数学基礎論の産業応用

国立情報学研究所／株式会社イミロン
蓮尾　一郎

筆者は情報学と数学の境界領域にあって，数学──特に「数学基礎論」とよばれる分野──の産業応用を目指し研究を行っている者である．ここで産業応用はそれ自体が最終目的というわけではなく，以下のように，（あくまで個人的には）理論と応用の大同団結に向けた活動の一環とみなしている．

- 情報学における理論的研究分野においては，容易に手法自体が目的と化して，分野自体が「特殊化の果ての緩やかな死」を迎えてしまう．これを避けるために，抽象理論の現実への “grounding” を常に意識したい．
- 理論研究は極めて個人的・内省的営みであると考えられがちだが，大きな体制で取り組む協働的な理論研究の形も数多く存在するし，ぜひその強みを追求したい．産業応用はすなわち「仕事のために成果を使ってくれるシリアス・シビアなユーザー」という仲間・共同研究者を得ることを意味し，研究体制の維持・拡大に有効である．

平たく言うと「裾野を広げていくことで見える理論的高みもあるのではないか」ということである．本稿では，筆者らが進める上記の研究内容を手短に説明したのち，そこで得た数学の産業応用に関する一般的・実践的ノウハウをいくつか共有したい．

「数学基礎論の産業応用」

多くの読者にとって，数学基礎論というと「あまり知らない」「数学会でそういう分科会を見た気がする」「気にする人がいるのは知っているが，自分が数学をやるにあたってはあまり気にしたくない」などという印象なのではないだろうか．特に，「役に立つ」「産業応用」という言葉とは遠いイメージだと思われる．

この理由の一つとして国内の数学コミュニティに特有の事情がある．国内では「数理論理学」という大きな分野と，その一応用としての「数学基礎論」という分野がしばしば混同され，歴史的に一括りに「数学基礎論」と呼ばれて来た．よって本稿のタイトルは「数理論理学の産業応用」でもまったく差し支えないわけだが，それだとパッと見のパンチ・インパクトがだいぶ落ちてしまうので，タイトルではあえて数学基礎論という言葉を使っている．読者の寛恕を請う．

さっそくだが脱線気味に話を展開したい．上で「一応用としての『数学基礎論』という分野」と言ったところがすでに違和感があるかもしれない．しかしこれは，数理論理学と数学基礎論を次のように定義することで自然に受け入れられるだろう．

- 数理論理学： 論理的・記号的な推論・操作を数学的に研究する学問．これら推論・操作の代表例は数学における証明であるが，人間の思考や法律上の論理展開，計算機のプログラムなどもその例であり，それぞれ哲学，法学，情報学における応用につながっていく．
- 数学基礎論：（数理物理学が物理現象を数学の言葉で研究するように）数学者の営為を数学的に研究する学問．ここで「数学者の営為」とは証明を書くことにほかならず，よって「数学的証明の数学的定義」や「特定の定理の証明が不可能であるという（メタレベルの）定理の（メタレベルの）証明」などが展開される．

よって数学基礎論は数理論理学の数学への応用に他ならず，その意味で「応用数学」なのである．実際 2017 年度までは科研費細目でも「数学基礎・応用数学」と一括りだったし，最新の区分でも「解析学，応用数学およびその関連分野」に入っている．

しかし一方で，数理論理学・数学基礎論が使役する数学的技術の種類は解析学からはだいぶ遠く，代数学にずっと近い．これも上記の定義からすると自然であり，数理論理学が記号的推論を研究対象とする一方で，代数学も「多項式という記号表現の数学的指示内容」や「記号列の商による自由代数の構成」など，記号操作を大本にする数学である（と筆者は思っている）．

ともかく以上は脱線であり（くわしくは [照井] などを参照されたい），以下話を戻して，数学基礎論（正確には数理論理学）の情報学応用について述べていく．

ソフトウェア科学における「プログラムのバグなし証明」

情報学の中のソフトウェア科学とよばれる分野では，「プログラムが正しいことを数学的に証明しよう」というパラダイムが長年追求されてきた．プログラムを「計算機の動作を司る記号的レシピ」と思うとこれはまさに数理論理学の研究対象であり，そのふるまいを数理論理学的に定義して（プログラムの意味の定義➔「意味論」），その性質を数学的に証明できる．（実はこの話は因果がひっくり返っており，歴史的には計算機自体が数学基礎論から生まれたのだが，もう脱線する紙幅はない．）

