$2^{ème}$ atelier annuel sur la cryptographie, Algèbre et Géométrie

Livret des résumés

Cours

SAGE et théorie des groupes

LEMDJO DJIODOP Guy Roger, MINDJA Habibatou, TIEUDJO Daniel
Université de Ngaoundéré

Résumé:
SAGE : Un environnement mathématique pour l'enseignement et la recherche
SAGE est un système de calcul formel, capable d'effectuer des calculs arithmétiques, algébriques, géométriques, ... Il permet d'expérimenter, de tester ou de valider des propriétés de l'algèbre, de la géométrie algébrique, de la théorie des nombres, etc. SAGE intègre d'autres interfaces de logiciels propriétaires comme GAP, MAXIMA, MAGMA, MAPLE, PARI, etc. SAGE est une plateforme adaptée pour l'enseignement et la recherche.
Ce cours donne les généralités sur l'utilisation de SAGE en théorie des nombres, géométrie algébrique (corps, courbes elliptiques), sur l'intégration de GAP pour la théorie des groupes et de MAPLE pour la résolution des systèmes polynomiaux.

Ce cours-TP se subdivise en 3 parties :

1. Présentation de SAGE (SAGE et arithmétique)
2. Géométrie algébrique (corps, courbes elliptiques)
3. Théorie des groupes et SAGE : intégration de GAP dans SAGE

Théorie de Galois

NKUIMI-JUGNIA Célestin
Université de Yaoundé I

Résumé: Ce cours vise à introduire la théorie de Galois et présenter les différentes applications en arithmétique, géométrie, algèbre et informatique. Il sera aussi dressé un état de l'avancement de la recherche dans ce domaine

Environnement de calcul distribué

YENKE Blaise
Université de Ngaoundéré

Résumé: Des algorithmes séquentiels et parallèles ont été (et sont encore) développés pour résoudre des problèmes scientifiques clairement formulés. Jusque dans les années 80, ces algorithmes étaient exécutés sur des machines uniques qui pouvaient être mono ou multiprocesseur (supercalculateur). Ces machines parallèles étaient peu tolérantes aux fautes et n'étaient pas à la portée de tous du fait de leur coût élevé. Depuis près de 20 ans, le développement des réseaux hauts débits et des ordinateurs standards a permis de construire de nouvelles architectures de machines de calcul haute performance à moindre coûts : les grappes/grilles de calcul.

Les grappes et les grilles de calcul font partie de la famille des environnements de calcul distribué. La principale différence entre ces environnements et les supercalculateurs réside au niveau de l'exécution des applications, à savoir en parallèle. Dans les environnements distribués, les applications sont chargées sur chaque machine et peuvent communiquer (dans le cas d'une application parallèle) au moyen des canaux de communication dans le réseau.

Le calcul parallèle est une méthode qui consiste à décomposer un problème en de petites unités qui sont exécutées en parallèle, prenant ainsi une fraction du temps nécessaire à l'exécution du même problème sur un PC standard..

Les environnements de calcul distribué offrent un bon rapport coût / performance, mais leur utilisation ouvre un grand nombre de question que l'on peut se poser : comment sont construits ces types de systèmes ; comment implanter efficacement de tels systèmes pour obtenir les performances attendues ; quel type de système d'exploitation pour ces environnements ; quel type de logiciels sont disponibles pour les utilisateurs de ce type de machine et comment pouvons-nous utiliser ces logiciels sur d'autres ordinateurs construits en utilisant la même la technologie ; peut-on utiliser les applications existantes ou faut-il en créer de nouvelles, si oui, comment ; comment pouvons-nous veiller à ce que chaque PC fait sa juste part de travail, ou qu'un n'est pas surchargé ; comment exécuter une application sur ce type de machine ?

Ce cours introductif prévu en trois leçons explore ces questions de la théorie à la pratique. Dans le premier exposé, nous présenterons les concepts fondamentaux des environnements distribués et la mise en place de ce types de systèmes. Les deux leçons qui suivront seront pratiques et visent à initier les auditeurs à l'utilisation des machines à mémoire distribuée.

Avant-Projets de thèse

Implantation des cryptosystèmes basés sur les groupes des tresses

BOUDJOU Hortense
Université de Maroua

Résumé: Les groupes de tresses présentent plusieurs problèmes difficiles qui sont à l'origine d'un bon nombre de schémas cryptographiques (cryptosystèmes). Cependant, l'utilisation quotidienne de ces cryptosystèmes au sein du commerce électronique, des systèmes embarqués tels les cartes à puces, l'électronique automobile, ou même la radio logicielle reste encore un défi. Cet exposé présente un avant projet de thèse sur le thème : implantation des cryptosystèmes basés sur les groupes des tresses. Un état de l'art sur le sujet est dressé, une problématique dégagée et un plan de rédaction de la thèse est proposé.

