



Du  
**03**  
NOV.  
2022  
au  
**04**  
NOV.  
2022

08h40  
-  
19h00

**TOUT PUBLIC**

### **Conference FLAIM: Formal Languages, AI and Mathematics**

Institut Henri Poincaré  
Amphithéâtre Hermite  
11 rue Pierre et Marie Curie 75005 Paris

INSCRIPTION

**Registrations are now closed as all seats have been booked**

**Please note that the FLAIM conference is an onsite event. It is not possible to attend the event virtually.**

### **FLAIM: Formal Languages, AI and Mathematics**

#### **Context of the conference:**

URL de la page : [https://www.ihp.fr/fr/agenda/conference-flaim-formal-languages-ai-and-mathematics&is\\_pdf=true](https://www.ihp.fr/fr/agenda/conference-flaim-formal-languages-ai-and-mathematics&is_pdf=true)

The focus of the conference will be recent work that lies at the intersection of Mathematics and Artificial intelligence. Large efforts in mathematics formalization have led to the formal verification of deep theorems and made large resources available to the mathematical community. Formalization and formal proofs seem to be destined to play a growing role in the future of mathematics. On the other hand, AI techniques can be leveraged to explore mathematical objects in new and surprising ways, leading to new insights about classical objects making new questions emerge. Advances in formal language theory, in the automation of reasoning and the upsurge of interest with respect to dependant type theory make it possible to envision a greater place for AI to partly automate mathematical reasoning.

**November 3<sup>rd</sup> and 4<sup>th</sup>, 2022 at the Institut Henri Poincaré, Paris.**

### **Topics to be discussed during the conference:**

- AI in theorem proving and mathematics,
- Large Language Models and mathematical reasoning,
- AI as an intuition enhancer for mathematics,
- Mathematical objects as data for AI,
- Formalization of mathematics,
- Dependant type theory,
- Formal Languages and program proving,
- Interactive theorem provers,
- Cryptography.

### **Guest speakers**

Kevin Buzzard (Imperial College London)  
François Charton (Meta AI)  
Alex Davies (DeepMind)  
Amaury Hayat (ENPC)  
Kristin Lauter (Meta AI)  
Patrick Massot (Université de Paris-Saclay)  
Lê Nguyễn Hoàng (Calicarpa)  
Stanislas Polu (OpenAI)  
Pierre Yves Strub (Meta)  
Geordie Williamson (University of Sydney)  
Tony Wu (Google, Stanford University)

### **Evariste Team (Meta AI)**

Marie Anne Lachaux  
Timothée Lacroix  
Guillaume Lample  
Thibaut Lavril  
Xavier Martinet  
Hugo Touvron

URL de la page : [https://www.ihp.fr/fr/agenda/conference-flaim-formal-languages-ai-and-mathematics&is\\_pdf=true](https://www.ihp.fr/fr/agenda/conference-flaim-formal-languages-ai-and-mathematics&is_pdf=true)

## List of Talks

**Kevin Buzzard** (Imperial College London)

**Title:** *Beyond the Liquid Tensor Experiment*

**Abstract:** Earlier this year, a team led by Johan Commelin completed an 18 month project to formalise a profound theorem of Dustin Clausen and Peter Scholze. I'll talk about the story of how it happened and where we go from here.

**Francois Charton** (Meta AI)

**Title:** *Transformers in mathematics*

**Abstract:** We present several applications of transformers to problems of mathematics and theoretical physics, and discuss efforts to mitigate their limitations, out-of-distribution generalization and explainability.

**Alex Davies** (DeepMind)

**Title:** *Using machine learning to guide intuition in mathematics*

**Abstract:** Can machine learning be a useful tool for research mathematicians? There are many examples of mathematicians pioneering new technologies to aid our understanding of the mathematical world: using very early computers to help formulate the Birch and Swinnerton-Dyer conjecture and using computer aid to prove the four colour theorem are among the most notable. Up until now there hasn't been significant use of machine learning in the field and it hasn't been clear where it might be useful for the questions that mathematicians care about. In this talk we will discuss our recent work together with top mathematicians to use machine learning to achieve two new results - proving a new connection between the hyperbolic and geometric structure of knots, and conjecturing a resolution to a 50-year problem in representation theory, the combinatorial invariance conjecture. Through these examples we demonstrate a way that machine learning can be used by mathematicians to help guide the development of surprising and beautiful new conjectures.

**Amaury Hayat** (École Nationale des Ponts et Chaussées)

**Title:** *Guessing solutions to mathematical problems and learning maths from examples*

**Abstract:** In this talk we will see how a deep language model can learn to guess solutions to master level problems in mathematics with an impressive accuracy (higher than most humans) and without any built-in mathematical knowledge. We will illustrate this on several examples and we will discuss a possible extension to some mathematical problems for which no solution is currently known.

