The AIM Conjecture

History and Current Progress

Michael Kinyon

Department of Mathematics

AITP16, Obergurgl, Austria, 1 April 2016

Dedication

William McCune (1953–2011)

- Developer of OTTER, PROVER9 and other tools.
- Best known (to mathematicians) for using automated deduction to solve the *Robbins problem* in Boolean algebra.

Who?

Collaborators include: P. Vojtěchovský, J.D. Phillips, A. Drápal, P. Csörgő, and especially

Bob Veroff

Philosophy

A work of [automated theorem proving] is good if it has arisen out of necessity. That is the only way one can judge it.

– Rainer Maria Rilke, Letters to a Young Poet, 1929

Philosophy

A work of [automated theorem proving] is good if it has arisen out of necessity. That is the only way one can judge it.

– Rainer Maria Rilke, Letters to a Young Poet, 1929

(Freely translated)

Apology

I would like to start by giving you a bit of history and mathematical background about the problem.

There are *very* few mathematicians here, so this is quite far from most of your interests. I ask for your patience for a few slides.

Combinatorial definition

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that for each $a, b \in Q$, the equations

$$ax = b \qquad \text{and} \qquad ya = b$$

have unique solutions $x, y \in Q$.

Combinatorial definition

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that for each $a, b \in Q$, the equations

$$ax = b \qquad \text{and} \qquad ya = b$$

have unique solutions $x, y \in Q$.

Multiplication tables of quasigroups $=$ Latin squares

Example:

1	3	2
3	2	1
2	1	3

Loops

A *loop* is a quasigroup with an identity element:

$$1 \cdot x = x \cdot 1 = x\,.$$

Loops

A *loop* is a quasigroup with an identity element:

$$1 \cdot x = x \cdot 1 = x\,.$$

The term “loop” is due to A. A. Albert (U. of Chicago)

Loops

A *loop* is a quasigroup with an identity element:

$$1 \cdot x = x \cdot 1 = x\,.$$

The term “loop” is due to A. A. Albert (U. of Chicago)

Loop has a specific meaning to those from Chicago. It is the name of the downtown region.

Loops

A *loop* is a quasigroup with an identity element:

$$1 \cdot x = x \cdot 1 = x\,.$$

The term “loop” is due to A. A. Albert (U. of Chicago)

Loop has a specific meaning to those from Chicago. It is the name of the downtown region.

Also, it rhymes with “group” and is easier to say than “quasigroup with identity element”.

Universal algebra definition

```
% loop axioms in Prover9 syntax
1 * x = x. x * 1 = x.
x \ (x * y) = y. x * (x \ y) = y.
(x * y) / y = x. (x / y) * y = x.
```

The universal algebra definition is better suited to automated theorem proving. (Use your own binary operations instead of ugly skolemization.)

Concepts

Most concepts from group theory (or better, universal algebra) transfer quite easily to loops:

- subloops
- normal subloops
- factor loops
- homomorphisms
- etc.

These terms mean what you think they should mean.

Multiplication Groups

In a loop (or quasigroup) Q, the *left* and *right translations*

$$L_x : Q \to Q; \quad yL_x = xy \qquad R_x : Q \to Q; \quad yR_x = yx\,.$$

are permutations of Q (by definition).

The *multiplication group* $\mathrm{Mlt}(Q)$ is the permutation group generated by the translations:

$$\mathrm{Mlt}(Q) = \langle L_x, R_x \mid x \in Q \rangle$$

The stabilizer of $1 \in Q$ is the *inner mapping group*

$$\mathrm{Inn}(Q) = (\mathrm{Mlt}(Q))_1$$

Center

For a loop Q, the *center* of Q is

$$Z(Q) = \left\{ a \in Q \;\middle|\; \begin{array}{c} ax = xa, \\ ax \cdot y = a \cdot xy, \\ xa \cdot y = x \cdot ay, \\ xy \cdot a = x \cdot ya \end{array} \quad \forall x, y \in Q \right\}.$$

In other words, it is the set of all elements that commute *and associate* with everything.
The center of a loop is a normal subloop.

Nilpotency

The *upper central series* of a loop Q is defined just as it is for groups:

$$1 = Z_0(Q) \leq Z_1(Q) \leq \cdots \leq Z_n(Q) \leq \cdots$$

where for $n > 0$, $Z_n(Q)$ is the preimage of $Z(Q/Z_{n-1}(Q))$ under the natural homomorphism $Q \to Q/Z_{n-1}(Q)$.

A loop is *nilpotent* of class n if $Z_n(Q) = Q$ and n is the smallest index for which this occurs.

A Standard Exercise

For a group G, the easy exercise

$$\mathrm{Inn}(G) \cong G/Z(G)$$

leads to the observation

G is nilpotent of class n $\iff$ $\mathrm{Inn}(G)$ *is nilpotent of class* $n-1$.

