Using automated reasoning in universal algebra: Several examples

David Stanovský

Charles University in Prague
Czech Republic

stanovsk@karlin.mff.cuni.cz
http://www.karlin.mff.cuni.cz/~stanovsk

University of New Mexico, Albuquerque
ADAM 2007

The ways I use AR tools

- Produce a solution, translate the result *(Ježek-Kepka problem)*
- Produce a solution, look at hints, find a better proof by hand *(Biquandles, Complex Condition)*
- Exhaustive search for a solution *(Linear theories)*
- Checking conjectures on small models *(very very often)*

Ježek-Kepka problem

In groupoids, the identities

$$x * yz = xy * xz, \quad xy * z = xz * yz$$

imply the identities

$$(xy * zu) * ((xy * zu) * (xz * yu)) = xz * yu$$

$$(xy * zu) * (xz * yu) = (xz * yu) * (xy * zu)$$

Ježek-Kepka problem

In groupoids, the identities

$$x * yz = xy * xz, \quad xy * z = xz * yz$$

imply the identities

$$(xy * zu) * ((xy * zu) * (xz * yu)) = xz * yu$$

$$(xy * zu) * (xz * yu) = (xz * yu) * (xy * zu)$$

- first shown by J. Ježek and T. Kepka using infinite mathematics in early 1980's
- they immediately asked, to find an elementary proof

Ježek-Kepka problem

Use of AR:

- in fall 2005 solved by people around Otter
- being unaware of it, I obtained and *translated* another proof with Prover9 in fall 2006.

Ježek-Kepka problem

Use of AR:

- in fall 2005 solved by people around Otter
- being unaware of it, I obtained and *translated* another proof with Prover9 in fall 2006.

Proof found using Prover9 in the *autonomous mode*.

axioms $\Rightarrow$ (2): *30 hours*, length 152, level 24, max. clause wt. 45
axioms $\Rightarrow$ (1): *5 minutes*, length 26, level 12, max. clause wt. 41
ax., (1) $\Rightarrow$ (2): *5 seconds*, length 25, level 11, max. clause wt. 47

The proof of (1) was translated almost literally.
The rest was divided into several lemmas, thus made it quite readable.

Biquandles

... one of the "simplify axioms" tasks

A *birack* is an algebra $(A, \circ, *, \backslash_\circ, \backslash_*)$ satisfying

$$x \circ (y \circ z) = (x \circ y) \circ ((y * x) \circ z)$$

$$x * (y * z) = (x * y) * ((y \circ x) * z)$$

$$((x * y) \circ z) * (y \circ x) = ((x \circ z) * y) \circ (z * x)$$

$$x \circ (x \backslash_\circ y) = y, \quad x \backslash_\circ (x \circ y) = y$$

$$x * (x \backslash_* y) = y, \quad x \backslash_* (x * y) = y$$

In every birack,

$$(x \backslash_\circ x) \backslash_* (x \backslash_\circ x) = x \quad \Leftrightarrow \quad (x \backslash_* x) \backslash_\circ (x \backslash_* x) = x.$$

Biquandles

Use of AR:

Otter in the autonomous mode found a proof within a minute.

Looking at the proof, I started to understand the identities and produced a different (shorter, perhaps more natural) proof.

Complex condition vs. mediality

I omit the semantical meaning ...

... the syntactical problem is as follows:

In an idempotent groupoid with terms t, s such that

$$(x * y) * (u * v) = t(x, u) * s(y, v),$$

is it true that

$$(x * y) * (u * v) = (x * u) * (y * v) \ ?$$

Complex condition vs. mediality

I omit the semantical meaning ...
... the syntactical problem is as follows:

In an idempotent groupoid with terms t, s such that

$$(x * y) * (u * v) = t(x, u) * s(y, v),$$

is it true that

$$(x * y) * (u * v) = (x * u) * (y * v) \ ?$$

(Does not hold for non-idempotent groupoids.)

Complex condition vs. mediality

$$(x * y) * (u * v) = t(x, u) * s(y, v)$$

$$\Downarrow \;?$$

$$(x * y) * (u * v) = (x * u) * (y * v)$$

Use of AR:

- testing various particular cases, like $t = x$ (or y, xy, yx, ...) and few term properties for s

Complex condition vs. mediality

$$(x * y) * (u * v) = t(x, u) * s(y, v)$$

$$\Downarrow \ ?$$

$$(x * y) * (u * v) = (x * u) * (y * v)$$

Use of AR:

- testing various particular cases, like $t = x$ (or y, xy, yx, ...) and few term properties for s
- getting insight enough to prove the following: *If t or s is linear, then the conclusion holds.*

Linear theories of groupoids

Problem. Describe **-linear theories* = equational theories where every term is equivalent to a unique *linear* term.

