiennent à des ensembles finis d'ordres différents. Un tel code n'est pas défini sur un corps, mais sur le groupe produit des différents groupes auxquels appartiennent les noeuds de donnée $G(q_{min}) \times \cdots \times G(q_{max})$. On ne considère que des groupes dont le cardinal q_k est une puissance de 2, c'est-à-dire des groupes du type $G(q_k) = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{p_k}$ avec $p_k = \log_2(q_k)$. Les codes définis dans un groupe produit ont la particularité d'être linéaires dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$, mais peuvent être non-linéaires dans $G(q_{min}) \times \cdots \times G(q_{max})$. Pour des raisons d'encodage, on limite l'étude aux codes LDPC hybrides qui sont linéaires dans leur groupe produit, on ne considère que des matrices de parité triangulaires supérieures, et un arrangement spécifique des ordres des symboles du mot de code (figure 1). Il est possible de généraliser le décodeur par propagation de croyance aux codes hybrides, et d'en dériver une version rapide utilisant des FFT [5]. Un élément h_{ij} non-nul de la matrice de parité d'un code hybride est une application liant une ligne dans $G(q_l)$ à une colonne dans $G(q_k)$. Dans ce travail, on ne considère que les codes LDPC hybrides dont les éléments non-nuls de la matrice de parité sont des applications linéaires de rang plein.

3 Définitions et Propriétés

Définissons l'utilisation des applications linéaires constituant la matrice de parité. Soient deux groupes $G(q_1)$ et $G(q_2)$. On a respectivement $G(q_1) = \{\alpha_0, \ldots, \alpha_{q_1-1}\}$ et $G(q_2) = \{\alpha'_0, \ldots, \alpha'_{q_2-1}\}$. L'image de l'application linéaire A de $G(q_1)$ vers $G(q_2)$ est notée $\mathrm{Im}(A)$ et définie par $\mathrm{Im}(A) = \{\alpha'_j \in G(q_2) | \exists i \in [0, q_1 - 1] : A(\alpha_i) = \alpha'_j\}$.

Definition 1 *L'extension du vecteur de probabilité* $\mathbf{x}$ *par*

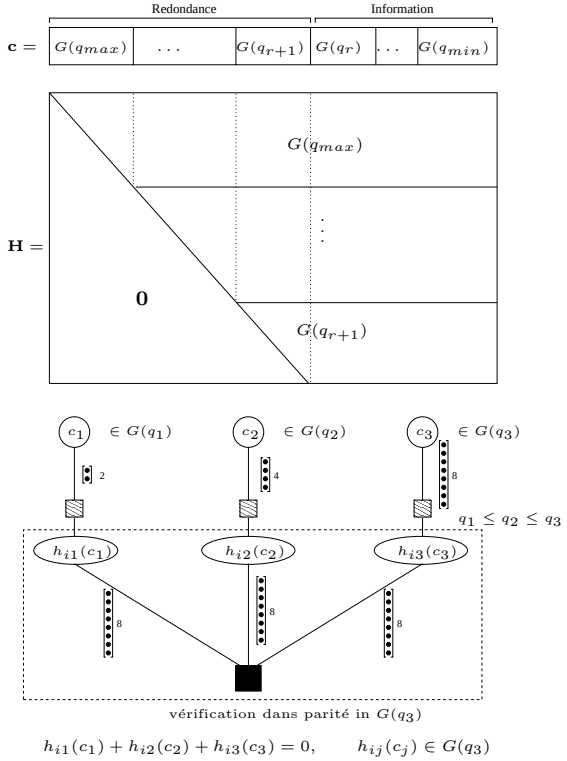

FIG. 1 – Figure du haut : Mot de code et matrice de vérification de parité hybrides. Figure du bas : Noeud de parité d'un code LDPC hybride.

l'application linéaire A est notée $\mathbf{y} = \mathbf{x}^{\times A}$ et définie, $\forall j \in [0, q_2 - 1]$, par :

$$\begin{aligned} &\text{si } \alpha'_j \notin Im(A), \quad y_j = 0 \\ &\text{si } \alpha'_j \in Im(A), \quad y_j = x_i \text{ avec } i \text{ tel que } A(\alpha_i) = \alpha'_j \end{aligned}$$

