Communiquer sans erreurs : les codes correcteurs

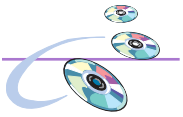
Gilles Lachaud

Pour détecter et corriger les inévitables erreurs qui affectent les échanges d'information numérisée, les spécialistes du codage en appellent à des méthodes abstraites qui relèvent de l'algèbre ou de la géométrie.

Nous sommes en pleine ère numérique. Qu'est-ce que cela veut dire ? Tout simplement qu'une partie énorme des informations échangées à travers la planète est matériellement représentée sous la forme de nombres. Messages électroniques, téléphonie mobile, transactions bancaires, téléguidage de satellites, télétransmission d'images, disques CD ou DVD, etc. : dans tous ces exemples, l'information est traduite — on dit *codée* (à ne pas confondre avec cryptée) — en suites de nombres entiers, et correspondant physiquement à des signaux électriques ou autres. Plus précisément même, l'information est généralement codée sous forme de suites de chiffres binaires — des 0 ou des 1, appelés aussi bits. Par exemple, dans le code ASCII (*American Standard Code for Information Interchange*) utilisé par les micro-ordinateurs, le A majuscule est codé par l'octet (séquence de 8 bits) 01000001, le B majuscule par 01000010, etc.

Un problème majeur de la transmission de l'information est celui des erreurs. Il suffit d'une petite rayure sur un disque, d'une perturbation de l'appareillage, ou d'un quelconque phénomène parasite pour que le message transmis comporte des erreurs, c'est-à-dire des « 0 » qui ont malencontreusement été changés en « 1 », ou inversement. Or l'un des nombreux atouts du numérique est la possibilité de détecter, et même de corriger, de telles erreurs !

Le Matrimandir à Auroville (Tamil Nadu, Inde), géode construite par l'architecte français Roger Anger. Dans la conception de codes correcteurs efficaces, on rencontre des problèmes apparentés à des questions difficiles de pure géométrie, comme celui de recouvrir une sphère par le plus grand nombre possible de disques de même taille, sans qu'ils se chevauchent.



On rallonge les mots du message de façon qu'après dégradation, on puisse quand même les reconnaître

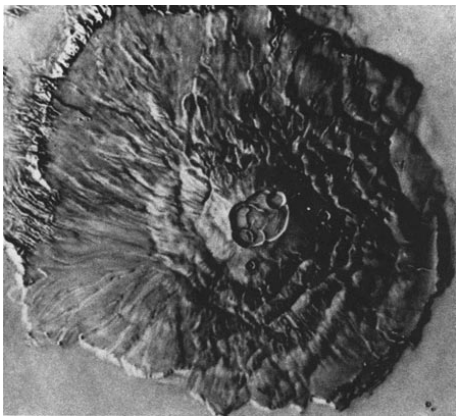
Telle est la fonction des *codes correcteurs d'erreurs*, dont les premiers ont été conçus à la même époque que les premiers ordinateurs, il y a plus d'une cinquantaine d'années. Comment font-ils ? Le principe est le suivant : on allonge les « mots » numériques qui composent le message, de façon qu'une partie des bits servent de bits de contrôle. Par exemple, dans le code ASCII évoqué plus haut, l'un des huit bits est un bit de contrôle : il doit valoir 0 si le nombre de « 1 » dans les 7 autres bits est pair, et 1 sinon. Si l'un des huit bits a inopinément basculé de valeur, la parité indiquée par le bit de contrôle ne correspond plus et une erreur est alors détectée. La même idée se retrouve dans bien des numéros que l'on rencontre dans la vie quotidienne. Par exemple, dans les relevés d'identité bancaire, on ajoute une lettre-clé à un numéro de compte pour pouvoir détecter une erreur de transmission. De même, les numéros des billets de banque en euros sont codés pour éviter les contrefaçons. Autrement dit, la philosophie des codes correcteurs est de composer des messages *redondants* : chaque mot du message est allongé de façon à contenir une information sur le message lui-même !

Un exemple simple et éclairant, mais peu réaliste, de code correcteur d'erreurs est la triple répétition : chaque bit du message à coder est triplé, c'est-à-dire que 0 devient 000 et 1 devient 111. Ce code permet de détecter et corriger une erreur éventuelle sur un triplet. En effet, si l'on reçoit, mettons, la séquence 101, on en déduit immédiatement que la bonne séquence était 111 (on suppose qu'un seul bit sur les trois reçus est erroné), et donc que l'information initiale était le bit 1. Le code de triple répétition n'est pas réaliste car il est coûteux : pour chaque bit d'information, il faut en envoyer trois ; on dit que son taux de rentabilité est 1/3. Ce taux a des répercussions directes sur la durée nécessaire à la transmission des messages et sur le coût des communications.

Un bon code correcteur doit posséder d'autres qualités en plus d'un taux de rentabilité élevé. Il lui faut également une bonne capacité de détection et correction d'erreurs, et la procédure de décodage doit être suffisamment simple et rapide. Tout le problème de la théorie des codes correcteurs d'erreurs est là : construire des codes qui détectent et corrigent le plus possible d'erreurs, tout en allongeant le moins possible les messages, et qui soient faciles à décoder.

