The 3rd NOVI SAD ALGEBRAIC
CONFERENCE (NSAC 2009)
August 20, 2009

(I)NFB Results for Finite Unary Semigroups

Igor Dolinka

Department of Mathematics and Informatics
Faculty of Science, University of Novi Sad
`dockie@dmi.uns.ac.rs`

Glossary

A fundamental property that a (finite) algebra $\mathcal{A}$ may have is that of being

NFB (NonFinitely Based) = the equational theory of $\mathcal{A}$ is not finitely axiomatizable

Glossary

A fundamental property that a (finite) algebra $\mathcal{A}$ may have is that of being

NFB (NonFinitely Based) = the equational theory of $\mathcal{A}$ is not finitely axiomatizable

An even stronger property (and a method to prove that $\mathcal{A}$ is NFB) is

INFB (Inherently NFB) = $\mathbb{V}(\mathcal{A})$ is locally finite + any l.f. variety that contains $\mathcal{A}$ is NFB

The NFB problem for finite semigroups

M. V. Volkov: *The finite basis problem for finite semigroups*, Sci. Math. Jpn. **53** (2001), 171–199.

The NFB problem for finite semigroups

M. V. Volkov: *The finite basis problem for finite semi-groups*, Sci. Math. Jpn. **53** (2001), 171–199.

The ultimate goal:

Characterize the NFB finite semigroups.

The NFB problem for finite semigroups

M. V. Volkov: *The finite basis problem for finite semigroups*, Sci. Math. Jpn. **53** (2001), 171–199.

The ultimate goal:

Characterize the NFB finite semigroups.

But: Is an algorithmic description possible in the first place? (The Tarski-Sapir Problem)

INFB finite semigroups

Fully described by M. V. Sapir (1987).

INFB finite semigroups

Fully described by M. V. Sapir (1987).

Zimin words: $Z_1 \equiv x_1$, and $Z_{n+1} \equiv Z_n x_{n+1} Z_n$ for $n \geqslant 1$

INFB finite semigroups

Fully described by M. V. Sapir (1987).

Zimin words: $Z_1 \equiv x_1$, and $Z_{n+1} \equiv Z_n x_{n+1} Z_n$ for $n \geqslant 1$

Let $\mathcal{S}$ be a finite semigroup.

$$\mathcal{S} \text{ is INFB} \iff \mathcal{S} \not\models Z_n = W$$

for all n and any word $W \not\equiv Z_n$.

INFB finite semigroups: an example

The example: the 6-element Brandt monoid

$$\mathcal{B}_2^1 = \langle a, b : \; a^2 = b^2 = 0, \; aba = a, \; bab = b \rangle \cup \{1\}.$$

INFB finite semigroups: an example

The example: the 6-element Brandt monoid

$$\mathcal{B}_2^1 = \langle a, b : \; a^2 = b^2 = 0, \; aba = a, \; bab = b \rangle \cup \{1\}.$$

$\mathcal{B}_2^1$ is representable by

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

INFB finite semigroups: an example

The example: the 6-element Brandt monoid

$$\mathcal{B}_2^1 = \langle a, b : \ a^2 = b^2 = 0, \ aba = a, \ bab = b \rangle \cup \{1\}.$$

$\mathcal{B}_2^1$ is representable by

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

Consequence: Every matrix semigroup $M_n(R)$, $n \geqslant 2$, over a finite (semi)ring R with 1 is (I)NFB.

Unary semigroups

Unary semigroup: a structure $\mathcal{S} = (S, \cdot, ^*)$ such that $(S, \cdot)$ is a semigroup and * is a unary operation on S.

Unary semigroups

Unary semigroup: a structure $\mathcal{S} = (S, \cdot, {}^*)$ such that $(S, \cdot)$ is a semigroup and * is a unary operation on S.

Involution semigroup: a unary semigroup satisfying the identities $(xy)^* = y^*x^*$ and $(x^*)^* = x$.

Unary semigroups

Unary semigroup: a structure $\mathcal{S} = (S, \cdot, ^*)$ such that $(S, \cdot)$ is a semigroup and * is a unary operation on S.

Involution semigroup: a unary semigroup satisfying the identities $(xy)^* = y^*x^*$ and $(x^*)^* = x$.

Examples: groups, inverse semigroups, regular *-semigroups ($x = xx^*x$),...

Does * make any difference?

Does $*$ make any difference?

