Matrix Identities
Involving Multiplication and Transposition

Mikhail Volkov
(with Karl Auinger and Igor Dolinka)

Ural Federal University, Ekaterinburg, Russia

Turku, January 7, 2016

Identities

The idea of an identity or a law is very basic and is arguably one of the very first abstract ideas that school children encounter when they start to learn math.

I mean laws like the commutative law of addition:
A sum isn't changed at rearrangement of its addends.

At the end of the high school, a student is aware (or, at least, is supposed to be aware) of a good dozen of laws:
– the commutative and associative laws of addition,
– the commutative and associative laws of multiplication,
– the distributive law of multiplication over addition,
– the difference of two squares identity,
– the Pythagorean trigonometric identity,
etc, etc.

Identities

The idea of an identity or a law is very basic and is arguably one of the very first abstract ideas that school children encounter when they start to learn math.

I mean laws like the commutative law of addition:
A sum isn't changed at rearrangement of its addends.

At the end of the high school, a student is aware (or, at least, is supposed to be aware) of a good dozen of laws:
– the commutative and associative laws of addition,
– the commutative and associative laws of multiplication,
– the distributive law of multiplication over addition,
– the difference of two squares identity,
– the Pythagorean trigonometric identity,
etc, etc.

Identities

The idea of an identity or a law is very basic and is arguably one of the very first abstract ideas that school children encounter when they start to learn math.

I mean laws like the commutative law of addition:
A sum isn't changed at rearrangement of its addends.

At the end of the high school, a student is aware (or, at least, is supposed to be aware) of a good dozen of laws:
– the commutative and associative laws of addition,
– the commutative and associative laws of multiplication,
– the distributive law of multiplication over addition,
– the difference of two squares identity,
– the Pythagorean trigonometric identity,
etc, etc.

Identities

The idea of an identity or a law is very basic and is arguably one of the very first abstract ideas that school children encounter when they start to learn math.

I mean laws like the commutative law of addition:
A sum isn't changed at rearrangement of its addends.

At the end of the high school, a student is aware (or, at least, is supposed to be aware) of a good dozen of laws:
– the commutative and associative laws of addition,
– the commutative and associative laws of multiplication,
– the distributive law of multiplication over addition,
– the difference of two squares identity,
– the Pythagorean trigonometric identity,
etc, etc.

Inference of Identities

Moreover, the student may feel (though probably cannot explain) the difference between "main" or "primary" identities such as

$$ab = ba \tag{Comm-M}$$

or

$$(ab)c = a(bc) \tag{Asso-M}$$

and "secondary" ones such as, for instance,

$$(ab)^2 = a^2b^2. \tag{Example}$$

"Primary" laws such as (Comm-M) or (Asso-M) are intrinsic properties of objects (say, numbers) we multiply and of the way the multiplication is defined while "secondary" identities can be formally inferred from "primary" ones without any knowledge of which objects are multiplied and how we define the multiplication.

Inference of Identities

Moreover, the student may feel (though probably cannot explain) the difference between "main" or "primary" identities such as

$$ab = ba \tag{Comm-M}$$

or

$$(ab)c = a(bc) \tag{Asso-M}$$

and "secondary" ones such as, for instance,

$$(ab)^2 = a^2b^2. \tag{Example}$$

"Primary" laws such as (Comm-M) or (Asso-M) are intrinsic properties of objects (say, numbers) we multiply and of the way the multiplication is defined while "secondary" identities can be formally inferred from "primary" ones without any knowledge of which objects are multiplied and how we define the multiplication.

Inference of Identities

Moreover, the student may feel (though probably cannot explain) the difference between "main" or "primary" identities such as

$$ab = ba \tag{Comm-M}$$

or

$$(ab)c = a(bc) \tag{Asso-M}$$

and "secondary" ones such as, for instance,

$$(ab)^2 = a^2b^2. \tag{Example}$$

"Primary" laws such as (Comm-M) or (Asso-M) are intrinsic properties of objects (say, numbers) we multiply and of the way the multiplication is defined while "secondary" identities can be formally inferred from "primary" ones without any knowledge of which objects are multiplied and how we define the multiplication.