人間が書くプログラムはとかくバグを多く含むものだが，バグが人命に関わる局面は枚挙に暇がない．プログラムの品質・正しさ・安全性の保証のやり方というとテストが思いつくだろうが（「いろんな入力で試してみて期待通りの出力を得たから，まあ大丈夫であろう」），上記の数学的証明のアプローチの強みは「任意の入力 i について…」という証明が書けてしまうことである．無限通りあり得る入力値について，数学的証明という絶対の品質保証を与えることができるというわけである．

筆者の博士課程以来の研究もまさにこのパラダイムに従うものであり，さまざまな情報システムの正しさ・安全性に対して，実効的証明を行うための数学的理論（特に圏論を用いた意味論）とアルゴリズム・ツールについて研究を行ってきた．

ソフトウェア科学の危機：「モデルがない！」すなわち「定義がない！」

筆者はこのような研究の伝統の中で，「圏論の一般性をうまく使えば，今日多様化しているさまざまな情報システムの統一的『バグなし証明』手法が樹立できるはずである」と謳って 2016 年から大きな研究プロジェクトを開始した（JST ERATO 蓮尾メタ数理システムデザインプロジェクト）．しかし開始後しばらくして，そもそも「バグなし証明」というパラダイム自体が危機に瀕していることに気づき大いに慌てた．他人が慌てているところを見るのは楽しいものであるから，以下この話をしたい．（しかもまあまあハッピーエンドに着地するので，安心して見ていてほしい．）

我々のプロジェクトでは自動運転車の安全性保証──できれば数学的証明──を目標の一つとして掲げた．当然であるが，数学で何かを証明するためには，登場するすべての概念の正確な定義が必要となる．たとえば図 1 左では Banach の不動点定理を証明するため完備性の定義を行っているわけだが，ひるがえって自動運転車のために安全性定理を述べてこれを証明するためには，登場する「自動運転車」という概念を定義する必要がある（図 1 右）．この定義は，自動運転車のふるまいの正確な数学的記述でなければならず，また同時に，単純で本質を捉えていることが望まれる（単純でないとその後の証明が大変になる）．この定義を行う営みは，たとえば自然現象を微分方程式で記述するように，数学の外にある実体や現象を数学の俎上に載せてあげる数理モデリングの営みにほかならない．

そして問題は，自動運転車の定義すなわち（論理的な）数理モデリングが困難であるということである．自動運転車は巨大なシステムであり（デジタル制御と，物理コンポーネント，さらに物体認識用のニューラルネットなどの組み合わせ），また，サードパーティ製部品など内部の動作原理が不明なブラックボックスを多く含む．

そしてより大きな問題は，この「モデル（定義）がない」という問題が自動運転車に限らないことである．航空宇宙や化学プラントといった物理情報システムでも問題は同じだ．さらに最近の AI（正確には統計的機械学習）においても，その動作原理はノイジーなビッグデータから数理的最適化で学習した巨大な重み行列であり，これを「定義」として論理的に安全性証明を行うことは非常にむずかしい．

