Universal Algebra and Computational Complexity
Lecture 3

Ross Willard

University of Waterloo, Canada

Třešť, September 2008

Summary of Lecture 2

Recall from Tuesday:

$$\begin{array}{ccccccccccccc}
L & \subseteq & NL & \subseteq & P & \subseteq & NP & \subseteq & PSPACE & \subseteq & EXPTIME & \cdots \\
\Cup & & \Cup & & \Cup & & \Cup & & \Cup & & \Cup & \\
FVAL, & & PATH, & & CVAL, & & SAT, & & 1\text{-}CLO & & CLO & \\
2COL & & 2SAT & & HORN\text{-} & & 3SAT, & & & & & \\
 & & & & 3SAT & & 3COL, & & & & & \\
 & & & & & & 4COL, \text{ etc.} & & & & & \\
 & & & & & & HAMPATH & & & & &
\end{array}$$

Today:

- Some decision problems involving finite algebras
- How hard are they?

Encoding finite algebras: size matters

Let $\mathbf{A}$ be a finite algebra (always in a finite signature).

How do we encode $\mathbf{A}$ for computations? And what is its *size*?

Assume $A = \{0, 1, \ldots, n-1\}$. Thus A is encoded using $\log n$ bits.

For each fundamental operation f: If $\text{arity}(f) = r$, then f is given by its *table*, having ...

- n^r entries;
- each entry requires $\log n$ bits.

Hence the size of $\mathbf{A}$ is

$$||\mathbf{A}|| = \left(1 + \sum_{fund\ f} n^{\text{arity}(f)}\right) \log n.$$

Size of an algebra

Define some parameters:

$$\begin{aligned} R &= \text{maximum arity of the fundamental operations (assume } > 0) \\ T &= \text{number of fundamental operations (assume } > 0). \end{aligned}$$

Then

$$n^R \log n \;\leq\; ||\mathbf{A}|| \;\leq\; T \cdot n^R \log n.$$

In particular, if we restrict our attention to algebras of some **fixed** similarity type, then T and R become constant, so

$$||\mathbf{A}|| \;\in\; O(\mathrm{poly}(|A|)).$$

Some decision problems involving algebras

INPUT: a finite algebra $\mathbf{A}$.

1. Is $\mathbf{A}$ simple? Subdirectly irreducible? Directly indecomposable??
2. Is $\mathbf{A}$ primal? Quasi-primal? Maltsev?
3. Is $\mathbf{V}(\mathbf{A})$ congruence distributive? Congruence modular?

INPUT: two finite algebras $\mathbf{A}, \mathbf{B}$.

4. Is $\mathbf{A} \cong \mathbf{B}$?
5. Is $\mathbf{A} \in \mathbf{V}(\mathbf{B})$

INPUT: A finite algebra $\mathbf{A}$ and two terms $s(\vec{x}), t(\vec{x})$.

6. Does $s = t$ have a solution in $\mathbf{A}$?
7. Is $s \approx t$ an identity of $\mathbf{A}$?

INPUT: an operation f on a finite set.

8. Does f generate a minimal clone?

How hard are these problems?

Categories of answers

Suppose D is some decision problem involving finite algebras.

1. What is the "obvious" algorithm for D? What is its complexity?
   - If an obvious algorithm obviously has complexity Y, then we call Y an obvious upper bound for the complexity of D.
2. Do we know a clever (nonobvious) algorithm? Does it give a lesser complexity (relative to the spectrum $L < NL < P < NP$ etc.)?
   - If so, call this a nonobvious upper bound.
3. Can we find a clever reduction of some X-complete problem to D?
   - If so, this gives X as a lower bound to the complexity of D.

In a perfect world, we would like to find an $X \in \{L, NL, P, NP, \ldots\}$ which is both an upper and a lower bound to the complexity of D.

- Then D is X-complete.

An easy problem: Subalgebra Membership (*SUB-MEM*)

Subalgebra Membership Problem (*SUB-MEM*)

INPUT:

- An algebra $\mathbf{A}$.
- A set $S \subseteq A$.
- An element $b \in A$.

