Several results, questions and notions of loop theory relevant for universal algebra

Aleš Drápal

(Joint work with Petr Vojtěchovský, Denver University)

Charles University in Prague
Czech Republic

September 6, 2023, Stará Lesná, Slovensko
Summer School on General Algebra and Ordered Sets

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying
  $x \cdot (x\backslash y) = x\backslash(x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x \backslash y) = x \backslash (x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q\ \exists\,! x, y \in Q$ such that $a \cdot x = b = y \cdot a$.

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x\backslash y) = x\backslash(x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q\ \exists!x, y \in Q$ such that $a \cdot x = b = y \cdot a$.
  The connection: $x = a\backslash b$ and $y = b/a$.

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x \backslash y) = x \backslash (x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q \; \exists \, ! x, y \in Q$ such that $a \cdot x = b = y \cdot a$.
  The connection: $x = a \backslash b$ and $y = b/a$.
- Definition using transformations: $(Q, \cdot)$ such that the left translation $L_a \colon x \mapsto a \cdot x$ and the right translation $R_a \colon x \mapsto x \cdot a$ permute Q for all $a \in Q$, and $L_e = R_e = \mathrm{id}_Q$ for some $e \in Q$.

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x \backslash y) = x \backslash (x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q \; \exists ! x, y \in Q$ such that $a \cdot x = b = y \cdot a$.
  The connection: $x = a \backslash b$ and $y = b/a$.
- Definition using transformations: $(Q, \cdot)$ such that the left translation $L_a \colon x \mapsto a \cdot x$ and the right translation $R_a \colon x \mapsto x \cdot a$ permute Q for all $a \in Q$, and $L_e = R_e = \mathrm{id}_Q$ for some $e \in Q$.

Normal subloops

$S \trianglelefteq Q \iff S \leq Q$ and $\forall x \in Q \colon xS = Sx = S(Sx) = (xS)S$.

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x\backslash y) = x\backslash(x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q \ \exists! x, y \in Q$ such that $a \cdot x = b = y \cdot a$.
  The connection: $x = a\backslash b$ and $y = b/a$.
- Definition using transformations: $(Q, \cdot)$ such that the left translation $L_a \colon x \mapsto a \cdot x$ and the right translation $R_a \colon x \mapsto x \cdot a$ permute Q for all $a \in Q$, and $L_e = R_e = \mathrm{id}_Q$ for some $e \in Q$.

Normal subloops

$S \trianglelefteq Q \iff S \leq Q$ and $\forall x \in Q \colon xS = Sx = S(Sx) = (xS)S$.
If $S \trianglelefteq Q$, then $\{xS : x \in Q\}$ partitions Q and yields a congruence $\bmod S$ such that

$$(x, y) \in \bmod S \iff xS = yS.$$

Definition of a loop

- Universal algebra: $(Q, \cdot, /, \backslash, 1)$ satisfying $x \cdot (x\backslash y) = x\backslash(x \cdot y) = y = (y \cdot x)/x = (y/x) \cdot x$ and $x \cdot 1 = x = 1 \cdot x$.
- Standard definition: $(Q, \cdot, 1)$ such that 1 is a neutral element and $\forall a, b \in Q\ \exists!x, y \in Q$ such that $a \cdot x = b = y \cdot a$.
  The connection: $x = a\backslash b$ and $y = b/a$.
- Definition using transformations: $(Q, \cdot)$ such that the left translation $L_a \colon x \mapsto a \cdot x$ and the right translation $R_a \colon x \mapsto x \cdot a$ permute Q for all $a \in Q$, and $L_e = R_e = \mathrm{id}_Q$ for some $e \in Q$.

Normal subloops

$S \trianglelefteq Q \iff S \leq Q$ and $\forall x \in Q \colon xS = Sx = S(Sx) = (xS)S$.
If $S \trianglelefteq Q$, then $\{xS : x \in Q\}$ partitions Q and yields a congruence $\bmod S$ such that

$$(x, y) \in \bmod S \iff xS = yS.$$

Equivalences $\bmod S$, $S \trianglelefteq Q$, are exactly the congruences of a loop Q.

