

# Journée du Laboratoire

## L'IFORCE

**JoLIFORCE'2017**

**Jeudi 27 Avril 2017**

**Lieu**

**Faculté de Mathématiques**

**Salle de Conférences**

**Organisée par**

**LABORATOIRE D'INFORMATIQUE  
FONDAMENTALE, DE RECHERCHE  
OPERATIONNELLE, DE COMBINATOIRE  
ET D'ÉCONOMÉTRIE**



Le Laboratoire L'IFORCE est heureux d'organiser le 27 Avril 2017 la troisième édition de ses journées scientifiques JoLIFORCE'2017. Cette journée a pour but de réunir tous les chercheurs du Laboratoire.

<http://www.liforce.usthb.dz>

---

# Conception et réalisation

Pr. Sadek BOUROUBI

---

# RECUEIL DES RESUMÉS

Journée du Laboratoire L'IFORCE

JoLIFORCE'17

27 Avril 2017

Faculté de Mathématiques

USTHB

Organisée par :

Le Laboratoire d'Informatique  
Fondamentale, de Recherche Opérationnelle,  
de Combinatoire et d'Économétrie

## TABLE DES MATIÈRES

<b>MOT DE LA DIRECTRICE DE L'IFORCE .....</b>	<b>02</b>
<b>ORGANISATEUR .....</b>	<b>03</b>
COMITÉS .....	03
COMITÉ DE PROGRAMME .....	03
COMITÉ D'ORGANISATION.....	03
<b>PROGRAMME DÉTAILLÉ .....</b>	<b>04</b>
<b>RÉSUMÉ DE LA CONFÉRENCE .....</b>	<b>06</b>
<b>RÉSUMÉS DES COMMUNICATIONS .....</b>	<b>08</b>

# MOT DE LA DIRECTRICE DE L'IFORCE

Créé en 2012, le Laboratoire d'Informatique Fondamentale, de Recherche Opérationnelle, de Combinatoire et d'Econométrie (L'IFORCE) regroupe 34 enseignants-chercheurs (04 Professeurs, 05 Maitres de conférences, 25 Maitres Assistants), 16 doctorants du cycle LMD et 01 doctorant ancien régime, répartis en quatre équipes de recherche :

Equipe 1 : Combinatoire et algorithmique des structures discrètes.

Equipe 2 : Structures Finies et Applications.

Equipe 3 : De la Combinatoire Algébrique à la Combinatoire Algorithmique et Applications.

Equipe 4 : Modélisation Mathématique des Maladies émergentes et ré-émergentes en Algérie : Dynamique et Contrôle.

Les activités de recherche du laboratoire sont orientées autant pour la recherche fondamentale que pour la recherche appliquée. Parmi ses thèmes de recherche, on peut citer la combinatoire énumérative, les graphes (domination, coloration, plongements, ), la cryptologie et la sécurité de l'information, la modélisation dans le secteur de la santé, ...

Après sa première édition qui a eu lieu le 31 novembre et le 01 décembre 2014 à l'ISGP, Bordj El Kiffan, et la seconde le 21 Avril 2016 à l'USTHB, le laboratoire organise sa troisième édition JoLIFORCE'17, le 27 Avril 2017, à la Faculté de Mathématiques de l'USTHB.

L'objectif de cette journée scientifique est de réunir tous les chercheurs du laboratoire pour présenter leurs travaux de recherche et les discuter. Il a été retenu pour JoLIFORCE'17, une allocution de la Présidente de l'AWMA (African Women in Mathematics Association), 01 conférence plénière et 08 communications orales.

Nous espérons que JoLIFORCE'17 soit une journée bénéfique à tous les participants et plus particulièrement aux doctorants.