QUESTION: Is $b \in \mathrm{Sg}^{\mathbf{A}}(S)$?

How hard is *SUB-MEM*?

An obvious upper bound for *SUB-MEM*

INPUT:

- An algebra $\mathbf{A}$.
- A set $S \subseteq A$.
- An element $b \in A$.

Algorithm:

INPUT: $\mathbf{A}, S, b$.
$S_0 := S$
For $i = 1, \ldots, n$ — n loops
  $S_i := S_{i-1}$
  For each operation f (of arity r) — T operations
    For each $(a_1, \ldots, a_r) \in (S_{i-1})^r$ — $\leq n^r$ instances
      $c := f(a_1, \ldots, a_r)$
      $S_i := S_i \cup \{c\}$.
  Next i.
OUTPUT: whether $b \in S_n$ $(n = |A|)$.

Heuristics:
$n\left(\sum_f n^{\mathrm{ar}(f)}\right) \leq n||\mathbf{A}||$ steps

The Complexity of *SUB-MEM*

So $\mathit{SUB\text{-}MEM} \in \mathit{TIME}(N^2)$, or maybe $\mathit{TIME}(N^{4+\epsilon})$, or surely in $\mathit{TIME}(N^{55})$, and so we get the obvious upper bound:

$$\mathit{SUB\text{-}MEM} \in P.$$

Next questions:

- Can we obtain P as a *lower* bound for *SUB-MEM*?
- What was that P-complete problem again?. . . (*CVAL* or *HORN-3SAT*)
- Can we show $\mathit{HORN\text{-}3SAT} \leq_L \mathit{SUB\text{-}MEM}$?

Theorem (N. Jones & W. Laaser, '77)

Yes.
In other words, SUB-MEM is P-complete.

A variation: 1-*SUB-MEM*

1-*SUB-MEM*: the restriction of *SUB-MEM* to unary algebras (all fundamental operations are unary). I.e.,

INPUT: A *unary* algebra $\mathbf{A}$, a set $S \subseteq A$, and $b \in A$.
QUESTION: Is $b \in \mathrm{Sg}^{\mathbf{A}}(S)$?

Here is a nondeterministic log-space algorithm:

NALGORITHM: guess a sequence $c_1, c_2, \ldots, c_k$ such that

- $c_1 \in S$
- $c_{i+1} = f(c_i)$ for some fundamental operation f
- $c_k = b$.

Theorem (N. Jones, Y. Lien & W. Laaser, '76)

1-SUB-MEM is NL-complete.

Some tractable problems about algebras

The following problems are tractable (in P).

1. Given $\mathbf{A}$, $S \subseteq A$, and $b \in A$, determine whether $b \in \mathrm{Sg}^{\mathbf{A}}(S)$.
2. Given $\mathbf{A}$, $U \subseteq A^2$, and $(a,b) \in A^2$, determine whether $(a,b) \in \mathrm{Cg}^{\mathbf{A}}(U)$. (Bonus: prove that it is in NL.)
3. Given $\mathbf{A}$ and $S \subseteq A$, determine whether S is a subalgebra of $\mathbf{A}$.
4. Given $\mathbf{A}$ and $\theta \in Eqv(A)$, determine whether θ is a congruence of $\mathbf{A}$.
5. Given $\mathbf{A}$ and $h : A \to A$, determine whether h is an endomorphism (or an automorphism) of $\mathbf{A}$.
6. Given $\mathbf{A}$, determine whether $\mathbf{A}$ is simple.

$$\mathbf{A} \text{ simple} \quad \Leftrightarrow \quad \forall a,b,c,d[c \neq d \ \to \ (a,b) \in \mathrm{Cg}^{\mathbf{A}}(c,d)].$$

7. Given $\mathbf{A}$, determine whether $\mathbf{A}$ is abelian.

$$\mathbf{A} \text{ abelian} \quad \Leftrightarrow \quad \forall a,c,d[c \neq d \ \to \ ((a,a),(c,d)) \notin \mathrm{Cg}^{\mathbf{A}^2}(0_A)].$$

Clone Membership Problem (*CLO*)

INPUT: $\mathbf{A} = \langle A; f_1, \ldots, f_t \rangle$ and $g : A^k \to A$.

