17e Forum des jeunes mathématicienn.ne.s
22-24 novembre 2017, Université de Lorraine

RÉSUMÉS DES EXPOSÉS

Conférences plénières

Véronique CORTIER.
Protocoles de sécurité : la logique comme outil d'analyse

Les protocoles de sécurité sont utilisés dans de nombreuses applications de la vie courante : automates bancaires, communication sécurisée sur Internet, porte-monnaie électronique, etc. La mise au point de ces protocoles, en apparence simples, est délicate. Certaines attaques ne sont découvertes que des années après le déploiement d'un protocole.

L'objectif de cet exposé est de présenter les objets et techniques, du domaine de la vérification, qui peuvent contribuer à la mise au point de protocoles sûrs. Nous étudierons ainsi certains fragments de la logique du 1er ordre et les procédures de décision associées. Certaines de ces procédures sont au coeur de l'outil ProVerif, utilisé pour détecter (automatiquement) des attaques sur des protocoles existants.

Marie-Pierre ETIENNE.
Quelques approches statistiques pour l'écologie du déplacement

L'inférence de modèles de mouvement donne un éclairage pertinent sur les mécanismes écologiques responsables des dynamiques au niveau individuel et/ou populationnel. Ces analyses sont essentielles pour les gestionnaires de la faune sauvage pour comprendre les comportements complexes des animaux. Dans le domaine de l'halieutique, Identifier les motifs qui expliquent l'utilisation que les pêcheurs font de l'espace est un élément essentiel d'une gestion durable des ressources marines. Ces deux domaines développent aujourd'hui de grands campagnes de déploiement de GPS. Les questions écologiques que l'ont peut étudier grâce à l'analyse de ce type de données sont très larges et la spécifité des données de trajectoires(objet spatio temporel) réclame de nouveaux développements méthodologiques.
Le domaine des statistiques pour l'écologie du mouvement est donc en plein essor et de nombreuses approches différentes sont proposées pour extraire des informations pertinentes de l'analyse des trajectoires. Parmi celles-ci nous pouvons distinguer :

— des modèles discret en temps et en espace (essentiellement des modèles de Markov sur grille)
— des modèles à temps discrets mais à espace d'états continu (marche aléatoire, modèle auto regressif vectoriel et modèles de Markov cachés)
— des modèles continus en temps et en espace (mouvement Brownien, Processus de Ornstein Uhlenbeck et plus généralement équation différentielle stochastique)

Dans cet exposé, nous mettrons en avant des développements récents relevant des deux derniers points.

En supposant que le mouvement est caractéristique d'un type d'activité, on peut chercher à identifier la succesion des activités en s'intéressant aux changements dans les propriétés du mouvement. Des méthodes de segmentations peuvent être utilisées pour réussir à identifier ces instants de changements.

Une autre hypothèse classique consiste à supposer que la partie déterministe d'un mouvement est dirigée par le potentiel de l'environnement.

Etudier la trajectoire doit ainsi donner de l'information sur ce potentiel environnemental. Le lien entre trajectoire et environnement est étudié grâce à des modèles d'équations différentielles stochastiques.

Sonia FLISS.

Les métamatériaux : de la quête de l'invisibilité à des problèmes mathématiques bien réels

Les metamaterieux suscitent depuis quelques années un grand intérêt de la communauté physicienne. Et pour cause, ces materiaux qui ont des caracteristiques effectives negatives pourraient permettre de réaliser des antennes miniatures, des super-lentilles et même des capes d'invisibilité. Les applications sont donc nombreuses. Mais pour l'instant nous en sommes loin. Pour comprendre ce qu'il se joue, il est utile de disposer de modèles mathématiques et de méthodes numériques adaptés pour simuler la propagation des ondes dans ces nouveaux matériaux. Je vais présenter des résultats récents, obtenus en collaboration avec Xavier Claeys (LJLL, Paris 6) et Valentin Vinoles qui a effectué sa thèse sur ce sujet, où nous avons amélioré certains modèles existants.

Sabrina SINIGAGLIA-AMADIO.

Filles et mathématiques : une histoire de petites empêchées...

