The Weak AIM Conjecture

Michael Kinyon

University of Denver

LOOPS'23
29 June 2023

Whom to blame?

This is joint work with Petr Vojtěchovský (U. Denver) and especially Bob Veroff (U. New Mexico)

Multiplication Group and Inner Mapping Group

In a loop Q, *left* and *right translations*

$$L_x : Q \to Q;\ L_x(y) = xy \qquad R_x : Q \to Q;\ R_x(y) = yx\,.$$

are permutations of Q that generate the *multiplication group* of Q:

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

The stabilizer of the identity element is the *inner mapping group*:

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

Nuclei and Center

The *nuclei* of a loop Q:

$$\begin{aligned}
\mathrm{Nuc}_\ell(Q) &= \{a \in Q \,|\, ax \cdot y = a \cdot xy\,,\ \forall x, y \in Q\} \\
\mathrm{Nuc}_m(Q) &= \{a \in Q \,|\, xa \cdot y = x \cdot ay\,,\ \forall x, y \in Q\} \\
\mathrm{Nuc}_r(Q) &= \{a \in Q \,|\, xy \cdot a = x \cdot ya\,,\ \forall x, y \in Q\} \\
\mathrm{Nuc}(Q) &= \mathrm{Nuc}_\ell(Q) \cap \mathrm{Nuc}_m(Q) \cap \mathrm{Nuc}_r(Q)
\end{aligned}$$

Each nucleus is a (not necessarily normal) subloop.
The *center* of a loop Q:

$$Z(Q) = \mathrm{Nuc}(Q) \cap \{a \in Q \,|\, ax = xa,\ \forall x, y \in Q\}\ .$$

This is always a normal subloop.

Nilpotency

The *upper central series* of 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 $Q \to Q/Z_{n-1}(Q)$.

Q is *nilpotent* of class n if $Z_n(Q) = Q$ and n is the smallest positive integer where this occurs.

Standard Exercise

An easy exercise in beginning group theory:

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

This doesn't generalize to loops.

- $Q/Z(Q)$ need not be associative, but even if it is...
- **Example**: Each of the nonassociative left Bol loops Q of order 8 has $Q/Z(Q) \cong C_2^2$ but $\mathrm{Inn}(Q) \cong C_2^3$.

Back to nilpotence

In a group G, the easy exercise has the following corollary:

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

So what about loops?

AIM loops

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

We say that Q is an *AIM* (**A**belian **I**nner **M**appings) loop if $\mathrm{Inn}(Q)$ is an abelian group.

Problem

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

- *Q is nilpotent of class at most 2;*
- *Q is an AIM loop.*

(1) $\Longrightarrow$ (2): [Bruck (1946)].

(2) $\Longrightarrow$ (1): . . . .

Positive result

The best positive general result was the following:

Theorem (Niemenmaa & Kepka (1994))

Every finite AIM loop is nilpotent.

The proof uses finiteness; it assumes the existence of a minimal counterexample and finds a contradiction. There is no upper bound on the nilpotency class.

A later improvement:

Theorem (Niemenmaa (2009))

Every finite loop with nilpotent inner mapping group is nilpotent.

Special varieties

Jumping out of historical order, there are a few positive results in special varieties:

Every AIM loop in each of the following varieties is nilpotent of class at most 2

[Csörgő & Drapal (2005)]	left conjugacy closed
[Phillips & Stanovský (2012)]	Bruck
[KVV]	automorphic

However, there is a good reason no progress was made in the general case. . . .

Counterexamples

The first counterexample was announced by Csörgő in 2005; her paper appeared in 2007. She found

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

Loops of Csörgő type

AIM loops of nilpotency class 3 have been called loops of *Csörgő type*.

More examples:

[Nagy & Vojtěchovský (2009)]: Moufang loop of order 2^{14}
[Drápal & Vojtěchovský (2011)]: general construction from groups
[Drápal & Kinyon (2015)]: Buchsteiner loop of order 2^7

No counterexample of order smaller than 2^7 is known.

Open Problem: Is 2^7 the smallest possible order for a loop of Csörgő type?

What now?

What can we salvage?

I spent some time studying the known AIM loops Q of nilpotency class 3, and I noticed two things were true of all of them:

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

(By the way, convince yourself that in an AIM loop Q, each of the nuclei is normal.)