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images.
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

Fresh results about Moufang loops

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images.
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

When $\bmod S$ is an abelian congruence in a Moufang loop Q.

Theorem. *If and only if $S \trianglelefteq Q$ is abelian and weakly nuclear.* (This means that if $s, t \in S$ and $x \in Q$, then $s \cdot (x \cdot t) = (s \cdot x) \cdot t$.)

Fresh results about Moufang loops

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images. $(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

When $\bmod S$ is an abelian congruence in a Moufang loop Q.

Theorem. *If and only if $S \trianglelefteq Q$ is abelian and weakly nuclear.* (This means that if $s, t \in S$ and $x \in Q$, then $s \cdot (x \cdot t) = (s \cdot x) \cdot t$.)

When a finite Moufang loop Q is solvable

Theorem. *Let Q be a finite Moufang loop. Then Q is classically solvable whenever Q is congruence solvable.*

Fresh results about Moufang loops

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images.
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

When $\bmod S$ is an abelian congruence in a Moufang loop Q.

Theorem. *If and only if $S \trianglelefteq Q$ is abelian and weakly nuclear.* (This means that if $s, t \in S$ and $x \in Q$, then $s \cdot (x \cdot t) = (s \cdot x) \cdot t$.)

When a finite Moufang loop Q is solvable

Theorem. *Let Q be a finite Moufang loop. Then Q is classically solvable whenever Q is congruence solvable.*

Both solvabilities require a series $1 = S_0 \leq \cdots \leq S_k = Q$, $S_i \trianglelefteq Q$.

Fresh results about Moufang loops

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images.
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

When $\bmod S$ is an abelian congruence in a Moufang loop Q.

Theorem. *If and only if $S \trianglelefteq Q$ is abelian and weakly nuclear.* (This means that if $s, t \in S$ and $x \in Q$, then $s \cdot (x \cdot t) = (s \cdot x) \cdot t$.)

When a finite Moufang loop Q is solvable

Theorem. *Let Q be a finite Moufang loop. Then Q is classically solvable whenever Q is congruence solvable.*

Both solvabilities require a series $1 = S_0 \leq \cdots \leq S_k = Q$, $S_i \trianglelefteq Q$.
Classical solvability: S_i/S_{i-1} abelian, $1 \leq i \leq k$.

Fresh results about Moufang loops

Moufang loops are loops that satisfy Moufang laws

There are four Moufang laws: the ensuing two and their mirror images.
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ and $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$.

When $\mathrm{mod}\, S$ is an abelian congruence in a Moufang loop Q.

Theorem. *If and only if $S \trianglelefteq Q$ is abelian and weakly nuclear.* (This means that if $s, t \in S$ and $x \in Q$, then $s \cdot (x \cdot t) = (s \cdot x) \cdot t$.)

When a finite Moufang loop Q is solvable

Theorem. *Let Q be a finite Moufang loop. Then Q is classically solvable whenever Q is congruence solvable.*

Both solvabilities require a series $1 = S_0 \leq \cdots \leq S_k = Q$, $S_i \trianglelefteq Q$.
Classical solvability: S_i/S_{i-1} abelian, $1 \leq i \leq k$.
Congruence solvability: $\mathrm{mod}(S_i/S_{i-1})$ abelian congruence in Q/S_{i-1}, $1 \leq i \leq k$.

Fresh results about Moufang loops II

Counterexamples

There exists an abelian group $S \trianglelefteq Q$ such that Q is Moufang and $\bmod S$ is not an abelian congruence. (Q may be chosen to be nilpotent of order 16.)

Fresh results about Moufang loops II

Counterexamples

There exists an abelian group $S \trianglelefteq Q$ such that Q is Moufang and $\bmod S$ is not an abelian congruence. (Q may be chosen to be nilpotent of order 16.)
There exists a classically solvable finite Bol loop of order 16 that is not congruence solvable.

Fresh results about Moufang loops II

Counterexamples

There exists an abelian group $S \trianglelefteq Q$ such that Q is Moufang and $\bmod S$ is not an abelian congruence. (Q may be chosen to be nilpotent of order 16.)
There exists a classically solvable finite Bol loop of order 16 that is not congruence solvable.

