IRIF Doc-Postdoc Seminar, 2017-2022

Year 2022

Thursday December 8, 2022, 4PM, 3052 and Zoom link
Srinidhi N *Domain specific language for Testing consensus implementations*

I will introduce some consensus protocols and give an overview of some of the implementations. Following that, I will introduce what are the existing approaches to testing the implementations and then explain our approach which is akin to unit testing.
No prior knowledge of distributed systems/algorithms is required.

Thursday November 24, 2022, 4PM, 3052 and Zoom link
Esaïe Bauer *Method of analytic tableaux for first-order logic*

I will give an introduction to first order logic and proof theory in order to present a proof-search algorithm called “Method of analytic tableaux”. I will take this opportunity to talk about nice properties of proof theory and sequent calculus. The talk is more or less a lecture of the book “Introduction à la logique : Théorie de la démonstration” from David, Nour and Raffalli. It will not be about research I am currently working on and therefore should be more accessible to everyone. Looking forward to see you there!

Thursday November 17, 2022, 4PM, 3052 and Zoom link
Sander Gribling *Quantum query complexity*

Everything you always wanted to know (but were afraid to ask): What is it? Why should we care? How do we deal with it? No prior knowledge of quantum computing is required.

Thursday November 10, 2022, 4PM, 3052 and Zoom link
El Mehdi Cherradi *(∞-)Categorical semantic of type theory: an introduction*

The Curry-Howard correspondence is a very well-known result among (theoretical) computer scientists. However, the link it establishes between programs and proofs has also been extended by Lambek to a certain class of categories. As such, from the perspective that category theory provides a foundational framework for reasoning and logic, it is interesting to identify the underlying categorical structure of models of a given type theory. While the connection is fairly well-understood for intensional flavor of type theory following the work of Hofmann, it is notable that the extension to homotopy type theory is more recent and still incomplete. The goal of this talk is to introduce the basic concepts of the so-called categorical semantic of type theory and its challenging homotopy counterpart.

Thursday November 3, 2022, 4PM, 3052
Mouna Safir *Agreement Problems: Optimal Algorithm for Synchronous Byzantine Agreement*

The agreement problems has been extensively studied in distributed computing. Beyond the practical interest of this problem, particularly regarding fault-tolerant distributed computing, one of the main reasons behind the focus on agreement problem is the fact that it can be used to define and compare computational power properties of systems. In this presentation I will introduce two agreement problems: Byzantine General problem and k-set Agreement. In k-set agreement, each process must decide on value such that no more than k different values are decided by processes. In addition, the processes must guarantee a validity condition according to the failure models of the processes. Therefore, with crash process failures, the validity condition ensures that the decided values are initial values proposed by processes. In the case where k=1, the k-set agreement is the very classical consensus problem which is fundamental for fault tolerant distributed algorithms.

Thursday October 27, 2022, 4PM, 3052
All Non-Permanent Members *Introductory session*

This will be an introductory session where we invite all (new and old!) non-permanent members to come and talk about their research interests. Each talk should be 2-5 minutes long, and understandable by everyone.

Thursday October 13, 2022, 11AM, 3052
Amanda Burcroff (Harvard University) *Fundamentals of Hyperplane Arrangements*

Imagine you are high-dimensional being with scissors that can make d-dimensional cuts into (d+1)-dimensional objects. How many regions can you split an object into with a fixed number of cuts? What if all of your cuts must pass through the center of the object? Are there special patterns of cuts with nice properties? We will study these questions and more through a brief introduction to hyperplane arrangements. Hyperplane arrangements are of much interest to combinatorialists, and as they encode the structure of many important combinatorial problems. We will also briefly discuss how hyperplane arrangements have played a fundamental role in the understanding of certain neural networks.

Thursday October 6, 2022, 4PM, 3052 and Zoom link
Adrienne Lancelot (IRIF) *Equivalences of Programs in the lambda calculus*

In the study of programming languages, an essential point is the ability to state program equivalence, whether it is to reason abstractly or to establish that some program transformations, used typically when compiling programs, preserve the behavior of programs. The topic of this talk is the study of program equivalence for the case of programs expressed as terms of the λ-calculus, seen as a mathematical model of functional programming languages. We will survey existing program equivalences and focus on normal form bisimulations, in different variants of the lambda calculus. The lambda calculus was first introduced as a way to represent computable functions, with the Call-by-Name variant which has been extensively studied. Nowadays, functional programming languages use mostly the Call-by-Value variant (OCamL) and some the Call-by-Need variant (Haskell). In Call-by-Name, normal form bisimulations yield very satisfactory results. Unfortunately, these do not export to Call-by-Value. Part of my thesis work will be trying to find a satisfactory program equivalence in Call-by-Value.
The previous talk by Victor Arrial is a nice introduction to this talk but concepts tied to the lambda calculus (and its variants) will be re-explained. We will also need the (more generic) concept of co-induction to form program equivalences, which will be briefly explained as well.

Thursday September 22, 2022, 4PM, 3052 and Zoom link
Victor Arrial (IRIF) *Introduction to Lambda-Calculus and Quantitative Typing Systems*

This talk is planned to be an informal (very much non-exhaustive) introduction to lambda calculus (from a syntactical point of view). The idea is to give intuition on the calculus and two different reduction strategies (Call-by-Value and Call-by-Name). We will then briefly explore/compare three typing systems (simple types, graded linear types, multitypes). It is intended as an introduction to a forthcoming talk on “Quantitative Inhabitation in Call-by-Push-Value” (non-permanents seminar).

Thursday September 15, 2022, 4PM, 3052 and Zoom link
Vincent Moreau (IRIF) *Categories for the uninitiated*

The talk will be a 1-hour introductory session on category theory accessible to everyone. We introduce categories as generalizations of ordered sets and then focus on the notion of universal property and show through examples how such properties can be used to describe behaviours in different areas of mathematics in a unified way. No prerequisites.

Thursday June 2, 2022, 4PM, Salle 3052
Avinandan Das *Streaming and computing Frequency Moments in Streaming.*

In this talk, we will talk about the Data Stream Model of computation. In this model, the input arrives as a stream of items and the workspace of the algorithm is very low and therefore, the whole input cannot be stored in the memory. Due to space constraints, data streaming algorithms use elegant and non trivial randomization techniques to store summary of the input seen so far. The model is inspired by the advent of data explosion, where it is impossible to store all of the data in the memory and also by database applications, where random access cost is high. We will see algorithms for frequency moments computation (F_0 and F_2) over a stream of elements, which actually kickstarted the field of data stream algorithms. This talk is based on lecture notes from the course “Communication Complexity (for Algorithm Designers)” by Tim Roughgarden (http://timroughgarden.org/notes.html).

Thursday May 19, 2022, 4PM, Salle 1007
Lucía Rossi (University of Leoben, Austria) *Limit words for N-continued fractions*

We begin by introducing Sturmian words, which are infinite words on a two letter alphabet. An infinite word ω is said to be Sturmain if, for any given n, there exist exactly n+1 distinct subwords of ω of length n. They are, in some sense, the simplest possible non-trivial words. Geometrically, they correspond to a cutting sequence obtained from a line of irrational slope on a square grid, and there is a very nice correspondence between the coding sequence of ω and the continued fraction expansion of the slope. Given $N \geq 1$ and $x \in [0, 1] \setminus Q$, an N-continued fraction expansion of x is defined analogously as the classical continued fraction, but with the numerators being all equal to N. An infinite word $\omega(x, N)$ on a two letter alphabet is obtained as a limit word of a sequence of substitutions, which we call an NCF word. When $N = 1$, we find a Sturmian word. We present some combinatorial and analytic results obtained for NCF words, namely: balance properties, letter frequency, factor complexity. This is joint work with Niels Langeveld and Jörg Thuswaldner.

Thursday May 12, 2022, 4PM, Salle 1007
Daniel Szabo *Quantum algorithms for the longest common substring problem*

The longest common substring problem (LCS) is one of the most fundamental string problems. We look at the decision version of LCS: given two texts s and t and a parameter d we want to find out if there is a string of length d that appears as a substring in both s and t. Its classical complexity is well understood: it is linear in the length of s and t, which we denote by n. In the quantum setting, two algorithms can be combined to get the best known upper bound: one has query (and time) complexity O(n^(2/3)) for any value of d; and the other one uses O(n/sqrt(d)) queries. In the talk I will try to present the main ideas behind these results in such a way that people without much knowledge on quantum computing can follow too.

Thursday April 28, 2022, 4PM, Salle 3052
Félix Castro *An interpretation of E-HA^ω inside HA^ω*

HA^ω (Higher Type Arithmetic) is a first order many sorted theory. It is a conservative extension of HA (Heyting Arithmetic a.k.a the intuitionistic version of Peano Arithmetic) obtained by extending the syntax of terms to all the System T : the objects of interest here are the functionals of "higher types". While equality between natural numbers is well understood (it is canonical and decidable), how equality between functionals can be defined ? From this question, different versions of HA^ω arise : an extensional version (E-HA^ω) and an intentional version (I-HA^ω).

