Programme du Colloque scientifique

Théorie de l'information : nouvelles frontières

dans le cadre du Centenaire de Claude Shannon

Du 26 au 28 octobre 2016, à l'Institut Henri Poincaré, Paris V^{ème}

Informations pratiques

- Gratuit dans la limite des places disponibles
- Adresse : 11 rue Pierre et Marie Curie, 75005 Paris
- Inscriptions en ligne à partir du 5 septembre 2016 sur www.shannon100.fr
- Contact : shannon100@ihp.fr

Avec le soutien du Cercle des partenaires de l'IHP et de l'Institut Mines-Télécom

Programme synthétique du colloque

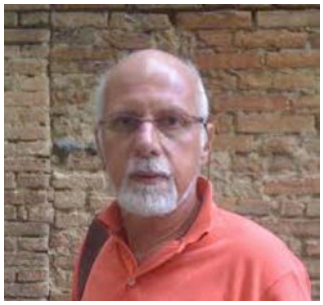
	Heure	Exposé	Intervenant
Mercredi 26 octobre - matin	9.45	Discours d'ouverture	Cédric Villani, IHP
	10.00	Shannon's legacy in combinatorics	János Körner, Université de Rome
	11.00	Entropie, compression et statistique	Elisabeth Gassiat, Université Paris-Sud
Mercredi 26 octobre - après-midi	13.30	Comment concevoir un algorithme de chiffrement sûr et efficace : L'héritage de Shannon	Anne Canteaut, INRIA Paris
	14.30	Random Matrices and Telecommunications	Mérouane Debbah, CentraleSupélec
	16.00	Shannon's Formula W log(1+SNR): A Historical Perspective	Olivier Rioul, Télécom-ParisTech
Jeudi 27 octobre - matin	10.00	How information theory sheds new light on black-box optimization	Anne Auger, INRIA Saclay
	11.00	Mesure de l'énergie minimale nécessaire à l'effacement d'un bit d'information et relation avec l'égalité de Jarzynski	Sergio Ciliberto, ENS Lyon
Jeudi 27 octobre - après-midi	13.30	Vers une théorie de l'information mentale	Vincent Gripon, Télécom Bretagne
	14.30	Information, simplicité et pertinence	Jean-Louis Dessalles, Télécom-ParisTech
	16.00	En suivant Shannon : de la technique à la compréhension de la vie	Gérard Battail, Télécom-ParisTech ER
Vendredi 28 octobre - matin	10.00	The dual geometry of Shannon information and its applications	Frank Nielsen, Polytechnique
	11.00	Happy Numbers: 68 Years of Coding, $6^2 + 8^2 = 100$ Years of Shannon, $1^2 + 0^2 + 0^2 = 1$ Goal	Ruediger Urbanke, EPFL
Vendredi 28 octobre - après-midi	13.30	Claude Shannon: His life, modus operandi, and impact	Robert Gallager, MIT ER

Programme détaillé du colloque

Mercredi 26 octobre 2016

10h 00 : Shannon's legacy in combinatorics

János Körner (Université de Rome La Sapienza)



Abstract: In 1956 Claude Shannon defined the zero-error capacity of a discrete memoryless channel. He realized that the problem of its determination is immensely difficult and a simple formula for this capacity might not exist. Nevertheless, through the fortunate notion of perfect graphs of Claude Berge inspired by the concept of Shannon a new and beautiful chapter in graph theory was born. More generally, Shannon's notion leads to a theory about the asymptotic behaviour of basic invariants in product structures. We explore the resulting merger of combinatorics and information theory.

János Körner was born in Budapest on November 30, 1946. He got his degree in mathematics from Eötvös Loránd University, Budapest in 1970. He was a member of the Rényi Institute of Mathematics of the Hungarian Academy of Sciences from 1970 to 1991. He has been working in Italy from 1992 where he became a professor at Sapienza University of Rome in 1994. His research is concerned with Information Theory and Extremal Combinatorics. He is a Honorary Member of the Rényi Institute of Mathematics. In 2010 he got elected to the Hungarian Academy of Sciences as an External Member. In 2014 he obtained the Claude Shannon Award of the Information Theory Society of the IEEE.

