Machine Learning and Automated Reasoning - Introduction

Josef Urban

Czech Technical University in Prague

March 8, 2019

European Research Council
Established by the European Commission

Course Overview

- Connections between two AI fields: Machine Learning (ML) and Automated Reasoning (AR)
- ML: apply various forms of *inductive reasoning* to large datasets to obtain the most plausible explanations, models and conjectures
- AR: apply various forms of *deductive reasoning* to prove that particular explanations and conjectures are correct.
- Humans combine induction and deduction - let's teach computers too!
- We will mostly explore ML/AR combinations in a *formal proof* setting
- *Typical problem:* How can learning help with logical reasoning?

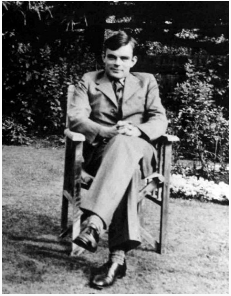
Course Overview - Particular settings and topics

- ML and first-order logic (FOL), saturation-style theorem provers (ATPs)
- Higher-order logic (HOL), Set theory, formal proof assistants (ITPs)
- ML and reasoning in large theories, hammers for ITP, premise selection
- Symbolic vs statistical learning for theorem proving
- ML in tableau-style and tactical reasoning systems
- Learning in propositional logic (SAT), QBF, SMT, instantiation-based methods and model finding.
- Representations and conjecturing - how do we characterize reasoning data for learning?
- Feedback loops for proving and learning, reinforcement learning of ATP, positive/negative proof mining
- Alignment and translation between informal and formal corpora, automated formalization
- Exam: do a small project in combining ML and AR

Induction/Learning vs Reasoning – Henri Poincaré

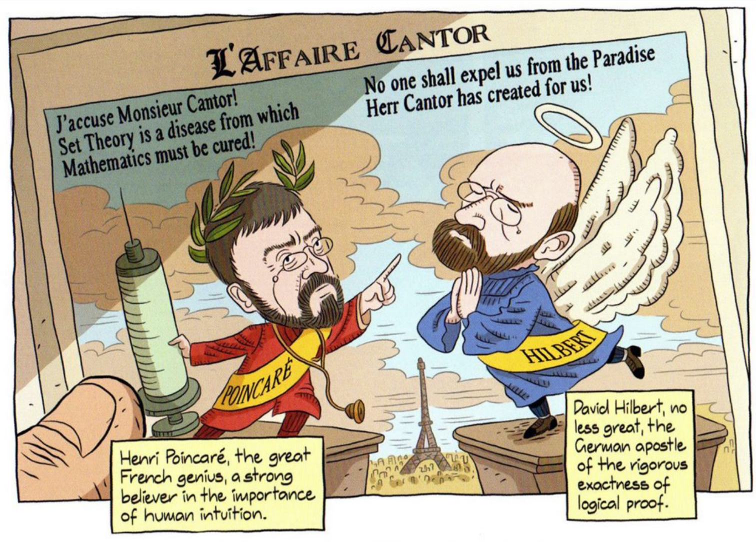
- Science and Method: Ideas about the interplay between correct deduction and induction/intuition
- *"And in demonstration itself logic is not all. The true mathematical reasoning is a real induction [...]"*
- I believe he was right: strong general reasoning engines have to combine deduction and induction (learning patterns from data, making conjectures, etc.)

Learning vs Reasoning – Alan Turing 1950 – AI



- 1950: *Computing machinery and intelligence* – AI, Turing test
- *"We may hope that machines will eventually compete with men in all purely intellectual fields."* (regardless of his 1936 undecidability result!)
- last section on Learning Machines(!):
- *"But which are the best ones [fields] to start [learning on] with?"*
- *"... Even this is a difficult decision. Many people think that a very abstract activity, like the playing of chess, would be best."*
- Why not try with large computer-understandable math corpora?

Intuition vs Formal Reasoning – Poincaré vs Hilbert



[Adapted from: *Logicomix: An Epic Search for Truth* by A. Doxiadis]

What is Formal Mathematics?

- Developed thanks to the Leibniz/Russell/Frege/Hilbert/... program
- Mathematics put on formal logic foundations (*symbolic computation*)
- ... which btw. led also to the rise of computers (Turing/Church, 1930s)
- Formal math (1950/60s): combine formal foundations and the newly available computers
- Conceptually very simple:
- Write all your axioms and theorems so that computer understands them
- Write all your inference rules so that computer understands them
- Use the computer to check that your proofs follow the rules
- But in practice, it turns out not to be so simple
- Many approaches, still not mainstream, but big breakthroughs recently

Irrationality of $\sqrt{2}$ (informal text)

tiny proof from Hardy & Wright:

Theorem 43 (Pythagoras' theorem). $\sqrt{2}$ is irrational.
The traditional proof ascribed to Pythagoras runs as follows. If $\sqrt{2}$ is rational, then the equation

$$a^2 = 2b^2 \tag{4.3.1}$$

is soluble in integers a, b with $(a, b) = 1$. Hence a^2 is even, and therefore a is even. If $a = 2c$, then $4c^2 = 2b^2$, $2c^2 = b^2$, and b is also even, contrary to the hypothesis that $(a, b) = 1$. $\square$