Thursday March 24, 2022, 4:30PM, Salle 3052
Patrick Lambein-Monette *Average consensus in spite of dynamic interactions*

Picture a networked system of autonomous agents, each starting with some initial value. In the /average consensus/ problem, the agents should collectively compute the arithmetic mean of those values, through local interactions over a connected network.
Classically, this problem is considered in a setting where the agents hold no unique identifier, and do not start knowing a bound over the size of the system. These restrictive assumptions give rise to two major obstacles to our problem. First, it is generally impossible for an agent to detect that it has reached the desired answer; as such, we only expect the system to asymptotically converge towards the average, rather than to irrevocably decide on it. Second, it is generally impossible to properly account for the multiplicities of the initial values; we therefore restrict our considerations to bidirectional communication links.

For fixed bidirectional networks, an efficient solution is to be found in the /Metropolis/ averaging algorithm, first proposed by Xiao and colleagues in 2005. However, when moving to consider /dynamic/ networks – i.e., where the communication links can arbitrarily change at each step of the execution – the Metropolis rule isn't algorithmic, in the sense that it requires the agents cannot themselves gather all the information required to implement the rule. Other average consensus protocols proposed in the literature fare no better for the same reasons.

We propose the /MaxMetropolis/ rule, an adaptation of the Metropolis rule that is history-dependent, and admits a totally decentralized and local implementation. Over bidirectional dynamic networks with n agents and connectivity delay B, $O(B n^4 log n/r)$ communication rounds are required to achieve a relative disagreement of $r > 0$ over the value of the average. This is the first truly distributed average consensus algorithm for bidirectional dynamic networks.

Thursday March 10, 2022, 4PM, Salle 3052
Robin Vacus *Early Adapting to Trends: Self-Stabilizing Information Spread using Passive Communication*

How to efficiently and reliably spread information in a system is one of the most fundamental problems in distributed computing as well as in the animal world. In this talk, we will consider the self-stabilizing bit-dissemination problem, motivated by biological scenarios, in the extremely constrained model of passive communication.

Thursday February 24, 2022, 4PM, Salle 3052
Filippo Brunelli *Walk Temporalisation and Reachability Maximisation in Temporal Graphs*

In a temporal graph, each edge appears and can be traversed at specific points in time. In such a graph, temporal reachability of one node from another is naturally captured by the existence of

a temporal path where edges appear in chronological order. Inspired by the optimisation of bus/metro/tramway schedules in a public transport network, we consider the problem of turning a collection of walks (called trips) in a directed graph into a temporal graph by assigning a starting time to each trip so as to maximise the reachability among pairs of nodes. Each trip represents the trajectory of a vehicle and its edges must be scheduled one right after another. Setting a starting time to the trip thus forces the appearing time of all its edges. We call such a starting time assignment a trip temporalisation.
We will speak about results on the complexity of maximising reachability via trip temporalisation. We will show that the problem is hard to approximate even when we assume the nice property that for each pair of nodes, there exists a trip temporalisation connecting them. On the positive side, we show that there must exist a trip temporalisation connecting a constant fraction of all pairs if we additionally assume symmetry in the trip network.

Thursday February 17, 2022, 4PM, Salle 3052
Klara Nosan *On matrix groups, the Zariski topology and what they both have to do with automata and verification*

Finitely generated groups of matrices are fundamental mathematical objects that appear in a wide variety of areas in computer science, including algebraic complexity theory, quantum computation, dynamical systems, graph theory, control theory, and program verification. Unfortunately, matrix groups are challenging from the algorithmic point of view, with many natural problems being undecidable. In order to get a better handle on a finitely generated matrix group, it turns out to be worth over-approximating it by its Zariski closure, which admits a finite representation.
This talk will be a gentle introduction to (computing) the Zariski closure of finitely generated matrix groups with examples of applications in automata theory and program verification. We will describe an existing algorithm for computing the closure due to Derksen, Jeandel and Koiran. We will conclude by discussing our result, which is to obtain an upper bound on the degree of the polynomials that define the Zariski closure. Having an a priori bound allows us to give a simple algorithm for the problem, via linear algebra, similar to Karr's algorithm for obtaining affine invariants for affine programs.

Year 2021

Thursday December 16, 2021, 11AM, Salle 3052
Abhishek De & Pierre Meyer *Multi-party encrypted communication between ASD, ASV and PPS*

Talk 1 (Abhishek): How can someone from PPS chat up someone from ASD or ASV?
PPS looks at abstractions of programming languages and studies logics motivated to better understand these abstractions. How can tools developed here be used in other fields like automata theory and complexity theory? In this talk, I will give some ideas roughly along the lines of implicit complexity and hope to forge further collaborations between the 3rd floor and 4th floor.

Talk 2 (Pierre): What does it take to hide patterns of communication?

Secure Multiparty Computation (MPC) allows N mutually distrusting parties to perform some computation f(x_1,...,x_N) without having to reveal anything about their private inputs x_1,...,x_N beyond what is revealed by the output of the computation itself. Making sure that "adversaries", which are internal to the system rather than external, cannot learn more information than they should is a well-understood task in the setting where any pair of parties can communicate directly (and privately). However, in many scenarios, setting up a complete communication network is impractical (e.g. too expensive) or impossible (e.g. some parties may outright refuse to communicate with some others). Therefore, we consider the more realistic setting where the parties are nodes in some incomplete graph, and can communicate only along the edges. In fact, knowledge of this network could be kept private too: each party knows who they are talking to but they do not need to know the metadata of how others are communicating, which may be sensitive information. There are two difficulties to achieving this extra privacy requirement: (1) the MPC protocol must be run even if the each party only knows their local view of the network (i.e. their neighbourhood), and (2) the MPC protocol should reveal nothing more about the graph.

In this talk, we will try and understand how hard this task is by relating it to a foundational hierarchy of cryptographic primitives: - Secure Communication: Two parties need to communicate privately even in the presence of an external eavesdropper monitoring all their interactions. - Secure Computation: Two parties need to compute some function without trusting each other with their inputs. Prerequisites: No background in cryptography is required.

Wednesday November 24, 2021, 11AM, Salle 3052
Corentin Henriet & Simon Mauras *Fighting fish and assigning students*

Talk 1 (Corentin): Combinatorics of fighting fishes and related structures
Fighting fishes are combinatorial objects generalizing parallelogram polyominoes introduced in 2016 by Duchi et al. The enumeration of these objects with respect to their natural parameter of size (the half-perimeter) leads to a sequence that counts also other objects : two-stack sortable permutations, non-separable planar rooted maps, synchronized intervals of the Tamari lattice. In this presentation, I will define some bijections between fighting fishes and other objects that preserve a lot of structure and statistics, and I will give some perspectives about the generalization of considered objects and bijections.

Talk 2 (Simon): Random models for stable matching

In a two sided matching market, two types of agents have preferences over one another. Examples include college admissions (students and colleges), residency programs (doctors and hospitals), job markets (workers and jobs) and, in the classical analogy, stable marriages (men and women). In a founding paper, Gale and Shapley introduced the deferred acceptance procedure, where one side proposes and the other disposes, which computes a stable matching. In the worst case, the choice of which side of the market proposes has a big importance, both in terms of outcome (the output matching is optimal for the proposing side) and truthfulness (the receiving side might have incentives to lie). We will show that things are much nicer in the average case. Assuming that preferences of agents are drawn from certain distributions, then each agent receives with high probability the same allocation in the two variants of deferred acceptance.

Wednesday June 2, 2021, 4PM, Salle 3052
Quentin Ferro (IRIF) *Distributed Recoloring using the LOCAL Model*

Recoloring is a reconfiguration problem : given a graph and two proper coloring of this graph, how to recolor from one coloring to the other by a series of elementary changes ? The talk will be based on the Distributed Recoloring paper from Marthe Bonamy, Paul Ouvrard, Mikaël Rabie, Jukka Suomela, and Jara Uitto (Disc 2018) which introduced the notion of distributed recoloring as follow : the input graph represent a network of computers that need to be recolored. Each node know its input color and its target color. Nodes are allowed to exchange messages with each other synchronously and, given rounds of messages, each node have to output its recoloring schedule, indicating when the node changes its color and to which color. The recoloring schedules have to be globally consistent so that the graph remains properly colored at each point, and we require that adjacent nodes do not change their colors simultaneously. This paper gave a lot of results for different situations of coloring (different types of graph, different number of color, different number of extra color), particularly problems with 1 extra colors, and left some open questions. I will present some results we have on some of those open questions.

