2024年度共同利用研究報告書

2025年02月26日

所属・職名 名古屋大学多元数理科学研究科・教授

Jacques Garrigue

	整理番号	2024a024

1.研究計画題目	コンピュータによる定理証明支援とその応用			
2.新規・継続	新規			
3.種別	プロジェクト研究			
4.種目	短期共同研究			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	Jacques Garrigue		
	所属 部局名	名古屋大学多元数理科学研究科	職名	教授
7.研究実施期間	2024年11月25日(月曜日)～2024年11月26日(火曜日)			
8.キーワード	定理証明支援系、形式論理、型理論、高階論理、プログラミング言語理論、アルゴリズム論、形式証明			
9.参加者人数	76人			

10.本研究で得られた成果の概要

この短期共同研究は元々、定理証明および定理証明支援系の研究者を集め、現状を確認し、今後の研究の方向性を提示するために計画された。この分野の多数の研究者が集まり、自分の経験をもとに様々な研究結果を発表し合った。Pédrot氏の講演などでは、強固な論理基盤を守りながら定理証明支援系を実装することの難しさが共有できた。また、それぞれの分野での定理証明の応用を通じて、形式証明の利用が現実的になっていることも再確認できた。中でも、定理証明支援系による論理学や数学基礎論に関する証明が多く紹介され、この分野の基盤強化に貢献できた。議事録はMIレクチャーノートとして出版予定である。また、来年も同様の集まりを東北大学で開き、研究の継続推進を図る予定である。

成果報告書「コンピュータによる定理証明支援とその応用」

2024 年 11 月 25 日から 26 日にかけて，九州大学マス・フォア・インダストリ研究所にて，上記短期共同研究の一環として第 20 回定理証明と証明支援系に関するミーティング（TPP2024）が開催された．このミーティングは，2005 年から毎年開催されており，定理証明システムの開発者やユーザーが集まり，幅広いトピックについて議論し，アイデアを交換する場となっている．今年は 10 年振りに九州大学で開催され，現地参加者 45 名という盛況振りであった．さらに 31 名のオンライン参加者もいた．講演の数も歴代で最も多いと思われる．

20 回目という大台を記念して，フランス INRIA の Pierre-Marie Pédrot 氏を招待講演者としてお迎えし，定理証明支援系 Coq の理想と現実に関する講演が行われた (図 1)．それに対する質問が多く，議論が湧いた．また，日本におけるこの分野の大御所である佐藤名誉教授が最近の研究に関する講演をしてくれて，存在感を示した (図 2)．企業参加者からは, 保険数理学の形式検証, ブロックチェーンにおける支払い認証, LLM による暗号プロトコル形式記述支援, などの講演が行われ, 形式証明支援の産業応用に関する報告と議論が行われた.

また，25 日の午前中にオーガナイザーたちと Pédrot 氏を交えたインフォーマルなディスカッションが行われ，特に Coq を利用する方々の様々な問題の解決につながった．予定外のハプニングとして，26 日の朝に筑肥線の強風による運休のため，開始が遅らせられ，佐藤氏の講演を録画する形で再開された．

1. 開催報告

日時 2024 年 11 月 25 日（月）13:00 〜 11 月 26 日（火）16:40

場所 九州大学 伊都キャンパス ウエスト 1 号館 D 棟 4 階 IMI オーディトリアム（W1-D-413）

形式 ハイブリッド開催（現地参加およびオンライン参加）

会議録 各講演の原稿を収録する MI Lecture Notes が準備中．また，各講演のスライドはプログラムのオンライン版に掲載されている．(`https://www.math.nagoya-u.ac.jp/~garrigue/tpp2024/program.html`)

11 月 25 日（月）

13:00-14:00 招待講演

- A Kernel of Truth, Pierre-Marie Pédrot（Galinette, INRIA)
  In this talk we will dive into the innards of a proof assistant based on type theory. We will focus more precisely on the technical constraints that this foundational setting generates, notably about the importance of computation at large. Contrarily to the dry and out-of-fashion feeling that this kind of topic may convey, it actually is a lively research area with many consequences, both for design and usage of such software.