Definition 2 *Le tronqué du vecteur de probabilité $\mathbf{y}$ par A est noté $\mathbf{x} = \mathbf{y}^{\times A^{-1}}$ et défini, $\forall i \in [0, q_1 - 1]$,par :*

$$x_i = y_j \text{ avec } j \text{ tel que } \alpha'_j = A(\alpha_i)$$

Soit un vecteur $\mathbf{x}$ de probabilités de taille q, les composantes du vecteur $\mathbf{w}$, rapport logarithmique de densités (LDR) qui lui est associé, sont définies par $w_i = \log\left(\frac{x_0}{x_i}\right)$, $\forall i \in [0, q-1]$. En sortie du canal, les messages LDR sont en fait des rapports logarithmiques de vraisemblances (LLR). Une famille de codes LDPC hybrides est paramétrée par $\pi(i, j, k, l)$ qui est la proportion de branches liant un noeud de donnée de degré i dans $G(q_k)$ à un noeud de parité de degré j dans $G(q_l)$. Les codes LDPC hybrides ont donc une paramétrisation très riche puisque l'espace des paramètres a quatre dimensions.
Le canal de transmission est supposé être sans mémoire, symétrique et à entrée binaire. On appelle v un symbole d'un mot de code transmis.

Definition 3 *Un message LDR est symétrique si et seulement si*

$$\forall a \in G(q), \quad P(\mathbf{W} = \mathbf{w}|v = a) = e^{-w_a} P(\mathbf{W} = \mathbf{w}|v = 0)$$

De la même façon, un canal est symétrique si et seulement si les LLR observés en sortie sont symétriques. La condition de symétrie est essentielle à l'étude asymptotique des familles de codes hybrides puisqu'elle assure que la probabilité d'erreur est indépendante du mot de code émis :

Lemma 1 *La probabilités d'erreur d'un code d'une famille hybride, sur un canal symétrique, est indépendante du mot de code émis.*

On montre que

Lemma 2 *Si $\mathbf{W}$ est un vecteur aléatoire LDR symétrique, alors son extension $\mathbf{W}^{\times A}$, par n'importe quelle application linéaire A de rang plein, est aussi symétrique. Le tronqué $\mathbf{W}^{\times A^{-1}}$ est également symétrique.*

Par manque de place, les démonstrations n'apparaîtront que dans une prochaine publication. Comme la spécificité des codes LDPC hybrides réside dans les noeuds de fonctions sur les branches du graphe factoriel (figure 1) et qu'ils sont décodés avec l'algorithme de propagation de croyance (BP) habituel, les passages par les noeuds de données et de parités sont inchangés par rapport aux codes LDPC classiques. Ces étapes de décodage conservant la symétrie [6], le lemme 2 assure alors que le décodeur BP hybride conserve la symétrie des messages circulant sur les branches au cours du décodage.

Nous introduisons maintenant une propriété spécifique aux familles de codes hybrides : l'invariance par application linéaire (ou LA-invariance), qui permet notamment, alliée à la symétrie, de caractériser la densité d'un vecteur message par un scalaire. Soit E l'ensemble des applications linéaires injectives d'un groupe donné vers un autre.

Definition 4 *Le vecteur aléatoire de probabilités $\mathbf{Y}$ est LA-invariant si et seulement si pour tout $(A, B) \in E \times E$, les vecteurs aléatoires de probabilités $\mathbf{Y}^{\times A^{-1}}$ et $\mathbf{Y}^{\times B^{-1}}$ sont identiquement distribués.*

Le lemme qui suit permet la projection sur un scalaire des densités des messages du décodeur.

Lemma 3 *Si un vecteur aléatoire de probabilités $\mathbf{Y}$ de taille q_2 est LA-invariant, alors pour tout $(i, j) \in G(q_2) \times G(q_2)$, les variables aléatoires Y_i and Y_j sont identiquement distribués.*

Voyons maintenant les hypothèses à faire pour considérer les messages du décodeur LA-invariants.