At the first glance, it may seem that the unary operation $*$ cannot spoil the picture, in the sense of the expectation that the vast majority of (I)NFB results for finite semigroups can be easily “translated” into the realm of finite unary/involution semigroups.

Does $*$ make any difference?

At the first glance, it may seem that the unary operation $*$ cannot spoil the picture, in the sense of the expectation that the vast majority of (I)NFB results for finite semigroups can be easily “translated” into the realm of finite unary/involution semigroups.

Fortunately – and somewhat surprisingly – this is quite far from the truth.

Someone said *no*? Think again.

Someone said *no*? Think again.

Of course, $\mathcal{B}_2^1$ is an inverse semigroup as soon as we define $a^* = b$ (which forces $b^* = a$, while the remaining 4 elements (the idempotents: $0, 1, ab, ba$) are fixed).

Someone said *no*? Think again.

Of course, $\mathcal{B}_2^1$ is an inverse semigroup as soon as we define $a^* = b$ (which forces $b^* = a$, while the remaining 4 elements (the idempotents: $0, 1, ab, ba$) are fixed).

However, $\mathcal{B}_2^1$ is not INFB as an inverse semigroup.

Someone said *no*? Think again.

Of course, $\mathcal{B}_2^1$ is an inverse semigroup as soon as we define $a^* = b$ (which forces $b^* = a$, while the remaining 4 elements (the idempotents: $0, 1, ab, ba$) are fixed).

However, $\mathcal{B}_2^1$ is not INFB as an inverse semigroup.

Namely, M. V. Sapir proved (around 1992) that there is no INFB finite inverse semigroup at all!

Someone said *no*? Think again.

Of course, $\mathcal{B}_2^1$ is an inverse semigroup as soon as we define $a^* = b$ (which forces $b^* = a$, while the remaining 4 elements (the idempotents: $0, 1, ab, ba$) are fixed).

However, $\mathcal{B}_2^1$ is not INFB as an inverse semigroup.

Namely, M. V. Sapir proved (around 1992) that there is no INFB finite inverse semigroup at all!

Moreover, by using the techniques developed a year later by Margolis and Sapir for finitely generated quasivarieties, it follows that the same holds for all finite regular *-semigroups as well.

On the other hand...

Around the same time (1992/93), K. Auinger and M. V. Volkov obtained a unary counterpart of Volkov's well-known NFB criterion. Let's recall what is this all about.

On the other hand...

Around the same time (1992/93), K. Auinger and M. V. Volkov obtained a unary counterpart of Volkov's well-known NFB criterion. Let's recall what is this all about.

- For a unary semigroup $\mathcal{S}$, let $\mathbf{He}(\mathcal{S})$ be its *Hermitian subsemigroup*, the one generated by all elements xx^*, $x \in S$.

On the other hand...

Around the same time (1992/93), K. Auinger and M. V. Volkov obtained a unary counterpart of Volkov's well-known NFB criterion. Let's recall what is this all about.

- For a unary semigroup $\mathcal{S}$, let $\mathbf{He}(\mathcal{S})$ be its *Hermitian subsemigroup*, the one generated by all elements xx^*, $x \in S$.
- For a unary semigroup variety $\mathbb{V}$, let $\mathbf{He}(\mathbb{V})$ be the variety generated by all $\mathbf{He}(\mathcal{S})$, $\mathcal{S} \in \mathbb{V}$.

On the other hand... (continued)

- Let $\mathcal{K}_3$ be the combinatorial unary Rees matrix semigroup with the sandwich matrix

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

the unary operation being defined by $(i,j)^* = (j,i)$ and $0^* = 0$.

On the other hand... (continued)

- Let $\mathcal{K}_3$ be the combinatorial unary Rees matrix semigroup with the sandwich matrix

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

the unary operation being defined by $(i, j)^* = (j, i)$ and $0^* = 0$.

Theorem. Let $\mathbb{V}$ be a unary semigroup variety containing $\mathcal{K}_3$. If there exists a group $\mathcal{G} \in \mathbb{V} \setminus \mathbf{He}(\mathbb{V})$, then $\mathbb{V}$ is NFB.