Directrice de L'IFORCE

Professeur Isma BOUCHEMAKH

# ORGANISATEUR

Le Laboratoire d'Informatique Fondamentale, de Recherche Opérationnelle,  
de Combinatoire et d'Économétrie

**L'IFORCE**

## COMITÉS

---

### COMITÉ DE PROGRAMME

Isma BOUCHEMAKH (Directrice de L'IFORCE)	Chef de l'équipe CASDI
Abdelhafid BERRACHEDI	Chef de l'équipe SFINA
Sadek BOUROUBI	Chef de l'équipe COMB3A
Schehrazed SELMANE	Chef de l'équipe MMM

---

### COMITÉ D'ORGANISATION

I. BOUCHEMAKH  
A. BERRACHEDI  
S. BOUROUBI  
S. SELMANE  
S. BEKKAI  
N. KAHOUL  
N. BENYAHIA-TANI  
M. AOUANE  
Z. YAHY  
S. KERDJOUJ  
A. AINOUCHE  
B. AMARI

**PROGRAMME**  
**DÉTAILLÉ**

**Jedi** | **27 Avril 2017**

**08h30 - 09h00 : Réception**

**09h00 - 09h30 : Ouverture**

---

Président : Isma BOUCHEMAKH

**09h30 - 09h45 : Schehrazad SELMANE**

Présentation de l'AWMA (African Women in Mathematics Association)

---

**09h45 - 10h15 : PAUSE CAFÉ**

---

Président : Isma BOUCHEMAKH

**10h15 - 11h00 : Sadek BOUROUBI**

An Overview of Steganography

---

Président : Abdelhafid BERRACHEDI

**11h10 - 11h30 : Messaouda AHMANE**

On the Broadcast Independence Number of Caterpillars

**11h30 - 11h50 : Saliha OUATIKI**

Some results on the global offensive alliance numbers in graphs

**11h50 - 12h10 : Samia KERDJOUJ**

Le nombre  $b$ -chromatique du produit cartésien de graphes

**12h10 - 12h30 : Amina AINOUCHE**

The contamination game of grid  $G(m, n)$

---

**12h30 - 14h00 : PAUSE**

---

Président : Sadek BOUROUBI

**14h00 - 14h20 : Seif eddine AKERMI**

Forecasting and Prediction of Human Brucellosis : the case of Tebessa Province

**14h20 - 14h40 : Meriem GHANEM**

Un protocole de partage de secret basé sur le principe de domination stable

**14h40 - 15h00 : Bedrane AMARI**

Graphes quasi-médians et application au problème de reconstruction d'ADN en phylogénétique

**15h00 - 15h20 : Nedjmeddine KANTOUR**

Cryptanalyse du Chiffre de Merkle-Hellman par un Algorithme Génétique Parallèle

**15h20 : CLÔTURE**



**RÉSUMÉ**  
**DE LA CONFÉRENCE**

# An Overview of Steganography

**Sadek BOUROUBI**

USTHB, Faculty of Mathematics

sbouroubi@usthb.dz

**Résumé :** With the advent of the computer and its "all-digital" reign, techniques exist to hide any document in another document, thus hiding the existence of the communicated information. In this presentation we will see how it is possible to hide a document in a support (image, sound, word document) through a software application realized within our team Comb3A in L'IFORCE Laboratory.

## Références

- [1] A. Westfeld., *F5* steganographic algorithm, In I.S Moskowitz diteur : proc Information Hiding 4th International Workshop, IHW 2001.
- [2] F. Galand, G. Kabatiansky., Information Hiding by Coverings, in proceedings of IEEE Information Theory Workshop 2003, IEEE, pp.151-154.
- [3] R. Crandall., Some notes on steganography, available at <http://os.inf.tu-dresden.de/westfeld/crandall.pdf>, 1998.

**RÉSUMÉS**  
**DES COMMUNICATIONS**

# On the Broadcast Independence Number of Caterpillars

Messaouda AHMANE, Isma BOUCHEMAKH and Éric SOPENA

USTHB, Faculty of Mathematics

nacerahmane@yahoo.fr

**Résumé :** Let  $G$  be a simple undirected graph. A broadcast on  $G$  is a function  $f : V(G) \rightarrow \mathbb{N}$  such that  $f(v) \leq e_G(v)$  holds for every vertex  $v$  of  $G$ , where  $e_G(v)$  denotes the eccentricity of  $v$  in  $G$ , that is, the maximum distance from  $v$  to any other vertex of  $G$ . The cost of  $f$  is the value  $cost(f) = \sum_{v \in V(G)} f(v)$ . A broadcast  $f$  on  $G$  is independent if for every two distinct vertices  $u$  and  $v$  in  $G$ ,  $d_G(u, v) > \max\{f(u), f(v)\}$ , where  $d_G(u, v)$  denotes the distance between  $u$  and  $v$  in  $G$ . The broadcast independence number of  $G$  is then defined as the maximum cost of an independent broadcast on  $G$ . We study independent broadcasts of caterpillars and give an explicit formula for the broadcast independence number of caterpillars having no pair of adjacent vertices with degree 2.

