Theory exploration for working algebraists

David Stanovský

Charles University in Prague
Czech Republic

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

Automatheo Workshop, July 2010
Automated reasoning in algebraic research

Current state:
- first order ATP
  - problems in a small theory, mostly equational problems
  - quasigroups, semigroups, algebraic logic
  - user makes conjectures, computer provides proofs (sometimes)
- nothing else (to my knowledge)

Future:
- smarter methods?
  - combination of various techniques, building conjectures, restricted higher order languages, knowledge bases...
Automated reasoning in algebraic research

Current state:
- first order ATP
  - problems in a small theory, mostly equational problems
  - quasigroups, semigroups, algebraic logic
  - user makes conjectures, computer provides proofs (sometimes)
- nothing else (to my knowledge)

Future:
- smarter methods?
  (combination of various techniques, building conjectures, restricted higher order languages, knowledge bases ...)

David Stanovský (Prague)
Outline

I. Structure theorems

- automatically derive structure theorems in the spirit of, say, classification of finite abelian groups
- automatically derive representation theorems in the spirit of, say, classification of cyclic groups, or of finite fields

II. Term conditions

- does an algebra have a term satisfying certain equational condition?
- does one term condition imply another?
- “beautification” of term conditions
Structure theorems, finite abelian groups

**Theorem.** Let $G$ be a finite abelian group. Then $G$ is isomorphic to a direct product of cyclic groups of prime power order.

**Key lemma.** If $G$ is an abelian group, $A, B$ its subgroups, $A \cap B = \{1\}$, $AB = G$, then $G \cong A \times B$.

**Proof of theorem.**
If $G$ is not cyclic, let $A$ be the largest cyclic subgroup, assume there is no such $B$, compute for a while, get contradiction.
If $G$ is cyclic, use Chinese Remainder theorem.
Structure theorems, finite abelian groups

**Theorem**

Let $G$ be a finite abelian group. Then $G$ is isomorphic to a direct product of cyclic groups of prime power order.

**Key lemma.** If $G$ is an abelian group, $A, B$ its subgroups, $A \cap B = \{1\}$, $AB = G$, then $G \cong A \times B$.

**Proof of theorem.**

If $G$ is not cyclic, let $A$ be the largest cyclic subgroup, assume there is no such $B$, compute for a while, get contradiction.

If $G$ is cyclic, use Chinese Remainder theorem.

**A simpler theorem.** If $G$ is any abelian group of finite exponent, then $G$ is isomorphic to a direct product of its prime components

$$G_p = \{a : \text{the order of } a \text{ is } p^k \text{ for some } k\}.$$
Structure theorems, finite abelian groups

structure theorem:

**Theorem (Finite abelian groups)**

Let $G$ be a finite abelian group. Then $G$ is isomorphic to a direct product of cyclic groups of prime power order.

representation theorem:

**Theorem (Cyclic groups)**

Let $G$ be a finite cyclic group. Then $G \cong \mathbb{Z}_n$ for some $n$.

combine:

**Corollary**

Let $G$ be a finite abelian group. Then $G \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}}$. 

Structure theorems, differential modes

Differential mode = an algebra \( A = (A, \ast) \) satisfying

\[
x \ast x = x, \quad x \ast (y \ast z) = x \ast y, \quad (x \ast y) \ast z = (x \ast z) \ast y
\]

Left projection algebra = an algebra \( A = (A, \ast) \) with \( x \ast y = x \).

Theorem

Let \( A \) be a differential mode. Then \( A \) is a Mal'cev product of left projection algebras.

I.e., there is a congruence \( \alpha \) of \( A \) such that all blocks \([a]_\alpha\) are left projection algebras, and the factor \( A/\alpha \) is also left projection algebra.

Proof. Put \( \alpha = \{(a, b) : x \ast a = x \ast b \text{ for all } x\} \). Easy to verify.

A more challenging variant: differential modes of higher arities.

\( \alpha = \{(a, b) : f(x, y, a) = f(x, y, b) \text{ and } f(x, a, y) = f(x, b, y) \text{ for all } x, y\} \)
Structure theorems, simple LDLQ

Left distributive left quasigroup = an algebra \( A = (A, *, \backslash) \) satisfying

\[
x * (y * z) = (x * y) * (x * z), \quad x * (x \backslash y) = x \backslash (x * y) = y
\]

simple = no non-trivial congruences

**Theorem**

Let \( A \) be a simple LDLQ. Then \( A \) is either idempotent \((x * x = x)\), or does not depend on the first variable \((x * y = f(y) \text{ for some } f)\).

