Facets of the Finite Basis Problem for Finite Involution Semigroups

Igor Dolinka

dockie@dmi.uns.ac.rs

Department of Mathematics and Informatics, University of Novi Sad

Będlewo, June 2010

Glossary of terms

The equational theory $Eq(A)$ of an algebra A

$=$ the set of all identities (over some fixed countably infinite set X of variables, or letters) satisfied by A.

Let Σ be a set of identities. An identity $p \approx q$ is a consequence of Σ, written $\Sigma \models p \approx q$,

$=$ every algebra that satisfies all identities from Σ also satisfies $p \approx q$.

If $\Sigma \subseteq Eq(A)$ is such that every identity from $Eq(A)$ is a consequence of Σ, then Σ is called an (equational) basis of A.

A fundamental property that an algebra A may or may not have is that of having a finite basis. If there is a finite basis for identities of A, then A is said to be finitely based (FB). Otherwise, it is nonfinitely based (NFB).

Some classical positive results

Each of the following algebras is FB:

- finite groups (Oates & Powell, 1964)
- commutative semigroups (Perkins, 1968)
- finite lattices and lattice-based algebras (McKenzie, 1970)
- finite (associative) rings (L'vov; Kruse, 1973)
- algebras generating congruence distributive varieties with a finite residual bound (Baker, 1977)
- algebras generating congruence modular varieties with a finite residual bound (McKenzie, 1987)
- algebras generating congruence $\wedge$-semidistributive varieties with a finite residual bound (Willard, 2000)

Negative results

Examples of finite NFB algebras:

	0	1	2
0	0	0	0
1	0	0	1
2	0	2	2

  (Murskiĭ, 1965)
- a certain 6-element semigroup of matrices (Perkins, 1968)
- a certain finite *pointed* group (Bryant, 1982)
- the full transformation semigroup $\mathcal{T}_n$ for $n \geq 3$ and the full semigroup of binary relations $\mathcal{R}_n$ for $n \geq 2$
- a certain 7-element semiring of binary relations (ID, 2007)

Tarski's Finite Basis Problem: Is there any algorithmic way to distinguish between finite FB and NFB algebras?

McKenzie's solution of the Tarski problem

No!

Theorem (McKenzie, 1996)

There is no algorithm to decide whether a finite algebra is FB.

This is exactly why it is so interesting to study the (N)FB property, especially for finite algebras.

The Tarski-Sapir problem: Is there an algorithm to decide whether a finite semigroup is FB? This problem is still open.

M. V. Volkov: *The finite basis problem for finite semigroups*, Sci. Math. Jpn. **53** (2001), 171–199.
http://csseminar.kadm.usu.ru/MATHJAP_revisited.pdf

Volkov's NFB criterion (1989)

Let A_2 be the 5-element semigroup given by the presentation

$$\langle a, b : \; a^2 = a = aba, \; b^2 = 0, \; bab = b \rangle.$$

This is just the Rees matrix semigroup over a trivial group $E = \{e\}$ with the sandwich matrix

$$\begin{pmatrix} e & e \\ 0 & e \end{pmatrix}$$

Fact

Of all varieties generated by Rees matrix semigroups with trivial subgroups, A_2 generates the largest one.

Fact

A_2 is representable by matrices (over any field).

Volkov's NFB criterion (1989)

Theorem (M. V. Volkov, 1989)

Let S be a semigroup and T a subsemigroup of S. Assume that there exist a positive integer d and a group G satisfying $x^d \approx e$ such that

- *$a^d \in T$ for all $a \in S$, and*
- *$G \in \operatorname{var} S$, but $G \notin \operatorname{var} T$.*

If $A_2 \in \operatorname{var} S$, then S is NFB.