**Mots-clés :** Independence ; Distance ; Broadcast independence ; Caterpillar.

## Références

- [1] I. Bouchemakh and M. Zemir. On the Broadcast Independence Number of Grid Graph. *Graphs Combin.* 30 :83–100 (2014).
- [2] J. Dabney, B.C. Dean, and S.T. Hedetniemi. A linear-time algorithm for broadcast domination in a tree. *Networks* 53(2) :160–169 (2009).
- [3] J.E. Dunbar, D.J. Erwin, T.W. Haynes, S.M. Hedetniemi and S.T. Hedetniemi. Broadcasts in graphs. *Discrete Appl. Math.* 154 :59–75 (2006).
- [4] P. Heggenes and D. Lokshtanov. Optimal broadcast domination in polynomial time. *Discrete Math.* 36 :3267–3280 (2006).
- [5] S.M. Seager. Dominating Broadcasts of Caterpillars. *Ars Combin.* 88 :307–319 (2008).

# The contamination game of grid $G(m, n)$

Amina AINOUCHE and Sadek BOUROUBI

USTHB, Faculty of Mathematics

aainouche@usthb.dz

**Résumé :** The contamination game of grid  $G(m, n)$  by viruses is a dynamic variant and very particular of the domination showing similarities with power domination, which is well-known problem in graph theory and recently introduced by Haynes, Hedetniemi and Henning in 2002. The Power domination is defined initially as a standard domination for a set  $S$  of vertices and then a propagation of this domination in all vertices of the graph  $G$ , while starting with  $S$ . Note that the minimum cardinal of power domination by  $\gamma_\pi$ . The virus contamination in grid  $G(m, n)$  is interpreted by an automaton cellular evolutionary, which aims to propagate viruses according to appropriate propagation rules. This contamination can be interpreted as biological phenomenon or a social phenomenon evolutionary. The goal of this presentation is to find the minimum number of contaminated cells,  $\gamma_{cv}G(m, n)$ , with viruses so that the entire grid is contaminated.

**Mots-clés :** Domination ; Power domination in graph ; Domination games.

## Références

- [1] A.Azami, Domination in graphs with bounded propagation : algorithms, formulations and hardness results. *J. Comb. Optim.* 19 (2010), no. 4, 429 - 456.
- [2] T.L. Baldwin, L. Mili, M.B. Boisen, R. Adapa, Power system observability with minimal phasor measurement placement, *IEEE Trans Power System* 8(2) (1993) p 707-715.
- [3] J.G. Chang, P. Dorbec, M. Montassier and A. Raspaud, Generalized power domination of graphs. *Discrete Appl. Math.* 160 (2012), no. 12, 1691 - 1698.
- [4] P. Dorbec, M. Mollard, S. Klavzar ; S. Spacapan, Power Domination in product graphs, *SIAM J. Discrete Math.* 22(2) (2008) p 554-567.
- [5] M. Dorfling, M.A. Henning, A note on power domination in grid graph, *Discrete Applied Math.* 154(6) (2006) p 1023-1027.
- [6] T.W. Haynes, S.M. Hedetniemi, S.T. Hedetniemi et M.A. Henning, Domination in graphs applied to electric power networks, *SIAM J. Discrete Math.* 15(4) (2002) p 519-529.

# Forecasting and Prediction of Human Brucellosis : the case of Tebessa Province

**Seif eddine AKERMI** and Schehrazad SELMANE

USTHB, Faculty of Mathematics

akeseif@gmail.com

**Résumé :** Brucellosis, a zoonosis, is an infection transmitted by direct or indirect contact with infected animals or their products. Brucellosis remains a public health problem in Algeria. Since the middle of 1980s, several outbreaks were reported in Ghardaia, Tlemcen, and Setif, resulting in a rise in the number of human cases. This led the public health services to implement control and eradication measures, regarding animal and human brucellosis. Despite the adopted control measures, the disease is still present with more than 5000 confirmed infections annually.

