SMF

Mot du Président

Les mathématiques françaises se portent-elles bien ? La réponse la plus fréquente est oui pour la recherche, non pour l'enseignement. Le forum sur le serveur de la SMF est éloquent sur ce point. Or, pour assurer durablement la qualité d'une école scientifique, le plus important est de prévoir la relève, donc de se préoccuper de la génération montante. De plus une des caractéristiques de l'Université est de permettre à la recherche et à l'enseignement d'interagir.

La SMF a entrepris depuis longtemps une réflexion de fond sur les questions d'enseignement. La commission d'enseignement de la SMF a organisé de nombreux débats, et a fortement contribué à sensibiliser les adhérents, les mathématiciens, et plus largement la communauté scientifique. Le problème est vaste : il n'est limité ni à la France, ni aux mathématiques. Cela étant il ne s'agit pas de rechercher une solution universelle, mais il faut quand même regarder globalement la question de l'enseignement des sciences en France.

Après la réflexion et les débats, nous sommes passé dans une phase d'action depuis un an. Avec 14 autres associations la SMF participe à « Action Sciences », qui vise à promouvoir les sciences auprès de personnalités politiques, avec deux demandes très précises :

– une programmation des postes a moyen terme, et un prérecrutement des enseignants, accompagné d'un développement de la formation continue.

– un renforcement de la cohérence de la voie scientifique au lycée. Ces objectifs sont relativement modestes ; ils ont l'avantage d'être précis, argumentés, possibles à obtenir, et ils portent sur des points importants du système éducatif.

Des délégations des 15 associations sont allées voir diverses personnalités politiques qui les ont très bien accueillies. Quand un aussi grand nombre de scientifiques s'entendent pour transmettre un message commun, cohérent et raisonnable, l'impact est assuré. Ce mouvement va se poursuivre et, je l'espère, s'amplifier – je compte sur les adhérents de la SMF pour relayer le message.

Le gouvernement lance une vaste consultation nationale sur l'avenir de l'école. Une commission a été créée, placée auprès du Ministre de la Jeunesse, de l'Éducation Nationale et de la Recherche (voir `http://www.debatnational.education.fr/`). Je vous encourage vivement à participer à ce grand débat national. « Action Sciences » ne doit pas demeurer seulement une préoccupation des états majors, il faut que le plus grand nombre possible de membres de ces associations, et notamment de la SMF, y participent.

Michel Waldschmidt

Vie de la société

Un hommage a été rendu à la mémoire de Laurent Schwartz du 1 au 4 juillet 2003 à l'École polytechnique. La SMF était l'une des associations qui patronnait cette manifestation. Un numéro spécial de la *Gazette* de la SMF sera consacré à Laurent Schwartz.

Le président de la Wiskundig Genootschap, Eduard Looijenga, a remercié la SMF ainsi que tous ceux qui sont intervenus pour protester contre la fermeture prévue du département de mathématiques de l'université de Nijmegen ; il les informe que l'Université est revenue sur sa décision et a entrepris de rajeunir ce département en créant trois nouveaux postes permanents.

En conclusion d'une rencontre avec les sociétés latino-américaines à Saint-Jacques-de-Compostelle du 22 au 25 décembre, un réseau a été créé le « ROLMa » pour Red de Organizaciones Latinoamericanas de Matematicas. La SMF est l'une des 25 sociétés mathématiques signataires de l'accord final.

Avec la Société Française de Chimie (SFC), la Société Française de Physique (SFP) et la Société de Mathématiques Appliquées et Industrielles (SMAI), la SMF a écrit le 16 septembre au Premier Ministre pour demander que les problèmes liés à l'enseignement des sciences soient convenablement pris en compte dans le débat national sur l'école qui vient d'être lancé.

Enfin la SMF lance un appel à candidatures pour le Prix d'Alembert et le Prix Anatole Decerf qui seront décernés lors de la journee annuelle le 19 juin 2004. Voir les informations sur le serveur de la SMF à l'adresse :
`http://smf.emath.fr/VieSociete/PrixAlembert`.

MATHÉMATIQUES ET INFORMATIQUE

Les travaux de Madhu Sudan sur les codes correcteurs d'erreurs

Daniel Augot

Nous présentons les travaux de Madhu Sudan en théorie des codes correcteurs, qui, parmi d'autres[1]*, lui valurent de recevoir le prix Nevanlinna en août 2002*[2]*, qui est le pendant de la médaille Fields, dans le domaine des aspects mathématiques de l'informatique. La percée majeure de M. Sudan est d'avoir produit un algorithme de décodage des codes de Reed-Solomon bien au-delà de la capacité de correction de ces codes, en autorisant de pouvoir décoder en retournant comme résultat une liste de solutions plutôt qu'une unique solution, ce que l'on appelle le « décodage en liste ».*

Il s'agit d'une avancée théorique fondamentale dont les conséquences pratiques et théoriques ne sont pas encore mesurées. Dans cette présentation, nous introduirons l'arrière-plan pratique de la théorie des codes, puis les codes de Reed-Solomon et les codes géométriques. Enfin, nous présenterons l'algorithme de M. Sudan, comme une généralisation de l'algorithme de Berlekamp-Welsh.