**Proof.** Define \( \alpha = \{(a, b) : a^m = b^n \text{ for some } m, n\} \). It is a congruence, \( A/\alpha \) is idempotent, blocks are subalgebras that do not depend on the first variable. If \( A \) is simple, either \( \alpha = 0 \) and \( A \) is idempotent, or \( \alpha = 1 \) and the latter holds.

Case 1. (David Joyce): it can be represented by conjugation classes in simple groups with \( x * y = xyx^{-1} \).

Case 2. (easy): \(|A|\) is prime and \( f \) a permutation with a single cycle.
Structure theorems, algorithmically?

Maybe the following approach could work:

Hardwire:
- structural concepts - substructures, generators, congruences, products, etc.
- tricks to prove structure theorems

Algorithm:
- inputs a set of axioms
- tries to instantiate structural concepts to fit assumptions of the tricks
Term conditions

strong Mal’cev condition = “there is a term $t$ satisfying ...”
Mal’cev condition = “$\exists n$ s.t. there are terms $t_1, \ldots, t_n$ satisfying ...”

Example:
Let $\mathcal{K}$ be an equationally defined class of algebras. TFAE:

1. for all $A \in \mathcal{K}$, all congruences of $A$ permute one another
2. there is a term $t$ such that every $A \in \mathcal{K}$ satisfies

$$t(x, x, y) = t(y, x, x) = y.$$
Term conditions

strong Mal’cev condition = “there is a term \( t \) satisfying ...”
Mal’cev condition = “\( \exists n \) s.t. there are terms \( t_1, \ldots, t_n \) satisfying ...”

Example:
Let \( \mathcal{K} \) be an equationally defined class of algebras. TFAE:

1. for all \( A \in \mathcal{K} \), all congruences of \( A \) permute one another
2. there is a term \( t \) such that every \( A \in \mathcal{K} \) satisfies

\[
t(x, x, y) = t(y, x, x) = y.
\]

Questions:

- Does a given (finite) algebra satisfy a term condition?
- Does one Mal’cev condition imply another one? (For all finite algebras? For all finitely related algebras?)
- Given a Mal’cev condition, can you find a nicer one, equivalent to it?
Some important term conditions

**Taylor:** $t$ that cannot be interpreted with projection

**weak near-unanimity($n$):** $t(yxx \ldots x) = t(xyx \ldots x) = \cdots = t(xxx \ldots xy)$

**cyclic($n$):** $t(x_1, \ldots, x_n) = t(x_2, \ldots, x_n, x_1)$

**Siggers:** $t(x, y, y, z) = t(y, x, z, x)$

**Jónsson($k$):** $t_0 = x$, $t_k = z$, $t_i(x, x, y) = t_{i+1}(x, x, y)$ for $i$ even, $t_i(x, y, y) = t_{i+1}(x, y, y)$ for $i$ odd, $t_i(x, y, x) = x$.

**near-unanimity($n$):** $t(yxx \ldots x) = t(xyx \ldots x) = \cdots = t(xxx \ldots xy) = x$

(all idempotent)

- (easy to do) prove $\exists n$ near unanimity($n$) $\Rightarrow \exists k$ Jónsson($k$)

- (a challenge) prove $\exists k$ Jónsson($k$) $\Rightarrow$ weak near unanimity($3$)

- (Valeriote’s problem) nice conditions for omitting types
Term conditions, a different problem

Let $\mathcal{K}$ be an equationally defined class of algebras, in the language of a single binary operation $\ast$. TFAE:

1. all $A \in \mathcal{K}$ have well defined algebra of subalgebras
2. there are terms $t, s$ such that every $A \in \mathcal{K}$ satisfies

$$
(x \ast y) \ast (u \ast v) = t(x, u) \ast s(y, v).
$$

An open problem:
prove that if $\mathcal{K}$ is idempotent, then every $A \in \mathcal{K}$ satisfies

$$
(x \ast y) \ast (u \ast v) = (x \ast u) \ast (y \ast v).
$$

(i.e., beautification to the extent that $t(x, u) = x \ast u$ and $s(y, v) = y \ast v$)