Analyse asymptotique et conception robuste de codes Raptor pour le décodage conjoint

Auguste VENKIAH[1], Charly POULLIAT[1], David DECLERCQ[1]

ETIS, CNRS UMR 8051
6 av du Ponceau, 95014 Cergy Pontoise Cedex, France
venkiah@ensea.fr, poulliat@ensea.fr, declercq@ensea.f

Résumé – Dans cet article, nous nous intéressons au décodage conjoint de codes Raptor sur canal à bruit additif blanc gaussien (BABG). Les codes Raptor sont des codes fontaine sans rendement, ayant la propriété d'être universels sur le canal binaire à effacements, dans le sens où ils atteignent la capacité du canal indépendamment du taux d'effacement. Nous utilisons une analyse asymptotique sous approximation gaussienne du décodeur itératif, pour montrer que, bien qu'il ait été prouvé qu'ils ne sont pas universels au sens strict sur le canal gaussien, les codes Raptor s'avèrent cependant efficaces sur une grande plage de RSB grâce au décodage conjoint.

Abstract – In this paper, we consider the joint decoding of Raptor codes on a binary input additive white Gaussian noise channel. Raptor codes are rateless fountain codes that have the attractive property of being universal on the binary erasure channel: they can approach arbitrarily close the capacity, independently of the channel parameter. It has been recently shown that Raptor codes are not universal on other symmetric channels than the erasure channel. We use an analytical asymptotic analysis under Gaussian approximation to characterize the joint iterative decoder and we show that Raptor codes designed for a channel parameter performs reasonnably well under joint decoding for a very large range of channel parameters.

1 Introduction

Sur un réseau tel qu'Internet, la fiabilité des transmissions repose sur l'utilisation de protocoles tels que TCP, où le récepteur accuse réception de chacun des paquets. Cette stratégie peut poser plusieurs problèmes pratiques : d'une part, elle suppose la présence d'un canal de retour, et d'autre part, elle est largement inefficace dans le cadre d'applications multicast, particulièrement lorsque le nombre d'utilisateurs est très élevé, auquel cas le réseau peut être saturé par les acquittements et retransmissions de paquets perdus.

Une transmission sur un réseau tel qu'Internet peut être modélisée par un canal binaire à effacements (CBE). Dans ce cadre, il existe plusieurs solutions en codage de canal permettent de recouvrir des effacements d'un canal. Ces solutions classiques, qui sont basées sur l'utilisation de codes bloc correcteurs d'erreurs, s'avèrent inefficaces dans le cadre d'applications multicast. En effet dans ce cas, chaque utilisateur voit un canal de transmission différent, et le rendement du code bloc doit alors être dimensionné pour le plus mauvais canal parmi tous les utilisateurs, ce qui pénalise les utilisateurs ayant un bon canal.

Les codes fontaine sont une famille de codes *sans rendement* : des symboles de parité sont émis de façon ininterrompue, ce qui justifie par ailleurs le qualificatif *fontaine*. Ils ont été introduits pour transmettre efficacement sur un canal à effacement [1], et ne supposent ni la connaissance du paramètre du canal, ni l'utilisation d'un canal de retour. Les codes LT, introduits par Luby dans [2] sont les premiers codes fontaine efficaces. Ils atteignent asymptotiquement la capacité du CBE [2, 3], mais au prix d'une complexité d'encodage et de décodage croissant en $O(K\log(K))$, K étant la taille du message à transmettre, ce qui est trop contraignant pour une implantation matérielle. Les codes Raptor sont une extension des codes LT introduits par Shokrollahi dans [3], et sont construits en concaténant un code LT et un code interne appelé "précode" qui est un code bloc correcteur d'erreur. Celui-ci permet de relâcher des contraintes pour l'optimisation du code LT, et ainsi de se ramener à une complexité d'encodage et de décodage linéaires en la taille du mot de code.

Une propriété fondamentale qui a fait le succès des codes LT et Raptor sur le CBE est qu'ils sont "universels", dans le sens où ils atteignent asymptotiquement la capacité d'un canal à effacement quelque soit le taux d'erreur associé ; leur optimisation pour le CBE ne dépend pas du taux d'effacement du canal. Cela est dû au fait que le graphe de Tanner à la réception est construit uniquement à partir des symboles reçus. Cette propriété n'est plus valable pour des canaux bruités symétriques quelconques, ce qui constitue l'un des résultats principaux de [4].