The aim of this study is to analyse and interpret the available data of human brucellosis in Tebessa province, Algeria, and to develop a forecasting model. To this end, we used the Box-Jenkins approach to fit a seasonal autoregressive integrated moving average (SARIMA) model to the monthly recorded human brucellosis cases in Tebessa from 2000 to 2014.

The time series analysis showed that a  $(3, 1, 3) \times (0, 1, 1)_{12}$  SARIMA model offered the best fit to the human brucellosis surveillance data. This model was used to predict human brucellosis cases for the year 2015, and the fitted data showed considerable agreement with the actual data.

SARIMA models are useful for monitoring human brucellosis cases, and provide an estimate of the variability to be expected in future cases. This knowledge is helpful in predicting whether an unusual situation is developing or not, and could therefore assist decision-makers in strengthening the province's prevention and control measures and in initiating rapid response measures.

**Mots-clés :** Box-Jenkins, Human brucellosis, Forecasting, Tebessa, Time series.

## Références

- [1] Guler et al, Human brucellosis in turkey : different clinical presentations, J infect Dev Ctries 2014 ; 8(5) :581-588.
- [2] M.Kardjadj, The Epidemiology of Human and Animal Brucellosis in Algeria, J Bacteriol Mycol3(2) : id1025 (2016).
- [3] Box, G., and Jenkins, G. (1976). Time series analysis : forecasting and control. Holden-Day INC, California.

# Graphes quasi-médians et application au problème de reconstruction d'ADN en phylogénétique

Bedrane AMARI et Abdelhafid Berrachedi

USTHB, Faculté de Mathématiques

bedrane.amari@gmail.com

**Résumé :** Les graphes quasi-médians constituent un outil couramment utilisé en biologie pour visualiser des séquences moléculaires. Ils contiennent tous les arbres construits sur les différents haplotypes (ensemble de gènes situés côte à côte sur un même chromosome), le but est de trouver l'arbre le plus parcimonieux (arbre minimisant le nombre de mutations entre les sous-ensembles d'haplotypes), ce problème est récurrent en phylogénétique. Les graphes quasi-médians ont été introduits par Mulder (1980). Leur application en biologie moléculaire est due à Bandelt et al. (1995); Bandelt et Dur (2007) ont montré que l'arbre cherché est contenu dans le graphe quasi-médian associé. Du fait qu'on a caractérisé les graphes quasi-médians comme étant les graphes pour lesquels il y a unicité de projections sur les quasi-intervalles, on s'est intéressé à l'utilisation de cette nouvelle propriété pour la reconstruction d'arbres parcimonieux.

**Mots-clés :** Application des graphes quasi-médians, problème d'arbre le plus parcimonieux, arbres phylogénétiques, graphes médians généralisés, rétractes des graphes de Hamming.

## Références

- [1] B. Amari and A. Berrachedi, "*Generalized Hamming graphs : some new results*," à paraître dans *Dissc. Math. Graph Theory*.
- [2] H. J. Bandelt, "*Retracts of hypercubes*", *J. Graphs Theory* 8 (1984) 501–510.
- [3] H. J. Bandelt, A. Dür, "*Translating DNA data tables into quasi-median networks for parsimony analysis and error detection*", *Mol. Phylogenet. Evol.* 42 (2007) 256271.
- [4] H. J. Bandelt, P. Forster, B. C. Sykes, M. B. Richards, "*Mitochondrial portraits of human populations using median networks*", *Genetics* 141 (2) (1995) 743753.
- [5] A. Berrachedi, "*A new characterization of median graphs*", *Discrete Math.* 128 (1994) 385–387.
- [6] A. Berrachedi, M. Mollard, "*Median graphs and hypercubes, some new characterizations*", *Discrete Math.* 208/209 (1999) 71–75.
- [7] F.R.K. Chung, R.L. Graham, M.E. Saks, "*A dynamic location problem for graphs*", *Combinatorica* 9 (1989) 111–131.
- [8] S. Herrmann, V. Moulton, "*Computing the blocks of a quasi-median graph*", *Discrete App. Math.* 179 (2014) 129138.
- [9] H.M. Mulder, "*The interval function of a graph*", *Mathematical Center Tracks* 132, *Mathematisch Centrum, Amsterdam* 1980.
- [10] E. Wilkeit, "*The retracts of Hamming graphs*", *Discrete Math.* 102 (1992) 197–218.

