

Automated Reasoning and Artificial Intelligence

Josef Urban

Czech Institute for Informatics, Robotics and Cybernetics
Czech Technical University in Prague

ERC Consolidator grant

AI4REASON



European Research Council
Established by the European Commission

Not So Distant Future

I suspect that the following problem A in computational geometry is in P ..., what do you think?



Not So Distant Future



Cluster of 10k CPUs is searching and reasoning over a knowledge base of 1M definitions, 20M theorems and proofs and 100B lemmas...

Not So Distant Future



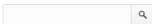
Indeed, it is similar to a less known problem B number 13501 in my knowledge base. We can use a similar polynomial reduction to planar graphs as in B, and for the resulting constraint-solving problem we use a modified version Y of the $O(n^9)$ algorithm X published last year in Proc. of Indian Conf. on Graph Theory.

Not So Distant Future



Here is my verified formal proof with 100k basic inference steps. Here are two high-level versions of the proof, one for experts and one for textbooks.

Today: Computers Checking Large Math Proofs



Scientists Deliver Formal Proof of Famous Kepler Conjecture

Jun 16, 2017 by News Staff / Source

◀ Previous | Next ▶

Published in
Mathematics

Tagged as
Johannes Kepler
Kepler conjecture

**Follow
You Might Like**



Researchers Develop First-Ever 3D Numerical Model of Melting Snowflake



Researchers Develop Mathematical Model for How Innovations

An international team of mathematicians led by University of Pittsburgh Professor **Thomas Hales** has delivered a formal proof of the **Kepler conjecture**, a famous problem in discrete geometry. The team's paper is published in the journal *Forum of Mathematics, Pi*.



LATEST NEWS



SPHERE Captures Young Exoplanet Beta Pictoris b Orbiting around Its Star

Nov 13, 2018 | [Astronomy](#)



Mirace eatoni: Newly-Discovered Cretaceous Bird Lived Among Dinosaurs, Was Strong Flier

Nov 13, 2018 | [Paleontology](#)



Juno Takes Closer Look at Jupiter's Magnificent, Swirling Clouds

Nov 13, 2018 | [Space Exploration](#)



Physicists Solve Structure of Unusually Complex Form of Nitrogen

Nov 13, 2018 | [Physical Chemistry](#)



Natural Compound Protects Hypertensive Rats against Heart Disease

Nov 13, 2018 | [Medicine](#)



Inventive Orangutans Make Hook Tools to Retrieve Food

Nov 12, 2018 | [Biology](#)



Researchers Find 40,000-Year-Old Figurative Paintings in Bornean Cave

Nov 12, 2018 | [Archaeology](#)



Hubble Sees Lensing Galaxy Cluster,

cdn.sci-news.com/images/enlarge3/image_4960e-Kepler-Conjecture.jpg

Kepler conjecture, Automated Reasoning and AI

- **J. Kepler** (1611, Prague): The most compact way of stacking balls of the same size in space is a pyramid.

$$V = \frac{\pi}{\sqrt{18}} \approx 74\%$$



- Big proof: 300 pages + computations (**Hales, Ferguson**, 1998)
- Formal proof finished in 2014, 20000 theorems & proofs
- All of it **computer-understandable and verified**
- polyhedron s /\ c face_of s ==> polyhedron c
- My work:
 - **Learn/reason automatically** over the large corpus of proofs
 - Our methods can **fully automate 40%** of the proofs (2014)

THE DAILY NEWSLETTER

Sign up to our daily email newsletter

NewScientist

SUBSCRIBE AND SAVE 64%

News Technology Space Physics Health Environment Mind Video | Travel Live Jobs

Sign In Search

Home | News | Technology

TECHNOLOGY NEWS 16 September 2015

Unhackable kernel could keep all computers safe from cyberattack

From helicopters to medical devices and power stations, [mathematical proof](#) that software at the heart of an operating system is secure could keep hackers out



Unhackable kernel could keep all computers safe from cyberattack

POPULAR

We thought the Incas couldn't write. These knots change everything

End of days: Is Western civilisation on the brink of collapse?

The origins of sexism: How men came to rule 12,000 years ago

The brain's 7D sandcastles could be

Is quantum physics behind your brain's ability to think?

Today's Applications

The screenshot shows a web browser window with the URL <https://www.prover.com/references/>. The Prover logo is in the top left, and navigation links for Solutions, References, Expertise, News, Company, and SDA Forum are in the top right. A dark blue menu bar contains location filters: ALL, BELGIUM, CANADA, CHINA, ENGLAND, NEW YORK, NORWAY, PARIS, and STOCKHOLM. The main content area features three columns, each with an image and a text block.

Implementing Prover Trident for SL, Stockholm

In this project, Prover Technology provides the Prover Trident solution to Ansaldo STS, for development and safety approval of interlocking software for Roslagsbanan, a mainline railway line that connects...