Corollary

The following semigroups are NFB:

- *the full transformation semigroup $\mathcal{T}_n$ $(n \geq 3)$*
- *the full semigroup of binary relations $\mathcal{B}_n$ $(n \geq 2)$*
- *the semigroup of partial transformations $\mathcal{PT}_n$ $(n \geq 2)$*
- *matrix semigroups $\mathcal{M}_n(\mathbb{F})$ for any $n \geq 2$ and any finite field $\mathbb{F}$*

Unary semigroups

Unary semigroup

$=$ a structure $(S, \cdot, ^*)$ such that $(S, \cdot)$ is a semigroup and * is a unary operation on S

Involution semigroup

$=$ a unary semigroup satisfying $(xy)^* \approx y^*x^*$ and $(x^*)^* \approx x$

Examples

- groups
- inverse semigroups
- regular *-semigroups $(xx^*x \approx x)$
- matrix semigroups with transposition $\mathcal{M}_n(\mathbb{F}) = (\mathrm{M}_n(\mathbb{F}), \cdot, ^{\mathrm{T}})$

'Unary version' of Volkov's Theorem

For a unary semigroup S, let $\mathrm{H}(S)$ denote the Hermitian subsemigroup of S, generated by aa^* for all $a \in S$.

For a variety $\mathbf{V}$ of unary semigroups, let $\mathrm{H}(\mathbf{V})$ be the subvariety of $\mathbf{V}$ generated by all $\mathrm{H}(S)$, $S \in \mathbf{V}$.

Furthermore, let K_3 be the 10-element unary Rees matrix semigroup over a trivial group $E = \{e\}$ with the sandwich matrix

$$\begin{pmatrix} e & e & e \\ e & e & 0 \\ e & 0 & e \end{pmatrix},$$

while $(i, e, j)^* = (j, e, i)$ and $0^* = 0$.

Fact

K_3 generates the variety of all strict combinatorial regular *-semigroups (studied by K. Auinger in 1992).

'Unary version' of Volkov's Theorem

Theorem (K. Auinger, M. V. Volkov, cca. 1991/92)

Let S be a unary semigroup such that $\mathbf{V} = \mathrm{var}\, S$ contains K_3. If there exist a group G which belongs to $\mathbf{V}$ but not to $\mathrm{H}(\mathbf{V})$, then S is NFB.

Corollary

The following unary semigroups are NFB:

- *the full involution semigroup of binary relations $\mathcal{R}_n^\vee$ ($n \geq 2$), endowed with relational converse*
- *matrix semigroups with transposition $\mathcal{M}_n(\mathbb{F})$, where $\mathbb{F}$ is a finite field, $|\mathbb{F}| \geq 3$*
- *matrix semigroups $(\mathrm{M}_2(\mathbb{F}), \cdot, ^\dagger)$, where $\mathbb{F}$ is either a finite field such that $|\mathbb{F}| \equiv 3 \pmod 4$, or a subfield of $\mathbb{C}$ closed under complex conjugation, and † is the unary operation of taking the Moore-Penrose inverse.*

However...

The Auinger-Volkov paper remained unpublished for $>$15 (that is, almost 20) years, because the following question remained unsettled.

Problem

Exactly which of the involution semigroups $\mathcal{M}_n(\mathbb{F})$ are NFB, $n \geq 2$, $\mathbb{F}$ is a finite field?

Also, the following open problem was both intriguing and inviting.

Problem

Do finite INFB involution semigroups exist at all?

INFB...(?)

An algebra A is inherently nonfinitely based (INFB) if:

- A generates a locally finite variety, and
- any locally finite variety $\mathbf{V}$ containing A is NFB.

Said otherwise, for any finite set of identities Σ satisfied by A, the variety defined by Σ is not locally finite.

Therefore, problems concerning INFB algebras are in fact Burnside-type problems.

INFB algebras are a powerful tool for proving the NFB property; namely, the INFB property is "contagious":

> if $\operatorname{var} A$ is locally finite and contains an INFB algebra B, then A is NFB.

In particular, B is NFB.