Inference: Example

Here is a simple example of such a formal inference:

$$(ab)^2$$

Inference: Example

Here is a simple example of such a formal inference:

$$(ab)^2 = (ab)(ab) \qquad \text{by the definition of squaring}$$

Inference: Example

Here is a simple example of such a formal inference:

$$\begin{aligned}(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\ &= a(ba)b && \text{by the law (Asso-M)}\end{aligned}$$

Inference: Example

Here is a simple example of such a formal inference:

$$\begin{aligned}
(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\
&= a(ba)b && \text{by the law (Asso-M)}\\
&= a(ab)b && \text{by the law (Comm-M)}
\end{aligned}$$

Inference: Example

Here is a simple example of such a formal inference:

$$
\begin{aligned}
(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\
&= a(ba)b && \text{by the law (Asso-M)}\\
&= a(ab)b && \text{by the law (Comm-M)}\\
&= (aa)(bb) && \text{by the law (Asso-M)}
\end{aligned}
$$

Inference: Example

Here is a simple example of such a formal inference:

$$\begin{aligned}
(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\
&= a(ba)b && \text{by the law (Asso-M)}\\
&= a(ab)b && \text{by the law (Comm-M)}\\
&= (aa)(bb) && \text{by the law (Asso-M)}\\
&= a^2b^2 && \text{by the definition of squaring}
\end{aligned}$$

Inference: Example

Here is a simple example of such a formal inference:

$$
\begin{aligned}
(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\
&= a(ba)b && \text{by the law (Asso-M)}\\
&= a(ab)b && \text{by the law (Comm-M)}\\
&= (aa)(bb) && \text{by the law (Asso-M)}\\
&= a^2b^2 && \text{by the definition of squaring}
\end{aligned}
$$

Thus, (Example) is a formal corollary of (Asso-M) and (Comm-M) and holds whenever and wherever the two laws hold.

Inference: Example

Here is a simple example of such a formal inference:

$$
\begin{aligned}
(ab)^2 &= (ab)(ab) && \text{by the definition of squaring}\\
&= a(ba)b && \text{by the law (Asso-M)}\\
&= a(ab)b && \text{by the law (Comm-M)}\\
&= (aa)(bb) && \text{by the law (Asso-M)}\\
&= a^2b^2 && \text{by the definition of squaring}
\end{aligned}
$$

Thus, (Example) is a formal corollary of (Asso-M) and (Comm-M) and holds whenever and wherever the two laws hold.

That's why, when extending $\mathbb{N}$ to $\mathbb{Z}$, and then to $\mathbb{Q}$, and then to $\mathbb{R}$, and then to $\mathbb{C}$, we have to care of preserving (Asso-M) and (Comm-M) but there is no need to care of preserving (Example).

Identity Basis

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.
However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

Identity Basis

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.

However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

Identity Basis

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.
However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

Identity Basis

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.
However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

Identity Basis

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.
However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

A big part of algebra in fact deals with inferring some useful "secondary identities" from some "primary" laws. Identities to be inferred may be quite complicated, and the inference itself may be highly non-trivial—think, for instance, of the product rule for determinant: $\det AB = \det A \det B$.
However, one can observe that usually only a few 'primary' laws are invoked in the course of inference.

This observation leads to the idea of composing a complete list of 'primary' laws that would allow us to infer every possible identity. Such a list is called an identity basis.

Warning: the word 'basis' here doesn't mean any independence assumption! Hence no uniqueness, etc.

High School Identities-I

Of course, in order to speak about an identity basis, one has to specify which identities are under consideration. More precisely, one has to specify 1) a set of objects (say, numbers, or functions, or matrices, etc) and 2) a set of operations on these objects (say, addition, and/or multiplication, and/or exponentiation, etc).

For instance, let our objects be natural numbers (i.e. positive integers) and let our operations be addition and multiplication. Then it is not hard to show that the following 6 laws form a basis:

$$a + b = b + a,$$

$$a + (b + c) = (a + b) + c,$$

$$a \cdot 1 = a,$$

$$a \cdot b = b \cdot a,$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

High School Identities-I

Of course, in order to speak about an identity basis, one has to specify which identities are under consideration. More precisely, one has to specify 1) a set of objects (say, numbers, or functions, or matrices, etc) and 2) a set of operations on these objects (say, addition, and/or multiplication, and/or exponentiation, etc).