L'analyse sociologique des mécanismes sociaux qui contribuent à la construction du (dé)goût pour les sciences, notamment des mathématiques, permettra d'interroger le rapport aux sciences des femmes et des hommes et de comprendre ce qui produit les discriminations et inégalités de traitement que l'on peut observer entre les sexes dans ce champ. Nous verrons ainsi comment les stéréotypes sexistes touchant aux sciences prennent place dans l'éducation réelle des enfants et participent à la constitution des réalités sociales du monde adulte.

Exposés courts

Zeina AL MASRY.

Processus gamma étendus en vue des applications à la fiabilité

Dans ce travail je m'intéresse à l'étude du fonctionnement d'un système industriel. Il s'agit de proposer et de développer un nouveau modèle de la dégradation accumulative d'un système. Le processus gamma standard est fréquemment utilisé pour étudier l'évolution de la détérioration d'un système (voir van Noortwijk (2009)) . Toutefois, ce processus peut s'avérer inadapté pour décrire le phénomène de dégradation car le rapport variance sur moyenne est constant dans le temps, ce qui est relativement restrictif en pratique. Afin de surmonter cette restriction, nous proposons d'utiliser un processus gamma étendu (EGP) introduit par Çinlar (1980), qui ne souffre plus de cette restriction. Mais ce dernier présente quelques difficultés techniques. A titre d'exemple, la loi d'un EGP n'est pas connue sous une forme explicite.
Le but de cette présentation est de présenter des outils techniques permettant d'utiliser un EGP dans un contexte applicatif.

Elena BERARDINI.

Courbes algébriques et codes correcteurs d'erreurs

Un code correcteur d'erreur est un objet qui a été introduit pour corriger les erreurs de transmission ou de lecture de données. La structure mathématique privilégiée pour ces codes sont les corps finis et, en particulier, la théorie des courbes algébriques sur les corps finis a permis de développer une famille spécifique des codes, les codes géométriques algébriques.
Soit $q = p^n$ une puissance d'un nombre premier, un code (linéaire) de type $[n, k, d]$ est la donnée d'un sous-espace vectoriel de dimension k sur $\mathbb{F}_q$ de distance minimale d, où l'on définit cette dernière quantité comme le minimum des distances entre chaque deux mots (vecteurs) du code. Un $[n, k, d]$-code peut détecter $d-1$ erreurs et en corriger au plus $\lfloor d - 1/2 \rfloor$. La borne de Singleton nous dit que la distance minimale d'un code ne peux pas dépasser $n+1-k$ et donc un des but de la théorie des codes correcteurs est de construire des codes avec distance minimale maximale par rapport à cette borne supérieure, les codes MDS (Maximum Distance Separable). Le code de Reed-Solomon, utilisant l'évaluation d'un polynôme défini sur un corps fini, est un code MDS. Sa généralisation aux polynômes de l'espace de Riemann Roch associé à une courbe algébrique projective, est un code géométrique algébrique, le code de Goppa. Les deux codes sont utilisés notamment dans le système cryptographique de McEliece.Dans cet exposé nous allons introduire la notion de code correcteur d'erreurs et la théorie liée aux courbes algébriques projectives sur les corps finis, pour présenter ensuite la construction de quelque codes géométriques algébriques.

Nacera DJEHAF.

Toward synthesizing numerically accurate code for Gauss pivoting method guided by interval and affine arithmetics

In numerical analysis of mechanical contact problems, we usually have to solve huge linear systems, which may be non-symmetric or hill-conditioned. For these reasons, it is necessary to develop original and domain specific approaches to treat these families of systems. In this work, we introduce a new methodology to synthesize numerically accurate programs for the Gauss pivoting method. The synthesis is guided by affine arithmetic which is an extension of interval arithmetic that responds to the variable dependency problem, which occurs in particular in the estimation of the range of a function. We aim at applying our code synthesis to the resolution of systems coming from finite element method.