Irrationality of $\sqrt{2}$ (Formal Proof Sketch)

exactly the same text in Mizar syntax:

```
theorem Th43: :: Pythagoras' theorem
  sqrt 2 is irrational
proof
  assume sqrt 2 is rational;
  consider a,b such that
4_3_1: a^2 = 2*b^2 and
    a,b are relative prime;
  a^2 is even;
  a is even;
  consider c such that a = 2*c;
  4*c^2 = 2*b^2;
  2*c^2 = b^2;
  b is even;
  thus contradiction;
end;
```

Irrationality of $\sqrt{2}$ in HOL Light

```
let SQRT_2_IRRATIONAL = prove
 (`~rational(sqrt(&2))`,
  SIMP_TAC[rational; real_abs; SQRT_POS_LE; REAL_POS] THEN
  REWRITE_TAC[NOT_EXISTS_THM] THEN REPEAT GEN_TAC THEN
  DISCH_THEN(CONJUNCTS_THEN2 ASSUME_TAC MP_TAC) THEN
  SUBGOAL_THEN `~((&p / &q) pow 2 = sqrt(&2) pow 2)`
    (fun th -> MESON_TAC[th]) THEN
  SIMP_TAC[SQRT_POW_2; REAL_POS; REAL_POW_DIV] THEN
  ASM_SIMP_TAC[REAL_EQ_LDIV_EQ; REAL_OF_NUM_LT; REAL_POW_LT;
               ARITH_RULE `0 < q <=> ~(q = 0)`] THEN
  ASM_MESON_TAC[NSQRT_2; REAL_OF_NUM_POW; REAL_OF_NUM_MUL; REAL_OF_NUM_EQ]);;
```

Irrationality of $\sqrt{2}$ in Isabelle/HOL

```
theorem sqrt2_not_rational:
  "sqrt (real 2) ∉ ℚ"
proof
  assume "sqrt (real 2) ∈ ℚ"
  then obtain m n :: nat where
    n_nonzero: "n ≠ 0" and sqrt_rat: "¦sqrt (real 2)¦ = real m / real n"
    and lowest_terms: "gcd m n = 1" ..
  from n_nonzero and sqrt_rat have "real m = ¦sqrt (real 2)¦ * real n" by simp
  then have "real (m²) = (sqrt (real 2))² * real (n²)"
    by (auto simp add: power2_eq_square)
  also have "(sqrt (real 2))² = real 2" by simp
  also have "... * real (m²) = real (2 * n²)" by simp
  finally have eq: "m² = 2 * n²" ..
  hence "2 dvd m²" ..
  with two_is_prime have dvd_m: "2 dvd m" by (rule prime_dvd_power_two)
  then obtain k where "m = 2 * k" ..
  with eq have "2 * n² = 2² * k²" by (auto simp add: power2_eq_square mult_ac)
  hence "n² = 2 * k²" by simp
  hence "2 dvd n²" ..
  with two_is_prime have "2 dvd n" by (rule prime_dvd_power_two)
  with dvd_m have "2 dvd gcd m n" by (rule gcd_greatest)
  with lowest_terms have "2 dvd 1" by simp
  thus False by arith
qed
```

Irrationality of $\sqrt{2}$ in Coq

```
Theorem irrational_sqrt_2: irrational (sqrt 2%nat).
intros p q H H0; case H.
apply (main_thm (Zabs_nat p)).
replace (Div2.double (q * q)) with (2 * (q * q));
 [idtac | unfold Div2.double; ring].
case (eq_nat_dec (Zabs_nat p * Zabs_nat p) (2 * (q * q))); auto; intros H1.
case (not_nm_INR _ _ H1); (repeat rewrite mult_INR).
rewrite <- (sqrt_def (INR 2)); auto with real.
rewrite H0; auto with real.
assert (q <> 0%R :> R); auto with real.
field; auto with real; case p; simpl; intros; ring.
Qed.
```

