A Nonfinitely Based Finite Semiring

Igor Dolinka
The finite basis problem

\( A \) – a finite algebra
\( \text{Eq}(A) \) – the set of all identities true in \( A \)

Is \( \text{Eq}(A) \) finitely axiomatizable (finitely based)?

McKenzie (1996): in general, \textcolor{red}{\text{undecidable}}
Finitely based finite algebras

- groups: Oates & Powell (1966)
- commutative semigroups: Perkins (1968)
- rings: Львов, Kruse (1973)
Some NFB finite algebras

- Мурский (1965): a 3-element groupoid
  - this is a special case of NFB graph algebras – Baker, McNulty, Werner (1987)
- Perkins (1968): a 6-element semigroup = the Brandt monoid $B_2^1$ of order 2

\[
\begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}, \begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \begin{pmatrix}
0 & 1 \\
0 & 0
\end{pmatrix}, \begin{pmatrix}
0 & 0 \\
1 & 0
\end{pmatrix}, \begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix}, \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\]

- the Perkins’ semigroup is INFB = each l.f. variety containing it is NFB (Sapir, 1987)
Semirings

Semiring = an algebra \((\Sigma,+,\cdot,0)\) such that
- \((\Sigma,+ ,0)\) is a commutative monoid,
- \((\Sigma, \cdot)\) is a semigroup,
- the multiplication distributes over addition.

If + is an idempotent operation \((x + x = x)\), then we have ai-semirings.
a subsemiring of $\text{Rel}(2)$, the semiring of binary relations on a two element set, formed by:
  - the four relations with 3 pairs,
  - the empty, the diagonal, and the full relation

alternatively, the ai-semiring formed by 7 Boolean matrices

\[
\begin{bmatrix}
0 & 0 \\
0 & 0 \\
\end{bmatrix}, \begin{bmatrix}
1 & 0 \\
1 & 1 \\
\end{bmatrix}, \begin{bmatrix}
1 & 1 \\
0 & 1 \\
\end{bmatrix}, \\
\begin{bmatrix}
0 & 1 \\
1 & 1 \\
\end{bmatrix}, \begin{bmatrix}
1 & 1 \\
1 & 0 \\
\end{bmatrix}, \begin{bmatrix}
1 & 0 \\
0 & 1 \\
\end{bmatrix}, \begin{bmatrix}
1 & 1 \\
1 & 1 \\
\end{bmatrix}.
\]

(remember that we have $1+1=1$ in the 2-element Boolean semiring)
\( \Sigma_7 \) (continued)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>a</td>
<td>f</td>
<td>c</td>
<td>f</td>
<td>a</td>
<td>f</td>
</tr>
<tr>
<td>b</td>
<td>0</td>
<td>f</td>
<td>b</td>
<td>f</td>
<td>d</td>
<td>b</td>
<td>f</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>f</td>
<td>c</td>
<td>f</td>
<td>a</td>
<td>c</td>
<td>f</td>
</tr>
<tr>
<td>d</td>
<td>0</td>
<td>d</td>
<td>f</td>
<td>b</td>
<td>f</td>
<td>d</td>
<td>f</td>
</tr>
<tr>
<td>e</td>
<td>0</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
</tr>
<tr>
<td>f</td>
<td>0</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
</tr>
</tbody>
</table>

equations of \( B_2^1 = \) semigroup equations of \( \Sigma_7 \)
Is there such a thing as a NFB finite semiring?

**Theorem A.** $\Sigma_7$ is NFB.

According to *MathSciNet*, this is a first example of such kind.

What follows is a (hopefully) **VERY** short outline of the proof idea.
IMAGIGAM words

- a word of the form
  \[ yLyL^R \]
  where \( L \) is a linear word not containing \( y \), and \( L^R \) is the reverse of \( L \)

- for all \( n \), \( B_2^1 \) (and so \( \Sigma_7 \)) satisfies the \textbf{imagigam equations}
  \[ yx_1x_2 \ldots x_nyx_n \ldots x_2x_1 = yx_n \ldots x_2x_1yx_1x_2 \ldots x_n \]
Isoterm #1

A word $u$ is an isoterm for an ai-semiring identity

$$\sum_i u_i = \sum_j v_j$$

if for each semigroup substitution $\phi$ such that $\phi(u_i)$ is (for some $i$) a subword of $u$ we have that

- either not all $\phi$-values of $u_i$'s are equal, or
- all $\phi$-values of both $u_i$'s and $v_j$'s are equal
Isoterm #2

- for a fixed ai-semiring \( \Sigma \) and words \( u, v \) we write \( u \leq v \) if \( \Sigma \) satisfies \( u + v = v \)
- a word \( w \) is minimal if \( u \leq w \) implies that \( u \) is either 0, or \( w \)
- a minimal word = an isoterm for all identities of \( \Sigma \) (an isoterm of \( \Sigma \))
Isoterm #3

Let $n$ be a natural number and $\Sigma$ an ai-semiring.