Charles DUMENIL.
Expected size of the Delaunay triangulation of a surface

Dans le plan, la triangulation de Delaunay d'un ensemble P de n points du plan est une triangulation $DT(P)$ telle qu'aucun point de P n'est à l'intérieur du cercle circonscrit d'un des triangles de $DT(P)$. On appelle taille de la triangulation le nombre de triangles ainsi construits. La relation d'Euler permet de calculer cette taille, à savoir $O(n)$. Dans l'espace $3d$, la relation d'Euler n'est pas suffisante et on peut trouver des triangulations en $\Omega(n^2)$.

Lorsque les points sont répartis sur une surface de manière suffisamment homogène, on sait borner la taille de la triangulation d'une surface dite générique par $O(n \ln n)$ alors que les observations laissent penser que la triangulation est en $\Theta(n)$. Cette différence a été résolu par une modélisation aléatoire dans le cas du cylindre (qui n'est pas une surface générique). Là où la taille de la triangulation était en $O(n\sqrt{n})$ dans le pire des cas avec des moyens déterministes, considérer un échantillon aléatoire de points mène à une taille en $\Theta(n \ln n)$ en moyenne, ce qui correspond aux observations.

Au vu de ce résultat, on cherche donc à appliquer cette méthode pour les surfaces génériques afin de retrouver une taille en $\Theta(n)$ en moyenne.

Youssef ESSTAFA.
Estimation des modèles FARIMA avec un bruit non corrélé mais non indépendant

Travail en collaboration avec Yacouba Boubacar et Bruno Saussereau.
Dans ce travail, nous étudions les propriétés asymptotiques (convergence et normalité) de l'estimateur des moindres carrés des paramètres d'un modèle FARIMA (pour Fractionally AutoRegressive Integrated Moving-Average) avec un bruit non corrélé mais qui peut contenir des dépendances non linéaires. Les modèles FARIMA occupent une place centrale pour la modélisation des processus à mémoire longue, ils permettent d'identifier les phénomènes de persistance. Relâcher l'hypothèse standard d'indépendance sur le bruit permet à ces modèles de couvrir une large classe de processus à mémoire longue non linéaires. La convergence forte et la normalité asymptotique de l'estimateur sont démontrées sous certaines hypothèses d'ergodicité et de mélange.

Anna FLORIO.
La dynamique des maps twist et ses propriétés.

Les maps twist qui préservent l'aire représentent un cadre utile à décrire différentes phénomènes. Introduits pour la première fois par Poincaré, les maps twist décrivent, pour exemple, la dynamique des voisinages des points particuliers dans le problème des 3 corps en mécanique céleste. En plus, ces maps sont aussi liées au modèle discrète de Frenkel-Kontorova (qui explique comment chaînes des particules interagissent) et aux autres systèmes appliqués. L'étude des propriétés des maps twist nous permit de mieux comprendre ces différentes phénomènes. Après l'introduction de ces définitions, je présent des propriétés relatives au comportement rotationnel asymptotique du système.

