Université de Dschang
The University of Dschang

Université de Ngaoundéré
The University of Ngaoundere

$4^{ème}$ atelier annuel sur la cryptographie, Algèbre et Géométrie

4^{th} annual workshop on cryptography, algebra and geometry

Livret des résumés
Booklet of abstracts

Dschang, 21-25 Juillet 2014/ ***Dschang, July 21-25 2014***

Cours/*Courses*

New trends in Elliptic Curves Cryptography

Abdoul Aziz Ciss *École Polytechnique de Ties, Sénégal*

Encryption and signature schemes, scalar multiplication, new families of (hyper)elliptic curves with efficient arithmetic hashing into elliptic curves, pairings on elliptic curves, pseudorandom number generators and randomness extractors based on elliptic curves.

Algebraic groups, surfaces, and algorithms for computing Discrete Logarithms

Tony Ezome *Université des Sciences et Techniques de Masuku (USTM), Franceville, Gabon*

This course in based on an article written by Couveignes and Lercier. Their works are concerned with improvements of the computation of Discrete Logarithms in the multiplicative group of a finite field K. In fact, they look for a smoothness basis for $K*$ that is left invariant by automorphisms of K. We are going to recall the the rudiments of Kummer and Artin-Schreier theories. This produce the Known examples of such smoothness basis. We show that elliptic curves produce a range of such invariant basis, provided the degree of the field is not to large. We finish by describing the ideas underlying a family of algorithms for computing discrete logarithms involving algebraic surfaces.

Algorithmes et complexité

Réné Ndoundam *Université de Yaoundé I, Cameroun*

Ce cours donne les outils pour la calculabilité et la complexité des algorithmes.

Curves on surfaces

Patrick Rabarison F. *Université d'Antanarivo, Madagascar*

This is an introductive course to the geometry of surfaces. It aims to give some basis on the subject at the research level. If the classification of curves are well understood, it is not the case for surfaces and we will talk about it but with no pretension to make an exhaustive treatment. We will also introduce topics that are useful throughout projective and algebraic geometry. Then, we will discuss about curves on surfaces and intersection theory. At last, We will treat the cases of special surfaces such as elliptic surfaces and K^3 surfaces.

Complexity of mapping DAG with affines schedules onto parallel embedded systems

Clémentin Tayou *Université de Dschang, Cameroun*

We study here the complexity of the issue of mapping DAGs associated with affine timing functions onto regular arrays. mapping transformations are used in the design (or compilation) of highly parallel embedded systems such as VLSI arrays. We formally introduce an allocation method based on a preprocessing by re-indexation that transforms the initial DAG into a new one that enables the projection method to minimize the number of processors along a number of directions. Compared to previous allocation methods this new allocation method provides better results, in term of the overall number of processors. Furthermore, for two-dimensional DAGs it systematically leads to space-optimal designs. For DAGs of upper dimension it systematically leads to designs for which the space complexities are bounded by the best space complexity that both the projection method and the so-called grouping method can give for the initial DAG.

An introduction to digital signal processing for mathematicians

Christopher Thron *Texas A&M University, USA*

Digital signal processing is currently an area of applied mathematics that has enormous practical importance. Although the application is very concrete, it uses a great deal of highly abstract mathematics including complex Hilbert space methods, Fourier theory, optimization theory, algebraic geometry, and numerical methods. We present an overview of the digital signal processing required for wireless communication, with special emphasis on mathematical aspects and possible areas of mathematical research.

Two-way relay adaptive beamforming : an application of algebraic geometry to signal processing

Christopher Thron *Texas A&M University, USA*

In designing communications systems, the systems designer is concerned with optimizing the signals received by the systems' users. In many cases, the mathematical optimization problem can be re-expressed as a problem involving intersections of quadratic surfaces in n-dimensional complex space. We consider one particular communication system (two-way relay), and show how geometrical insight can be used to exactly solve the signal optimization problem in a special case, which can then be used as the initial guess for a numerical iterative solution in the general case.

