Deciding subpower membership for semigroups

Markus Steindl
ma.steindl@gmx.at

JKU Linz, Austria

Novi Sad, June 5, 2015

Supported by the Austrian Science Fund (FWF): P24285

JOHANNES KEPLER UNIVERSITY LINZ | JKU

FWF Der Wissenschaftsfonds.

Deciding subpower membership for semigroups

Joint work with

- Andrei Bulatov (Vancouver)
- Peter Mayr (Linz)

Deciding subpower membership for semigroups

Fix a finite semigroup S.
Define the *subpower membership problem for S* (Willard, 2007 [5])

SMP(S)

Input: Tuples $a_1, \ldots, a_k, b \in S^n$.

Problem: Is b in the subsemigroup of S^n generated by $a_1, \ldots, a_k$?

Deciding subpower membership for semigroups

Fix a finite semigroup S.
Define the *subpower membership problem for S* (Willard, 2007 [5])

SMP(S)

Input:	Tuples $a_1, \ldots, a_k, b \in S^n$.
Problem:	Is b in the subsemigroup of S^n generated by $a_1, \ldots, a_k$?

Convention

All semigroups in this talk are finite.

Deciding subpower membership for semigroups

Fix a finite semigroup S.
Define the *subpower membership problem for S* (Willard, 2007 [5])

SMP(S)

Input: Tuples $a_1, \ldots, a_k, b \in S^n$.

Problem: Is b in the subsemigroup of S^n generated by $a_1, \ldots, a_k$?

Convention

All semigroups in this talk are finite.

What is the complexity with respect to n, k?

Theorem (Bulatov, Mayr, S., manuscript 2015)

SMP(S) *for a semigroup S is in* PSPACE.

Theorem (S., manuscript 2014)

Let S be a semigroup. If there are $a, e, f \in S$ s.t.

$$a \notin \{a^2, a^3, \dots\} \quad \textit{and} \quad ea = a = af, \tag{1}$$

then SMP(S) *is* NP-*hard.*

Proof.

By reducing SAT to SMP(S). □

Theorem (S., manuscript 2014)

Let S be a semigroup. If there are $a, e, f \in S$ s.t.

$$a \notin \{a^2, a^3, \ldots\} \quad \text{and} \quad ea = a = af, \tag{1}$$

then SMP(S) *is* NP*-hard.*

Proof.

By reducing SAT to SMP(S). □

Lemma (Bulatov, Mayr, S., manuscript 2015)

In a commutative semigroup S, TFAE:

1. *S violates (1)*
2. *S has an ideal C which is a union of groups, and S/C is nilpotent, i.e.*

$$\exists d \in \mathbb{N}\ \forall s_1, \ldots, s_d \in S \colon s_1 \cdots s_d \in C.$$

In this case we say S is a nilpotent ideal extension of C.

Lemma (Bulatov, Mayr, S., manuscript 2015)
SMP(C) *for a commutative union of groups* C *is in* P.

Lemma (Bulatov, Mayr, S., manuscript 2015)

SMP(C) *for a commutative union of groups* C *is in* P.

Theorem (Bulatov, Mayr, S., manuscript 2015)

If S *is a nilpotent ideal extension of a semigroup* C*,*
then SMP(S) $\leq$ SMP(C).

Lemma (Bulatov, Mayr, S., manuscript 2015)
SMP(C) *for a commutative union of groups C is in* P*.*

Theorem (Bulatov, Mayr, S., manuscript 2015)
If S is a nilpotent ideal extension of a semigroup C, then SMP(S) $\leq$ SMP(C)*.*

Lemma (Bulatov, Mayr, S., manuscript 2015)
SMP(S) *for a commutative semigroup S is in* NP*.*

Lemma (Bulatov, Mayr, S., manuscript 2015)

SMP(C) *for a commutative union of groups* C *is in* P.

Theorem (Bulatov, Mayr, S., manuscript 2015)

If S *is a nilpotent ideal extension of a semigroup* C*,*
then $\mathrm{SMP}(S) \leq \mathrm{SMP}(C)$.

Lemma (Bulatov, Mayr, S., manuscript 2015)

SMP(S) *for a commutative semigroup* S *is in* NP.

Proof.