# Un protocole de partage de secret basé sur le principe de domination stable

Meriem GHANEM et Sadek BOUROUBI

USTHB, Faculté de Mathématiques

ghanem.meriem@gmail.com

**Résumé :** Un protocole de partage de secret est une méthode utilisée dans le but de protéger un secret. Cette méthode consiste en la distribution du secret  $K$  sur un ensemble fini de participants, de telle manière à ce que seuls les sous-ensembles qualifiés peuvent reconstruire le secret en regroupant leurs parts. Un protocole de partage de secret est parfait si les sous-ensembles non qualifiés n'ont aucune information concernant le secret.

Dans cette communication, il sera sujet de présenter un protocole de partage de secret parfait dont le choix des sous-ensembles qualifiés est basé sur le principe de domination stable.

**Mots-clés :** Partage de secret ; Domination stable ; Ensembles qualifiés.

## Références

- [1] N.M.G. AL-Saidi, N.A. Rajab, M.R. Md. Said K.A. Kadhim (2015) Perfect secret sharing scheme based on vertex domination set, International Journal of Computer Mathematics, 92 :9, 1755-1763
- [2] H. Sun and S. Shieh, Constructing perfect secret sharing schemes for general and uniform access structures, J. Inf. Sci. Eng. 15 (1999), pp. 679-689.
- [3] H. Sun and S. Shieh, Recursive constructions for perfect secret sharing schemes, Comput. Math. Appl. 37 (1999), pp. 87-96.
- [4] A. Shamir, How to share a secret, Commun. ACM 22 (1979), pp. 612-613.



# Cryptanalyse du Chiffre de Merkle-Hellman par un Algorithme Génétique Parallèle

Nedjmeddine KANTOUR et Sadek BOUROUBI

USTHB, Faculté de Mathématiques

KANTOURNedjm@gmail.com

**Résumé :** La cryptographie à clé publique ou asymétrique est introduite en 1976 par *Whitfield Diffie* et *Martin Hellman* qui repose sur la notion de fonction à sens unique, deux ans plus tard, *Ralph Merkle* et *Martin Hellman* ont publié le premier cryptosystème asymétrique dit  $\mathcal{MH}$  basé sur une variante du problème du sac à dos à savoir, le problème de la somme de sous ensembles (*subset-sum problem*) qui est reconnu *NP-difficile*.

D'autre part, au cours des quatre dernières décennies, les métaheuristiques ont permis de réaliser un progrès remarquable dans la résolution des problèmes d'optimisation combinatoire réputés difficiles, néanmoins, la conception de ces méthodes soulève plusieurs challenges, notamment l'adaptation et le choix des paramètres. Dans cette modeste contribution, un algorithme génétique est adapté, caractérisé par son exploration rapide de l'espace de recherche connu par sa taille assez importante, permettant ainsi de décrypter des informations chiffrées à l'aide du  $\mathcal{MH}$ .

**Mots-clés :** Cryptanalyse, Chiffre du Merkle-Hellman, Problème du sac à dos, Algorithme génétique.

## Références

- [1] Martin Hellman Ralph Merkle. Hiding Information and Signatures in Trapdoor Knapsacks. *IEEE Transactions on Information Theory*, 24(5) : 525 - 530, September 1978.
- [2] Martin E. Hellman Whitfield Diffie. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) : 644 - 654, 1976.
- [3] Richard M. Karp. Reducibility among combinatorial problems. *Miller R.E. & Thatcher, J.W. (eds.) Complexity of Computer Computations*, Plenum Press, New York, page 85 - 103, 1972.
- [4] Colin R. Reeves, Jonathan E. Rowe. *Genetic Algorithms - Principles and Perspectives : A Guide to GA Theory*. Kluwer Academic Publishers, Dordrech : 2003.
- [5] Bruno Martin. *Codage, cryptologie et applications*. Presses polytechniques et universitaires romandes, Lausanne : 2004.