Applications of the Auinger-Volkov Theorem

The following are NFB:

Applications of the Auinger-Volkov Theorem

The following are NFB:

- for each finite $n > 1$, the involution semigroup $\mathcal{R}e\ell(n)$ of all binary relations on an n-element set, endowed with relational converse;

Applications of the Auinger-Volkov Theorem

The following are NFB:

- for each finite $n > 1$, the involution semigroup $\mathcal{R}e\ell(n)$ of all binary relations on an n-element set, endowed with relational converse;
- matrix involution semigroups $(\mathrm{M}_2(\mathcal{K}), \cdot, {}^T)$, where $\mathcal{K}$ is a finite field with more than 2 elements;

Applications of the Auinger-Volkov Theorem

The following are NFB:

- for each finite $n > 1$, the involution semigroup $\mathcal{R}e\ell(n)$ of all binary relations on an n-element set, endowed with relational converse;
- matrix involution semigroups $(\mathrm{M}_2(\mathcal{K}), \cdot, ^T)$, where $\mathcal{K}$ is a finite field with more than 2 elements;
- unary matrix semigroups $(\mathrm{M}_2(\mathcal{K}), \cdot, ^\dagger)$, where $\mathcal{K}$ is either a finite field such that $|K| \equiv 3 \pmod 4$ or a subfield of $\mathbb{C}$ closed under complex conjugation, and † is the operation of taking the Moore-Penrose inverse.

However, some nagging questions remained...

However, some nagging questions remained...

(1) Do finite INFB involution semigroups exist at all?

(2) In particular, what about $\mathcal{R}e\ell(n)$?

(3) Exactly which of the $(\mathrm{M}_n(\mathcal{K}), \cdot, {}^T)$ are NFB? ($\mathcal{K}$ finite and either $n \geqslant 3$, or $n = 2$ and $|K| = 2$)

However, some nagging questions remained...

(1) Do finite INFB involution semigroups exist at all?

(2) In particular, what about $\mathcal{R}e\ell(n)$?

(3) Exactly which of the $(\mathrm{M}_n(\mathcal{K}),\cdot,{}^T)$ are NFB? ($\mathcal{K}$ finite and either $n \geqslant 3$, or $n = 2$ and $|K| = 2$)

These questions had to wait some 15 years to be answered.

However, some nagging questions remained...

(1) Do finite INFB involution semigroups exist at all?

(2) In particular, what about $\mathcal{R}e\ell(n)$?

(3) Exactly which of the $(\mathrm{M}_n(\mathcal{K}), \cdot, {}^T)$ are NFB? ($\mathcal{K}$ finite and either $n \geqslant 3$, or $n = 2$ and $|K| = 2$)

These questions had to wait some 15 years to be answered. The answers turned out to be:

(1) Yes.

(2) They are all INFB whenever $n > 1$.

(3) All of them. They also allow an exact characterization of the INFB property.

Theorem 1

Let $\mathcal{S}$ be a finite involution semigroup failing to satisfy any nontrivial identity of the form

$$Z_n = W,$$

where W is an *involutorial* word (a word over a 'doubled' alphabet $X \cup X^*$). Then $\mathcal{S}$ is INFB.

Theorem 1

Let $\mathcal{S}$ be a finite involution semigroup failing to satisfy any nontrivial identity of the form

$$Z_n = W,$$

where W is an *involutorial* word (a word over a 'doubled' alphabet $X \cup X^*$). Then $\mathcal{S}$ is INFB.

The proof, of course, relies in part on the ordinary semigroup case, but requires extra ingredients. The same ingredients are integral parts of Sapir's own proof of the BEM-Zimin Theorem developed for his Combinatorics on Words with Applications course.

Theorem 1

Let $\mathcal{S}$ be a finite involution semigroup failing to satisfy any nontrivial identity of the form

$$Z_n = W,$$

where W is an *involutorial* word (a word over a 'doubled' alphabet $X \cup X^*$). Then $\mathcal{S}$ is INFB.

The proof, of course, relies in part on the ordinary semigroup case, but requires extra ingredients. The same ingredients are integral parts of Sapir's own proof of the BEM-Zimin Theorem developed for his Combinatorics on Words with Applications course.

However, is there such a finite involutorial semigroup? As we saw, $\mathcal{B}_2^1$ won't do, since it satisfies $x = xx^*x$.

Theorem 1: an example

It is often forgotten that the semigroup $\mathcal{B}_2^1$ 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 $\mathcal{TB}_2^1$.

Theorem 1: an example

It is often forgotten that the semigroup $\mathcal{B}_2^1$ 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 $\mathcal{TB}_2^1$.

