Rapport INRIA 1994 — Programme 2

Codes et Protection de l'Information

PROJET CODES

3 mai 1995

PROJET CODES

Codes et Protection de l'Information

Localisation : *Rocquencourt*

Mots-clés : algorithme (1), code correcteur (1), erreur (1), protection de l'information (1), transmission de signal (1).

1 Composition de l'équipe

Responsable scientifique

Paul Camion, directeur de recherche CNRS

Responsable permanent

Pascale Charpin, directeur de recherche INRIA

Secrétariat

Christelle Guiziou

Conseiller scientifique

Guy Chassé, Ecole des Mines de Nantes

Personnel INRIA

Nicolas Sendrier, Chargé de Recherche
Daniel Augot, Chargé de Recherche

Chercheurs doctorants

Francis Blanchet, Education Nationale
Françoise Levy-dit-Vehel, Boursière INRIA, depuis Octobre 91
Gaétan Haché, Boursier INRIA, depuis Janvier 93

Anne Canteaut, Boursière DRET, depuis Septembre 93

Chercheurs extérieurs

Thierry Berger, Université Limoges
Claude Carlet, Université Caen
Sami Harari, Université Toulon
François Laubie, Université Limoges
Dominique Le Brigand, Université Paris 6
Augustin Thyong-Ly, Université Toulouse le Mirail
Jacques Wolfmann, Université Toulon

Chercheurs Invités

Thomas Ericson, Université de Linköping, Suède, du 1^{er} septembre 93 au 31 juillet 94
Victor Zinoviev, Académie des Sciences de Moscou, Russie, du 1^{er} février 94 au 30 septembre 94

Stagiaires

Grégoire Bommier, Stagiaire DEA, ENS Ulm et Université Paris 6, du 1^{er} mars au 30 juin
Frédéric Bihan, Stagaire de DEA, Université de Rennes 1, du 1^{er} juin au 31 juillet

2 Présentation du projet

Le domaine de recherche du projet *CODES* reste centré sur les Codes Correcteurs d'Erreurs. Toutefois le projet a ce double objectif : développer la recherche fondamentale en théorie du codage tout en se situant délibérement dans le domaine des Applications en "Protection de l'Information".

Depuis les premiers codes de HAMMING et surtout la découverte des fameux codes BCH (Bose-Chaudhury-Hocquenghem, 1960), la Théorie Algébrique des Codes Correcteurs connait un développement constant. On peut mesurer ceci au nombre d'ouvrages et de publications parus ces dernières décennies, tant dans le secteur théorique (mathématiques discrètes ou appliquées) que dans le domaine de l'ingénierie (voir l'ouvrage de J. MAC-WILLIAMS et N. SLOANE, des Bell Labs, qui comporte plus de 1200 références, ou encore la revue IEEE, *Transaction on Information Theory.*).

Les codes correcteurs servent à protéger une information transitant à travers un canal de transmission. Ce canal peut être une ligne téléphonique, une liaison radio ou encore un support magnétique ou optique : bande magnétique ou disque compact. Il sera généralement perturbé par un bruit qui dépendra de l'environnement et de la nature du canal : perturbations électriques, rayures, ... Le codage consistera en l'ajout d'une redondance pour combattre les effets du bruit. Le décodage devra permettre, à partir de la sortie codée puis perturbée du canal de restituer de façon acceptable l'information fournie par la source.

Pour les codes en bloc, si le taux d'erreur en ligne est inférieur à la capacité de correction, la probabilité d'erreur au décodage tend vers zéro lorsque la longueur du code augmente, à taux de transmission et capacité de correction constants. C'est une conséquence du théorème central limite. Il en découle que *la construction de codes longs avec de bons paramètres, munis d'un algorithme de décodage dont la complexité croit aussi faiblement que possible avec la longueur, est un sujet fondamental de recherche.*

La mise en oeuvre des codes se fait en VLSI, processeur de signaux, circuits logiques rapides et circuits programmables. Il s'agit de trouver de "bons" codes -du point de vue de la théorie de l'information-. En gros, l'objectif est de minimiser le temps d'occupation de la ligne pour un pouvoir de correction donné. De plus, il faut que les temps de codage et de décodage soient très courts. Chaque code doit donc être accompagné d'un algorithme de codage et d'un autre de décodage. Les applications les plus familières des codes correcteurs sont l'utilisation des codes très élaborés de Reed-Solomon pour les disques compacts, et les plus importantes concernent les télécommunications et en particulier les liaisons avec les satellites et les sondes spatiales. Le disque compact est un exemple remarquable de ligne très bruitée où l'on peut corriger les erreurs dues aux empreintes digitales, poussières, salissures ou érosions laissant une trace d'environ 2,5 mm sur le disque qui, pour 74 minutes de musique, est le support d'environ 20 milliards de bits, élaborés sur la saisie de deux fois 16 bits d'information, 44 100 fois par seconde.

La recherche "pure" sur les codes correcteurs consiste en l'étude in abstracto des meilleurs codes possibles, sans se soucier, à ce stade de recherche, de l'existence d'un bon algorithme de décodage. On est ainsi amené à construire des codes ayant une structure algébrique de plus en plus complexe, en utilisant tous les outils de Mathématique Discrète (al-

gèbre des structures finies, combinatoire, géométries finies...). L'autre versant de la recherche se situe au niveau de la *performance des codes*, ce qui impose la recherche systématique de tous les paramètres d'un code donné ; l'existence et la complexité d'algorithmes de décodage sont alors un élément de l'étude. Ainsi le domaine de recherche, bien que centré sur l'étude d'un objet "mathématique", doit intégrer les outils modernes de l'Informatique Théorique, notamment l'Algorithmique et le Calcul Formel.