11h00 : Entropie, compression et statistique

Elisabeth Gassiat (Université de Paris-Sud)

Résumé : Claude Shannon est l'inventeur de la théorie de l'information. Il a introduit la notion d'entropie comme mesure de l'information contenue dans un message vu comme provenant d'une source stochastique et démontré son lien avec les possibilités de compression de ce message. Le lien avec les méthodes statistiques est profond et la théorie de l'information a été source d'inspiration pour les théoriciens des statistiques. La compression de sources dont le nombre de valeurs possibles est grand peut être comprise comme un problème de statistique adaptative. Quelques résultats récents de codage adaptatif seront présentés.

E. Gassiat est diplômée de l'école Polytechnique, a soutenu une thèse de mathématiques en 1988 à l'Université Paris-Sud et obtenu son HDR en 1993. Elle est professeur à l'Université Paris-Sud (Orsay) depuis 1998.

13h30 : Comment concevoir un algorithme de chiffrement sûr et efficace : l'héritage de Shannon

Anne Canteaut (INRIA)

Résumé : Dans son article fondateur publié en 1949 posant les fondements de la cryptographie, Claude Shannon a énoncé deux méthodes de conception visant à éviter les attaques statistiques : la diffusion et la confusion. Ces deux techniques sont toujours au cœur des algorithmes symétriques modernes et permettent d'optimiser leur résistance aux cryptanalyses les plus connues, notamment aux cryptanalyses différentielle et linéaire. Ces principes ont par exemple présidé à la conception du standard actuel de chiffrement symétrique, l'AES, et ont motivé de nombreuses recherches liant cryptographie et mathématiques discrètes.

Anne Canteaut est directrice de recherche à l'Inria de Paris, et responsable scientifique de l'équipe-projet SECRET. Son domaine de recherche est la cryptographie symétrique. Ses travaux portent à la fois sur la

conception de nouveaux systèmes cryptographiques, l'attaque de systèmes existants, et l'étude des objets mathématiques mis en jeu.

14h30 : Random Matrices and Telecommunications

Mérouane Debbah (CentraleSupélec et Huawei France R&D)

Abstract: The asymptotic behaviour of the eigenvalues of large random matrices has been extensively studied since the fifties. One of the first related result was the work of Eugène Wigner in 1955 who remarked that the eigenvalue distribution of a standard Gaussian hermitian matrix converges to a deterministic probability distribution called the semi-circular law when the dimensions of the matrix converge to infinity. Since that time, the study of the eigenvalue distribution of random matrices has triggered numerous works, in the theoretical physics as well as probability theory communities. However, as far as communications systems are concerned, until the mid 90's, intensive simulations were thought to be the only technique to get some insight on how communications behave with many parameters. All this changed in 2000 when large system analysis based on random matrix theory was discovered as an appropriate tool to gain intuitive insight into communication systems. In particular, the self-averaging effect of random matrices was shown to be able to capture the parameters of interest of communication schemes. Since then, the results led to very active research in many fields such as MIMO systems or Ultra-Dense Networks. This talk is intended to give a comprehensive overview of random matrices and their application to the latest design of 5G Networks.

Mérouane Debbah entered the Ecole Normale Supérieure de Cachan (France) in 1996 where he received his M.Sc and Ph.D. degrees respectively. Since 2007, he is a Full Professor at CentraleSupelec (Gif-sur-Yvette, France). From 2007 to 2014, he was the director of the Alcatel-Lucent Chair on Flexible Radio. Since 2014, he is Vice-President of the Huawei France R&D center and director of the Mathematical and Algorithmic Sciences Lab. His research interests lie in fundamental mathematics, algorithms, statistics, information & communication sciences research. M. Debbah is a recipient of the ERC grant MORE (Advanced Mathematical Tools for Complex Network Engineering). He is a IEEE Fellow and a WWRF Fellow. In his career, he received more than 16 Best Paper Awards, the latest being the 2015 IEEE Communications Society Leonard G. Abraham Prize, the 2015 IEEE Communications Society Fred W. Ellersick Prize as well as the 2016 IEEE Communications Society Best Tutorial paper award.

