List-decoding Reed-Solomon codes: re-encoding techniques and Wu algorithm via simultaneous polynomial approximations

Claude-Pierre Jeannerod[†], Vincent Neiger[†‡], Éric Schost[‡] and Gilles Villard[†]
[†] LIP, ENS de Lyon, France
[‡] University of Western Ontario, London ON, Canada

L'algorithme de Guruswami et Sudan pour le décodage en liste des codes de Reed-Solomon, tel qu'il est présenté dans [6], a un coût élevé et est ainsi difficilement exploitable en pratique y compris pour tailles de codes usuelles et des jeux de paramètres qui ne sont pas très éloignés du cadre du décodage unique. Ainsi, depuis une quinzaine d'années beaucoup de travaux se sont intéressés à réduire la complexité de l'étape la plus coûteuse de cet algorithme, souvent appelée « étape d'interpolation », qui consiste à calculer un polynôme bivarié non trivial qui s'annule en un certain nombre de points avec une multiplicité donnée et des contraintes de degré.

L'algorithme original construit un système linéaire, sous-déterminé par choix des paramètres de décodage, et en calcule une solution non triviale. Il y a essentiellement deux approches qui ont permis d'améliorer la complexité théorique pire-cas de cet algorithme, en résolvant exactement le même problème d'interpolation mais en le reformulant afin de tirer parti d'algorithmes rapides en calcul formel. Une approche, développée d'abord dans un cas particulier dans [9] puis récemment généralisée [12, 4] exploite l'algorithmique des matrices structurées ; l'autre approche [1, 8, 2] exploite la réduction de réseaux polynomiaux, et est en ce sens une transcription au contexte polynomial des algorithmes de PGCD approché dans le cas entier [5]. Dans cet exposé, nous insisterons d'abord sur le fond commun de ces deux approches : la recherche d'une solution non triviale d'un problème d'approximations polynomiales simultanées avec des contraintes de degrés.

Ensuite, nous aborderons la technique dite de *ré-encodage* [7] qui, par le biais d'une translation du mot reçu, permet de connaître partiellement la solution de l'étape d'interpolation. Nous observerons que cette technique se traduit en une réduction de la taille du problème d'approximation, dans des proportions très intéressantes pour les paramètres pratiques. Tous les algorithmes basés sur ce problème d'approximation semblent pouvoir bénéficier directement de cette technique. Une autre technique, également observable comme une réduction de la taille du problème d'approximation, a été récemment introduite [10] ; si la réduction semble moins spectaculaire, cette technique peut se combiner à la précédente et son intérêt pratique est à étudier.

Une autre grande avancée vers un décodage en liste utilisable en pratique a été réalisée avec l'algorithme de Wu [11]. Cet algorithme commence par transformer le problème de décodage en un autre problème similaire, pour lequel l'étape d'interpolation demande une multiplicité nettement inférieure (dans les cas pratiques où la dimension du code est proche de sa longueur) à celle demandée par l'étape d'interpolation de l'algorithme de

Guruswami-Sudan. Nous montrerons comment l'étape d'interpolation de l'algorithme de Wu peut se voir comme un problème d'approximations polynomiales simultanées, de telle manière que les algorithmes rapides développés pour le décodage en liste usuel pourront être réutilisés dans ce cadre. Ceci étend certains résultats présentés dans [3].

Bibliographie

[1] M. Alekhnovich. Linear diophantine equations over polynomials and soft decoding of Reed-Solomon codes. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS'02, pages 439–448, Washington, DC, USA, 2002. IEEE Computer Society.

[2] P. Beelen and K. Brander. Key equations for list decoding of Reed-Solomon codes and how to solve them. *Journal of Symbolic Computation*, 45(7):773–786, 2010.

[3] P. Beelen, T. Hoholdt, J.S.R. Nielsen, and Yingquan Wu. On rational interpolation-based list-decoding and list-decoding binary Goppa codes. *IEEE Transactions on Information Theory*, 59(6):3269–3281, June 2013.

[4] M. F. I. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster algorithms for multivariate interpolation with multiplicities and simultaneous polynomial approximations. *http://arxiv.org/abs/1402.0643*, 2014.

[5] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. In Bernard Chazelle, editor, *ICS*, pages 298–308. Tsinghua University Press, 2011.

[6] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[7] R. Koetter, J. Ma, and A. Vardy. The re-encoding transformation in algebraic list-decoding of Reed-Solomon codes. *Information Theory, IEEE Transactions on*, 57(2):633–647, Feb 2011.

[8] K. Lee and M. E. O'Sullivan. List decoding of Reed-Solomon codes from a Gröbner basis perspective. *Journal of Symbolic Computation*, 43(9):645 – 658, 2008.

[9] R. M. Roth and G. Ruckenstein. Efficient decoding of Reed-Solomon codes beyond half the minimum distance. *IEEE Transactions on Information Theory*, 46(1):246 –257, January 2000.

[10] C. Senger. Prefactor reduction of the Guruswami-Sudan interpolation step. *Information Theory, IEEE Transactions on*, PP(99):1–1, 2014.

[11] Y. Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Transactions on Information Theory*, 54(8):3611 –3630, August 2008.

[12] A. Zeh, C. Gentner, and D. Augot. An interpolation procedure for list decoding Reed-Solomon codes based on generalized key equations. *IEEE Transactions on Information Theory*, 57(9):5946–5959, September 2011.