14:15-16:10 一般講演

- Formalizing Premium Calculation of Life Insurance, 伊藤洋介（SOMPO ひまわり生命）
  Calculating premiums of life insurance is not an easy task. It requires mortality rates, interest rates, and future projections. The area of numerical analysis of insurance is called actuarial science. I report the ongoing work of formalization of life insurance mathematics, which is the life insurance part of the actuarial science.
- Coq/SSReflect における Inductive 型と seq T 型の cons の型変更に関する考察, 井上健太
  Coq/SSReflect に関する 2 つのショートトークです. 1 つ目は「コンストラクタ数が引数に依存して変化する (ある形式の)Inductive で定義された型」を定義したいときに Coq ではどのように表現すればいいのか考察しました. 特に引数として型と自然数の対のリストを引数にとり, このリストの各要素 (T_i, n_i) に対し, T_i 型の引数と n_i 個の再帰呼び出しを行う引数からなるコンストラクタを構成するような Inductive 型について考察します. 2 つ目はリストの型である seq 型のコンストラクタ cons の型は型引数 T に対し, $T \to \mathsf{seq}\ T \to \mathsf{seq}\ T$ で定義されますが, これを $T \to \mathsf{seq}\ (\mathsf{seq}\ T) \to \mathsf{seq}\ T$ に 変更して定義した型について考察します.
- Verification of the Garsia-Wachs algorithm, 金沢誠 (法政大学理工学部)
  The Garsia-Wachs algorithm is an algorithm for finding a binary leaf tree with a given leaf sequence whose cost is as small as possible, where the cost is the sum of the costs associated with the leaf labels weighted by the depths of the leaves. The algorithm, along with a proof of correctness due to Kingston, is given in Knuth's The Art of Computer Programming, Vol. 3. I outline a formalization of this correctness proof in Dafny and make a few observations about the algorithm.
- ブロックチェーンにおける支払い認証ポリシーの静的検証ツールの形式検証, 今井宜洋 (株式会社 proof ninja)
  本発表では，株式会社 DMM Crypto において管理している支払い認証ポリ シー TAP の設定を検証するために開発したツールについて述べる．TAP は Fireblocks によって提供される，ブロックチェーン上の資産管理および支払い認証における信頼性の高いソリューションを提供しているが，認証ポリシーが正確に設定され，安全に運用されていることを保証するための形式的検証が求められる．本研究では，Coq を用いて支払い認証ポリシーの安全性を形 式的に証明するツールを開発し，ポリシーが意図通りに動作し，潜在的な脆 弱性を排除することを実証した．これによりブロックチェーンにおける支払 い認証ポリシーの信頼性と安全性を向上させるとともに，業務効率の向上に も寄与することが期待される．

16:25-17:55

- Automated Theorem Proving by HyperTree Proof Search with Retrieval-Augmented Tactic Generator, 園田翔 (理研)
  We developed an automated theorem proving system using a large language model (LLM). The LLM generates proofs (precisely, sequences of tactics) by interacting with the Lean theorem prover. Generation of the tactic sequences is based on a Monte Carlo tree search called HyperTree Proof Search (HTPS) combined with a retrieval-augmented generator (RAG) called ReProver.
- Isabelle/HOL を用いた差分プライベートなアルゴリズムの安全な実装, 松岡和貴 (東京科学大学理工学系情報理工学院数理・計算科学系数理・計算科学コース)
  離散ラプラス分布を用いた差分プライベートなアルゴリズムを対象に， 定理証明支援系 Isabelle/HOL を用いてその形式化と検証を行う．さらに，Isabelle/HOL のコード生成機能を用いて差分プライバシーが検証された安全な実装を得る．
- 標準的な様相論理の Lean での形式化について, 野口真柊 (神戸大学システム情報学科)
  命題論理に様相演算子□と◇を導入した標準的な様相論理の Lean での形 式化について，現在の進捗と今後の展望について軽く紹介する
- Post の対応問題のインスタンスの証明生成, 大森章裕 (東京科学大学 情報理工学院 数理計算科学系 南出研究室)
  Post の対応問題のインスタンスの集合である PCP[3,4] を全て解決すると いう取り組みの過程で，その結果の信頼性を高めるために Isabelle/HOL の証 明を生成した試みを紹介します．インスタンスの数が 3170 個と大量にあり， それぞれへの結果を証明するためには適切な証拠を発見し，それを元に証明 を自動生成する必要がありました．自動生成の方針と，必要だったオートマトン理論の形式化について話します.
- 重複を除き辞書順で最小の部分リストを返す効率的なアルゴリズムの Agda による検証, 城戸道仁 (法政大学大学院理工学研究科システム理工学専攻)
  Richard Bird(2014) は，著作，関数プログラミングによる珠玉のアルゴ リズムデザイン (原題:Pearls of Functional Algorithm Design) にて， Haskell のライブラリ関数 nub の型を変更することで，計算量がΘ (n log n) であり，リストから重複を取り除いた上で，辞書順で最小のものを返す関 数のプログラムが構成できることを示し，実際に構成したプログラムを著書 に著した．この関数の正当性を検証を定理証明支援系 Agda を用いて行う．
- Complete graphs and independence numbers, 才川隆文 (名古屋大学)
  I will report on an ongoing formalization of graph-theoretic invariants. This is a continuation of the work presented at TPP2023, this time expanded by complete graphs and their characterization by independence numbers of graphs. This is a joint work with Kazunori Matsuda and Yosuke Tsuji.