Wednesday May 26, 2021, 4PM, Salle 3052
Avinandan Das (IRIF) *Combinatorial Proof for Chernoff-Hoeffding Concentration Bound*

In this talk, I will give a combinatorial proof of the Chernoff-Hoeffding concentration bound, which says that the sum of independent $\{0,1\}$-valued random variables is highly concentrated around the expected value. Unlike the standard proofs, this proof does not use the method of higher moments, but rather uses a simple and intuitive counting argument. In addition, this proof is constructive in the following sense: if the sum of the given random variables is not concentrated around the expectation, then we can efficiently find (with high probability) a subset of the random variables that are statistically dependent. This talk is based on the paper “Constructive Proofs of Concentration Bounds” by Russell Impagliazzo and Valentine Kabanets.

Year 2020

Wednesday December 2, 2020, 11AM, Online
Phd Students *Welcome session!*

Wednesday May 6, 2020, 11AM, Online
Cédric Ho Thanh (IRIF) *An introduction to Docker*

This presentation aims to be a quick introduction to docker: its role, inner workings, ecosystem, and most importantly, how to use it. We will start with a little bit of theory, and swiftly move to a demo. Some notions about operating systems might be beneficial, but I will try to review what we need.

Wednesday April 22, 2020, 11AM, Online
Simon Mauras (IRIF) *How to aggregate top-lists*

A top-list is a possibly incomplete ranking of elements: only a subset of the elements are ranked, with all unranked elements tied for last. Top-list aggregation takes as input a collection of top-lists and aggregates them into a single complete output ranking, aiming to minimize the number of upsets (pairs ranked in opposite order in the input and in the output).
This talk will start with a quick survey on rank aggregation (the special case where every input list is a complete ranking of the elements), its relation to feedback arc sets in directed graphs, NP-Hardness, and approximation algorithms. Then we will discuss how such results can be extended to the aggregation of top-lists.

Preprint available: https://arxiv.org/abs/1811.01537

Wednesday April 15, 2020, 11AM, Online
Chaitanya Leena Subramaniam (IRIF) *The plus-construction for sheaves and factorisation systems*

Sheaves are a fundamental kind of algebraic structure in mathematics, and iterating the so-called plus-construction is a well known process of turning a presheaf into a sheaf.
However, the plus-construction makes sense in much more generality than sheaves, and a result (joint with M. Anel) shows that it is in fact closely related to orthogonal factorisation systems on a category. Indeed, it can be used to construct such factorisation systems.

This has many applications, including in dependent type theory, where it has a fundamental application to modalities.

The talk will be a gentle introduction to the plus-construction and its various examples.

Wednesday April 8, 2020, 11AM, Online
Nicolas Jeannerod (IRIF) *Analysing installation scenarios of Debian packages*

Debian GNU/Linux is a Linux distribution composed of free and open-source software. It is heavily used all over the world as an operating system for personal computers and servers, and is the basis for many other distributions.
Deban currently includes more than 28 thousand maintainer scripts, almost all of them written in POSIX shell. These scripts are executed with root privileges at installation, update, and removal of a package, which make them critical for system maintenance. While Debian policy provides guidance for package maintainers producing the scripts, few tools exist to check the compliance of a script to it.

This presentation reports on the application of a formal verification approach based on symbolic execution to find violations of some non-trivial properties required by Debian policy in maintainer scripts. We present our methodology and give an overview of the toolchain. We focus in particular on the tree logics used to represent symbolically a file system transformation, and the use of such a logic in the symbolic engine.

Wednesday April 1, 2020, 11AM, Online
Simona Etinski (IRIF & INRIA) *Stern's Zero Knowledge Identification Scheme*

In the first part of the talk, I will present the class of interactive proofs (IP) and special property of some of the interactive proofs called zero-knowledge. Public and private coin methods will also be introduced as they play a major role in most of the interactive proofs. The second part of the talk will concern Stern's identification scheme: a zero-knowledge interactive proof that enables one party to prove its identity to the other party without revealing any further information about it. Relying on the syndrome decoding problem, which is believed to be NP-complete, the scheme is considered to be post-quantum and thus a valid candidate for identification schemes to be used long-term. Nevertheless, the rather high communication complexity prevents Stern's scheme from being widely used at the moment and thus poses an issue to address. Some of the recent results and suggested future directions in addressing this issue will be presented in this talk.

Wednesday March 25, 2020, 11AM, Online
Nguyễn Lê Thành Dũng (LIPN) *Aperiodicity in a non-commutative logic*

We give a characterization of star-free languages in a λ-calculus with support for non-commutative affine types (in the sense of linear logic), via the algebraic characterization of the former using aperiodic monoids. Since this work is at the interface of two areas, namely automata theory and programming languages, the talk will assume very little background knowledge and recall the prerequisites for both. I will also present our main inspiration: Hillebrand and Kanellakis's little-known characterization of regular languages in the simply typed λ-calculus (LICS'96). This is a joint work with Pierre Pradic (Oxford); preprint available at https://hal.archives-ouvertes.fr/hal-02476219/document

Monday March 2, 2020, 3PM, Salle 3014
Pierre Cagne *Les symmétries des sphères en fondations univalentes*

Year 2019

Wednesday November 27, 2019, 11AM, Salle 3052
(Old) Phd Students *Return of the PhD Seminar*

Every new/old PhD student is invited to come and talk about her/his research interests.
Each talk will be 2-5 minutes long, and should be understandable by everyone.

Wednesday November 20, 2019, 11AM, Salle 3052
Pierre Ohlmann (IRIF) *Controlling a random population*

Bertrand et al. (2017) introduced a model of parameterised systems, where each agent is represented by a finite state system, and studied the following control problem: for any number of agents, does there exist a controller able to bring all agents to a target state? They showed that the problem is decidable and EXPTIME-complete in the adversarial setting, and posed as an open problem the stochastic setting, where the agent is represented by a Markov decision process. In this paper, we show that the stochastic control problem is decidable. Our solution makes significant uses of well quasi orders, of the max-flow min- cut theorem, and of the theory of regular cost functions.

Wednesday November 13, 2019, 11AM, Salle 3052
(New) Phd Students *The PhD Seminar strikes back*

Every new/old PhD student is invited to come and talk about her/his research interests.
Each talk will be 2-5 minutes long, without any slides, and should be understandable by everyone

Wednesday July 24, 2019, 11AM, Salle 3052
Hugo Moeneclaey (IRIF) *Toward a Cubical Type Theory Univalent by Definition*

Univalent foundations are based on a geometric interpretation of identity types in type theory. We will explain this interpretation, then we will give a brief introduction to Cubical Type Theory and explain why it is useful in this context. Then we will present some ideas from parametricity and sketch how we are trying to use them to build a variant of Cubical Type Theory.

Wednesday March 6, 2019, 11AM, Salle 3014
Isaac Konan (IRIF) *Partitions and Bijections*

“For any positive integer n, there are as many partitions of n into distincts parts as partitions of n into odd parts”. This identity stated by Euler is quite trivial to prove by calculations, but not easy show bijectively.
I will discuss bijections for some well-known partition identities, such as Schur partition identity and q-binomial coefficient.

NB: Open talk, all you need is just how to count objects.

Wednesday February 27, 2019, 11AM, Salle 3052
Pierre Ohlmann (IRIF) *Lower bounds for arithmetic circuits via the Hankel matrix*

We study the complexity of representing polynomials by arithmetic circuits in both the commutative and the non-commutative settings. Our approach goes through a precise understanding of the more restricted setting where multiplication is not associative, meaning that we distinguish (xy)z from x(yz).

Our first and main conceptual result is a characterization result: we show that the size of the smallest circuit computing a given non-associative polynomial is exactly the rank of a matrix constructed from the polynomial and called the Hankel matrix. This result applies to the class of all circuits in both commutative and non-commutative settings, and can be seen as an extension of the seminal result of Nisan giving a similar characterization for non-commutative algebraic branching programs.

The study of the Hankel matrix provides a unifying approach for proving lower bounds for polynomials in the (classical) associative setting. We demonstrate this by giving alternative proofs of recent results proving superpolynomial and exponential lower bounds for different classes of circuits as corollaries of our characterization result.

Our main technical contribution is to provide generic lower bound theorems based on analyzing and decomposing the Hankel matrix. This yields significant improvements on lower bounds for circuits with many parse trees, in both (associative) commutative and non-commutative settings. In particular in the non-commutative setting we obtain a tight result showing superpolynomial lower bounds for any class of circuits which has a small defect in the exponent of the total number of parse trees.

Year 2018

Wednesday November 28, 2018, 11AM, Salle 3052
Cédric Ho Thanh (IRIF) *Type theoretical approach to opetopes*

Opetopes are shapes (akin to globules, cubes, simplices, etc.) introduced to describe laws and coherence in higher categories. Their classical definitions, however, makes them difficult to manipulate efficiently. In this presentation, I will present ongoing works aiming to describe them completely from a type-theoretic standpoint. If time permits, I will showcase a proof checker for opetopes.