It is not difficult to establish that $\mathcal{TB}_2^1$ meets the conditions of Theorem 1 $\Longrightarrow$ $\mathcal{TB}_2^1$ is INFB.

Theorem 1: an example

It is often forgotten that the semigroup $\mathcal{B}_2^1$ 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 $\mathcal{TB}_2^1$.

It is not difficult to establish that $\mathcal{TB}_2^1$ meets the conditions of Theorem 1 $\Longrightarrow$ $\mathcal{TB}_2^1$ is INFB.

Similarly to $\mathcal{B}_2^1$, this little guy is quite powerful.

Theorem 1: applications

$\mathcal{TB}_2^1$ embeds into $\mathcal{R}e\ell(2) \Longrightarrow \mathcal{R}e\ell(n)$ is INFB for all $n \geqslant 2$.

Theorem 1: applications

$\mathcal{TB}_2^1$ embeds into $\mathcal{R}e\ell(2) \Longrightarrow \mathcal{R}e\ell(n)$ is INFB for all $n \geqslant 2$.

$\mathcal{TB}_2^1$ embeds into $(\mathrm{M}_2(\mathcal{K}), \cdot, ^T)$ whenever $|K| \not\equiv 3 \pmod 4$ (for this is exactly the case when -1 has a square root in $\mathcal{K}$).

Theorem 1: applications

$\mathcal{TB}_2^1$ embeds into $\mathcal{R}e\ell(2) \Longrightarrow \mathcal{R}e\ell(n)$ is INFB for all $n \geqslant 2$.

$\mathcal{TB}_2^1$ embeds into $(\mathrm{M}_2(\mathcal{K}), \cdot, {}^T)$ whenever $|K| \not\equiv 3 \pmod 4$ (for this is exactly the case when -1 has a square root in $\mathcal{K}$).

$\mathcal{TB}_2^1$ embeds into $(\mathrm{M}_n(\mathcal{K}), \cdot, {}^T)$ for all $n \geqslant 3$ and all finite $\mathcal{K}$, as a consequence of the Chevalley-Warning Theorem (!!!) from algebraic number theory (argument courtesy & ingenuity of K. Auinger).

Theorem 1: applications

$\mathcal{TB}_2^1$ embeds into $\mathcal{R}e\ell(2) \Longrightarrow \mathcal{R}e\ell(n)$ is INFB for all $n \geqslant 2$.

$\mathcal{TB}_2^1$ embeds into $(\mathrm{M}_2(\mathcal{K}), \cdot, ^T)$ whenever $|K| \not\equiv 3 (\mathrm{mod}\ 4)$ (for this is exactly the case when -1 has a square root in $\mathcal{K}$).

$\mathcal{TB}_2^1$ embeds into $(\mathrm{M}_n(\mathcal{K}), \cdot, ^T)$ for all $n \geqslant 3$ and all finite $\mathcal{K}$, as a consequence of the Chevalley-Warning Theorem (!!!) from algebraic number theory (argument courtesy & ingenuity of K. Auinger).

Other applications as well...

Theorem 2

Let $\mathcal{S}$ be a finite involution semigroup satisfying an identity of the form

$$Z_n = Z_n W$$

for some $n \geqslant 1$ and an involutorial word W. Then $\mathcal{S}$ is not INFB.

Theorem 2

Let $\mathcal{S}$ be a finite involution semigroup satisfying an identity of the form

$$Z_n = Z_n W$$

for some $n \geqslant 1$ and an involutorial word W. Then $\mathcal{S}$ is not INFB.

The proof uses the ideas from the Margolis-Sapir approach to finitely generated quasivarieties of semigroups, and the result seems to be the final 'stretching' of that method to involution semigroups.

Theorem 2: applications

By an old result of S. Crvenković (1982), if a finite involution semigroup admits a Moore-Penrose inverse, then the inverse is term-definable. Consequently, any such involution semigroup will satisfy an identity of the form $x = xw(x, x^*)x \implies$ it is not INFB.

Theorem 2: applications

By an old result of S. Crvenković (1982), if a finite involution semigroup admits a Moore-Penrose inverse, then the inverse is term-definable. Consequently, any such involution semigroup will satisfy an identity of the form $x = xw(x, x^*)x \Longrightarrow$ it is not INFB.

This settles the case of 2×2 matrix semigroups with transposition as they admit a Moore-Penrose inverse iff $|K| \equiv 3 \pmod 4$.

