Version du 25-04-2013.

M. Gérald BOURGEOIS.

Né le 21-07-1947.

NUMEN : 02S9322453NAG

Section de CNU : 25.

Maître de conférence(s) Hors Classe.
Retraité depuis le 31 Aout 2012.

Maître de conférence(s) honoraire.

Membre du laboratoire GAATI, Université de Polynésie Française.

Publications de niveau « A » dans des revues internationales à comité de lecture, depuis 2007.

1) **On commuting exponentials in low dimensions.**

Article publié dans: **Linear Algebra and its Applications, 423 (2007) 277-286.**

2) Algebraic systems of matrices and Gröbner basis theory.

Article publié dans: **Linear Algebra and its Applications, 430 (2009) 2157-2169.**

3) Algebraic attack on NTRU using Witt vectors and Gröbner bases .

Avec **Jean Charles Faugère, LIP 6 (CNRS-Paris 6)**.

Article publié dans: **Journal of Mathematical Cryptology, 3 (2009) 205-214.**

4) **The matrix equation log(XY)=log(X)+log(Y).**

Article publié dans: **Linear Algebra and its Applications, 432 (2010) 1878-1884**

5) How to solve the matrix equation XA-AX=f(X).
Article publié dans: **Linear Algebra and Applications, 434 (2011) 657-668.**

6) Dynamical systems of simplices in dimension 2 or 3.

Avec S. Orange, Université du Havre.
Article publié dans: **Automated Deduction in Geometry,**

Lecture Notes in Computer Science, Springer, 6301 (2011) 1-21.

7) Pairs of matrices, one of which commutes with their commutator.
Article publié dans: **Electronic journal of Linear Algebra, 22-38 (2011) 593-597.**

8) Similar powers of a matrix.

Article publié dans : **Linear And Multilinear Algebra. Vol. 61-6 (2013) 699-709.**

9) Common invariant subspace and commuting matrices.

Article publié dans **: Linear Algebra and its Applications. Vol. 438-7 (2013) 3030-3038.**

10) The matrix application X -> AX+XA.

Papier accepté par : **Linear And Multilinear Algebra. (Avril 2013).**

Déposé sur **arXiv : 1210.0766.**

Publications soumises.

1) Commuting exponentials in dimension at most 3.

Papier soumis à : **Bulletin of the Australian academy of sciences.,**

Déposé sur **arXiv : 1107-2278, (2011).**

2) Nonsymmetric generic matrix equations.

Papier soumis à : **Linear Algebra and its Applications.**

Déposé sur **arXiv : 1304.2506.**

Affectations

De 1969 à 2008 :

Université d'Aix-Marseille II à Marseille.

De 2008 à 2012 :
Université de la Polynésie Française à Tahiti .

Evolution de carrière.

1983 : Maitre-Assistant de première classe.

2010 : Maitre de Conférence(s) Hors Classe.

RAYONNEMENT

I- De 1992 à 1994 : Modélisation mathématique et simulation numérique de l'activité des neurones (en collaboration avec le laboratoire CNRS dirigé par Mme Tyc-Dumont à Marseille).

De 1995 à 2000 : Mon sujet d'intérêt est la fiabilité des grands systèmes dans le cadre du « Programme de Recherche Coordonnée (CNRS, AMI, groupe : Structures Discrètes de la Décision) ».

Tout le long de ces années de travail concernant le calcul des probabilités, j'ai obtenu plusieurs contrats d'expertise avec EDF (Direction des Etudes et Recherches à Clamart) dans le cadre de la sûreté nucléaire et de la gestion des déchets.

Lors de ma collaboration avec EDF, j'ai publié 2 articles classés « Accessibilité Restreinte » donc non joignables à mon dossier.

De 2000 à 2004 : je fais partie de l'équipe de JF Michon (Rouen-Marseille); notre groupe bénificie d'un contrat lié à l'Action Coordonnée Incitative « Cryptologie » mise en place par le

Ministère de la Recherche.

A partir de 2002 je travaille sur les générateurs aléatoires utilisables en cryptographie.