For instance, let our objects be natural numbers (i.e. positive integers) and let our operations be addition and multiplication. Then it is not hard to show that the following 6 laws form a basis:

$$a+b=b+a,$$
$$a+(b+c)=(a+b)+c,$$
$$a\cdot 1=a,$$
$$a\cdot b=b\cdot a,$$
$$a\cdot(b\cdot c)=(a\cdot b)\cdot c,$$
$$a\cdot(b+c)=a\cdot b+a\cdot c.$$

Of course, in order to speak about an identity basis, one has to specify which identities are under consideration. More precisely, one has to specify 1) a set of objects (say, numbers, or functions, or matrices, etc) and 2) a set of operations on these objects (say, addition, and/or multiplication, and/or exponentiation, etc).

For instance, let our objects be natural numbers (i.e. positive integers) and let our operations be addition and multiplication.

Then it is not hard to show that the following 6 laws form a basis:

$$a + b = b + a,$$
$$a + (b + c) = (a + b) + c,$$
$$a \cdot 1 = a,$$
$$a \cdot b = b \cdot a,$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

High School Identities-I

Of course, in order to speak about an identity basis, one has to specify which identities are under consideration. More precisely, one has to specify 1) a set of objects (say, numbers, or functions, or matrices, etc) and 2) a set of operations on these objects (say, addition, and/or multiplication, and/or exponentiation, etc).

For instance, let our objects be natural numbers (i.e. positive integers) and let our operations be addition and multiplication. Then it is not hard to show that the following 6 laws form a basis:

$$
\begin{gathered}
a+b=b+a, \\
a+(b+c)=(a+b)+c, \\
a \cdot 1=a, \\
a \cdot b=b \cdot a, \\
a \cdot(b \cdot c)=(a \cdot b) \cdot c, \\
a \cdot(b+c)=a \cdot b+a \cdot c .
\end{gathered}
$$

High School Identities-II

Another "high school" operation on the set $\mathbb{N}$ is exponentiation.

High school students know the following 5 laws involving addition, multiplication, and exponentiation:

$$1^a = 1,$$
$$a^1 = a,$$
$$a^{b+c} = a^b \cdot a^c,$$
$$(a \cdot b)^c = a^c \cdot b^c,$$
$$(a^b)^c = a^{b \cdot c}.$$

We collectively refer to the 11 "standard" laws (the 6 from the previous slide and the 5 from this slide) as (HSI).

High School Identities-II

Another "high school" operation on the set $\mathbb{N}$ is exponentiation. High school students know the following 5 laws involving addition, multiplication, and exponentiation:

$$
\begin{aligned}
1^a &= 1, \\
a^1 &= a, \\
a^{b+c} &= a^b \cdot a^c, \\
(a \cdot b)^c &= a^c \cdot b^c, \\
(a^b)^c &= a^{b \cdot c}.
\end{aligned}
$$

We collectively refer to the 11 "standard" laws (the 6 from the previous slide and the 5 from this slide) as (HSI).

High School Identities-II

Another "high school" operation on the set $\mathbb{N}$ is exponentiation. High school students know the following 5 laws involving addition, multiplication, and exponentiation:

$$1^a = 1,$$
$$a^1 = a,$$
$$a^{b+c} = a^b \cdot a^c,$$
$$(a \cdot b)^c = a^c \cdot b^c,$$
$$(a^b)^c = a^{b \cdot c}.$$

We collectively refer to the 11 "standard" laws (the 6 from the previous slide and the 5 from this slide) as (HSI).

Arguably, it was Richard Dedekind who (in his famous book "Was sind und was sollen die Zahlen?" of 1888) seemed to be asking if the 11 laws (HSI) were somehow sufficient to tell us everything we could want to know about the natural numbers.

At that time, however, no mathematical language existed in which such a question could be stated precisely.

Such a language was developed in the first half of the 20th century, and Alfred Tarski was one of the major contributor to this development. In the 1960s Tarski formulated the problem in the terms that we use nowadays:

Arguably, it was Richard Dedekind who (in his famous book "Was sind und was sollen die Zahlen?" of 1888) seemed to be asking if the 11 laws (HSI) were somehow sufficient to tell us everything we could want to know about the natural numbers.
At that time, however, no mathematical language existed in which such a question could be stated precisely.
Such a language was developed in the first half of the 20th century, and Alfred Tarski was one of the major contributor to this development. In the 1960s Tarski formulated the problem in the terms that we use nowadays:

Arguably, it was Richard Dedekind who (in his famous book "Was sind und was sollen die Zahlen?" of 1888) seemed to be asking if the 11 laws (HSI) were somehow sufficient to tell us everything we could want to know about the natural numbers.