Il faut noter aussi que les liens existant entre la cryptographie et la théorie des codes correcteurs se concrétisent en de nouveaux thèmes de recherche. Il peut s'agir par exemple de construire des protocoles dont la confidentialité est basée sur un problème NP-complet relevant de la théorie des codes. Plus généralement, l'utilisation des fonctions booléennes, de la théorie des corps finis ou de certains algorithmes de codage, nécessitent la compétence de spécialistes de théorie des codes.

Généralement parlant, l'ensemble des actions de recherche que nous avons décrites fournissent les matériaux scientifiques indispensables à la conception de toute application des codes autocorrecteurs à la transmission et à la conservation des données en télécommunication moderne et dans les systèmes d'enregistrement. Ces recherches comprennent les études des domaines potentiels d'application du codage et des moyens de pourvoir en haute capacité de correction, pour combattre le bruit, qu'il soit spécifié ou aléatoire.

3 Actions de recherche

3.1 Codes correcteurs : aspects théoriques

3.1.1 Distribution de poids des codes cycliques

D. Augot, P. Charpin et N. Sendrier ont introduit (en 91-92) une méthode d'exploration des mots des codes cycliques classiques, plus particulièrement des mots de poids minimum de certains codes BCH (i.e. les codes de Bose-Chaudhury-Hocquenghem) binaires. Cette méthode était basée sur l'exploration systématique des identités de Newton, utilisant en interactif les possibilités du logiciel Maple. D. Augot, pour sa thèse, a amélioré de façon décisive cette étude préliminaire. Il a montré que *s'il existe des solutions au système algébrique défini par les identités de Newton, alors le problème posé dans le domaine des codes correcteurs*

admet une solution. Utilisant des techniques de base standard et les possibilités du logiciel AXIOM, il a obtenu des résultats précis, prouvant l'efficacité de son point de vue.

D. Augot a soutenu sa thèse en Décembre 93 [3]. Les logiciels mis en oeuvre permettent maintenant de soutenir la recherche théorique, menée par le projet, sur la distance minimale des codes cycliques. Ces méthodes ont été présentées à ISIT'94 [28], et un article est soumis à la revue "Finite Fields". Un rapport sur ces résultats a été édité par l'Université de Sherbrooke [57], où D. Augot a séjourné en Juillet et Aout 94.

D. Augot a généralisé ces travaux pour certains codes alternants. Toutefois les moyens algorithmiques actuels ne permettent pas d'étudier ces codes. Il travaille avec Jean-Charles Faugère pour étendre aux corps finis *non premiers* les calculs de bases de Grobner en Gb (programme performant de calcul de bases de Grobner). Du point de vue théorique, D. Augot étudie aussi la généralisation de ces méthodes aux codes *géométriques*. D'autres auteurs ayant utilisé des méthodes analogues à celle introduite par D. Augot, P. Charpin et N. Sendrier pour ces codes, il semble prévisible que les résultats de la thèse soient aussi généralisables.

Les travaux suivants utilisent ces logiciels ou bien sont des prolongements de l'étude menée avec les Identités de Newton:

- C. Carlet a obtenu une nouvelle démonstration d'un des résultats, portant sur une classe infinie de codes BCH. Cette preuve utilise des outils nouveaux, introduits à cette occasion [12],
- des résultats originaux sur les idempotents des codes BCH ont été obtenus par D. Augot et N. Sendrier [7]. Ces résultats s'appuient sur le calcul à l'aide d'un programme en C, du corps de décomposition d'un nombre important de polynômes à coefficients dans $\mathbf{F}_2$,
- F. Levy-dit-Vehel a étudié avec D. Augot, le cas précis des duaux des codes BCH. L'idée est d'obtenir la meilleure approximation de la distance minimale, par comparaison de différents algorithmes. Les résultats ont été présentés à ISIT'94 [26] ; un article est en préparation.

F. Levy-dit-Vehel soutiendra sa thèse en Octobre 94 [5]. Le sujet en est la *divisibilité* des codes cycliques– i.e. caractère de divisibilité des poids des mots du code. Son principal résultat est l'obtention de nouvelles bornes théoriques pour la distance minimale des codes duaux des BCH

[48][22]. C'est cette approche théorique qui est le point de départ de l'étude menée avec D. Augot.

J. Wolfmann a obtenu la distribution de poids de certains codes cycliques primitifs à partir de celles de codes non primitifs [24].

3.1.2 Codes primitifs dans une algèbre de groupe

Les travaux de l'équipe concernant la description des codes primitifs dans une algèbre de groupe modulaire, sont reconnus au plan international. Ils sont notamment à l'origine de la détermination des groupes d'automorphismes des codes de Reed et Muller (codes GRM) généralisés par T. Berger et P. Charpin en 92, problème qui demeurait non résolu depuis les travaux de Delsarte et al. (1969).

T. Berger a poursuivi l'étude des groupes des codes affines-invariants [8] ; ces codes sont cycliques étendus, idéaux de l'algèbre modulaire et recouvrent des classes célèbres (codes BCH ou GRM). Ses résultats récents relèvent de la théorie des groupes finis [9] [10][30]. Ils apportent des éléments décisifs pour déterminer les groupes des codes BCH (article en préparation).

P. Charpin et F. Levy-dit-Vehel ont étudié les codes autoduaux affine-invariants. Ceci a fait l'objet d'un article à paraitre dans "Journal of Combinatorial Theory"[17] ; les auteurs exhibent une classe infinie de codes autoduaux affine-invariants non equivalente à la classe des codes de Reed et Muller. Dans [18], P. Charpin étudie le comportement asymptotique d'une classe d'idéaux principaux de l'algèbre des codes primitifs.

3.1.3 Codes et combinatoire

Les *Partitions Cohérentes* ont été introduites sous le nom de *Partition Designs* dans l'article : *Weight Distribution of translates of Linear Codes and Generalized Pless Identities*, par P. Camion, B. Courteau, G. Fournier et S.V. Kanektar (1987, Journal of Information & Optimization Sciences).