Fix an instance $a_1, \ldots, a_k, b \in S^n$.
Assume $b \in \langle a_1, \ldots, a_k \rangle$.
Then $b = {a_1}^{e_1} \cdots {a_k}^{e_k}$

Lemma (Bulatov, Mayr, S., manuscript 2015)

SMP(C) *for a commutative union of groups C is in* P.

Theorem (Bulatov, Mayr, S., manuscript 2015)

If S is a nilpotent ideal extension of a semigroup C, then SMP(S) $\leq$ SMP(C).

Lemma (Bulatov, Mayr, S., manuscript 2015)

SMP(S) *for a commutative semigroup S is in* NP.

Proof.

Fix an instance $a_1, \ldots, a_k, b \in S^n$.
Assume $b \in \langle a_1, \ldots, a_k \rangle$.
Then $b = {a_1}^{e_1} \cdots {a_k}^{e_k}$ for some $e_1, \ldots, e_k \leq |S|!$.
Now $(e_1, \ldots, e_k)$ is a witness whose size is linear in k. □

Dichotomy for commutative semigroups

We have established:

Theorem (Bulatov, Mayr, S., manuscript 2015)

Let S be a commutative semigroup.

1. SMP(S) *is in* P *if S is a nilpotent ideal extension of a union of groups.*
2. *It is* NP*-complete otherwise.*

SMP for semigroups

Reminder:

Theorem (S., manuscript 2014)

Let S be a semigroup. If there are $a, e, f \in S$ s.t.

$$a \notin \{a^2, a^3, \ldots\} \quad \text{and} \quad ea = a = af, \tag{1}$$

then SMP(S) *is* NP-*hard.*

SMP for semigroups

Reminder:

Theorem (S., manuscript 2014)

Let S be a semigroup. If there are $a, e, f \in S$ s.t.

$$a \notin \{a^2, a^3, \dots\} \quad \text{and} \quad ea = a = af, \tag{1}$$

then SMP(S) *is* NP-*hard.*

Let $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}, \mathcal{D}$ denote Green's equivalences.

Corollary

If a semigroup S has a $\mathcal{D}$-class with group and non-group $\mathcal{H}$-classes, then SMP(S) *is* NP-*hard.*

SMP for the Brandt semigroup

Corollary

The SMP *for the Brandt Semigroup*

$$B_2 := \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

is NP-*hard.*

SMP for the Brandt semigroup

Corollary

The SMP *for the Brandt Semigroup*

$$B_2 := \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \}$$

is NP-*hard.*

Theorem (S., manuscript 2014)

SMP(B_2) *is* NP-*complete.*

Proof.

Fix an instance $a_1, \ldots, a_k, b \in {B_2}^n$.
Assume $b = f(a_1, \ldots, a_k)$ for some k-ary term f.

SMP for the Brandt semigroup

Corollary

The SMP *for the Brandt Semigroup*

$$B_2 := \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \}$$

is NP-*hard.*

Theorem (S., manuscript 2014)

SMP(B_2) *is* NP-*complete.*

Proof.

Fix an instance $a_1, \ldots, a_k, b \in {B_2}^n$.
Assume $b = f(a_1, \ldots, a_k)$ for some k-ary term f.
Now there is a k-ary term g s.t.

1. $g(a_1, \ldots, a_k) = f(a_1, \ldots, a_k)$, and
2. $\ell(g) \leq (n+1)k$.

□

SMP for 0-simple semigroups

The Brandt semigroup is 0-simple.

SMP for 0-simple semigroups

The Brandt semigroup is 0-simple.

A nonempty subset $I \subseteq S$ of a semigroup S is an *ideal* if

$$I \cdot S \subseteq I \quad \text{and} \quad S \cdot I \subseteq I.$$

SMP for 0-simple semigroups

The Brandt semigroup is 0-simple.

A nonempty subset $I \subseteq S$ of a semigroup S is an *ideal* if

$$I \cdot S \subseteq I \quad \text{and} \quad S \cdot I \subseteq I.$$

A semigroup with zero is *0-simple* if $\{0\}$ is the only proper ideal.

SMP for 0-simple semigroups

The Brandt semigroup is 0-simple.

A nonempty subset $I \subseteq S$ of a semigroup S is an *ideal* if

$$I \cdot S \subseteq I \quad \text{and} \quad S \cdot I \subseteq I.$$

A semigroup with zero is *0-simple* if $\{0\}$ is the only proper ideal.