Communications

Session 1 : Algèbre, Géométrie et Cryptographie/ Algebra, Geometry and Cryptography

Implementation of the Theta-Valent Chrysippian Structures

ACHINI Emmanuel Fifi *The University of Ngaoundere, Cameroon*

Chrysippian structures are, in some sense, based on a generalization of classical (Boolean) logic. In this master's thesis, we review the notions of theta-valent chrysippian rings. We give and prove some conditions under which a divisor ring can be complemented and then used to define an appropriate theta-valent chrysippian ring. We propose and implement algorithms for constructing theta-valent chrysippian rings on finite Boolean rings. We also define some operations and perform computations on the theta-valent chrysippian rings generated. These operations and their computation can further be used to sketch cryptographic protocols.

Keywords: Boolean lattices, Boolean rings, theta-valent chrysippian rings, implementation.

Sommes de Kloosterman et applications

Etienne Assongmo Tanedjeu, Christophe Mouaha
Université de Yaoundé I, Cameroun

Les Sommes de Kloosterman ont récemment fait l'objet de beaucoup de recherche, notamment en raison de leurs applications en cryptographie et en théorie du codage. Cet exposé porte sur l'étude des sommes de Kloosterman et leurs applications en cryptographie et en théorie du codage. A cet effet nous allons :

- Donner les notions préliminaires sur les caractères de groupes.
- Définir la notion de somme de kloosterman et donner ses propriétés générales.
- Déterminer à l'aide de ces sommes, le nombre de points rationnels pour certaines courbes elliptiques en caractéristiques 2 et 3.
- Définir les codes de Kloosterman , estimer le poids de ces codes de kloosterman et quelques propriétés générales.

Mots-Clés: Caractère de groupe, Sommes de Kloosterman, Courbe elliptique, Code de Kloosterman.

Confidentiality of SMS for SMS-Banking based on Elliptic Curves.

Flaubert Dakmedeu Yamdjeu*, **Emmanuel Fouotsa**†

* *Université de Dschang,* † *University of Bamenda*

Many banking companies today increasingly implement a solution called "electronic money" for many monetary operations or transactions. Particularly in Cameroon, none the less, the solution offered by telephone operators necessitate signing of a contract permitting them to use USSD(Unstructured Supplementary Service Data) channel which they consider to be secured, the security of the transactions remains an actual problem ; because most solutions proposed today are based on "formatted SMS"(SMS-banking). A study carried out on the weaknesses of GSM network, shows the transmission of unencrypted SMS. This presents a double dimensional problem not only for the users of the system but also for the banking companies. The idea of proposing an efficient Cryptosystem has many advantages especially for a limited functioning environment like the SIM card is what initiated this research : the elliptical curve(EC) presenting a high level of security based on the difficulty of solving the Discrete Logarithm Problem(DLP) responded best to this expectation. In this paper, we present an implemented solution based on EC for the confidentiality of SMS between Customers and those Bank itself.

Keywords: GSM, SMS, security of information, confidentiality, SMS-Banking, Elliptic Curve.

A countermeasure against the Fault Attack on Point Blinding Coutermeasure of Pairing Algorithms

Nadia El Mrabet*, **Emmanuel Fouotsa**†

* *Université Paris 8,* † *University of Bamenda*

Pairings are mathematical tools that have been proven to be very useful in the construction of many cryptographic protocols. Some of these protocols are suitable for implementation on power constrained devices such as smart cards which are subject to fault attacks. In this paper, we analyse many existing fault attacks on pairing algorithms and study the proposed countermeasures. In particular, we generalize the fault attack on a point blinding countermeasure of Park et al. [13] and propose an hybrid countermeasure against that attack.

Keywords: Miller's algorithm, Identity Based Cryptography, Fault Attacks, Countermeasure.

Counting subgroups of $\mathbf{D_{2^n-1} \times C_2}$

M. Enioluwafe *University of Ibadan, Oyo State, Nigeria*

The main goal of this note is to determine the number of subgroups of finite group formed by taking the cartesian product of the dihedral group two power order with a order two cyclic group.