Irrationality of $\sqrt{2}$ in Metamath

```
${
    $d x y $.
    $( The square root of 2 is irrational. $)
    sqr2irr $p |- ( sqr ` 2 ) e/ QQ $=
      ( vx vy c2 csqr cfv cq wnel wcel wn cv cdiv co wceq cn wrex cz cexp
      cmulc sqr2irrlem3 sqr2irrlem5 bi2rexa mtbir cc0 clt wbr wa wi wb nngt0t
      adantr cr ax0re ltmuldivt mp3an1 nnret zret syl2an mpd ancoms 2re 2pos
      sqrgt0i breq2 mpbii syl5bir cc nncnt mulzer2t syl breq1d adantl sylibd
      exp r19.23adv anc2li elnnz syl6ibr impac r19.22i2 mto elq df-nel mpbir )
      CDEZFGWDFHZIWEWDAJZBJZKLZMZBNOZAPOZWKWJANOZWLWFCQLCWGCQLRLMZBNOANOABSWIWM
      ABNNWFWGTUAUBWJWJAPNWFPHZWJWFNHZWNWJWNUCWFUDUEZUFWOWNWJWPWNWIWPBNWNWGNHZW
      IWPUGWNWQUFZWIUCWGRLZWFUDUEZWPWRWTUCWHUDUEZWIWQWNWTXAUHZWQWNUFUCWGUDUEZXB
      WQXCWNWGUIUJWGUKHZWFUKHZXCXBUGZWQWNUCUKHXDXEXFULUCWGWFUMUNWGUOWFUPUQURUSW
      IUCWDUDUEXACUTVAVBWDWHUCUDVCVDVEWQWTWPUHWNWQWSUCWFUDWQWGVFHWSUCMWGVGWGVHV
      IVJVKVLVMVNVOWFVPVQVRVSVTABWDWAUBWDFWBWC $.
      $( [8-Jan-02] $)
  $}
```

Irrationality of $\sqrt{2}$ in Metamath Proof Explorer

sqr2irr - Metamath Proof Explorer - Chromium

sqr2irr - Metamat ×

us.metamath.org/mpegif/sqr2irr.html

Proof of Theorem sqr2irr

Step	Hyp	Ref	Expression
1		sqr2irrlem3 10838	....5 $\vdash \neg \exists x \in \mathbb{N} \exists y \in \mathbb{N} (x \uparrow 2) = (2 \cdot (y \uparrow 2))$
2		sqr2irrlem5 10840	.....6 $\vdash ((x \in \mathbb{N} \land y \in \mathbb{N}) \to ((\surd`2) = (x / y) \leftrightarrow (x \uparrow 2) = (2 \cdot (y \uparrow 2))))$
3	2	2rexbiia 2329	....5 $\vdash (\exists x \in \mathbb{N} \exists y \in \mathbb{N} (\surd`2) = (x / y) \leftrightarrow \exists x \in \mathbb{N} \exists y \in \mathbb{N} (x \uparrow 2) = (2 \cdot (y \uparrow 2)))$
4	1, 3	mtbir 288	...4 $\vdash \neg \exists x \in \mathbb{N} \exists y \in \mathbb{N} (\surd`2) = (x / y)$
5		2re 8838	...........12 $\vdash 2 \in \mathbb{R}$
6		2pos 8849	...........12 $\vdash 0 < 2$
7	5, 6	sqrgt0ii 10213	..........11 $\vdash 0 < (\surd`2)$
8		breq2 3595	..........11 $\vdash ((\surd`2) = (x / y) \to (0 < (\surd`2) \leftrightarrow 0 < (x / y)))$
9	7, 8	mpbii 200	.........10 $\vdash ((\surd`2) = (x / y) \to 0 < (x / y))$
10		zre 9029	...........12 $\vdash (x \in \mathbb{Z} \to x \in \mathbb{R})$
11	10	adantr 444	..........11 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to x \in \mathbb{R})$
12		nnre 8788	...........12 $\vdash (y \in \mathbb{N} \to y \in \mathbb{R})$
13	12	adantl 445	..........11 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to y \in \mathbb{R})$
14		nngt0 8807	...........12 $\vdash (y \in \mathbb{N} \to 0 < y)$
15	14	adantl 445	..........11 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to 0 < y)$
16		gt0div 8683	..........11 $\vdash ((x \in \mathbb{R} \land y \in \mathbb{R} \land 0 < y) \to (0 < x \leftrightarrow 0 < (x / y)))$
17	11, 13, 15, 16	syl3anc 1145	.........10 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to (0 < x \leftrightarrow 0 < (x / y)))$
18	9, 17	syl5ibr 210	........9 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to ((\surd`2) = (x / y) \to 0 < x))$
19		simpl 436	........9 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to x \in \mathbb{Z})$
20	18, 19	jctild 522	.......8 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to ((\surd`2) = (x / y) \to (x \in \mathbb{Z} \land 0 < x)))$
21		elnnz 9035	.......8 $\vdash (x \in \mathbb{N} \leftrightarrow (x \in \mathbb{Z} \land 0 < x))$
22	20, 21	syl6ibr 216	......7 $\vdash ((x \in \mathbb{Z} \land y \in \mathbb{N}) \to ((\surd`2) = (x / y) \to x \in \mathbb{N}))$
23	22	rexlimdva 2414	.....6 $\vdash (x \in \mathbb{Z} \to (\exists y \in \mathbb{N} (\surd`2) = (x / y) \to x \in \mathbb{N}))$
24	23	impac 598	....5 $\vdash ((x \in \mathbb{Z} \land \exists y \in \mathbb{N} (\surd`2) = (x / y)) \to (x \in \mathbb{N} \land \exists y \in \mathbb{N} (\surd`2) = (x / y)))$
25	24	reximi2 2396	...4 $\vdash (\exists x \in \mathbb{Z} \exists y \in \mathbb{N} (\surd`2) = (x / y) \to \exists x \in \mathbb{N} \exists y \in \mathbb{N} (\surd`2) = (x / y))$
26	4, 25	mto 165	..3 $\vdash \neg \exists x \in \mathbb{Z} \exists y \in \mathbb{N} (\surd`2) = (x / y)$
27		elq 9308	..3 $\vdash ((\surd`2) \in \mathbb{Q} \leftrightarrow \exists x \in \mathbb{Z} \exists y \in \mathbb{N} (\surd`2) = (x / y))$
28	26, 27	mtbir 288	.2 $\vdash \neg (\surd`2) \in \mathbb{Q}$
29		df-nel 2210	.2 $\vdash ((\surd`2) \notin \mathbb{Q} \leftrightarrow \neg (\surd`2) \in \mathbb{Q})$
30	28, 29	mpbir 198	1 $\vdash (\surd`2) \notin \mathbb{Q}$