Strong AIM Conjecture

Conjecture (Strong AIM)

Let Q be an AIM loop. Then:

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

Weak AIM Conjecture

Conjecture (Weak AIM)

Every AIM loop is nilpotent of class at most 3.

The Strong AIM Conjecture implies the Weak AIM Conjecture. (If Q is an AIM loop satisfying the conclusion of the SAC, then $Q/Z(Q)$ is an AIM group, hence nilpotent of class at most 2.)

Generators of the Inner Mapping Group

$\mathrm{Inn}(Q)$ is generated by a useful set of inner mappings:

$$T_x = R_x^{-1} L_x \qquad \text{(generalized conjugations)}$$

$$L_{x,y} = L_{xy}^{-1} L_x L_y \qquad \text{(measures of}$$

$$R_{x,y} = R_{yx}^{-1} R_x R_y \qquad \text{nonassociativity)}$$

AIM loops form a variety

A loop Q is an AIM loop if and only if the following (universally quantified) identities are satisfied:

$$
\begin{aligned}
L_{x,y}L_{u,v}(z) &= L_{u,v}L_{x,y}(z)\\
L_{x,y}R_{u,v}(z) &= R_{u,v}L_{x,y}(z)\\
R_{x,y}R_{u,v}(z) &= R_{u,v}R_{x,y}(z)\\
L_{x,y}T_{u}(z) &= T_{u}L_{x,y}(z)\\
R_{x,y}T_{u}(z) &= R_{u}L_{x,y}(z)\\
T_{u}T_{v}(z) &= T_{v}T_{u}(z)
\end{aligned}
$$

Thus AIM loops form a variety (equational class) and are therefore closed under taking subloops, direct products, and homomorphic images.

Associators and Commutators

We use Bruck's conventions:

Associators:

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

Commutators

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

(It can be reasonably argued that other conventions for associators and commutators might be better tailored to the problem.)

Equational Formulation of the Goal

The conclusion of the Strong AIM Conjecture is encoded by these identities:

Identity	Interpretation
$[[x, y, z], u, v] = 1$	$Q/\mathrm{Nuc}_\ell(Q)$ associative
$[x, [y, z, u], v] = 1$	$Q/\mathrm{Nuc}_m(Q)$ associative
$[x, y, [z, u, v]] = 1$	$Q/\mathrm{Nuc}_r(Q)$ associative
$[[x, y], z, u] = 1$	$Q/\mathrm{Nuc}_\ell(Q)$ commutative
$[x, [y, z], u] = 1$	$Q/\mathrm{Nuc}_m(Q)$ commutative
$[x, y, [z, u]] = 1$	$Q/\mathrm{Nuc}_r(Q)$ commutative
$[[x, y, z], u] = 1$	

Automated Theorem Proving

Since both the hypothesis and conclusions of the AIM Conjectures have equational formulations, Bob Veroff and I decided to try automated theorem proving, specifically Prover9.

A direct proof from hypotheses to conclusion is way out of reach, so progress has been incremental, but (somewhat) steady.

Key Lemmas

Theorem (KVV via Prover9, after *many* years of work)

In any AIM loop, the following identities hold:

$$[[x, y, z], u] = [x, y, [z, u]] = [x, [y, u], z] = [[x, y], z, u]$$

Further, this 4-ary term is invariant under permutations of the variables under the action of the alternating group A_4.

Corollary

In an AIM loop Q, $Q/\mathrm{Nuc}(Q)$ is commutative iff $Q/\mathrm{Nuc}_k(Q)$ is commutative for some $k \in \{\ell, m, r\}$.

Key Lemmas II

Theorem (KVV via Prover9)

In AIM loops, the following identities are equivalent:

$$[[x, y, z], u, v] = 1$$
$$[x, [y, z, u], v] = 1$$
$$[x, y, [z, u, v]] = 1$$

Corollary

In an AIM loop Q, $Q/\mathrm{Nuc}(Q)$ is associative iff $Q/\mathrm{Nuc}_k(Q)$ is associative for some $k \in \{\ell, m, r\}$.