Finite INFB semigroups: a success story

M. V. Sapir, 1987: a full description of (finite) INFB semigroups.

Zimin words: $Z_1 = x_1$ and $Z_{n+1} = Z_n x_{n+1} Z_n$ for $n \geq 1$.

Theorem (Sapir, 1987)

Let S be a finite semigroup. Then

$$S \text{ is INFB} \Longleftrightarrow S \not\models Z_n \approx W$$

for all $n \geq 1$ and all words $W \neq Z_n$.

Sapir also found an effective structural description of finite INFB semigroups, thus proving

Theorem (Sapir, 1987)

It is decidable whether a finite semigroup is INFB or not.

Examples of finite INFB semigroups

The example: the 6-element Brandt inverse monoid

$$B_2^1 = \langle a, b : \; a^2 = b^2 = 0, \; aba = a, \; bab = b \rangle \cup \{1\}.$$

B_2^1 is representable by matrices (over any field):

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

B_2^1 is obtained by adjoining an identity element to the Rees matrix semigroup over the trivial group $E = \{e\}$ with the sandwich matrix

$$\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}$$

Examples of finite INFB semigroups

Proposition

B_2^1 fails to satisfy a nontrivial identity of the form $Z_n \approx W$. Hence, it is INFB.

Corollary

For any $n \geq 2$ and any (semi)ring R, the matrix semigroup $\mathcal{M}_n(R)$ is (I)NFB.

Since $B_2^1 \in \operatorname{var} A_2^1$, where A_2 is the 5-element semigroup from Volkov's theorem, we have that A_2^1 is (I)NFB as well.

The same argument applies to $\mathcal{T}_n$ ($n \geq 3$), $\mathcal{R}_n$ ($n \geq 2$), $\mathcal{PT}_n$ ($n \geq 2$),...

What a difference an involution makes? Well...

How on Earth is the case of unary semigroups different?

For example, an involution * can be defined on B_2^1 by $a^* = b$, $b^* = a$, the remaining 4 elements (which are idempotents: $0, 1, ab, ba$) being fixed. This turns B_2^1 into an inverse semigroup.

Surprise...!!!

Theorem (Sapir, 1993)

B_2^1 is not INFB as an inverse semigroup. In fact, there is no finite INFB inverse semigroup at all!

Still, the inverse semigroup B_2^1 is NFB (Kleiman, 1979).

So, once again:

Problem

Do finite INFB involution semigroups exist at all?

An INFB criterion for involution semigroups

Yes!

Theorem (ID, cca. 2007/08)

Let S be an involution semigroup such that $\operatorname{var} S$ *is locally finite. If S fails to satisfy any nontrivial identity of the form*

$$Z_n \approx W,$$

where W is an involutorial word (a word over the 'doubled' alphabet $X \cup X^*$), then S is INFB.

How about a (finite) example?

‘C’mon baby, let’s do the twist...!’

Rescue: Luckily, B_2^1 admits one more involution aside from the inverse one: define the nilpotents a, b (and, of course, $0, 1$) to be fixed by *, which results in $(ab)^* = ba$ and $(ba)^* = ab$.

In this way we obtain the twisted Brandt monoid TB_2^1.

Proposition

TB_2^1 fails to satisfy a nontrivial identity of the form $Z_n \approx W$. Hence, it is INFB.

Similarly to B_2^1, this little guy is quite powerful.

Remark

Analogously, one can also define TA_2^1, the “involutorial version” of A_2^1, which is also INFB.

Examples of finite INFB involution semigroups

- $\mathcal{R}_n^{\vee}$, the involution semigroup of binary relations, is (I)NFB for all $n \geq 2$,
  - Reason: TB_2^1 embeds into $\mathcal{R}_2^{\vee}$.
- $\mathcal{M}_2(\mathbb{F})$, provided $|\mathbb{F}| \not\equiv 3 \pmod 4$,
  - Reason: This is precisely the case when -1 has a square root in $\mathbb{F}$, which is sufficient and necessary for TB_2^1 to embed into $\mathcal{M}_2(\mathbb{F})$.
- $\mathcal{M}_n(\mathbb{F})$ for all $n \geq 3$ and all finite fields $\mathbb{F}$.
  - Reason: TB_2^1 embeds into $\mathcal{M}_n(\mathbb{F})$ as a consequence of the Chevalley-Warning theorem from algebraic number theory (!!!).