Theorem (S., manuscript 2014)

1. *If a 0-simple semigroup S is a union of groups, then* $\mathrm{SMP}(S)$ *is in P.*
2. *Otherwise it is* NP*-hard.*

SMP for bands

Commutative unions of groups and 0-simple unions of groups have SMP in P.

Questions

- Do unions of groups have SMP in P?

SMP for bands

Commutative unions of groups and 0-simple unions of groups have SMP in P.

Questions

- Do unions of groups have SMP in P?
- An idempotent semigroup (*band*) is a union of groups of order 1. Do bands have SMP in P?

SMP for bands

Commutative unions of groups and 0-simple unions of groups have SMP in P.

Questions

- Do unions of groups have SMP in P?
- An idempotent semigroup (*band*) is a union of groups of order 1. Do bands have SMP in P?

A band is called *regular* iff it satisfies $xyxzx \approx xyzx$.

SMP for bands

Commutative unions of groups and 0-simple unions of groups have SMP in P.

Questions

- Do unions of groups have SMP in P?
- An idempotent semigroup (*band*) is a union of groups of order 1. Do bands have SMP in P?

A band is called *regular* iff it satisfies $xyxzx \approx xyzx$.

Theorem (S., manuscript 2014)

SMP(S) *for a regular band S is in* P.

Proof.

Is based on $xyxzx \approx xyzx$. □

Varieties of bands (idempotent semigroups)

The lattice of varieties of bands is well-known:

Theorem (Birjukov, Fennemore, Gerhard, 1970s [1, 2, 3])

1. *There are countably many varieties of bands.*

Varieties of bands (idempotent semigroups)

The lattice of varieties of bands is well-known:

Theorem (Birjukov, Fennemore, Gerhard, 1970s [1, 2, 3])

1. *There are countably many varieties of bands.*
2. *Each variety is defined by*

$$(xy)z \approx x(yz),$$
$$x^2 \approx x,$$
one additional identity.

Varieties of bands (idempotent semigroups)

The lattice of varieties of bands is well-known:

Theorem (Birjukov, Fennemore, Gerhard, 1970s [1, 2, 3])

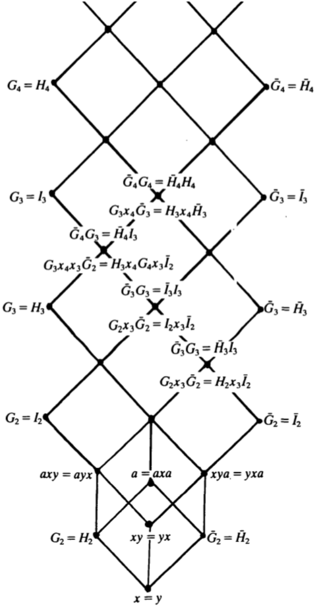
1. *There are countably many varieties of bands.*
2. *Each variety is defined by*

   $(xy)z \approx x(yz)$,

   $x^2 \approx x$,

   one additional identity.
3. *The proper subvarieties form the lattice on the next slide.*

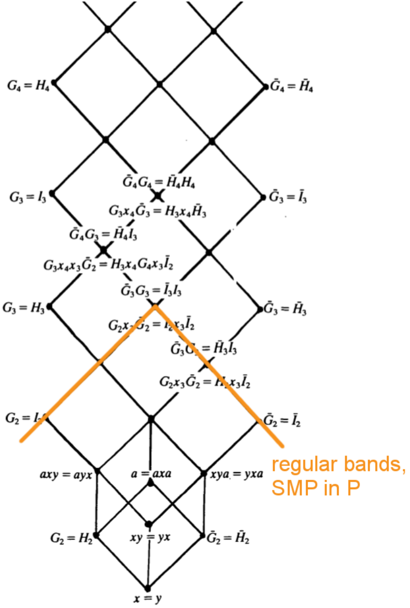
Varieties of bands (idempotent semigroups)



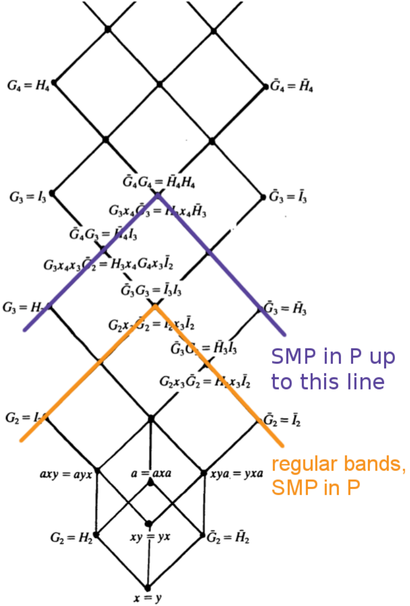
Lattice of varieties of bands, taken from "Varieties of bands revisited" by Gerhard and Petrich, 1989 [4].