Reducing the number of goals

To prove the Strong AIM Conjecture, it is enough to prove two identities, say,

$$[[x,y],z,u] = [[x,y,z],u,v] = 1$$

(We can simplify further, as we'll see shortly.)

Successes

Theorem (KVV via Prover9)

The Strong AIM Conjecture holds for the following varieties of loops:

- *left (or right) automorphic*
- *left (or right) Bol (therefore, Moufang)*
- *LC (or RC) (therefore C, therefore Steiner)*
- *Buchsteiner*
- *. . . and other more obscure ones*

Failures (so far)

It is unknown if the Strong AIM Conjecture holds for *commutative* loops:

$$xy = yx$$

If the Strong AIM Conjecture is true, then any commutative AIM loop would have nilpotency class 2. We have made essentially no progress toward this.

More on this later.

Ta-daa!

The Weak AIM Conjecture is true.

Theorem (KVV)

Every AIM loop is nilpotent of class at most 3.

We do *not* have a direct PROVER9 proof of this, but rather something more interesting: a mix of PROVER9 lemmas and high level human reasoning.

In the rest of this talk, I will outline the proof.

Principal Loop Isotopes

Given a loop Q, fix elements $a, b \in Q$ and define a new binary operation by

$$x \circ y = (x/a) \cdot (b \backslash y) \,.$$

This is a new loop operation with identity element ba. The new loop, which we will denote by $Q_{a,b}$, is a *principal loop isotope* of Q, and $Q_{a,b}$ and Q are *isotopic* loops.

Isotopically invariant varieties

A variety of loops is *isotopically invariant* (or universal) if, whenever a loop is in the variety, so is every (principal) loop isotope.

Well known isotopically invariant varieties:

- groups
- Moufang loops
- Bol loops
- conjugacy closed loops
- nilpotent loops of class at most n

Isotopically invariant varieties II

One can also just stipulate that the defining identities of a variety hold in all isotopes by writing them in every $Q_{a,b}$.

Example: For the flexible law $xy \cdot x = x \cdot yx$, here is the identity defining the variety of *isotopically invariantly flexible* loops:

$$(x/u \cdot v\backslash y)/u \cdot v\backslash x = x/u \cdot v\backslash(y/u \cdot v\backslash)$$

Here we view u and v as universally quantified.

Multiplication groups of isotopes

1. $\mathrm{Mlt}(Q) = \mathrm{Mlt}(Q_{a,b})$, and
2. $\mathrm{Inn}(Q)$ is conjugate to $\mathrm{Inn}(Q_{a,b})$.

(*Proof*: (1) Just write down the generators.
(2) $\mathrm{Mlt}(Q)$ is transitive and inner mapping groups are point stabilizers.)

Important observation

AIM loops are an isotopically invariant variety!

This places a large role in the proof of the Weak AIM Conjecture.

Normal subloops of isotopes

A subset $N \subseteq Q$ is a normal subloop of Q if and only if $ba \cdot N$ is a normal subloop of $Q_{a,b}$.

$(\mathrm{Mlt}(Q) = \mathrm{Mlt}(Q_{a,b})$ and a normal subloop of a loop is a block of its multiplication group containing the identity element.)

Why we need this: In AIM loops, the nuclei are all normal subloops.

Quotients of isotopes = isotopes of quotients

For a normal subloop H of Q,

$$\frac{Q_{a,b}}{ba \cdot H} \cong \left(\frac{Q}{H}\right)_{aH,bH}$$

Here is a very important idea for what follows:

Let P be a property of loops preserved by isomorphism. The following are equivalent:

- For every loop isotope $Q_{a,b}$ of Q, $Q_{a,b}/(ba \cdot H)$ satisfies P
- Every loop isotope of Q/H satisfies P

Step 1a

Theorem

Let $\mathcal{V}$ be an isotopically invariant variety of AIM loops and assume that for every loop Q in $\mathcal{V}$, $Q/\mathrm{Nuc}(Q)$ is commutative. Then the Strong AIM Conjecture holds in $\mathcal{V}$.

Proof.