La notion de *Partitions Cohérentes* a, dans un premier temps, été étendue de façon à pouvoir étudier, dans cette théorie, des codes non linéaires, définis sur un alphabet fini. Ceci a t fait dans une publication où contribua Philippe Delsarte. A. Montpetit a ensuite porté la notion

de “Partitions Cohérentes” dans le cadre plus général des graphes réguliers. Cette étude fut l'objet de sa thèse. P. Camion, B. Courteau et A. Montpetit ont continué à développer cette théorie en revenant aux applications dans les espaces de Hamming.

Dans le prolongement de ces travaux, plusieurs études furent mises en chantier. Les résultats parurent en 1992 et 1993 dans diverses publications.

Ceci nécessita l'emploi de logiciels de calcul formel. Une propriété observée suggèra une conjecture naturelle mais apparemment difficile à appréhender : quelle que soit la longueur où les codes BCH 2-correcteurs vérifient les mêmes hypothèses, les translatés auraient-ils toujours huit distributions de poids distinctes ?

La réponse affirmative est donnée par P. Charpin ; dans [20], non seulement la conjecture est démontrée mais ces distributions de poids sont données par des formules explicites. Ceci a fait l'objet d'une note à l'Académie des Sciences en 1993. P. Charpin montre dans [19] que les outils mis en place à l'occasion de cette étude, peuvent être utilisés dans un cadre plus large. Les résultats sur les codes BCH 3-correcteurs ont été présentés à ACCT4 (Novgorod, Russie) récemment [38].

Dans l'une des publications évoquées plus haut, on obtient en raffinant l'outil théorique et avec l'appui du calcul formel les distributions complètes des poids des translatés du Golay ternaire. Ceci mena à une nouvelle étude où l'on généralise de façon naturelle les schémas de Hamming. Ceci fait l'objet d'une communication à EUROCODE'94 intitulée "Weighted Hamming spaces and partition designs" [33]. On y obtient des Schémas d'Associations qui généralisent légèrement les Schémas P-polynomiaux. Ceci permet de passer de la matrice usuelle des distances d'un code à une matrice où apparaissent les poids complets de la différence d'un mot de l'espace ambiant et d'un mot de code.

Paul Camion a présenté un exposé de synthèse sur les Partitions cohérentes lors de la conférence de Cargèse organisée par le PRC Mathématiques et Informatique en octobre 1993.

Des résultats ultérieurs sur l'existence de codes à deux poids ont été obtenus par Paul Camion. Ils seront présentés lors d'une "Special Session" de l'American Mathematical Society à Richmond le 12 novembre 1994.

3.1.4 Codes et Géométrie Algébrique

Depuis les travaux de GOPPA (1960-70), on sait que les codes géométriques constituent une classe importante de codes correcteurs ; leurs "bons" paramètres et leur structure algébrique complexe les désignent naturellement pour certaines applications (construction de codes longs, protocole de protection ...). Constructions et classifications sont en cours d'étude, qui nécessitent une collaboration étroite entre Mathématiciens (spécialistes de géométrie algébrique), Théoriciens du Codage et spécialiste de Calcul Formel. L'apport des logiciels de Calcul Formel, qui dans ce contexte doivent être utilisés et même développés par des spécialistes, est très important. Le projet s'est donné les moyens, il y a deux ans de développer ce thème (collaboration avec D. Le Brigand, acquisition d'un IBM RS/6000 avec logiciel AXIOM).

D. Le Brigand poursuit l'étude systématique des corps de fonctions (quadratiques ou non) dont le nombre de classes, qui est le nombre de points rationnels de la jacobienne de la courbe associée, est égal à 2. Elle a résolu le problème pour les corps de fonctions quadratiques [47] ; un article est soumis pour publication.

A. Thiong Ly étudie les problèmes concernant les points de Weirstrass et les semi-groupes d'entiers associés, ceci en relation avec le décodage des codes géométriques [45].

G. Haché, dans le cadre de sa thèse, assiste D. Le Brigand sur l'aspect calculatoire de la construction de codes géométriques. Pour cela, il a élaboré un logiciel écrit en AXIOM. Tout ce qui est nécessaire pour la construction de codes géométriques à partir de courbes planes a été réalisé ; on peut effectuer la dessingularisation des courbes planes, le calcul du genre, le calcul des bases des espaces vectoriels $L(D)$ associés à un diviseur D et le calcul de l'ordre (et l'évaluation le cas échéant) d'une fonction en tout point de la normalisée de la courbe. L'aspect théorique et algorithmique de cette réalisation a fait l'objet d'un article écrit conjointement par G. Haché et D. Le Brigand ([64], soumis pour publication à IEEE Transactions, édition spéciale sur les codes géométriques).

F. Blanchet étudie la cyclicité des codes de Goppa, prolongeant les travaux de H. Stitchenoth [31]. Plusieurs articles sont en préparation.

J. Wolfmann s'est intéressé aux liens existant entre équations, courbes algébriques sur les corps finis et codes correcteurs. Ont été obtenus : des

bornes sur les poids des codes cycliques, une description polynomiale et des bornes pour les codes binaires, des résultats sur le nombre de solutions de certaines équations diagonales [23].

3.2 Codes correcteurs: aspects algorithmiques

3.2.1 Calcul dans les corps finis

D. Augot et G. Haché participent à l'étude et au développement du logiciel AXIOM, qui s'avère très puissant pour le calcul dans les extensions de corps finis. Le projet disposant d'un RISC 6000, participe à des réseaux de chercheurs qui testent et développent AXIOM et collabore de façon régulière avec l'équipe de D. Lazard (LITP, Paris 6). Les projets précis du groupe sont : logiciel d'exploration des mots des codes cycliques, considérés comme des polynômes sur une extension du corps à 2 éléments ; logiciel de construction de codes géométriques.