Colors of variables: wff set class

Today: Computers Checking Large Math Proofs

SCI NEWS

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

HOME ASTRONOMY SPACE EXPLORATION ARCHAEOLOGY PALEONTOLOGY BIOLOGY PHYSICS MEDICINE GENETICS GEOLOGY MORE

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 Emerge

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

Mirarce 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

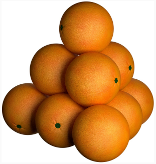
Hubble Sees Lensing Galaxy Cluster,

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

Big Example: The Flyspeck project

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

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



- Formal proof finished in 2014
- 20000 lemmas in geometry, analysis, graph theory
- All of it at `https://code.google.com/p/flyspeck/`
- All of it computer-understandable and verified in HOL Light:
- `polyhedron s /\ c face_of s ==> polyhedron c`
- However, this took 20 – 30 person-years!

What Has Been Formalized?

top 100 of interesting theorems/proofs
(Paul & Jack Abad, 1999, tracked by Freek Wiedijk)

1. $\sqrt{2} \notin \mathbb{Q}$
2. fundamental theorem of algebra
3. $|\mathbb{Q}| = \aleph_0$
4. 

$\Rightarrow a^2 + b^2 = c^2$
5. $\pi(x) \sim \frac{x}{\ln x}$
6. Gödel's incompleteness theorem
7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
8. impossibility of trisecting the angle and doubling the cube

$\vdots$

32. four color theorem
33. Fermat's last theorem

$\vdots$

99. Buffon needle problem
100. Descartes rule of signs

What Has Been Formalized?

top 100 of interesting theorems/proofs
(Paul & Jack Abad, 1999, tracked by Freek Wiedijk)

1. $\sqrt{2} \notin \mathbb{Q}$
2. fundamental theorem of algebra
3. $|\mathbb{Q}| = \aleph_0$
4. 

$\Rightarrow a^2 + b^2 = c^2$
5. $\pi(x) \sim \frac{x}{\ln x}$
6. Gödel's incompleteness theorem
7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
8. impossibility of trisecting the angle and doubling the cube

$\vdots$

32. four color theorem
33. Fermat's last theorem

$\vdots$

99. Buffon needle problem
100. Descartes rule of signs

all together	88%
HOL Light	86%
Mizar	57%
Isabelle	52%
Coq	49%
ProofPower	42%
Metamath	24%
ACL2	18%
PVS	16%

What Has Been Formalized?

top 100 of interesting theorems/proofs
(Paul & Jack Abad, 1999, tracked by Freek Wiedijk)

1. $\sqrt{2} \notin \mathbb{Q}$
2. fundamental theorem of algebra
3. $|\mathbb{Q}| = \aleph_0$
4. 

$\Rightarrow a^2 + b^2 = c^2$
5. $\pi(x) \sim \frac{x}{\ln x}$
6. Gödel's incompleteness theorem
7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
8. impossibility of trisecting the angle and doubling the cube

$\vdots$

32. four color theorem
33. Fermat's last theorem

$\vdots$

99. Buffon needle problem
100. Descartes rule of signs

all together	88%
HOL Light	86%
Mizar	57%
Isabelle	52%
Coq	49%
ProofPower	42%
Metamath	24%
ACL2	18%
PVS	16%

What Has Been Formalized?

top 100 of interesting theorems/proofs
(Paul & Jack Abad, 1999, tracked by Freek Wiedijk)

1. $\sqrt{2} \notin \mathbb{Q}$
2. fundamental theorem of algebra
3. $|\mathbb{Q}| = \aleph_0$
4. 