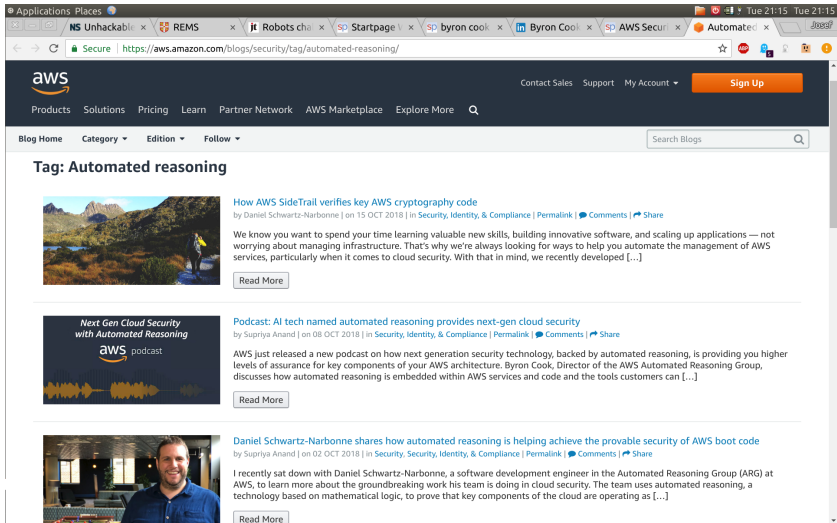
Formal Verification of SSI Software for NYCT, New York

New York City Transit (NYCT) is modernizing the signaling system in its subway by installing CBTC and replacing relay-based interlockings with computerized, solid state interlockings (SSIs).

Our Formal Verification Solution for RATP, Paris

In this project Prover Technology collaborated with RATP in creating a formal verification solution to meet RATP demand for safety verification of interlocking software. RATP had selected a computerized...

Today's Applications



The screenshot shows a web browser window with multiple tabs open. The active tab is the AWS blog page for the tag 'Automated reasoning'. The page header includes the AWS logo, navigation links for Products, Solutions, Pricing, Learn, Partner Network, AWS Marketplace, and Explore More, along with a search icon. A 'Sign Up' button is visible in the top right. Below the header, there are navigation links for 'Blog Home', 'Category', 'Edition', and 'Follow', and a search bar for 'Search Blogs'. The main content area is titled 'Tag: Automated reasoning' and features three article cards. Each card includes a thumbnail image, a title, a byline, a date, and a 'Read More' button.


aws

Contact Sales Support My Account [Sign Up](#)

Products Solutions Pricing Learn Partner Network AWS Marketplace Explore More

Blog Home Category Edition Follow Search Blogs

Tag: Automated reasoning




How AWS SideTrail verifies key AWS cryptography code

by Daniel Schwartz-Narbonne | on 15 OCT 2018 | in Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

We know you want to spend your time learning valuable new skills, building innovative software, and scaling up applications — not worrying about managing infrastructure. That's why we're always looking for ways to help you automate the management of AWS services, particularly when it comes to cloud security. With that in mind, we recently developed [...]

[Read More](#)




Podcast: AI tech named automated reasoning provides next-gen cloud security

by Supriya Anand | on 08 OCT 2018 | in Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

AWS just released a new podcast on how next generation security technology, backed by automated reasoning, is providing you higher levels of assurance for key components of your AWS architecture. Byron Cook, Director of the AWS Automated Reasoning Group, discusses how automated reasoning is embedded within AWS services and code and the tools customers can [...]

[Read More](#)



Daniel Schwartz-Narbonne shares how automated reasoning is helping achieve the provable security of AWS boot code

by Supriya Anand | on 02 OCT 2018 | in Security, Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

I recently sat down with Daniel Schwartz-Narbonne, a software development engineer in the Automated Reasoning Group (ARG) at AWS, to learn more about the groundbreaking work his team is doing in cloud security. The team uses automated reasoning, a technology based on mathematical logic, to prove that key components of the cloud are operating as [...]

[Read More](#)

Today's Applications

Applications Places

Secure | <https://www.absint.com/compcert/>

Absint Products Support News About us Contact Search

CompCert How it works New in 18.10 Try now

Formally verified compilation

CompCert is a formally verified optimizing C compiler. Its intended use is compiling safety-critical and mission-critical software written in C and meeting high levels of assurance. It accepts most of the ISO C 99 language, with some exceptions and a few extensions. It produces machine code for ARM, PowerPC, x86, and RISC-V architectures.

What sets CompCert apart?

CompCert is the only production compiler that is formally verified, using machine-assisted mathematical proofs, to be exempt from miscompilation issues. The code it produces is proved to behave exactly as specified by the semantics of the source C program.

This level of confidence in the correctness of the compilation process is unprecedented and contributes to meeting the highest levels of software assurance.

The formal proof covers [all transformations](#) from the abstract syntax tree to the generated assembly code. To preprocess and

serveimage.jpeg

Show all

Today's Applications

Overview About Research Education Industry People Projects Events Publications Institutions Jobs Visitors Student Positions Login



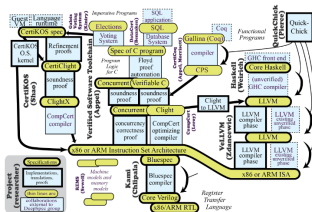
the science of deep specification

DeepSpec is an [Expedition in Computing](#) funded by the [National Science Foundation](#).