L'aboutissement du logiciel de G. Haché permet de concevoir l'étude pratique de codes. En particulier le programme d'énumération des poids de N. Sendrier peut être utilisé pour les codes géométriques. G. Haché a présenté son logiciel de construction de codes géométriques lors de deux rencontres nationales [43, 44].

Une étude algorithmique a été menée par P. Camion et D. Augot pour calculer le polynôme minimal d'un endomorphisme, ainsi que d'autres paramètres invariants (notamment les "diviseurs élémentaires"). Le problème de l'optimisation du calcul d'un vecteur cyclique a aussi été étudié. Le résultat principal est l'obtention d'un algorithme déterministe en $O(n^3)$ pour le calcul d'une base normale dans un corps fini. Les meilleurs algorithmes déterministes connus étaient de complexité $O(n^4)$. De plus un algorithme de calcul du polynôme minimal de complexité $O(n^3)$ en moyenne sur un corps fini est proposé. La complexité dans le pire des cas est de $O(n^{3.5})$, alors qu'elle était $O(n^4)$ pour les algorithmes connus. Tous ces résultats constituent donc une avancée algorithmique en algèbre linéaire sur les corps finis.

Ces algorithmes ont été implantés en AXIOM, et, bien que déterministes, sont plus rapides que les algorithmes *probabilistes* déjà existants en AXIOM, ce qui prouve la validité du point de vue de D. Augot et P. Camion. Une présentation des ces résultats théoriques et pratiques

a été faite au Rhine Workshop on Computer Algebra, à Karlsruhe [29]. Un article condensant ces résultats est soumis pour publication [65].

3.2.2 Décodage

H. Chabanne, dans le cadre de sa thèse (soutenue en Mai 93), a étudié le décodage des codes abéliens semi-simples. En collaboration avec G. Norton de l'Université de Bristol, une généralisation de l'algorithme de Berlekamp-Massey au cas abélien a été conduite [15].

Les outils dévelopés dans la thèse de N. Sendrier s'appliquent aux algorithmes de décodage des codes "produit". En s'appuyant sur des résutats théoriques d'une part et sur des simulations d'autre part il a été possible de prouver que les codes "produit" se comparent très favorablement aux classes de codes habituellement utilisés, et ce tant au niveau des taux de correction d'erreurs qu'au niveau de la complexité algorithmique de la procédure de décodage [52].

3.3 Polynôme des poids

Un logiciel permettant le calcul de l'enumérateur des poids des codes binaires linéaires et de leurs translatés a pu être mis au point. Celui-ci fait appel à des techniques algorithmiques pointues (code de Gray, polynômes de Krawtchouk pour la transformée de MacWilliams, ...), et s'est avéré performant puisqu'il a permis le calcul d'énumérateurs de poids encore inconnus. En particulier, les énumérateurs de poids de tous les codes cycliques de longueur 63 ont pu être calculés [55]. De plus l'utilisation du logiciel a permis de démontrer l'équivalence de certains codes binaires. Des études dans des domaines variés de la théorie des codes sont en cours, et ont été facilitées par l'usage de ce programme.

3.4 Codes et cryptographie

3.4.1 Fonctions booléennes

Les fonctions booléennes sont un objet de codage, au sens large: leur utilisation dans les protocoles de protection est trés importante et leurs propriétés sont celles des codes de Reed et Muller, codes de référence dans la théorie. Il s'agit là d'un des thèmes de recherche du projet, tant théorique (cf. sections précédentes) qu'en vue d'applications.

C. Carlet a présenté son habilitation à diriger des recherches cette année [4]. Les fonctions constituent le thème central de ses travaux, avec une triple orientation: théorie des codes, cryptographie, applications. Après avoir introduit et étudié une généralisation de la notion de fonction courbe, celle de fonction partiellement courbe [13], C. Carlet a obtenu deux nouvelles classes de fonctions courbes [14, 67]. D'autre part, C. Carlet poursuit ses travaux sur la dualité des codes de Kerdock et de Preparata [37].

3.4.2 Protocoles basés sur les codes correcteurs

A. Canteaut a débuté une thèse sous la direction de P. Camion. Dans ce cadre, elle a étudié avec H. Chabanne la sécurité de certains systèmes cryptographiques fondés sur les codes correcteurs d'erreurs, tels les systèmes de chiffrement de McEliece et de Niederreiter, ou le schéma d'authentification de Stern. Tous ces systèmes reposent sur la difficulté de décoder un code linéaire quelconque de grande taille en un temps raisonnable.

Une technique itérative de décodage des codes linéaires a été mise au point et a permis la conception d'un algorithme dont les performances améliorent toutes les attaques précédentes de ces systèmes cryptographiques. Un calcul théorique de la complexité de ce nouvel algorithme a permis notamment de cerner les paramètres admissibles pour les codes utilisés à des fins cryptographiques ; cette étude théorique a été validée par de nombreuses simulations [36, 60].

Anne Canteaut travaille actuellement en collaboration avec F. Chabaud, du département de Mathématiques et Informatique de l'Ecole Normale Supérieure, à l'adaptation de cette nouvelle technique à d'autres algorithmes de décodage. Cette étude a notamment conduit à une amélioration considérable des performances de décodage des codes linéaires aléatoires puisque le temps de calcul, par rapport aux algorithmes précédents, a été divisé par un facteur supérieur à 100. Un article présentant ces résultats, est actuellement en préparation.