QUESTION: Is $g \in \mathrm{Clo}\,\mathbf{A}$?

Obvious algorithm: Determine whether $g \in \mathrm{Sg}^{\mathbf{A}^{(A^k)}}(pr_1^k, \ldots, pr_k^k)$.

The running time is polynomial in $||\mathbf{A}^{A^k)}||$.
Can show

$$\log ||\mathbf{A}^{(A^k)}|| \leq n^k ||\mathbf{A}|| \leq (||g|| + ||\mathbf{A}||)^2.$$

Hence the running time is bounded by the exponential of a polynomial in the size of the input $(\mathbf{A}, g)$. I.e., $CLO \in EXPTIME$.

By reducing a known *EXPTIME*-complete problem to *CLO*, Friedman and Bergman *et al* showed:

Theorem

CLO is EXPTIME-complete.

The Primal Algebra Problem (*PRIMAL*)

INPUT: a finite algebra $\mathbf{A}$.

QUESTION: Is $\mathbf{A}$ primal?

The obvious algorithm is actually a reduction to *CLO*.

For a finite set A, let g_A be your favorite binary Sheffer operation on A.

Define $f : PRIMAL_{inp} \to CLO_{inp}$ by

$$f : \mathbf{A} \mapsto (\mathbf{A}, g_A).$$

Since

$$\mathbf{A} \text{ is primal} \quad \Leftrightarrow \quad g_A \in \operatorname{Clo} \mathbf{A},$$

we have $PRIMAL \leq_f CLO$. Clearly f is P-computable, so

$$PRIMAL \leq_P CLO$$

which gives the obvious upper bound

$$PRIMAL \in EXPTIME.$$

PRIMAL

But testing primality of algebras is special. Maybe there is a better, "nonobvious" algorithm?

(E.g., using Rosenberg's classification?)

Open Problem 1.

Determine the complexity of *PRIMAL*.

- Is it in *PSPACE*? ($=$ *NPSPACE*)
- Is it *EXPTIME*-complete? ($\Leftrightarrow$ $CLO \leq_P PRIMAL$)

MALTSEV

INPUT: a finite algebra **A**.

QUESTION: Does **A** have a Maltsev term?

The obvious upper bound is *NEXPTIME*, since *MALTSEV* is a projection of

$$\{\,(\mathbf{A}, p)\ :\ \underbrace{p \in \mathrm{Clo}\,\mathbf{A}}_{\textit{EXPTIME}}\ \text{ and }\ \underbrace{p \text{ is a Maltsev operation}}_{P}\,\}$$

which is itself in *EXPTIME*.

But a slightly less obvious algorithm puts *MALTSEV* in *EXPTIME*. Use the fact that if x, y name the two projections $A^2 \to A$, then **A** has a Maltsev term iff

$$(y, x) \in \mathrm{Sg}^{\mathbf{A}^{(A^2)}}((x,x),(x,y),(y,y))$$

(which is decidable in *EXPTIME*).

Similarly slightly nonobvious characterizations give *EXPTIME* as an upper bound to the following:

Some problems in *EXPTIME*

Given $\mathbf{A}$:

1. Does $\mathbf{A}$ have a majority term?
2. Does $\mathbf{A}$ have a semilattice term?
3. Does $\mathbf{A}$ have Jónsson terms?
4. Does $\mathbf{A}$ have Gumm terms?
5. Does $\mathbf{A}$ have terms equivalent to $\mathbf{V}(\mathbf{A})$ being congruence meet-semidistributive?
6. Etc. etc.

Are these problems easier than *EXPTIME*, or *EXPTIME*-complete?