At that time, however, no mathematical language existed in which such a question could be stated precisely.

Such a language was developed in the first half of the 20th century, and Alfred Tarski was one of the major contributor to this development. In the 1960s Tarski formulated the problem in the terms that we use nowadays:

Tarski's HSI Problem

Arguably, it was Richard Dedekind who (in his famous book "Was sind und was sollen die Zahlen?" of 1888) seemed to be asking if the 11 laws (HSI) were somehow sufficient to tell us everything we could want to know about the natural numbers.

At that time, however, no mathematical language existed in which such a question could be stated precisely.

Such a language was developed in the first half of the 20th century, and Alfred Tarski was one of the major contributor to this development. In the 1960s Tarski formulated the problem in the terms that we use nowadays:

Tarski's HSI Problem

Do the laws (HSI) form a basis for the identities that involve addition, multiplication, and exponentiation and hold in $\mathbb{N}$?

Tarski's HSI Problem

Arguably, it was Richard Dedekind who (in his famous book "Was sind und was sollen die Zahlen?" of 1888) seemed to be asking if the 11 laws (HSI) were somehow sufficient to tell us everything we could want to know about the natural numbers.

At that time, however, no mathematical language existed in which such a question could be stated precisely.

Such a language was developed in the first half of the 20th century, and Alfred Tarski was one of the major contributor to this development. In the 1960s Tarski formulated the problem in the terms that we use nowadays:

Tarski's HSI Problem

Do the laws (HSI) form a basis for the identities that involve addition, multiplication, and exponentiation and hold in $\mathbb{N}$?

Surprisingly, the answer is NO.

Wilkie's Identity

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$((1+a)^a + (1+a+a^2)^a)^b \cdot \left((1+a^3)^b + (1+a^2+a^4)^b\right)^a =$$
$$= \left((1+a)^b + (1+a+a^2)^b\right)^a \cdot ((1+a^3)^a + (1+a^2+a^4)^a)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

Wilkie's Identity

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$\left((1+a)^a+(1+a+a^2)^a\right)^b\cdot\left((1+a^3)^b+(1+a^2+a^4)^b\right)^a=$$
$$=\left((1+a)^b+(1+a+a^2)^b\right)^a\cdot\left((1+a^3)^a+(1+a^2+a^4)^a\right)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

Wilkie's Identity

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$\left((1+a)^a+(1+a+a^2)^a\right)^b\cdot\left((1+a^3)^b+(1+a^2+a^4)^b\right)^a=$$
$$=\left((1+a)^b+(1+a+a^2)^b\right)^a\cdot\left((1+a^3)^a+(1+a^2+a^4)^a\right)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$\left((1+a)^a+(1+a+a^2)^a\right)^b\cdot\left((1+a^3)^b+(1+a^2+a^4)^b\right)^a=$$
$$=\left((1+a)^b+(1+a+a^2)^b\right)^a\cdot\left((1+a^3)^a+(1+a^2+a^4)^a\right)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

Wilkie's Identity

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$\left((1+a)^a + (1+a+a^2)^a\right)^b \cdot \left((1+a^3)^b + (1+a^2+a^4)^b\right)^a =$$
$$= \left((1+a)^b + (1+a+a^2)^b\right)^a \cdot \left((1+a^3)^a + (1+a^2+a^4)^a\right)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

In 1980 Alex Wilkie found the following identity that holds in $\mathbb{N}$ but cannot be inferred from (HSI).

$$\left((1+a)^a+(1+a+a^2)^a\right)^b\cdot\left((1+a^3)^b+(1+a^2+a^4)^b\right)^a =$$
$$=\left((1+a)^b+(1+a+a^2)^b\right)^a\cdot\left((1+a^3)^a+(1+a^2+a^4)^a\right)^b.$$

Wilkie's identity looks complicated but in fact it is easy to show that it holds in $\mathbb{N}$.

A more delicate question is how to prove that the identity cannot be inferred from (HSI). For this, one construct a counter-model: a set M with 3 operations such that (HSI) hold in M but Wilkie's identity does not. A counter-model with 12 elements is known.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based. Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based. Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based. Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.

Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.

Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis.
In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.
Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.

Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.

Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

No Finite Basis for $(\mathbb{N}; +, \cdot, \uparrow)$

Can one save the situation by including Wilkie's identity in the high school curriculum? Fortunately, for kids, this is not possible: the identities of $(\mathbb{N}; +, \cdot, \uparrow)$ admit no finite basis. (This was shown by R. Gurevič in "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", Ann. Pure and Applied Logic 49 (1990) 1–30.) Thus, if one chooses any finite set Σ of identities of $(\mathbb{N}; +, \cdot, \uparrow)$, there always exists an identity τ that plays the same role with respect to Σ as Wilkie's identity does with respect to (HSI): τ holds in $\mathbb{N}$ but cannot be inferred from Σ.

Here we encounter the phenomenon when the identities of a natural and apparently simple structure admit no finite basis. In this situation, we say that the answer to the Finite Basis Problem (FBP) for the structure is negative and the structure is nonfinitely based. Otherwise it is finitely based.
Thus, $(\mathbb{N}; +, \cdot)$ is finitely based while $(\mathbb{N}; +, \cdot, \uparrow)$ is not.

The Finite Basis Problem

It is the FBP that underlies the research reported in this talk.

The FBP is natural by itself, but it has also revealed a number of interesting and unexpected relations to many issues of theoretical and practical importance ranging from feasible algorithms for membership in certain classes of formal languages to classical number-theoretic conjectures such as the Twin Prime, Goldbach, existence of odd perfect numbers and the infinitude of even perfect numbers. (See P. Perkins, "Finite axiomatizability for equational theories of computable groupoids", J. Symbolic Logic 54 (1989), 1018–1022, where it is shown that each of these conjectures is equivalent to the FBP for a structure of the form $(S, \cdot)$.)

It is the FBP that underlies the research reported in this talk.

The Finite Basis Problem

Given an interesting structure M (a set with a bunch of operations on it), determine whether or not M is finitely based.

The FBP is natural by itself, but it has also revealed a number of interesting and unexpected relations to many issues of theoretical and practical importance ranging from feasible algorithms for membership in certain classes of formal languages to classical number-theoretic conjectures such as the Twin Prime, Goldbach, existence of odd perfect numbers and the infinitude of even perfect numbers. (See P. Perkins, "Finite axiomatizability for equational theories of computable groupoids", J. Symbolic Logic 54 (1989), 1018–1022, where it is shown that each of these conjectures is equivalent to the FBP for a structure of the form $(S, \cdot)$.)

The Finite Basis Problem

It is the FBP that underlies the research reported in this talk.

The Finite Basis Problem

Given an interesting structure M (a set with a bunch of operations on it), determine whether or not M is finitely based.

The FBP is natural by itself, but it has also revealed a number of interesting and unexpected relations to many issues of theoretical and practical importance ranging from feasible algorithms for membership in certain classes of formal languages to classical number-theoretic conjectures such as the Twin Prime, Goldbach, existence of odd perfect numbers and the infinitude of even perfect numbers. (See P. Perkins, "Finite axiomatizability for equational theories of computable groupoids", J. Symbolic Logic 54 (1989), 1018–1022, where it is shown that each of these conjectures is equivalent to the FBP for a structure of the form $(S, \cdot)$.)

The Finite Basis Problem

It is the FBP that underlies the research reported in this talk.

The Finite Basis Problem

Given an interesting structure M (a set with a bunch of operations on it), determine whether or not M is finitely based.

The FBP is natural by itself, but it has also revealed a number of interesting and unexpected relations to many issues of theoretical and practical importance ranging from feasible algorithms for membership in certain classes of formal languages to classical number-theoretic conjectures such as the Twin Prime, Goldbach, existence of odd perfect numbers and the infinitude of even perfect numbers. (See P. Perkins, "Finite axiomatizability for equational theories of computable groupoids", J. Symbolic Logic 54 (1989), 1018–1022, where it is shown that each of these conjectures is equivalent to the FBP for a structure of the form $(S, \cdot)$.)

The Finite Basis Problem for Finite Structures

Even a finite structure can be nonfinitely based. The smallest example is a 3-element structure of the form $(S, \cdot)$ known as Murskiĭ's groupoid, but, IMHO, the most striking example (the Brandt monoid) is formed by the following six 2×2-matrices:

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

the operation being the usual matrix multiplication. (This example is due to P. Perkins, "Bases for equational theories of semigroups", J. Algebra 11 (1969) 298–314.)