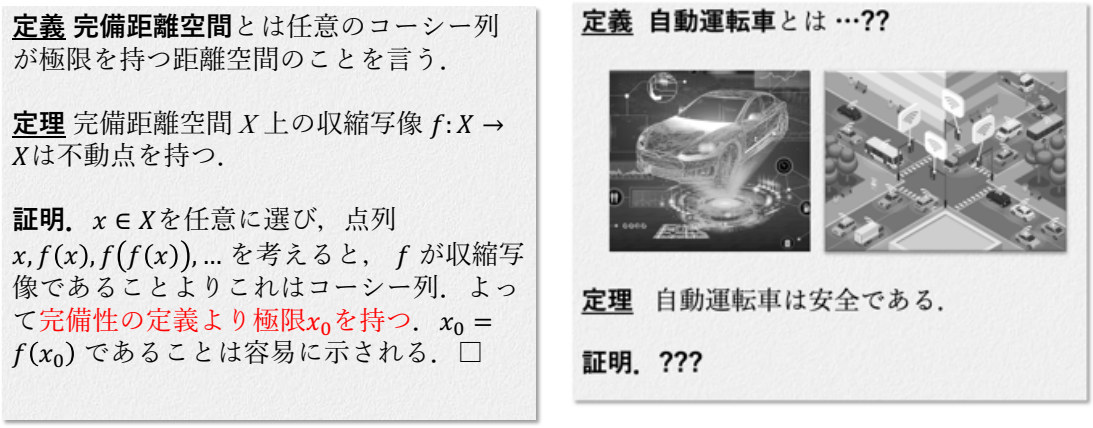


図 1 数学における定理と定義（左），ソフトウェア科学における定義すなわちモデリング（右）

以上をまとめると次のような現状認識となる．すなわち，情報システムの安全性保証という重大な社会的責務に対し，ソフトウェア科学は「数学的証明」という情報学の根源的方法論に基づいて，その遂行を目指してきた．この方法論は「情報システム＝プログラム」という伝統的な状況ではうまくいくものの（記号的動作レシピたるプログラムそのものを数理モデルとみなせる），今日多様化して物理情報システムや AI システムを包摂する広範な情報システムに対しては，「論理的解析に適した数理モデルが得られない」という重大な困難に直面してしまう．

自動運転車の安全性証明： RSS の割り切り方

以上の困難に気づいて筆者は 2018 年頃に非常に慌てたわけだが，幸いマツダ株式会社との協働を通じて，この困難の乗り越え方の一つのアーキタイプを自動運転車に対して得ることができた．これは最初に述べた産業応用の理論研究的価値（仲間が増える）の一例であるとも考えている．

この成果 [Hasuo et al. 2023] では，RSS (responsibility-sensitive safety) という方法論 [Shalev-Shwartz et al. 2017] を（数理論理学で言うところの）形式的論理体系として数学的に整理し，自動運転車の安全性証明を厳密に与えることができることを示した．

この成果では上記の「自動運転車の中身のモデルがない！」という困難を乗り越えるため，さまざまな詳細を削ぎ落として理論体系を「割り切った」ものとした．一方でこの割り切り方は，現在の交通システムという応用的・社会的状況にうまく整合するように設計されており，成果の有効性──自動運転が広く実世界展開するための「社会的安全ルール策定」の問題に対する有効性──が広く認識されつつある．実際，国際安全規格への打ち込みや（IEEE 2846 規格），いくつかの企業の研究開発に

おける活用，さらに自動車業界全体の取り組みにおける活用について，筆者らや他の研究者・技術者による活動が進行中である．

上記成果の詳細については論文 [Hasuo et al. 2023] や解説記事 [日経ロボティクス 2022] [蓮尾 2023] [蓮尾 2024] 等にゆずるが，本稿では本成果の「割り切り方」について説明したい．ここでのポイントは以下のようになる．

- ソフトウェア科学が直面する「モデルがない」という方法論危機に対する一つの回答は，モデリングの粒度を必死に選ぶこと．詳細であればよいということは決してなく，数理論理学的解析の実行可能性と，応用的・社会的意義のバランスをうまくとる必要がある．

具体的に上記成果では，RSS のオリジナル論文 [Shalev-Shwartz et al. 2017] の「数理論理学的本質」を図 2 のように整理することから始めた．すなわち，複雑でモデリングの望みが薄い自動運転車内部の動作原理は「見ない」と割り切って，代わりに各車のふるまいに RSS ルールという論理的規則を課すのである．そして安全性保証は，「各車が RSS ルールに従うという仮定のもとで，事故は発生しない」という，条件付き・契約ベースの安全性定理を数学的に証明する，という内容になる．

（ところで RSS のオリジナル論文 [Shalev-Shwartz et al. 2017]は機械学習及び自動運転の専門家の手によるものであり，上記数理論理学的本質を含む多数の重要なアイデアが明示的・暗示的にかかわらずちりばめられた，読み手の解釈の可能性を大いに残した論文である．そこから数理論理学的に重要なモデリング指針を抽出できたのは，異分野協働のご利益の一例だと思えなくもない．）