11 月 26 日 (火) 9:00-10:30

- λ-計算の代数と幾何, 佐藤雅彦 (京都大学 情報学研究科)
  It is well-known that the set Λ of open terms of type-free λ-calculus dose not behave naturally when we regard Λ as an algebra equipped with the operation of function application. For example, the standard translation of λ-terms into combinatory terms does not admit the ξ-rule of the λ-calculus. In this talk, we will introduce a modified version of the λ-calculus without the ξ-rule but can prove exactly the same set of equations (under the β-equality) as those provable in the original λ-calculus. We proved our main results in Coq. (Joint work with Keisuke Nakano (Tohoku University))
- ZF+¬ AC の相対的無矛盾性証明の Isabelle/ZF による形式化, 舟根大喜 (東北大学大学院情報科学研究科)
  We formalize the relative consistency proof of ZF+¬ AC using Isabelle/ZF proof assistant. Our approach assumes the existence of a transitive countable model of ZF and uses forcing to construct a symmetric extension which is a model of ZF+¬ AC. We show that the symmetric extension satisfies ZF+¬ AC by formalizing a relativized forcing relation based on the formalization of forcing by Gunther et al.
- Lean を用いた Gödel の第一・第二不完全性定理の形式化, 齋藤彰悟 (東北大学大学院理学研究科数学専攻)
  Gödel の第一・第二不完全性定理の Lean4 を用いた形式化について報告す る．不完全性定理の形式化は 80 年代からすでに何度か行われているが，ここでは過去のものより強い結果である Cobham の R_0 上の第一不完全性定理と $I\Sigma_1$ 上の第二不完全性定理の証明の形式化を行った.

10:45-12:25

- 暗号プロトコルの形式記述に向けた LLM チャットボットの活用, 櫻田英樹 (NTT コミュニケーション科学基礎研究所)
  LLM チャットボットを活用して暗号プロトコルの形式記述を効率的に作 成することを試みた．具体的には LLM チャットボットが自然言語で記述され たプロトコル仕様を理解し，これを形式的な記述に変換する過程を説明する．この手法を用いることで，形式検証ツールへの入力作成の最初のステップを支援し，形式検証ツールを使い始める際の労力を削減することを目指す.
- A Formalization of Prokhorov's Theorem in Isabelle/HOL, 平田路和 (東京科学大学)
  本講演は，ITP2024 で発表した"A Formalization of the Lévy-Prokhorov Metric in Isabelle/HOL"において，口頭発表では詳細に触れなかったプロホロフの定理を題材とする．プロホロフの定理によれば，ポーランド空間上の一様に有界な有限測度の集合について，相対コンパクト性と緊密性は同値である．プロホロフの定理は，中心極限定理や Sanov の定理，輸送理論における最適カップリングの存在性を示すために用いられる確率論における主要定理の一つである．本発表では，プロホロフの定理とその証明で必要となるリースの表現定理，アラオグルの定理の特殊な場合の Isabelle/HOL における形式化について論じる．
- Delay モナドを用いた一般再帰関数に対する等式変形による検証, 川上竜司 (名古屋大学 多元数理学研究科)
  副作用を含む計算は，モナドと呼ばれる構造を用いることで関数型プログラムの中でうまく表現できることが広く知られている．Coq のライブラリ Monae は，そういったモナド構造に着目した，等式変形による副作用を含む計算に対する検証ツールである．一方で，Coq では無矛盾性を保証するため停止性を確認できる関数しか定義することができない． 従って本研究では，Monae に Delay モナドを追加することで，非停止な関数を含む一般再帰関数を表現し検証することに取り組んでいる． 本講演では，1.Delay モナドをどのように実装したか　2. それらを用いた検証 例　3. 現在取り組んでいる Delay モナドと他のモナドとの組み合わせについて説明する．
- On Representability of Multiple-Valued Functions by Linear Lambda Terms Typed with Second-order Polymorphic Type System, 松岡聡 (産業技術総合研究所工学計測標準部門データサイエンス研究グループ)
  We show that any many-valued function can be represented by a linear lambda term that is typed in second-order polymorphic type system.

