INSTITUT DE FRANCE
Académie des sciences

FRENCH-ISRAELI INTER ACADEMIC MEETING ON MATHEMATICS

22 - 23 MAY 2013

FRENCH ACADEMY OF SCIENCES

ISRAEL ACADEMY OF SCIENCES AND HUMANITIES

PROGRAM COMMITTEE

Catherine BRÉCHIGNAC
David KAZHDAN
Michael RABIN
Christophe SOULÉ
Jean-Christophe YOCCOZ

PARIS

Académie des sciences – Salle Hugot
23 quai de Conti – 75006 Paris

Registration required, before May 20, 2013
nathalie.zajdman@academie-sciences.fr

INSTITUT DE FRANCE
Académie des sciences

WEDNESDAY, MAY 22ND Morning

8h30 ***Welcome***

9h ***Welcome addresses***
Catherine BRÉCHIGNAC, Secrétaire perpétuel of the French Academy of Sciences
Ruth ARNON, President of the Israel Academy of Sciences and Humanities
Christophe SOULÉ, French Co-President of the meeting
Michael RABIN, Israeli Co-President of the meeting
David KAZHDAN, Israeli Co-President of the meeting

9h30 **Leonid POLTEROVICH** (Tel Aviv University)
Symplectic Topologist's Tale of Quantum Mechanics

10h30 - coffee break

10h45 **Vincent LAFFORGUE** (CNRS, université d'Orléans)
Langlands parameters and the cohomology of the moduli space of G-shtukas

11h45 **David KAZHDAN** (The Hebrew University)
An interaction between the Representation Theory and the Category Theory

WEDNESDAY, MAY 22ND Afternoon

14h30 **Michèle VERGNE** (CNRS, université Paris VII)
Equivariant index of an elliptic operator and splines

15h30 **Tamar ZIEGLER** (Technion-Israel Institute of Technology)
Dynamics and Prime Solutions to Linear Systems

16h30 **Jean-François QUINT** (université Paris XIII)
Random walks on homogeneous spaces

INSTITUT DE FRANCE
Académie des sciences

THURSDAY, MAY 23RD Morning

9h **Welcome**

9h15 **Opening remarks by Michael Rabin**

9h30 **Olivier FAUGERAS** (INRIA, Sophia Antipolis)
A large deviation principle for networks of rate neurons with correlated synaptic weights

10h30 - coffee break

10h45 **Michael RABIN** (The Hebrew University, Harvard University, Columbia University)
Cryptography and preventing collusion in auctions

11h45 **Gil KALAI** (The Hebrew University)
Why quantum computers cannot work

THURSDAY, MAY 23RD Afternoon

14h30 **Claude BERROU** (Télécom Bretagne)
A mental information theory

15h30 **Ran RAZ (**The Weizmann Institute of Science)
Interactive Channel Capacity

16h30 **Claire MATHIEU** (CNRS, École normale supérieure)
Better algorithms with hierarchies of semi-definite programs

French organising Committee

Maurice Gross - tél. 33(0)1.44.41.44.24

Monique Royer - tél. 33(0)1.44.41.43.93
monique.royer@academie-sciences.fr

Nathalie Zajdman - tél. 33(0)1.44.41.44.31
nathalie.zajdman@academie-sciences.fr

ABSTRACTS

Symplectic Topologist's Tale of Quantum Mechanics

Leonid POLTEROVICH, Tel Aviv University

We focus on constraints on the Poisson brackets found within Symplectic topology. Their interpretation and proof are related to Quantum Mechanics. In the talk, we discuss an exchange of ideas between these fields.

Langlands parameters and the cohomology of the moduli space of G-shtukas

Vincent LAFFORGUE, CNRS, université d'Orléans

For any reductive group G over a global function field, we use the cohomology of the moduli space of G-shtukas with multiple legs to prove the global Langlands correspondence for G in the direction "from automorphic to Galois". Moreover we obtain a canonical decomposition of cuspidal automorphic forms indexed by Langlands parameters.

An interaction between the Representation Theory and the Category Theory

David KAZHDAN, The Hebrew University

The theory of representations of not necessarily abelian finite groups *G* was created by Frobenius. More precisely, Frobenius originally defined the commutative representation ring *R*(*G*), which he later upgraded to the category *C*(*G*) of finite-dimensional representations of *G*. In the recent years, the new level of the categorification became important in different areas of the Representation Theory. I will discuss some examples of this phenomenon.

Equivariant index of an elliptic operator and splines

Michèle VERGNE, CNRS, université Paris VII

Let G be a torus, and let D be a transversally elliptic operator on a manifold M. Then index(D) decomposes as a sum of characters e_lambda of G, with multiplities m(\lambda).
We determine a piecewise polynomial function (a spline function) on the dual g^* of the Lie algebra of G which restricted to the lattice of weights coincide with the function m(lambda).
The equivariant Riemann-Roch theorem is equivalent to a deconvolution formula for the Box spline, a particular spline function familiar in approximation thory.
This work is in common with De Concini and Procesi.

Dynamics and Prime Solutions to Linear Systems

Tamar ZIEGLER, Technion-Israel Institute of Technology

A classical theorem of Dirichlet establishes the existence of infinitely many primes in arithmetic progressions, so long as there are no local obstructions. In 2006 Green and Tao set up a programme for proving a vast generalization of this theorem. They conjectured a relation between the existence of linear patterns in primes and dynamics on nilmanifolds. In joint work with Green and Tao, we completed the final step of this programme, establishing Hardy-Littlewood type estimates for the number of prime solutions to systems of linear equations of finite complexity.