Simon GIREL.
Modélisation mathématique de la réponse immunitaire T-CD8

Suite à l'infection d'un organisme par un pathogène intra-cellulaire, les cellules T-CD8+ naïves situées dans les ganglions lymphatiques sont activées par les cellules présentatrices d'antigène. Il s'ensuit une phase dite d'expansion clonale au cours de laquelle les cellules T activées prolifèrent rapidement et se différencient en cellules effectrices, capables d'éliminer les cellules infectées pour combattre l'infection. Enfin, après élimination de l'infection, 90 à 95 % des cellules effectrices meurent par apoptose pendant la phase de contraction tandis que les cellules restantes se différencient en cellules mémoires et garantissent une réponse plus rapide et plus efficace en cas de rencontre ultérieure de l'organisme avec le même pathogène. Un modèle hybride discret-continu et multi-échelle de la réponse immunitaire T-CD8 a été développé au sein de l'équipe Inria Dracula. À l'échelle cellulaire, une population discrète de cellules T-CD8 est décrite par un modèle à base d'agents, implémenté dans CompuCell3D. Chaque cellule est modélisée par un ensemble de pixels sur grille en 2D sur laquelle elle peut se déplacer, se diviser, intéragir avec son environnement, se différencier ou mourir. À l'échelle moléculaire, un réseau génétique intracellulaire simplifié, dont l'état caractérise la différenciation et la mort cellulaire, a été identifié puis modélisé par un système d'EDOs. Ce réseau moléculaire, identique dans chaque cellule, reste influencé par les interactions cellule-cellule, permettant à chaque cellule de développer un profil moléculaire unique. Ce modèle permet de s'intéresser aux conséquences d'événements moléculaires, notamment lors de l'activation des cellules, sur la dynamique de la population cellulaire dans les premiers instants de la réponse immunitaire T-CD8, la différenciation en cellule mémoire n'étant pas considérée. Considérant une répartition asymétrique des protéines intracellulaires entre deux cellules filles au moment de la division cellulaire, nous avons étudié l'effet du degré d'asymétrie sur l'évolution du profil moléculaire d'une cellule au moyen d'une équation non-linéaire à impulsions, issue du système d'EDOs. Dans cette étude nous montrons, à partir de résultats d'existence et de stabilité de solutions périodiques, comment le phénomène de division asymétrique peut affecter le destin cellulaire et, en particulier, le développement d'une population mémoire. Je présenterai les principaux résultats de cette étude, puis comment ces résultats ont permis d'enrichir le modèle à base d'agents précédent, désormais capable de décrire qualitativement les différentes phases (activation, expansion, contraction, mémoire) de la réponse T-CD8, au niveaux cellulaire et moléculaire.

Zhen Wai Olivier HO.
Le modèle Hüssler-Reiss Pareto

On s'intéresse à la théorie des valeurs extrêmes multivariées. La théorie probabiliste y est bien développée, on peux citer par exemple Gudendorf et Segers pour un revue du point de vue copule. Des travaux récents se concentrent sur la modélisation d'excès dans un cadre multivarié et qu'on appelle les modèles de Pareto généralisé. Les papiers précurseurs sont dûs à Coles et Tawn ainsi que Rootzén et Tajvidi. Des développements plus récent de Rootzén et co ainsi que Kiriliouk et co développent l'aspect modélisation et statistique du sujet. Dans ce travail, on adopte le point de vue des variations régulières multivariées et on étudie les modèles limites issus de modèles simples de la forme X=RZ où X est une variable réelle à queue lourde et Z un vecteur aléatoire suffisament intégrable. Dans le cas où Z suit une loi log-normale, le modèle limite associé est le modèle Hüssler-Reiss. On développe ainsi le modèle de Pareto associé sous le contexte de la théorie de familles exponentielles et on fini par une étude de simulations.

Clémence KARMANN.
Inférence de réseaux pour modèles inflatés en zéros

Un graphe est composé de noeuds et d'arêtes entre ces noeuds. L'inférence de graphe s'est largement développée ces dernières années. Supposons que l'on connaisse la valeur de p variables sur n sujets (dans beaucoup d'applications, $n << p$). L'inférence de réseau consiste à évaluer le lien entre deux variables connaissant les autres variables ; souvent, deux variables sont connectées si elles ne sont pas indépendantes conditionnellement aux autres variables de l'ensemble. L'inférence de réseaux a de plus en plus d'applications notamment en santé humaine et en environnement pour l'étude de données micro-biologiques et génomiques. Le traitement des données d'abondance (de micro-organismes comme les bactéries par exemple) est notamment particulier par le fait qu'une espèce peut être absente dans beaucoup d'échantillons. On est alors dans le cadre de données à zéros inflatés. Beaucoup de méthodes d'inférence de réseaux existent pour les données gaussiennes, les données binaires et les données mixtes mais les modèles à zéros inflatés sont très peu étudiés alors qu'ils reflètent bien la structure de nombreux jeux de données.

Marie KERJEAN.
Logique linéaire et EDP linéaires.

La logique linéaire (LL) est un système formel dont l'étude se nourrit de ses interprétations sémantiques. En particulier, la logique linéaire transmet la notion algébrique de linéarité aux domaines de la théorie de la démonstration et de la programmation. Suite à l'étude de modèles vectoriels quantitatifs de LL, Ehrhard et Regnier ont introduit la logique linéaire différentielle, un raffinement de LL où les preuves peut être différenciées.