13:30-15:10

- ペトリネットにおける到達可能性問題の変種間の還元可能性の形式化, 手塚 凜 (千葉大学大学院 融合理工学府)
  ペトリネットにおけるいくつかの到達可能性問題の変種間の還元可能性 が 1976 年に Hack によって示されている．本研究では，この証明を MathComp 上 で形式化した．この中には，還元先の決定問題に用いる新しいペトリネット を構成する必要がある非自明なものもいくつか含まれる．これらをアドホッ クに形式化するのではなく，系統的に証明するための共通手順を作成し，それに従って形式化を行った．
- Axiomatic real numbers for verified exact real-number computation, Sewon Park (Kyoto University)
  In this talk, I present cAERN, our axiomatic formalization of real numbers of computable analysis in dependent type theory, and the Coq proof assistant. The axioms argued to be sound for realizability interpretation enable us to extract certified exact real-number computation programs from proofs. I will further introduce our recent progress in cAERN in hyperspace computations and ordinary differential equation solving. This talk is based on my joint work with Holger Thies and Michal Konečný.
- Combining cost and behavior in type theory, Yue Niu (National Institute of Informatics)
- Lean を用いたスイッチング回路の安全性検証, 瀬川秀一 (北陸先端科学技術大学院大学)
  スイッチング回路の安全性検証における客観性と網羅性を確保するため， 定理証明支援系 Lean および数学ライブラリ Mathlib を用いた検証を試行して いる．検証にあたり，すでに構築された特殊関数や ODE に関する定理を活用 し，製品ごとに求められる特性を証明する．証明を効率的に実現するには， 状態空間の理論やハイブリッドシステムの検証理論の定式化が必要である．本発表では，検証手法の概要および証明の進行状況について紹介する．

15:25-16:40

- TPPmark 2024, Jacques Garrigue (名古屋大学)
- 導出原理の逆適用による定理の自動生成手法の提案, 西島海斗 (山口大学)
  本研究では，一階述語論理における証明技法の一つである導出原理を逆 方向に適用することで，新たな定理を自動生成する手法を提案する．現在， 定理証明コーパスが量・質ともに不足しており，データ不足が機械学習型の 自動定理証明器の性能向上を妨げていた．本手法では，結論から仮定を逆推 論することで多様な定理を生成し，データセットを拡充することを目指す． 提案手法の具体的なアルゴリズムの設計と実装について詳述し，今後の実験 計画についても述べる．
- Coq 証明支援系による DNA 計算の形式化, 早川銀河 (九州大学 数理学府 数理学専攻)
  DNA 分子のもつ性質を利用して計算するモデルの一つとしてスティッカー システムというものがあり，一部のスティッカーシステムは有限オートマトンと同等の計算能力が有ることが知られている．今回，Coq,ssreflect を用いてオートマトンを模倣するスティッカーシステム を構成し，その正しさを形式的に示した．
- Coq による実解析のための実用的な補題の開発, 石黒吉洋 (名古屋大学)
  Coq で確率プログラムの意味論を検証するために，我々は MathComp-Analysis を拡張してきた． 特に，基本的な確率分布を形式化するために，微積分の基本定理や積分の変数変換などの限定的なバージョンなど，微分と積分に関する様々な定理を作成した． 本講演では，Coq での確率論における重要な補題であるガウス積分の定式化に焦点を当て，連続関数の積分の評価をより扱いやすくする非有界区間への補題の一般化についても説明する．

