

AND NOW FOR SOMETHING COMPLETELY DIFFERENT



LOOPS, QUASIGROUPS AND AUTOMATED REASONING

Michael K. Kinyon

Department of Mathematics



Kunen Fest

University of Wisconsin, 4 April 2009

Dedicated to ...



Ken Kunen, Loop Theorist

Dedicated to ...



Ken Kunen, Loop Theorist
(Occasionally dabbles in set theory and topology)

Although Ken was by no means the first to prove interesting results in algebra using the tools of automated deduction, his approach to problems in loop theory revolutionized the field.

Main Tools

At the time:

- McCune's OTTER, an automated deduction tool
- Zhang's SEM, a finite model builder

Main Tools

At the time:

- McCune's OTTER, an automated deduction tool
- Zhang's SEM, a finite model builder

Nowadays:

- McCune's PROVER9
- McCune's MACE4

Groups of exponent 4

Theorem

Each of the following is a shortest single axiom for groups of exponent 4:

- $y((y((yy)(xz)))(z(zz))) = x.$
- $((yy)y)(((y(xz))(zz))z) = x.$
- $(y((((yy)y)(xz))z))(zz) = x.$

Here “shortest” means with respect to the number of variable occurrences.

The Shortest Single Axioms for Groups of Exponent 4
Computers and Mathematics and Applications, **29** (1995), 1-12.

The Humanization Dogma

In

Single Axioms for Odd Exponent Groups, *J. Automated Reasoning* **14** (1995), 383-412,

Ken and Joan Hart found general schema that provide shortest single axioms.

Significantly, we find:

“We . . . found that by examining the output from our assistant, we could provide conceptual proofs that a human could also understand.”

Hints of Nonassociativity

In the same paper, to show that candidate axioms must have at least three variables, Ken and Joan constructed examples of structures which are not associative but in which every equation valid in groups and containing two or fewer variables is true.

(More on that in a bit.)

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

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

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

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

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

Multiplication tables of quasigroups = Latin squares

Example:

1	3	2
3	2	1
2	1	3

Universal algebra definition

A *quasigroup* $(Q, \cdot, \backslash, /)$ is a set Q with three binary operations $\cdot, \backslash, /$ such that for all $x, y \in Q$:

$$x \backslash (xy) = y$$

$$x(x \backslash y) = y$$

$$(xy) / y = x$$

$$(x / y)y = x$$

Thus loops form a *variety* (in the universal algebra sense).

Universal algebra definition

A *quasigroup* $(Q, \cdot, \backslash, /)$ is a set Q with three binary operations $\cdot, \backslash, /$ such that for all $x, y \in Q$:

$$x \backslash (xy) = y$$

$$x(x \backslash y) = y$$

$$(xy) / y = x$$

$$(x / y)y = x$$

Thus loops form a *variety* (in the universal algebra sense).

The universal algebra definition is better suited to automated deduction.

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 Albert.

Loops

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

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

The term “loop” is due to Albert.

Loop has a very specific meaning to those from Chicago.

Loops

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

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

The term “loop” is due to Albert.

Loop has a very specific meaning to those from Chicago.

German: *Die Loop*

Russian: *Lupa*

Loops

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

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

The term “loop” is due to Albert.

Loop has a very specific meaning to those from Chicago.

German: *Die Loop*

Russian: *Lupa*

French: *La Boucle* (???)

A familiar example

Think of $x \setminus x$ as a “local right identity at x ”.

Think of x / x as a “local left identity at x ”.

Proposition

Every associative quasigroup is a group.

Proof.

$xy = x(x \setminus x)y$, so $y = (x \setminus x)y$, so $x \setminus x = y / y$. □

What are *Moufang loops*?

What are *Moufang loops*?

First, who was Moufang?

Ruth Moufang (1905 - 1977)



- 1931: Ph.D, projective geometry, advisor: Max Dehn
- 1931-1937: studied (what we now call) Moufang planes and Moufang loops
- 1937: Bernhard Rust forbade her from teaching; became an industrial mathematician (elasticity theory)
- 1946: Taught at Frankfurt, eventually becoming professor

Definition

A *Moufang loop* is a loop satisfying any, *and hence all*, of the following identities:

$$x(y(xz)) = ((xy)x)z \qquad ((zx)y)x = z(x(yx))$$

$$x((yz)x) = (xy)(zx) \qquad (x(yz))x = (xy)(zx)$$

Definition

A *Moufang loop* is a loop satisfying any, *and hence all*, of the following identities:

$$x(y(xz)) = ((xy)x)z \qquad ((zx)y)x = z(x(yx))$$

$$x((yz)x) = (xy)(zx) \qquad (x(yz))x = (xy)(zx)$$

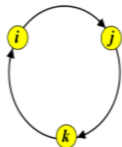
A point we will come back to:

These identities are equivalent in loops.