Dans les approches existant dans la littérature, les deux codes constituants d'un code Raptor sont décodés séquentiellement. Dans [5], nous avons proposé et étudié le décodage conjoint de la fontaine et du précode. Pour cela, nous avons développé une analyse asymptotique sous approximation gaussienne du décodeur conjoint sur canal BABG, proposé une méthode d'optimisation, et montré que les codes ainsi optimisés pour le décodage conjoint opèrent plus proche de la capacité que dans le cas du décodage séparé.

Ici, nous prolongeons notre étude sur le décodage conjoint ; plus particulièrement, les apports originaux de ce papier sont les suivants : bien que les codes Raptor ne soient pas universels sur d'autres canaux que le CBE, nous montrons qu'ils sont efficaces sur une large plage de RSB sur le canal BABG. Ceci est un point très important, car le succès des codes Raptor sur

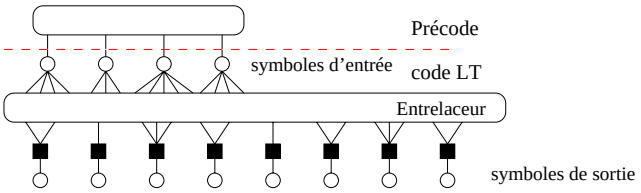

FIG. 1 – Graphe de Tanner d'un code Raptor. Les carrés représentent des noeuds de parité et les cercles représentent des noeuds de données.

le CBE est essentiellement dû à leur caractère universel. Pour cela, nous montrons d'abord que les codes Raptor ont un comportement à seuil.

2 Notations

On appelle *symboles d'entrée* les symboles d'information à transmettre, et *symboles de sortie* les symboles de redondance produits par la fontaine. Un code LT est complètement caractérisé par sa *distribution des degrés* (DD) : pour générer un symbole de sortie, on tire au sort un *degré* d suivant cette distribution ; le symbole de sortie est alors la somme modulo 2 de d symboles d'entrée tirés aléatoirement et uniformément parmi les K symboles d'information. Ainsi, les d symboles d'entrée et le symbole de sortie vérifient une équation de parité.

Soit $\Omega_1, \Omega_2, \ldots, \Omega_{d_c}$ une distribution sur $1, 2, \ldots, d_c$ telle que Ω_d soit la probabilité de tirer un degré d. La DD est représentée par son polynôme générateur $\Omega(x) = \sum_{i=1}^{d_c} \Omega_i x^i$. A cette distribution, on peut associer la DD de branches suivante : $\omega(x) = \sum_{i=1}^{d_c} \omega_i x^{i-1} = \Omega'(x)/\Omega'(1)$.

Les symboles d'entrée étant choisis uniformément à chaque génération de symbole de sortie, leur DD est binomiale, et peut être approximée par une loi de Poisson de paramètre α : $I(x) = e^{\alpha(x-1)}$ [3]. La distribution de branches associée est alors : $\iota(x) = \sum_{i=1}^{d_v} \iota_i x^{i-1} = I'(x)/I'(1)$ et vaut également $e^{\alpha(x-1)}$. Les deux distributions sont de moyenne α.

Un code Raptor est construit en concaténant un code LT avec un code interne appelé "précode", qui est un code bloc correcteur d'erreur de fort rendement.

On note $f_0 \triangleq J^{-1}\big(1 - J\big(\frac{2}{\sigma^2}\big)\big)$ Le rendement *a posteriori* d'un code fontaine est défini par : $R = \frac{\Omega'(1)}{\alpha}$. Pour une capacité de canal donnée, ce rendement est associé à un *overhead*, qui représente l'écart à la capacité : $C = (1+\epsilon)R$.

3 Analyse asymptotique du décodeur conjoint et optimisation pour le canal gaussien

Notre analyse repose sur l'étude asymptotique de l'évolution de l'information mutuelle (IM), sous approximation gaussienne proposée dans [5]. Contrairement à [4], l'étude asymptotique et l'optimisation de DD associée que nous proposons sont toutes deux analytiques, ce qui est un avantage important en termes de robustesse et de rapidité d'optimisation.