Definition 5 *Soit $\mathbf{X}$ un vecteur aléatoire de probabilités de taille q_1, on définit l'extension aléatoire de taille q_2 de $\mathbf{X}$, notée $\tilde{\mathbf{X}}$, par le vecteur aléatoire de probabilités $\mathbf{X}^{\times A}$, où A est uniformément choisi dans E et indépendant de $\mathbf{X}$.*

On a alors le résultat clé :

Lemma 4 *Un vecteur aléatoire de probabilités $\mathbf{Y}$ est LA-invariant si et seulement si il existe un vecteur aléatoire de probabilités $\mathbf{X}$ tel que $\mathbf{Y} = \tilde{\mathbf{X}}$.*

On étudie donc des familles de codes LDPC hybrides dont les applications linéaires on été choisies suivant une loi uniforme, et ainsi on peut considérer LA-invariants certains

des messages circulant sur le graphe au cours du décodage. Ainsi, pour pouvoir obtenir une condition de stabilité du décodeur et projeter les densités des messages sur un scalaire, on choisit d'étudier des familles hybrides définies par $\pi(i,j,k,l)$ et constituées des codes tels que les éléments non-nuls de la matrice de parité soient choisis uniformément dans E.

4 Condition de Stabilité

Introduite dans [6], la condition de stabilité est une condition nécessaire et suffisante pour que la probabilité d'erreur ne soit pas bornée par une constante strictement positive lorsque le nombre d'itérations tend vers l'infini, sachant qu'elle a déjà décru sous une certaine valeur à une itération donnée.
Soit une famille de codes LDPC hybrides définie par $\pi(i,j,k,l)$. On définit un paramètre Ω, propre à la famille, de la façon suivante :

$$\Omega = \sum_{j,k,l} \pi(i=2,k,j,l)\frac{q_k-1}{q_l-1}(j-1)$$

Soit un canal symétrique sans mémoire, de probabilités de transition $p(y|x)$. On définit le paramètre suivant, propre au canal et à la famille :

$$\Delta = \sum_{k,l} \pi(k,l)\frac{1}{q_l-1}\sum_{i=1}^{q_k-1}\int \sqrt{p(y|\delta(i))p(y|\delta(0))}dy$$

Grâce aux propriétés de symétrie et de LA-invariance, on peut montrer le théorème suivant.

Theorem 1 *La probabilité d'erreur des codes de la famille définie par $\pi(i,j,k,l)$, converge vers zéro si et seulement si $\Omega\Delta < 1$.*

Ce théorème démontre que s'il existe un point fixe du décodage d'une famille de codes LDPC hybrides, alors ce point peut être stable sous certaines conditions. Les codes LDPC hybrides ont donc un comportement à seuil. La première remarque est que pour un code LDPC non-binaire classique sur $GF(q)$ sur canal gaussien à entré binaire (BI-AWGN) avec une variance de bruit de σ^2, la condition de stabilité hybride revient à la condition de stabilité non-binaire présentée dans [4] :

$$\begin{aligned}\Omega_{nb} &= \rho'(1)\lambda'(0)\\ \Delta_{nb} &= \frac{1}{q-1}\sum_{i=1}^{q-1} exp(-\frac{1}{2\sigma^2}n_i) \qquad (1)\end{aligned}$$

où n_i est le nombre de 1 dans le représentation binaire de $\alpha_i \in GF(q)$. On montre facilement que Δ tend vers zéro quand q tend vers l'infini. Ceci signifie que sur canal BI-AWGN, n'importe quel point fixe de l'évolution de densité est stable quand q tend vers l'infini.
La deuxième remarque concerne la comparaison entre conditions de stabilité hybride et non-hybride. Sur la figure 2, on considère deux codes de rendements un demi. Le premier est un code LDPC de connectivité $(d_v = 2, d_c = 4)$ sur $GF(q)$, le deuxième est un code LDPC hybride sur $G(q) - G(2)$ avec $d_v = 2$, q variant entre 2 et 256. On considère un canal BI-AWGN avec une variance de 1. En notant Ω_{hyb} et Δ_{hyb} les paramètres de la famille hybride pour les distinguer de ceux de la famille classique, on observe sur la figure 2 que $\Omega_{hyb} < \Omega_{nb}$ et $\Delta_{hyb} < \Delta_{nb}$. Ceci signifie qu'avec un tel canal et de tels codes, un point fixe de l'évolution de densité peut être stable à plus faible rapport signal à bruit pour un code LDPC hybride que pour les codes LDPC classiques, ce qui est un avantage pour les codes LDPC hybrides.