Cet exposé repose sur la présentation que M. Sudan a lui même faite dans [6].

Introduction et définitions

La théorie des codes est la discipline des mathématiques appliquées dont le sujet est la transmission fiable d'informations sur un canal de transmission bruité, en utilisant des objets combinatoires et algorithmiques appelés *codes correcteurs d'erreurs*. Pour introduire le sujet, il est d'abord nécessaire de préciser les notions de base du codage.

Suivons pour cela un message sur le chemin depuis la source jusqu'au récepteur, et observons les notions intéressantes qui apparaissent. Il y a trois entités impliquées dans le processus : l'émetteur, le récepteur et le canal de transmission. L'objectif de l'émetteur est de communiquer au récepteur un *message*, m, appartenant à $\mathcal{M}$ où $\mathcal{M}$ est un ensemble fini, *l'espace des messages*. Le canal de transmission bruité est capable de communiquer des suites arbitrairement longues de symboles d'un alphabet Σ, qui est « petit » (un des cas les plus intéressants étant $\Sigma = \{0, 1\}$). Alors l'espace des messages à coder est Σ^k, l'ensemble des suites de symboles de longueur k.

Émetteur et récepteur se mettent d'accord sur la longueur n des suites codées transmises, appelée la *longueur du code*, les messages échangés appartenant

[1] Ses autres travaux portent sur la théorie de la complexité, et il est l'un des auteurs du célèbre théorème PCP [8], en rapport avec la conjecture $P \neq NP$.

[2] `http://www.maa.org/news/fields02.html/`

donc à Σ^n, que l'on appellera l'*espace ambiant*. L'émetteur et le récepteur se mettent aussi d'accord sur une *fonction de codage*, E, injective.
$E : \mathcal{M} \to \Sigma^n$, utilisée pour coder les messages avant transmission. L'image $C = \{E(m), \quad m \in \mathcal{M}\}$ est appelée le *code*. Le taux k/n, noté en général R, est appelé le *taux de transmission* ou *rendement* du code, c'est le premier paramètre fondamental d'un code, en théorie des codes.

En ce qui concerne le canal de transmission, il « bruite » les messages transmis. Ce bruit peut être vu comme une application de l'espace ambiant dans lui-même. Prescrivons maintenant une structure de corps sur l'alphabet Σ (par exemple Σ est un corps fini, de petite taille), ce qui induit une structure d'espace vectoriel sur Σ^n. Il devient alors plus commode de considérer des *codes linéaires* c'est-à-dire l'image par une application linéaire de Σ^k dans Σ^n, que l'on supposera toujours non singulière. On spécifiera dorénavant un code linéaire C par sa matrice génératrice (une base de C), ce qui est une manière compacte de décrire un ensemble a priori de taille q^k. En ce qui concerne le canal de transmission, il produit un vecteur de bruit $e \in \Sigma^n$, et le mot reçu est $y = E(m) + e$, m étant le message. Le récepteur utilise alors une fonction de décodage $D : \Sigma^n \to \mathcal{M}$. Le décodage D doit être rapide, et être tel que $D(y) = m$, avec grande probabilité. Intuitivement, le code introduit une redondance en augmentant la longueur des messages, et cette redondance sera utilisée pour décoder le message transmis, même s'il est bruité. Du point de vue de la fiabilité de la transmission, la question fondamentale de la théorie des codes est

> Étant donnée une distribution de probabilité P sur le canal de transmission (*i.e.* une distribution de probabilité sur les erreurs de transmission), quelles sont les meilleures fonctions de codage et de décodage, c'est-à-dire quelle est la plus petite probabilité d'erreur
>
> $$\min_{E,D} \left\{ \mathbf{E}_{m \in \mathcal{M}} \left(\Pr_{\eta \in P}[D(E(m) + \eta) \neq m] \right) \right\}$$
>
> où $\mathbf{E}$ désigne l'espérance mathématique.