Freese & Valeriote's theorem

For some of these problems we have an answer:

Theorem (R. Freese, M. Valeriote, '0?)

The following problems are all EXPTIME-complete:
Given $\mathbf{A}$,

1. *Does* $\mathbf{A}$ *have Jónsson terms?*
2. *Does* $\mathbf{A}$ *have Gumm terms?*
3. *Is* $\mathbf{V}(\mathbf{A})$ *congruence meet-semidistributive?*
4. *Does* $\mathbf{A}$ *have a semilattice term?*
5. *Does* $\mathbf{A}$ *have any nontrivial idempotent term?*
    - *idempotent means "satisfies* $f(x, x, \ldots, x) \approx x$."
    - *nontrivial means "other than* x."

Freese & Valeriote's theorem

Proof.

Freese and Valeriote give a construction which, given an input $\Gamma = (\mathbf{A}, g)$ to CLO, produces an algebra $\mathbf{B}_\Gamma$ such that:

- $g \in \mathrm{Clo}\,\mathbf{A} \;\Rightarrow\;$ there is a flat semilattice order on B_Γ such that $(x \wedge y) \vee (x \wedge z)$ is a term operation of $\mathbf{B}_\Gamma$.
- $g \notin \mathrm{Clo}\,\mathbf{A} \;\Rightarrow\;$ $\mathbf{B}_\Gamma$ has no nontrivial idempotent term operations.

Moreover, the function $f : \Gamma \mapsto \mathbf{B}_\Gamma$ is easily computed (in $\mathbf{P}$).

Hence f is simultaneously a P-reduction of CLO to all the problems in the statement of the theorem. $\square$

Open Problem 2.

Are the following easier than *EXPTIME*, or *EXPTIME*-complete?

- Determining if **A** has a majority operation.
- Determining if **A** has a majority operation (*MALTSEV*).

If *MALTSEV* is easier than *EXPTIME*, then so is *PRIMAL*, since

Theorem

A *is primal iff:*

$$\left.\begin{array}{l}\bullet\ \mathbf{A}\ \textit{has no proper subalgebras,}\\ \bullet\ \mathbf{A}\ \textit{is simple,}\\ \bullet\ \mathbf{A}\ \textit{is rigid,}\\ \bullet\ \mathbf{A}\ \textit{is not abelian, and}\end{array}\right\}\ \textit{in P}$$

- **A** *is Maltsev.*

Surprisingly, the previous problems become significantly easier when restricted to *idempotent* algebras.

Theorem (Freese & Valeriote, '0?)

The following problems for ***idempotent*** *algebras are in* **P***:*

1. $\mathbf{A}$ *has a majority term.*
2. $\mathbf{A}$ *has Jónsson terms.*
3. $\mathbf{A}$ *has Gumm terms.*
4. $V(\mathbf{A})$ *is congruence meet-semidistributive.*
5. $\mathbf{A}$ *is Maltsev.*
6. $V(\mathbf{A})$ *is congruence k-permutable for some k.*

Proof.

Fiendishly nonobvious algorithms using tame congruence theory. □

Variety Membership Problem (*VAR-MEM*)

INPUT: two finite algebras $\mathbf{A}, \mathbf{B}$ in the same signature.

QUESTION: Is $\mathbf{A} \in \mathbf{V}(\mathbf{B})$?

The obvious algorithm (J. Kalicki, '52): determine whether the identity map on A extends to a homomorphism $\mathbf{F}_{\mathbf{V}(\mathbf{B})}(A) \to \mathbf{A}$.

Theorem (C. Bergman & G. Slutzki, '00)

The obvious algorithm puts VAR-MEM in 2-EXPTIME.

$$2\text{-}EXPTIME = \bigcup_{k=1}^{\infty} TIME(2^{(2^{O(N^k)})})$$

$$\cdots NEXPTIME \subseteq EXPSPACE \subseteq 2\text{-}EXPTIME \subseteq N(2\text{-}EXPTIME) \cdots$$

What is the "real" complexity of *VAR-MEM*?