Example: Octonions

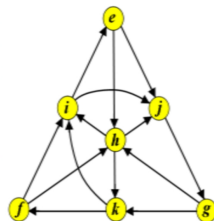
	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

The Quaternions



	1	i	j	k	e	f	g	h
1	1	i	j	k	e	f	g	h
i	i	-1	k	$-j$	f	$-e$	h	$-g$
j	j	$-k$	-1	i	$-g$	h	e	$-f$
k	k	j	$-i$	-1	h	g	$-f$	$-e$
e	e	$-f$	g	$-h$	-1	i	$-j$	k
f	f	e	$-h$	$-g$	$-i$	-1	k	j
g	g	$-h$	$-e$	f	j	$-k$	-1	i
h	h	g	f	e	$-k$	$-j$	$-i$	-1

The Octonions



The nonzero octonions form a Moufang loop.

Moufang's Theorem

A loop is *diassociative* if every subloop which can be generated by no more than two elements is associative.

Theorem

In a Moufang loop, any three elements which associate generate a group.

Corollary

Every Moufang loop is diassociative.

Moufang quasigroups

Moufang Quasigroups, *J. Algebra* **183** (1996) 231-234.

Theorem

A quasigroup satisfying any one of the Moufang identities is a loop.

Corollary

The four Moufang identities are equivalent in quasigroups.

Inner Mappings

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

$$L_x : Q \rightarrow Q; \quad yL_x = xy \quad R_x : Q \rightarrow Q; \quad yR_x = yx$$

are permutations.

Various permutation groups act on loops:

- The *multiplication group* $Mlt Q = \langle L_x, R_x \mid x \in Q \rangle$
- The *inner mapping group* $Inn Q = (Mlt Q)_1$
(stabilizer of $1 \in Q$)
- The *automorphism group* $Aut Q$

Bruck and Paige

Definition

A loop is *automorphic* (or an *A-loop*, for short) if $\text{Inn } Q \leq \text{Aut } Q$.

These were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms,
Ann. of Math. (2) **63** (1956), 308–323.

Bruck and Paige

Definition

A loop is *automorphic* (or an *A-loop*, for short) if $\text{Inn } Q \leq \text{Aut } Q$.

These were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms,
Ann. of Math. (2) **63** (1956), 308–323.

- Bruck's interest: Commutative Moufang loops are A-loops. How much of their structure comes from that fact?

Bruck and Paige

Definition

A loop is *automorphic* (or an *A-loop*, for short) if $\text{Inn } Q \leq \text{Aut } Q$.

These were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms,
Ann. of Math. (2) **63** (1956), 308–323.

- Bruck's interest: Commutative Moufang loops are A-loops. How much of their structure comes from that fact?
- Paige's interest: he was Bruck's student.

Basic results

Already known: For a loop Q , $\text{Inn } Q$ has a set of canonical generators:

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

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

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

Basic results

Already known: For a loop Q , $\text{Inn } Q$ has a set of canonical generators:

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

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

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

Thus the A-loop condition $\text{Inn } Q \leq \text{Aut } Q$ can be expressed as three universally quantified equations.

Basic results

Already known: For a loop Q , $\text{Inn } Q$ has a set of canonical generators:

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

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

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

Thus the A-loop condition $\text{Inn } Q \leq \text{Aut } Q$ can be expressed as three universally quantified equations. Thus A-loops form a variety, and therefore are closed under taking subloops, direct products, and homomorphic images.

B & P's Main Question

Recall that a loop is *diassociative* if for each x, y , $\langle x, y \rangle$ is a group.

B & P's Main Question

Recall that a loop is *diassociative* if for each x, y , $\langle x, y \rangle$ is a group.

B & P's Question: *Is every diassociative A-loop Moufang?*

The commutative case

Osborn gave an affirmative answer in the commutative case in

A theorem on A-loops,
Proc. Amer. Math. Soc. **9** (1958), 347–349.

The proof is a triumph of human-generated formal reasoning.