L'étude des *codes permutés* est un autre aspect de la recherche sur les protocoles basés sur les codes correcteurs. Il s'agit de savoir dans quelle mesure l'action d'une permutation détruit la structure d'un code donné. N. Sendrier a commencé à étudier les codes concaténés. L'étude des duaux des codes concaténés et de leur distribution des poids à permis la

conception d'un algorithme permettant de retrouver une structure autorisant dans certain cas le décodage d'un code concaténé dont le support a été permuté aléatoirement [51] . Cette étude a des conséquences immédiates en cryptographie puisque qu'elle montre que l'utilisation de ces codes dans des cryptosystèmes à clé publique de type McEliece ou Niedereitter, n'est pas fiable.

4 Actions industrielles

A la demande de la société COGENIT, l'*expertise d'une fonction d'authentification* a été réalisée par le projet CODES. Cette expertise a consisté à analyser les propriétés statistiques de la fonction proposée. Une fonction à sens unique, dont la solidité au sens cryptographique a pu être mesurée, a ainsi été mise au point et validée. Ce travail a débouché sur un brevet conjoint INRIA et COGENIT déposé en début d'année 1994.

5 Contacts nationaux et internationaux

5.1 Groupes de recherche

Le projet participe à deux groupements de recherche nationaux:

- PRC *Mathématiques et Informatique*, équipe *Protection des Communication*, responsables P. Charpin & D. Le Brigand. Dans ce cadre, l'équipe a pu répondre à l'appel d'offre *Codage, Compléxité et Cryptographie*, visant à regrouper les chercheurs de ces thèmes ; le projet a massivement participé aux journées organisées à cet effet (cf. Section 5.2).
- GDR MEDICIS, équipe *Codage*, responsable J. Wolfmann.

Dans le cadre de relations suivies avec la DRET, le projet participe à une série de séminaires sur le codage – une séance par mois. Le séminaire de la DRET dont le responsable est S. Harari, est destiné à établir des liens concrets entre les chercheurs et les ingénieurs. C'est dans cet esprit aussi qu'ont été organisés les colloques EUROCODE au sein du séminaire.

Ces relations avec la DRET ont été renforcées depuis 1989 par un contrat portant sur les codes pour lignes très bruitées. En 94, plusieurs projets de

collaboration avec la DRET ont été envisagés. D'autre part un contrat est en cours de signature pour l'invitation de chercheurs russes.

5.2 Expertises

P. Camion est éditeur dans les revues suivantes :

- Discrete Mathematics,
- Journal of Information and Optimisation Science (Analytic Publishing co., DELHI),
- Applicable Algebra in Engineering, Communication and Computing (AAECC), Springer Verlag,
- Design, Codes and Cryptography (Kluwer Academic Publishers),
- Cahiers du Centre d'Etudes de Recherche Opérationnelle (Univ. Libre de Bruxelles).

J. Wolfmann est éditeur dans les revues:

- Applicable Algebra in Engineering, Communication and Computing (AAECC), Springer Verlag,
- Finite Fields : theory and applications (nouvelle revue).

Le projet participe régulièrement à l'élaboration de rapports sur des publications présentées dans des revues internationales ou pour des colloques. On peut citer notamment pour cette année, les revues *"IEEE on Info. Theory"*, *"IEEE on Communications"*, les *"SIAM Journals"*, les journaux dont des membres du projet sont éditeurs, et les colloques *EUROCRYPT* et *ISIT*.

5.3 Colloques

Les résultats obtenus par les participants au projet sont largement diffusés, dans des séminaires nationaux, à l'étranger dans les séminaires des universités visitées et dans les colloques internationaux. D'autre part, le projet s'efforce de participer aux principaux colloques ou workshops portant sur ses thèmes de recherche. Les membres du projet ont participé récemment à l'organisation de:

- *Journées PRC Math-Info, Codage Complexité et cryptographie*, 11-16 Octobre 93, Cargèse (Corse).
  Responsable du pôle *codage* : P. Charpin.

Quinze membres du projet ont participé aux journées, donnant onze conférences.

- *EUROCODE'94*, Abbaye de la Bussière, Côte d'Or, France, 24-28 Octobre 1994. Ce colloque International est majoritairement organisé par des membres du projet: P. Camion (responsable scientique), C. Carlet (organisation locale), P. Charpin (édition), S. Harari (organisation générale), N. Sendrier (aspects techniques), J. Wolfmann (bourses pour étudiants).
  Les actes du colloques sont publiés par l'INRIA. Onze membres du projet y ont participé, donnant sept conférences.

Participation à des Colloques en 94 :

- *Symposium in honor of Jim Massey's 60th birthday*, Suisse, 10-13 février 1994.
  Conférencier : T. Ericson.
- *The Rhine Workshop on Computer Algebra*, Karlsruhe, Allemagne, 22-24 mars 1994.
  Conférencier : D. Augot.
- *Workshop on Applicable Algebra*, Oberwolfach, Allemagne, 17-23 avril 1994.
  Conférencier invité : V. Zinoviev.
- *EUROCRYPT'94*, Perugia, Italie, 9-12 mai 1994.
  Conférencier : C. Carlet.
  Participants : P. Camion, A. Canteaut, P. Charpin.
- 15th Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgique, 30-31 mai 1994.
  Participants : T. Ericson, N. Sendrier.
- *Colloque IEEE on Information Theory*, Trondheim, Norvège, 27-1 juillet 1994.
  Conférenciers : D. Augot, T. Berger, C. Carlet, T. Ericson, F. Levy-dit-Vehel, N. Sendrier, J. Wolfmann, V. Zinoviev.
  Participants : P. Camion, P. Charpin.
- *CRYPTO'94*, Santa-Barbara, 21-25 août 1994.
  Participant : N. Sendrier.
- *Fourth International Workshop on Algebraic and Combinatorial Coding Theory, (ACCT-4)*, Novgorod, 11-17 septembre 1994.
  Conférencier : P. Charpin.

- *Meeting of American Mathematical Society*, 10-13 Novembre 94, Richmond, USA.
  Conférencier invité : P. Camion.