Thus, here we see a very transparent, very natural, and very finite structure whose identities cannot be axiomatized by finite means.

The Finite Basis Problem for Finite Structures

Even a finite structure can be nonfinitely based. The smallest example is a 3-element structure of the form $(S, \cdot)$ known as Murskiĭ's groupoid, but, IMHO, the most striking example (the Brandt monoid) is formed by the following six 2×2-matrices:

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

the operation being the usual matrix multiplication. (This example is due to P. Perkins, "Bases for equational theories of semigroups", J. Algebra 11 (1969) 298–314.)

Thus, here we see a very transparent, very natural, and very finite structure whose identities cannot be axiomatized by finite means.

Even a finite structure can be nonfinitely based. The smallest example is a 3-element structure of the form $(S, \cdot)$ known as Murskiĭ's groupoid, but, IMHO, the most striking example (the Brandt monoid) is formed by the following six 2×2-matrices:

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

the operation being the usual matrix multiplication. (This example is due to P. Perkins, "Bases for equational theories of semigroups", J. Algebra 11 (1969) 298–314.)

Thus, here we see a very transparent, very natural, and very finite structure whose identities cannot be axiomatized by finite means.

Even a finite structure can be nonfinitely based. The smallest example is a 3-element structure of the form $(S, \cdot)$ known as Murskiĭ's groupoid, but, IMHO, the most striking example (the Brandt monoid) is formed by the following six 2×2-matrices:

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

the operation being the usual matrix multiplication. (This example is due to P. Perkins, "Bases for equational theories of semigroups", J. Algebra 11 (1969) 298–314.)

Thus, here we see a very transparent, very natural, and very finite structure whose identities cannot be axiomatized by finite means.

Even a finite structure can be nonfinitely based. The smallest example is a 3-element structure of the form $(S, \cdot)$ known as Murskiĭ's groupoid, but, IMHO, the most striking example (the Brandt monoid) is formed by the following six 2×2-matrices:

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

the operation being the usual matrix multiplication. (This example is due to P. Perkins, "Bases for equational theories of semigroups", J. Algebra 11 (1969) 298–314.)

Thus, here we see a very transparent, very natural, and very finite structure whose identities cannot be axiomatized by finite means.

In the early 1960's, Tarski suggested to study the FBP for finite structures as a decision problem. Indeed, since any finite structure S is an object that can be given in a constructive way, one can ask for an algorithm which when presented with an effective description of S, would determine whether or not S is finitely based.

In the early 1960's, Tarski suggested to study the FBP for finite structures as a decision problem. Indeed, since any finite structure S is an object that can be given in a constructive way, one can ask for an algorithm which when presented with an effective description of S, would determine whether or not S is finitely based.

In the early 1960's, Tarski suggested to study the FBP for finite structures as a decision problem. Indeed, since any finite structure S is an object that can be given in a constructive way, one can ask for an algorithm which when presented with an effective description of S, would determine whether or not S is finitely based.

Tarski's Finite Basis Problem

Is there an algorithm that when given an effective description of a finite structure S decides whether S is finitely based or not?

In the early 1960's, Tarski suggested to study the FBP for finite structures as a decision problem. Indeed, since any finite structure S is an object that can be given in a constructive way, one can ask for an algorithm which when presented with an effective description of S, would determine whether or not S is finitely based.

Tarski's Finite Basis Problem

Is there an algorithm that when given an effective description of a finite structure S decides whether S is finitely based or not?

This fundamental question was answered in the negative by Ralph McKenzie ("Tarski's finite basis problem is undecidable", Int. J. Algebra and Computation 6 (1996) 49–104), even for finite structures with a single operation!

In the early 1960's, Tarski suggested to study the FBP for finite structures as a decision problem. Indeed, since any finite structure S is an object that can be given in a constructive way, one can ask for an algorithm which when presented with an effective description of S, would determine whether or not S is finitely based.

Tarski's Finite Basis Problem

Is there an algorithm that when given an effective description of a finite structure S decides whether S is finitely based or not?

This fundamental question was answered in the negative by Ralph McKenzie ("Tarski's finite basis problem is undecidable", Int. J. Algebra and Computation 6 (1996) 49–104), even for finite structures with a single operation!

I think it is a good news for people involved in studying the FBP: since no mechanical procedure exists, you should be more clever than your computer to get an answer!