Cryptographie des images

CIDJEU Didérot
Université de Ngaoundéré

Résumé: De nos jours une grande masse d'informations est représentée sous formes d'images. Celles-ci transitent sur des canaux peu ou pas sécurisés. Plusieurs mécanismes/algorithmes cryptographiques sont proposés pour la sécurisation des images. Cependant, lors des traitements (transfert, transport, segmentation...) des images, ces algorithmes ne répondent pas toujours aux problèmes de sécurité (conservation, intégrité...). De plus, le poids des données de type images reste encore un problème lors du transfert de l'image et sa manipulation dans des domaines tels que l'imagerie médicale, la sécurité routière... Cet exposé présente un avant projet de thèse portant sur « La Cryptographie des images ». Un état de l'art sur la sécurisation des images sera présenté, une problématique sera dégagée ainsi qu'un plan de rédaction de thèse.

Groupes profinis et applications

MANTIKA Gilbert
Université de Ngaoundéré

Résumé: Les groupes profinis sont connus depuis 1964 lorsque J.P.Serre l'a exposé dans son livre intitulé *Cohomologie Galoisienne*. Ces groupes profinis sont très riches parce qu'ils possèdent à la fois des propriétés algébriques et topologiques. Ils sont de ce point de vue, vus sous trois aspects. D'abord un

groupe profini est une limite projective d'un système projectif de groupes finis. Ensuite c'est un groupe topologique compact, de Haussdorf et totalement déconnecté. Enfin un groupe profini est aussi vu comme groupe de Galois d'une extension galoisienne de corps. L'étude des groupes profinis constitue un thème de recherche actuel très intéressant. De nos jours les groupes profinis ont été généralisés aux groupes pro-$\mathcal{C}$ où $\mathcal{C}$ désigne une classe abstraite de groupes. Lorsque $\mathcal{C}$ désigne la classe de tous les groupes finis, tous les p-groupes finis (p nombre premier donné), tous les groupes nilpotents et tous les groupes résolubles, on parle de profini, pro-p, pro-nilpotent et pro-résoluble respectivement.

Le but de ce travail est de présenter l'avant projet de thèse qui s'intitule Groupes Profinis et Applications. Ce travail qui est une investigation sur les groupes profinis, dresse un état de l'art de la recherche sur les groupes profinis, sur l'étude des constructions libres des groupes profinis, l'étude sur ces objets des propriétés résiduelles, des endomorphismes, des automorphismes et des calculs des complétés profinis.

Communications

Comparing watermarked CFA (Color Filter Array) images and watermarked color images

ABENA NDONGO Herve[1], BARZINA Robert[1,2], BITJOKA Laurent[1], BOUKAR Ousman[1]

[1]Équipe de Recherche Modélisation, Traitement d'Images et Applications (MOTRIMA)
Laboratoire Signal, Image, Automatique et Biosystèmes (SIAB)
Département Génie Électrique, Énergétique et Automatique
École Nationale Supérieure des Sciences Agro-Industrielles (ENSAI)
Université de Ngaoundéré BP 455, Cameroun
[2]Département Informatique et Télécommunications
Institut du Sahel B.P. 46 Maroua
Université de Maroua

Abstract: The aim of this work was to compare the watermarking of CFA (Color Filter Array) images with the watermarking of color images. To achieve this goal, watermarking according to additive and substitutive methods in the fields space and frequently was implemented. The CFA watermark and its corresponding color image were imbedded respectively in CFA image and its corresponding color image. Then the watermarked CFA images and color images performance were evaluated by the mean square error (MSE) between original image and watermarked image, the power signal to noise ratio ($PSNR$) between original image and watermarked image, and the coefficient of correlation (CC) between the original watermark and the watermark extracted after watermarking with and without attack. The results obtained showed that the quality of watermarked CFA images ($PSNR = 39.9, MSE = 5.0$) is comparable with the quality of an image watermarked color images ($PSNR = 43.1, MSE = 2.9$) whereas watermarked CFA images resist more to attacks by rotation or directional filtering ($CC = 0.9994; CC_R = 0.5099; CC_F = 0.8244$) than the watermarked color images ($CC = 0.9999; CC_R = -0.4276; CC_F = 0.6873$).