5.4 Invitations

Le projet a une politique d'invitation "large", nationale et internationale. Cette année, des jeunes chercheurs de l'Université de Toulon, (Philippe Langevin, Pascal Véron et Jean-Pierre Zanotti) ont séjourné afin de mettre en place une collaboration sur des sujets communs. Ceci devrait se poursuivre en 95.

Le projet s'efforce d'accueillir chaque année un ou deux collègues pour une durée supérieure à deux mois. Thomas Ericson, Professeur à l'Université de Linköping, Suède, a séjourné au projet *CODES* de Septembre 1993 à Juillet 1994. Victor Zinoviev, Professeur à l'Académie des Sciences de Moscou, Russie, a séjourné au projet *CODES* de Février à Septembre 1994.

D'autre part, le projet a accueilli, pour de courtes durées, en 1994 :

- Ulrich Sorger (Institut für Netzwerk and Signaltheorie, Germany),
- Iwan Duursma (Eindhoven University of Technology, The Netherlands),
- Vladimir Levenshtein (Académie des Sciences de Moscou, Russie),
- Zhe-Xian Wan (Chinese Academy of Sciences, China),
- Jennifer Key (Clemson University, USA),
- Juerg Ganz (ETH-Zentrum, Suisse)
- Simon Litsyn (Tel Aviv University, Israel),
- Edward Assmus (Lehigh University, USA),
- Bernard Courteau (Université de Sherbrooke, Canada),
- Jim Massey (Ecole polytechnique de Zurich).

5.5 Contacts universitaires

Le projet *CODES* entretient des relations suivies avec de nombreux organismes d'enseignement et/ou de recherche français et étrangers. Particulièrement, cette année :

- Télécom Paris,
- Laboratoire d'Informatique Théorique et de Programmation (LITP, Paris 6),
- Laboratoire LIENS de l'ENS-Ulm (groupe GRECC).
- l'Université de Limoges (Dpt. Math.),
- le Groupe d'Etude du Codage de Toulon (GECT),
- L'Université de Sherbrooke (Québec),
- L'Université de LEHIGH (USA),
- L'Ecole Polytechnique de Zurich (Suisse)
- l'Université de Louvain (Belgique).

Plusieurs chercheurs du projet appartiennent à ces différents organismes d'enseignement et de recherche ; collaboration scientifique et échanges se sont poursuivis en 1994, notamment à l'occasion des séminaires de l'INRIA (projet CODES), l'ENST (G. Cohen), l'ENS-Ulm (J. Stern), de Toulon (J. Wolfmann) et Limoges (T. Berger).

D. Augot organise avec J.C. Faugère un séminaire sur AXIOM, à la demande de la communauté nationale. Ce séminaire a lieu à Jussieu tous les mois (équipe de D. Lazard, LITP).

Dans le cadre de la collaboration avec l'Université de Sherbrooke, D. Augot a été invité deux mois par B. Courteau au Québec, dans le but de faire bénéficier l'équipe de B. Courteau de notre expérience acquise en AXIOM.

D. Le Brigand et P. Charpin assurent un enseignement sur les codes correcteurs d'Erreurs dans la DEA Informatique et Théorique, Calcul et Programmation, organisé par Paris 6 sous la direction de J. Sakarovitch.

Les chercheurs de 3ème cycle du projet sont inscrits dans la formation doctorale suivant ce DEA et associés à l'équipe n^{o}3 du LITP (Calcul Formel et Algorithmique, responsable : D. Lazard).

D. Augot, P. Charpin et N. Sendrier, assurent un enseignement dans le DEA "Informatique Mathématique et Applications" (X - Ulm - Paris 6 - Paris 7, filière Cryptographie).

J. Wolfmann et S. Harari participe à la formation Doctorale "Informatique et Mathématiques" de l'Université de Marseille-Luminy et assurent les cours de "Codage" et de "Cryptographie".

Le projet *CODES* a accueilli cette année 2 stagiaires.

Les membres du projet CODES ont participé à plusieurs jurys de thèse fin 93 et en 94 :

Décembre 93 D. AUGOT, Thèse d'Université de Paris 6.
Jury : P. Charpin (direction), P. Camion, J. Wolfmann (rapporteur).

Janvier 94 J.-P. MARTIN, Thèse d'Université de Toulon.
Jury : J. Wolfmann (direction), P. Camion, P. Charpin (rapporteur).

Janvier 94 J.-P. TILLICH, Thèse d'Université ENST.
Jury : P. Camion (rapporteur).

Février 94 C. CARLET, Habilitation, Université de Picardie.
Jury : P. Charpin (direction), P. Camion (rapporteur).

Mai 94 B. PEIRANI, Thèse d'Université de Marseille-Provence.
Jury : P. Charpin.

Mai 94 I. WOUNGANG, Thèse d'Université de Toulon.
Jury : P. Charpin, N. Sendrier.

Octobre 94 F. LEVY-DIT-VEHEL, Thèse d'Université de Paris 6.
Jury : P. Charpin (direction), P. Camion, E. Assmus.

6 Publications

Livres et monographies

[1] P. CHARPIN, J. STERN (réd.), *Complexité, Codage, Compression, Cryptographie, Actes des Journées de Cargèse, 10-16 Octobre 93*, INRIA, 1994. A paraître.

[2] P. CHARPIN (réd.), *EUROCODE'94*, INRIA, 1994. A paraître.

Thèses

[3] D. AUGOT, *Etude algébrique des mots de poids minimum des codes cycliques, méthodes d'algèbre linéaire sur les corps finis*, Thèse de doctorat, Université Paris 6, décembre 1993.

[4] C. CARLET, *Fonctions booléennes en théorie des codes correcteurs d'erreurs et en cryptologie*, Habilitation à diriger des recherches, Université de Picardie, février 1994.