Keywords: Dihedral groups, cyclic groups, cartesian products, number of subgroups, recurrence relations.

Counting subgroups of a class of finite nonmetacyclic 2-groups

M. Enioluwafe *University of Ibadan, Oyo State, Nigeria*

The aim of this note is to give an explicit formula for the number of subgroups of finite nonmetacyclic 2-groups having no elementary abelian subgroup of order 8.

Keywords: Finite nonmetacyclic 2-groups, dihedral groups, cyclic groups, central products, number of subgroups.

Linear recurring sequence and Hensel Lift ; Period of subset-sum generator on elliptic curves, EC-SSG

Serge Feukoua, Thierry Mefenza
University of Yaoundé I, Cameroon

We introduce the Hensel lifts of linear recurrence sequences over Galois ring and give another proof to deduce its periods. To proof our result we need some results on the period of polynomials over Galois field, properties of linear recurrence over galois field and the hensel's lemma. Furthermore, we give some conditions that guarantee that the period of the Subset-Sum Generator on Elliptic Curves (EC-SSG) is the same as the period of the underlying linear recurrence sequence which is an open question in [21].

Keywords: Linear recurring sequence,Subset-Sum Generator on Elliptic Curves

On note on fuzzy relation generated by a probability distribution

Louis Aimé Fono[*], Siméon Fotso[†], Eyke Hüllermeier[‡]
[*] Université de Douala, [†] Université de Yaoundé I, Cameroun, [‡] University of Paderborn, Germany

In this paper, we present a recent development on fuzzy binary relations generated by a probability distribution on the set of permutations on a finite universe.

Arcs in Projective H-Plans

Alexandre Fotue Tabue *Université de Yaoundé I, Cameroun*

The finite chain rings are under-adjacent to Desarguesian projective Hjelmslev plans and the determination of the size of a maximal arc in a projective Hjelmslev plan is the tackled problem.

Keywords: Projective Hjelmslev plane ; Maximal arcs, Linear codes over finite chain rings.

n-fold filters in algebras of non-commutative fuzzy logics

Albert Kadji[†], **Celestin Lele**[*], **Marcel Tonga**[*]

[*] *Université de Dschang,* [†] *Université de Yaoundé I, Cameroun*

This paper presents a generalization of many particular results about folding theory on algebras of non classical(mostly fuzzy)logics. Our Approach is rooted in the framework of Abstract Algebraic Logic, and is based on the close connection between some n-fold filter- defining conditions and alternative axiomatization of the logics involved. We introduce some new classes of n-fold pseudo-residuated lattices satisfying some four mains kind results proved in the literature. We reduce all these results to a simple, purely syntactical, problem of alternative axiomatization of some particulars logics introduce in this paper. At the end of this paper, we draw diagrams summarizing the relations between different types of filters, classes of pseudo-residuated lattices and the new logics introduce in this paper.

Keywords: pseudo-residuated lattices, n-fold strongly ((integral, boolean, normal) filters,pseudo-residuated lattice), Abstract Algebraic Logic, pseudo-Rasiowa-Implicative logics, n-fold logic.

On the use of Random Redundancy in code based PKC

Kalachi Hervé[*], **Otmani Ayoub**[†] **and Ndjeya Selestin**[*]

[*] *Université de Yaoundé I, Cameroun ;* [†] *Université de Rouen, France*

The use of Random Redundancy in code based PKC was proposed for the first time by Wieschebrink. Its goal was to avoid the Sidelnikov-Shestakov attack on the McEliece cryptosystem using generalized Reed-Solomon codes. Although this proposal had effectively avoided the original attack of Sidelnikov and Shestakov, recent studies have shown that in that case of generalized Reed-Solomon codes, the random redundancies inserted can be found through considerations of dimensions of product codes. Recently, Cheikh Thiecoumba Gueye and El Hadji Modou Mboup also proposed a similar description, but based on Reed-Muller codes. Unfortunately, like the Reed-Solomon Codes, Reed-Muller codes are evaluation codes ; these two families of codes thus have common or sometimes similar properties which make easy the looking of random redundancy. We present a cryptanalysis of this version proposed in by Cheikh Thiecoumba Gueye and El Hadji Modou Mboup. The cryptanalysis is inspired by the attack presented by Couvreur é al. We also show that this technique is successful in the case of high rate Goppa/alternant codes.