The usual way to get a loop theorist to salivate:

Question: *What happens when we try to extend this to loops?*

A Bad Answer

If $Q/Z(Q)$ is not associative, then obviously there is no isomorphism between $\mathrm{Inn}(Q)$ and $Q/Z(G)$.

Even if $Q/Z(Q)$ is a group, it still doesn't work:

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	1	2	4	3
6	6	5	2	1	3	4

In this loop, $Q/Z(Q)$ is cyclic of order 3, $\mathrm{Inn}(Q)$ is elementary abelian of order 4.

So forget the isomorphism and focus on the nilpotence.

$n = 2$

Let's restrict the question to the "easiest" (ha!) case:

Problem

Let Q be a loop. Are the following statements equivalent?

- $\mathrm{Inn}(Q)$ *is abelian;*
- Q *is nilpotent of class (at most)* 2.

In his 1946 "Contributions..." paper, Bruck proved (2) $\Longrightarrow$ (1). (1) $\Longrightarrow$ (2) attracted the attention of many loop theorists. The primary (but not exclusive) interest was in the finite case.

Positive result

The best positive general result was the following:

Theorem (Niemenmaa & Kepka 1994)

Let Q be a finite loop with $\mathrm{Inn}(Q)$ abelian. Then Q is nilpotent.

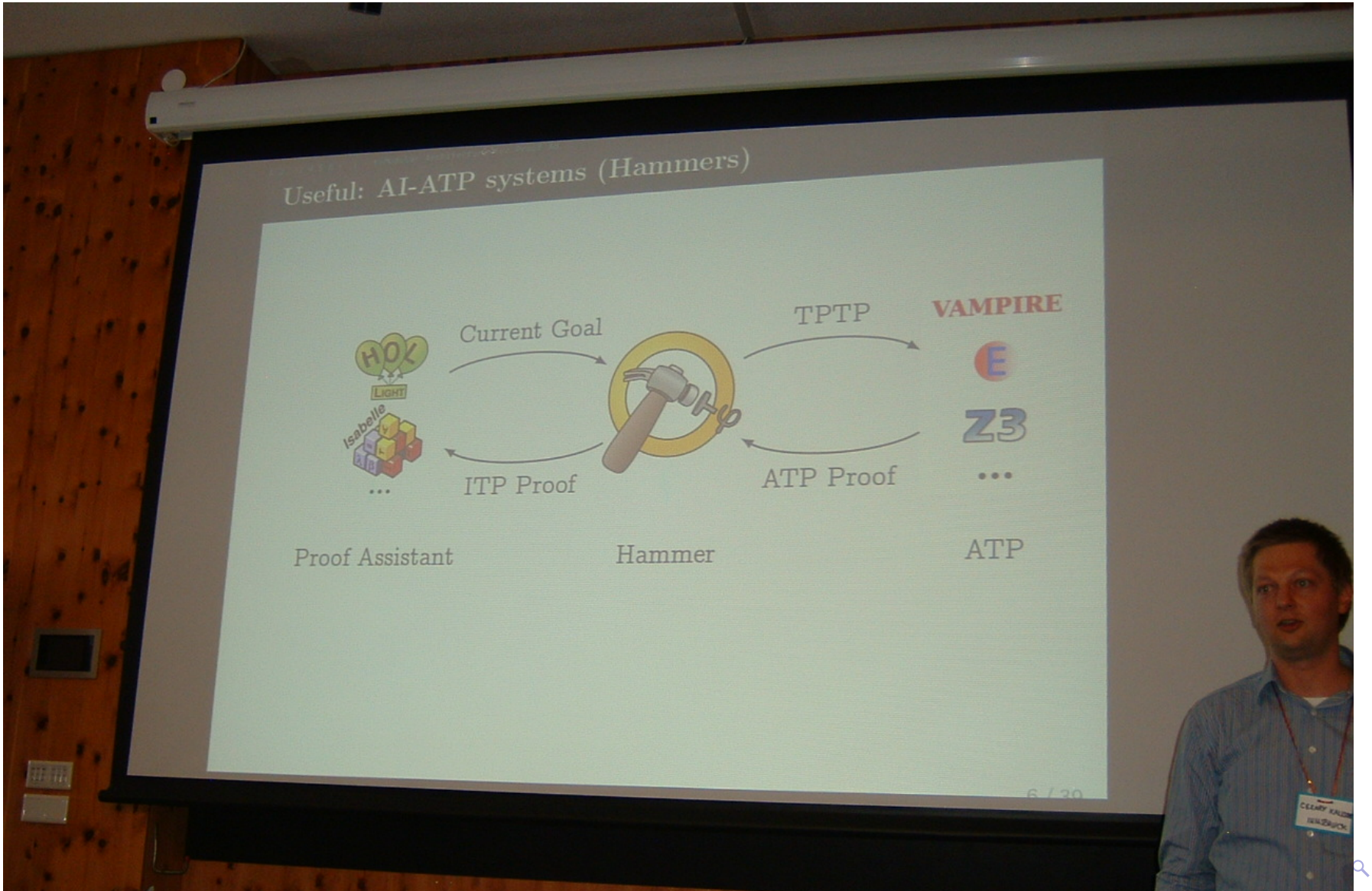
The proof is specific to the finite case, and there is no upper bound on the nilpotency class.

