LOOPS WITH SQUARES IN TWO NUCLEI

Michael Kinyon

CODESCO24, 8 July

The second talk???

There are a couple of disadvantages to being the first *contributed* talk immediately after the first *invited* talk:

The second talk???

There are a couple of disadvantages to being the first *contributed* talk immediately after the first *invited* talk:

- After the first talk, everyone wants coffee, not to hear another talk.

The second talk???

There are a couple of disadvantages to being the first *contributed* talk immediately after the first *invited* talk:

- After the first talk, everyone wants coffee, not to hear another talk.
- Ian is a tough act to follow!

The second talk???

There are a couple of disadvantages to being the first *contributed* talk immediately after the first *invited* talk:

- After the first talk, everyone wants coffee, not to hear another talk.
- Ian is a tough act to follow!

This talk will be algebraic, but I'll try to make it too technical.

Why is an algebraist here?

Question: Why is an algebraist at a combinatorics conference?

Why is an algebraist here?

Question: Why is an algebraist at a combinatorics conference?
Answer:

Quasigroups

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 finite quasigroups = latin squares

Example: $\begin{matrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{matrix}$

Loops

A *loop* is a quasigroup with an identity element $1 \cdot x = x \cdot 1 = x$.

Multiplication tables of loops $=$ reduced Latin squares

Example:

1	2	3	4	5
2	1	4	5	3
3	4	5	1	2
4	5	2	3	1
5	3	1	2	4

This is evidently not a group table. (Exercise)

Multiplication Group

In a 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.

The *multiplication group* of Q is generated by all of these:

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

(Think of the group generated by all rows and all columns of the corresponding latin square.)

Multiplication groups give a lot of information about loops, but do not determine them (e.g. $\mathrm{Mlt}(D_8) \cong \mathrm{Mlt}(Q_8)$).

Normality

An equivalence relation θ on a quasigroup Q is a congruence if and only if its equivalence classes form a block system for $\mathrm{Mlt}(Q)$

Normality

An equivalence relation θ on a quasigroup Q is a congruence if and only if its equivalence classes form a block system for $\mathrm{Mlt}(Q)$

Congruences on a loop Q are determined by *normal subloops*: A subloop $A \subseteq Q$ is a congruence class of the identity element 1 if and only if it is a block of $\mathrm{Mlt}(Q)$ containing 1.

Normality

An equivalence relation θ on a quasigroup Q is a congruence if and only if its equivalence classes form a block system for $\mathrm{Mlt}(Q)$

Congruences on a loop Q are determined by *normal subloops*: A subloop $A \subseteq Q$ is a congruence class of the identity element 1 if and only if it is a block of $\mathrm{Mlt}(Q)$ containing 1.

A useful way of proving normality for a subloop:

If K is a normal subgroup of $\mathrm{Mlt}(Q)$, then $A := 1^K$ is a normal subloop of Q.

(Conversely, every normal subloop is the orbit of 1 for some normal subgroup of $\mathrm{Mlt}(Q)$, but we won't need this.)

Nuclei

The *left, middle* and *right nuclei* of a loop Q are the sets

$$\mathrm{Nuc}_\ell(Q) = \{a \in Q \mid ax \cdot y = a \cdot xy,\ \forall x, y \in Q\}$$
$$\mathrm{Nuc}_m(Q) = \{a \in Q \mid xa \cdot y = x \cdot ay,\ \forall x, y \in Q\}$$
$$\mathrm{Nuc}_r(Q) = \{a \in Q \mid xy \cdot a = x \cdot ya,\ \forall x, y \in Q\}$$

Nuclei

The *left, middle* and *right nuclei* of a loop Q are the sets

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

The *nucleus* is the intersection of these:

$$\mathrm{Nuc}(Q) = \mathrm{Nuc}_\ell(Q) \cap \mathrm{Nuc}_m(Q) \cap \mathrm{Nuc}_r(Q)\,.$$

Each of the three nuclei (and hence the nucleus) is a subloop.

None of the nuclei need be normal, though in "nice" classes of loops, one or more of them often is.

Moufang loops

The best known class of loops are *Moufang loops*. They are defined by any one of the following identities:

$$(xy)(zx) = x((yz)x)$$
$$((xy)x)z = x(y(xz))$$
$$((zx)y)x = z(x(yx))$$

Moufang loops

The best known class of loops are *Moufang loops*. They are defined by any one of the following identities:

$$(xy)(zx) = x((yz)x)$$
$$((xy)x)z = x(y(xz))$$
$$((zx)y)x = z(x(yx))$$

Examples: the nonzero octonions; the sphere S^7 under octonion multiplication.