Alors que l'étude de LL est traditionnellement algébrique, cette introduction de la différentiation sur la syntaxe de LL pose l'exigence d'une interprétation des preuves par des objets lisses, par exemple comme des fonctions lisses entre espaces vectoriels topologiques. Or l'étude sémantique de LL pose des exigences fortes qui sont rarement satisfaites dans le cadre topologique. Dans cet exposé, je parlerai de la catégorie des espaces nucléaires Fréchet, et de la manière dont on peut interpréter les preuves d'une certaine logique linéaire différentielle comme des espaces de distributions. Je montrerai comment, à chaque EDP linéaire à coefficient constant nous pouvons associer un sous-système de cette logique linéaire différentielle. Nous verrons aussi comment, à l'inverse, nous parvenons à isoler la structure catégorique et syntaxique permettant de résoudre une EDP linéaire.

Anna KORBA.
A learning theory for ranking aggregation

Joint work with Stephan Clémençon and Eric Sibony.
We develop a statistical learning theory for ranking aggregation and assess the generalization ability of empirical ranking medians. Beyond the characterization of optimal solutions for the Kemeny aggregation problem, universal rate bounds are established and the situations where convergence occurs at an exponential rate are fully characterized.

Florian LIETARD.
Evitabilité des k-puissances additives

En 2011, un article de J. Cassaigne, J. D. Currie, L. Schaeffer et J. Shallit montrait qu'il était possible, en utilisant un alphabet de 4 chiffres, de construire un mot infini qui évite les cubes additifs. Autrement dit on ne peut pas trouver dans ce mot trois blocs consécutifs de mêmes tailles et de mêmes sommes de chiffres. Au delà de ce résultat, l'étude de la structure de cette preuve permet d'étendre le travail effectué par Cassaigne et al. et d'émettre plusieurs conjectures sur les mots évitant les cubes additifs.

Aline MOUFLEH.
Détection de tendance dans les extrêmes

La théorie des valeurs extrêmes univariée classique étudie la queue distribution pour des observations indépendamment et identiquement distribuées. Dans notre travail, on s'intéresse au cas où les observations sont indépendantes mais non identiquement distribuées. Cette variation dans la distribution est quantifiée en utilisant une fonction dite "skedasis function" notée c qui représente la fréquence des extrêmes. Ce modèle a été introduit par Einmahl et al. dans le papier « Statistics of heteroscedastic extremes » où les auteurs donnent une estimation non paramétrique de la fonction primitive de c basée sur les k plus grandes valeurs de la série d'observations. On présentera plusieurs modèles paramétriques pour c (log-linéaire, linéaire, log-linéaire discret) ainsi que les résultats de consistance et de normalité asymptotique du paramètre θ représentant la tendance. Le test $\theta = 0$ versus $\theta \neq 0$ est interprété alors comme un test de détection de tendance dans les extremes. Nos résultats seront illustrés dans une étude par simulation. Enfin, les simulations montrent que les tests paramétriques sont en général plus puissants que les tests non paramétriques pour la détection de la tendance, d'où l'utilité de notre travail.

Lauréline PEROTIN.
Séparation de sources de parole avec des réseaux de neurones

La séparation de source audio consiste à extraire une ou plusieurs sources d'un mélange. C'est notamment un pré-traitement indispensable pour la reconnaissance automatique de la parole en situation difficile, comme la commande vocale à distance ou la transcription automatique de réunions. Dans ces cas, la reconnaissance est mise à mal par la présence de réverbération, de bruit de fond ou de plusieurs locuteurs s'exprimant en même temps. On présentera ici un système de séparation de sources audio qui utilise un filtre multicanal calculé grâce à un réseau de neurones récurrent (LSTM).