Keywords: Square code, McEliece and Niederreiter cryptosystems, Reed-Muller codes, Alternant codes.

n-fold sub-implicative and n-fold sub-commutative ideal in BCI-algebra

C. Lele*, S.F. Tebu*, M. Tonga†

** Université de Dschang, † Université de Yaoundé I, Cameroun*

The notions of n-fold sub-implicative ideals and n-fold sub-commutative ideals of BCI-algebras are introduced. We show that a nonempty subset of a BCI-algebra is an n-fold sub-implicative ideal if and only if it is both an n-fold sub-commutative ideal and an n-fold positive implicative ideal. We prove that any p-ideal is always a n-fold sub-implicative ideal and a n-fold sub-commutative ideal. We give a new characterization of n-fold positive implicative ideals of BCI-algebras. Moreover some other properties about n-fold sub-implicative ideals and n-fold sub-commutative ideals of BCI-algebras are given.

Keywords: BCI-algebras, n-fold sub-implicative BCI-algebra, n-fold sub-commutative BCI-algebra, n-fold positive implicative BCI-algebra.

On the Elliptic curves Power Generator

Thierry Mefenza Nountu *Université de Yaoundé I, Cameroun*

A pseudorandom bit generator is a deterministic algorithm which given a truly random binary sequence of length k, outputs a binary sequence of length $l \geq k$ which appears to be random (pass all polynomial-time statistical tests and the next-bit test). The security of many cryptographic systems depends upon the generation of pseudorandom sequences. For example the keystream in the one-time pad, the secret key in DES, the primes p, q in the RSA encryption, the private key in the DSA etc. The output sequence of a pseudorandom generator should have the following properties :

– large period
– large linear complexity
– good statistical properties

We show that the elliptic curve Power Generator produces a sequence with large linear complexity and good statistical properties.

Keywords: elliptic curves, power generator, discrepancy, linear complexity.

Quelques opérateurs sur le groupe des tresses

Terance Magloire Nzomou *Université de Ngaoundéré, Cameroun*

Dans cet exposé, nous présentons 3 opérateurs des groupes des tresses : la torsion des tresses (twist of braid), le cyclage (cycling), le décyclage (decycling), ainsi que leurs applications en cryptographie.

Mots-Clés: opérateurs, groupe des tresses, protocoles d'authentification

The action of a group on a fuzzy set via fuzzy membership function

Onasanya B. O. and Ilori S. A.
University of Ibadan, Oyo State, Nigeria

Study has been conducted on the action of a group on a set. Also, there is existing work on the action of a fuzzy group on a set. This paper studies some properties of the action of a group on a fuzzy set T_μ via the membership function $\mu_T : X \leftarrow [0, 1]$. It also seeks to establish some properties of this action in respect of the stabilizers of an element $t \in T_\mu$ among other things. In particular, it establishes that fuzzy middle cosets of some sort is a group action on a fuzzy subset. It also states and proves fuzzy version of orbit-stabilizer theorem.