Linear theories of groupoids

Problem. Describe **-linear theories* = equational theories where every term is equivalent to a unique *linear* term.

Linear term = each variable at most once

- 1 variable: x
- 2 variables: x, y, xy, yx
- 3 variables: $x, y, z,\ xy, yx, xz, zx, yz, zy,\ x(yz), (xy)z, \dots$

Linear theories of groupoids

Problem. Describe **-linear theories* = equational theories where every term is equivalent to a unique *linear* term.

Linear term = each variable at most once

- 1 variable: x
- 2 variables: x, y, xy, yx
- 3 variables: $x, y, z,\ xy, yx, xz, zx, yz, zy,\ x(yz), (xy)z, \dots$

Auxilliary problem. Describe *n-linear theories* = every term *in* $\leq$ *n variables* is equivalent to a unique linear term.

Determined by its n-generated free groupoid.

Linear theories of groupoids

In search for **-linear theories*, we did the following:

1. Found all *2-linear* and *3-linear* theories.
2. Proved that only 3 of them can be extended to a *4-linear* one.

Linear theories of groupoids

In search for **-linear theories*, we did the following:

1. Found all *2-linear* and *3-linear* theories.
2. Proved that only 3 of them can be extended to a *4-linear* one.
3. *-linear theory is generated by its 4-generated free groupoid.
4. Each of the remaining three 3-linear theories extends to at most one *-linear theory.

Linear theories of groupoids

In search for **-linear theories*, we did the following:

1. Found all *2-linear* and *3-linear* theories.
2. Proved that only 3 of them can be extended to a *4-linear* one.
3. *-linear theory is generated by its 4-generated free groupoid.
4. Each of the remaining three 3-linear theories extends to at most one *-linear theory.
5. Explicit construction of the three **-linear* theories.

Linear theories of groupoids

In search for **-linear theories*, we did the following:

1. Found all *2-linear* and *3-linear* theories.
2. Proved that only 3 of them can be extended to a *4-linear* one.
3. *-linear theory is generated by its 4-generated free groupoid.
4. Each of the remaining three 3-linear theories extends to at most one *-linear theory.
5. Explicit construction of the three **-linear* theories.

Use of AR:

Steps 1. and 2. can be done automatically.

Linear theories of groupoids

Facts:

- Sizes of free groupoids: 1, 4, 21, 184.
- About $1/(\#\text{ of vars.})$ of the multiplication table determines the free groupoid.
- n-generated = extension of $(n-1)$-generated.

Linear theories of groupoids

Facts:

- Sizes of free groupoids: 1, 4, 21, 184.
- About $1/(\#\text{ of vars.})$ of the multiplication table determines the free groupoid.
- n-generated = extension of $(n-1)$-generated.

Solution:

- A Perl script prepares all possible completions of the multiplication table.
- For each of them, Otter checks whether the corresponding theory collapses different linear terms.

Linear theories

Results:

- 2-generated free groupoids appeared earlier in literature.
- It took about *one minute* to compute them.
- It took *several days* to one of my coauthors to find the free 3-generated groupoids by hand.
- It took about *two hours* to compute them.
- It wasn't difficult to prove by hand that 4 out of 7 free 3-generated groupoids don't have 4-linear extension.
- It took *several weeks* to compute this fact.

Conclusions

... too early to make any conclusions

When AR tools can outperform mathematician's brain:

- "unnatural conditions"
  - out of classical algebra
  - operators
  - not-really-well-understood equations
- find complicated syntactic proofs
- quickly find small models, without their real understanding

References

D. Stanovský, *An elementary proof for a problem of Ježek-Kepka*, 2007.

D. Stanovský, *On axioms of biquandles*, J. Knot Th. Ramifications 15/7 (2006) 931–933.

K. Adaricheva, A. Pilitowska, D. Stanovský, *On complex algebras of subalgebras*, 2005.

P. Djapić, J. Ježek, P. Marković, R. McKenzie, D. Stanovský, $*$*-linear equational theories of groupoids*, to appear in Algebra Universalis.

http://www.karlin.mff.cuni.cz/~stanovsk