Matrix $=$ $n \times n$-matrix over a field K with $n > 1$;
$\mathrm{M}_n(K)$ stands for the set of all such matrices.
We are interested in the FBP for $\mathrm{M}_n(K)$
equipped with various natural operations.

The most classical case: addition and multiplication

Matrix = $n \times n$-matrix over a field K with $n > 1$;
$\mathrm{M}_n(K)$ stands for the set of all such matrices.
We are interested in the FBP for $\mathrm{M}_n(K)$
equipped with various natural operations.

The most classical case: addition and multiplication

Matrices: Addition and Multiplication

Matrix $=$ $n \times n$-matrix over a field K with $n > 1$;
$\mathrm{M}_n(K)$ stands for the set of all such matrices.
We are interested in the FBP for $\mathrm{M}_n(K)$
equipped with various natural operations.

The most classical case: addition and multiplication

Matrix $=$ $n \times n$-matrix over a field K with $n > 1$;
$\mathrm{M}_n(K)$ stands for the set of all such matrices.
We are interested in the FBP for $\mathrm{M}_n(K)$
equipped with various natural operations.

The most classical case: addition and multiplication

Theorem (Kemer (1987) for char $K = 0$; Kruse and L'vov (1973) for finite K)

$(\mathrm{M}_n(K); +, \cdot)$ is finitely based.

Matrix $= n \times n$-matrix over a field K with $n > 1$;
$\mathrm{M}_n(K)$ stands for the set of all such matrices.
We are interested in the FBP for $\mathrm{M}_n(K)$
equipped with various natural operations.

The most classical case: addition and multiplication

Theorem (Kemer (1987) for char $K = 0$; Kruse and L'vov (1973) for finite K)

$(\mathrm{M}_n(K); +, \cdot)$ is finitely based.

A precise basis is known only for $n = 2$ in the case char $K = 0$ and for $n \leq 4$ for finite K.

Matrices: Multiplication Only

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such "multiplicative" identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $\langle M_n(K); \cdot\rangle$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such “multiplicative” identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K);\cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such "multiplicative" identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K); \cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

Matrices: Multiplication Only

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such "multiplicative" identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K);\cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such "multiplicative" identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K);\cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

Matrices: Multiplication Only

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such "multiplicative" identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K); \cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

Matrices: Multiplication Only

All identities of matrices over an infinite field involving only multiplication are known to follow from the associative law. Thus, the associative law forms a basis of such “multiplicative” identities.

In contrast, multiplicative identities of matrices over a finite field admit no finite basis (Mark Sapir and MV., mid-1980s). It is worth noting that methods used by Sapir and by MV. were very different but each of them sufficed to cover multiplicative identities of matrices of every fixed size over every finite field.

Thus, finiteness of $(M_n(K);\cdot)$ implies non-finiteness of its identity basis and vice versa. It is a good example of somewhat surprising interplays between finiteness and non-finiteness that drive the whole area.

Multiplication and Transposition

Karl Auinger, Igor Dolinka, and MV. studied matrix identities involving multiplication and one or two natural one-place operations such as taking various transposes or Moore–Penrose inversion (Matrix identities involving multiplication and transposition, J. Europ. Math. Soc. 14 (2012) 937–969).

Multiplication and Transposition

Karl Auinger, Igor Dolinka, and MV. studied matrix identities involving multiplication and one or two natural one-place operations such as taking various transposes or Moore–Penrose inversion (Matrix identities involving multiplication and transposition, J. Europ. Math. Soc. 14 (2012) 937–969).
For the classical transpose, we have:

Theorem

$(M_n(K); \cdot, {}^T)$ is finitely based iff K is infinite.

Multiplication and Transposition

Karl Auinger, Igor Dolinka, and MV. studied matrix identities involving multiplication and one or two natural one-place operations such as taking various transposes or Moore–Penrose inversion (Matrix identities involving multiplication and transposition, J. Europ. Math. Soc. 14 (2012) 937–969).
For the classical transpose, we have:

Theorem

$(M_n(K); \cdot, {}^T)$ is finitely based iff K is infinite.

For the proof that $(M_n(K); \cdot, {}^T)$ with K finite is nonfinitely based we had to extend both approaches used by Sapir and MV. for the purely multiplicative case.

