Revue synthétique des communications présentées au colloque

« Trois journées d'étude sur les codes correcteurs »

Les « Trois journées d'étude sur les codes correcteurs » se sont tenues les 28, 29 et 30 mai dernier. Nous présentons ici une revue synthétique de l'ensemble des communications de ce colloque. Ce numéro spécial de *TS* contient la plupart des communications. Nous publierons dans les numéros suivants les articles parvenus.

Jean-Louis LACOUME.

G. Battail retrace l'évolution du codage depuis les promesses de Shannon, jusqu'aux problèmes actuels d'adaptation des codes connus à des voies de transmission dont les caractéristiques sont variables. Il dégage un certain nombre d'approches et de notions antagonistes qui illustrent 'a complexité et la richesse du domaine.

Six exposés sont consacrés à des méthodes algébriques de caractérisation ou de construction de codes.

– Des techniques de démultiplication de codes sont présentées par Jacques Wolfmann. Elles permettent en particulier d'obtenir des codes binaires autoduaux à partir de codes de Reed-Solomon.

– MM. Poli, Thiong Ly déterminent des groupes d'automorphismes de codes définis comme idéaux d'algèbres modulaires.

– M. Rigoni donne une procédure permettant d'énumérer tous les codes autoduaux k circulants à poids multiples de quatre.

– M^{me} Charpin construit une classe de codes dits « codes de Reed et Muller 1-translatés » dont les propriétés algébriques les rapprochent des codes de Reed et Muller classiques et les situent entre deux codes de Reed-Muller « consécutifs » $R(p, m)$ et $R(p+1, m)$.

– Enfin M. Thiong Ly présente une caractérisation des codes de Reed-Solomon généralisés autoduaux qui permet de les construire tous dans le cas des corps de caractéristique 2.

– M. Solé étudie des familles de séquences complexes ayant de bonnes propriétés de corrélation. Ces séquences sont construites à partir de codes cycliques sur des corps non premiers.

Six exposés illustrent des aspects plus combinatoires.

– M. Beveraggi* étend la problématique du codage à l'ensemble S_n des permutations et construit des codes sur S_n de cardinalité maximale.

– M. Face* recherche des métriques extrêmales bi-invariantes sur S_n.

– G. Roux* détermine des bornes sur la dimension d'un tableau binaire k-surjectif, c'est-à-dire, tel qu'un sous-tableau extrait, formé de k colonnes quelconques du tableau initial, voit apparaître dans ses lignes toutes les 2^k configurations de k éléments binaires.

– G. Cohen présente une construction de ces tableaux k-surjectifs à partir de codes linéaires. Ce qui simplifie leur génération lorsqu'ils sont utilisés pour tester des circuits VLSI.

– H. Hollmann utilise le cadre des schémas d'association pour généraliser des bornes sur les t-designs à points répétés.

– Enfin A. Lobstein détermine le nombre minimal de mots d'un code binaire de longueur $n=2p+3$, non nécessairement linéaire, ayant un rayon de recouvrement égal à p.

Deux exposés sont consacrés à des problèmes algorithmiques qui surgissent dans l'étude des codes (en dehors du décodage) ou en cryptographie.

– Le premier, présenté par M. Poli, concerne la factorisation de polynômes sur le corps à deux éléments.

– M. Harari* propose dans un second exposé une adaptation de l'algorithme dit des « 3 L » qui permet de trouver un point de petite norme dans un réseau, à la détermination de la distance minimale d'un code.

Trois exposés sont consacrés aux algorithmes de décodage pour des familles de codes bien connues.

– M^{elle} Papini dans son étude du décodage par permutations montre que l'invariance des codes de Reed-Solomon étendue sous l'action du groupe affiné permet de trouver des ensembles de permutations plus riches que les décalages circulaires habituellement

utilisés. Le décodage de toutes les configurations d'erreurs de multiplicité compatible avec la distance minimale du code est rendue possible pour certains codes par cette procédure.

– M. Bonneau présente une méthode de décodage par vote majoritaire pour les codes de Reed-Muller qui permet de justifier d'une nouvelle façon l'algorithme classique de Reed.

– Enfin M. Dornstetter montre que la matrice de contrôle des codes de Reed-Solomon est similaire à une matrice de Cauchy et en déduit une nouvelle méthode de décodage algébrique des codes en question basée sur un algorithme d'identification rationnelle. Cette méthode supprime la nécessité d'évaluer le reste d'une division polynomiale le long des racines du générateur du code associée aux méthodes classiques de décodage par développement en fractions continues.

L'utilisation sur des canaux réels des codes de Reed-Solomon semble assez répandue puisque quatre exposés relatifs à des réalisations pratiques décrivent des dispositifs de décodage pour cette famille de codes.

– M. Boulenouar* présente une réalisation sous forme de circuit intégré d'un décodeur du type « piège à erreur » pour un code de Reed-Solomon en longueur 255 de distance 6 utilisé pour la protection d'enregistrements magnétiques sur disques durs.

– L'exposé de M. Laurent décrit l'architecture d'un coprocessor spécialisé dans les opérations sur des corps de Galois de caractéristique 2 qui permet d'effectuer toutes les opérations nécessaires à la mise en œuvre des méthodes de décodage algébriques désormais bien connues pour les codes BCH et Reed-Solomon. La grande versatilité du circuit est obtenue grâce à une structure microprogrammée et à des opérateurs spécialisés pouvant travailler dans des corps de Galois ayant de 16 à 256 éléments.

– L'exposé de M. Froidevaux est relatif à la description d'un circuit intégré destiné à localiser une erreur affectant deux caractères de 16 bits consécutifs dans des enregistrements de très grande longueur sur disque magnétique. La structure du polynôme générateur du code utilisé est choisie de façon à pouvoir localiser rapidement l'erreur par l'utilisation du théorème des restes chinois.

– Le dernier exposé concernant des mises en œuvre matérielles est présenté par M. Catrevaux* qui décrit une réalisation en circuits discrets d'une étonnante compacité pour un codeur-décodeur utilisant un code de Reed-Solomon en longueur 255 permettant de corriger quatre erreurs.

M. Godlewski présente dans son exposé les liens qui existent entre les différentes mesures existantes de la complexité d'une méthode de décodage. Il met en évidence les conclusions paradoxales que l'on tire parfois de la comparaison de différentes évaluations relatives à une même méthode en fonction du critère retenu et de la façon de présenter les résultats.

M[lle] Gennero décrit les possibilités offertes par son logiciel « LOUSTICC » pour l'évaluation des méthodes de codage pour protéger les transmissions contre les erreurs.

M. Merkx propose l'utilisation de codes de Hamming pour stocker de l'information sur des mémoires à écriture irréversible. Il montre avec des arguments géométriques que l'on peut écrire $(n . \log n/4)$ fois $\log n$ bits sur n positions binaires.

Enfin l'exposé du Professeur Goutelard aborde le délicat problème de l'utilisation des techniques d'entrelacement pour lutter contre les canaux à évanouissements profonds et susceptibles d'être perturbés par des parasites à caractère plus ou moins périodique. Après avoir souligné les méfaits des entrelaceurs rectangulaires classiques dans ce genre de situation (apparition de phénomènes de synchronisme entre le parasite et l'entrelaceur) il décrit des méthodes plus sophistiquées ne présentant pas ces inconvénients sans sacrifier les autres performances.

J. L. DORNSTETTER
P. GODLEWSKI

N.B. Les communications des auteurs marquées d'un astérisque ne figurent pas dans les numéros spéciaux 1984.