We focus on the **specification and verification of full functional correctness of software and hardware**.

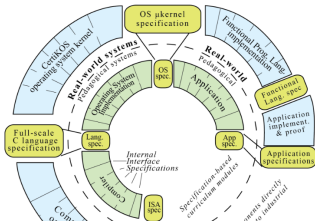
Research

We have several major research projects, and our ambitious goal is to connect them at specification interfaces to prove end-to-end correctness of whole systems.



Education

To deliver secure and reliable products, the software industry of the future needs engineers trained in specification and verification. We'll produce that curriculum.



Today's Applications

PHYS ORG Nanotechnology ▾ Physics ▾ Earth ▾ Astronomy & Space ▾ Technology ▾ Chemistry ▾ Biology ▾ Other Sciences ▾


f t r e m

search

Home » Other Sciences » Mathematics » October 12, 2012

Six-year journey leads to proof of Feit-Thompson Theorem

October 12, 2012 by Rob Kries, Microsoft








Georges Gonthier.

At 5:46 p.m. on Sept. 20, Georges Gonthier, principal researcher at Microsoft Research Cambridge, sent a brief email to his colleagues at the Microsoft Research-Inria Joint Centre in Paris. It read, in full: "This is really the End."

These five innocuous words heralded the culmination of a project that had consumed more than six years and resulted in the formal proof of the Feit-Thompson Theorem, the first major step of the classification of finite simple groups.

The theorem, first proved by Walter Feit and John Griggs Thompson in 1963 and also known as the Odd-Order Theorem, states that in mathematical group theory, every finite group of odd order is solvable.

Featured Last comments Popular

-  Gaia spots a 'ghost' galaxy next door @ 19 hours ago 81
-  How plants evolved to make ants their servants @ Nov 12, 2018 21
-  Physicists build fractal shape out of electrons @ Nov 12, 2018 0
-  Dark matter 'hurricane' offers chance to detect axions @ 18 hours ago 36
-  How to drive a robot on Mars @ Nov 12, 2018 2

Future Potential - Science

- Use strong AI/reasoning and formal verification for:
- **Science**
 - Routinely verify complex math, software, hardware?
 - Make all of math/science computer-understandable?
 - Strong AI assistants for math/science?
- **Examples**
 - Automatically understand/verify/explain all arXiv papers?
 - Can we train a superhuman system like AlphaGo/Zero for math/physics? What will it take?
 - Can we prove that the Amazon Cloud cannot be hacked?
 - The same for critical government/private IT systems?

Future Potential - Society

- Use strong AI/reasoning and formal verification for:
- **Society**
 - Leibniz's dream: **Let us Calculate!** (solve any dispute)
 - J. McCarthy: **Mathem. Objectivity and the Power of Initiative**
 - AI/reasoning assistants for law/regulations
 - Verification of financial, transport/traffic systems, ...
 - **Explainable** and very securely **verified** systems
- **Examples**
 - Prove that two Paris metro trains will never crash?
 - Prove that a trading system doesn't violate regulations?
 - Prove that a new law is inconsistent with an old one?
 - Automatically debunk fallacies in political campaigns?

Possible Pitfalls and Avoiding Them

Keep informed, don't fall for the hype

- AI is much more than just (deep) learning/neural nets
- E.g., SAT/SMT/model-checking may be one of the biggest recent AI successes – Amazon, Facebook, Microsoft, etc.
- Don't expect miracles/singularity due to the current hype
- We can train image recognition & language models, but ...
- .. don't know what it takes to solve hard science problems
- However, some breakthroughs can happen quickly
- Researchers/society/lawmakers need to talk more/faster
- AI infrastructure for EU (CLAIRE) could serve this purpose

Possible Pitfalls and Avoiding Them

Don't let US, China, ...

- ... take away the best EU science minds
- In reasoning and formal methods EU is the leader!
- Make a deal with big AI companies to seriously support **open university-based research**
- Example: **PRAIRIE** institute in Paris,
- ... **CLAIRE** centers modelled after that?
- Infrastructure like CLAIRE very needed in countries like CR
- Larger **brain-drain** and local incompetence aggravating it
- Use such infrastructure to **impose EU values on AI**

Links and Impacts on Other AI Areas

- Main areas: Machine Learning, Automated Reasoning
- Needs advances in Representation Learning
- AI needs **intuition**, but also **reasoning and explanations**
- Impact on Formal Verification (SW, HW, etc.)
- Potentially on any (hard) science/thinking/arguing
- **Alan Turing**, 1950, AI:

“We may hope that machines will eventually compete with men in all purely intellectual fields.”

Outlook – Scientific Revolution, AI?

- What did Kepler, Galileo & Co start to do in 1600s?
- What are we trying to do today?
- Kepler's Conjecture in Strena in 1611 (with many others)
- Kepler's laws, Newton, ..., age of science, math, machines
- ..., Hilbert, ..., Turing, ... age of computing machines?
- 1998 machine **helps to find** a proof of Kepler's Conjecture
- 2014 machine **verifies** a proof of Kepler's Conjecture
- ... 2050? machine **finds** a proof of Kepler's Conjecture?