2. TPPmark について

それぞれの定理証明支援系の特徴を比較するために，TPPmark 2024 という証明問題を皆で解いて，解を比較した．今年の TPPmark は互換による整列をテーマにしていた．整列のコストを比較の数ではなく，整列するのに必要な互換の数とする．この問題は回路設計や量子プログラムのコンパイルなどで現われる．

例えば，リスト $[5, 9, 1, 3, 7]$ を整列するには，すなわちリスト $[1, 3, 5, 7, 9]$ に変えるには，3 つの互換を適用すればいい．まず位置 1 と 3 を交換し，次に 2 と 4 を交換し，しまいに 4 と 5 を交換すればいい (ただし位置を 1 から数えた場合)．別の見方をすれば，置換 $[1 \to 3, 2 \to 5, 3 \to 1, 4 \to 2, 5 \to 4]$ を適用する必要がある．線形代数の講義を思い出すと，置換はまず循環に分解できる．ここでは (1 3) と (2 5 4) である (循環内に各位置が次のものになり，最後の位置が最初のものになる)．そして循環がまた互換に分解される．長さ m の循環が $(m - 1)$ 互換で実現できるので，最適なアルゴリズムが (要素の数 − 循環の数) 個の互換で整列を完成させる．

タスクは以下のとおりである．

1. 置換をその置換を実現する最小の互換の列に変換する関数を書きなさい．
2. この関数の正しさ，そして列の最小性を証明せよ．この際，置換に関する理論が必要だろう．
3. 重複のない自然数のリストを与えられたら，それを整列する最小の互換列を返す関数を書きなさい．正しさと列の最小性を証明せよ．
4. 重複のありうる自然数のリストを与えられたら，それを整列する最小の互換列を返す関数を書きなさい．正しさと列の最小性を証明せよ．