16h00 : Shannon's Formula Wlog(1+SNR): A Historical Perspective

Olivier Rioul (Télécom-ParisTech)

Abstract: As is well known, the milestone event that founded the field of information theory is the publication of Shannon's 1948 paper entitled "A Mathematical Theory of Communication". This article brings together so many fundamental advances and strokes of genius that Shannon has become the hero of thousands of researchers, praised almost as a deity. One can say without exaggeration that Shannon's theorems are the mathematical theorems which have made possible the digital world as we know it today. We first describe some of his most outstanding contributions, culminating with Shannon's emblematic capacity formula C = W.log(1+P/N) where W is the channel bandwidth and P/N is the channel signal-to-noise ratio (SNR). Incidentally, Hartley's name is often associated with the same formula, owing to "Hartley's rule": Counting the highest possible number of distinguishable values for a given amplitude A and precision D yields a similar expression log(1 + A/D). In the information theory community, the following "historical" statements are generally well accepted:
(1) Hartley put forth his rule in 1928, twenty years before Shannon;
(2) Shannon's formula as a fundamental trade-off between transmission rate, bandwidth, and signal-to-noise ratio came unexpected in 1948;
(3) Shannon's formula is exact while Hartley's rule is imprecise;
(4) Hartley's expression is not an appropriate formula for the capacity of a communication channel.

We show that all these four statements are somewhat wrong:
(1) Hartley's rule does not seem to be Hartley's.
(2) At least seven other authors have independently derived formulas very similar to Shannon's in the same year 1948 — the earliest published original contribution being a Note at the Académie des Sciences by a French engineer Jacques Laplume.
(3) A careful calculation shows that Hartley's rule does coincide with Shannon's formula.
(4) Hartley's rule is in fact mathematically correct as the capacity of a communication channel, where the noise is not Gaussian but uniform, and the signal limitation is not on the power but on the amplitude.
(This talk was presented in part at the MaxEnt 2014 conference in Amboise as a joint work with José Carlos Magossi (Unicamp, São Paulo State, Brasil)).

Olivier Rioul (PhD, HDR) is professor at Télécom ParisTech and École Polytechnique, France. His research interests are in applied mathematics and include various, sometimes unconventional, applications of information theory such as inequalities in statistics, hardware security, and experimental psychology.

Jeudi 27 octobre 2016

10h00: How information theory sheds new light on black-box optimization

Anne Auger (INRIA)

Abstract: Black-box optimization problems occur frequently in many domains ranging from engineering to biology or medicine. In black-box optimization, no information on the function to be optimized besides current and past evaluations of search solutions can be exploited. Particularly, the existence of gradients or convexity of the function is not assumed in a numerical black-box scenario. Black-box optimization methods should typically be able to solve a wide range of problems exhibiting many difficulties (non-convex, noisy, multi-modal, ...). In this talk I will explain how information theory has recently shed new light on the domain of black-box optimization. I will show how stochastic black-box algorithms for optimization on an arbitrary search space can be derived from principles issued from information theory. I will then explain that the ensuing information-geometric optimization (IGO) algorithm instantiated on the family of Gaussian distributions or Bernoulli distributions turns out to partially coincide with state-of-the art stochastic black-box algorithms like CMA-ES or PBIL. Both algorithms were introduced years before recognizing that information geometry is at the core of their theoretical foundations. I will discuss how information theory then allowed deriving new theoretically founded black-box algorithms, notably in the context of large-scale optimization.

Anne Auger is a researcher in the Inria project-team TAO, in the Laboratoire de Recherche en Informatique, Orsay, France. She received a Master's degree in applied mathematics from University Paris 6 in 2001 and earned her PhD in 2004 from the Paris 6 University. She then worked for two years as a postdoctoral researcher at ETH Zurich before obtaining a permanent researcher position at Inria in 2006. Her main research interest is on black-box continuous optimization including theoretical aspects and algorithm design.