Wednesday November 14, 2018, 11AM, Salle 3052
Thomas Colcombet (Automata team) *Writing (large) LaTeX documents with the knowledge package.*

Writing your PhD thesis is a huge work (took me nine months). A burden. Everyone wants it to be THE document that the next generation will read in order to learn the wonderful stuff you have developed at IRIF.
Clearly, there are some pitfalls to avoid. Sometimes a scientifically excellent thesis turns out to be barely usable, because definitions are difficult to find, hard to parse, etc… And the reviewers get mad at you (but say it gently because they are polite). It is your duty to pay attention to all these details (it is also the duty of your PhD advisor to help you in that) and make a document as user friendly as possible.

One can find many documents describing how to write good science/a good thesis on the internet (read some of them!). I will not try to cover this wide subject. My goal in this talk will be to emphasize on some presentation points, and show you how some tools can help you in your writing (this is an advertisement for the LaTeX package « knowledge »).

If you want to test, you can bring your laptop with an up-to-date distribution of LaTeX.

Wednesday October 31, 2018, 11AM, Salle 3052
Anupa Sunny & Zhouningxin Wang *New PhD session*

Explicit, Almost Optimal Epsilon-Biased Sets

---

by Anupa Sunny

Abstract: This talk is based on a paper by Amnon Ta-Shma on the construction of epsilon biased sets which have a support size close to the Gilbert-Varshamov bound, a notion from coding theory. We will look at the Rozenman-Wigderson construction of the epsilon-biased set in which the bias of a set is amplified by taking a walk over an expander graph. We will then look at Ta-Shma's construction which is based on a modified version of the zigzag product, namely the s-wide replacement product.

Homomorphism of signed graphs

---

by Zhouningxin Wang

Abstract: The signed graph is a graph whose edges are assigned with the signs + and -. A homomorphism of one graph to the other preserves the adjacencies and incidences of these two edges. We extend the concept of homomorphism for signed graphs. An intuitive example will be given to explain why we consider the homomorphism of signed graphs. We will give the minimum signed graph, namely Spal_5, to which all the signed K_4-minor-free graph admits homomorphism to. In the last part, we will show the necessary and sufficient conditions for a signed K_4-subdivision being a core.

Wednesday October 17, 2018, 11AM, Salle 3052
Abishek De & Simon Mauras *Newcomers' session*

Abishek De : Distributed Control Problem for Free Choice Systems
The distributed synthesis problem is about constructing correct distributed systems, i.e., systems that satisfy a given specification. We consider a slightly more general problem of distributed control, where the goal is to restrict the behavior of a given distributed system in order to satisfy the specification. Our systems are finite state machines that communicate via rendezvous (asynchronous automata). There are a few classes of systems for which the problem has been shown decidable. We solve it for free choice systems, systems whose entire behaviour can be expressed in a (possibly infinite) tree.

Simon Mauras : Social choice theory, and a small survey about rank aggregation

How should we vote? This question has been adressed by philosophers and mathematicians since the XVIIIth century, but no satisfactory solution exists. The talk will start with classical results on social choice theory and move on to the aggregation of rankings seen as an optimization problem. We will discuss NP-Hardness, Hardness of approximation and Approximation algorithms for several variants of this problem.

Wednesday September 12, 2018, 11AM, Salle 3052
Farzad Jafarrahmani *Denotational semantics of Linear Logic with least and greatest fixpoints*

We develop a denotational semantics of full propositional classical linear logic extended with least and greatest fixpoints of formulae (\mu LL) in coherence spaces with totality. The presence of totality predicates, which are a denotational account of the syntactic notion of normalization, allows for dual and non-trivial denotational interpretations of the mu and nu fix point operators involving Knaster Tarski's theorem. We illustrate the construction by means of several examples such as integer numbers system, and by an embedding of Gödel's system T in \mu LL. This specific denotational semantics of muLL is clearly an instance of a more general pattern. We also encode the exponentials of linear logic using least and greatest fixpoints and then explain the difference between the new exponentials and the original ones from denotational semantics point of view. This is based on joint work by Thomas Ehrhard.
Short session

Wednesday June 27, 2018, 11AM, Salle 3052
Victor Lanvin (Équipes Preuves, programmes, et Systèmes) *Introduction to gradual typing with union and intersection types*

Since the advent of types in programming languages, the two concepts of static typing and dynamic typing have been engaged in a terrible battle. Simply querying “static typing vs dynamic typing” yields more than half a million results on Stack Overflow. On the one hand, static typing provides strong safety guarantees before a program is even executed, by checking during

compilation that types are not misused. On the other hand, dynamic typing is more flexible and is better suited to rapid prototyping. With both approaches having strong arguments in their favor, the battle seems endless. Yet, all hope is not lost. Gradual typing is a recent approach that aims at combining the safety guarantees of static typing with the flexibility and development speed of dynamic typing. The idea behind it is to introduce an “unknown” type, used to inform the compiler that additional type checks may need to be performed at run time in some places. Programmers can then “gradually” add type annotations to a program, and control precisely how much checking is done statically versus dynamically. Our work aims at integrating union and intersection types with gradual typing to allow for stronger safety guarantees and a finer control over dynamic types.
Note: this will (should) be a very general presentation about gradual typing and set-theoretic types consisting mostly of practical examples and without too many technical details. Don't hesitate to bring your computer, a book, or your Nintendo Switch™ if you already know the topic. 🙂

Wednesday June 20, 2018, 11AM, Salle 3052
Laurent Feuilloley (Équipes Compsys, GANG et graphes) *Distributed decision*

In this talk, I will introduce the domain of distributed decision, and review some of the results and insights gathered during my PhD.
The underlying model of this study is the local model. The local model is defined to answer questions of the following type: given a communication network, whose nodes are machines, and edges are communication links, is it possible that the nodes solve some task X, if they communicate only with the nodes that are close to them? A classic problem is colouring: can a node choose a colour, with only the knowledge of a small neighbourhood of the graph, such that the colours chosen by the nodes form a proper colouring of the graph? As in the centralized setting, it is interesting to study decision problems, that are yes-no questions, and to define complexity classes to classify these problems; this is distributed decision.

The complexity class we use as the equivalent of the class P in the centralized setting, is pretty small, and it is then natural to look at some form of non-determinism, to have a chance to understand more problems. In this model, non-determinism can be thought as a piece of global information that can be verified locally. The theoretical motivation is that to understand how local a problem is, one can ask how much global information is needed to solve it. The more practical motivation is that if one can design schemes with little global information then it can help to design more robust distributed algorithms such as self-stabilizing algorithms. The results I will present play with different natural notions of non-determinism, and how they influence the complexity classes defined.

I will spend time to carefully describe the model, thus no prior knowledge is needed.

Wednesday June 6, 2018, 11AM, Salle 3052
Pierre Ohlmann & Sidi Mohammed Beillahi (Équipe automate & Équipe vérification) *Unifying non-commutative arithmetic circuit lower bounds & Robustness of Programs Against Consistency Relaxation*

Unifying non-commutative arithmetic circuit lower bounds (Pierre Ohlmann)
We develop an algebraic lower bound technique in the context of non-commutative arithmetic circuits. To this end, we introduce polynomials for which the multiplication is also non-associative, and focus on their circuit complexity. We show a connection with multiplicity tree

automata, leading to a general algebraic characterization. We use it to derive meta-theorems for the non-commutative case, and highlight numerous consequences in terms of lower bounds.

&&

Robustness of Programs Against Consistency Relaxation (Sidi Mohammed Beillahi)

Sequential Consistency (SC) and Serializability (Ser) are the classical consistency models for concurrent and distributed programs. They are the intuitive models for developers. Due to the costly synchronization required by the two models, most of existing memory models and distributed implementations of data structures do not use these two models. Instead, in order to reduce the latency and remove unnecessary synchronization, modern processors and databases adopt relaxed and weaker consistency models. However, this weakening of the consistency models implies new unexpected behaviors when running programs over the weaker models. We address in this work the problem of detecting unexpected behaviors of a program that were observed when weakening the consistency model. In particular, we check whether the two sets of executions traces of a program over the SC (resp, Ser) model and some weaker consistency model coincide or not. We characterize the set of executions traces that violate this equality and drive a decision procedure to detect these traces. In the case where there are no traces that violate this equality we refer to a program to be Robust.

A joint work with Ahmed Bouajjani and Constantin Enea

Wednesday May 23, 2018, 11AM, Salle 3052
Léo Stefanesco (Algebra and calculus, proofs and programs teams) *An Asynchronous Soundness Theorem for Concurrent Separation Logic*

The talk will start with an introduction to (concurrent) separation logic.
—

Abstract:

Concurrent separation logic (CSL) is a specification logic for concurrent imperative programs with shared memory and locks. In this talk, we develop a concurrent and interactive account of the logic inspired by asynchronous game semantics. To every program C, we associate a pair of asynchronous transition systems [C]S and [C]L which describe the operational behavior of the Code when confronted to its Environment, both at the level of machine states (S) and of machine instructions and locks (L). We then establish that every derivation tree π of a judgment Γ ⊢ {P}C{Q} defines a winning and asynchronous strategy [π] with respect to both asynchronous semantics [C]S and [C]L. From this, we deduce an asynchronous soundness theorem for CSL, which states that the canonical map L : [C]S → [C]L from the stateful semantics [C]S to the stateless semantics [C]L satisfies a basic fibrational property. We advocate that this fibrational property provide a clean and conceptual explanation for the usual soundness theorem of CSL, including the absence of data races.