RSS ルールの例を見てみよう（オリジナル論文からのもの）．図 3 では一車線の単純な状況で追突を避けるために，後車に「車間距離をこれだけ確保せよ」「それが難しいなら，適切にブレーキせよ」というふるまいの外形的規則（RSS ルール）を要求している．この RSS ルールを仮定し，さらに前車の最大減速度を仮定すれば（$a_{max,brake}$），衝突が起きないことの証明は易しく，ほぼ高校物理の範囲でできる．

図 3 の例では運転シナリオは非常に単純だが，たとえば「高速道路に合流したい」「追越車線から他車を避けながらレーン変更を繰り返して安全に路肩に停止したい」といった複雑なシナリオでは，ルールの導出は段違いに困難なものになり，適切な場合分けを行いながら数学的証明を形式的に（＝数学的に定義された論理体系の中で ≒ ソフトウェアの中で）書いていくことが欠かせない．これを可能にしたのが我々の数理論理学的成果 [Hasuo et al. 2023] である．

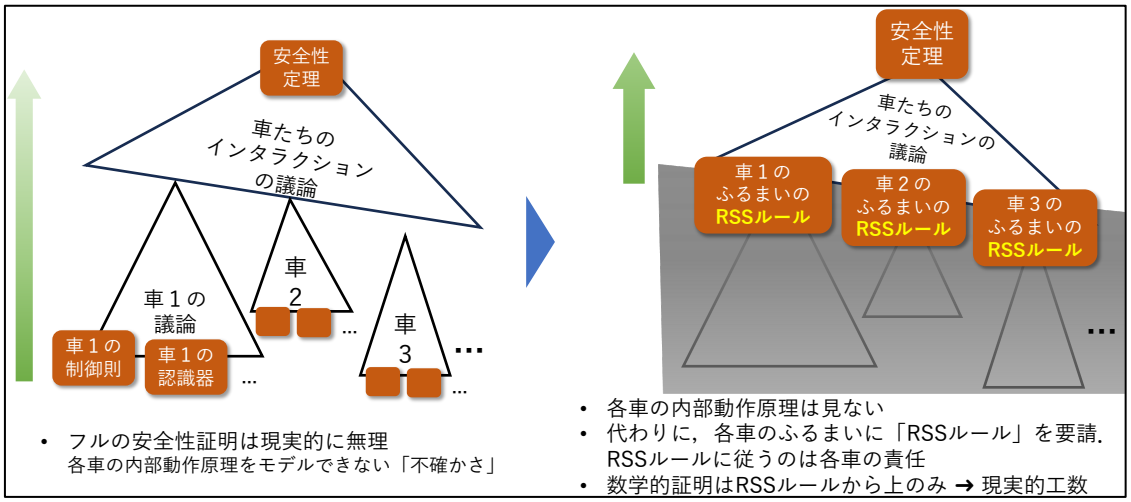
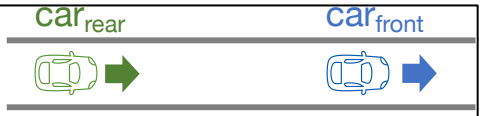


図 2 RSS の数理論理学的本質．数理モデリングを「RSS ルールより上」に限定

RSS条件：
車間距離を



$$d_{\min} = \left[v_r\,\rho + \frac{1}{2} a_{\max,\mathrm{accel}}\,\rho^2 + \frac{(v_r + \rho\, a_{\max,\mathrm{accel}})^2}{2a_{\min,\mathrm{brake}}} - \frac{v_f^2}{2a_{\max,\mathrm{brake}}} \right]_+$$

以上確保すること

適切反応 (proper response)：
（上記RSS条件の違反が予見される場合）
反応時間 ρ 以内に 減速度 $a_{\min,\mathrm{brake}}$ でブレーキすること

条件付き安全性補題：
RSS条件が真である状態から適切反応を実行すれば，衝突は発生しない

図 3 RSS ルールの例．一車線同方向シナリオにおける追突回避のためのルール

数学と社会との間の界面： RSS の場合

図 2 については「思い切って割り切ったものだ」「確かにこれだったら定義・証明ができそう」と思ってもらえたと思うが，「割り切り過ぎで役にたたないのでは？」という読者もあろう．この問題──数学と社会の界面の問題──について論じたい．