G_n, H_n, I_n are systems of terms. $\bar{G}_n$, $\bar{H}_n$, $\bar{I}_n$ are the reversed counterparts.

Varieties of bands (idempotent semigroups)



Varieties of bands (idempotent semigroups)



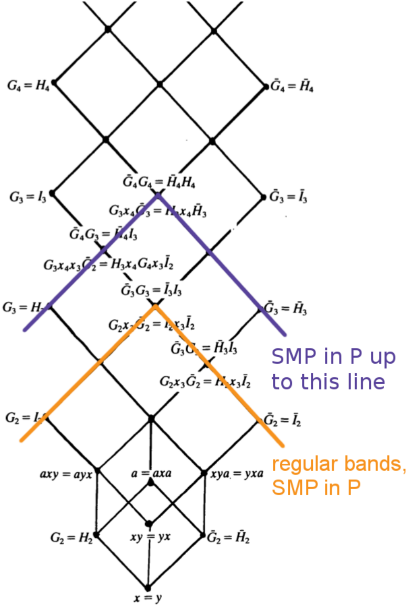
Theorem (S., manuscript 2014)

Bands in the variety $[\bar{G}_4 G_4 \approx \bar{H}_4 H_4]$ *have* SMP *in* P.

Proof.

Is based on the identities $G_4 \approx H_4$ and $\bar{G}_4 \approx \bar{H}_4$. □

Varieties of bands (idempotent semigroups)



Theorem (S., manuscript 2014)

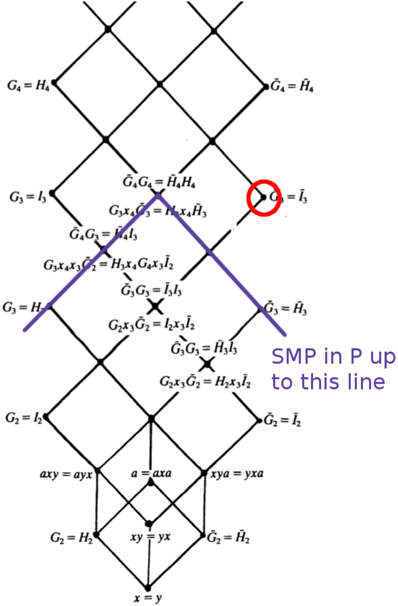
Bands in the variety $[\bar{G}_4 G_4 \approx \bar{H}_4 H_4]$ *have* SMP *in* P.

Proof.

Is based on the identities $G_4 \approx H_4$ and $\bar{G}_4 \approx \bar{H}_4$. □

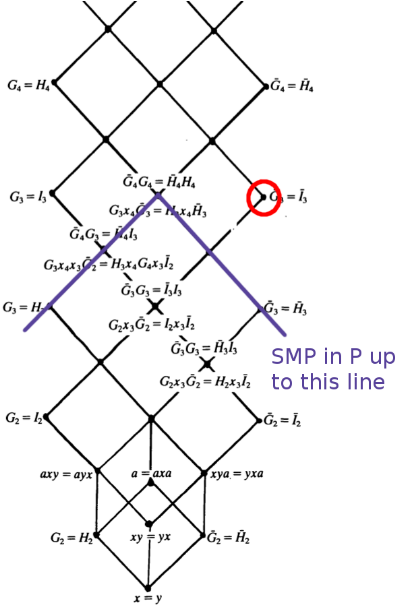
The goal was to work our way up this lattice.

Varieties of bands (idempotent semigroups)



We started with the variety $\mathcal{V} := [\bar{G}_3 \approx \bar{I}_3]$ (red circle).

Varieties of bands (idempotent semigroups)



We started with the variety $\mathcal{V} := [\bar{G}_3 \approx \bar{I}_3]$ (red circle).

We were not able to determine the complexity for bands in $\mathcal{V}$ using the equations of $\mathcal{V}$.