The assumption implies $Q_{a,b}/(ba \cdot \mathrm{Nuc}(Q))$ is commutative for every loop isotope of Q. Thus loop every isotope of $Q/\mathrm{Nuc}(Q)$ is commutative. But if every isotope of a loop is commutative, the loop itself is an abelian group. Thus $Q/\mathrm{Nuc}(Q)$ is an abelian group. Since $[[x, y, z], u] = [[x, y], z, u] = 1$, $Q/Z(Q)$ is associative. □

Step 1b

Corollary

If $\mathcal{V}$ is an isotopically invariant variety of AIM loops, then the Strong AIM Conjecture holds in $\mathcal{V}$ if and only if the identity

$$[[x, y], z, u] = 1$$

holds for all loops in $\mathcal{V}$.

Step 2

Theorem (Prover9)

If Q is an AIM loop, then

$$[x, [y, z]] \in Z(Q)$$

In other words, $[x, [y, z]] = 1$ holds in $Q/Z(Q)$.

(We don't need the isotopically invariant version of this one.)

Step 3

Theorem (Prover9)

If Q is an AIM loop, then $Q/Z(Q)$ is flexible:

$$xy \cdot x = x \cdot yx$$

Corollary

If Q is an AIM loop, then $Q/Z(Q)$ is isotopically invariantly flexible.

Aside 1: Middle Bol loops

A loop Q is a *middle Bol loop* if it is isotopically invariant for the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$. Middle Bol loops are characterized by the middle Bol identity

$$x((yz)\backslash x) = x/z \cdot y\backslash x\,..$$

Middle Bol loops are inverse isostrophes of left (or right) Bol loops and have not been studied much on their own. See [Drápal & Syrbu 2022] for the most recent work.

Aside 2: Middle Bol loops and flexibility

Left Bol loops	are isot. inv. for	LIP ($x^{-1} \cdot xy = y$)
	and for	LAlt ($xx \cdot y = x \cdot xy$)
Right Bol loops	are isot. inv. for	RIP ($xy \cdot y^{-1} = x$)
	and for	RAlt ($xy \cdot y = x \cdot yy$)
Middle Bol loops	are isot. inv. for	AAIP ($(xy)^{-1} = y^{-1}x^{-1}$)
	and for	???

By analogy, it was thought that middle Bol loops might be isotopically invariant for flexibility. Indeed, many middle Bol loops are isotopically invariantly flexible.

Step 4a

- There is a middle Bol loop of order 16 which is not flexible.
- There is an isotopically invariantly flexible loop of order 32 which is not middle Bol.

However

Theorem (Prover9)

An AIM loop is isotopically invariantly flexible if and only if it is a middle Bol loop.

Step 4b

Theorem (Prover9)

Let Q be a middle Bol AIM loop. Then $Q/Nuc(Q)$ is commutative.

Middle Bol loops are an isotopically invariant variety. Therefore:

Corollary

The variety of middle Bol AIM loops satisfies the Strong AIM Conjecture.

Final step!

If Q is an AIM loop, then $Q/Z(Q)$ satisfies $[[x, y], z] = 1$ and is a middle Bol loop satisfying the Strong AIM Conjecture.

Thus $(Q/Z(Q))/Z(Q/Z(Q))$ is a group satisfying $[x, y] = 1$.

Thus $(Q/Z(Q))/Z(Q/Z(Q))$ is an *abelian* group.

Thus $Q/Z(Q)$ is nilpotent of class at most 2.

Therefore Q is nilpotent of class at most 3.

QED

Status of the Strong AIM Conjecture

Our intuition is that although the Strong AIM Conjecture is true many varieties, it is false in general.

In fact, there might be a (not necessarily finite) *commutative* counterexample.

Aside: AIM loops and Yang-Baxter

I got Prover9 to prove that in every AIM loop, the binary operation $(x, y) \mapsto T_x(y)$ satisfies Rump's left cycle identity:

$$T_{T_x(y)} T_x(z) = T_{T_y(x)} T_y(z) .$$

(It is *not*, in general, left distributive.) From this and other facts, we get:

$$R : Q \times Q \to Q \times Q; (x, y) \mapsto (T_x^{-1}(y), T_{T_x^{-1}(y)}(x))$$

is an involutive, nondegenerate set-theoretic solution of the Yang-Baxter equation.

I don't know what this says about AIM loops.

Thanks!

Dziękuję bardzo!

And be sure to follow me on Twitter: **@ProfKinyon**