(Joint work with Paul-André Melliès)

Wednesday May 2, 2018, 11AM, Salle 3052
Emiliano Lancini (Laboratoire d'Informatique de Paris Nord) *Box-Total Dual Integrality and k-Edge-Connectivity*

In the first half of the 20th century the distribution of electricity became a major issue for many european nations. From this situation arose the problem of building a connected network of minimum length. The mathematical model underlying this problem is the minimum spanning

tree problem, it has been investigated by many authors and is now considered a classical problem of combinatorial optimisation.
Nowadays it is often required that telecommunication networks keep unaltered their functionality even after the failure of some of their links. This leads to a generalisation of the minimum spanning tree problem named k-edge-connected spanning subgraph problem.

In this talk we show a characterisation of a graph class in terms of integrality properties of polyhedra naturally associated to the k-edge-connected spanning subgraph problem.

The concept of total dual integrality (TDI) dates back to the works of Edmonds, Giles and Pulleyblank in the late 70's, and is strongly connected to min-max relations in combinatorial optimisation.

The system Ax>=b is TDI if, in the following equation, for each integer vector c, for which the minimum in the following equation is finite, there exists an integer optimal solution for the maximum.

min {cx: Ax>= b} = max {yb: yA = c, y >= 0}

We are interested in the stronger property of box-TDIness. A system Ax>=b is called *box-TDI* if the system Ax >= b, l ⇐ x ⇐ u is TDI for all rational vectors l and u.

We prove that, for k>=2, the k-edge-connected spanning subgraph polyhedron is a box-TDI polyhedron if and only if the graph is series-parallel. Moreover, in this case, we provide a box-TDI system with integer coefficients describing this polyhedron.

Wednesday April 25, 2018, 11AM, Salle 3052
Raphaëlle Crubillé (Algebra and calculus, proofs and programs teams) *Probabilistic Stable Functions on Discrete Cones are Power Series.*

The category of probabilistic coherence spaces (PCoh_!), introduced by Danos and Ehrhard, is a fully abstract model for PCF with *discrete* probabilities, where morphisms can be seen as power series. The category Cstab_m, of measurable cones and measurable stable functions, has been introduced by Ehrhard, Pagani and Tasson as a model for PCF with *continuous* probabilities. In this talk, we will study the shape of stable functions when they are between *discrete* cones, and it will allow us to see that PCoh_! is a full subcategory of Cstab_m.

Wednesday April 18, 2018, 11AM, Salle 3052
Paulina Cecchi & Antoine Allioux (Automata, Combinatorics teams & Algebra and calculus, proofs and programs teams) *New PhD student introduction session*

* Paulina Cecchi
Title: Some interactions between words combinatorics and symbolic dynamics.

Abstract: Word combinatorics has been fruitfully used to study several topological and mesure-theoretic properties of dynamical systems, through the analysis of suitably chosen symbolic dynamical systems. In this talk, we will introduce some notions of symbolic dynamics and present some examples which illustrate how word combinatorics can be used as a tool to solve questions arising from this branch of mathematics.

*

* Antoine Allioux

Title: The curse of Martin-Löf identity type

Abstract: The identity type of Intuitionistic Type Theory (ITT) endows types with a structure of infinity-groupoid. This higher structure follows from the fact that the Uniqueness of Identity Proof (UIP) is not derivable in ITT. Homotopy Type Theory (HoTT) takes advantage of this observation by enriching ITT with new principles which are coherent with this interpretation, namely the Univalence Axiom and the Higher Inductive Types (HITs).

HITs are a generalization of inductive types which allow, in addition to create regular inhabitants of an inductive type, to postulate identities between them as well as identities between these identities, and that ad infinitum. It is then tempting to try to present mathematical structures using these new types like one would do in mathematics using generators and relations.

However, problems quickly arise as soon as one needs a strict equality. Indeed, the identity type expresses a weak equality leading to the usual coherence problems. Trying to solve these naively, we run into the problem of having to define an infinite sequence of coherence data.

If HoTT is to be a credible foundation of mathematics, the question of formalizing structures which need a strict equality is crucial. The answer to this question rests, in part, upon our achievement to either present these structures differently in the existing theory or to enrich it so that it becomes tractable to express them.

*

Wednesday April 11, 2018, 11AM, Salle 3052
Brieuc Guinard *Intermittent Locomotion in Graphs*

Everyone who has ever lost their keys in a busy room knows that they cannot move at full speed and hope to find them ; one must slow down enough as not to miss them. This compromise between speed of moving and success of detection is not specific to humans, of course, and in fact is commonly encountered in foraging animals, and even in cell biology. This opposition between relocation and detection can even lead to an intermittent behavior, i.e. with different phases during the search. We model such search processes by memoryless explorations on graphs, i.e. random walks, where you can decide at each step to query a node or not. The goal is to balance the time spent walking and the time spent querying.

Wednesday March 28, 2018, 11AM, Salle 3052
Yann Hamdaoui (Proofs and Programs and Conception and Analysis of Systems teams)
Translating a Concurrent Lambda Calculus into Linear Logic proof (nets)

Logical translations of intuitionnistic logic into linear logic have been studied for their sole interest. Incidentally, they provide translations of simply typed lambda calculus to linear logic: apart from its theoretical insights, the asynchronous nature of linear logic's cut-elimination make it also an interesting target of compilation, enabling distributed and/or parallel execution models. We present here translation of a richer typed calculus, featuring parallel threads and references, into a fragment of linear logic.

Wednesday March 21, 2018, 11AM, Salle 3052
Mengchuan Zou (Theory and algorithmics of graphs team) *Generalization of binary search in trees and other structures*

The tree search problem is the following generalization of the binary search problem. A search strategy is required to locate an unknown target node t in a given tree T. Upon querying a node v of the tree, the strategy receives as a reply an indication of the connected component of T \ {v} containing the target t. The cost of querying each node is given by a known non-negative weight

function, and the considered objective is to minimize the total query cost for a worst-case choice of the target.
We will also introduce some known facts on other structures and how tree search problem is related to other problems via equivalences.

Wednesday February 21, 2018, 11AM, Salle 3052
Zeinab Galal & Ranadeep Biswas (Algebra and computation & Modeling and verification)
Species of structure: a Bridge between Differential Lambda Calculus and Combinatorics & Verifying Database Histories

Species of structure: a Bridge between Differential Lambda Calculus and Combinatorics
Species of structure lie at the intersection of combinatorics and denotational semantics. They were first introduced by Joyal as a unified framework for the theory of generating series in enumerative combinatorics and multiple tools were developed for the resolution of differential equations of species in this setting. Later, Fiore presented a generalized definition that both encompasses Joyal's species and constitutes a model of linear logic.

We will first introduce and connect the different viewpoints of species of structure and their series counterpart (analytic and normal functors) presented by Joyal, Girard and Hasegawa. Next, we will examine how the bicategory of generalized species of structure forms a model of differential linear logic.

As our end goal is to develop methods of resolution of differential equations for λ-terms, we will investigate the possible directions to tackle this problem.

&

Verifying Database Histories

Popular databases offer control over the isolation level to which the operations in one transaction are visible to the operations in other concurrent transactions. Lower levels allow weaker consistency. So, we have to ensure that the histories of a database are consistent with their isolation levels.

Unfortunately, these isolation levels are mostly defined as low-level operations which makes it complicated to reason about the behavior of the system running under those isolations.

In this talk, we will present some popular isolation levels and consistency criteria for databases. We will introduce a framework, in which it becomes easier to formally reason about the behavior of a system. Then we will explore the complexities of deciding some consistency criteria using that framework.

Wednesday February 14, 2018, 11AM, Salle 3052
Narcisse Nya Kamtchoum (LIP6) *Modèles analytiques pour les performances des réseaux cellulaires*

Afin d'augmenter le débit et accroître la couverture réseau, les réseaux mobiles ne cessent d'évoluer rapidement vers des technologies caractérisées par des interfaces radio plus sophistiquées. Par exemple, alors que le déploiement des réseaux 4G ne faisait que commencer, les premières mises à jour des solutions LTE-A étaient déjà planifiées par les opérateurs et Actuellement, les technologies 5G font l'objet de recherches actives dans le monde entier. Ces changements rapides sont motivés par l'explosion du trafic mobile, tel que prédit par de nombreuses études et observé dans les réseaux actuels.