Moufang loops

The best known class of loops are *Moufang loops*. They are defined by any one of the following identities:

$$(xy)(zx) = x((yz)x)$$
$$((xy)x)z = x(y(xz))$$
$$((zx)y)x = z(x(yx))$$

Examples: the nonzero octonions; the sphere S^7 under octonion multiplication.

Modulo CFSG, finite simple Moufang loops have been classified: they are groups or loops in a particular infinite family.

Moufang loops

The best known class of loops are *Moufang loops*. They are defined by any one of the following identities:

$$(xy)(zx) = x((yz)x)$$
$$((xy)x)z = x(y(xz))$$
$$((zx)y)x = z(x(yx))$$

Examples: the nonzero octonions; the sphere S^7 under octonion multiplication.

Modulo CFSG, finite simple Moufang loops have been classified: they are groups or loops in a particular infinite family.

Moufang loops are often thought of as being the most "group-like" of loops.

Bol loops

The 2nd best known class are *(left) Bol loops*, defined by the following identity:

$$(x(yx))z = x(y(xz))$$

Right Bol loops are defined dually.

Bol loops

The 2nd best known class are *(left) Bol loops*, defined by the following identity:

$$(x(yx))z = x(y(xz))$$

Right Bol loops are defined dually.
Left Bol $+$ right Bol $=$ Moufang.

Bol loops

The 2nd best known class are *(left) Bol loops*, defined by the following identity:

$$(x(yx))z = x(y(xz))$$

Right Bol loops are defined dually.
Left Bol + right Bol = Moufang.

Example: Let $H^+(n, \mathbb{C})$ be the set of $n \times n$ positive definite, hermitian matrices. For $A, B \in H^+(n, \mathbb{C})$, take the polar decomposition of AB:

$$AB = CU$$

where $C \in H^+(n, \mathbb{C})$ and U is unitary. (In fact, $C = (AB^2A)^{1/2}$.)
Define $A * B := C$. Then $(H^+(n, \mathbb{C}), *)$ is a left Bol loop.

Loops of Bol-Moufang type

In 1969, F. Fenyves observed that both Bol loops and Moufang loops were defined by identities with the same characteristics:

- They involve only the multiplication (no divisions).
- Three variables occur on each side of the equality, in the same order.
- One variable occurs twice on each side, the others only once.

Moufang loops: $x((yz)x) = (xy)(zx)$ (and the other 2 equivalent identities)

(left) Bol loops: $(x(yx))z = x(y(xz))$

Loops of Bol-Moufang type

Fenyves decided to classify all such identities, which he referred to as identities of *Bol-Moufang type*, and to determine how many distinct varieties of loops they define.

Loops of Bol-Moufang type

Fenyves decided to classify all such identities, which he referred to as identities of *Bol-Moufang type*, and to determine how many distinct varieties of loops they define.

There are 60 such identities. It turns out that 30 of them are equivalent to associativity; for example, $(xy)(yz) = ((xy)y)z$.

Loops of Bol-Moufang type

Fenyves decided to classify all such identities, which he referred to as identities of *Bol-Moufang type*, and to determine how many distinct varieties of loops they define.

There are 60 such identities. It turns out that 30 of them are equivalent to associativity; for example, $(xy)(yz) = ((xy)y)z$.

In all, there are 14 distinct classes defined by identities of Bol-Moufang type.

Loops of Bol-Moufang type

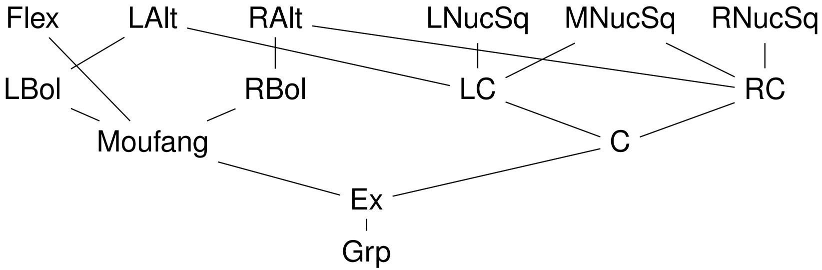
Fenyves decided to classify all such identities, which he referred to as identities of *Bol-Moufang type*, and to determine how many distinct varieties of loops they define.

There are 60 such identities. It turns out that 30 of them are equivalent to associativity; for example, $(xy)(yz) = ((xy)y)z$.