Cryptosystèmes fondés sur la métrique rang

Hermann Tchatchiem Kamche *Université de Yaoundé I, Cameroun*

En 1976, Diffie et Hellman ont proposé un modèle de cryptographie à clé publique.Ce modèle peut être formalisé par la RSA, le logarithme discret ou la théorie des codes correcteurs. Cette dernière approche fût proposée par McEliece en 1978 et la sécurité du système de chiffrement repose sur le problème du décodage borné d'un code correcteur. Un inconvénient de ce cryptosystème quand on utilise la métrique de Hamming est la taille de la clé publique. Une solution à ce problème à été proposée en 1991 par Gabidulin, Paramonov et Tretjakov qui proposèrent un cryptosystème dont la sécurité repose sur le problème du décodage borné d'un code, non plus pour la métrique de Hamming, mais pour la métrique rang. Cependant, Gibson a présenté plusieurs types d'attaques pour ce cryptosystème de complexité exponentielle. Dans nos travaux de recherche, nous avons généralisé la métrique rang sur les anneaux finis de chaîne. Le problème que nous nous posons est d'étudier les propretés du cryptosystème induites par cette métrique sur cet anneau. Dans cet exposé, nous allons tout d'abord présenter la théorie de la métrique rang, ensuite le cryptosystème utilisant cette métrique et enfin nous allons définir et donner quelque propriétés des anneaux finis de chaîne.

Mots-Clés: Cryptosystème de McEliece, métrique rang, code de Gabidulin, anneau fini de chaîne.

Sheaf cohomology on network codings : Maxflow-Mincut theorem

Calvin Tcheka, Miradain Atontsa Nguemo
University of Yaounde I, Cameroon

This note first surveys a novel algebraic topological application of sheaf theory into directed network coding problems. R. Ghrist and Y. Hiraoka have proved the maxflow bound using network coding sheaves and relative cohomology on a graph which contains only one source. We use the idea of the modified graph to obtain the weak duality in the multiple source scenario. Finally we construct an algebra isomorphism between the 0-th network coding sheaf cohomology and the 1-th sheaf cohomology using the general Poincaré duality,and so far we prove the Maxflow-Mincut theorem with network coding sheaves in the multiple source case.

Keywords: Network information theory, network coding sheaves, Topological cut, relative sheaf cohomology, Poincaré duality algebra.

Invariant measure on semihypergroups

Norbert Youmbi *Saint Francis University, Loretto, USA*

Let S be a locally compact semihypergroup. A measure m on S (not necessary bounded) will be called left subinvariant if δxm is defined and $\delta xm \leq m$ for all x in S. This talk is a review of some results on invariant measure on compact semihypergroups and locally compact semihypergroups.

Session 2 : Informatique et Modélisation/Modeling and Computer science

HCOL-BAC : Hierarchical and collaborative security access model of information systems

Benoît M. Q. Azanguezet*, Elie T. Fute*, Laure P. Fotso†

** University of Dschang, † University of Yaounde I, Cameroon*

Models of access control based on roles (Role Based Access Control - RBAC models) have a new organization rights focused on the role concept. This family of models mostly adopted by the company has favoured the proposal of models more refined and complex. However, as almost all models of access, it is based on the concept of trust in users and in the DataBase Administrator (DBA). This increases the internal vulnerability of the system because there is evidence that firms are more affected by internal attacks related to trust than external attacks. In addition, the excessive involvement of IT in the process of automatic processing of production information, has created a dichotomy between the computer models and organizational structure of the company. Thus, models of data access control have deviated significantly from organizational and structural models of the company because designed to be used by computer engineers and not by business employees. We propose in this paper a model of data access control whitch : - puts users at the center of business operations and data processing - unifies the organizational structure of the company and the structure of access control and automatic processing, - stratifying the business subsystem and defining a concept of hierarchy between the roles played by employees in the different sub-systems of the company ; - introduced the concept of validation in the process of monitoring and treatment in order to formalize the concept of confidence and enable on the one hand, hierarchical management and collaborative data and on the other hand, control of all system state changes by the actions of users. - Ensure that the computer administration actions are hierarchically and technical controlled by the business administrator.