特に，安全性定理の「RSS ルールに従えば安全」の仮定部分の妥当性はどうだろうか．すなわち，RSS ルールを策定したとして，各車がそれに従うという仮定は現実的なのであろうか．

自車がルールに従うかどうかについては，明確かつ技術的な解がある： 自動運転のコントローラを，RSS ルールに基づく「安全コントローラ」で適切に「安全ガー

ド」してあげれば，自車のふるまいに RSS ルールを強制することができる．詳細は[Eberhart et al. 2023]を参照されたい．

それでは他車についてはどうだろうか？ たとえば図 3 では，他車（前車）に「ブレーキ減速度は高々$a_{\max,\,\mathrm{brake}}$」という仮定をおいているが，これは現実的なのだろうか？ 他車のふるまいに安全コントローラを付加してまわるわけにはいかないので，上記安全ガードの方法は使えない．ここでの我々の解は，おおざっぱに言って「他車のルールは法律上・運転慣習上自然に要請されるものであり，仮にこれらが破られて事故が起きたら，その責任はルールを破った他車にある」というものである．

「そんな身も蓋もない…」と思う読者も多いだろうが，次のように説明できる．

- そもそも現在の道路交通システムは事故を完全に防ぐようにはできていない．人車混合の道路を許した時点で，ある程度の事故は社会として許容している，というわけである．（筆者が酔っ払って道路で寝ることを絶対に防ぐためには，お台場のゆりかもめのように鉄格子でレールを覆うべきだし，そこまでやっているからゆりかもめは無人運転できる．）ちなみに現在の道路交通システムは，馬車時代からのさまざまな変遷を経た歴史的産物である．
- 他車がルールを破っても最悪衝突だけは避けるように，RSS ルールの安全ガードを多重化し，「他車に強いルールを課して安全な合流を保証する」「他車に弱いルールを課して（合流はできないかもしれないが）衝突は避ける」という graceful degradation が考えられる．詳細は[Eberhart et al. 2023].

以上の議論をまとめる．（筆者を含め）数学者はとかくモデル・理論を詳細化しがちだが，詳細なモデリングが不可能なシステムが多くあり，「割り切り方」が重要となる．自動運転に関しては，RSS の数学的割り切り方（図 2）が「事故はゼロにできないが各車のふるまいルールに基づいて責任追及を行う」という社会システムにピッタリはまって，数学と社会の良い界面を与えている．

数学の異分野協働：「手を汚す」覚悟，モデリングを数学者が覚悟

以上，情報学の文脈で道路交通システムという身近な例も用いながら，数学と社会の界面──数学概念と社会概念の対応関係──を論じてきた．大きなポイントは (1) 数学と社会の界面を切り出す（すなわち，良いモデリングを行う）のはむずかしい，(2) しかし多くの場合何らかの良い界面が見つかるし，そう信じて強い気持ちで努力したい，この 2 つである．

そして筆者の応用数学の研究者としての信念は，

- 上記の界面の発見（すなわちモデリングの粒度の決定）を応用分野側に任せることはできず，数学側が汗をかかなければいけない

というものである．言い換えると「理論と応用のマッチングは理論研究者の脳内でしか起こり得ない」というものである．

数学者の多くはこの結論にゲンナリしてしまうであろう．彼ら彼女らにとって活躍の場は定理の証明であり，その準備たる定義・問題設定は誰かに任せたいのであり，泥臭い現実の中から数学的構造を切り出して定義するといった「ヨゴレ」仕事は避けて，すべてが定義済みであるような数学的にキレイな世界で働きたい．

ここで筆者はすべての数学者がヨゴレ仕事をすべきだと主張しているわけではもちろんない．応用数学においてヨゴレ仕事は必須であり，それをやる人も（他の数学者と同様に）評価されるべきである，と主張しているわけである．