SMP for bands (idempotent semigroups)

The following surprised us:

Lemma (S., manuscript 2014)

There is a 9-element band $S_9 \in \mathcal{V}$ *with* NP*-hard* SMP*.*

SMP for bands (idempotent semigroups)

The following surprised us:

Lemma (S., manuscript 2014)

There is a 9-element band $S_9 \in \mathcal{V}$ with NP*-hard* SMP*.*

Idea of Proof.

Reduce SAT to SMP(S_9). $\square$

SMP for bands (idempotent semigroups)

The following surprised us:

Lemma (S., manuscript 2014)

There is a 9-element band $S_9 \in \mathcal{V}$ with NP*-hard* SMP*.*

Idea of Proof.

Reduce SAT to SMP(S_9). □

Theorem (S., manuscript 2014)

There is a 10-element band $S_{10} \in \mathcal{V}$ such that:

1. *S_{10} generates the same variety as S_9;*

SMP for bands (idempotent semigroups)

The following surprised us:

Lemma (S., manuscript 2014)

There is a 9-element band $S_9 \in \mathcal{V}$ with NP*-hard* SMP.

Idea of Proof.

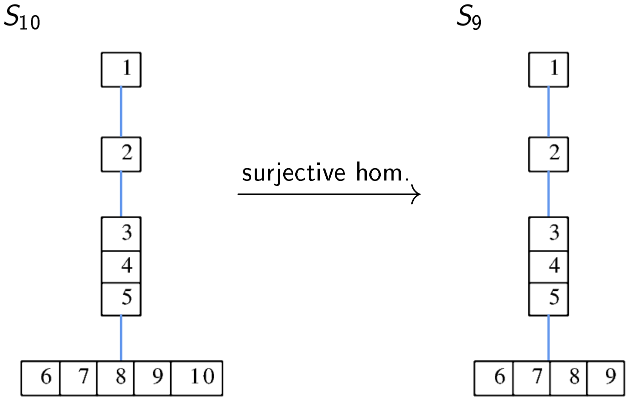
Reduce SAT to SMP(S_9). □

Theorem (S., manuscript 2014)

There is a 10-element band $S_{10} \in \mathcal{V}$ such that:

1. *S_{10} generates the same variety as S_9;*
2. SMP(S_{10}) *is still in* P.

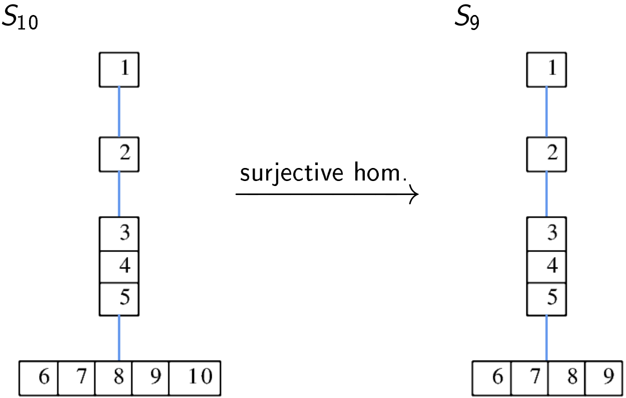
Eggbox diagrams of S_{10} and S_9



SMP in P

SMP NP-hard

Eggbox diagrams of S_{10} and S_9



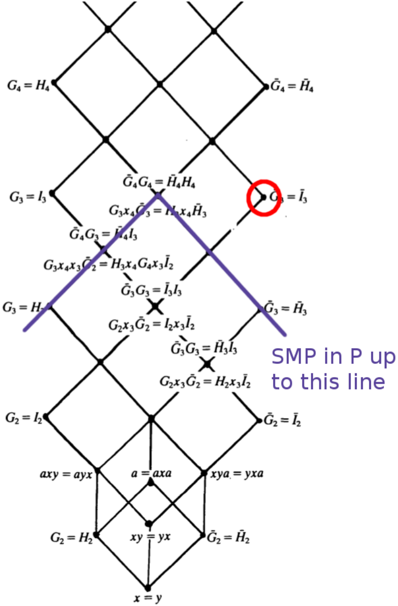
SMP in P

SMP NP-hard

Corollary

The SMP *for a homomorphic image can be harder than the* SMP *for the original semigroup (in case* P $\neq$ NP*).*

SMP for bands (idempotent semigroups)



The identities of $\mathcal{V} = [\bar{G}_3 \approx \bar{I}_3]$ do not help us anymore.

