Finite semigroups and CSPs

Pascal Tesson
Université Laval (Quebec City)

joint work with V. Dalmau, R. Gavaldà, O. Klíma,
B. Larose and D. Thérien

Bibliography

The talk is primarily based on

- O. Klíma, P. Tesson, D. Thérien: Dichotomies in the Complexity of Solving Systems of Equations over Finite Semigroups, Theory of Computing systems, 2006.
- V. Dalmau, R. Gavaldà, P. Tesson, D. Thérien: Tractable Clones of Polynomials over Semigroups, CP'05.

These are available from the electronic colloquium on computational complexity (ECCC).

Other references:

- G. Nordh, P. Jonsson: The Complexity of Counting Solutions to Systems of Equations over Finite Semigroups, COCOON'04.
- G. Nordh, The Complexity of Equivalence and Isomorphism of Systems of Equations over Finite Groups, MFCS'04.
- B. Larose, L. Zadori: Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras, available on B. Larose's webpage.

Semigroups, are you kidding?

- Semigroup = set + binary associative operation.
- Monoid = semigroup + identity element.

- Simplicity means that they cannot tell the whole story...
- ... but they tell an interesting one and we actually know what the story is!

From previous talks:

resolving the CSP-dichotomy conjecture is equivalent to classifying every algebra $\mathbb{A}$ as tractable or NP-complete.

$\mathbb{A}$ is tractable if CSP(Rel($\mathbb{A}$)) $\in$ P.

$\mathbb{A}$ is NP-complete if CSP(Rel($\mathbb{A}$)) is NPC.

$\Rightarrow$ Semigroups seem like a good warm-up.

Theorem: [Jeavons, Cohen, Gyssens]

If Pol(Γ) contains a semilattice operation then CSP(Γ) is tractable.

Theorem: [Jeavons, Cohen, Gyssens]

Any semilattice is a tractable algebra.

Theorem: [Bulatov, Jeavons, Volkov]

If S is a semigroup then S is tractable if S is a block-group and is NP-complete otherwise.

Another semigroup-related island of tractability

Theorem: [Feder & Vardi]

If Γ is a set of relations over a group G such that every k-ary R in Γ is a coset of a subgroup of G then CSP(Γ) is tractable.

Equivalently, if Pol(Γ) contains the polymorphism $m(x,y,z) = xy^{-1}z$ then CSP(Γ) is tractable.

Such Γ are called coset-generating.

Systems of equations over finite semigroups

Fix a semigroup S. Consider CSPs defined as a system of equations over S.

$$\left\{\begin{array}{rcl} x_1\, s\, x_2 &=& t\, x_3 \\ x_3\, x_4 &=& x_3\, x_1 \\ x_3\, s &=& s\, x_2 \end{array}\right. \Longleftrightarrow \left\{\begin{array}{rcl} x_s &=& s \\ x_t &=& t \\ x_1\, x_s &=& y_1 \\ y_1\, x_2 &=& y_2 \\ x_t\, x_3 &=& y_2 \\ x_3\, x_4 &=& y_3 \\ x_3\, x_1 &=& y_3 \\ x_3\, x_s &=& y_4 \\ x_s\, x_2 &=& y_4 \end{array}\right.$$

Systems of equations over finite semigroups

Fix a semigroup S. Consider CSPs defined as a system of equations over S.

- EQN^*_S: problem of deciding if a system over S has a solution.
- EQN^*_S is equivalent to $CSP(E_S)$ where E_S contains the unary relations $\{s\}$ for $s \in S$ and the ternary relation
  $R = \{(x,y,z): xy = z\}$.
- Obviously, the complexity of EQN^*_S depends on the structure of S. Can we prove a dichotomy?

Dichotomy for EQN* over monoids

Theorem: [Klíma, T., Thérien]

If M is a finite monoid then EQN^*_M is tractable if M is commutative and every element … ates a subgroup. Otherw … is NP-complete.

> homomorphic image of a subsemigroup

Alternatively, EQN^*_M is tractable iff M is a factor of the direct product of a semilattice with an abelian group.