Shannon a étudié les propriétés asymptotiques de cette quantité quand la distribution du bruit sur Σ^n est le produit cartésien d'une distribution sur Σ. Dans ce contexte, il existe une quantité $C_0 \in [0, 1]$, dépendant du canal, telle que pour tout $R < C_0$ et $\varepsilon > 0$, et, pour n assez grand, il existe toujours un couple codage/décodage avec un code de taux R tel que la probabilité d'erreur soit au plus ε. Dans le cadre de cet exposé, nous considérerons uniquement le cas du *canal q-aire symétrique*, défini de la manière suivante : chaque symbole de Σ transmis est préservé avec une certaine probabilité $1 - \delta$, ou bien est transformé en autre symbole parmi les $q - 1$ autres possibles avec probabilité $\delta/(q - 1)$, les événements étant indépendants d'un symbole à l'autre.

D'un autre coté, Hamming a défini les notions de *code correcteur d'erreur* et de code *détecteur d'erreur*. Définissons le *poids de Hamming* d'une séquence $x \in \Sigma^n$ comme le nombre de composantes non nulles de x, et la *distance de Hamming* entre x et y comme le poids de la différence $x - y$ (c'est-à-dire le nombre de composantes où x et y diffèrent). C'est bien une distance. On définit alors la distance minimale d'un code C comme la plus petite distance entre deux mots du code C. Le canal de transmission crée en général un vecteur η de petit

poids, par exemple de poids borné par e. On dira qu'un code correcteur corrige e erreurs si les boules de rayon e centrées sur les mots de code ne s'intersectent pas. En effet si le poids de l'erreur est inférieur à e, alors, si C est e-correcteur, il y a unicité du mot de code le plus proche. Une capacité de correction e implique que la distance minimale entre deux mots distincts du code est supérieure à $2e+1$. La distance minimale est le deuxième paramètre fondamental d'un code. On parlera d'un code $[n, k, d]$ pour un code de longueur n, de dimension k et de distance minimale d. Du point de vue de Hamming, la question fondamentale est

> Étant donné un alphabet Σ de taille q, et deux entiers n et k, $k < n$, quelle est la plus grande distance minimale d d'un code $C \subseteq \Sigma^n$ de taux de transmission k/n ?

En effet, une distance minimale élevée induit que le code est capable de corriger des erreurs de poids élevé. Signalons immédiatement que le problème de Hamming n'est pas résolu quand la taille de l'alphabet est petite. Il y a une réponse satisfaisante à la question quand $q \geqslant n$ (voir les codes de Reed-Solomon dans la section suivante).

Constructions de codes

Nous commencerons par la famille des codes aléatoires linéaires (en fait une *non-construction*). La borne de Varshamov-Gilbert indique qu'il existe des codes de paramètres $[n, k, d]$ si n, k et d vérifient :

$$q^k V_q(n, d) \leqslant q^n,$$

où $V_q(n, d)$ est le volume de la sphère de Hamming de rayon d (c'est-à-dire son cardinal). Donc il existe des codes tels que $q^k V_q(n, d) \geqslant q^n$. En prenant le logarithme et en approchant $V_q(n, \delta n)$ par $q^{H_q(\delta)n}$ (où $H_q(x)$ désigne la fonction d'entropie q-aire : $H_q(\delta) = -\delta \log_q(\frac{\delta}{q-1}) - (1-\delta)\log_q(1-\delta)$), on obtient l'existence de codes sur la borne suivante :

$$R \geqslant 1 - H_q(\delta), \qquad \text{avec } R = \frac{k}{n} \text{ et } \delta = \frac{d}{n}.$$

Ce résultat s'étend « particulièrement » aux codes aléatoires : avec une probabilité tendant vers 1 quand la longueur n croît, les codes aléatoires se trouvent sur la borne de Varshamov-Gilbert. La question qui en découle est de savoir s'il existe des codes dépassant la borne de Varshamov-Gilbert.

En dehors des codes aléatoires, la théorie des codes s'est donc appliquée depuis ses fondements à produire des familles explicites de bons codes, dont la dimension et la distance puissent être déterminées à l'avance. Cela a conduit à toute une « botanique » de codes, diversement utilisés en pratique.

Citons une autre borne, celle de Singleton. Suivant cette borne, tout code C linéaire voit ses paramètres $[n, k, d]$ vérifier $k + d \leqslant n + 1$. Pour la démontrer, considérons une *matrice de parité* de C, il s'agit d'une matrice H de taille $(n-k) \times n$ dans laquelle sont écrites $n-k$ formes linéaires qui s'annulent sur le code C : tout mot c du code vérifie $Hc = 0$. Le rang de la matrice H est $n-k$, et comme le code ne contient pas de mot de poids strictement inférieur à d, il n'y a pas de relations linéaires entre moins de d colonnes de H : $d - 1 \leqslant n - k$.