Keywords: Access model, signature book, organizational structure, query, information system

Supervision des systèmes de production modélisés par les Réseaux de Petri Stochastiques

Donfack Bidias Omer *Université de Ngaoundéré, Cameroun*

Les industries manufacturières sont confrontées à un problème de contrôle des systèmes de production. Ces systèmes sont identifiés comme étant des systèmes à évènements discrets dotés d'apparition d'évènements contrôlables et incontrôlables. Etant donné que la synthèse de la théorie de supervision par les automates à états finis conduit à une explosion d'un nombre d'état rendant ainsi difficile la recherche d'un système supervisé optimal, nous proposons dans cet article une approche de contrôle par supervision en utilisant les Réseaux de Petri Stochastiques. Cette approche vise premièrement à vérifier la contrôlabilité des spécifications imposées au procédé ceci passant par l'application de l'Algorithme de Kumar et secondement elle vise à mettre sur pied un procédé supervisé par les Réseaux de Petri Stochastiques sans introduction des places de contrôle.

Mots-Clés: Système de production, Système à évènement discrets, Théorie du contrôle par supervision, Réseaux de Petri Stochastiques.

Modeling an ecological process

Enu Ekaka-a

Rivers State University of Science and Technology, Nigeria

There is a strong link between the concepts of algebra, measure theory, numerical simulation and mathematical modelling. While the mathematical modelling which describes the survival of species dependent on a limited resource in a polluted environment is a not new, we have utilised the technique of a numerical simulation to study the impact of environmental random noise on the carrying capacities of a mathematical model of survival of species dependent on a resource in a polluted environment. Since the ecosystem is characteristically stochastic, random noise intensity on the maximum population size (otherwise called the carrying capacity) that supports the growth of a population is inevitable. On the basis of this study, it is a best-fit scenario to select the low random noise intensity of 0.8 which attracts lower error values of 4.9880, 1.6725 and 0.7904 using the three popular p-mathematical norms. This is one of the typical results which we have obtained in this study. These observations are in contrast with a high random intensity of 2.4 which attracts higher error values of 16.5637, 5.8055 and 2.3294 b using the 1-norm, 2-norm and infinity-norm measures. The policy implication of these novel contributions is briefly mentioned. This present study was also conducted for an instance when the random noise intensity is 1.6. The key contribution in this scenario is the fact that the errors between the K_{1new} and K_{1old} differentiated data sets are 9.6252, 3.3565 and 1.5568 by using the 1-norm, 2-norm and infinity-norm measures whereas the errors between the K_{2new} and K_{2old} differentiated data sets are 7.7413, 2.8141 and 1.3205 by using the 1-norm, 2-norm and infinity-norm measures. The implications of our present analysis in the mathematical fields of algebra, measure theory and numerical simulation will be illustrated. The results which we have obtained have not been seen elsewhere ; they are presented here and discussed.

Modeling and simulation of decentralized hybrid generation system of energy based on differential petri net

Kennedy Fohoue *University of Ngaoundere, Cameroon*

In this work we present the performance evaluation of decentralized hybrid generation system of energy based on differential petri net. These systems which consist of several sources of renewable or non-renewable energy generation system have a very important expansion in the developing countries. This with the aim of bearing the demand for electricity isolated sites. The purpose of this study is to analyze the interactions between discrete and continuous phenomena in these systems and to develop an algorithm for energy management in order to respond optimally to demand.

Keywords: Differential petri net, decentralized hybrid generation system of energy, modeling