11h00 : Mesure de l'énergie minimale nécessaire à l'effacement d'un bit d'information et relation avec l'égalité de Jarzynski

Sergio Ciliberto (ENS Lyon)

Résumé : Peut-on imaginer mettre au point un ordinateur parfait capable d'effectuer des opérations logiques irréversible sans consommer aucune énergie ? A cette question, Rolf Landauer a répondu non en 1961. Il avait en effet remarqué qu'à chaque fois qu'un bit d'information est créé, la mémoire binaire de l'ordinateur se voit réduite à un seul de ses deux états possibles. Faisant le lien avec la thermodynamique, Landauer a proposé que cette diminution du désordre exige pour être réalisée une quantité minimale d'énergie dont la valeur est aujourd'hui connue sous le nom de limite de Landauer. Dans ce séminaire on décrira comment cette énergie minimale peut être mesurée expérimentalement en utilisant une bille colloïdale piégée par un laser dans un potentiel à deux puits. Ce système peut être vu comme un modèle d'une mémoire à un bit. Par l'application d'une force externe, il est possible de forcer la particule à effectuer une transition, comme si on imposait au bit de prendre la valeur 1 par exemple. En mesurant le travail fait par cette force externe, on trouve que l'énergie minimale pour effectuer la transition, correspond précisément à la limite de Landauer. Nous démontrons aussi que pour cette opération d'effacement de la mémoire, qui est une opération logique irréversible, l'égalité détaillée de Jarzynski est vérifiée, et nous retrouvons la limite de Landauer à partir de cette égalité thermodynamique.

Sergio Ciliberto est Directeur de Recherche au CNRS et travaille depuis 1991 au Laboratoire de Physique de l'École normale supérieure de Lyon. Il a soutenu sa thèse en Physique en 1977. Il est l'auteur de 170 articles dans des journaux internationaux à comité de lecture et a déposé deux brevets. Ses recherches actuelles sont centrées sur la thermodynamique stochastique. Il a été directeur du Laboratoire de 2000 à 2006 et Directeur de la recherche de l'ENSL de 2012 à 2014. Il a été membre du Comité National du CNRS et de plusieurs comités internationaux.

13h30 : Vers une théorie de l'information mentale

Vincent Gripon (Télécom Bretagne)

Résumé : Dans les réseaux de neurones du néocortex viennent s'imprimer nos souvenirs par le biais du mécanisme de plasticité synaptique. Celui-ci nous permet de stocker des éléments d'information variés à l'échelle d'une vie avec une grande robustesse. Pourtant, les neurones, les connexions et les communications du néocortex sont loin d'être fiables. Pour répondre à ce problème, nous montrons comment l'utilisation de principes tirés des codes correcteurs d'erreurs modernes (parcimonie, distribution, traitement itératif) conduit à des modèles biologiquement plausibles du stockage de l'information mentale. Ces modèles offrent des efficacités mémoire optimales et ouvrent de nouvelles perspectives sur la compréhension de l'information mentale et sur l'intelligence artificielle.

Vincent Gripon, diplômé de l'école normale supérieure de Cachan et docteur de Télécom Bretagne en 2011, est chargé de recherche en neurosciences informationnelles à l'institut Mines Télécom et dans l'Unité CNRS Lab-STICC. Ses travaux portent sur la théorie des graphes, la théorie de l'information et les réseaux de neurones avec l'ambition de contribuer aux progrès de l'informatique neuro-inspirée. En s'appuyant sur les principes des codes correcteurs d'erreurs, il a proposé en 2011 de nouvelles familles de mémoires associatives binaires offrant une efficacité optimale de mémorisation. Il est le coauteur de "Petite mathématique du cerveau" (Éditions Odile Jacob, 2012). Il est également le cocréateur et coorganisateur de TaupIC, concours d'informatique à l'intention des étudiants en classes préparatoires.

14h30 : Information, simplicité et pertinence

Jean-Louis Dessalles (Télécom ParisTech)

Résumé : Claude Shannon fonda la notion d'information sur l'idée de surprise, mesurée comme l'inverse de la probabilité (en bits). Sa définition a permis la révolution des télécommunications numériques. En revanche, l'extension de la notion d'information à des domaines comme la biologie ou la communication humaine s'est révélée problématique. La probabilité n'est pas toujours calculable, ni même définissable. Son remplacement par la complexité de Kolmogorov s'est révélé utile pour aborder les domaines structurés. Toutefois, cela conduit à considérer que les objets aléatoires sont maximalement informatifs. Or pour un biologiste, un ADN aléatoire ne contient aucune information. Je propose de rester fidèle à l'hypothèse de base de Shannon et de définir l'*information pertinente* à partir de la *surprise*. La surprise est définie comme un **décalage de la complexité** de Kolmogorov (en ressources limitées). Cette définition se révèle utile pour étendre la notion d'information à des observateurs non-humains (par ex. en biologie). Elle est aussi essentielle pour définir la notion de *pertinence* et pour faire des prédictions concernant la communication humaine.