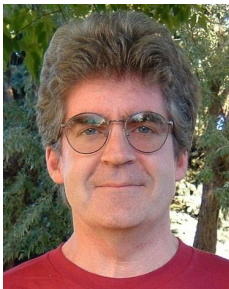
By the way . . .

The variety of *all* diassociative loops is not finitely based.
(Kowalszki, 2008)

However, within A-loops, diassociativity is finitely based, *e.g.*,
by the *alternative laws*:

$$(xx)y = x(xy) \quad (xy)y = x(yy).$$

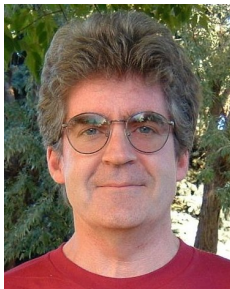
Interlude



J.D. Phillips



Interlude

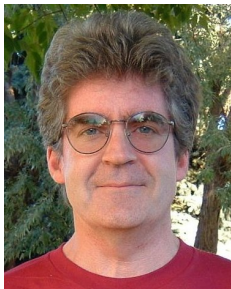


J.D. Phillips



Here's a good
problem

Interlude



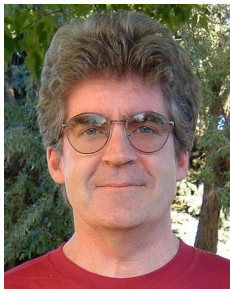
OK, let's try it.

J.D. Phillips



Here's a good
problem

Interlude

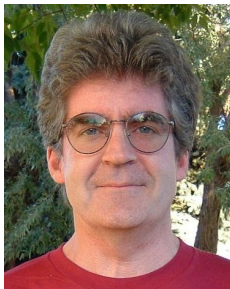


blah Moufang
loops blahblah

J.D. Phillips



Interlude

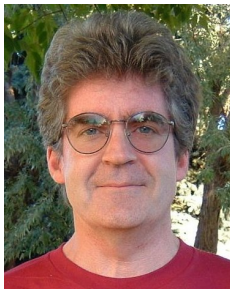


J.D. Phillips



blahblah inner
mappings blah

Interlude

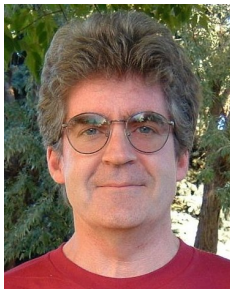


Now what?

J.D. Phillips



Interlude



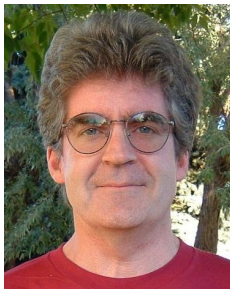
Now what?



J.D. Phillips

I dunno

Interlude



Hala Pflugfelder

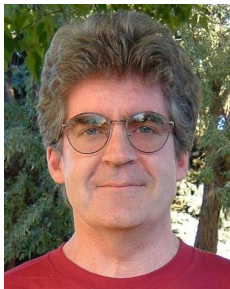


Why don't you boys
ask Ken Kunen?

J.D. Phillips



Interlude



Who?

Hala Pflugfelder

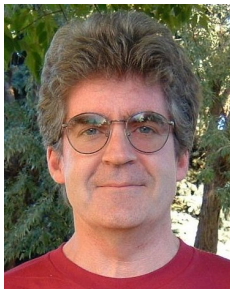


Why don't you boys
ask Ken Kunen?

J.D. Phillips



Interlude



Who?

Hala Pflugfelder



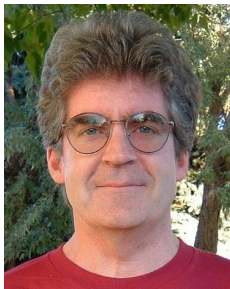
Why don't you boys
ask Ken Kunen?

J.D. Phillips



The set theorist?