Modélisation multi-agent de la dynamique d'une ruche d'abeilles

Elvire Chéryl Tcha'wu *Université de Ngaoundéré, Cameroun*

Les abeilles sont des insectes vivant en société organisée dans une ruche. Le résultat de leurs différentes activités quotidiennes est d'une très grande importance pour l'épanouissement et la survie de l'humanité. Depuis 2006, les apiculteurs du monde entier ont rapporté des taux élevés de perte de colonies d'abeilles, avec une disparition dans certaines zones du globe. L'une des causes est la non maîtrise de la dynamique de la colonie. Des auteurs ont proposé des modèles basés sur les équations différentielles, afin d'explorer les aspects de la dynamique de la colonie d'abeilles. Cependant, ces modèles ne prennent pas en compte les actions individuelles et par conséquent les variations de l'environnement qui en découlent. Le but de cette étude est de modéliser la dynamique de la colonie d'abeilles en incluant les comportements individuels par l'approche multi-agents. Nous avons construit un modèle multi-agents de la dynamique d'une ruche d'abeille *Apis mellifera* basé sur la méthodologie *Gaia*. Ce modèle a été implémenté grâce à l'outil de simulation *Multi-agent Simulator Of Neighborhoods*. La méthode d'*Analyse de Sensibilité Locale* et le logiciel de statistique R nous ont permis d'évaluer l'influence des sorties du modèle sur ses entrées et d'en tirer des conclusions. Une colonie d'abeilles naissante dans une ruche se déplace vers un équilibre qui à lieu environ 190 jours après sa naissance. Cet ajustement est perceptible à travers les pontes de la reine, l'âge de début de butinage et l'effectif de la population. Par conséquent, pour optimiser la production de miel les apiculteurs devront préparer leurs colonies environ 190 jours avant la forte floraison des plantes mellifères. L'activité de butinage intense induit un début de butinage précoce des ouvrières, alors qu'une activité non intense induit le report de leur âge de début de butinage.

Mots-Clés: dynamique, ruches d'abeilles, système multi-agents, Gaia.

Agent-based models of satisfaction and conflict in human populations

Christopher Thron *Texas A&M University,USA*

The mathematical modelling of human populations poses special and challenging difficulties as compared to the modelling of biological or physical systems. This is because the intelligent actions of individuals within the population may have a huge effect on the overall dynamics of the population. Modern computers have made possible a computationally-intensive modelling technique known as "agent-based modelling," in which large populations are modelled on an individual-by-individual basis. We demonstrate two applications of this technique to different sociological scenarios : the first deals with the evolution of personal satisfaction in a competitive society, while the second deals with inter-group relationships in a divided community. Although the models are unsuitable for making detailed predictions about such systems, they do provide some insight into the important factors that tend to drive overall trends in population behavior, and may suggest methods for guiding those trends in constructive directions.

Permission Based Group Mutual Exclusion Algorithms for a Cluster Tree network

Arlette Sylvie Touomguem *Université de Ngaoundéré, Cameroun*

Due to the growing application of peer to peer computing, distributed applications are continuously spreading over an extensive number of nodes. To cope with this large number of participants, various hierarchical cluster based solutions have been proposed. Cluster or group based solutions are scalable for a large number of participants. As far as group mutual exclusion solutions are concerned, some of them have good complexity but do not take into account the growing number of participants. Others take into account the previous aspect but do not have good complexity. We present two group mutual exclusion algorithms namely ; $TBGMEC_\alpha$ and $TGBMEAC_\alpha$.The proposed logical structure is a cluster tree. The first solution uses the partial flooding method, which is the partial propagation of information available at root level. In the second solution, information available at root level is propagated only towards the processes which issued a request for a session. Both algorithms have complexities of $O(p)$ and $O(logp)$ respectively(p is the number of clusters in the system).

Keywords: Distributed system, resource allocation, group mutual exclusion, cluster tree network, partial flooding

Synthèse de la commande supervisée d'un système totalement modélisé par Grafcet basée sur l'algorithme de Kumar

Wayang Senguel *Université de Ngaoundéré, Cameroun*

Pour assurer le bon fonctionnement d'un système, il est nécessaire de démontrer que les programmes de commande respectent les propriétés de sécurité spécifiées dans le cahier des charges. Cette démonstration peut se faire soit par la validation (ou vérification) soit par la synthèse de trajectoires de commande. Dans cet article, nous nous sommes basés sur l'approche de synthèse. Nous voulons une méthode de synthèse ne manipulant que le Grafcet afin d'être aussi utilisé par l'automaticien classique. Pour atteindre cet objectif, nous avons formalisé une technique de composition du Grafcet en respectant les règles d'évolution du Grafcet qui pour notre part, est plus riche que ceux des automates. Nous nous affranchirons ainsi de l'utilisation des automates dans le processus de synthèse. Les avantages de cette approches sont nombreuses :L'on peut directement obtenir le comportement commun des Grafcet par la composition directe de ces derniers, L'on peut exploiter certaines propriétés comme les divergences en ET qui n'existe pas dans le langage automate, manipulation facile ; par simple logique du comportement d'un Grafcet, manipulable par les automaticiens classiques. Etant donné les critères d'un bon superviseur (déterministe, réactif, sans blocages et maximal permissif), notre méthode est plus maximale permissif (permettre un maximum de possibilité d'évolution du système) qu'avec les automates, pour notre cas d'application, la supervision à base des automates a généré 6 étapes et 12 transitions tandis que la nôtre a généré 6 étapes et 15 transitions.