[5] F. Levy-dit-Vehel, *Divisibilité des codes cycliques : Applications et prolongements*, Thèse de doctorat, Université Paris 6, octobre 1994.

Articles et chapitres de livre

[6] D. Augot, P. Camion, «Forme de Frobenius et vecteurs cycliques», *Compte Rendus de l'Academie des Sciences de Paris t.318*, Serie I, 1994.

[7] D. Augot, N. Sendrier, «Idempotents and the BCH bound», *IEEE Transaction on Information Theory 40*, 1, 1994, p. 204–207.

[8] T. Berger, «The automorphism group of double-error-correcting BCH codes», *IEEE Transaction on Information Theory 40*, 2, 1994, p. 538–542.

[9] T. Berger, «Classification des groupes de permutations d'un corps fini contenant le groupe affine», *Compte Rendus de l'Academie des Sciences de Paris t.319*, Serie I, 1994, p. 117–119.

[10] T. Berger, «On the automorphism groups of affine-invariant codes», *Designs Codes and Cryptography*, 1994, A paraître.

[11] C. Carlet, J. Seberry, X.-M. Zhang, «Comments on generating and counting binary bent sequences», *IEEE Transaction on Information Theory 40*, 2, 1994, p. 600.

[12] C. Carlet, «The divisors of $x^{2^m}+x$ of constant derivatives and degree 2^m-2», *SIAM Journal on Applied Mathematics*, 1994, A paraître.

[13] C. Carlet, «Partially bent functions», *CRYPTO'92, LNCS*, 740, Springer-Verlag, 1993, p. 280–291.

[14] C. Carlet, «Two new classes of bent functions», *EUROCRYPT'93, LNCS*, 765, Springer-Verlag, 1994, p. 77–101.

[15] H. Chabanne, G. Norton, «The n-dimensional key equation and a decoding application», *IEEE Transaction on Information Theory 40*, 1, 1994, p. 200–203.

[16] H. Chabanne, «Factorizing x^n-1 over finite fields of even characteristic», *AAECC*, 1994, A paraître.

[17] P. Charpin, F. Levy-dit-Vehel, «On self-dual affine invariant codes», *Journal of Combinatorial Theory, Série A 67*, 2, 1994, p. 223–244.

[18] P. Charpin, «Self-dual codes which are principal ideals of the group algebra $\mathbf{F}_2[\{\mathbf{F}_{2^m},+\}]$», *The Journal of Statistical Planning and Inference, special volume : Affine Designs, Orthogonal Arrays and Related Topics*, 1994, A paraître.

[19] P. Charpin, «Tools for cosets weight enumerators of some codes», *Proceedings of the Second International Conference on Finite Fields : Theory, Applications and Algorithms, Las Vegas, 17-21 août 1993. Publications de l'AMS*, 1994, A paraître.

[20] P. Charpin, « Weight distribution of cosets of 2-error correcting binary BCH codes, extended or not », *IEEE Transaction on Information Theory*, 1994, A paraître.

[21] D. Lebrigand, « Quadratic algebraic function fields with ideal class number two », *Proceedings, AGCT4, Walter de Gruyte*, 1994, A paraître.

[22] F. Levy-dit-Vehel, « Bounds on the minimum distance of the duals of extended BCH codes over $\mathbf{F}_p$ », *AAECC*, 1994, A paraître.

[23] J. Wolfmann, « New results on diagonal equations over finite fields », *Proceedings of the Second International Conference on Finite Fields : Theory, Applications and Algorithms, Las Vegas, 17-21 août 1993. Publications de l'AMS*, 1994, A paraître.

[24] J. Wolfmann, « Weight distribution of some primitive binary primitive cyclic codes », *IEEE Transaction on Information Theory*, 1994, A paraître.

Communications à des congrès, colloques, etc.

[25] D. Augot, P. Camion, « A deterministic algorithm for computing a normal basis in a finite field », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[26] D. Augot, F. Levy-dit-Vehel, « Bounds on the minimum distance of the duals of BCH codes », *in : IEEE International Symposium of Information Theory*, p. 43, Trondheim, Norvège, juin 1994.

[27] D. Augot, « Présentation d'un algorithme d'approche de la distance minimale de codes cycliques », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargèse, Corse, France, octobre 1993.

[28] D. Augot, « Algebraic characterization of minimum weight codewords cyclic codes », *in : IEEE International Symposium of Information Theory*, p. 46, Trondheim, Norvège, juin 1994.

[29] D. Augot, « Computing normal bases in finite field », *in : The Rhine Workshop on Computer Algebra*, Karlsruhe, Allemagne, mars 1994.

[30] T. Berger, « On the automorphism groups of affine-invariant codes », *in : IEEE International Symposium of Information Theory*, p. 426, Trondheim, Norvège, juin 1994.

[31] F. Blanchet, « Régularité des codes de Goppa binaires », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargèse, Corse, France, octobre 1993.

[32] A. Calderbank, V. Zinoviev, « On nonisomorphic 2-resolvable Steiner quadruple systems », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[33] P. Camion, B. Courteau, A. Montpetit, « Weighted Hamming spaces and partition designs », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[34] P. Camion, « On R-partition designs and weight distribution of cosets », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargèse, Corse, France, octobre 1993.

[35] P. Camion, « Partition designs and two-weight codes », *in : Conférence American Mathematical Society*, Richmond, Virginia, USA, 11-13 novembre 1994.

[36] A. Canteaut, H. Chabanne, « A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[37] C. Carlet, « On the formal duals of Kerdock codes », *in : IEEE International Symposium of Information Theory*, p. 428, Trondheim, Norvège, juin 1994.

[38] P. Charpin, V. Zinoviev, « On weighted distributions of the cosets of the 3-error-correcting extended BCH-codes of length 2^m, m odd », *in : Fourth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-4)*, Novgorod, Russie, septembre 1994.