Cependant, les opérateurs ont du mal à s'adapter à la proportion toujours grandissante d'utilisateurs mobiles et à leur offrir une qualité d'expérience (QoE) satisfaisante. Dans ce contexte, il est importante pour les opérateurs et les équipementiers de disposer d'outils simples et efficaces pour mieux comprendre le comportement de leurs réseaux et évaluer la qualité des services offerts aux utilisateurs. Notre objectif est de proposer des modèles analytiques pour l'évaluation des performances des réseaux cellulaires en tenant compte de la mobilité des utilisateurs. Tout en permettant de résoudre des problèmes d'évaluation de performance les plus complexes, ces modèles se doivent d'être simple afin de faciliter leur utilisation.

Le séminaire sera donné en français.

Wednesday February 7, 2018, 11AM, Salle 3052
Nicolas Jeannerod (Team Analysis and conception of systems) *Unix filesystems and First-Order Theory of an Algebra of Feature Trees with Updates*

In the CoLiS project (for Correctness of Linux Scripts), our mid-term goal is to automatically verify certain properties on installation packages that may include shell scripts. In order to do that, we want to write a symbolic execution tool that would compute abstract specification for each installation script in term of filesystem transformations.
We investigate a logic of an algebra of trees with an update operation, which expresses that a tree is obtained from an input tree by replacing a particular direct subtree while leaving the rest intact. This operation improves on the expressivity of existing logics of tree algebras in our case of feature trees. These allow for an unbounded number of children of a node in a tree.

We show an efficient way of testing the satisfiability of existential clauses in this algebra that can lead to an efficient implementation of our symbolic execution engine. We also show the decidability of the first-order theory of this algebra via a weak quantifier elimination procedure which is allowed to swap existential quantifiers for universal quantifiers.

Wednesday January 31, 2018, 11AM, Salle 3052
Thomas Williams (Gallium, INRIA) *Refactoring ML programs using ornaments*

Ornaments are a way to describe changes in datatype definitions that preserve their recursive structure, reorganizing, adding, or dropping some pieces of data. The relation between two types given by an ornament can be used to define a lifting relation between functions operating on a bare definition and functions operating on the ornamented structures. Thus, ornaments provide a way to specify the desired behaviour of a program refactored to work on an ornamented datatype.
In this talk, I will explain how ornaments can be used to automatically lift a function. I will present a prototype implementation of lifting along ornaments for a subset of OCaml and describe some families of use cases. I will introduce a principled approach to obtaining a lifting from the base code, as abstraction followed by specialization. I will explain how this approach allows us to prove the correctness of the lifting.

Wednesday January 24, 2018, 11AM, Salle 3052
Alessandro Luongo & Ny Aina Andriambolamalala (Algorithms and complexity team & Combinatorics team) *Recent updates in quantum machine learning & Election de leader dans un réseau radio simple saut avec detection de collision*

Recent updates in quantum machine learning

In this talk we are going through some recent algorithms in the field of quantum machine learning. Most of the techniques use tools from quantum algorithmics such as counting, optimizing, estimating distances and singular values which will be introduced here. Using these primitives it's possible to build more complex operations of a matrix algebra. I'll also describe a classical machine learning algoritm in the process of being translated in a fully fledged quantum algorithm. This is the first biologically plausible quantum algorithm with an exponential speedup w.r.t the dimension of the space and the number of datapoints. This quantum algorithm has been simulated and used to classify handwritten digits with high accuracy.

Election de leader dans un réseau radio simple saut avec detection de collision

Les résultats de Dan Willard (1986) montrent un algorithme randomizé d'élection de leader en temps moyen $O(\log\log{n})$.

Depuis, la question de savoir s'il existe un algorithme convergeant en temps log-logarithmique mais avec très forte probabilité est ouverte.

Nous répondons affirmativement à cette question. Nous montrons aussi comment utiliser nos résultats pour élaborer des protocoles d'élection dans divers modèles de systèmes distribués.

These are two newcomers talk, 30 minutes each. The first will be in English, the second in French.

Year 2017

Wednesday December 20, 2017, 11AM, Salle 3052
Leo Stefanesco (Équipes “Preuves et Programmes” et “Algèbre et Calcul”) *“A concise introduction to logical relations” followed by “A Logical Relation for Monadic Encapsulation of State”*

1st part (E for Everyone): A concise introduction to logical relations
Logical relations are a powerful technique to prove properties about programs. In particular, for proving that two programs are contextually equivalent.

In this talk, we will see that, in System F (aka the polymorphic lambda calculus), the only program of type ∀ a, a → a is the identity.

I will also sketch how to extend logical relations to realistic languages such as ML.

2nd part (POPL talk rehearsal):

A Logical Relation for Monadic Encapsulation of State

We present a logical relations model of a higher-order functional programming language with impredicative polymorphism, recursive types, and a Haskell-style ST monad type with runST. We use our logical relations model to show that runST provides proper encapsulation of state, by showing that effectful computations encapsulated by runST are heap independent. Furthermore, we show that contextual refinements and equivalences that are expected to hold for pure computations do indeed hold in the presence of runST. This is the first time such relational results have been proven for a language with monadic encapsulation of state. We have formalized all the technical development and results in Coq.

Wednesday December 13, 2017, 11AM, Salle 3052
Simon Halfon (ENS Cachan) *Well Quasi-Orders and Extreme Stratospheric-Complexity-Classes of Death — Beaux pré-ordres et classes de complexité stratosphériques de la mort*

It is widely known how to prove the termination of an algorithm using well-founded orderings. It is however usually believed that no complexity upper bound can be derived from these termination proof, often seen as non-constructive. In this talk, I will present some ideas to infer upper bounds from such termination proofs. I will try to give you a taste of the complicated combinatorics behind, that results in surprisingly high complexities. Oxygen bottles and pressure suits required, we are going beyond Elementary.
No special knowledge is required to follow the talk.

—

Nous savons tous qu’il est très pratique pour prouver la terminaison d’un algorithme d’utiliser des ordres bien fondés. Cependant, il est commun de penser que cette technique ne donne aucune information sur la complexité de l’algorithme, car la preuve est non constructive. Dans cet exposé, je présenterai quelques idées pour extraire une borne supérieur de complexité d’une telle preuve de terminaison. J’essaierai de vous donner une idée de la combinatoire compliquée que cela engendre, et qui résulte en des complexité très élevée. Bouteilles d’oxygène et combinaisons pressurisées obligatoire, on s’envole au delà de l’Élémentaire.

Aucune connaissance spécifique n'est nécessaire pour suivre l'exposé.

Wednesday December 6, 2017, 11AM, Salle 3052
Axel Osmond & Yassine Hamoudi ([1] “Algebra and calculus” and “Proofs and programs” teams,

[2] Algorithms and complexity team) *New PhD student introduction session. [1] From pointless topology to formal topology [2] ACC0 and multiparty communication: fighting the log n barrier.*

[1] While point-set topology is highly practical as a framework to do spatial reasoning, one can rise some ontological and logical suspicions about naive notion of points as they constitute idealized objects with somewhat inaccessible aspects in a constructive and finite point of view. Locales and Frames theories are two deeply entangled realms aimed at rebuilding topology on latticial and categorical foundations, in which usual notions of points, opens, subspaces, separability, compacity… can be reexpressed as first order algebraic properties in latticial context, or both generalized and made constructive.
Formal topology goes further into this last direction, using systems of axioms about coverings as a deductive systems which leads to a type-theoretic flavored, predicative and constructive topology, endowed with multiple and finer notions of points, separability… and suited for intuitionistic reasoning.

[2] The Number On the Forehead model is a multiparty communication game between k players that collaboratively want to evaluate a given function F : X1 x … x Xk → Y on some input (x1, …, xk) by broadcasting bits according to a predetermined protocol. The input is distributed between the players in such a way that each player i sees all of it except xi (as if xi is written on the forehead of player i).

A central open question in this model, called the log n barrier, is to find a function which is hard to compute when the number of players is polylog(n) or more (where the xi's have size poly(n)). This has an important application in circuit complexity, as it could help to separate ACC0 from other complexity classes.

In this talk, we will recall first the connection between ACC0 and communication complexity, and then describe a new efficient communication protocol that prevents some important functions from breaking the log n barrier.

Wednesday November 22, 2017, 11AM, Salle 3052
Jules Chouquet (Proofs and Programs team) *Linear logic proof nets and Taylor expansion.*

I will first introduce linear logic proof nets, for the multiplicative and exponential fragment (MELL), and I will especially insist on the computational meaning of the exponential boxes: these are constructions containing the possibility of duplication and deletion of entire parts of the structures (all the non linear part of the calculus).
Once these notions are introduced, I will explain how it is possible to express this computational paradigm in a linear setting through a syntactical Taylor expansion. The idea is to understand exponential boxes in a differential variant of linear logic, and to represent it with linear combination.

If we have time, I will try to give an idea of some algebraic issues concerning this construction, and a method to show for example, that the normal form of the Taylor expansion of a MELL always converges.

NB: Taylor expansion is here analogical to the lambda calculus (with its differential version too) one, if someone heard about it, it can give a first intuition.

Wednesday November 15, 2017, 11AM, Salle 3052
Chaitanya Leena Subramaniam (“Algebra and calculus” and “proofs and programs” teams) *Homotopy type theory and the fibred structure of dependent types*

This is another session of the PhD introduction series.