Interlude



Hala Pflugfelder

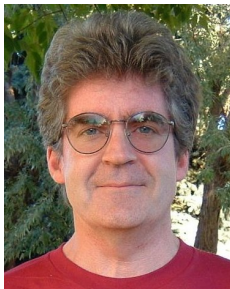


J.D. Phillips



He proves theorems
about loops using
computers

Interlude



Uh, OK

Hala Pflugfelder

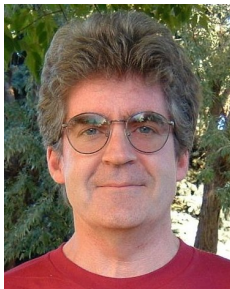


He proves theorems
about loops using
computers

J.D. Phillips



Interlude



Uh, OK

Hala Pflugfelder



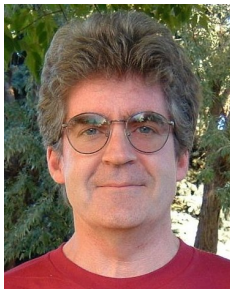
He proves theorems
about loops using
computers

J.D. Phillips



It's worth a shot

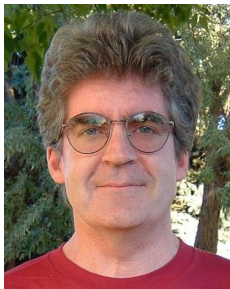
Interlude



J.D. Phillips



Interlude

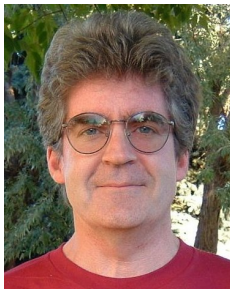


Look at this,
Prof. Kunen



J.D. Phillips

Interlude



Look at this,
Prof. Kunen

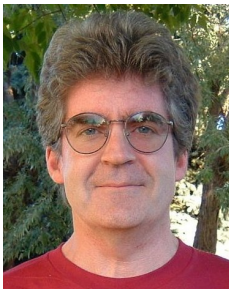


Interesting. . .

J.D. Phillips



Interlude

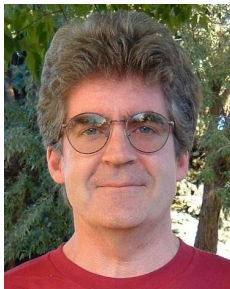


J.D. Phillips



Now what?

Interlude



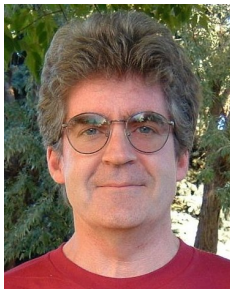
Now we wait.

J.D. Phillips



Now what?

Interlude

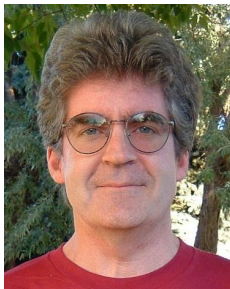


J.D. Phillips



Can we call him
“Ken”?

Interlude



Not yet.

J.D. Phillips



Can we call him
“Ken”?

A few days later

To: Michael Kinyon, J.D. Phillips

A few days later

To: Michael Kinyon, J.D. Phillips

From: Ken Kunen

A few days later

To: Michael Kinyon, J.D. Phillips

From: Ken Kunen

Subject: an ugly proof

A few days later

To: Michael Kinyon, J.D. Phillips

From: Ken Kunen

Subject: an ugly proof

Dear Michael and J.D.,

A few days later

To: Michael Kinyon, J.D. Phillips

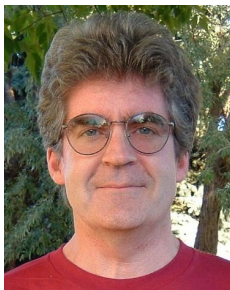
From: Ken Kunen

Subject: an ugly proof

Dear Michael and J.D.,

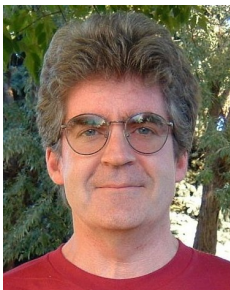
And so began the **KKP** collaboration...

The Next Step



What do we do?

The Next Step

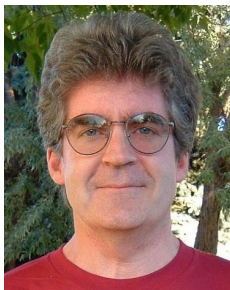


No, we translate it!



Write a paper saying
OTTER proved it?

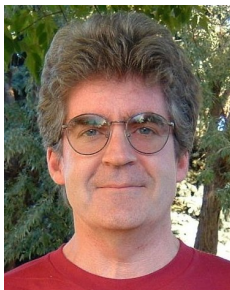
The Next Step



Blahblahblah



The Next Step



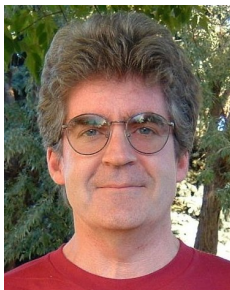
Blahblahblah



Blahblahblah



The Next Step



Blahblahblah



Blahblahblah



Here it is, guys

The Next Step II

Ken and I started from the beginning of the proof and worked forward.