Applying congruence solvability to Moufang loops

Theorem. *A finite Moufang loop Q is solvable if and only if* $\mathrm{Mlt}(Q)$ *is solvable.* — For $|Q|$ odd proved by Glauberman (1968).

Fresh results about Moufang loops II

Counterexamples

There exists an abelian group $S \trianglelefteq Q$ such that Q is Moufang and $\bmod S$ is not an abelian congruence. (Q may be chosen to be nilpotent of order 16.) There exists a classically solvable finite Bol loop of order 16 that is not congruence solvable.

Applying congruence solvability to Moufang loops

Theorem. *A finite Moufang loop Q is solvable if and only if* $\mathrm{Mlt}(Q)$ *is solvable.* — For $|Q|$ odd proved by Glauberman (1968).
Explanation: $\mathrm{Mlt}(Q)$ is the *multiplication group* of Q, i.e., the permutation group generated by left and right translations, $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle$.

Fresh results about Moufang loops II

Counterexamples

There exists an abelian group $S \trianglelefteq Q$ such that Q is Moufang and $\mathrm{mod}\, S$ is not an abelian congruence. (Q may be chosen to be nilpotent of order 16.)
There exists a classically solvable finite Bol loop of order 16 that is not congruence solvable.

Applying congruence solvability to Moufang loops

Theorem. *A finite Moufang loop Q is solvable if and only if* $\mathrm{Mlt}(Q)$ *is solvable.* — For $|Q|$ odd proved by Glauberman (1968).
Explanation: $\mathrm{Mlt}(Q)$ is the *multiplication group* of Q, i.e., the permutation group generated by left and right translations, $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle$.

Infinite Moufang loops

Infinite Moufang loops are little studied. Even the word problem for free Moufang loops has not been solved yet. I conjecture that for infinite Moufang loops both notions of solvability disagree.

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \leq B \leq Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \leq B \leq Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

Definition. Denote by $\mathcal{C}$ the class of loops Q such that

$$\text{a section } S \text{ of } Q \text{ is a group} \iff |S| = 1.$$

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \leq B \leq Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

Definition. Denote by $\mathcal{C}$ the class of loops Q such that

$$\text{a section } S \text{ of } Q \text{ is a group} \iff |S| = 1.$$

Easy: $\mathcal{C}$ closed under homomorphic images and subloops.

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \le B \le Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

Definition. Denote by $\mathcal{C}$ the class of loops Q such that

$$\text{a section } S \text{ of } Q \text{ is a group} \iff |S| = 1.$$

Easy: $\mathcal{C}$ closed under homomorphic images and subloops.

Easy: $Q \notin \mathcal{C} \iff Q$ has a section $\cong \mathbb{Z}/p\mathbb{Z}$, p a prime.

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \leq B \leq Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

Definition. Denote by $\mathcal{C}$ the class of loops Q such that

$$\text{a section } S \text{ of } Q \text{ is a group} \iff |S| = 1.$$

Easy: $\mathcal{C}$ closed under homomorphic images and subloops.

Easy: $Q \notin \mathcal{C} \iff Q$ has a section $\cong \mathbb{Z}/p\mathbb{Z}$, p a prime.

The antiassociative quasivariety

Lemma. $\mathcal{C}$ is closed under finite products.

A fresh problem—antiassociative varieties

Loops in which associative sections are trivial

Let Q be a loop. A loop S is a *section* of Q if there exist subloops $A \leq B \leq Q$ such that $A \trianglelefteq B$ and $B/A \cong S$.

Definition. Denote by $\mathcal{C}$ the class of loops Q such that

$$\text{a section } S \text{ of } Q \text{ is a group} \iff |S| = 1.$$

Easy: $\mathcal{C}$ closed under homomorphic images and subloops.

Easy: $Q \notin \mathcal{C} \iff Q$ has a section $\cong \mathbb{Z}/p\mathbb{Z}$, p a prime.

The antiassociative quasivariety

Lemma. $\mathcal{C}$ is closed under finite products.

Problem

Is $\mathcal{C}$ a variety?