Chaitanya will do a 30 minutes talk. Given that the talk will not last as long as usual, we will also take advantage of the opportunity to discuss the organization of the seminar.

Abstract:

The talk will not be about my particular research problem. It will seek instead to give a gentle pictorial introduction to the inherent structure of dependent types and how this structure determines what dependent types and dependently-typed programs (or proofs) *mean*.

The focus will be on why this structure naturally leads to homotopy type theory and univalence. As a bonus, and if time permits, there will be some remarks on univalence and extensionality.

Wednesday November 8, 2017, 11AM, Salle 3052
Francesco Antonio Genco (Technische Universität Wien) *Typing Parallelism and Communication through Hypersequents*

We present a Curry–Howard correspondence for Gödel logic based on a simple natural deduction reformulating the hypersequent calculus for this logic. The resulting system extends simply typed λ-calculus by a symmetric higher-order communication mechanism between parallel processes. The normalization proof employs reductions that implement forms of code mobility. We consider this result from a broader perspective and, following A. Avron's 1991 thesis on the connection between hypersequents and parallelism, we discuss the generalisation of the employed techniques for other intermediate logics.

Wednesday October 25, 2017, 11AM, Salle 3052
Cédric Ho Thanh & Isaac Konan (Algebra and calculus team / Combinatorics team) *New PhD student introduction session*

This special session will introduce two new PhD students who will each be giving a short talk.
Isaac Konan, Bijective proof and generalization of Siladic's theorem

In a recent paper, Dousse introduced a refinement of Siladic̀'s theorem on partitions, by using the method of weighted words, where the different parts could take 2 colours. The proof of that refined theorem used some recursive equations with q-series. In this presentation, I will give the big lines of a bijective proof of the Dousse's theorem, moreover which could be extended on a coloring with more than 2 colours.

Cédric Ho Thanh, Opétopes, Réécriture, et Koszulité

Ma thèse consiste en 3 mots que je vais tenter d'expliquer.

Wednesday October 11, 2017, 11AM, Salle 3052
Hadrien Batmalle (Équipe Preuves et Programmes) *From Cohen's Forcing to Classical Realisability: A New Approach*

English abstract below
Du forcing à la réalisabilité classique: une nouvelle approche

La réalisabilité classique permet d'interpréter des théories mathématiques classiques, comme la théorie des ensembles ZF, dans divers modèles de calculs (lambda-calcul avec continuations, domaines...). L'intérêt est double: côté informatique, il s'agit d'extraire des interprétations calculatoires de preuves classiques; côté mathématique, on obtient de nouveaux modèles de ces théories classiques (les deux aspects étant intimement liés). Une grande partie de la recherche en réalisabilité classique étudie la structure de ces modèles, qui apparaissent comme une généralisation du forcing de Cohen. Nous nous intéresserons ici à une nouvelle méthode pour exporter des propriétés des modèles de forcing aux modèles de réalisabilité, qui permet de construire des interprétations de deux théories contradictoires dans un même modèle de calcul, ce qui ouvre la voie à une analyse fine des conséquences calculatoires de la présence ou non de tel ou tel axiome.

From Cohen's Forcing to Classical Realisability: A New Approach

Classical realisability is a framework for interpreting classical theories in mathematics, such as the ZF set theory, in various models of computation (lambda-calculus with continuations, domains...). The goal is twofold: from the computer scientist's point of view, this is a method for extracting computational interpretations out of classical proofs; from the mathematician's, this is a trove of new models for these classical theories (both sides being tightly interwoven). A good deal of the research in this area is focussing on the structure of these models, arising as a generalisation of Cohen's forcing. In this talk we'll present some consequences of a new method for exporting properties of Cohen's forcing models into properties of classical realisability models. In particular we obtain interpretations of two incompatible theories in the same model of computation, which clears the path to studying the computational consequences of the presence, or lack thereof, of some axiom.

Wednesday September 27, 2017, 11AM, Salle 3052
Baptiste Louf & Victor Lanvin (Combinatorics and PPS teams) *New PhD student introduction session*

This special session will introduce two new PhD students who will each be giving a short talk. Here are the titles and abstracts of the talks:
Combinatorial maps : algebraic and bijective enumeration

Combinatorial maps (which are embeddings of graphs on surfaces) are well studied objects in combinatorics, which have applications in other domains, such as quantum gravity. The goal is to enumerate them (sometimes exactly, sometimes asymptotically). For this purpose, one can resort to (among other things) bijective or algebraic methods. The algebraic method is often more powerful and yields results more easily, however bijections give a more in-depth understanding of the models. Often, formulas are found via powerful methods, then people try to re-prove them bijectively. In this talk, I present what I'm focusing on, on the bijective side (Carell-Chappy formula) and on the algebraic side (KP equations). If time permits, I will explain a simple bijection I discovered during my Master's internship.

Gradual Set-Theoretic Types

A static type system can be an extremely powerful tool for a programmer, providing early error detection, and offering strong compile-time guarantees on the behavior of a program. However, compared to dynamic typing, static typing often comes at the expense of development speed and flexibility, as statically- typed code might be more difficult to adapt to changing requirements. Gradual typing is a recent and promising approach that tries to get the best of both worlds, by allowing the programmer to finely tune the distribution of dynamic and static checking over a program. However, this "gradualization" is sometimes too coarse, and an expression is often either fully dynamic or fully static. We argue that adding full-fledged union and intersection types (a.k.a. set-theoretic types) to a gradual type system solves this issue by making the transition between dynamic typing and static typing smoother.

Wednesday June 28, 2017, 11AM, Salle 3052
Tommaso Petrucciani (PPS team) *Semantic subtyping: an introduction*

Many type systems for programming languages include a notion of subtyping. Subtyping is often defined syntactically by a formal system, but this gets increasingly complex when union, intersection, and negation types are introduced.
In the semantic subtyping approach, instead, types are interpreted as sets and subtyping is defined in terms of set containment. Then, an algorithm is derived from the definition. While the algorithm is complex, the interpretation of types serves as a fairly simple specification. This approach also ensures that union and intersection on types behave as the corresponding operations on sets.

I will give an introduction to this approach and show how to define subtyping semantically for types including arrows, union, intersection, and negation, following [Frisch et al., 2008]. Then, we will look at ongoing work on adapting this approach (originally studied for call-by-value languages) to lazy semantics.

[Frisch et al., 2008] A. Frisch, G. Castagna, and V. Benzaken, Semantic subtyping, JACM, 2008.

Wednesday June 14, 2017, 11AM, Salle 3052
Timo Zijlstra & Emmanuel Arrighi *Quantum algorithms and Learning With Errors- based Cryptography & Distance Labels and Tree Skeletons*

Quantum algorithms and Learning With Errors- based Cryptography:
Post quantum cryptography is meant to replace today's standards like RSA and Elliptic Curve Cryptography (ECC), since these standards are threathened by quantum algorithms. The most researched post-quantum candidates are based on lattice problems, and in particular the Learning with Errors (LWE) problem. It is assumed that there exists no quantum algorithm that solves this problem efficiently. However, in a particular setting and under some strong hypothesis, it is very easy to solve LWE using a generalization of the Bernstein-Vazirani quantum algorithm. We will take a look at possible quantum cryptanalysis on LWE-based cryptographic applications.

Distance Labels and Tree Skeletons:

To answer distance queries on a fix known graph, it is interesting to do precalculation in order to reduce query time. A methode is to use Hub Labeling. Hub Labeling works well on road transport network. We will take a look at this methode and introduce the notion of Skeleton Dimension which give an insight on why it works well on road network.

Wednesday May 31, 2017, 11AM, Salle 3052
Clément Jacq (PPS team) *A playful introduction to game semantics (category-light)*

(English abstract below)
Une introduction ludique à la sémantique des jeux (allégée en catégories)

La sémantique des jeux est une branche de la théorie des modèles dont l'objectif est d'interpréter des formules de certaines logiques sous forme de jeux à deux joueurs. Son objectif initial était de lier les notions de vérité et de validité à des concepts de théorie des jeux tels que l'existence de stratégies gagnantes...

Après quelques exemples historiques, nous nous intéresserons dans cet exposé de manière informelle à un cas plus récent ou la sémantique des jeux modélise désormais des langages de programmation.

En guise de conclusion, nous évoquerons l'aspect formel avec la notion de structure catégorielle.

A playful introduction to game semantics (category-light)

Game semantics is a branch of model theory that aims at interpreting formulas of a given logic as two-player games. Initially, it was developed to link the notions of truth and validity to game-theoretic notions such as the existence of winning strategies.

After an historical example, we will look informally at a more recent case of game semantics where the games are used to model programming languages.

At the end, we'll mention the formal part with the notion of categorical model.