各解答とそれを紹介する資料は以下の URL で公開されている．

https://github.com/garrigue/tppmark2024

3. 開催中の写真

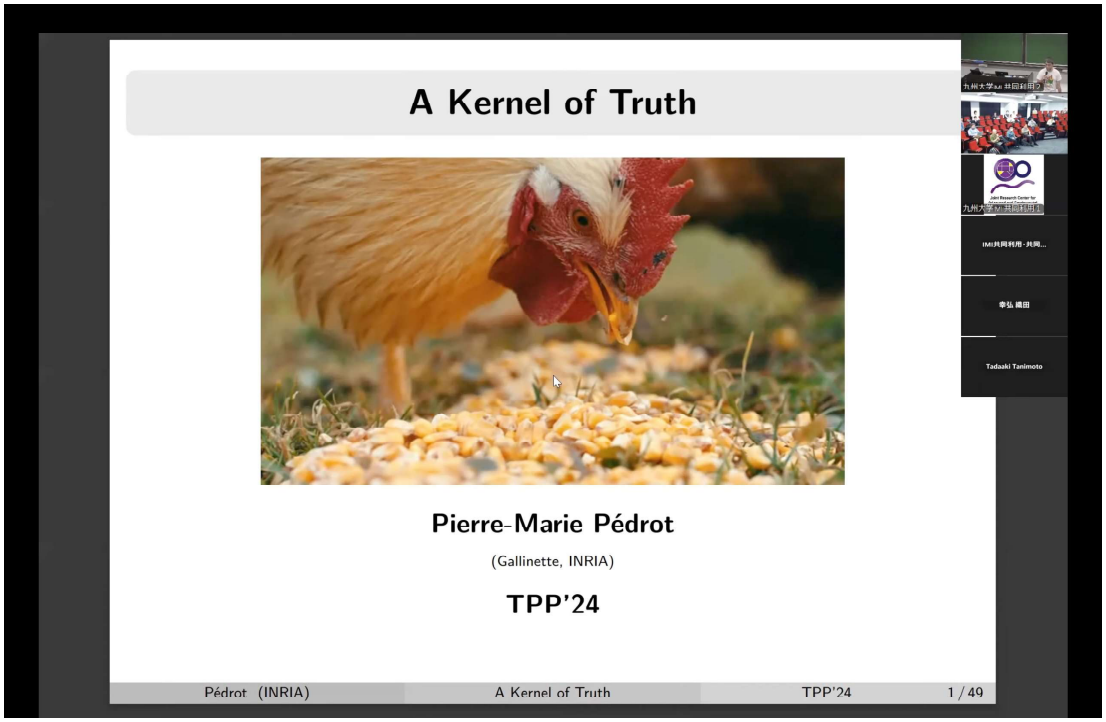

図 1: Pédrot 氏の講演

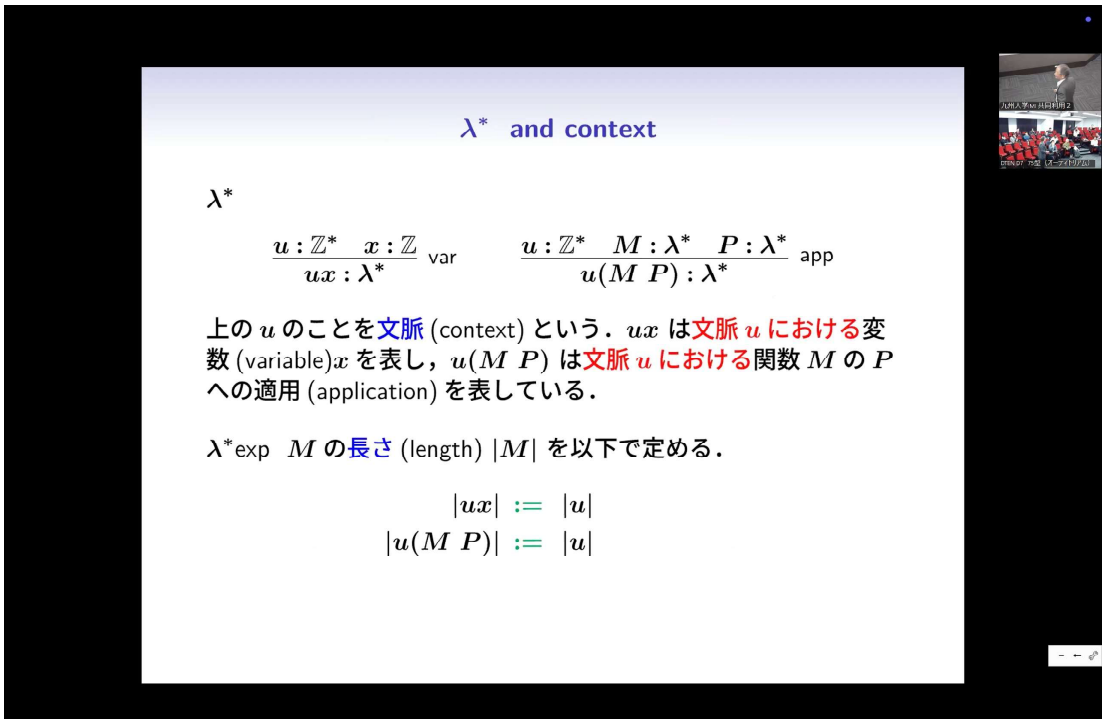

図 2: 佐藤氏の講演

開催日：2024/11/25～2024/11/26

コンピュータによる定理証明支援とその応用｜2024a024

カテゴリー：イベント　タグ：プロジェクト研究　短期共同研究

開催概要

- **開催方法**：九州大学 伊都キャンパスとZoomミーティングによるハイブリッド開催
- **開催場所**：九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIオーディトリアム（W1-D-413）
- **主要言語**：日本語
- **主催**：九州大学マス・フォア・インダストリ研究所
- **種別・種目**：プロジェクト研究-短期共同研究
- **研究計画題目**：コンピュータによる定理証明支援とその応用
- **研究代表者**：Jacques Garrigue（名古屋大学多元数理科学研究科・教授）
- **研究実施期間**：2024年11月25日（月）～2024年11月26日（火）
- **公開期間**：2024年11月25日（月）～2024年11月26日（火）
- **研究計画詳細**：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2024a024

プログラム

https://www.math.nagoya-u.ac.jp/~garrigue/tpp2024

11月25日（月）【公開】12:50-17:55

12:50-13:00:Opening

13:00-14:00

Pierre-Marie Pédrot (INRIA Atlantique)
A Kernel of Truth (Invited talk)

14:15-16:10

Yosuke Ito (Sompo Himawari Life Insurance Inc.)
Formalizing Premium Calculation of Life Insurance (30mn)

Kenta Inoue
Coq/SSReflectでコンストラクタ数が引数に依存して変化するInductive 型とseq T型のconsの型をT -> seq (seq T) -> seq Tに変更した型を定義したい