$\Rightarrow a^2 + b^2 = c^2$
5. $\pi(x) \sim \frac{x}{\ln x}$
6. Gödel's incompleteness theorem
7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
8. impossibility of trisecting the angle and doubling the cube

$\vdots$

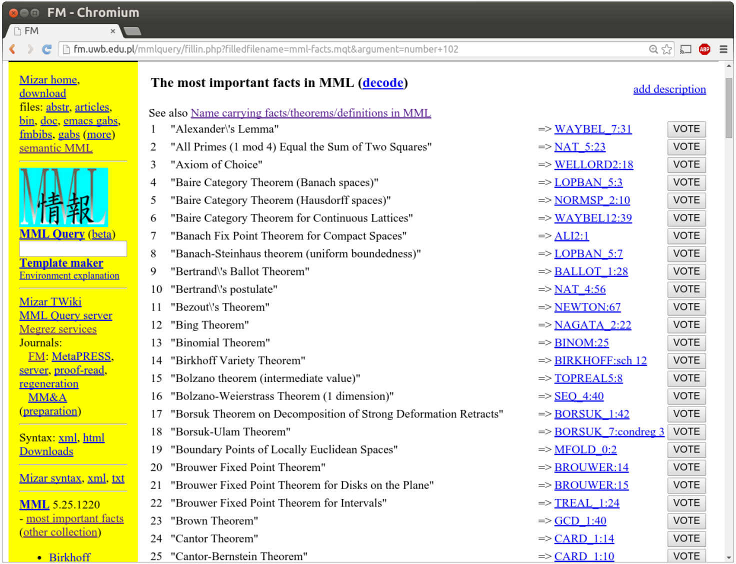
32. four color theorem
33. Fermat's last theorem

$\vdots$

99. Buffon needle problem
100. Descartes rule of signs

all together	88%
HOL Light	86%
Mizar	57%
Isabelle	52%
Coq	49%
ProofPower	42%
Metamath	24%
ACL2	18%
PVS	16%

Named Theorems in the Mizar Library



Big Formalizations

- Kepler Conjecture (Hales et all, 2014, HOL Light, Isabelle)
- Feit-Thompson (odd-order) theorem
  - Two graduate books
  - Gonthier et all, 2012, Coq
- Compendium of Continuous Lattices (CCL)
  - 60% of the book formalized in Mizar
  - Bancerek, Trybulec et all, 2003
- The Four Color Theorem (Gonthier and Werner, 2005, Coq)

Mid-size Formalizations

- Gödel's First Incompleteness Theorem — Natarajan Shankar (NQTHM), Russell O'Connor (Coq)
- Brouwer Fixed Point Theorem — Karol Pak (Mizar), John Harrison (HOL Light)
- Jordan Curve Theorem — Tom Hales (HOL Light), Artur Kornilowicz et al. (Mizar)
- Prime Number Theorem — Jeremy Avigad et al (Isabelle/HOL), John Harrison (HOL Light)
- Gödel's Second incompleteness Theorem — Larry Paulson (Isabelle/HOL)
- Central Limit Theorem – Jeremy Avigad (Isabelle/HOL)

Large Software Verifications

- seL4 – operating system microkernel
  - Gerwin Klein and his group at NICTA, Isabelle/HOL
- CompCert – a formally verified C compiler
  - Xavier Leroy and his group at INRIA, Coq
- EURO-MILS – verified virtualization platform
  - ongoing 6M EUR FP7 project, Isabelle
- CakeML – verified implementation of ML
  - Magnus Myreen, HOL4

Central Limit Theorem in Isabelle/HOL

The Top 100 Theorems in Isabelle - Chromium

The Top 100 Thec ×

www.cse.unsw.edu.au/~kleing/top100/#47

```
theorem (in prob_space) central_limit_theorem:
  fixes
    X :: "nat ⇒ 'a ⇒ real" and
    μ :: "real measure" and
    σ :: real and
    S :: "nat ⇒ 'a ⇒ real"
  assumes
    X_indep: "indep_vars (λi. borel) X UNIV" and
    X_integrable: "⋀n. integrable M (X n)" and
    X_mean_0: "⋀n. expectation (X n) = 0" and
    σ_pos: "σ > 0" and
    X_square_integrable: "⋀n. integrable M (λx. (X n x)²)" and
    X_variance: "⋀n. variance (X n) = σ²" and
    X_distrib: "⋀n. distr M borel (X n) = μ"
  defines
    "S n ≡ λx. ∑i<n. X i x"
  shows
    "weak_conv_m (λn. distr M borel (λx. S n x / sqrt (n * σ²)))
        (density lborel std_normal_density)"
```

Sylow’s Theorems in Mizar

```
theorem :: GROUP_10:12
  for G being finite Group, p being prime (natural number)
  holds ex P being Subgroup of G st P is_Sylow_p-subgroup_of_prime p;

theorem :: GROUP_10:14
  for G being finite Group, p being prime (natural number) holds
    (for H being Subgroup of G st H is_p-group_of_prime p holds
      ex P being Subgroup of G st
      P is_Sylow_p-subgroup_of_prime p & H is Subgroup of P) &
    (for P1,P2 being Subgroup of G
      st P1 is_Sylow_p-subgroup_of_prime p & P2 is_Sylow_p-subgroup_of_prime p
      holds P1,P2 are_conjugated);

theorem :: GROUP_10:15
  for G being finite Group, p being prime (natural number) holds
    card the_sylow_p-subgroups_of_prime(p,G) mod p = 1 &
    card the_sylow_p-subgroups_of_prime(p,G) divides ord G;
```

