

Théorie de l'information, codage correcteur

Gilles Zémor

Nous nous intéresserons principalement au problème de la transmission d'information à travers un canal soumettant les symboles transmis à des erreurs. Le théorème de Shannon nous dit qu'il est *possible* de transmettre de l'information fidèlement avec des rendements arbitrairement proches de la *capacité* du canal. Cependant il ne nous dit pas *comment* le faire. Plus précisément il nous dit qu'un code correcteur choisi aléatoirement convient presque sûrement. Mais cela ne nous donne pas de construction explicite de code correcteur convenable, et surtout les codes correcteurs aléatoires ne viennent pas avec un algorithme de décodage efficace.

Pendant des années, et même des décennies, la recherche de bons codes se cantonnait à des constructions algébriques où l'on n'essayait pas de corriger plus d'erreurs que la moitié de la distance minimale du code. Les années 1990 ont fait voler en éclat ce point de vue, et l'on a assisté à la naissance de deux approches très différentes du codage. La première est due à Sudan (1997), pour qui le problème du décodage est simplement un problème d'interpolation polynômiale où l'on dispose d'un ensemble de valeurs du polynôme dont certaines sont erronées. Sudan a trouvé comment lever le blocage psychologique (et technique) permettant d'aller plus loin dans la correction d'erreurs. L'autre approche concerne le décodage dit itératif, qui s'est développé fortement suite à l'invention des turbo codes (1993). Nous nous efforcerons de donner un aperçu de ces points de vue modernes de la théorie. En passant, nous mentionnerons quelques applications cryptographiques.

Références

- [1] G. Battail, *Théorie de l'information, applications aux techniques de communications*, Masson, 1997.
- [2] T. M. Cover et J. A. Thomas, *Elements of Information Theory*, Wiley, 2005.
- [3] J. H. van Lint, *An Introduction to coding theory*, Springer, 1998.
- [4] F. J. MacWilliams et N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 2003.
- [5] G. Zémor, *Cours de cryptographie*, Cassini, 2000.