De 2000 à 2002, j'étudie plus particulièrement les systèmes multivariés dont le type est le système HFE proposé par J. Patarin (ex Bull).

II- *Depuis quelques années, je travaille avec des membres du labo LIP 6 (Paris-CNRS) spécialisé dans le calcul formel. Nous avons déjà publié des articles en commun (application de la théorie des bases de Gröbner en cryptographie et en géométrie) et en préparons d'autres.*

III- *Je suis consultant de D. Bernstein (Michigan university) pour la nouvelle version de son livre*

> *« Matrix Mathematics,* theory, facts and formulas »*, Princeton University Press, 2008, spécialement pour ce qui concerne les fonctions de matrices.*

IV- *Je suis referee dans les journaux*

Proceedings of the American Mathematical Society.

Electronic journal of Linear Algebra.

Acta Mathematica Scientia.

Synthèse de la carrière :

Etudes et carrière universitaire :

J'ai occupé un poste de Maître de Conférence(s) à la faculté de Luminy, dans

l'Université d'Aix Marseille 2, jusqu'au 31 Janvier 2008.

Je suis actuellement Maître de Conférence(s) Hors classe,

à l'Université de la Polynésie Française, où j'ai été nommé le premier Février 2008.

J'ai été président du département de Mathématiques-Informatique de 1990 à 1996 à la faculté de Luminy (Département comprenant plus de 40 enseignants-chercheurs).

1982 : Passage en première classe des Maîtres-Assistants.

1981 : Obtention d'un poste de Maître-Assistant mis au concours national.

1978 : Publication d'une généralisation de ma thèse aux CRAS.

1977 : Thèse de 3ème cycle en topologie différentielle (mention très honorable) à la suite du DEA (mention très bien).

Inscription sur la LAFMA.

Enseignant-chercheur à la faculté de Marseille-Luminy depuis Octobre 1969.

1969 : Agrégation de Mathématiques (57ème) .

Assistant à la Faculté Saint Charles de Marseille (université I) de mars 1969 à septembre 1969.

Activité scientifique :

1. *Présentation des thématiques de recherche : grands axes de recherches et apport dans le ou les domaines*

Actuellement je travaille dans trois directions différentes :

i) **En cryptographie** : sur les systèmes à clé publique en Cryptographie, notamment le système NTRU.
En collaboration avec J.C. Faugère, qui dirige le laboratoire LIP 6

(Paris 6-CNRS) spécialisé dans le calcul formel, nous montrons que la technique d'attaque par les vecteurs de Witt est inopérante sur le système cryptographique NTRU.

ii) **En algèbre linéaire et calcul formel**: travaux sur les fonctions de matrices (exponentielle et logarithme) et la résolution de systèmes d'équations matricielles algébriques à l'aide de la théorie des bases de Gröbner dans les anneaux non commutatifs.
J'ai montré un nouveau résultat sur la fonction matricielle logarithme.

D'autre part, j'ai appliqué la théorie des bases de Gröbner à la résolution d'équations ou de systèmes d'équations algébriques de matrices, ce qui est absolument nouveau.

iii) **En calcul formel appliqué à la géométrie** : étude de systèmes dynamiques discrets dans l'espace à l'aide de la théorie des bases de Gröbner dans les anneaux commutatifs.
Avec S. Orange (LIP 6 et Université du Havre), nous avons étudié un système dynamique discret de tétraèdres. Il y a une grosse partie d'analyse classique (estimés,…) mais une convergence essentielle a été obtenue en étudiant des systèmes algébriques à l'aide de la théorie

des bases de Gröbner. Ici aussi il n'y a pratiquement pas de littérature sur ce dernier point. Le problème était connu mais non résolu jusqu'à présent.

Activités pédagogiques :

Le volet enseignement :

Dans l'université :

A Marseille jusqu'en Janvier 2008 :

j'assure des cours en Licence (3ème année, ex Licence) et en Master (ex Maîtrise, DEA, DESS); j'y encadre des projets d'analyse numérique, de probabilité et de cryptographie.