Quasiidentities

For a finite semigroup S, let $\mathsf{ISP}(S)$ denote the class of semigroups that can be embedded into direct powers of S.

Quasiidentities

For a finite semigroup S, let $\mathrm{ISP}(S)$ denote the class of semigroups that can be embedded into direct powers of S.

We call $\mathrm{ISP}(S)$ the *quasivariety generated by S*.

Theorem

For two finite semigroups S, T, we have:

1. $\mathrm{ISP}(S) = \mathrm{ISP}(T)$ *iff S and T satisfy the same quasiidentities.*

Quasiidentities

For a finite semigroup S, let $\mathrm{ISP}(S)$ denote the class of semigroups that can be embedded into direct powers of S.

We call $\mathrm{ISP}(S)$ the *quasivariety generated by S*.

Theorem

For two finite semigroups S, T, we have:

1. $\mathrm{ISP}(S) = \mathrm{ISP}(T)$ *iff S and T satisfy the same quasiidentities.*
2. *In this case* $\mathrm{SMP}(S) \equiv \mathrm{SMP}(T)$.

Quasiidentities

For a finite semigroup S, let $\mathrm{ISP}(S)$ denote the class of semigroups that can be embedded into direct powers of S.

We call $\mathrm{ISP}(S)$ the *quasivariety generated by S*.

Theorem

For two finite semigroups S, T, we have:

1. $\mathrm{ISP}(S) = \mathrm{ISP}(T)$ *iff S and T satisfy the same quasiidentities.*
2. *In this case* $\mathrm{SMP}(S) \equiv \mathrm{SMP}(T)$.

A *quasiidentity* is an expression of the form

$$(s_1 \approx t_1 \,\&\, \dots \,\&\, s_k \approx t_k) \to u \approx v.$$

We say a semigroup S *fulfills a quasiidentity* iff S satisfies the identity on the RHS whenever it satisfies the identities on the LHS.

Quasiidentities

The “behavior" of S_9 and S_{10} led us to the following quasiidentity:

$$\& \begin{pmatrix} dxye \approx de \\ he \approx e \\ hx \approx x \\ ded \approx d \\ exe \approx e \\ eye \approx e \end{pmatrix} \to dxe \approx de. \qquad (\lambda)$$

The band S_{10} fulfills λ, whereas S_9 does not.

Quasiidentities

The "behavior" of S_9 and S_{10} led us to the following quasiidentity:

$$\& \begin{pmatrix} dxye \approx de \\ he \approx e \\ hx \approx x \\ ded \approx d \\ exe \approx e \\ eye \approx e \end{pmatrix} \to dxe \approx de. \qquad (\lambda)$$

The band S_{10} fulfills λ, whereas S_9 does not.

Theorem (S., manuscript 2015)

1. *If a band S fulfills λ and the dual quasiidentity, then* $\mathrm{SMP}(S)$ *is in* P.
2. *Otherwise it is* NP*-hard.*

SMP for bands is in NP

Lemma (cf. Gerhard and Petrich, 1989 [4])

Let S be a finite band. Then there is a polynomial p such that each term function $t\colon S^k \to S$ is induced by a term of length $p(k)$.

SMP for bands is in NP

Lemma (cf. Gerhard and Petrich, 1989 [4])

Let S be a finite band. Then there is a polynomial p such that each term function $t\colon S^k \to S$ is induced by a term of length $p(k)$.

Corollary

SMP(S) *for a band S is in* NP.

SMP for bands is in NP

Lemma (cf. Gerhard and Petrich, 1989 [4])

Let S be a finite band. Then there is a polynomial p such that each term function $t\colon S^k \to S$ is induced by a term of length $p(k)$.

Corollary

SMP(S) *for a band S is in* NP*.*

Proof.

Fix an instance $a_1, \ldots, a_k, b \in S^n$.
Assume $b \in \langle a_1, \ldots, a_k \rangle$.

SMP for bands is in NP

Lemma (cf. Gerhard and Petrich, 1989 [4])

Let S be a finite band. Then there is a polynomial p such that each term function $t\colon S^k \to S$ is induced by a term of length $p(k)$.

Corollary

SMP(S) *for a band S is in* NP.

Proof.