Keywords: Digital watermarking, CFA images, color images, robustness.

CReVote : Un nouveau système de vote électronique résistant à la coercition basé sur les courbes elliptiques

AMBASSA Pacôme Landry
Université de Ngaoundéré

Résumé: Le vote électronique est un système électoral qui permet de s'exprimer de manière anonyme dans un environnement informatique. Son but est de faire mieux que le vote classique. Un protocole de vote pour être utilisable en pratique, doit assurer de nombreuses propriétés de sécurité parmi lesquelles la résistance à la coercition, qui implique que l'électeur ne doit pas être influencé lors de l'émission de son vote, le receipt-freeness, qui protège contre l'achat des votes. Nous présentons CReVote, un nouveau protocole cryptographique de vote électronique résistant à la coercition. Afin de satisfaire cette propriété nous avons défini un crédit anonyme qui est un jeton cryptographique représenté par une signature agrégée (signature de Boneh modifiée) et qui est transmis à l'électeur lors de la phase d'enregistrement par les autorités. L'anonymat repose sur le secret entre l'électeur et l'autorité d'enregistrement. Notre protocole utilise les systèmes cryptographiques sur les courbes elliptiques.

Mots-Clés: Vote électronique, Résistance à la coercition, Crédit anonyme, Courbes elliptiques.

Arithmetic of a new Edwards model of elliptic curves defined over any finite field

DIAO Oumar[1], **FOUOTSA Emmanuel**[2]
[1]Université de Rennes I, Laboratoire IRMAR Campus de Beaulieu,
35042 Rennes Cedex, France, oumar.diao@univ-rennes1.fr
[2]Département de Mathématiques, Université de Bamenda,
Ecole Normale Supérieure, BP 39, Bamenda-Cameroun,
emmanuelfouotsa@prmais.org

Abstract: The initial Edwards model for elliptic curves over non-binary fields, with equation $x^2 + y^2 = c^2(1 + x^2y^2)$ described by Edwards in [5] has been generalised by Bernstein and Lange in [1] to the model defined by the equation $x^2 + y^2 = c^2(1 + dx^2y^2)$ over non-binary fields. Several models over binary fields (see [2, 3, 6]) [6]) have been introduced but without any connection with the initial model. In his thesis, Diao in [4, chapter 7] introduced a new binary Edwards model which is deduced from the well known Edwards model but the addition law is not efficient and not unified. In this chapter, we present an Edwards model for elliptic curves defined over any finite field and in particular over fields of characteristic 2. This Edwards model is birationally equivalent to the well known Edwards model over non-binary fields. For this, we use theta functions of level 4 to obtain a model of elliptic curve that we will call

a level 4 theta model. This model enables us to obtain our new Edwards model. We study the arithmetic of these curves. We show that the group law, obtained by the Riemann relations of theta functions, is complete and unified. In particular, the addition in characteristic 2 and the differential addition on the Kummer lines of theses curves are competitive.

Keywords: Elliptic curve, level 4 theta model, Edwards model, efficient arithmetic, theta functions, Riemann relations.

References

[1] D. Bernstein and T. Lange, Faster Addition and Doubling on Elliptic Curves, *Springer Berlin/ Heidelberg. vol. 4833 of LNCS pp. 29-50* (2008) (cit. on p. 1).

[2] D. J. Bernstein et al. Twisted Edwards curves. In: *AFRICACRYPT 2008, Vol. 5023 of LNCS,Springer, pp. 389-405* (2008) (cit. on p. 1).

[3] D.J. Bernstein, T. Lange, and R.R. Farashahi. Binary Edwards curves. In: *CHES 2008, Vol. 5154 of LNCS, Springer, pp. 244-265 (2008)* (cit. on p. 1).

[4] 0. Diao. Quelques aspects de l'arithmétique des courbes hyperelliptique de genre 2. PhD thesis. Université de Rennes 1 - France, 2010 (cit. on p. 1).

[5] H. M. Edwards. A normal form for elliptic curves. In: *Bulletin of the AMS 44(2007), pp. 393-422, URL: http:// www.ams.org/ bul l/ 2007-44-03/ S0273-0979-07-01153-6/ home.html* (2007)(cit. on p. 1).

[6] H. Wu, C. Tang, and R. Feng. A New Model of Binary Elliptic Curves with Fast Arithmetic. In: *Cryptology ePrint Archive, Report 2010/608 (2010). http://eprint.iacr.org/* (cit. on p. 1).