# Le nombre $b$ -chromatique du produit cartésien de graphes

Samia KERDJOUJ et Abdelhafid BERRACHEDI

Université Saad Dahlab de Blida

s\_kerdjoudj@yahoo.fr

**Résumé :** Une  $b$ -coloration de  $G$  utilisant  $k$  couleurs est une coloration propre des sommets de  $G$  satisfaisant la propriété  $P$  suivante : Pour chaque couleur  $c$ , il existe un sommet  $u$  de couleur  $c$  ayant toutes les  $k - 1$  autres couleurs dans son voisinage. Le nombre  $b$ -chromatique d'un graphe  $G$  est le nombre maximum  $k$  pour lequel  $G$  admet une  $b$ -coloration par  $k$  couleurs. Le sommet  $u$  est dit  $b$ -dominant de couleur  $c$ . L'ensemble des sommets  $b$ -dominants est appelé système  $b$ -dominant. Pour cette notion, nous avons obtenu les valeurs du nombre  $b$ -chromatique du produit cartésien d'un graphe complet par un graphe complet biparti ; puis nous avons prouvé la  $b$ -continuité pour ce type de graphe.

## Références

- [1] A. El Sahili and M. Kouider, *About  $b$ -coloring of regular graphs*, Rapport de Recherche N : 1432. Unité mixte de recherche 8623. CNRS-Université Paris Sud- LRI (2006).
- [2] T. Faik, *About the  $b$ -continuity of graphs*, Electronic Notes in Discrete Mathematics, 17 :151-156 (2004).
- [3] S. Kerdjoudj, F. Affif Chaouche and A. Berrachedi, *The  $b$ -coloring and  $b$ -continuity of the cartesian product of some graphs*, accepted in Utilitas Mathematica.
- [4] R. W. Irving and D. F. Manlove, *The  $b$ -chromatic number of a graph*, Discrete Applied Mathematics, 91 :127-141 (1999).

# Some results on the global offensive alliance numbers in graphs

Saliha OUATIKI and Mohamed BOUZEFRANE

UMBB, Boumerdes

saliha\_ouatiki@yahoo.fr

**Abstract :** For a graph  $G = (V, E)$ , a set  $S \subseteq V$  is a dominating set if every vertex in  $V - S$  has at least a neighbor in  $S$ . A dominating set  $S$  is a global offensive alliance (respectively, global strong offensive alliance) if for each vertex  $v$  in  $V - S$  at least half the vertices from the closed neighborhood of  $v$  are in  $S$  (respectively, a strict majority of its closed neighborhood are in  $S$ ). The global offensive alliance number  $\gamma_o(G)$  (respectively, global strong offensive alliance  $\gamma_o^s(G)$ ) is the minimum cardinality of a global offensive alliance (respectively, global strong offensive alliance) of  $G$ . We first give upper bounds for those parameters for a cactus graphs. We also determine with M. Bouzefrane an upper bound for the offensive alliance number of a connected unicycle graph. Moreover, we characterize all extremal unicycle graphs attaining this bound.

**Key words :** Domination, global offensive alliance, unicycle graph, cactus.

## Références

- [1] M. Chellali. Offensive alliances in bipartite graphs, *J. Combin. Math. Combin. Comput.*, 73 : 245255, 2010.
- [2] M. Chellali, T.W. Haynes Global alliances and independence in trees, *Graph Theory* , 27 : 1927, 2007.
- [3] M. Chellali, L. Volkmann. Independence and global offensive alliance in graphs, *Australasian Journal of Combinatorics*, 47 : 125131, 2010.
- [4] O. Favaron, G. Fricke, W. Goddard, S.M. Hedetniemi, S.T. Hedetniemi, P.K. Kristiansen, R.C. Laskar, D. Skaggs. Offensive alliances in graphs, *Discussiones Math. Graph theory*, 24, No.2 :263275, 2004.
- [5] S.M. Hedetniemi, S.T. Hedetniemi and P. Kristiansen. Alliances in graphs, *J. Combin. Math. Combin. Comput.*, 48 : 157177, 2004.