Plus précisément j'ai assuré, en tronc commun ou option, plusieurs années chacun des cours suivants :

En licence (3ème année):

Analyse numérique (avec cours en ligne) – Intégration - Algèbre (classique)- Groupes –

Calcul scientifique (Maple) – Equations différentielles – Fonctions analytiques.

En maîtrise (1ère année) :

Probabilités (chaînes de Markov) - Géométrie différentielle - Compléments de mathématiques (préparation au CAPES) -.Algèbre (théorie de Galois).

J'ai suivi régulièrement des étudiants qui ont réalisé sous ma direction de bons projets sur lesquels j'ai pu m'appuyer pour leur faire des dossiers de candidature sur titres à l'entrée des grandes écoles :

Ainsi mes meilleurs étudiants ont pu intégrer ces dernières années:

Télécom Paris : Mr. Caternet, John Wilson , Francis Kochoedo, Séverine Tramoni.

L'école des Mines de Paris : Grégory Rolina.

L'ENSIMAG (Grenoble) : Mr. Chiesa.

L'Ecole d'Actuaires de Lyon (une des 2 meilleures en France) : Benoit Meyer.

L'ENSTA à Paris : Xavier Lemaire.

En maîtrise (2ème année) :

En filière professionnelle MINT, j'assure le tronc commun de cryptographie et une partie de l'option de cette spécialité orientée vers l'utilisation en entreprise.

En DEA, je participe à une option de cryptographie plus théorique.
Nos étudiants font régulièrement des stages chez Thales, Oberthur,…

Je donne aussi régulièrement des cours de préparation à l'agrégation interne de Mathématiques à l'université Aix Marseille I.

A Papeete à partir de Février 2008

- J'ai assuré des cours variés en Licence

L1 : intégration.

L2 : Probabilités, Statistiques, Algèbre linéaire

L3 : Equations Différentielles, Théorie des groupes , Géométrie, Intégrale de Lebesgue.

Master 1 et 2 : Probabilités, Statistiques. Corps finis. Préparation au CAPES.

- J'ai donné des cours de préparation à l'agrégation interne ainsi que des cours en IUFM pour la préparation au CAPES.

Hors de l'université :
Je fais passer, depuis de nombreuses années, des colles au Lycée Thiers de Marseille dans les classes préparatoires scientifiques MP et MP*.

Dans le cadre de cette activité, j'ai envoyé plusieurs papiers à la Revue de Mathématiques Spéciales et j'ai été durant plusieurs années examinateur à l'oral des concours d'entrée aux ENSI et à l'école d'ingénieurs de Marseille.

Ouvrages scientifiques :

- J'ai assuré la partie mathématique du « guide des manuels scolaires » paru chez Flammarion en 1990.
- J'ai participé à la réalisation de l'ouvrage (niveau 3ème année de licence de mathématiques): « Mathématiques MP-MP* » paru chez Lavoisier en 2006 dans la collection méthodes et annales.

Commission Masters :

Je fais partie de la commission Masters dirigée par Michel Granger.

2. *Rayonnement et activités internationales :*

Je m'investis beaucoup (plus de 1600 posts) dans un forum Californien (bien connu, du moins aux USA), le forum AOPS sous le pseudo « loup blanc » (sic).

Responsabilités Administratives :

J'ai été président du département de Mathématiques-Informatique de 1990 à 1996 à la faculté de Luminy (Département comportant plus de 40 enseignants-chercheurs).

- *Conférences, congrès et colloques à communication (Conférences internationales à comité de lecture et actes publiées) :*

Colloque WCIES, Lethbridge (Canada), Mai 2012.

Exposé « **Common invariant subspace and commuting matrices. »**

Colloque ILAS, Cancun (Mexique) , Juin 2008.

Exposé « **The equation log(XY)=log(X)+log(Y) ».**

Colloque SAGA 2007 (Mai 2007 à Tahiti) :

Exposé **«Algebraic attack on NTRU with Witt vectors) ».**