Étude de stabilité d'un modèle de transmission du paludisme: une implémentation sous SAGE

DJATCHA YALEU Ghislain
Université de Ngaoundéré

Résumé: Pour un modèle général de transmission du paludisme qui embrasse plusieurs configurations parmi les configurations classiques SEI, SEIR, SIR... connues en modélisation compartimentale, nous tirons profit de la plateforme SAGE pour faire l'étude qualitative des systèmes dynamiques ainsi décrits. De la recherche des équilibres qui nécessite la résolution d'un système d'équations polynomiales multivariées à la détermination des conditions seuils d'existence et de stabilité de ces équilibres, on fait appel à l'algorithme de calcul d'une base de Groebner et aux outils de calcul matriciel présents sous SAGE.

Mots-Clés: Systèmes dynamiques, base de Groebner, nombre de reproduction de base, matrice de Metzler, M-matrice.

Probabilité sur les groupes des tresses: Applications en cryptographie

DJIMNAIBEYE Sidoine
Univertsité de N'Djamena

Résumé: Dans sa thèse intitulée *Probability on graphs and groups : theory and applications* (2009), Mosina introduit la notion d'ensemble moyen ("mean-set") d'un graphe (un groupe ou une variable aléatoire). En utilisant ce concept, une généralisation de la loi forte des grands nombres sur les graphes (groupes) a été prouvée. Une analyse du protocole d'authentification basé sur les tresses montre que ce protocole ne respecte pas la propriété de non divulgation d'information. L'attaque par le "mean-set"présentée permet de rendre vulnérable le schéma d'authentification de Sibert, sans toutefois résoudre le problème difficile sous-jacent. Une amélioration de cette attaque conduit aux mêmes résultats mais avec un gain en temps considérable.

Sur les b-variétés de Poisson

Dongho Joseph
Université de Maroua

Résumé: Cette note est consacrée à l'étude algébro-géométrique des structures de Poisson dont l'application Hamiltonienne associée est à image dans le faisceau des champs de vecteurs logarithmiques le long d'un diviseur non nécessairement à croisements normaux. Après une brève présentation de ce

qu'est une algèbre de Poisson, nous revisitons, via K.Saito, la théorie des diviseurs libres; puis nous montrons que les b-variétés de Poisson introduites par Atiyah et Gualthiery sont un cas particulier des structures de Poisson logarithmiques.

Modélisation et simulation du système de production par les réseaux de pétri différentiels: Cas de la meunerie des brasseries

FOHOUE kennedy
Ecole Nationale des Sciences Agro-Industrielles
Université de Ngaoundéré

Résumé: De nos jours, les systèmes de production sont de plus en plus complexes. Leur comportement est très souvent décrit par des équations différentielles (non linéaires). Cependant obtenir un modèle de ces systèmes peut s'avérer difficile. L'approche multimodes et les réseaux de pétri représentent une alternative intéressante pour résoudre ce problème. Ce travail aborde la modélisation et la simulation par les réseaux de pétri différentiels du système de production de la meunerie des brasseries. La modélisation permet de connaître le procédé sur l'ensemble des modes de fonctionnement. La simulation quant à elle nous permet d'évaluer les performances du modèle. Cette méthode permettra d'élaborer des stratégies de supervision du système de production.

Mots-Clés: Multimode, réseau de pétri différentiel, système de production.

Fonctions floues

KOGUEP NJIONOU Blaise
Université de Yaoundé I

Résumé: Un sous-ensemble flou A d'un univers X est donné par sa fonction d'appartenance $\mu_A : X \to [0,1]$.
Une relation floue de X vers Y est un sous-ensemble flou du produit cartésien de X par Y.
Après le rappel sur la théorie des sous-ensembles flous, nous définissons une fonction floue comme étant une relation floue extensionnelle.