Gödel Theorems in Isabelle

The Top 100 Theorems in Isabelle - Chromium

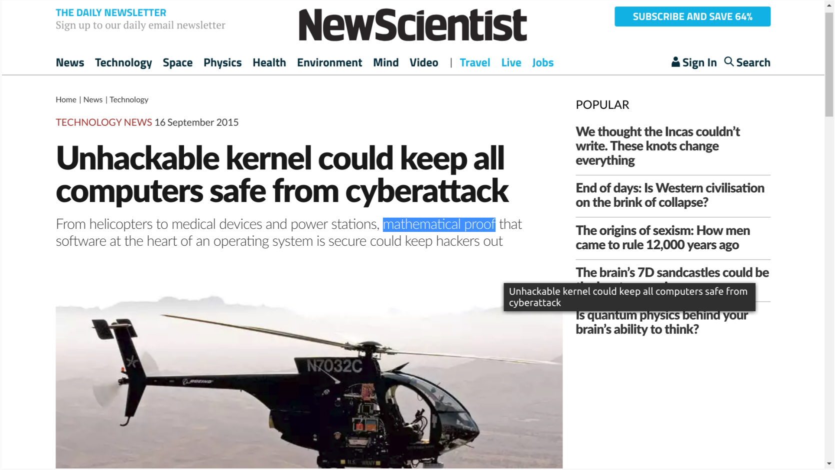
www.cse.unsw.edu.au/~kleing/top100/#6

```
theorem Goedel_I:
  assumes "¬ {} ⊢ Fls"
  obtains δ where
      "{} ⊢ δ IFF Neg (PfP ⌈δ⌉)"
      "¬ {} ⊢ δ"
      "¬ {} ⊢ Neg δ"
      "eval_fm e δ"
      "ground_fm δ"

theorem Goedel_II:
  assumes "¬ {} ⊢ Fls"
    shows "¬ {} ⊢ Neg (PfP ⌈Fls⌉)"
```

http://afp.sourceforge.net/entries/Incompleteness.shtml

Today's Applications



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

POPULAR

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

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

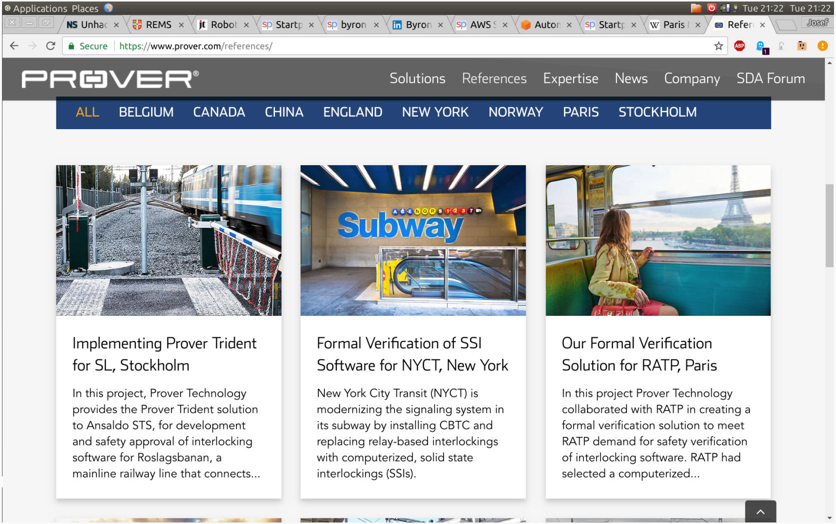
The origins of sexism: How men came to rule 12,000 years ago

The brain's 7D sandcastles could be

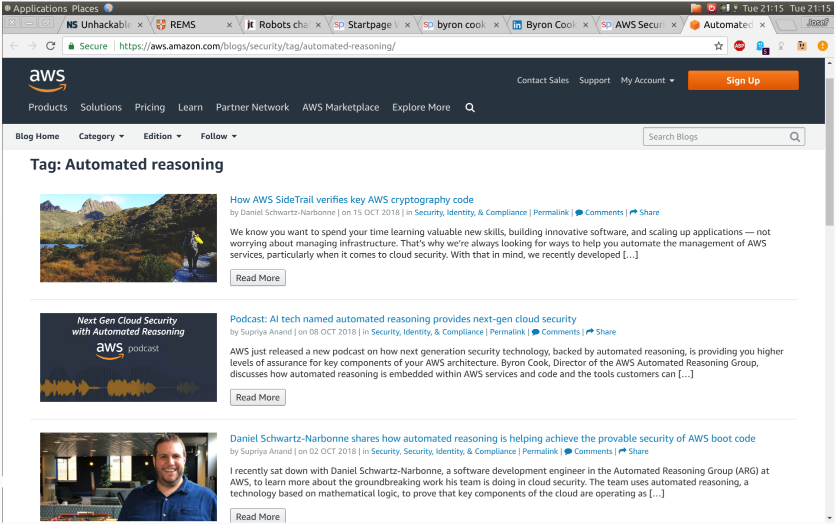
Unhackable kernel could keep all computers safe from cyberattack

