Décodage en liste des codes de Goppa Binaires et réduction de clé de McEliece

Morgan Barbier
Laboratoire d'Informatique de l'École Polytechnique - LIX
INRIA Saclay - Île de France
morgan.barbier@lix.polytechnique.fr

Résumé

Le premier décodage algébrique pour les codes de Goppa est dû à Patterson en 1975 [5]. Cette méthode décode jusqu'à t, la capacité de correction du code. Les codes de Goppa font partie de la famille des codes alternants, c'est-à-dire des codes restreints à un sous-corps de Reed-Solomon généralisé, il est donc possible d'adapter toutes les méthodes de décodages des codes de Reed-Solomon aux codes de Goppa, comme le célèbre algorithme de décodage en liste de Guruswami et Sudan [4]. Ce procédé nous permet alors de décoder jusqu'à la borne de Johnson générique, qui est plus grand que t, voire la figure 1. Dans son mémoire de thèse [3], Guruswami propose une méthode pour décoder en liste les codes restreints géométriques jusqu'à la borne de Johnson q-aire, qui est plus grande que la borne de Johnson générique. On propose alors d'appliquer cette même méthode aux codes alternants, et tout particulièrement aux codes de Goppa binaires [1]. Bernstein, Lange et Peters expliquent comment dans le cryptosystème de McEliece, on peut utiliser le décodage en liste [2]. On conclura alors par la réduction de clé de McEliece obtenue grâce à cet algorithme de décodage en liste.

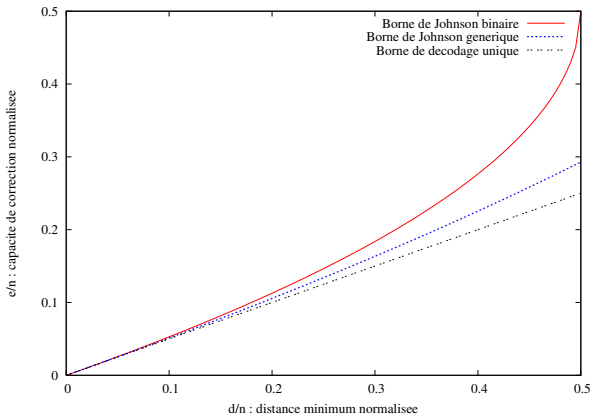

FIGURE 1 – Comparaison de la borne de décodage unique, de Johnson générique et binaire.

Références

[1] D. Augot, M. Barbier, and A. Couvreur, "List-decoding of binary Goppa codes up to the binary Johnson bound," TANC - INRIA Saclay - Polytechnique - Institut de Mathématiques de Bordeaux - IMB, Tech. Rep., 2010. [Online]. Available : http ://hal.archives-ouvertes.fr/inria-00547106/en/

[2] D. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, J. Buchmann and J. Ding, Eds. Springer Berlin / Heidelberg, 2008, vol. 5299, pp. 31–46.

[3] V. Guruswami, *List Decoding of Error-Correcting Codes - Winning Thesis of the 2002 ACM Doctoral Dissertation Competition*, ser. Lectures Notes in Computer Science. Springer, 2004, vol. 3282.

[4] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *Information Theory, IEEE Transactions on*, vol. 45, no. 6, pp. 1757–1767, 1999.

[5] N. Patterson, "The algebraic decoding of Goppa codes," *Information Theory, IEEE Transactions on*, vol. 21, no. 2, pp. 203 – 207, Mar. 1975.