Makoto Kanazawa (法政大学理工学部)
Verification of the Garsia-Wachs algorithm

Yoshihiro Imai (株式会社proof ninja)
ブロックチェーンにおける支払い認証ポリシーの静的検証ツールの形式検証

16:25-17:55 (short talks, 15min each)

Sho Sonoda (Riken)
Automated Theorem Proving by HyperTree Proof Search with Retrieval-Augmented Tactic Generator

松岡和貴 (東京科学大学　理工学系情報理工学院数理・計算科学系数理・計算科学コース)
Isabelle/HOLを用いた差分プライベートなアルゴリズムの安全な実装

野口真柊 (神戸大学システム情報学科)
標準的な様相論理のLeanでの形式化について

大森章裕 (東京科学大学 情報理工学院 数理計算科学系 南出研究室)
Postの対応問題のインスタンスの証明生成

城戸道仁 (法政大学大学院理工学研究科システム理工学専攻)
重複を除き辞書順で最小の部分リストを返す効率的なアルゴリズムの Agdaによる検証

Takafumi Saikawa (Nagoya University)
TBA

11月26日 (火) 【公開】 9:00-16:40

9:00-10:30

Masahiko Sato (京都大学 情報学研究科)
λ-計算の代数と幾何 (40min talk)

Daiki Funane (東北大学大学院情報科学研究科)
ZF+¬ACの相対的無矛盾性証明のIsabelle/ZFによる形式化

齋藤彰悟 (東北大学大学院理学研究科数学専攻)
Leanを用いたGödelの第一・第二不完全性定理の形式化

10:45-12:25

櫻田英樹 (NTTコミュニケーション科学基礎研究所)
暗号プロトコルの形式記述に向けたLLMチャットボットの活用

平田路和 (東京科学大学)
A Formalization of Prokhorov's Theorem in Isabelle/HOL

川上竜司 (名古屋大学 多元数理学研究科)
Delayモナドを用いた一般再帰関数に対する等式変形による検証

Satoshi Matsuoka (産業技術総合研究所工学計測標準部門データサイエンス研究グループ)
On Representability of Multiple-Valued Functions by Linear Lambda Terms Typed with Second-order Polymorphic Type System

13:30-15:10

手塚 凜 (千葉大学大学院 融合理工学府)
ペトリネットにおける到達可能性問題の変種間の還元可能性の形式化

Sewon Park (Kyoto University)
Axiomatic real numbers for verified exact real-number computation

Yue Niu (National Institute of Informatics)
Combining cost and behavior in type theory

瀬川秀一 (北陸先端科学技術大学院大学)
Leanを用いたスイッチング回路の安全性検証

15:25-16:40

Jacques Garrigue (Nagoya University) and provers
TPPmark 2024 (20min)

西島海斗 (山口大学)
導出原理の逆適用による定理の自動生成手法の提案 (25min)

早川銀河 (九州大学 数理学府 数理学専攻)
Coq証明支援系によるDNA計算の形式化 (15min)

石黒吉洋 (名古屋大学)
Coqによる実解析のための実用的な補題の開発 (15min)

申込方法

事前申込制（組織委員，講演者のかたも登録が必要です）
参加無料
定員になり次第，参加登録を締め切らせていただく場合がございます．

＼下記URLより参加登録をお願いいたします／

参加登録フォーム

Zoom（オンライン）からご参加の方

Zoomを使ったオンライン開催，ハイブリッド開催の場合

参加登録後に件名［九大IMIより］Zoom用URLのお知らせというメールがimikyoten@gmail.comから自動配信されます．
届いていない方は，お手数をおかけしますがもう一度ご登録いただくか下記にメールにてご連絡をお願い申し上げます．
（迷惑メールフォルダもご確認お願いいたします）

＜九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点事務室＞
imikyoten(at)jimu.kyushu-u.ac.jp
(at)を@に変更してください

Zoomについて

開催日までにZoomアプリをインストールしてください．
Zoomアプリは無料版で問題なくご視聴いただけます．

ミーティング用Zoomクライアントのダウンロードは下記からお願いします．
すでにインストールされている方は最新版にアップデートをお願いいたします．
https://zoom.us/download#client_4meeting

パソコンやスマホへのインストール方法は下記をご参照ください．
https://zoom.nissho-ele.co.jp/blog/manual/zoom-install.html