Random walks on homogeneous spaces

Jean-François QUINT, université Paris XIII

In this talk, I will present probabilistic tools which allow to get new results about orbits of group actions on homogeneous spaces, in the spirit of the works of Furstenberg, Margulis and Ratner.
This is a joint work with Yves Benoist.

A large deviation principle for networks of rate neurons with correlated synaptic weights

Olivier FAUGERAS, INRIA, Sophia Antipolis

We study the asymptotic law of a network of interacting neurons when the number of neurons becomes infinite. Given a completely connected network of firing rate neurons in which the synaptic weights are Gaussian correlated random variables, we describe the asymptotic law of the network when the number of neurons goes to infinity. We introduce the process-level empirical measure of the trajectories of the solutions to the equations of the finite network of neurons and the averaged law (with respect to the synaptic weights) of the trajectories of the solutions to the equations of the network of neurons.
The main result of this article is that the image law through the empirical measure satisfies a large deviation principle with a good rate function which is shown to have a unique global minimum. Our analysis of the rate function allows us also to characterize the limit measure as the image of a stationary.
Gaussian measure dened on a transformed set of trajectories. This is potentially very useful for applications in neuroscience since the Gaussian measure can be completely characterized by its mean and spectral density. It also facilitates the assessment of the probability of finite-size effects.
This is a joint work with James MacLaurin

Cryptography and preventing collusion in auctions

Michael RABIN, The Hebrew University, Harvard University, Columbia University

We present practically efficient methods for proving correctness of announced results of a computation while keeping input and intermediate values information theoretically secret. These methods are applied to proving correctness of announced outcome of an auction while keeping bid-values secret and to solve the long standing problem of preventing collusion in second-price (Vickery) auctions.

Why quantum computers cannot work

Gil KALAI, The Hebrew University

Quantum computers are hypothetical devices based on quantum physics that can out-perform classical computers. A famous algorithm by Peter Shor shows that quantum computers can factor an integer n in C(log n)^3 steps. The question if quantum computer are realistic is one of the most fascinating and clear-cut scientific problems of our time, and my work is geared toward a negative answer. The main concern from the start was that quantum systems are inherently noisy; we cannot accurately control them, and we cannot accurately describe them. To overcome this difficulty, a fascinating notion of quantum error-correction and a remarkable theory of quantum fault-tolerance were developed.

What makes it still hard to believe that superior quantum computers can be built is that building universal quantum computers represents a completely new reality in terms of controlled and observed quantum evolutions, and also a new computational complexity reality. What makes it hard to believe that quantum computers cannot be built is that this may require profoundly new insights in the understanding quantum mechanical systems (including in regimes where people do not expect such new insights.).

My explanation for why (fault-tolerant) quantum computers cannot be built is that quantum systems based on special-purpose quantum devices are subject to noise which systematically depends on the quantum evolution of the system; this dependence reflects dependence of the noise on the quantum device, and the dependence of the quantum device on the quantum evolution it is performing. (Here, "a quantum device" refers both to human-made and to natural devices.) This systematic dependence causes general-purpose quantum computers to fail. The challenge is to understand the systematic laws for this dependence.

In the lecture I will proposed a mathematical model for realistic noisy quantum systems called "smoothed Lindblad evolution," which excludes quantum fault-tolerance, and discuss some further conjectures on the behavior of realistic noisy quantum computers.

A mental information theory

Claude BERROU, Télécom Bretagne

The way information is stored, recalled and processed in the neocortex is assuredly one of the most puzzling enigmas that science will have to solve during this century.
This talk will address the question of “mental information” in the light of the most recent developments in information theory, especially distributed error correction coding and decoding. Under some reductionist hypotheses, distributed coding may explain the prominent properties of robustness and durability of mental information.

Interactive Channel Capacity

Ran RAZ, The Weizmann Institute of Science

Few papers in the history of science have affected the way people think in so many branches of science, as profoundly as Shannon's 1948 paper ``A Mathematical Theory of Communication''. One of the gems in that paper is an exact formula for the channel capacity of any communication channel. For example, for the binary symmetric channel with noise rate ϵ, the channel capacity is $1-H(\epsilon)$, where H denotes the binary entropy function. This means that one can reliably communicate n bits, with a negligible probability of error, by sending roughly $n/(1-H(\epsilon))$ bits over the channel.
We study the interactive channel capacity of an ϵ-noisy channel. The interactive channel capacity $C(\epsilon)$ is defined as the minimal ratio between the communication complexity of a problem (over a non-noisy channel), and the communication complexity of the same problem over the binary symmetric channel with noise rate ϵ, where the communication complexity tends to infinity. Our main result is the upper bound $C(\epsilon) \leq 1-\Omega(\sqrt{H(\epsilon)})$. This compares with Shannon's non-interactive channel capacity of $1-H(\epsilon)$. In particular, for a small enough ϵ, our result gives the first separation between interactive and non-interactive channel capacity, answering an open problem by Schulman (1992).
We complement this result by the lower bound $C(\epsilon) \geq 1-O(\sqrt{H(\epsilon)}),$ proved for the case where the players take alternating turns.

Better algorithms with hierarchies of semi-definite programs

Claire MATHIEU, CNRS, École normale supérieure

This is joint work with Anna Karlin and Thach Nguyen