Lemma: [Larose, Zádori] [Nordh, Jonsson]

Let S be a semigroup. Then $f: S^k \to S$ is a polymorphism of E_S iff

1. f is idempotent

$$f(x, \ldots, x) = x$$

2. f commutes with S

$$f(x_1y_1, \ldots, x_ky_k) = f(x_1, \ldots, x_k)\, f(y_1, \ldots, y_k)$$

Pf: Idempotency necessary and sufficient for being polymorphism of $x = s$ for all $s \in S$.

Commuting with S necessary and sufficient for being polymorphism of $xy = z$.

f is a polymorphism of $xy = z$ iff

$$
\begin{array}{ccccc}
x_1 & y_1 & = & z_1 \\
\vdots & \vdots & = & \vdots \\
x_k & y_k & = & z_k \\
\downarrow f & \downarrow f & & \downarrow f \\
f(x_1, \ldots, x_k) & f(y_1, \ldots, y_k) & = & f(z_1, \ldots, z_k) = f(x_1y_1, \ldots, x_ky_k)
\end{array}
$$

iff f commutes with s.

A sufficient criterion for hardness

Theorem: [Bulatov, Krokhin, Jeavons]
If $Pol(\Gamma)$ contains no Taylor term then $CSP(\Gamma)$ is NP-complete.

$t: S^k \to S$ is a Taylor term if for each $i \in \{1,\ldots,k\}$ it satisfies an identity in $\{x,y\}$

$$t(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k) = t(b_1, \ldots, b_{i-1}, y, b_{i+1}, \ldots, b_k)$$

with $a_r, b_r \in \{x,y\}$.

EQN* is hard for non-commutative monoids

Theorem: [Bulatov, Krokhin, Jeavons]
If Pol(Γ) contains no Taylor term then CSP(Γ) is NP-complete.

Lemma: [Larose, Zádori '06]
If a monoid M commutes with an idempotent Taylor term then M is commutative.

Corollary: [Klíma, T., Thérien 05]
If M is a non-commutative monoid then EQN^*_M is NP-complete.

EQN* is hard for non-commutative monoids

Pf by example. Suppose f is 4-ary such that $f(x,y,y,x) = f(x,x,x,y)$ and $f(y,x,y,x) = f(x,x,y,y)$.

Now, for any $a,b \in M$:

$$
\begin{aligned}
ab &= f(a,a,a,a)\, f(b,b,b,b) \\
&= f(a,a,a,1)\, f(1,1,1,a)\, f(b,b,b,b) \\
&= f(a,a,a,1)\, f(1,1,1,a)\, f(b,1,b,1)\, f(1,b,1,b) \\
&= f(a,a,a,1)\, f(b,1,b,1)\, f(1,1,1,a)\, f(1,b,1,b) \\
&= f(a,a,a,1)\, f(b,1,b,1)\, f(1,1,1,a)\, f(b,b,1,1) \\
&= f(a,a,a,1)\, f(b,1,b,1)\, f(b,b,1,1)\, f(1,1,1,a) \\
&= f(a,a,a,1)\, f(b,b,b,b)\, f(1,1,1,a) \\
&= f(a,a,1,1)\, f(1,1,a,1)\, f(b,b,b,b)\, f(1,1,1,a) \\
&= f(b,b,b,b)\, f(a,a,a,a) = ba
\end{aligned}
$$

Dichotomy for EQN* over monoids

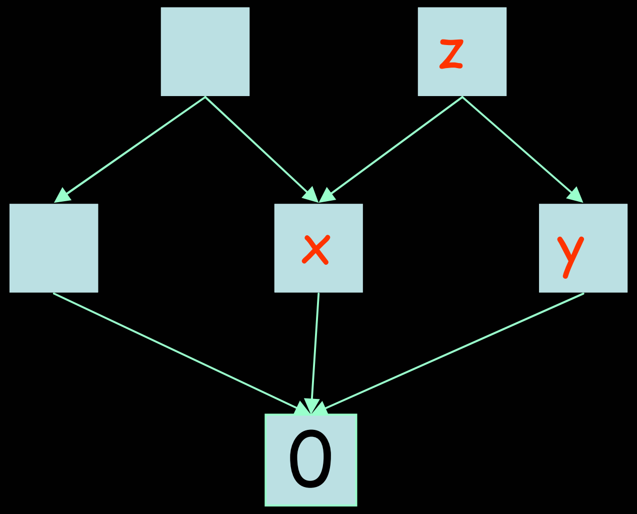
Theorem:

If M is a finite monoid then EQN^*_M is tractable if M is commutative and every element of M generates a subgroup. Otherwise, EQN^*_M is NP-complete.

Alternatively, EQN^*_M is tractable iff M is a factor of the direct product of a semilattice with an abelian group.

Upper bounds

- Let S be a semilattice. The operation of S is idempotent and commutes with itself. So EQN^*_S is tractable.



Straightforward algorithm

1. Set every non-constant variable to 0 and maintain lower bound to any solution.
2. If some equation $xy = z$ is unsatisfied, set these variables to the smallest upper bound of $\{x,y,z\}$.

Upper bounds

- Let G be an abelian group. The operation $m(x,y,z) = xy^{-1}z$ is a polymorphism of E_G.

$$\left.\begin{aligned} x_1 x_2 &= x_3 \\ y_1 y_2 &= y_3 \\ z_1 z_2 &= z_3 \end{aligned}\right\} \longrightarrow x_1x_2 (y_1y_2)^{-1} z_1z_2 = x_3y_3^{-1}z_3$$

and so

$$\begin{aligned} m(x_1,y_1,z_1)\, m(x_2,y_2,z_2) &= (x_1y_1^{-1}z_1)\,(x_2y_2^{-1}z_2) \\ &= x_3y_3^{-1}z_3 = m(x_3,y_3,z_3) \end{aligned}$$

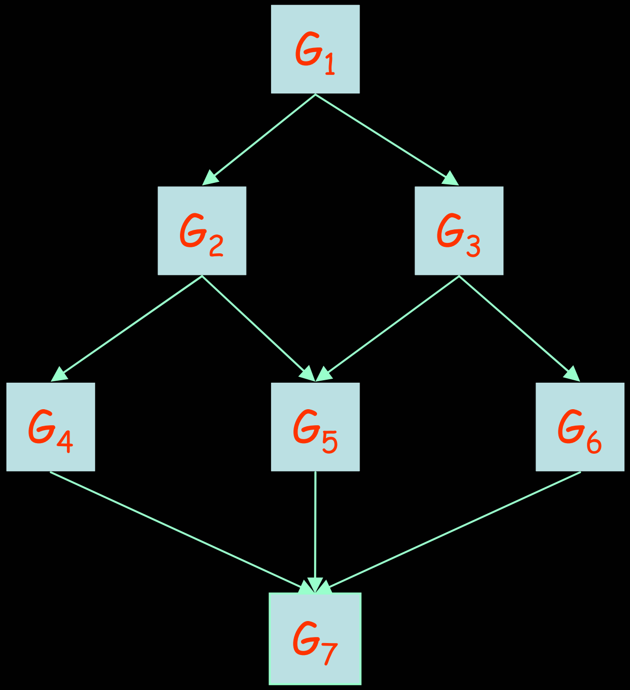
In fact, elementary linear algebra is sufficient to show EQN* is tractable over abelian groups.

...and so we are done?

- It trivially follows that EQN* is tractable over the direct product of a semilattice and an abelian group.
- Intuitively, an efficient algorithm for solving systems of equations over a semigroup S, yields efficient algorithms for any subsemigroup or any morphic image of S.
- Unfortunately, this is provably wrong for semigroups in general.

… back to the drawing board…

We can still salvage the previous ideas. Let M be a factor of $E \times G$ for a semilattice E and an abelian group G.



Algorithm works in two steps.