A word $u$ in at least $n$ letters is an $n$-isoterm of $\Sigma$ if it is an isoterm for all equations of $\Sigma$ in less than $n$ letters.
An easy proposition. Let $\Sigma$ be an ai-semiring. Suppose that for arbitrary large $n$ we manage to find a word $w_n$ which is an $n$-isoterm, but not an isoterm of $\Sigma$.

Then $\Sigma$ is NFB.
Why isotersms?

If one translates all notions to semigroups this is exactly the tool used by Perkins!

Namely, the imagigam words turn out to be suitable: Perkins proves that

$$yx_1x_2\ldots x_nyx_n\ldots x_2x_1$$

is always a (semigroup) $n$-isoterm, while the imagigam equations show that it is not an isoterm of the Perkins’ monoid.
René, I’ve got a plan...

Can we do the same for $\Sigma_f$?

I.e., is the $n$th imagigam word an $n$-isoterm (in the ai-semiring sense) of $\Sigma_f$? (It is obviously not an isoterm of $\Sigma_f$.)

How to find $n$-isot TERMS at all?
A good lemma always saves the day!

**Lemma.** Let $w$ be a word, with precisely $n$ letters occurring in it, let $\Sigma$ be an ai-semiring, and let $k<n$ be such that

1. each word $u$ in less than $n$ letters, such that $w$ contains a value of $u$ (under some substitution), is minimal with respect to $\Sigma$,
2. $w$ satisfies a certain combinatorial (and technical – but not too much) condition called the **$k$-joint substitution property**.

Then $w$ is a $(k+1)$-isoterm of $\Sigma$. 
In \( \Sigma_7 \), the imagigam words satisfy both conditions!

1) Each word in at most \( n \) variables that has a value in the \( n \)th imagigam word is minimal in \( \Sigma_7 \).

2) Each imagigam word containing at least \( 4k+2 \) letters has the \( k \)-joint substitution property.

1) is a classical combinatorics-on-words issue; for the proof of 2) the key thing is to use a fact from elementary geometry (!)
1) + 2) + Easy Prop. => Theorem A.

To tell the truth, we do not need the `full strength’ of Eq($\Sigma_7$), only 7 its particular features so that we obtain a slightly more general result...
Theorem B. Let $\Sigma$ be an $ai$-semiring. Call $\Sigma$ special if it satisfies the following conditions:

(a) the inequalities of $\Sigma$ are closed under deletion, i.e. for any words $u, v$ such that $u \leq v$ we have $c(u) = c(v)$, and if $u', v'$ are obtained respectively from $u, v$ by deleting all occurrences of a given variable (provided $u, v$ contain at least two variables), then $u' \leq v'$,

(b) $yx \not\leq xy$,
(c) $x$ and $xyx$ are minimal with respect to $\Sigma$,
(d) $x^2y, xyx, yx^2$ are mutually $\leq$-incomparable,
(e) $w \not\leq (xy)^2$ whenever $w \in \{xyx, yxyxy\}$ or $w$ contains one of $x^2, y^2$ as a subword,
(f) $xyzxy \not\leq xyzyx, yxzyx \not\leq xzyx$ and $xzyx \not\leq xzy^2x$,
(g) $w \not\leq xyzttxt$ for $w \in \{xzttxz, xzttxzt, zttxzt\}$.

If $\Sigma$ is special and satisfies all the imagigam identities, then it is nonfinitely based.
Open questions

- **Q1:** Are the semirings $\text{Rel}(n)$ of binary relations on an $n$-element set, $n>1$, finitely based or not?

- **Q2:** Is $\Sigma_7$ INFB?
  Clearly enough, A2: *Yes* $\Rightarrow$ A1: *They’re not.*

- **Q3:** If A2 is *Yes*, is the same conclusion true for each finite ai-semiring in which all *Zimin words* are minimal (a feature easily proved in $\Sigma_7$ by induction)?
Thank you!