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

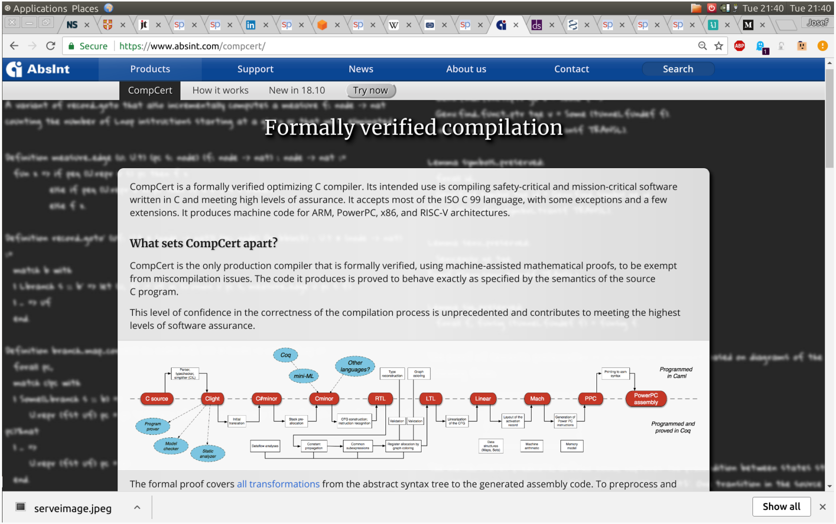
Today’s Applications



Today’s Applications



Today’s Applications



Today’s Applications

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

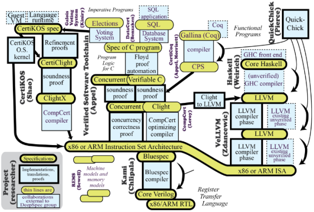
deep spec the science of deep specification

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.

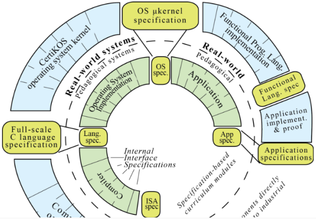
Research

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.

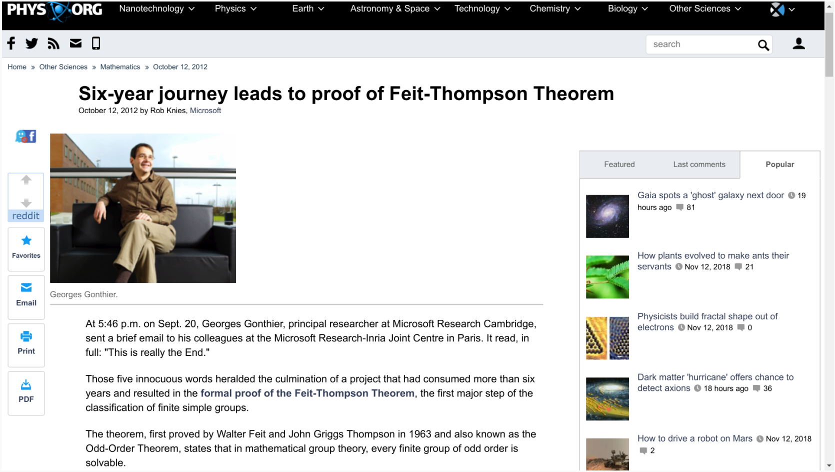


Education

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

search

Home » Other Sciences » Mathematics » October 12, 2012

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

October 12, 2012 by Rob Knies, Microsoft

reddit

Favorites

Email

Print

PDF

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."

Those 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

What Are Automated Theorem Provers?

- Computer programs that (try to) determine if
  - A conjecture C is a logical consequence of a set of axioms Ax
  - The derivation of conclusions that follow inevitably from facts.
- Systems: Vampire, E, SPASS, Prover9, Z3, CVC4, Satallax, iProver, ...
- Brute-force search calculi (resolution, superposition, tableaux, SMT, ...)
- Human-designed heuristics for pruning of the search space
- Fast combinatorial explosion on large knowledge bases like Flyspeck and Mizar
- Need to be equipped with good domain-specific inference guidance ...
- ... this what we will try to do here ...
- ... by learning from the knowledge bases and reasoning feedback ...
- Details on particular ATP systems and ML settings later

Mizar demo

```
http://grid01.ciirc.cvut.cz/~mptp/out4.ogv
```

Using Learning to Guide Theorem Proving

- **high-level**: pre-select lemmas from a large library, give them to ATPs
- **high-level**: pre-select a good ATP strategy/portfolio for a problem
- **high-level**: pre-select good *hints* for a problem, use them to guide ATPs
- **low-level**: guide every inference step of ATPs (tableau, superposition)
- **low-level**: guide every kernel step of LCF-style ITPs
- **mid-level**: guide application of tactics in ITPs
- **mid-level**: invent suitable ATP strategies for classes of problems
- **mid-level**: invent suitable conjectures for a problem
- **mid-level**: invent suitable concepts/models for problems/theories
- **proof sketches**: explore stronger/related theories to get proof ideas
- **theory exploration**: develop interesting theories by conjecturing/proving
- **feedback loops**: (dis)prove, learn from it, (dis)prove more, learn more, ...
- ...