In all, there are 14 distinct classes defined by identities of Bol-Moufang type.

Fenyves completed almost all of the classification; he only missed a few inclusions, and gave very few examples to separate the classes. These holes were later filled in by Phillips and Vojtěchovský (2005).

The 14 varieties



Defining Identities

Flex	$(xy)x = x(yx)$
LAlt	$(xx)y = x(xy)$
RAlt	$(xy)y = x(yy)$
Left Nuclear Squares	$(xx)(yz) = ((xx)y)z$
Middle Nuclear Squares	$(x(yy)z) = x((yy)z)$
Right Nuclear Squares	$(xy)(zz) = x(y(zz))$
Left Bol	$(x(yx))z = x(y(xz))$
Right Bol	$((xy)z)y = x((yz)y)$
Left C	$(xx)(yz) = (x(xy))z$
Right C	$(xy)(zz) = x((yz)z)$
Moufang	$(xy)(zx) = x((yz)x)$
C	$((xy)y)z = x(y(yz))$
Extra	$((xy)z)x = x(y(zx))$
Groups	$(xy)z = x(yz)$

Comments

- The strange names "extra" and "C" are due to Fenyves. No one knows exactly why he chose them.
- One guess is that he thought of "extra loops" as Moufang loops satisfying an "extra" condition (nuclear squares).
- It has been speculated that the somewhat uninspiring "C" is supposed to mean "central" (in the sense of middle, not in any algebraic sense), but as with "extra," there is no direct evidence in Fenyves' paper that this is what he had in mind.
- Anyway, there has been enough literature on these loops that we are stuck with the names.

Normality of nuclei

Variety	Coinciding	normal?	who?
Moufang	$\ell = m = r$	yes	R.H. Bruck
right Bol	$m = r$	yes	D.A. Robinson
left Bol	$\ell = m$	yes	dual
C	$\ell = m = r$	yes	Phillips-Vojtěchovský
left C	$\ell = m$	yes	Phillips, Drápal-Kinyon
right C	$m = r$	yes	dual

Normality of nuclei

Variety	Coinciding	normal?	who?
Moufang	$\ell = m = r$	yes	R.H. Bruck
right Bol	$m = r$	yes	D.A. Robinson
left Bol	$\ell = m$	yes	dual
C	$\ell = m = r$	yes	Phillips-Vojtěchovský
left C	$\ell = m$	yes	Phillips, Drápal-Kinyon
right C	$m = r$	yes	dual

For the flexible, left alternative or right alternative varieties, nothing can be said. By themselves (or even together), they don't have enough structure to prove anything interesting.

Normality of nuclei

Variety	Coinciding	normal?	who?
Moufang	$\ell = m = r$	yes	R.H. Bruck
right Bol	$m = r$	yes	D.A. Robinson
left Bol	$\ell = m$	yes	dual
C	$\ell = m = r$	yes	Phillips-Vojtěchovský
left C	$\ell = m$	yes	Phillips, Drápal-Kinyon
right C	$m = r$	yes	dual

For the flexible, left alternative or right alternative varieties, nothing can be said. By themselves (or even together), they don't have enough structure to prove anything interesting.

What about left, middle or right nuclear squares? Again, each one alone has almost no structure. However...

Main Result

Let

$$\mathrm{Nuc}_{\ell,m}(Q) := \mathrm{Nuc}_{\ell}(Q) \cap \mathrm{Nuc}_{m}(Q)$$
$$G := \{L_a \mid a \in \mathrm{Nuc}_{\ell,m}(Q)\}$$

Theorem

Let Q be a loop with left and middle nuclear squares. Then:

1. *G is a normal subgroup of $\mathrm{Mlt}(Q)$;*
2. *$\mathrm{Nuc}_{\ell,m}(Q)$ is a normal subloop of Q.*

Also true for:

- Loops with *middle and right* nuclear squares (duality)
- Loops with *left and right* nuclear squares (paratopy)

Consequence

Corollary

If Q is a loop with left and middle nuclear squares, then $Q/\mathrm{Nuc}_{\ell,m}(Q)$ has exponent 2 ($x^2 = 1$).

Corollary

A simple loop with left and middle nuclear squares is a group or a loop of exponent 2.

What is needed

If $a \in \mathrm{Nuc}_{\ell,m}(Q)$, then for all $x \in Q$, $L_a R_x = R_x L_a$.

Thus to show $L_{(\mathrm{Nuc}_{\ell,m}(Q))}$ is normal in $\mathrm{Mlt}(Q)$, it is enough to show that it is normalized by each left translation L_x.