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial. Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial.
Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial.
Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Loop isotopes of a loop

Informally: Loops Q_1 and Q_2 are *isotopic* if permuting rows and columns in the multiplication table of Q_1 may produce a loop isomorphic to Q_2.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial. Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Loop isotopes of a loop

Informally: Loops Q_1 and Q_2 are *isotopic* if permuting rows and columns in the multiplication table of Q_1 may produce a loop isomorphic to Q_2.
Formally: There exists bijections $\alpha, \beta, \gamma \colon Q_1 \to Q_2$ such that $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q_1$.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial. Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Loop isotopes of a loop

Informally: Loops Q_1 and Q_2 are *isotopic* if permuting rows and columns in the multiplication table of Q_1 may produce a loop isomorphic to Q_2.
Formally: There exists bijections $\alpha, \beta, \gamma \colon Q_1 \to Q_2$ such that $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q_1$.
Criterion: Q_1 isotopic to $Q_2 \iff Q_2$ is $\cong$ to a principal isotope of Q_1.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial. Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Loop isotopes of a loop

Informally: Loops Q_1 and Q_2 are *isotopic* if permuting rows and columns in the multiplication table of Q_1 may produce a loop isomorphic to Q_2.
Formally: There exists bijections $\alpha, \beta, \gamma \colon Q_1 \to Q_2$ such that $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q_1$.
Criterion: Q_1 isotopic to $Q_2 \iff Q_2$ is $\cong$ to a principal isotope of Q_1.
A loop is a *principal isotope* of a loop Q if and only if the operation of the loop may be expressed as $(x/f) \cdot (e \backslash y)$, for some $e, f \in Q$.

Another problem—Falconer varieties

Being antiassociative in all isotopes

Let $\mathcal{C}$ be again the class of loops in which associative sections are trivial. Let $\mathcal{F}$ be the class of all loops Q such that every loop isotope of Q is in $\mathcal{C}$.
Informally: $Q \in \mathcal{F} \iff$ pattern of addition modulo a prime p appears as a subsquare in no multiplication table of a section of Q.

Loop isotopes of a loop

Informally: Loops Q_1 and Q_2 are *isotopic* if permuting rows and columns in the multiplication table of Q_1 may produce a loop isomorphic to Q_2.
Formally: There exists bijections $\alpha, \beta, \gamma \colon Q_1 \to Q_2$ such that $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q_1$.
Criterion: Q_1 isotopic to $Q_2 \iff Q_2$ is $\cong$ to a principal isotope of Q_1.
A loop is a *principal isotope* of a loop Q if and only if the operation of the loop may be expressed as $(x/f) \cdot (e\backslash y)$, for some $e, f \in Q$.

Easy: $\mathcal{F}$ is a pseudovariety. **Problem**: Is it a variety?

Persons involved

Who was Falconer

Etta Zuber Falconer (1933–2002) was an African-American female mathematician who got her Master's Degree in Madison, U. of Wiscosin, and her Ph.D. at Emory University (Trevor Evans supervisor). Her thesis resulted in two publications. The *Isotopy invariants in quasigroups* (TAMS 1970) contains a problem to find a universal variety of loops (i.e., isotopically invariant variety) that intersects the variety of groups trivially. In other words, to find nontrivial subvarieties of $\mathcal{F}$.

Persons involved

Who was Falconer

Etta Zuber Falconer (1933–2002) was an African-American female mathematician who got her Master's Degree in Madison, U. of Wiscosin, and her Ph.D. at Emory University (Trevor Evans supervisor). Her thesis resulted in two publications. The *Isotopy invariants in quasigroups* (TAMS 1970) contains a problem to find a universal variety of loops (i.e., isotopically invariant variety) that intersects the variety of groups trivially. In other words, to find nontrivial subvarieties of $\mathcal{F}$.

Kinyon and Allsop

The problem was not widely known. But Michael Kinyon knew the problem and made Jack Allsop aware that his construction of certain latin squares (under supervision of Ian Wanless) solves the problem.