The Next Step II

Ken and I started from the beginning of the proof and worked forward.

J.D. started from the back and worked backward.

The Next Step II

Ken and I started from the beginning of the proof and worked forward.

J.D. started from the back and worked backward.

The (in retrospect) obvious advantage of this approach is that one will usually reach “obvious” facts before reaching the beginning.

The published version

Every diassociative A-loop is Moufang,
Proc. Amer. Math. Soc. **130** (2002), 619–624.

The published version

Every diassociative A-loop is Moufang,
Proc. Amer. Math. Soc. **130** (2002), 619–624.

The paper was accepted in 2000 about a week after we submitted it.

The published version

Every diassociative A-loop is Moufang,
Proc. Amer. Math. Soc. **130** (2002), 619–624.

The paper was accepted in 2000 about a week after we submitted it.

There is a key step in the proof that, although understandable, it is difficult to imagine a human discovering.

Commutative A-loops

Recently, Jedlička, Vojtěchovský and I have found a good structure theory for *commutative* A-loops:

- Lagrange Theorem
- Sylow Existence Theorem
- Every finite commutative A-loop is a direct product of a loop of odd order and a loop of order a power of 2.

Again, what got the whole ball rolling was a lemma obtained using Prover9.

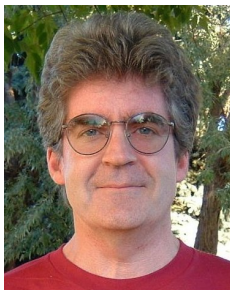
General case

Ken probably does not recall this, but his name is on a draft of a paper with the following as the main result:

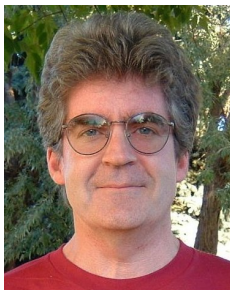
Theorem

Every A-loop of odd order is solvable.

Afterglow

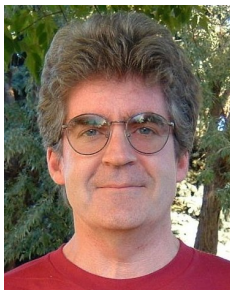


Afterglow



Do you guys have
other good problems?

Afterglow



Do you guys have
other good problems?



Well, I have one

RIF loops

A loop is *RIF* (**R**espects **I**nverses and **F**lexible) if the following hold:

- *Inverse property*: $x^{-1}(xy) = (yx)x^{-1} = y$
- *Flexible*: $(xy)x = x(yx)$
- *Inner mappings respect inverses*: $(x^{-1})h = (xh)^{-1}$ for all $h \in \text{Inn } Q$

Ex: Every Moufang loop is RIF.

Generalizing Moufang's theorem

A generalization of Moufang and Steiner loops, *Algebra Universalis* **48** (2002), 81-101.

Theorem

Every RIF loop is diassociative.

Generalizing Moufang's theorem

A generalization of Moufang and Steiner loops, *Algebra Universalis* **48** (2002), 81-101.

Theorem

Every RIF loop is diassociative.

The proof involves a a complicated induction. We did *not* use OTTER. Rather, we used OTTER to check many special cases until we saw the pattern of the proof.

More recently, Vojtěchovský and I found a nice structure theory for *commutative* RIF loops.

Theorem

Every finite commutative RIF loop is a direct product of a commutative Moufang 3-loop, a C 2-loop, and an abelian group of order prime to 6.

Once again, the main discovery tool was Prover9.

Definition

A loop is said to be *conjugacy closed* (or just CC) if for all x, y , $L_x L_y L_x^{-1}$ is a left translation and $R_x R_y R_x^{-1}$ is a right translation.

Definition

A loop is said to be *conjugacy closed* (or just CC) if for all x, y , $L_x L_y L_x^{-1}$ is a left translation and $R_x R_y R_x^{-1}$ is a right translation.

These were introduced independently by Goodaire and Robinson, and Soikis. The smallest nonassociative example has order 6.