3.1 Analyse du décodeur

Les messages sur le graphe de Tanner d'un code Raptor sont les "log density ratios" (LDR) des probabilités. Ces messages sont modélisés par une variable aléatoire suivant une loi normale, de moyenne m et de variance $\sigma^2 = 2m$, définissant une densité dite *symétrique* [6]. Pour de tels messages, l'information mutuelle associée à ces messages vaut $x = J(m)$ [7], où la fonction $J(.)$ est définie par :

$$J(m) = 1 - \frac{1}{\sqrt{4\pi m}} \int_R \log_2(1+e^{-\nu}) \exp\left(-\frac{(\nu-m)^2}{4m}\right) d\nu \tag{1}$$

On note $x_u^{(l)}$ (resp. $x_v^{(l)}$) l'IM sur une branche reliant un noeud de parité à un symbole d'entrée (resp. symbole d'entrée à noeud de parité) à l'itération l de décodage. On note alors $x_{\text{ext}}^{(l)}$ l'IM passée de la fontaine vers le précode à l'itération l. Soit $T : x \mapsto T(x)$ la fonction de transfert du précode décrivant le transfert d'information mutuelle du précode vers la fontaine. L'information fournie par le précode au code LT vaut alors $T(x_{\text{ext}}^{(l)})$ Pour l'optimisation, on supposera que la fonction T est connue, sous forme numérique ou analytique. Dans le cas d'un précode LDPC décrit par les polynômes $\lambda(x)$ et $\rho(x)$, la fonction T peut être exprimée de façon analytique :

$$T(x) = \sum_{i=2}^{d_v} \tilde{\lambda}_i J\left(iJ^{-1}\Big(1 - \sum_{j=2}^{d_c} \rho_j J\big((j-1)J^{-1}(1-x)\big)\Big)\right) \tag{2}$$

L'équation (3) décrit l'évolution de l'IM au cours des itérations de décodage : $x_u^{(l)} = F(x_u^{(l-1)}, \sigma^2)$. L'étude de ce système dynamique donne les deux résultats suivants qui sont nécessaires pour poser le problème d'optimisation :

Proposition 1 (Condition de démarrage) *Le décodage peut commencer ssi $F(0,\sigma^2) > 0$ et l'on a l'équivalence suivante :*

$$F(0,\sigma^2) > \varepsilon \quad \Longleftrightarrow \quad \omega_1 > \frac{\varepsilon}{J\big(\frac{2}{\sigma^2}\big)} \tag{4}$$

Ainsi, la condition de démarrage se traduit par présence de termes de degré 1 dans la DD ; le paramètre ε apparaît alors comme un paramètre permettant de contraindre le problème d'optimisation.

Par ailleurs, pour une distribution atteignant la capacité d'un canal gaussien, on doit avoir $F'(0,\sigma^2) > 1$. Cela peut se traduire par une condition sur la proportion de branches de degré 2, ce qui fait l'objet de la proposition suivante.

Proposition 2 *On a l'équivalence suivante :*

$$F'(0,\sigma^2) > 1 \Longleftrightarrow \omega_2 > \frac{1}{(\alpha-1)e^{-f_0/4}} \tag{5}$$

Cette condition est analogue à la condition de stabilité d'un code LDPC. En effet, la condition de stabilité d'un code LDPC assure que le point fixe $x = 1$ est un point fixe stable du décodeur BP, c'est à dire que lorsque l'information mutuelle est suffisamment proche de 1, alors le décodeur converge effectivement vers 1. Dans notre cas, la condition assure que le point fixe $x = 0$ d'un code Raptor atteignant la capacité est un point fixe instable, c'est à dire que dès que le décodage a commencé, alors la convergence continue.

$$x_u^{(l)} = F(x_u^{(l-1)}, \sigma^2) = 1 - \sum_{j=1}^{d_v} \omega_j J\Big((j-1) J^{-1}\Big(1 - \sum_{i=1}^{d_c} \iota_i J\big((i-1)J^{-1}(x_u^{(l-1)}) + J^{-1}\big(T(x_{ext}^{(l-1)})\big)\big)\Big) + f_0 \Big) \qquad (3)$$

La borne inférieure sur les degrés deux contient un terme f_0 qui dépend du paramètre du canal. Dans [4], une borne similaire est dérivée pour Ω_2, et de plus il est prouvé que dans le cas d'un code atteignant la capacité, la borne doit être atteinte.