New results in BL-algebras

LELE Celestin
University of Dschang

Abstract: The aim of this work is to introduce a new concept of ideals and addition in BL-algebras which has been an open problem for about 20 years. In fact, in the theory of MV-algebras [1, 8], like in various algebraic structures, the notion of ideal is central, while in BL-algebras [3], the focus has been shifted to deductive systems that are also called filters. The study of BL-algebras has experienced a tremendous growth over the recent years and the main object of study has been deductive systems. It is currently a very active research area. However, the shift to deductive systems rather than keeping ideals as in MV-algebras had never been reasonably justified, though some authors such as E. Turunen and S. Sessa in [9] had blamed this on a lack of suitable algebraic addition in BL-algebras. Nevertheless, several pioneers in the field, e.g. A. Di Nola, S. Sessa, F. Esteva, L Godo, P. Garcia in [2] and others researchers [4] had acknowledged the fact that the notion of ideal was still missing in BL-algebras. To fill this gap, which was long overdue, we have initiated the study of ideals and addition in BL-algebras that allow us to better understand the gap that separates MV-algebras from BL-algebras. This newly introduced notion of ideal in BL-algebras behaves quite differently from deductive systems and yields richer structures than those obtained from deductive systems. For future work, we could use the new concepts of BL-ideal and addition in BL-algebras to to lift some results from MV-algebras to Bl-algebras, MTL-algebras [11], residuated lattice and study other types of BL-ideals and establish some logic consequences. Moreover, there is clearly a big potential in this approach and interesting results in [5, 6, 7, 10]. It is now clear that with the introduction of addition and ideal, BL-algebra and related structure such as residuated lattice, MTL-algebras and pseudo-BL-algebras will be considered with a renewed attention.

References

[1] R. Cignoli, I.M.L Ottaviano and D. Mundici, Algebraic foundations of many-valued reasoning, *Kluwer Academic, Dordrecht*(2000).

[2] A. Di Nola, S. Sessa, F. Esteva, L. Godo and P. Garcia, The variety generated by perfect BL-algebras: An algebraic approach in fuzzy logic setting, *Ann. Math. Artif. Intell* ***35***,197-214(2002).

[3] P. Hájek, Metamathematics of fuzzy logic, *Kluwer Academic Publishers, Dordrecht*(1998).

[4] L.Z. Liu and K.T. Li, Fuzzy Boolean and positive implicative Filters of BL-algebra, *Fuzzy sets and Systems* ***152*** 333-348(2005).

[5] C. LELE and J.B. Nganou, MV-algebras derived from ideals in BL-algebras, *Fuzzy sets and Systems* (to appear)

[6] C. LELE, J.B. Nganou and E. Turunen, Some new properties of BL-algebras, *Preprint*

[7] C. LELE and J.B. Nganou, Spectral topology for BL-Algebras, *Preprint*

[8] D. Mundici, Mapping abelien l-groups with strong unit one-to-one into MV-algebras, *J. Algebra,* ***98*** 76-81(1986).

[9] E. Turunen and S. Sessa, Local BL-algebras, ,*Multi-Valued Logic* ***6***, 229-249(2000).

[10] E. Turunen, C. Nganteu and C. LELE, A new characterization of n-fold positive implicative BL-logics, *Advances on computationnal intelligence, communications in computer and information science* ***297***, 552-560(2002)

[11] T. Vetterlein, MTL-algebras arising from partially ordered groups, *Fuzzy sets and Systems* ***161*** 433-443(2010).

Nouveaux problèmes difficiles dans les groupes des tresses: problème de conjugaison multiple et problème de conjugaison par décalage multiple.

NANGA Joseph Fridolin
Université de Ngaoundéré

Résumé: L'exposé s'inscrit dans la thématique de la cryptographie algébrique, notamment la construction des cryptosystèmes sur les groupes des tresses. Nous présentons les problèmes de conjugaison multiple et de conjugaison par décalage multiple, ainsi que quelques cryptosystèmes reposant sur ces problèmes. Nous faisons la conjecture que les problèmes de conjugaison multiple et de conjugaison par décalage multiple sont plus difficiles que les problèmes de conjugaison et de conjugaison par décalage respectivement.

Une méthode de construction d'une signature logarithmique sur le groupe des tresses pures

NZOMOU Terrance
Université de Ngaoundéré

Résumé: Nous présentons dans cet exposé une nouvelle méthode de construction de signature logarithmique sur le groupe des tresses pures. Une suggestion pour une application à MST1 est proposée.

Mots-Clés: Signature logarithmique, groupe des tresses, MST1.

Quelques exemples non-triviaux d'anneaux chrysippiens θ-valents (ach θ)

TSIMI Jean Armand
Université de Douala

Résumé: L'anneau chrysippien θ-valent (ach θ) est la structure servant de modèle algébrique d'une logique ayant à la fois un caractère multivalent (θ-valent) et bivalent classique (chrysippien) : logique modale θ-valente chrysippienne. L'objectif de cette note est de présenter quelques exemples d'anneaux chrysippiens θ-valents en vue d'une implémentation à venir.

Décembre 2012