Definition

A loop is said to be *conjugacy closed* (or just CC) if for all x, y , $L_x L_y L_x^{-1}$ is a left translation and $R_x R_y R_x^{-1}$ is a right translation.

These were introduced independently by Goodaire and Robinson, and Soikis. The smallest nonassociative example has order 6.

Ken wrote a solo paper about them:

The structure of conjugacy closed loops, Trans. Amer. Math. Soc. **352** (2000), 2889–2911.

Main Problem

The *nucleus* of a loop is the set of all elements that associate with everything:

$$N := \{a \mid (ax)y = a(xy), (xa)y = x(ay), (xy)a = x(ya) \quad \forall x, y\}$$

This is *normal* in a CC-loop.

Main Problem

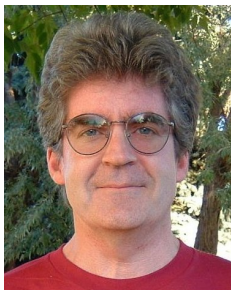
The *nucleus* of a loop is the set of all elements that associate with everything:

$$N := \{a \mid (ax)y = a(xy), (xa)y = x(ay), (xy)a = x(ya) \quad \forall x, y\}$$

This is *normal* in a CC-loop.

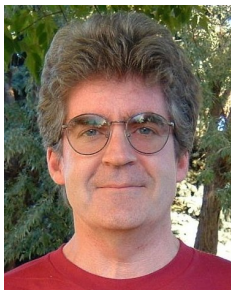
The main problem (posed by Goodaire and Robinson) was: *in a CC-loop Q , is Q/N an abelian group?*

Reading Russian



Hey, look at this!

Reading Russian



Hey, look at this!

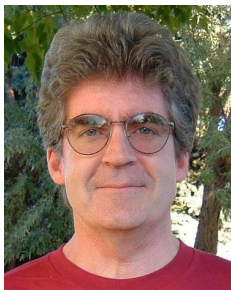


What?



What?

Reading Russian



This guy solved it
years ago!



Reading Russian



This guy solved it
years ago!



Let me check



Basarab's theorem

And indeed, so it had by A.S. Basarab (published obscurely).
The result is now known as *Basarab's theorem*.

Basarab's theorem

And indeed, so it had by A.S. Basarab (published obscurely).
The result is now known as *Basarab's theorem*.

It is a *very* difficult problem for automated deduction tools. I gave it is a challenge to an expert, Bob Veroff. It took him several days, using advanced techniques.

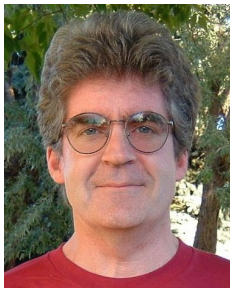
Making hay

Ken, J.D. and I exploited Basarab's theorem in

Diassociativity in conjugacy closed loops, *Comm Algebra* **32**
(2004) 767–786.

In re the title: our main results were descriptions of what types
of elements x, y have the property that $\langle x, y \rangle$ are groups.

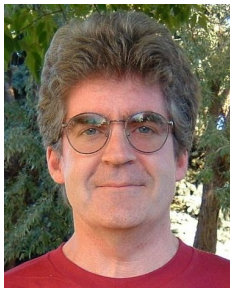
KKP — P



We don't need him!



KKP — P



We don't need him!



Now, now

More CC stuff

Ken and I wrote a couple of other papers on CC-loops:

The structure of extra loops, *Quasigroups and Related Systems* **12** (2004) 39–60.

Extra loops are both Moufang and CC. Main results: Sylow theorems, Hall theorems, constructions.

Power-associative, conjugacy closed Loops, *J. Algebra* **304** (2006) 679–711

Power-associative means each $\langle x \rangle$ is a group. Main results: each twelfth power lies in the nucleus; classifications.

Other papers

Solo:

Quasigroups, loops, and associative laws, *J. Algebra* **185** (1996) 194-204.

Alternative loop rings, *Comm. Algebra* **26** (1998) 557-564.

KKP or KK:

Universally and semi-universally flexible loops, preprint.
(Missing an example.)

Conjugacy closed loops of small order, languishing. (Mutual laziness, I guess.)

Ken's legacy

Ken introduced into quasigroup and loop theory a new methodological paradigm: not only can and should we use automated deduction tools to assist us, but we should also work to understand what those tools tell us. For this, the field owes Ken a great debt.

Enjoy your “change of employment status”, Ken!

Enjoy your “change of employment status”, Ken!

Thank you all for listening.