3.2 Optimisation de distributions

Il est facile de montrer que $\lim_{x\to 1} F(x) = J(2/\sigma^2) \triangleq x_0$, et $x \mapsto F(x)$ étant une fonction croissante, on en déduit que $F(x) < x_0 \quad \forall x \in [0;1]$, ce qui signifie que le point fixe du système dynamique décrit par (3) est inférieur à x_0. L'équation (3) étant linéaire en les coefficients ω_i de la distribution $\omega(x)$ L'optimisation de celle-ci peut alors être formulée de la manière suivante [5] :

$$\omega_{opt}(x) \quad = \quad \arg\min_{\omega(x)} \sum_j \frac{\omega_j}{j} \qquad (6)$$

sous les contraintes :
[C_1] $\sum_i \omega_i = 1$
[C_2] $F(x, \sigma^2) > x \quad \forall x \in [0; x_0 - \delta]$ pour $\delta > 0$
[C_3] $F(0, \sigma^2) > \varepsilon$ pour $\varepsilon > 0$
[C_4] $F'(0, \sigma^2) > 1$
où [C_1] est la contrainte de proportion, [C_2] est la contrainte de convergence, [C_3] est la contrainte de démarrage, et [C_4] l'analogue de la contrainte de stabilité pour les codes LDPC.

4 Robustesse des codes Raptor sous décodage conjoint

4.1 Seuil d'un code Raptor

Dans cette section, nous montrons qu'un code Raptor possède un seuil. Pour cela, nous distinguons deux phases lors du décodage d'un code Raptor. Durant la première phase, le code LT converge vers son point fixe, et la convergence est assurée grâce la contrainte d'optimisation [C_3]. Durant la deuxième phase, le décodage du code LT a atteint son point fixe, et l'information extrinsèque fournie par le code LT sert d'information *a priori* pour le précode qui converge à son tour.

Le précode étant un code LDPC à seuil, l'on peut distinguer deux cas : l'information extrinsèque fournie par le code LT est supérieur au seuil du précode, auquel cas le décodeur converge, ou bien celle-ci est inférieure au seuil du précode, auquel cas le décodage du code Raptor échoue.

Or l'information extrinsèque passée du code LT au précode est une fonction croissante de l'overhead. Il en résulte que si le précode est un code correcteur d'erreur à seuil, ce qui est le cas des codes LDPC, alors le code Raptor possède également un comportement à seuil.

Définition 1 *On appelle seuil d'un code Raptor l'overhead ϵ^* l'espérance de l'overhead du code. Pour un code de taille infinie, et pour un nombre d'itérations infini, le décodage d'un code Raptor réussit ssi $\epsilon > \epsilon^*$*

L'estimation du seuil d'un code Raptor peut se faire grâce à une technique appelée *évolution de densité*. L'évolution de densité consiste à suivre la densité réelle des messages sur le graphe de décodage, sans projeter ceux-ci sur une densité gaussienne, comme c'est le cas dans une analyse asymptotique analytique telle que l'évolution de l'information mutuelle. Numériquement, l'évolution de densité est implantée en décodant une version bruitée du mot de code nul [1] , et en procédant à chaque itération à une permutation aléatoire des branches du graphe de Tanner, ainsi qu'à une nouvelle réalisation de bruit sur le canal. Les permutation aléatoires permettent de casser les corrélations des messages et de simuler ainsi un graphe infini, tandis que les nouveaux tirages de bruit permettent de "gaussianiser" la densité du bruit. Lorsque le décodage réussit, l'overhead est diminué, et lorsqu'il échoue, l'overhead est augmenté. En procédant par dichotomie, il est ainsi possible de calculer l'overhead seuil d'un code Raptor.