So, what about $\mathcal{M}_2(\mathbb{F})$ if $|\mathbb{F}| \equiv 3 \pmod 4$?
(We already know it is NFB.)

Non-INFB results

Theorem (ID, 2010)

Let S be a finite involution semigroup satisfying a nontrivial identity of the form $Z_n \approx W$ such that $B_2^1 \notin \mathrm{var}\, S$. Then S is not INFB.

Proof idea: Either W is an ordinary semigroup word, or for any *-fixed idempotent e of S, $\mathrm{var}\, eSe$ consists of involution semilattices of Archimedean semigroups.

Theorem (ID, 2010)

Let S be a finite semigroup satisfying an identity of the form $Z_n \approx Z_n W$. Then S is not INFB.

Proof idea: Stretching the approach of Margolis & Sapir (1995) developed for finitely generated quasivarieties of semigroups to what seems to be the final limits of that method: certain semigroup quasiidentities can be "encoded" into unary semigroup identities.

Non-INFB results

Corollary

No finite regular *-semigroup is INFB.
(Namely, $x \approx x(x^*x)$ holds.)

Corollary (ID, 2010)

For any finite group G, the involution semigroup of subsets $\mathcal{P}_G^* = (\mathcal{P}(G), \cdot, ^*)$ is not INFB.
(Namely, $\mathcal{P}_G^*$ satisfies $Z_n \approx Z_n x_1^* x_1$ for $n = |G| + 2$.)

Remark

The ordinary power semigroup $\mathcal{P}_G = (\mathcal{P}(G), \cdot)$ is INFB if and only if G is not Dedekind.

Non-INFB results

Proposition (Crvenković, 1982)

If a finite involution semigroup S admits a Moore-Penrose inverse †, then the inverse is term-definable in S.

In particular, such a semigroup satisfies $x \approx x \cdot w(x, x^*) \cdot x$ for some $w \implies$ it is not INFB.

Proposition

The involution semigroup of 2×2 matrices over a finite field $\mathbb{F}$ with transposition admits a Moore-Penrose inverse if and only if $|\mathbb{F}| \equiv 3 \pmod 4$.

This completes our classification! ♡

Solution to the (I)NFB problem for matrix involution semigroups

Theorem (Auinger, ID, Volkov, 2008-10)

Let $n \geq 2$ and $\mathbb{F}$ be a finite field. Then

(1) $\mathcal{M}_n(\mathbb{F})$ *is not finitely based;*

(2) $\mathcal{M}_n(\mathbb{F})$ *is INFB if and only if either $n \geq 3$, or $n = 2$ and $|\mathbb{F}| \not\equiv 3 \pmod 4$.*

The gap

Unfortunately, we have not yet accomplished a full classification of finite involution semigroups with respect to the INFB property. We don't know what to do with finite involution semigroups (if they exist) such that:

(a) $B_2^1 \in \operatorname{var} S$,

(b) S satisfies a nontrivial identity of the form $Z_n \approx W$,

(c) S, however, fails to satisfy an identity of the form $Z_n \approx Z_n W'$.

This "gap" does not occur for ordinary semigroups, as (b) renders (a) impossible. But this is no longer the case for involution semigroups!

Test-Example

Is $xyxzxyx \approx xyxx^*xzxyx$ implying the non-INFB property?

THANK YOU!

Questions and comments to:

dockie@dmi.uns.ac.rs

Preprints may be found at:

http://sites.dmi.rs/personal/dolinkai