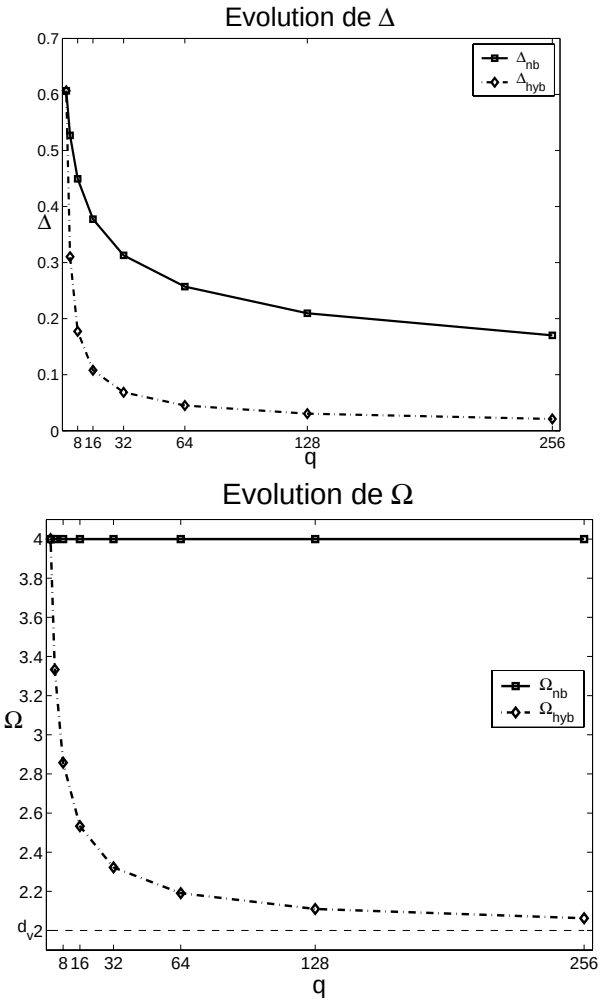

FIG. 2 – Paramètres Δ et Ω pour un code hybride et un code non-hybride en fonction de l'ordre maximum q des symboles.

5 Optimisation et Résultats

La projection des densités des messages circulant sur le graphe lors du décodage, sur un paramètre scalaire, se fait grâce aux propriétés précédentes. On suit ainsi l'évolution de l'information mutuelle par l'équation (2), pour le canal BI-AWGN [7]. $x_{vc}^{(t+1)}$ représente l'information mutuelle moyenne d'un message sortant d'un noeud de variable à l'itération $t+1$, tandis que $x_{cv,k}^{(j,l')(t)}$ représente l'information mutuelle d'un message sortant d'un noeud de parité de degré j dans $G(q_{l'})$ et tronqué dans $G(q_k)$. L'optimisation par EXIT chart [8] sous différentes contraintes, no-

$$x_{cv,k}^{(j,l')^{(t)}} = J_c\left(J_c^{-1}\left(1-J_c\left((j-1)J_c^{-1}(1-x_{vc}^{(t)},q_{l'}),q_{l'}\right),q_{l'}\right),q_k\right)$$

$$x_{vc}^{(t+1)} = \sum_{i,k}\pi(i,k)\sum_{l}\pi(l|i,k)\left(1-\frac{log(q_k)}{log(q_l)}\left(1-J_v\left(\mathbf{m}_{sc}^{q_k}+(i-1)J_c^{-1}(\sum_{j,l'}\pi(j,l'|i,k)x_{cv,k}^{(j,l')^{(t)}},q_k)\mathbf{1}_{q_k-1},q_k\right)\right)\right) \quad (2)$$

tamment celle de stabilité, se fait par programmation linéaire. Un gros avantage des codes LDPC hybrides, grâce à la paramétrisation par $\pi(i,j,k,l)$, est de pouvoir contrôler les densités locales de la matrice de parité et la taille des symboles dans chaque zone. Ceci, contrairement aux codes LDPC habituels, permet d'inclure directement des contraintes de taille finie dans l'optimisation sur critères asymptotiques. Ainsi, alors qu'habituellement on optimise une famille sur critères asymptotiques pour ensuite aller choisir à l'intérieur un code de taille finie ayant de bonnes propriétés, ici on peut, en un sens, choisir une famille avec de bonnes propriétés asymptotiques à l'intérieur d'une plus grande famille avec de bonne propriétés, prédéfinies, à taille finie.