**Kristin Lauter** (Meta AI)

**Title:** *Post quantum cryptography with transformers (virtual talk)*

**Abstract:** Currently deployed public-key cryptosystems will be vulnerable to attacks by fullscale quantum computers. Consequently, "quantum resistant" cryptosystems are in high demand, and lattice-based cryptosystems, based on a hard problem known as Learning With Errors (LWE), have emerged as strong contenders for standardization. In this work, we train transformers to perform modular arithmetic and combine half-trained models with statistical cryptanalysis techniques to propose SALSA: a machine learning attack on LWE-based cryptographic schemes. SALSA can fully recover secrets for small-to-mid size LWE instances with sparse binary secrets, and may scale to attack real-world LWE-based cryptosystems.

**Marie Anne Lachaux & Guillaume Lample** (Meta AI)

**Title:** *Formal mathematical reasoning using graph search*

**Abstract:** In the context of mathematics formalization and AI based reasoning, we will present an online training procedure for a transformer-based automated theorem prover. Our approach leverages a new search algorithm, HyperTree Proof Search (HTPS), inspired by the recent success of AlphaZero. We will illustrate how one can substantially increase the performance of transformer only based reasoning, using this online training approach. We will also talk about some of our recent work on Autoformalization using Large Language Models.

**Patrick Massot** (Université de Paris-Saclay)

**Title:** *Formalized mathematics for mathematicians*

**Abstract:** I will describe the main reasons why I think formalized mathematics and proof assistant software will be useful to many mathematicians. I will cover both existing achievements and my expectations about the future. In particular I will explain how AI could help in various ways.

**Lê Nguyễn Hoàng** (Calicarpa)

**Title:** *Security in Machine Learning*

**Abstract:** Machine learning is now deployed on planetary scales, e.g. in vocal assistants, targeted advertising and content recommendation. However, despite this state of affairs, known cyber-attacks and evident vulnerabilities, the theory of machine learning security is still underdeveloped and lagging behind.

In this talk, I will highlight three leading security concerns (privacy, evasion and poisoning). I will then focus more particularly on poisoning. Unfortunately, as we will see, several impossibility theorems expose a fundamental vulnerability of any learning system, under modest adversarial attacks. I will also discuss the current leading ideas to increase, to some extent, the security of the training of machine learning models.

**Stanislas Polu** (OpenAI)

**Title:** *Mathematical reasoning capabilities of large language models*

**Abstract:** We will explore the application of large language models to mathematical reasoning, in particular their capabilities to produce informal reasoning as well as formal proof artifacts. We will discuss the trade-offs involved in generating informal vs formal proofs, the inherent limitations of large language models in both these modalities as well as potential directions to circumvent them. We will also review use of language models at the intersection of these modalities, in particular their use for auto-formalization.

**Pierre Yves Strub** (Meta)

**Title:** *Computer-Aided Cryptography*

**Abstract:** Cryptography plays a key role in the security of modern communication and computer infrastructures; therefore, it is of paramount importance to design cryptographic systems that yield strong security guarantees. To achieve this goal, cryptographic systems are supported by security proofs that establish an upper bound for the probability that a resource-constrained adversary is able to break the cryptographic system.

In most cases, security proofs are reductionist, i.e. they construct from an (arbitrary but computationally bounded) adversary that would break the security of the cryptographic construction with some reasonable probability another computationally bounded adversary that would break a hardness assumption with reasonable probability. This approach, known as provable security, is in principle able to deliver rigorous and detailed mathematical proofs.

However, new cryptographic designs (and consequently their security analyses) are increasingly complex, and there is a growing emphasis on shifting from algorithmic descriptions to implementation-level descriptions that account for implementation details, recommendations from standards when they exist, and possibly side-channels. As a consequence, cryptographic proofs are becoming increasingly error-prone and difficult to check.

One promising solution to address these concerns is to develop machine-checked frameworks that support the construction and verification of cryptographic systems. In this talk, I will present the state of the art in computer-assisted cryptography and outline future directions for computer-assisted cryptography, notably in terms of automated reasoning.

**Geordie Williamson** (University of Sydney)

**Title:** *How can machine learning help pure mathematicians?*

**Abstract:** The last few years have seen the first applications of machine learning in pure mathematics. I will survey some of these, including recent work with the DeepMind team on Bruhat intervals. All applications that I know of so far are tentative. My sense is that we are beginning to explore a rich world, but I could certainly be wrong. I will try to explain the main lessons that I have learnt and where we might hope to see interesting results in the future.

**Tony Wu** (Google, Stanford University)

**Title:** *Autoformalization with Large Language Models*

**Abstract:** Autoformalization is the process of automatically translating from natural language mathematics to formal specifications and proofs. A successful autoformalization system could advance the fields of formal verification, program synthesis, and artificial intelligence. While the long-term goal of autoformalization seemed elusive for a long time, we show large language models provide new prospects towards this goal.



## **INSTITUT HENRI POINCARÉ - UAR839**

Sorbonne Université / CNRS  
11 rue Pierre et Marie Curie  
75231 Paris Cedex 05

### **HORAIRES**

L'institut :

- lundi au vendredi de 8h30 à 18h,
- fermé les jours fériés.

Le musée - Maison Poincaré :

- lundi, mardi, jeudi et vendredi de 9h30 à 17h30,
- samedi de 10h à 18h,
- fermé le mercredi et le dimanche.