Early attempts

Already in the early 2000's, ATP-savvy loop theorists (J.D. Phillips and I) realized that the problem has a first-order formulation because . . .

- The assumption "$\mathrm{Inn}(Q)$ is abelian" can be stated equationally.
- The goal "Q is nilpotent of class 2" can be stated equationally.

Where Are We?


Useful: AI-ATP systems (Hammers)
Current Goal
TPTP
VAMPIRE
E
Z3
...
ITP Proof
ATP Proof
Proof Assistant
Hammer
ATP

Abelian Inner Mappings

```
% generators of Inn(Q)
(y * x) \ (y * (x * u)) = L(u,x,y).
((u * x) * y) / (x * y) = R(u,x,y).
x \ (y * x) = T(y,x).

% AIM
T(T(x,y),z) = T(T(x,z),y)                  # label("TT").
T(L(u,x,y),z) = L(T(u,z),x,y)              # label("TL").
T(R(u,x,y),z) = R(T(u,z),x,y)              # label("TR").
L(L(u,x,y),z,w) = L(L(u,z,w),x,y)          # label("LL").
L(R(u,x,y),z,w) = R(L(u,z,w),x,y)          # label("LR").
R(R(u,x,y),z,w) = R(R(u,z,w),x,y)          # label("RR").
```

Associators and Commutators

To formulate the goals, we need two more defined functions:

Associators:

$$\cdot[x, y, z] = (x \cdot yz)\backslash(xy \cdot z)$$

Commutators

$$[x, y] = (yx)\backslash(xy)$$

These are conventional choices out of the literature. They are not necessarily well-adapted to the problem at hand!

Goals

```
% associator and commutator
(x * (y * z)) \ ((x * y) * z) = a(x,y,z).
(x * y) \ (y * x) = K(y,x).

% nilpotent of class 2
K(K(x,y),z) = 1          # label("KK").
a(K(x,y),z,u) = 1        # label("aK1").
a(x,K(y,z),u) = 1        # label("aK2").
a(x,y,K(z,u)) = 1        # label("aK3").
a(a(x,y,z),u,w) = 1      # label("aa1").
a(x,a(y,z,u),w) = 1      # label("aa2").
a(x,y,a(z,u,w)) = 1      # label("aa3").
K(a(x,y,z),u) = 1        # label("Ka").
```

Results?

J.D. worked on this (back in the OTTER days) but didn't really get anywhere. Neither he nor I knew much about user-controlled strategies, so we were treating the theorem prover as a black box.

Results?

J.D. worked on this (back in the OTTER days) but didn't really get anywhere. Neither he nor I knew much about user-controlled strategies, so we were treating the theorem prover as a black box.

As it turns out, there was a good reason J.D. wasn't going to succeed completely.

Counterexamples

The first counterexample was found by Csörgő sometime in 2004. She formally announced it in talks in 2005, and the paper finally appeared in 2007. She found

- a loop Q of order 2^7 with
- $\mathrm{Inn}(Q)$ an abelian group, but
- of nilpotency class 3.

More counterexamples (now all called *loops of Csörgő type*) quickly followed in the literature. No counterexample of smaller size is known. It is difficult to imagine a finite model builder (MACE4, PARADOX) finding one.

Special cases

The original AIM problem does have a positive answer in various special cases where we...

- restrict the structure of $\mathrm{Inn}(Q)$, or
- restrict the structure of Q, or
- both

In Bob Veroff's terminology, these are "extensions" of the theory because we are adjoining additional assumptions.

Special cases

For this audience, I'll only mention one special case:

Theorem (Phillips & Stanovský 2012)

A Bruck loop with abelian inner mapping group is nilpotent of class at most 2.

They proved this result using WALDMEISTER, running for a couple of weeks.

Special cases

For this audience, I'll only mention one special case:

Theorem (Phillips & Stanovský 2012)

A Bruck loop with abelian inner mapping group is nilpotent of class at most 2.

They proved this result using WALDMEISTER, running for a couple of weeks.

(***Interesting* problems take a while to run!**)

What now?

I spent some time carefully studying the known loops of Csörgő type, and I noticed something interesting.

The only goal which was false was

```
K(K(x,y),z) = 1        # label("KK").
```

The other seven goals are all true! Taken together, those seven have a high order meaning.