Mots-Clés: Théorie de supervision, Automates finis, Grafcet.

Proposition d'un méta-ordonnancement distribué de grille et de modélisation multi-agents

Jérémie S. Wouansi, Vivient Corneille Kamla, Daniel Tieudjo
Université de Ngaoundéré, Cameroun

Le méta-ordonnancement attribue aux tâches des utilisateurs, des ressources de calcul appartenant aux noeuds d'une grille informatique. Les méta-ordonnanceurs existants visent l'optimisation soit des métriques système-centré, tel que l'utilisation des ressources et la bande passante, soit l'attribution des priorités aux applications, basée sur des métriques d'utilité fournies par les utilisateurs. La première, comme avec le modèle multi-agents distribué de Solar, accorde moins d'importance à l'utilité individuelle des utilisateurs. La seconde, telle l'approche multi-agents centralisée d'Aguilar basée sur la vente aux enchères, peut avoir des effets adverses tels qu'une pauvre performance du système et un traitement inéquitable des utilisateurs. Le modèle centralisé basé sur la vente aux doubles enchères de Saurabh concilie les deux approches. Cependant, la centralisation impose de nombreuses communications longues, et nécessite une base d'information globale pouvant entraîner une perte de cohérence d'information due aux temps de communication et de prise de décision. En plus, il n'est pas efficace quand au temps de réponse et à la garantie des tâches.

Dans ce papier, après avoir proposé un système de méta-ordonnancement distribué basé sur la vente aux doubles enchères et l'appel d'offre, nous faisons une modélisation multi-agents basée sur la méthodologie GAIA de ce système, ensuite nous implémentons un simulateur du modèle obtenu en utilisant la bibliothèque de simulations des systèmes distribués Simgrid, et enfin nous faisons une analyse des performances. Il en ressort que le modèle de méta-ordonnancement distribué basé sur les doubles enchères et l'appel d'offre, en plus des deux approches de métriques pris en compte dans les précédents, améliore le temps de réponse et la garantie des tâches.

Mots-Clés: Grille informatique, Système multi-agents, Allocation de ressources,Méta-ordonnancement, Vente aux doubles enchères, Appel d'offres, Simgrid.

Intranet comme environnement de calcul scientifique tolérant aux fautes.

Blaise Omer Yenké, Cyrille Dibamou

Université de Ngaoundéré, Cameroun

Dans les laboratoires informatiques de nos universités, les machines sont souvent laissées allumées par inadvertance les soirs et pendant les weekends ce qui peut entraîner un surcoût de consommation énergétique, voire même entraîner une dégradation prématurée de l'état des machines.
Pour pallier ces problèmes, une idée serait d'arrêter systématiquement les machines en fin de journée pour les jours ouvrables et les weekends. Cependant, un arrêt systématique pourrait entraîner la terminaison de certaines tâches de calcul scientifique et entraîner ainsi une perte de temps de calcul déjà effectuée.
Dans ce travail, nous proposons des techniques et des outils permettant d'administrer un intranet, particulièrement d'arrêter systématiquement les machines ayant au préalable sauvegardé le contexte d'exécution des applications de calcul qui auront été lancées en spécifiant qu'elles peuvent être candidates à la sauvegarde. La solution proposée a été implantée dans un laboratoire informatique d'une de nos institutions.

Mots-Clés: Sauvegarde/Reprise, Application de calcul, Administration réseau, Intranet.