In other words, we must show that for all $x \in Q$,

$$L_x L_a L_x^{-1} = L_{(xa)/x}$$
$$L_x^{-1} L_a L_x = L_{x\backslash(ax)}$$

and that $(xa)/x,\ x\backslash(ax) \in \mathrm{Nuc}_{\ell,m}(Q)$.

What is needed

If $a \in \mathrm{Nuc}_{\ell,m}(Q)$, then for all $x \in Q$, $L_a R_x = R_x L_a$.

Thus to show $L_{(\mathrm{Nuc}_{\ell,m}(Q))}$ is normal in $\mathrm{Mlt}(Q)$, it is enough to show that it is normalized by each left translation L_x.

In other words, we must show that for all $x \in Q$,

$$L_x L_a L_x^{-1} = L_{(xa)/x}$$
$$L_x^{-1} L_a L_x = L_{x\backslash(ax)}$$

and that $(xa)/x,\ x\backslash(ax) \in \mathrm{Nuc}_{\ell,m}(Q)$.

This is a purely equational problem! Let us not waste our precious brain cells on it.

Prover9

```
% loop
1 * x = x. x * 1 = x.
(x * y) / y = x. (x / y) * y = x.
x \ (x * y) = y. x * (x \ y) = y.

% left & middle nuclear squares
((x * x) * y) * z = (x * x) * (y * z).
(x * (y * y)) * z = x * ((y * y) * z).

% a in left & middle nucleus
(a * x) * y = a * (x * y).
(x * a) * y = x * (a * y).

% goals
x \ (a * (x * y)) = (x \ (a * x)) * y.
x * (a * (x \ y)) = ((x * a) / x) * y.
```

Success! (But then what?)

There are different attitudes about how to react once an automated theorem prover succeeds in finding a proof:

- Archiving the proof is enough.
- One should humanize the proof.

Success! (But then what?)

There are different attitudes about how to react once an automated theorem prover succeeds in finding a proof:

- Archiving the proof is enough.
- One should humanize the proof.

I come down somewhere between these. For very long proofs, the Law of Diminishing Returns kicks in as to whether or not humanization is worthwhile. Otherwise it is worth trying.

Success! (But then what?)

There are different attitudes about how to react once an automated theorem prover succeeds in finding a proof:

- Archiving the proof is enough.
- One should humanize the proof.

I come down somewhere between these. For very long proofs, the Law of Diminishing Returns kicks in as to whether or not humanization is worthwhile. Otherwise it is worth trying.

“Humanization” does not just mean doing a line-by-line literal translation of the proof. It means writing a proof for human consumption that uses existing theory to simplify steps and then identifies new key steps.

Success! (But then what?)

There are different attitudes about how to react once an automated theorem prover succeeds in finding a proof:

- Archiving the proof is enough.
- One should humanize the proof.

I come down somewhere between these. For very long proofs, the Law of Diminishing Returns kicks in as to whether or not humanization is worthwhile. Otherwise it is worth trying.

"Humanization" does not just mean doing a line-by-line literal translation of the proof. It means writing a proof for human consumption that uses existing theory to simplify steps and then identifies new key steps.

In this case, the Prover9 proofs were reasonably short (a few hundred steps), so it was straightforward to humanize them.

Loops with central squares

Finally, consider loops with *central* squares: Nuclear squares + commuting squares: $x^2y = yx^2$.

Loops with central squares

Finally, consider loops with *central* squares: Nuclear squares + commuting squares: $x^2y = yx^2$.

Such loops are *power-associative*, that is, each 1-generated subloop is a group. Informally, powers of elements are unambiguous.

Loops with central squares

Finally, consider loops with *central* squares: Nuclear squares + commuting squares: $x^2y = yx^2$.

Such loops are *power-associative*, that is, each 1-generated subloop is a group. Informally, powers of elements are unambiguous.

Lemma

The following are equivalent in a loop with central squares:

- *Automorphic inverse property (AIP):* $(xy)^{-1} = x^{-1}y^{-1}$;
- *Endomorphic squaring (ES):* $(xy)^2 = x^2y^2$.

Decomposition

Theorem

Let Q be a loop with squares in two nuclei. If Q has AIP or ES, then it has central squares (hence both AIP and ES).

Theorem

Let Q be a finite loop with squares in two nuclei and AIP/ES. Then

$$Q \cong E \times O$$

where

- *E is a loop in which every element has order a power of 2, and*
- *O is a loop of odd order.*

Now let's have coffee!