Theorem (Z. Székely, thesis '00)

VAR-MEM is NP-hard (i.e., 3SAT $\leq_P$ VAR-MEM).

Theorem (M. Kozik, thesis '04)

VAR-MEM is EXPSPACE-hard.

Theorem (M. Kozik, '0?)

VAR-MEM is 2-EXPTIME-hard and therefore 2-EXPTIME-complete.
Moreover, there exists a specific finite algebra $\mathbf{B}$ *such that the subproblem:*

> *INPUT: a finite algebra* $\mathbf{A}$ *in the same signature as* $\mathbf{B}$.
>
> *QUESTION: Is* $\mathbf{A} \in \mathbf{V}(\mathbf{B})$

is 2-EXPTIME-complete.

The Equivalence of Terms problem (*EQUIV-TERM*)

INPUT:

- A finite algebra $\mathbf{A}$.
- Two terms $s(\vec{x}), t(\vec{x})$ in the signature of $\mathbf{A}$.

QUESTION: Is $s(\vec{x}) \approx t(\vec{x})$ identically true in $\mathbf{A}$?

It is convenient to name the *negation* of this problem:

The Inequivalence of Terms problem (*INEQUIV-TERM*)

INPUT: (same)

QUESTION: Does $s(\vec{x}) \neq t(\vec{x})$ have a solution in $\mathbf{A}$?

How hard are these problems?

Obviously *INEQUIV-TERM* is in *NP*. (Any solution $\vec{x}$ to $s(\vec{x}) \neq t(\vec{x})$ serves as a certificate.)

On the other hand, and equally obviously, $SAT \leq_P$ *INEQUIV-TERM*. (Map $\varphi \mapsto (\mathbf{2}_{BA}, \varphi, 0)$.)

Hence *INEQUIV-TERM* is obviously *NP*-complete.

EQUIV-TERM, being its negation, is said to be co-*NP*-complete.

Definition

- Co-*NP* is the class of problems D whose negation $\neg D$ is in *NP*.
- A problem D is co-*NP*-complete if its negation $\neg D$ is *NP*-complete, or equivalently, if D is in the top $\equiv_P$-class of co-*NP*.

Done. End of story. Boring.

But WAIT!!!! There's more!!!!

For each fixed finite algebra $\mathbf{A}$ we can pose the problem for $\mathbf{A}$:

$\mathit{EQUIV\text{-}TERM}(\mathbf{A})$

INPUT: two terms $s(\vec{x}), t(\vec{x})$ in the signature of $\mathbf{A}$.

QUESTION: (same).

The following are obviously obvious:

- $\mathit{EQUIV\text{-}TERM}(\mathbf{A})$ is in co-NP for any algebra $\mathbf{A}$.
- $\mathit{EQUIV\text{-}TERM}(\mathbf{2}_{BA})$ is co-NP-complete. (Hint: $\varphi \mapsto (\varphi, 0)$.)
- $\mathit{EQUIV\text{-}TERM}(\mathbf{A})$ is in P when $\mathbf{A}$ is nice, say, a vector space or a set.

Problem: for which finite algebras $\mathbf{A}$ is $\mathit{EQUIV\text{-}TERM}(\mathbf{A})$ NP-complete? For which $\mathbf{A}$ is it in P?

There are a huge number of publications in this area. Here is a sample:

Theorem (H. Hunt & R. Stearns, '90; S. Burris & J. Lawrence, '93)

Let $\mathbf{R}$ *be a finite ring.*

- *If* $\mathbf{R}$ *is nilpotent, then EQUIV-TERM*$(\mathbf{R})$ *is in P.*
- *Otherwise, EQUIV-TERM*$(\mathbf{R})$ *is co-NP-complete.*

Theorem (T. Gorazd, '0?)