Dans le premier exemple, on optimise le profil de connection d'un code LDPC hybride sur $G(8)-G(2)$. Les bits d'information sont tous rassemblés dans des symboles sur $G(2)$, tandis que ceux de redondance sont regroupés dans des symboles sur $G(8)$. Pour abaisser le plancher d'erreur, on introduit des contraintes de taille finie dans l'optimisation : les degrés 2 sont interdits sur les noeuds dans $G(2)$ pour éviter l'apparition de trapping sets catastrophiques durant la construction du code de taille finie. Pour avoir le graphe le plus creux possible dans la partie sur $G(8)$, on y fixe la connectivité à 2. Les résultats de la figure 3 montrent que pour un rendement 1/2, le code hybride correspond au compromis attendu entre bon seuil de convergence, habituellement associé aux codes irréguliers, et bon plancher d'erreur, habituellement associé aux codes plus creux.

Dans le deuxième exemple est optimisé, pour un rendement de 1/6, le profil d'ordre de groupe d'un code LDPC hybride dont le profil de connection est fixé à $(d_v=2,d_c=3)$. La figure 3 montre que le code hybride obtenu a les meilleures performances, battant le meilleur code de rendement 1/6 présenté dans la littérature [9].

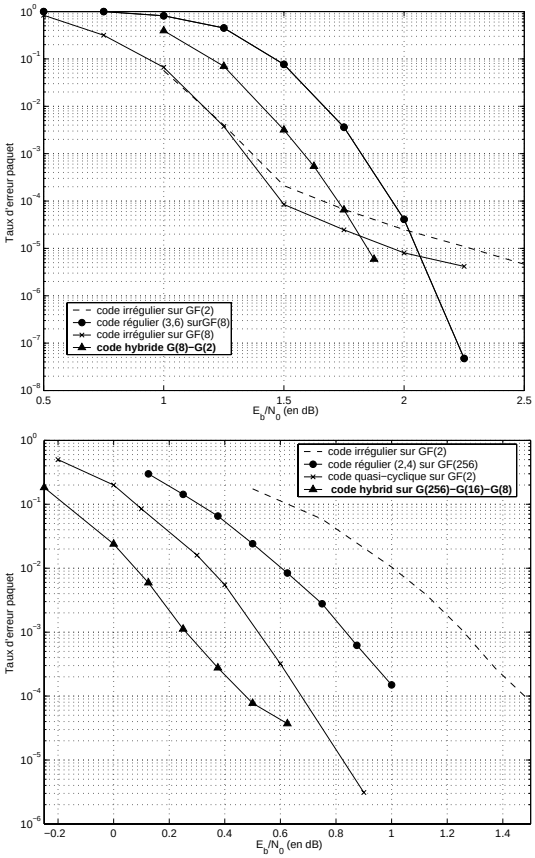

FIG. 3 – Comparaisons des taux d'erreur paquet de codes hybrides avec d'autres bons codes. Nombre maximum d'itérations fixé à 500. Figure du haut : $R=1/2$, $N_{bit}=3008$. Figure du bas : $R=1/6$, $N_{bit}=6144$

Références

[1] M. Davey and D. MacKay, "Low density parity check codes over GF(q)," *IEEE Trans. Commun.*, vol. 2, pp. 165–167, June 1998.

[2] X.-Y. Hu and E. Eleftheriou, "Binary representation of cycle Tanner-graph GF(2^q) codes," in *Proc. of IEEE Intern. Conf. on Comm.*, pp. 528–532, June 2004.

[3] M. F. C. Poulliat and D. Declercq, "Using binary image of nonbinary LDPC codes to improve overall performance," in *Proc. of IEEE Intern. Symp. on Turbo Codes*, Apr. 2006.

[4] A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 52, pp. 549–583, Feb. 2006.

[5] G. G. A. Goupil, M. Colas and D. Declercq, "FFT-based bp decoding of general LDPC codes over abelian groups," *IEEE Trans. Commun.*, vol. 55, pp. 644–649, Apr. 2007.

[6] A. S. T.J. Richardson and R. Urbanke, "Design of capacity-approaching irregular LDPC codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 619–637, Feb. 2001.

[7] L. Sassatelli and D. Declercq, "Non-binary hybrid LDPC codes : Structure, decoding and optimization," in *Proc. of IEEE Inform. Theory Workshop*, Oct. 2006.

[8] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, pp. 1727–1737, Oct. 2001.

[9] W. R. G. Liva and M. Chiani, "Design of quasi-cyclic Tanner codes with low error floors," in *Proc. of IEEE Intern. Symp. on Turbo Codes*, Apr. 2006.