4.2 Région des capacités atteignables

L'un des résultats principaux de [4] est qu'il n'existe pas de codes Raptor *universels*. En effet, pour un code approchant la capacité, la proportion Ω_2 de symboles de sortie de degré 2 tend vers une quantité qui dépend du paramètre de canal, sauf dans le cas particulier du CBE ; la proportion Ω_2 d'un code Raptor atteignant la capacité un CBE est $\Omega_2 = 0.5$, quelque soit le taux d'effacement du canal. Il est ainsi possible d'optimiser des distributions qui atteignent asymptotiquement la capacité du CBE pour toute valeur du taux d'effacement.

En revanche, un code Raptor ne peut pas s'approcher arbitrairement proche de la capacité d'un canal indépendamment du paramètre de canal sur un canal symétrique sans mémoire autre que le CBE, et pour chaque canal, il faut donc optimiser une nouvelle distribution. Nous allons néanmoins montrer que, malgré ce résultat théorique fort, un codes Raptor optimisé pour une capacité donnée se comporte bien sur un canal de capacité différente. Pour cela, il est possible d'utiliser des calculs de seuil, comme cela est décrit dans la section précédente.

Nous avons optimisé une distribution pour le décodage conjoint avec un précode LDPC régulier de rendement $R = 0.95$, sur un canal BABG de capacité $C = 0.8$. Les seuils de ce code ont ensuite été calculés pour des canaux BABG de différentes capacités, c'est à dire pour différentes valeures de E_s/N_o. Le seuil ainsi calculés correspondant à un rendement du code, il est alors possible de tracer la région des capacités atteignables par le code. Les résultats sont présentés sur la figure 2, et montrent que le code Raptor optimisé pour un bon canal $(C = 0.8)$ se comporte bien également sur des canaux très bruités.

5 Conclusion

Sur un canal à effacement les codes Raptor atteignent asymptotiquement la capacité indépendamment du taux d'effacement, ce qui justifie l'engouement récent pour cette famille de code.

[1] Ceci est possible car un code Raptor est un code linéaire.

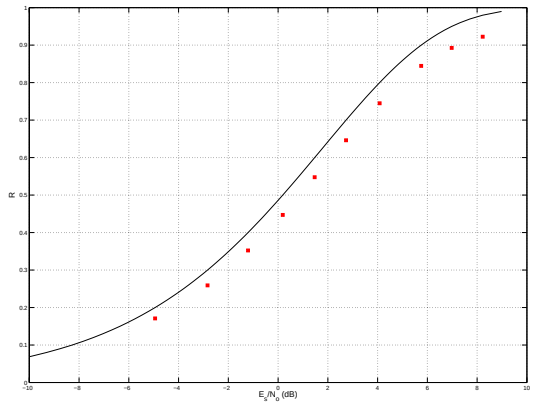

FIG. 2 – Région des capacités atteignables pour un code Raptor optimisé pour $C = 0.8$.

Or cette propriété intéressante est perdue sur des canaux bruités tels que le canal BABG. Dans cet article, nous avons étudié la robustesse d'un code Raptor sous hypothèse asymptotique et sous approximation gaussienne. Pour cela, nous avons d'abord montré qu'un code Raptor possède un comportement à seuil, et que ce seuil peut facilement être calculé par une méthode numérique appelée évolution de densité. C'est ainsi que nous avons pu montrer que bien qu'ils ne sont pas universels au sens strict, les codes Raptor se comportent bien sur une plage de fonctionnement assez large sous décodage conjoint. Cela permet de justifier de leur intérêt sur un canal autre que le canal à effacement, et consititue un premier pas dans cette direction.

Références

[1] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A digital fountain approach to distribution of bulk data," *Proc. of ACM SIGCOMM 98*, pp. 56–67, Sept. 1998.

[2] Michael Luby, "LT codes," *Proc. of the 43rd Annual IEEE Symposium on the Foundations of Computer Science (STOC)*, pp. 271–280, 2002.

[3] Amin Shokrollahi, "Raptor codes," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2551–2567, June 2006.

[4] Omid Etesami and Amin Shokrollahi, "Raptor codes on binary memoryless symmetric channels," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2033–2051, May 2006.