筆者は一度面接で応用数学への心意気を質問して「応用問題を作用素環論の言葉にして持ってきてくれますか？ そしたら解きます」と答えられたことがある（これがちゃんと笑い話に聞こえたら，本稿の意が読者に伝わっている）．その機会はチーム体制の事情で採用しなかったが（ヨゴレ仕事を過剰にいやがる人がいるとチーム全体の士気に影響する），十分ちからのあるチームになったら，そういう人にもうまく活躍してもらえる仕組みを作りたいものだと考えている．

産業応用の実践の経験から

本稿では数学基礎論の（多分に偏った）導入からはじめて，数理論理学の情報学応用，特に自動運転への応用から，数学と社会との界面の話を述べてきた．せっかくなので最後に，筆者の産業協働の経験から実践的なノウハウをいくつか述べたい．

まず，産業協働は（分野内協働や異分野協働と同じく）作法がたくさんあり，これらの作法はやってみないとわからない．最初はよくわからなくても・うまくいかなくても，しばらくやっていて初めて見えてくる景色もあるので，ぜひチャレンジしてほしい．この際大切なことは一つだけで，協働相手のニーズにとことん寄り添うことである．大概の場合相手のニーズは相手自身も明確に知らないので，議論しながらニーズを明確化していくこともこちらの仕事である．

筆者は最初の頃共同研究の値付けに悩んだし，同じ悩みは他の研究者からもよく聞く．この際「自分の時間」の値付けでなく「（自分の時間という）大学の資源」の値付けだと考えるとだいぶ気が楽になる．たとえば「あまり安くしてしまうと，国の資産たる国立大学教員の時間を使って一私企業に不当な便益を供与してしまう」というわけである．具体的には 1 時間 3 万円くらいはもらってよいのではないだろうか（当然ながら，打ち合わせが 1 時間なら実働はその 3〜10 倍と思って良い）．ここでは「本来これくらいもらうべきだが，こちら（研究者及び所属機関）としても研究が進むメリットがあるので 1 時間 1 万円でよいです」と言うこともできる．

大学発スタートアップについても述べたい．研究成果活用において「技術供給元が大学の研究室だと永続的サポート体制が望めるか不安」という声は多く，サポート・改良体制を商業化するのは意義がある．レベニューによる研究体制の維持もできる．

筆者らは実際，研究成果をもとにした（正確には「研究機関の所有する知財のライセンスを受けた」の意）スタートアップ企業を立ち上げた．数年前は起業なんてどうやるのか想像もできなかったが，起業にしろ特許出願にしろ，「非常に大きなエコシステムがどこか存在するので，一度そこにつながればあとはどんどん進む」ということをお伝えしておきたい．起業のエコシステムにはベンチャーキャピタルやインキュベーション支援制度等があり，特許のエコシステムには弁理士事務所や TLO，INPIT の知財支援制度等がある．（ところで弁理士事務所はアタリハズレが非常に大きいので良いところをみつけたい．）筆者は JST（科学技術振興機構）の支援を通じてこれらエコシステムにつながることができた．手厚い支援に感謝するとともに，応用数学の志を持った研究者が同じ支援を受けられること，及びこれら支援を活用して数学のちからを社会に示す同僚が次々に現れること，以上を願ってやまない．

参考文献

- 「自動運転の安全性を数学的に証明する技術、NII が運転ルールの構築法を開発」．日経ロボティクス 2022 年 10 月号，日経 BP
- C. Eberhart et al. Formal Verification of Safety Architectures for Automated Driving. Proc. IEEE Intell. Veh. Symposium (IV), 2023
- 照井 一成．「コンピュータは数学者になれるのか? 数学基礎論から証明とプログラムの理論へ」，青土社，2015
- 蓮尾 一郎．「自動運転車の安全性の数学的証明──論理学の社会応用の一例として」，科学 2023 年 3 月号，岩波書店
- 蓮尾 一郎 他．「要求仕様と責任範囲の明確化のための論理学的技術： ソフトウェア科学からのアプローチ」，自動車技術会春季大会学術講演会予稿集，2024
- I. Hasuo et al. Goal-Aware RSS for Complex Scenarios via Program Logic. IEEE Trans. Intell. Veh. 8(4): 3040-3072, 2023
- S. Shalev-Shwartz, S. Shammah, A. Shashua. On a Formal Model of Safe and Scalable Self-driving Cars. arXiv:1708.06374, 2017