Original AIM Conjecture

Here is the high-level version I would state to other loop theorists.

Conjecture (AIM, Version 1)

Let Q be a loop with $\mathrm{Inn}(Q)$ abelian. Then:

- *$Q/\mathrm{Nuc}(Q)$ is an abelian group, and*
- *$Q/Z(Q)$ is a group.*

(Hence Q is nilpotent of class at most 3.)

The two items are expressed equationally by the remaining seven goals.

The equational form of this is how I dragged Bob into the problem.

Successes

Thanks to herculean efforts by Bob using proof sketches (a.k.a. the hints strategy), proofs of all 7 goals have been found in many classes of loops of interest. These won't mean anything to those outside of quasigroup theory, but they cover most of the classes of loops which people study in detail (e.g., Moufang loops).

One could make a case that for "important" loops, the question is settled.

We have not published much...

In my earlier work in ATP-driven loop theory, it was easy to "translate" PROVER9 proofs into something humanly readable, down to maybe one or two technical lemmas.

Current proofs are too long for this to be reasonable.

(Maybe go back to a proof assistant using a hammer?)

Dependencies

It is natural to study dependencies among the goals, that is, if we assume the AIM hypotheses and some of the goals, do other goals follow?

- Ka $\Longrightarrow$ {aK1,aK2,aK3}
- aK1 $\Longrightarrow$ {Ka,aK2,aK3}
- aK3 $\Longrightarrow$ {Ka,aK1,aK2}
- any of aa1, aa2 or aa3 implies the other two

So to prove the AIM conjecture it is enough to prove, say, aK1 and aa1.

Notice anything missing?

Dependencies

Despite a lot of effort, Bob has not able to get a proof of

aK2 $\Longrightarrow$ anything!

Is this evidence against the AIM Conjecture? I don't know!

Generalization

It is evident that the seven AIM goals are not *sufficient* for a loop to be an AIM loop. *Every* group satisfies them, for instance.

So maybe the full power of the AIM assumption is not necessary?

“Middle” Inner Mappings

Let

```
M(u,x,y) = y \ ((y * (u * x)) / x).
```

Set

$$\mathrm{Inn}_*(Q) = \langle L_{x,y}, R_{x,y}, M_{x,y} \mid x, y \in Q \rangle.$$

Generalized AIM Conjecture

Conjecture (Generalized AIM)

Let Q be a loop. The following are equivalent.

1. $\mathrm{Inn}_*(Q)$ *is in the center of* $\mathrm{Inn}(Q)$*;*
2. $Q/\mathrm{Nuc}(Q)$ *is an abelian group and* $Q/Z(Q)$ *is a group.*

- The middle inner mappings are needed or this isn't true.
- If Q is a group, both parts are vacuously true.

More Successes

Theorem (K)

(2) $\Longrightarrow$ (1) is true.

So far...

The Generalized AIM Conjecture has been proven for every class of loops for which the AIM Conjecture has been proven.

Back to AIM

The successes of the Generalized AIM Conjecture lead us to ask:

Can we modify the AIM Conjecture to get a full characterization?

The answer is yes, but first we need a brief interlude.

Levi's Theorem

Theorem (Levi 1942)

The following are equivalent.

- *G is nilpotent of class 2;*
- *The commutator* `K( , )` *is associative.*

AIM Conjecture

Conjecture (AIM, Current Version (high level))

Let Q be a loop. The following are equivalent.

1. $\mathrm{Inn}(Q)$ *is abelian;*
2. $Q/\mathrm{Nuc}(Q)$ *is an abelian group,* $Q/Z(Q)$ *is a group, and* $\mathtt{K}(\ ,\ )$ *is associative.*

- If Q is a group, this follows from Levi's Theorem.

Theorem (K, Veroff)

- *(2)* $\Longrightarrow$ *(1) is true.*
- *If (1) holds, then* $\mathtt{K}(\ ,\ )$ *is associative.*

Ecstasy and Despair

Reasons to be happy: The (Generalized) AIM Conjecture holds for so many interesting types of loops!

Reasons to be sad: We still don't know...

Conjecture (Commutative AIM)

Let Q be a commutative loop. The following are equivalent.

1. $\mathrm{Inn}(Q)$ *is abelian;*
2. Q *is nilpotent of class* 2.

(Original Problem $=$ AIM $=$ Generalized AIM in this case)

Final Remarks

Final Remarks

- My gut intuition is that if the AIM Conjecture is false, then something close to it is true.

Final Remarks

- My gut intuition is that if the AIM Conjecture is false, then something close to it is true.
- *It is clear that we must embrace struggle.*
  – Rilke

Final Remarks

- My gut intuition is that if the AIM Conjecture is false, then something close to it is true.
- *It is clear that we must embrace struggle.*
  – Rilke
- That's all! Thanks!