Persons involved

Who was Falconer

Etta Zuber Falconer (1933–2002) was an African-American female mathematician who got her Master's Degree in Madison, U. of Wiscosin, and her Ph.D. at Emory University (Trevor Evans supervisor). Her thesis resulted in two publications. The *Isotopy invariants in quasigroups* (TAMS 1970) contains a problem to find a universal variety of loops (i.e., isotopically invariant variety) that intersects the variety of groups trivially. In other words, to find nontrivial subvarieties of $\mathcal{F}$.

Kinyon and Allsop

The problem was not widely known. But Michael Kinyon knew the problem and made Jack Allsop aware that his construction of certain latin squares (under supervision of Ian Wanless) solves the problem. In loops derived from the constructed latin squares all nontrivial left translations are semiregular permutations of prime order p, while in no nontrivial right translation there exists a cycle of length divisible p.

Building varieties from finite loops

Easy: To produce an isomorphically isotopic anti-associative variety of loops (i.e., a subvariety of $\mathcal{F}$, and thus a solution to the problem of Falconer).

Building varieties from finite loops

Easy: To produce an isomorphically isotopic anti-associative variety of loops (i.e., a subvariety of $\mathcal{F}$, and thus a solution to the problem of Falconer). Just take $\mathbf{HSP}(Q)$, where Q is a finite loop such that the multiplication table of Q has no proper subsquare and Q is not a group.

Building varieties from finite loops

Easy: To produce an isomorphically isotopic anti-associative variety of loops (i.e., a subvariety of $\mathcal{F}$, and thus a solution to the problem of Falconer). Just take $\mathbf{HSP}(Q)$, where Q is a finite loop such that the multiplication table of Q has no proper subsquare and Q is not a group.

More difficult: To describe subvarieties of $\mathcal{F}$ that would be finitely based (Allsop's construction belongs to such a variety).

Building varieties from finite loops

Easy: To produce an isomorphically isotopic anti-associative variety of loops (i.e., a subvariety of $\mathcal{F}$, and thus a solution to the problem of Falconer). Just take $\mathbf{HSP}(Q)$, where Q is a finite loop such that the multiplication table of Q has no proper subsquare and Q is not a group.

More difficult: To describe subvarieties of $\mathcal{F}$ that would be finitely based (Allsop's construction belongs to such a variety).

Difficult: To describe maximal varieties in $\mathcal{F}$. (Maybe there is only one such variety, namely $\mathcal{F}$ itself.)

Building varieties from finite loops

Easy: To produce an isomorphically isotopic anti-associative variety of loops (i.e., a subvariety of $\mathcal{F}$, and thus a solution to the problem of Falconer). Just take $\mathbf{HSP}(Q)$, where Q is a finite loop such that the multiplication table of Q has no proper subsquare and Q is not a group.

More difficult: To describe subvarieties of $\mathcal{F}$ that would be finitely based (Allsop's construction belongs to such a variety).

Difficult: To describe maximal varieties in $\mathcal{F}$. (Maybe there is only one such variety, namely $\mathcal{F}$ itself.)

In general, there seem to be very few results that take a finite loop Q and prove that $\mathbf{HSP}(Q)$ is not finitely based.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

Steiner loop of order 10

Up to $\cong$ there $\exists!$ such Q, given by the STS of affine lines in $\mathbb{F}_3^2$.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

Steiner loop of order 10

Up to $\cong$ there $\exists!$ such Q, given by the STS of affine lines in $\mathbb{F}_3^2$.
Fact: Q is in the variety $\mathcal{V}$ of Steiner loops that fulfil

$$(x \cdot z) \cdot (((x \cdot y) \cdot z) \cdot (y \cdot z)) = ((x \cdot z) \cdot ((x \cdot y) \cdot z)) \cdot (y \cdot z).$$

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

Steiner loop of order 10

Up to $\cong$ there $\exists!$ such Q, given by the STS of affine lines in $\mathbb{F}_3^2$.