Let $\mathbf{A}$ *be a 2-element algebra. Then EQUIV-TERM*$(\mathbf{A})$ *is co-NP-complete if* $\mathbf{V}(\mathbf{A})$ *is congruence distributive, and is in P otherwise.*

Theorem (Burris & Lawrence, '04; G. Horváth & C. Szabó, '06; Horváth, Lawrence, L. Mérai & Szabó, '07)

Let $\mathbf{G}$ *be a finite group.*

- *If* $\mathbf{G}$ *is nilpotent, or of the form* $\mathbf{Z}_{m_1} \rtimes (\mathbf{Z}_{m_2} \rtimes \cdots (\mathbf{Z}_{m_k} \rtimes \mathbf{A}) \cdots)$ *with each* m_i *square-free and* $\mathbf{A}$ *abelian, then EQUIV-TERM*$(\mathbf{G})$ *is in P.*
- *If* $\mathbf{G}$ *is nonsolvable, then EQUIV-TERM*$(\mathbf{G})$ *is co-NP-complete.*

An outrageous scandal

Theorem (G. Horváth & C. Szabó)

Consider the group $\mathbf{A}_4$*.*

- *EQUIV-TERM*($\mathbf{A}_4$) *is in P.*
- *Yet there is an algebra* $\mathbf{A}$ *with the same clone as* $\mathbf{A}_4$ *such that EQUIV-TERM*($\mathbf{A}$) *is NP-complete.*

This is either wonderful or scandalous.

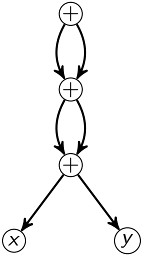
In my opinion, this is evidence that *EQUIV-TERM* is the wrong problem.

Definition

A circuit (in a given signature for algebras) is an object, similar to a term, except that repeated subterms need be written only once.

Example: Let $t = ((x + y) + (x + y)) + ((x + y) + (x + y))$.

A circuit for t:



Straight-line program:

$$\begin{aligned} v_1 &= x + y \\ v_2 &= v_1 + v_1 \\ t &= v_2 + v_2. \end{aligned}$$

Note that circuits may be significantly shorter than the terms they represent.

Equivalence of Terms Problem (correct version)

Fix a finite algebra $\mathbf{A}$.

The Equivalence of Circuits problem ($EQUIV\text{-}CIRC(\mathbf{A})$)

INPUT: two circuits $s(\vec{x}), t(\vec{x})$ in the signature of $\mathbf{A}$.

QUESTION: is $s(\vec{x}) \approx t(\vec{x})$ identically true in $\mathbf{A}$?

This is the correct problem.

Open Problem 3.

For which finite algebras $\mathbf{A}$ is $EQUIV\text{-}CIRC(\mathbf{A})$ NP-complete? For which $\mathbf{A}$ is it in P?

Relational Clone Membership (*RCLO*)

INPUT:

- A finite relational structure $\mathbf{M}$.
- A finitary relation $R \subseteq M^k$.

QUESTION: Is $R \in \mathrm{Inv}\,\mathrm{Pol}(\mathbf{M})$?

A slightly nonobvious characterization gives *NEXPTIME* as an upper bound. For a lower bound, we have:

Theorem (W,'0?)

RCLO is EXPTIME-hard.

Open Problem 4.

Is *RCLO* in *EXPTIME*? Is it *NEXPTIME*-complete?

Fix a finite relational structure $\mathbf{B}$.

Consider the following problem associated to $\mathbf{B}$:

A problem

INPUT: a finite structure $\mathbf{A}$ in the same signature as $\mathbf{B}$.

QUESTION: Is there a homomorphism $h : \mathbf{A} \to \mathbf{B}$?

This problem is called $CSP(\mathbf{B})$.

Obviously $CSP(\mathbf{B}) \in NP$ for any $\mathbf{B}$.

If $\mathbf{K}_3$ is the triangle graph, then $CSP(\mathbf{K}_3) = 3COL$, so is NP-complete in this case.

CSP Classification Problem

For which finite relational structures $\mathbf{B}$ is $CSP(\mathbf{B})$ in P? For which is it NP-complete?