L'algèbre des corps finis s'applique naturellement aux codes, car ceux-ci utilisent un alphabet fini

Les mathématiques interviennent depuis longtemps dans ces questions. Déjà en 1948, le mathématicien américain Claude Shannon, un des pères de la théorie de l'information, obtenait des résultats théoriques généraux affirmant qu'il existe des codes ayant des qualités optimales, en un sens technique précis. Cependant, si le théorème de Shannon établissait l'existence de très bon codes correcteurs, il ne fournissait pas de méthode pratique pour les construire. Par ailleurs, on disposait de codes correcteurs aux performances modestes, comme les codes de Hamming, du nom de leur inventeur, le mathématicien américain Richard



Olympus Mons, sur la planète Mars, est le plus grand volcan du système solaire : environ 600 km de diamètre et 27 km de hauteur ! Cette image a été obtenue grâce à la sonde spatiale Mariner 9, en 1971-1972. La sonde envoyait à la Terre ses informations en utilisant un code correcteur capable de corriger jusqu'à 7 bits erronés sur 32. Dans chaque groupe de 32 bits, 26 étaient des bits de contrôle, et les 6 autres constituaient l'information nette. Aujourd'hui, on dispose de codes correcteurs encore plus performants. (Cliché NASA/JPL)

W. Hamming (1915-1998), dans les années 1950 (dans ces codes, qui ont été beaucoup utilisés, les bits de contrôle sont déterminés en fonction des bits d'information par des équations linéaires simples).

Les spécialistes se sont alors mis à étudier de manière systématique les codes correcteurs et leurs propriétés, dans le but d'obtenir concrètement des codes aussi performants ou presque que le prédisaient les résultats théoriques de Shannon. Pour ce faire, ils ont utilisé à fond l'algèbre. Si le codage de l'information se fait directement dans l'« alphabet » binaire 0 et 1, l'algèbre sous-jacente est celle du pair et de l'impair, connue déjà de Platon (pair + pair = pair, pair + impair = impair, pair x pair = pair, impair x impair = impair, etc.). En fait, il s'avère plus intéressant de considérer des « alphabets » de codage ayant plus de deux chiffres, et de traduire seulement à la fin de la procédure le résultat en suites binaires de 0 et 1. Comme un alphabet comporte un nombre fini de symboles, et que l'on souhaite effectuer des calculs sur ces symboles, l'algèbre sous-jacente est l'objet de la *théorie des corps finis*, créée par le jeune mathématicien français Évariste Galois au début du XIX^e^ siècle, en étudiant la résolubilité des équations algébriques (un corps fini est un ensemble d'éléments en nombre fini qui peuvent s'additionner, se multiplier et se diviser de manière analogue aux nombres ordinaires, le résultat des opérations restant à l'intérieur de cet ensemble. L'ensemble constitué par 0 et 1, avec les règles arithmétiques du pair et de l'impair, est le corps fini à deux éléments ; c'est le corps fini le plus simple).

Ainsi, c'est à l'aide d'algèbre abstraite et élaborée, en liaison avec la théorie des corps finis, qu'ont été construits des codes correcteurs d'erreurs très efficaces, adaptés à tel ou tel type de transmission d'information. Deux exemples parmi une multitude d'autres sont le code employé pour la gravure des disques audionumériques (il permet de corriger jus-

Quoi qu'en dise ce timbre français émis en 1984, Évariste Galois n'était pas un géomètre mais un algébriste. C'était le pionnier de la théorie des groupes, ainsi que de la théorie des corps finis utilisée notamment par les spécialistes des codes correcteurs d'erreurs. Provoqué en duel, Galois est mort à l'âge de 21 ans à peine.

qu'à environ 4 000 bits erronés consécutifs, l'équivalent d'une rayure sur plus de 2 millimètres de piste !), et celui qu'a utilisé la sonde spatiale Mariner 9 pour nous envoyer ses images de la planète Mars.

Une nouvelle famille de codes faisant appel à la géométrie algébrique des courbes

L'algèbre abstraite n'est pas le seul instrument dont disposent les spécialistes des codes correcteurs. Il y a aussi la géométrie, et plus particulièrement la géométrie algébrique. Celle-ci, très vaste partie des mathématiques actuelles, a pour point de départ l'étude des objets géométriques — courbes, surfaces, etc. — définis par des équations algébriques. Tout lycéen sait par exemple qu'une parabole peut être représentée par une équation algébrique, de type $y = ax^2 + bx + c$, où x et y sont les coordonnées des points de la parabole. On peut aussi étudier des courbes définies sur des corps finis, c'est-à-dire que dans les équations algébriques qui les représentent, les grandeurs comme x et y ne sont pas n'importe quels nombres, mais uniquement des éléments d'un certain corps fini. En utilisant de telles courbes et l'algèbre associée aux coordonnées de leurs points (qui sont en nombre fini), on a inauguré, il y a environ vingt ans, une nouvelle famille de codes correcteurs : les codes géométriques. Cela a permis récemment d'obtenir de nouveaux résultats concernant les codes binaires, et de construire des codes encore plus performants que ceux prédits par les travaux de Shannon. En contrepartie, l'analyse des codes géométriques a conduit les mathématiciens à examiner de plus près le nombre de points d'une courbe algébrique définie sur un corps fini. On a là un bel exemple de la rétroaction positive qu'un domaine d'application peut exercer sur la discipline théorique dont il se sert.

Gilles Lachaud
Institut de mathématiques de Luminy,
CNRS, Marseille

Quelques références :

- P. Arnoux, « Codage et mathématiques », *La science au présent* (édition Encyclopædia Universalis, 1992).
- P. Arnoux, « Minitel, codage et corps finis », *Pour la Science* (mars 1988).
- G. Lachaud et S. Vladut, « Les codes correcteurs d'erreurs », *La Recherche* (juillet-août 1995).
- O. Papini, « Disque compact : « la théorie, c'est pratique ! » dans « Secrets de nombres », Hors-série n° 6 de la revue *Tangente* (1998).
- O. Papini et J. Wolfmann, *Algèbre discrète et codes correcteurs* (Springer-Verlag, 1995).
- J. Vélu, *Méthodes mathématiques pour l'informatique* (Dunod, 1995).
- M. Demazure, *Cours d'algèbre — primalité, divisibilité, codes* (Cassini, 1997)