Tom RIBLET.
Le processus de contact en environnement aléatoire

Dans cet exposé, je commencerai par introduire le processus de contact qui est un des plus simples systèmes de particules en interaction. Le comportement de ce processus dépend fortement de l'environnement sur lequel on le fait vivre. Aussi, je présenterai ensuite l'environnement aléatoire auquel je me suis intéressé dans le cadre de ma thèse et enfin, j'expliquerai certains résultats comme le théorème de forme asymptotique qui décrit assez précisément l'évolution du processus de contact.

Meryem SLAOUI.
La solution de l'équation de la chaleur stochastique dirigée par un bruit Hermite

La classe des processus d'Hermite inclut le mouvement Brownian fractionnaire , qui est le seul processus d'Hermite gaussien et le processus de Rosenblatt. De par leurs propriétés, les processus d'Hermite possèdent un grand champ d'applications : hydrologie, télécomunications, économie, physique, etc. Nous considérons la solution mild de l'équation de chaleur stochastique dirigée par un processus d'Hermite multidimensionnel. Nous étudions l'existence et quelques propriétés analytiques de la solution mild. Nous établissons également un théorème de décomposition de la solution et détaillons le cas où nous avons plus d'éléments pour étudier la loi de la solution. Nous utiliserons enfin, la décomposition obtenue pour le calcul des variations du processus par rapport à la variable temps.

Zhiwei WANG.
Sur les plus grands facteurs premiers d'entiers consécutifs et d'entiers consécutifs voisins d'un entier criblé

Un enjeu important en cryptographie est de comprendre la factorisation des entiers. Si on sait déterminer les facteurs premiers des entiers de grande taille alors on remet en cause la sécurité de chiffrements à clé publique tels le système RSA. Pour le moment des questions d'énoncé très simple sont toujours hors d'atteinte. Désignons par $P(n)$ le plus grand facteur premier d'un entier n. Quelle est la densité de l'ensemble des entiers n tels que $P(n+1) > P(n)$? La réponse attendue est $1/2$. C'est l'un des problèmes "non conventionnels" d'Erdos. Dans cet exposé nous montrons que cette proportion est supérieure à $1/8$. C'est une amélioration de travaux récents de La Bretèche, Pomerance et Tenenbaum. Nous montrons également qu'il existe une proportion positive d'entiers n tels que $P(n) = \max(P(n-1), P(n), P(n+1))$. On obtient un résultat analogue pour les entiers n tels que $P(n) = \min(P(n-1), P(n), P(n+1))$.

Hanane ZERDOUM
On the Harborth constant of $C_3 \oplus C_{3p}$

Let $(G, +, 0)$ be a finite abelian group. The Harborth constant of G, denoted $g(G)$, is the smallest integer t such that every subset A of G of size $|A| \geq t$ contains a subset of size $\exp(G)$ whose elements have sum 0. This constant was introduced by Harborth ; it is a variant of the Erdös–Ginzburg–Ziv constant. Its value is so far only known for a few types of groups. For groups of exponent 2 it is easy to see that $g(G) = |G| + 1$ as the sum of two distinct elements is never 0, and for cyclic groups one finds easily that the Harborth constant is equal to $|G|$ if $|G|$ is odd and $|G| + 1$ otherwise. These simple cases apart the problem becomes challenging. For groups of exponent 3 it is equivalent to the cap-set problem in ternary spaces, a well- known hard problem in discrete geometry and additive combinatorics. For the direct sum of two cyclic groups of prime order $p \geq 67$, it was shown by Gao and Thangadurai that $g(C_p^2) = 2p - 1$. Moreover, for groups of the form $C_2 \oplus C_{2n}$ it is known by a result of Marchan, Ordaz, Ramos, and Schmid that $g(C_2 \oplus C_{2n})$ is equal to $2n + 2$ for even n and equal to $2n + 3$ for odd n. The talk gives an overview on ongoing joint work with Marchan, Guillot, Ordaz, and Schmid on the value of the Harborth constant for the groupe $C_3 \oplus C_{3n}$. As our main result we determine the exact value in case n is a prime number ; concretely we show that $g(C_3 \oplus C_{3n}) = 3n + 3$ for prime $n \neq 3$ and $g(C_3 \oplus C_{3n}) = 3n + 4$ for $n = 3$.