Sample of Learning Approaches We Have Been Using

- **neural networks** (statistical ML) – backpropagation, deep learning, convolutional, recurrent, etc.
- **decision trees, random forests, gradient tree boosting** – find good classifying attributes (and/or their values); more explainable
- **support vector machines** – find a good classifying hyperplane, possibly after non-linear transformation of the data (*kernel methods*)
- **k-nearest neighbor** – find the *k* nearest neighbors to the query, combine their solutions
- **naive Bayes** – compute probabilities of outcomes assuming complete (naive) independence of characterizing features (just multiplying probabilities)
- **inductive logic programming** (symbolic ML) – generate logical explanation (program) from a set of ground clauses by generalization
- **genetic algorithms** – evolve large population by crossover and mutation
- combinations of statistical and symbolic approaches (probabilistic grammars, semantic features, ...)
- supervised, unsupervised, reinforcement learning (actions, explore/exploit, cumulative reward)

Learning – Features and Data Preprocessing

- Extremely important - if irrelevant, there is no use to learn the function from input to output ("garbage in garbage out")
- Feature discovery – a big field
- Deep Learning – design neural architectures that automatically find important high-level features for a task
- Latent Semantics, dimensionality reduction: use linear algebra (eigenvector decomposition) to discover the most similar features, make approximate equivalence classes from them
- word2vec and related methods: represent words/sentences by *embeddings* (in a high-dimensional real vector space) learned by predicting the next word on a large corpus like Wikipedia
- math and theorem proving: syntactic/semantic patterns/abstractions
- how do we represent math objects (formulas, proofs, ideas) in our mind?

Neural Autoformalization (Wang et al., 2018)

- generate about 1M Latex - Mizar pairs based on Bancerek's work
- train neural seq-to-seq translation models (Luong – NMT)
- evaluate on about 100k examples
- many architectures tested, some work much better than others
- very important latest invention: *attention* in the seq-to-seq models
- more data very important for neural training – our biggest bottleneck (you can help!)

Neural Autoformalization data

Rendered LaTeX	If $X \subseteq Y \subseteq Z$, then $X \subseteq Z$.
Mizar	`X c= Y & Y c= Z implies X c= Z;`
Tokenized Mizar	`X c= Y & Y c= Z implies X c= Z ;`
LaTeX	`If $X \subseteq Y \subseteq Z$, then $X \subseteq Z$.`
Tokenized LaTeX	`If $ X \subseteq Y \subseteq Z $ , then $ X \subseteq Z $ .`

Neural Autoformalization results

Parameter	Final Test Perplexity	Final Test BLEU	Identical Statements (%)	Identical No-overlap (%)
128 Units	3.06	41.1	40121 (38.12%)	6458 (13.43%)
256 Units	1.59	64.2	63433 (60.27%)	19685 (40.92%)
512 Units	1.6	**67.9**	66361 (63.05%)	21506 (44.71%)
1024 Units	**1.51**	61.6	**69179 (65.73%)**	**22978 (47.77%)**
2048 Units	2.02	60	59637 (56.66%)	16284 (33.85%)

Neural Fun – Performance after Some Training

Rendered LaTeX	Suppose s_8 is convergent and s_7 is convergent . Then $\lim(s_8+s_7) = \lim s_8 + \lim s_7$
Input LaTeX	`Suppose $ { s _ { 8 } } $ is convergent and $ { s _ { 7 } } $ is convergent . Then $ \mathop { \rm lim } ( { s _ { 8 } } { + } { s _ { 7 } } } ) \mathrel { = } \mathop { \rm lim } { s _ { 8 } } { + } \mathop { \rm lim } { s _ { 7 } } } $ .`
Correct	`seq1 is convergent & seq2 is convergent implies lim ( seq1 + seq2 ) = ( lim seq1 ) + ( lim seq2 ) ;`
Snapshot-1000	`x in dom f implies ( x * y ) * ( f | ( x | ( y | ( y | y ) ) ) ) = ( x | ( y | ( y | ( y | y ) ) ) ) ) ;`
Snapshot-2000	`seq is summable implies seq is summable ;`
Snapshot-3000	`seq is convergent & lim seq = 0c implies seq = seq ;`
Snapshot-4000	`seq is convergent & lim seq = lim seq implies seq1 + seq2 is convergent ;`
Snapshot-5000	`seq1 is convergent & lim seq2 = lim seq2 implies lim_inf seq1 = lim_inf seq2 ;`
Snapshot-6000	`seq is convergent & lim seq = lim seq implies seq1 + seq2 is convergent ;`
Snapshot-7000	`seq is convergent & seq9 is convergent implies lim ( seq + seq9 ) = ( lim seq ) + ( lim seq9 ) ;`