1. Find the minimal solution of the system projected into the semilattice. This allows us to associate each variable x in the system to a maximal subgroup G_x such that the system has a solution iff it has one in which each x lies in G_x.
2. We end up with a multi-sorted CSP in which the constraint language is coset-generating.

Theorem: [KTT]

For every constraint language Γ, there exists a semigroup S_Γ such that CSP(Γ) is poly-time equivalent to $EQN^*_{S_\Gamma}$.

Seems interesting...

... but (honestly) useless.

Moral of the story

Systems of equations over semigroups provide an interesting case study for CSPs.

- Problem seems fairly easy to reason about, yet is rich enough to require the deployment of the full arsenal of CSP techniques.
- Algebraic structure fits in nicely with algebraic analysis of CSPs.
- Develops our intuition about more general tractability or hardness criteria.
- Can generate new ideas.

Related work

- Larose & Zádori:
  Consider the problem of solving systems over arbitrary finite algebras ⇒ dichotomies for rings, lattices, quasigroups.

- Nordh:
  Problem of testing if two systems are equivalent or isomorphic.

- Nordh & Jonsson + Klíma, Larose,T.:
  Counting the number of solutions to a system. A complete dichotomy can be obtained: the problem is always tractable or #P-complete. Hopefully will be a good introduction to Bulatov's #CSP-dichotomy.

A new island of tractability

Direction for future progress on tractable CSPs: combining existing tractable cases.

In particular, the algorithm sketched for solving EQN* over sufficiently simple monoids combines a local consistency algorithm (semilattices) and a linear algebra algorithm.

A new island of tractability

Theorem: [Dalmau, Gavaldà, T. & Thérien]

If S is a block-group and Γ is such that Pol(Γ) contains the ternary operation t defined by

$$t(x,y,z) = x\, y^{\omega-1}\, z$$

then CSP(Γ) is tractable.

ω is the smallest integer such that $s^{\omega} s^{\omega} = s^{\omega}$ for all $s \in S$.

The tractability of EQN* over f
products of semilattices and abe
be obtained as a corollary.

A new island of tractability

Theorem:

If S is a ~~block~~ group and Γ is such that Pol(Γ) contains the ternary operation t defined by

$$t(x,y,z) = x\, y^{\omega-1}\, z$$

then CSP(Γ) is tractable.

Specializes to the result of Feder & Vardi about coset-generating relations.

If S is a block-group and Γ is such that Pol(Γ) contains the operation of S then it must also contain the ternary operation t defined by

$$t(x,y,z) = x\, y^{\omega-1}\, z$$

and CSP(Γ) is tractable.

Implies that block-groups are tractable algebras [BJV].

Instance $\mathcal{I}$ of CSP(Γ)

↓ Impose arc-consistency

If $\mathcal{I}$ is inconsistent it is unsatisfiable.
If $\mathcal{I}$ is consistent then we can assign every variable x_i to a subgroup G_i of S such that if $\mathcal{I}$ has a solution then it has one where each x_i takes a value in G_i.

↓ Use the tractability of coset-generating relations.

Original constraints $(x_1,x_2,x_3) \in R$ in $\mathcal{I}$ have implicitly become $(x_1,x_2,x_3) \in R_{G_1,G_2,G_3}$ where $R_{G_1,G_2,G_3} = R \cap G_1\times G_2\times G_3$. Since Pol($\Gamma$) contains $xy^{-1}z$ this new relation is a coset of $G_1\times G_2\times G_3$.

Bingo!

Open questions

- V. Dalmau: "CSP is not about finding the right algorithm for your problem, it's about finding the right problem for your algorithm".

⇒ what CSPs can be solved by using an arc-consistency algorithm to reduce the problem to a multi-sorted Mal'cev CSP.

Over a domain S equipped with a semigroup operation, consider clones in which every operation $f(x_1,\ldots,x_t)$ is idempotent and can be written as a polynomial over S (such as $xy^{\omega-1}z$).

1. Classify all clones of the above type.
2. Conjecture: every tractable clones of polynomials over a group contains a Mal'cev operation.