[39] T. Ericson, V. Zinoviev, « Spherical codes by balanced $Y4$ construction », *in : Fourth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-4)*, Novgorod, Russie, septembre 1994.

[40] T. Ericson, V. Zinoviev, « Spherical codes from unsymmetric alphabets », *in : 15th Symposium on Inform. Theory in Benelux*, Louvain-la-Neuve, Belgique, may 1994.

[41] T. Ericson, « Spherical codes : a tutorial », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[42] T. Ericson, « Spherical codes from the hexagonal lattice », *in : Symposium in honor of Jim Massey's 60th birthday*, Suisse, février 1994.

[43] G. Haché, « Eléments de calcul pour la construction des codes géométriques », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargèse, Corse, France, octobre 1993.

[44] G. Haché, « Construction de codes géométriques à l'aide d'AXIOM: aspects utiles du logiciel », *in : Conférence au Séminaire AXIOM (NAG)*, Ecole Nationale Supérieure des Télécommunications, Paris, France, mai 1994.

[45] T. Henocq, A. Thyong-Ly, « Distance de Feng et Rao de certains codes », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[46] V. KUMAR, O. MORENO, V. ZINOVIEV, « The exact minimum distance of some cyclic codes », *in : IEEE International Symposium of Information Theory*, p. 50, Trondheim, Norvège, juin 1994.

[47] D. LEBRIGAND, « Corps de fonctions de nombre de classe 2 », *in : Journées Arithmétiques*, Caen, mai 1994.

[48] F. LEVY-DIT-VEHEL, « Bornes sur le poids minimal de duaux de codes BCH étendus sur $GF(p)$ », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargése, Corse, France, octobre 1993.

[49] O. MORENO, D. POLEMI, V. ZINOVIEV, D. ZINOVIEV, « On algebraic geometric codes from singular projective curves over $GF(2^m)$ », *in : IEEE International Symposium of Information Theory*, p. 157, Trondheim, Norvège, juin 1994.

[50] N. SENDRIER, « Polynôme des motifs corrigibles des codes concaténés », *in : Rencontre sur la Complexité, Codage et Cryptographie*, Cargése, Corse, France, octobre 1993.

[51] N. SENDRIER, « On the structure of a randomly permuted concatenated code », *in : EUROCODE'94*, Côte d'Or, France, 24-28 octobre 1994.

[52] N. SENDRIER, « Polynomial of correctable patterns of product codes », *in : IEEE International Symposium of Information Theory*, p. 245, Trondheim, Norvège, juin 1994.

[53] W. WAFO, J. WOLFMANN, « Cyclic q-ary images of codes and burst correction », *in : IEEE International Symposium of Information Theory*, p. 49, Trondheim, Norvège, juin 1994.

[54] V. ZINOVIEV, « On Preparata like codes and 2-resolvable Steiner systeme », *in : International Designs and Codes*, Oberwolfach, Allemagne, avril 1994.

Rapports de recherche et publications internes

[55] D. AUDIBERT, N. SENDRIER, « Weight distribution of the binary cyclic codes of length 63 », *Rapport de recherche*, INRIA, 1994, A paraître.

[56] D. AUDIBERT, *Programmes d'évaluation par méthodes combinatoires des performances des codes correcteurs d'erreurs et d'effacements*, Rapport de stage, ESA IGELEC, 1993, 175 pages.

[57] D. AUGOT, « Description of minimum weight codewords of cyclic codes by algebraic systems », *Rapport n° 134*, Université de Sherbrooke, 1994.

[58] F. BIHAN, *Codes cycliques sur les entiers p-modulaires et sur les entiers p-adiques*, Mémoire de DEA, Université de Rennes, 1994.

[59] G. BOMMIER, *Un logiciel dédié aux codes de Goppa*, Mémoire de DEA, ENS Ulm et Université Paris 6, 1994.

[60] A. CANTEAUT, H. CHABANNE, «A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem», *Rapport de Recherche n°2227*, INRIA, 1994.

[61] P. CHARPIN, «Self-dual codes which are principals ideals of the group algebra $\mathbf{F}_2[\{\mathbf{F}_{2^m}, +\}]$», *Rapport de recherche*, INRIA, 1994, A paraître.

[62] P. CHARPIN, «Weight distribution of cosets of 2-error correcting binary BCH codes, extended or not», *Rapport de Recherche n°2228*, INRIA, 1994.

[63] T. ERICSON, «Permutation codes», *Rapport de Recherche n°2109*, INRIA, 1994.

[64] G. HACHÉ, D. LEBRIGAND, «Effective construction of algebraic geometry codes», *Rapport de Recherche n°2267*, INRIA, 1994.

Divers

[65] D. AUGOT, P. CAMION, «The minimal polynomials, characteristic subspaces, normal bases and the Frobenius form», 1994, Soumis pour publication - RR 2006, 1993.

[66] T. BERGER, «Classification des permutations d'un corps fini contenant le groupe affine», 1994, Soumis pour publication.

[67] C. CARLET, «Partial spreads généralisés», 1994, Soumis pour publication.

[68] A. THYONG-LY, «Quasi-cyclic codes on the Klein Quatric over $GF(2^r)$ a procedure for correcting 1 or 2 errors», 1993, Soumis pour publication.

7 Abstract

The research area of the CODES project remains focused on Error-Correcting Codes. The project has however a double aim : developing fundamental research in Coding Theory as well as placing itself in the application area of "Information protection".

By and large, the studies we are concerned with provide conditions for practical applications of error-correcting coding for transmission and storage of data in modern telecommunication and data storage systems. They include investigations of potential areas of coding applications and of the ways of providing high error-correcting capacity under random and specific noise.

Table des matières