Theorem 2: applications

By an old result of S. Crvenković (1982), if a finite involution semigroup admits a Moore-Penrose inverse, then the inverse is term-definable. Consequently, any such involution semigroup will satisfy an identity of the form $x = xw(x, x^*)x \implies$ it is not INFB.

This settles the case of 2×2 matrix semigroups with transposition as they admit a Moore-Penrose inverse iff $|K| \equiv 3 \pmod 4$.

So, one cannot hope for INFB results whenever the MP-inverse is around...

Theorem 3

Let $\mathcal{S}$ be a finite involution semigroup satisfying a non-trivial identity of the form $Z_n = W$ such that the variety $\mathbb{V}(\mathcal{S})$ omits the inverse semigroup $\mathcal{B}_2^1$. Then $\mathcal{S}$ is not INFB.

Theorem 3

Let $\mathcal{S}$ be a finite involution semigroup satisfying a non-trivial identity of the form $Z_n = W$ such that the variety $\mathbb{V}(\mathcal{S})$ omits the inverse semigroup $\mathcal{B}_2^1$. Then $\mathcal{S}$ is not INFB.

Key argument: Under the given conditions, W is either an ordinary word (when everything goes smoothly), or for an arbitrary *-fixed idempotent e, $\mathbb{V}(e\mathcal{S}e)$ consists entirely of involution semilattices of Archimedean semigroups (by a result of I.D. from 2005).

So, what remains...?

$\mathcal{S}$ – a finite involution semigroup such that:

(1) $\mathcal{B}_2^1 \in \mathbb{V}(\mathcal{S})$,
(2) $\mathcal{S}$ satisfies a nontrivial identity of the form $Z_n = W$,
(3) $\mathcal{S}$ fails to satisfy a nontrivial identity of the form $Z_k = Z_k U$.

So, what remains...?

$\mathcal{S}$ – a finite involution semigroup such that:

(1) $\mathcal{B}_2^1 \in \mathbb{V}(\mathcal{S})$,
(2) $\mathcal{S}$ satisfies a nontrivial identity of the form $Z_n = W$,
(3) $\mathcal{S}$ fails to satisfy a nontrivial identity of the form $Z_k = Z_k U$.

A tantalizing question: is there such $\mathcal{S}$ in the first place?

So, what remains...?

$\mathcal{S}$ – a finite involution semigroup such that:

(1) $\mathcal{B}_2^1 \in \mathbb{V}(\mathcal{S})$,
(2) $\mathcal{S}$ satisfies a nontrivial identity of the form $Z_n = W$,
(3) $\mathcal{S}$ fails to satisfy a nontrivial identity of the form $Z_k = Z_k U$.

A tantalizing question: is there such $\mathcal{S}$ in the first place?

In the ordinary semigroup case the answer is no, as (2) makes (1) impossible (while in the involutorial case these two are not automatically incompatible).

So, what remains...?

$\mathcal{S}$ – a finite involution semigroup such that:

(1) $\mathcal{B}_2^1 \in \mathbb{V}(\mathcal{S})$,
(2) $\mathcal{S}$ satisfies a nontrivial identity of the form $Z_n = W$,
(3) $\mathcal{S}$ fails to satisfy a nontrivial identity of the form $Z_k = Z_k U$.

A tantalizing question: is there such $\mathcal{S}$ in the first place?

In the ordinary semigroup case the answer is no, as (2) makes (1) impossible (while in the involutorial case these two are not automatically incompatible).

If the answer is yes, then there is still work to do. Some identities can be taken care of by combining all the previous approaches.

So, what remains...?

$\mathcal{S}$ – a finite involution semigroup such that:

(1) $\mathcal{B}_2^1 \in \mathbb{V}(\mathcal{S})$,
(2) $\mathcal{S}$ satisfies a nontrivial identity of the form $Z_n = W$,
(3) $\mathcal{S}$ fails to satisfy a nontrivial identity of the form $Z_k = Z_k U$.

A tantalizing question: is there such $\mathcal{S}$ in the first place?

In the ordinary semigroup case the answer is no, as (2) makes (1) impossible (while in the involutorial case these two are not automatically incompatible).

If the answer is yes, then there is still work to do. Some identities can be taken care of by combining all the previous approaches.

Test-example: Is $xyxzxyx = xyxx^*xzxyx$ 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