Wednesday May 17, 2017, 11AM, Salle 3052
Pierre Vial (PPS team) *An Introduction to Intersection Type Systems, and a New Answer to Klop's Problem*

Although the following abstract is (mostly) in French, the talk will be in English if there are non-French speakers in the room.
L'exposé aura deux buts:

1) Présenter les systèmes de types-intersection (ITS, intersection type systems), en particulier, les ITS à intersection non-idempotente. Je commencerai par des rappels basiques en lambda-calcul. On verra en quoi la représentation des lambda-termes par des arbres (bien qu'élémentaire) permet de comprendre la façon dont les ITS sont conçus et vérifient naturellement des propriétés que les systèmes de types simples ne peuvent (raisonnablement) pas avoir. Par exemple, dans un ITS, un terme est normalisable (i.e. il termine) ssi il est typable. Par opposition, dans un système de types simples, on aura seulement l'implication “Si le terme t est typable, alors il est normalisable” (*Propriété de Terminaison*). La notion de normalisation (i.e. terminaison) admet de nombreuses variantes: on en verra deux, la réduction de tête (HN, Head Normalization) et la réduction faible (WN, Weak Normalization). On verra aussi que les ITS ont des conséquences en lambda-calcul qui sont *externes* à la théorie des types.

Etant donné un système de type Sys (que Sys soit un ITS ou un système de types simples, d'ordre supérieur ou non), la propriété de terminaison (typable dans Sys ⇒ normalisable) est souvent difficile à établir (on doit généralement recourir à un argument dit de réalisabilité, attribué à Tait). Cependant, je présenterai le système R, introduit par Gardner et de de Carvalho, dans lequel l'opérateur d'intersection peut être vu comme non-idempotent et la terminaison repose sur un argument très simple que nous verrons ensemble.

2) Présenter un article (accepté récemment à LICS) traitant de lambda-calcul et de réduction infinitaires et dont voici l'abstract:

Infinitary Intersection Types as Sequences: a New Answer to Klop’s Problem

We provide a type-theoretical characterization of weakly-normalizing terms in an infinitary lambda-calculus. We adapt for this purpose the standard quantitative (with non-idempotent intersections) type assignment system of the lambda-calculus to our infinite calculus. Our work provides a positive answer to a semi-open question known as Klop’s Problem, namely, finding out if there is a type system characterizing the set of hereditary head-normalizing (HHN) lambda-terms. Tatsuta showed in 2007 that HHN could not be characterized by a finite type system. We prove that an infinitary type system endowed with a validity condition called approximability can achieve it. As it turns out, approximability cannot be expressed when intersection is represented by means of multisets. Multisets are then replaced coinductively by sequences of types indexed by integers, thus defining a type system called System S.

Wednesday May 3, 2017, 11AM, Salle 3052
Alexandre Nolin (Algorithms and complexity Group) *Quantum, a look through nonlocality*

In this talk I will try to give an introduction to the mathematical framework of quantum computing, completely disconnected of the underlying theory of quantum physics. After an exposition of a circuit model for quantum computing, we will split those circuits into two parts (the infamous Alice and Bob) and talk about the behaviours of those bipartite systems, more specifically somewhat counter-intuitive phenomenons like entanglement and nonlocality. Finally, we will see how those phenomenons are relevant in the study of communication complexity, and discuss recent results.

Wednesday April 19, 2017, 11AM, Salle 3052
Pierre Cagne (PPS team) *Lawvere's hyperdoctrines and notions of equality*

This talk will present hyperdoctrines, a widget invented by Lawvere in the late 70's to give a categorical account of type theories. It has the advantage to dissociate every construction/rules of a type theory: structural rules, logical rules, quantifier rules, equality rules, etc. As a welcomed side effect, it questions the legitimacy of such rules. In particular, we will take some time to study the equality and the relevance of its usual definition, and try to give a feeling of Lawvere's seminal thoughts on HoTT. If time permits, we shall discuss the insight of such an approach about a (for now non well established) "directed type theory", by which is roughly meant a type theory in which paths between terms are not necessarily reversible.

Wednesday April 5, 2017, 11AM, Salle 3052
Guillaume Lagarde (Automata and applications Group) *On the stability of the Lempel-Ziv compression algorithm*

LZ78 is a very simple lossless data compression algorithm published by Abraham Lempel and Jacob Ziv in 1978. It is fair enough to expect a certain stability from a data compression algorithm against small perturbation on the input. In this direction, Jack Lutz among with others asked the following question, so-called "the one-bit catastrophe": given an infinite word w, can the compression ratio of w be different from 1w? In this presentation, I will give some results in this fashion; in particular I would like to give the intuition of the fact that a catastrophe can indeed occur in LZ78. Joint work with Sylvain Perifel.
The presentation will just use basic combinatorics.

Wednesday March 22, 2017, 11AM, Salle 3052
Gabriel Radanne (PPS team) *GADTs gone mild*

Generalized Algebraic Data Types, often also called "Poor man's dependent types", are an extension of regular sum and product types that is available in OCaml and Haskell.
Since their adoption in "mainstream" languages, GADTs have been known for allowing to elegantly write toy typed interpreter at the cost of horrible type error messages and numerous headaches. Or, as Yaron Misky said, "I assumed that it was the kind of nonsense you get when you let compiler writers design your programming language.".

In this talk, I will present GADTs, what they are, and what useful things we can do with them. This will take us on quite a journey, with some traces of C, a pinch of memory layout, a cameo from pushdown automata and a healthy amount of Prolog. The only requirements will be a passing familiarity with OCaml and the caffeinated beverage of your choice.

Wednesday March 8, 2017, 11AM, Salle 3052
Pablo Eduardo Rotondo (Automata and applications Group) *Continued Fractions and the Recurrence of Sturmian Words*

In this talk I will present various aspects of Continued Fractions, motivating and explaining their relation to the factors of the so-called Sturmian Words. We conclude by a probabilistic study of the recurrence function of Sturmian Words, which is common work with Brigitte Vallée (CNRS, Univ. Caen).

Wednesday February 22, 2017, 11AM, Salle 3052
Lucas Boczkowski (Algorithms and complexity Group) *Minimizing Message Size in Stochastic Communication Patterns: Fast Self-Stabilizing Protocols with 3 bits*

The talk is based on a paper whose abstract is the following:
This paper considers the basic PULL model of communication, in which in each round, each agent extracts information from few randomly chosen agents. We seek to identify the smallest amount of information revealed in each interaction (message size) that nevertheless allows for efficient and robust computations of fundamental information dissemination tasks. We focus on the Majority Bit Dissemination problem that considers a population of n agents, with a designated subset of source agents. Each source agent holds an input bit and each agent holds an output bit. The goal is to let all agents converge their output bits on the most frequent input bit of the sources (the majority bit). Note that the particular case of a single source agent corresponds to the classical problem of Broadcast (also termed Rumor Spreading). We concentrate on the severe fault-tolerant context of self-stabilization, in which a correct configuration must be reached eventually, despite all agents starting the execution with arbitrary initial states. In particular, the specification of who is a source and what is its initial input bit may be set by an adversary.

We first design a general compiler which can essentially transform any self-stabilizing algorithm with a certain property (called “the bitwise-independence property”) that uses l-bits messages to one that uses only (log l)-bits messages, while paying only a small penalty in the running time. By applying this compiler recursively we then obtain a self-stabilizing Clock Synchronization protocol, in which agents synchronize their clocks modulo some given integer T, within O(log n log T) rounds w.h.p., and using messages that contain 3 bits only. We then employ the new Clock Synchronization tool to obtain a self-stabilizing majority broadcast protocol which converges in O(log n) time, w.h.p., on every initial configuration, provided that the ratio of sources supporting the minority opinion is bounded away from half. Moreover, this protocol also uses only 3 bits per interaction.

Based on joint work with A. Korman and E. Natale.

Wednesday January 25, 2017, 11AM, Salle 3052
Thibaut Girka (PPS team) *Oracle-based Differential Operational Semantics (or Explaining program differences with programs)*

We present a formal framework to characterize differences between deterministic programs in terms of their small-step semantics. This language-agnostic framework defines the notion of /difference languages/ in which /oracles/—programs that relate small-step executions of pairs of programs written in a same language—can be written, reasonned about and composed.
We illustrate this framework by instantiating it on a toy imperative language and by presenting several /difference languages/ ranging from trivial equivalence-preserving syntactic transformations to characterized semantic differences. Through those examples, we will present

the basis of our framework, show how to use it to relate syntactic changes with their effect on semantics, how one can abstract away from the small-step semantics presentation, and discuss the composability of oracles.

Wednesday January 11, 2017, 11AM, Salle 3052
Fabian Reiter (Automata and applications Group) *Asynchronous Distributed Automata*

The goal of this talk is to raise interest in the connections between distributed computing and formal logic. I will illustrate this relatively unexplored area of research by presenting an equivalence result between two very specific systems. The distributed computing side will be represented by a network of identical finite-state machines that communicate in an asynchronous manner, while the formal logic side will be represented by a small fragment of least fixpoint logic (more specifically, a fragment of the modal mu-calculus).