Jean-Louis Dessalles est Maître de Conférences à Télécom ParisTech, Université Paris-Saclay. Depuis une décennie, il développe la Théorie de la Simplicité, qui sert de base à la modélisation de l'intérêt narratif et de la pertinence argumentative. Il est l'auteur ou co-auteur de plusieurs livres, notamment « La pertinence et ses origines cognitives » (éd. Hermes-science, 2008) et « Le fil de la vie » (éd. Odile Jacob, 2016).

16h00 : En suivant Shannon : de la technique à la compréhension de la vie

Gérard Battail (Télécom ParisTech ER)

Résumé : L'application de la théorie de l'information à la biologie est le thème principal de cette conférence. Shannon, étudiant au MIT, a soutenu en 1940 une thèse intitulée *An algebra for theoretical genetics*, après avoir écrit un mémoire sur les réseaux de commutation publié en 1938. La publication du mémoire a valu à Shannon une grande notoriété alors que la thèse est passée inaperçue. En 1948, ingénieur aux Bell Labs, il a publié l'article qui fondait la théorie de l'information, *A mathematical theory of communication*. Son succès, considérable, résultait en partie d'un malentendu. La séparation entre la sémantique et l'information en un sens technique restreint en est la pierre angulaire mais son assimilation est difficile. Faute d'être vulgarisée et enseignée, la théorie de l'information reste méconnue encore de nos jours. Un bref rappel de ses principaux résultats est présenté.
La théorie de l'information permet de revenir à la génétique parce que l'hérédité est une communication (à travers le temps). Ignorant cette théorie, la biologie en rend compte de manière inadéquate, admettant implicitement que l'ADN, molécule donc objet quantique, se conserve spontanément pendant des centaines de millions d'années, alors qu'il subit des mutations perceptibles à l'échelle de la durée d'une vie humaine. Cette contradiction ne peut être résolue qu'en supposant les génomes munis de codes correcteurs d'erreurs fondés sur les multiples contraintes physico-chimiques et linguistiques auxquelles ils sont soumis. Cette hypothèse permet d'expliquer des propriétés essentielles de la vie que la biologie constate sans les comprendre. Une définition de l'information comme classe d'équivalence, basée sur l'expérience des ingénieurs, montre qu'elle est une entité abstraite bien qu'elle soit nécessairement inscrite sur un support physique. La vie résulte du jeu de l'information et de la matière, et le monde vivant est la partie du monde physique où réside et agit l'information.

Gérard Battail est né en 1932 à Paris. Il étudie au lycée Charlemagne puis à la faculté des sciences pour obtenir une licence ès sciences en mathématique et physique. Il assiste en 1951 à une série de conférences sur la théorie de l'information organisée à la Sorbonne par Louis de Broglie, ce qui l'incite à lire le texte fondateur de Shannon, paru en 1948, et décide de sa vocation. En 1953, il est admis sur titres à l'École nationale supérieure des Télécommunications de Paris. Il en sort en 1956 avec le diplôme d'ingénieur civil des télécommunications. En 1959, il est ingénieur au Centre national d'études des Télécommunications (CNET) à Issy-les-Moulineaux. En 1966, il entre à la division 'communications' de la Compagnie française Thomson-Houston-Hotchkiss-Brandt (CFTH) à Gennevilliers dont l'activité principale est la radioélectricité. En 1973, il devient professeur à l'École nationale supérieure des Télécommunications de Paris jusqu'à sa retraite en 1997. Après son départ en retraite, il poursuit des recherches (qui n'exigent pas de moyens expérimentaux) en abandonnant progressivement la technique au profit des sciences de la nature. Il s'intéresse surtout à la compréhension de la vie, estimant que les connaissances acquises dans la technique des communications peuvent y contribuer. Son premier article sur le sujet paraît en novembre 1997. Il rencontre en 2003 Marcello Barbieri, professeur d'embryologie à Ferrare, dont les recherches convergent avec les siennes. Il approfondit la compréhension du rôle de l'information dans la vie, exposée notamment dans son dernier livre, *Information and Life*, publié par Springer en 2014.