Fix an instance $a_1, \ldots, a_k, b \in S^n$.
Assume $b \in \langle a_1, \ldots, a_k \rangle$.
Then $b = t(a_1, \ldots, a_k)$ for a term t with length $p(k)$. □

Conclusion

Theorem (Bulatov, Mayr, S., manuscript 2015)

Let S be a commutative semigroup.

1. SMP(S) *is in* P *if S is a nilpotent ideal extension of a union of groups.*
2. *It is* NP*-complete otherwise.*

Conclusion

Theorem (Bulatov, Mayr, S., manuscript 2015)

Let S be a commutative semigroup.

1. SMP(S) *is in* P *if S is a nilpotent ideal extension of a union of groups.*
2. *It is* NP*-complete otherwise.*

Theorem (S., manuscript 2014)

1. *If a 0-simple semigroup S is zero divisor free, then* SMP(S) *is in P.*
2. *Otherwise it is* NP*-hard.*

Conclusion

Theorem (S., manuscript 2014)

There are two finite bands

1. *which generate the same variety, and*
2. *whose* SMP*s have distinct complexity (in case* $\mathrm{P} \neq \mathrm{NP}$*).*

Conclusion

Theorem (S., manuscript 2014)

There are two finite bands

1. *which generate the same variety, and*
2. *whose* SMP*s have distinct complexity (in case* P $\neq$ NP*).*

Theorem (S., manuscript 2015)

1. *If a band S fulfills λ and the dual quasiidentity, then* SMP(S) *is in* P.

$$\& \begin{pmatrix} dxye \approx de \\ he \approx e \\ hx \approx x \\ ded \approx d \\ exe \approx e \\ eye \approx e \end{pmatrix} \to dxe \approx de. \qquad (\lambda)$$

2. *Otherwise it is* NP*-complete.*

A. P. Birjukov.
Varieties of idempotent semigroups.
Algebra i Logika, 9:255–273, 1970.

C. F. Fennemore.
All varieties of bands. I, II.
Math. Nachr., 48:237–252; ibid. 48 (1971), 253–262, 1971.

J. A. Gerhard.
The lattice of equational classes of idempotent semigroups.
J. Algebra, 15:195–224, 1970.

J. A. Gerhard and M. Petrich.
Varieties of bands revisited.
Proc. London Math. Soc. (3), 58(2):323–350, 1989.

R. Willard.
Four unsolved problems in congruence permutable varieties.
Talk at International Conference on Order, Algebra, and Logics, Vanderbilt University, Nashville, June 12–16, 2007.

Много вам хвала!

Multiplication tables

S_9	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	2	4	4	5	6	7	8	9
3	3	3	3	3	3	6	7	8	9
4	4	4	4	4	4	6	7	8	9
5	5	5	5	5	5	6	7	8	9
6	6	7	8	9	8	6	7	8	9
7	7	7	9	9	8	6	7	8	9
8	8	8	8	8	8	6	7	8	9
9	9	9	9	9	9	6	7	8	9

S_{10}	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	2	3	5	5	6	7	8	9	10
3	3	3	3	3	3	6	7	8	9	10
4	4	4	4	4	4	6	7	8	9	10
5	5	5	5	5	5	6	7	8	9	10
6	6	7	10	8	9	6	7	8	9	10
7	7	7	10	9	9	6	7	8	9	10
8	8	8	8	8	8	6	7	8	9	10
9	9	9	9	9	9	6	7	8	9	10
10	10	10	10	10	10	6	7	8	9	10

Reduce SAT to SMP(S_9)

SAT *(satisfiability of boolean formulas)*

Input: A boolean formula $\phi := \bigwedge_{i=1}^{n} c_i(x_1, \ldots, x_k)$ in conjunctive normal form.

Problem: Is ϕ satisfiable?

Reduce SAT to SMP(S_9)

SAT *(satisfiability of boolean formulas)*

Input: A boolean formula $\phi := \bigwedge_{i=1}^{n} c_i(x_1, \ldots, x_k)$ in conjunctive normal form.

Problem: Is ϕ satisfiable?

Encode the SAT instance into one of SMP(S_9):

$$\{a_1^0, \ldots, a_k^0, a_1^1, \ldots, a_k^1, u, v\}, \; b \quad \text{in} \quad {S_9}^{n+2k}.$$

In a_i^0 we encode in which clauses $\neg x_i$ occurs.
In a_i^1 we encode in which clauses x_i occurs.