Fact: Q is in the variety $\mathcal{V}$ of Steiner loops that fulfil

$$(x \cdot z) \cdot (((x \cdot y) \cdot z) \cdot (y \cdot z)) = ((x \cdot z) \cdot ((x \cdot y) \cdot z)) \cdot (y \cdot z).$$

Problem: Show that $\mathbf{HSP}(Q)$ is not finitely based.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

Steiner loop of order 10

Up to $\cong$ there $\exists!$ such Q, given by the STS of affine lines in $\mathbb{F}_3^2$.
Fact: Q is in the variety $\mathcal{V}$ of Steiner loops that fulfil

$$(x \cdot z) \cdot (((x \cdot y) \cdot z) \cdot (y \cdot z)) = ((x \cdot z) \cdot ((x \cdot y) \cdot z)) \cdot (y \cdot z).$$

Problem: Show that $\mathbf{HSP}(Q)$ is not finitely based.

Moufang's theorem

is true in a loop Q if $x \cdot (y \cdot z) = (x \cdot y) \cdot z \Rightarrow \langle x, y, z \rangle$ is a group.

The existence of finite basis and Moufang's theorem

Steiner triple systems (STS) and loops

An STS is a system of 3-element subsets (blocks) of a set X; each 2-element subset of X is in exactly one block. Define a loop Q on $X \cup \{1\}$ in such a way that $x \cdot x = 1$, $1 \cdot x = x = x \cdot 1$, while if $x \neq y$ and $1 \notin \{x, y\}$, then $x \cdot y = z$, where $\{x, y, z\}$ is the block containing $\{x, y\}$. Equationally, Steiner loops are the loops with $x \cdot y = y \cdot x$, $x \cdot x = 1$ and $x \cdot (y \cdot z) = y$.

Steiner loop of order 10

Up to $\cong$ there $\exists!$ such Q, given by the STS of affine lines in $\mathbb{F}_3^2$.
Fact: Q is in the variety $\mathcal{V}$ of Steiner loops that fulfil

$$(x \cdot z) \cdot (((x \cdot y) \cdot z) \cdot (y \cdot z)) = ((x \cdot z) \cdot ((x \cdot y) \cdot z)) \cdot (y \cdot z).$$

Problem: Show that $\mathbf{HSP}(Q)$ is not finitely based.

Moufang's theorem

is true in a loop Q if $x \cdot (y \cdot z) = (x \cdot y) \cdot z \Rightarrow \langle x, y, z \rangle$ is a group.
Theorem: The variety $\mathcal{V}$ fulfils Moufang's theorem.

Moufang's theorem and propagating identities

1935 Ruth Moufang: Moufang loops fulfil the Moufang theorem.
2011 Andrew Rajah: Which other loop varieties fulfil Moufang's theorem?
2020 The variety induced by an STS of order 9 (*Aequ. Math.*).

Moufang's theorem and propagating identities

1935 Ruth Moufang: Moufang loops fulfil the Moufang theorem.
2011 Andrew Rajah: Which other loop varieties fulfil Moufang's theorem?
2020 The variety induced by an STS of order 9 (*Aequ. Math.*).

Many varieties fulfil Moufang's theorem

Result: Let $\mathcal{A}$ be a variety of abelian groups. Let $X_1, \dots X_n$ be finite loops that fulfil Moufang's theorem. Suppose that each X_i has this property: every subloop is an abelian group or a simple loop. Then $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{A}$ fulfils Moufang's theorem.

Moufang's theorem and propagating identities

1935 Ruth Moufang: Moufang loops fulfil the Moufang theorem.
2011 Andrew Rajah: Which other loop varieties fulfil Moufang's theorem?
2020 The variety induced by an STS of order 9 (*Aequ. Math.*).

Many varieties fulfil Moufang's theorem

Result: Let $\mathcal{A}$ be a variety of abelian groups. Let $X_1, \ldots X_n$ be finite loops that fulfil Moufang's theorem. Suppose that each X_i has this property: every subloop is an abelian group or a simple loop. Then $\mathbf{HSP}(X_1, \ldots, X_n) \vee \mathcal{A}$ fulfils Moufang's theorem.

Generalization to propagating identities

Let A be an algebra and $\varepsilon(x_1, \ldots, x_n)$ an equation in the signature of A. Say that ε *propagates* in A if this implication holds for all $a_1, \ldots, a_n \in A$: $\varepsilon(a_1, \ldots, a_n) \implies \varepsilon(b_1, \ldots, b_n)$ for any $b_1, \ldots, b_n \in \langle a_1, \ldots, a_n \rangle$.