Vendredi 28 octobre 2016

10h00 : The dual geometry of Shannon information and its applications

Frank Nielsen (École Polytechnique)

Abstract: In information geometry, the negative Shannon entropy, called the Shannon information, is a strictly convex and differentiable function that induces a dually flat manifold structure equipped with the Kullback-Leibler divergence. In this talk, I review the concept of dual geometries, introduce the dual space of spheres, and describe the role of divergences in information theory, statistics, pattern recognition and machine learning.

Frank Nielsen received his PhD (1996) and his habilitation (2006) on computational geometry from the University of Nice-Sophia Antipolis, France. After the French national service, he joined Sony CSL (Japan) in 1997. He is currently professor in the computer science department of École Polytechnique (France). He co-organizes with Frédéric Barbaresco (Thales) the biannual Geometric Sciences of Information (GSI) conference, and is an associate editor of the Springer Journal of Mathematical Imaging and Vision and of MDPI Entropy.

11h00: Happy Numbers: 68 Years of Coding, $6^2 + 8^2 = 100$ Years of Shannon, $1^2 + 0^2 + 0^2 = 1$ Goal

Ruediger Urbank (EPFL)

Abstract: This year, we celebrate Shannon's **100**th birthday and it has been **68** years since he laid the foundations of communications. To realize his number **1** goal or error free communication we use error

correcting codes. Every time we make a call, connect to WiFi, download a movie, or store a file, they help us get things right. The journey began with codes based on algebraic structures such as Reed-Muller and Reed-Solomon codes. Then lattices helped convey continuous-valued signals. Slowly, deterministic codes made way for random sparse graphs codes with low-complexity message-passing decoding, such as Turbo codes and LDPC codes. The new millennium brought us Polar codes that use the chain rule of mutual information to achieve capacity and spatially-coupled codes that exploit the physical mechanism that makes crystals grow to simultaneously achieve the capacity of a large family of communication channels. Recently, the story has come full circle, and the symmetry inherent in algebraic constructions has brought the focus back on Reed-Muller codes. I will describe how ideas from such diverse areas as abstract algebra, number theory, probability, information theory, and physics slowly made it from the blackboard into products, and outline the main challenges that we face today.

Ruediger Urbanke (Phd, WashU, St. Louis, 1995) has been obsessed with questions in coding theory for the past 20 years. Fortunately his progress has been slow so that there are many problems left for him for the next 20 years. He likes sabbaticals and owns more bicycles than can be rationally justified. Before joining EPFL in 1999, he enjoyed working at Bell Labs (Murray Hill) at the Mathematics of Communications Group.

13h30: Claude Shannon: His life, modus operandi, and impact

Robert G. Gallager (MIT)

ABSTRACT: Claude Shannon (1916-2001) created Information Theory (i.e., the mathematical theory of communication) in 1948 after about 10 years of effort. The theory was based on the notion that sources of voice, text, pictures, video, whatever, can be viewed as stochastic choices between pre-specified alternatives. These choices can be encoded into a stream of bits which can then be transmitted over systems designed to transmit bits. He showed that this universal bit interface causes no essential loss in efficiency of transmission. This bit interface is now used in almost all engineering communication systems and is commonplace even to children. The development of efficient coding took much longer, and generalization to human systems is in its infancy. The tools used by Shannon in developing information theory and his many other important contributions are quite different from those commonly used in science, mathematics, and engineering, and we discuss these tools and their applicability in current research and technology.

Robert G. Gallager invented LDPC (low density parity check codes) in his doctoral thesis (MIT 1960), and has remained (still occasionally active) on the MIT faculty. His early research on information theory is included in his 1968 text 'Information Theory and Reliable Communication' still in print. Later research focused on distributed algorithms, data networks, and stochastic processes. His IEEE awards include the 1990 Medal of Honor and the 1983 IT Society Shannon Award. He is a member of the U.S. National Academies of Sciences and of Engineering and has received the 1999 Harvey prize, the 2002 Eduard Rhein prize, and the 2003 Marconi prize.