[5] A. Venkiah, C. Poulliat, and D. Declercq, "Analysis and design of raptor codes for joint decoding using information content evolution," in *Proc. of the IEEE International Symposium on Information Theory (ISIT), France*, 2007.

[6] T. J. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, Feb. 2001.

[7] A. Roumy, S. Guemghar, G. Caire, and S. Verdú, "Design methods for irregular reapeat accumulate codes," *IEEE Trans. Inform. Theory*, vol. 50, pp. 1711–1727, Aug. 2004.

A Preuve de la proposition 2

Soit la fonction $F = (\psi \circ \phi)$, ou la fonction ϕ décrit la mise à jour de l'IM au niveau d'un noeud de donnée : $x_v^{(l)} = \phi(x_u^{(l-1)})$:

$$\phi(x) = \sum_{i=1}^{d_v} \iota_i J\Big((i-1)J^{-1}(x) + \tau(x)\Big) \tag{7}$$

avec

$$\tau(x) = J^{-1}\Big(T\Big(\sum_{i=1}^{d_v} I_i J\big(iJ^{-1}(x)\big)\Big)\Big) \tag{8}$$

et la fonction ψ décrit la mise à jour de l'IM au niveau d'un noeud de parité : $x_u^{(l)} = \psi(x_v^{(l)})$:

$$\psi(x) = 1 - \sum_{j=1}^{d_c} \omega_j J\Big((j-1)J^{-1}(1-x) + f_0\Big) \tag{9}$$

Il suffit alors de prouver le résultat suivant : $\lim_{x\to 0} F'(x) = \omega_2(\alpha-1)e^{-f_0/4}$

Pour la suite, notons que $J(0) = 0$, $J'(0) \neq 0$. De plus, $T'(0) = 0$ dans le cas d'un précode LDPC tel que $\rho_2 = 0$, ce qui est toujours le cas en pratique. Un calcul simple donne alors $\tau'(0) = 0$. Calculons d'abord $\phi'(0)$:

$$\phi'(x) = \sum_{i=1}^{d_v} \iota_i\big((i-1)(J^{-1})'(x) + \tau'(x)\big)J'[(i-1)J^{-1}(x)]$$

$$\lim_{x\to 0}\phi'(x) = \lim_{x\to 0}\sum_{i=1}^{d_v}\iota_i(i-1)\frac{J'((i-1)J^{-1}(x))}{J'(J^{-1}(x))}$$

$$= \sum_{i=1}^{d_v}\iota_i(i-1) = \alpha - 1 \tag{10}$$

Calculons ensuite $\psi'(0)$:

$$\psi'(x) = \sum_{j=1}^{d_c}\omega_j(j-1)(J^{-1})'(1-x)J'[(j-1)J^{-1}(1-x)+f_0]$$

Soit $\mu = \mu(x) = (J^{-1})(1-x)$. Alors, il vient :

$$\psi'(x) = \sum_{j=1}^{d_c}\omega_j(j-1)\frac{J'[(j-1)\mu + f_0]}{J'(\mu)}$$

Ensuite, en utilisant l'approximation de $J'(\mu)$ pour μ grand donnée dans [7], nous trouvons : $J'(\mu) \sim \log_2(e)\frac{\sqrt{\pi}e^{-\mu/4}}{4\sqrt{\mu}}$

$$\lim_{x\to 0}\psi'(x) = \lim_{\mu\to\infty}\sum_{j=1}^{d_c}\omega_j(j-1)\frac{J'[(j-1)\mu+f_0]}{J'(\mu)}$$

$$= \lim_{\mu\to\infty}\sum_{j=1}^{d_c}\omega_j(j-1)\sqrt{\frac{\mu}{(j-1)\mu+f_0}}e^{-\frac{(j-2)\mu+f_0}{4}}$$

$$= \omega_2 e^{\frac{-f_0}{4}} \tag{11}$$

Finalement, $\phi(0) = 0$, et l'égalité $F'(x) = \phi'(x)(\psi'\circ\phi)(x)$ donne le résultat attendu, à savoir :

$$\lim_{x\to 0} F'(x) = \omega_2(\alpha-1)e^{\frac{-f_0}{4}}$$

□