Moufang's theorem and propagating identities

1935 Ruth Moufang: Moufang loops fulfil the Moufang theorem.
2011 Andrew Rajah: Which other loop varieties fulfil Moufang's theorem?
2020 The variety induced by an STS of order 9 (*Aequ. Math.*).

Many varieties fulfil Moufang's theorem

Result: Let $\mathcal{A}$ be a variety of abelian groups. Let $X_1, \dots X_n$ be finite loops that fulfil Moufang's theorem. Suppose that each X_i has this property: every subloop is an abelian group or a simple loop. Then $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{A}$ fulfils Moufang's theorem.

Generalization to propagating identities

Let A be an algebra and $\varepsilon(x_1, \dots, x_n)$ an equation in the signature of A. Say that ε *propagates* in A if this implication holds for all $a_1, \dots, a_n \in A$: $\varepsilon(a_1, \dots, a_n) \implies \varepsilon(b_1, \dots, b_n)$ for any $b_1, \dots, b_n \in \langle a_1, \dots, a_n \rangle$.

"ε propagates in $\mathcal{V}$" = "ε propagates in every $A \in \mathcal{V}$".

Propagating identities

Equations that propagate in a variety

Result: Let $\mathcal{V}$ be a variety in which there propagates an equation ε. Let $X_1, \dots X_n$ be finite loops in which ε propagates too. Suppose that each X_i has this property: every subloop is in $\mathcal{V}$ or a nonabelian simple loop. Then ε propagates in $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{V}$ too.

Propagating identities

Equations that propagate in a variety

Result: Let $\mathcal{V}$ be a variety in which there propagates an equation ε. Let $X_1, \ldots X_n$ be finite loops in which ε propagates too. Suppose that each X_i has this property: every subloop is in $\mathcal{V}$ or a nonabelian simple loop. Then ε propagates in $\mathbf{HSP}(X_1, \ldots, X_n) \vee \mathcal{V}$ too.

Research suggestion

Transfer the above result to Mal'cev varieties.

Propagating identities

Equations that propagate in a variety

Result: Let $\mathcal{V}$ be a variety in which there propagates an equation ε. Let $X_1, \dots X_n$ be finite loops in which ε propagates too. Suppose that each X_i has this property: every subloop is in $\mathcal{V}$ or a nonabelian simple loop. Then ε propagates in $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{V}$ too.

Research suggestion

Transfer the above result to Maľcev varieties.

Examples of propagating identities in a variety

$xx = x$ in groupoids, commutativity in semigroups, $x^m = 1$ in groups.

Propagating identities

Equations that propagate in a variety

Result: Let $\mathcal{V}$ be a variety in which there propagates an equation ε. Let $X_1, \dots X_n$ be finite loops in which ε propagates too. Suppose that each X_i has this property: every subloop is in $\mathcal{V}$ or a nonabelian simple loop. Then ε propagates in $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{V}$ too.

Research suggestion

Transfer the above result to Mal'cev varieties.

Examples of propagating identities in a variety

$xx = x$ in groupoids, commutativity in semigroups, $x^m = 1$ in groups.

Propagating core of equation ε in variety $\mathcal{V}$

is defined as the class of all $A \in \mathcal{V}$ in which ε propagates. It is a quasivariety.

Propagating identities

Equations that propagate in a variety

Result: Let $\mathcal{V}$ be a variety in which there propagates an equation ε. Let $X_1, \dots X_n$ be finite loops in which ε propagates too. Suppose that each X_i has this property: every subloop is in $\mathcal{V}$ or a nonabelian simple loop. Then ε propagates in $\mathbf{HSP}(X_1, \dots, X_n) \vee \mathcal{V}$ too.

Research suggestion

Transfer the above result to Mal'cev varieties.

Examples of propagating identities in a variety

$xx = x$ in groupoids, commutativity in semigroups, $x^m = 1$ in groups.

Propagating core of equation ε in variety $\mathcal{V}$

is defined as the class of all $A \in \mathcal{V}$ in which ε propagates. It is a quasivariety. But what else?