Multiplication and Transposition

Karl Auinger, Igor Dolinka, and MV. studied matrix identities involving multiplication and one or two natural one-place operations such as taking various transposes or Moore–Penrose inversion (Matrix identities involving multiplication and transposition, J. Europ. Math. Soc. 14 (2012) 937–969).
For the classical transpose, we have:

Theorem

$(M_n(K); \cdot, {}^T)$ is finitely based iff K is infinite.

For the proof that $(M_n(K); \cdot, {}^T)$ with K finite is nonfinitely based we had to extend both approaches used by Sapir and MV. for the purely multiplicative case. Interestingly, none of the two suffice alone for identities involving both multiplication and transposition.

Karl Auinger, Igor Dolinka, and MV. studied matrix identities involving multiplication and one or two natural one-place operations such as taking various transposes or Moore–Penrose inversion (Matrix identities involving multiplication and transposition, J. Europ. Math. Soc. 14 (2012) 937–969).
For the classical transpose, we have:

Theorem

$(M_n(K); \cdot, {}^T)$ is finitely based iff K is infinite.

For the proof that $(M_n(K); \cdot, {}^T)$ with K finite is nonfinitely based we had to extend both approaches used by Sapir and MV. for the purely multiplicative case. Interestingly, none of the two suffice alone for identities involving both multiplication and transposition. For instance, for $n = 2$, the extension of Sapir's approach works when $|K| = 2, 4, 5, 8, 9, \dots$ and does not when $|K| = 3, 7, 11, \dots$.

For a $2m \times 2m$-matrix $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with A, B, C, D being $m \times m$-matrices, the symplectic transpose X^S is defined by

$$X^S = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}.$$

The symplectic transpose satisfies $(XY)^S = Y^S X^S$ and $(X^S)^S = X$ so it is an involution of $(\mathrm{M}_{2m}(K), \cdot)$. In fact, every involution of $(\mathrm{M}_{2m}(K), \cdot)$ that fixes all scalar matrices is similar to either the usual transposition or the symplectic transpose.

Multiplication and Symplectic Transposition

For a $2m \times 2m$-matrix $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with A, B, C, D being $m \times m$-matrices, the symplectic transpose X^S is defined by

$$X^S = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}.$$

The symplectic transpose satisfies $(XY)^S = Y^S X^S$ and $(X^S)^S = X$ so it is an involution of $(\mathrm{M}_{2m}(K), \cdot)$. In fact, every involution of $(\mathrm{M}_{2m}(K), \cdot)$ that fixes all scalar matrices is similar to either the usual transposition or the symplectic transpose.

Multiplication and Symplectic Transposition

For a $2m \times 2m$-matrix $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with A, B, C, D being $m \times m$-matrices, the symplectic transpose X^S is defined by

$$X^S = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}.$$

The symplectic transpose satisfies $(XY)^S = Y^S X^S$ and $(X^S)^S = X$ so it is an involution of $(\mathrm{M}_{2m}(K), \cdot)$. In fact, every involution of $(\mathrm{M}_{2m}(K), \cdot)$ that fixes all scalar matrices is similar to either the usual transposition or the symplectic transpose.

Multiplication and Symplectic Transposition

For a $2m \times 2m$-matrix $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with A, B, C, D being $m \times m$-matrices, the symplectic transpose X^S is defined by

$$X^S = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}.$$

The symplectic transpose satisfies $(XY)^S = Y^S X^S$ and $(X^S)^S = X$ so it is an involution of $(\mathrm{M}_{2m}(K), \cdot)$. In fact, every involution of $(\mathrm{M}_{2m}(K), \cdot)$ that fixes all scalar matrices is similar to either the usual transposition or the symplectic transpose.

For the symplectic transpose, we have the same result as above:

Theorem

$(M_n(K); \cdot, {}^S)$ is finitely based iff K is infinite.

Now let $K = \mathbb{C}$, the field of complex numbers.

Now let $K = \mathbb{C}$, the field of complex numbers.

Theorem (Penrose, 1955)

For every $n \times k$-matrix A over $\mathbb{C}$, there exists a unique $k \times n$-matrix $A^\dagger$ such that

$$AA^\dagger A = A,\ A^\dagger AA^\dagger = A^\dagger,\ (A^\dagger A)^* = A^\dagger A,\ (AA^\dagger)^* = AA^\dagger.$$

Now let $K = \mathbb{C}$, the field of complex numbers.

Theorem (Penrose, 1955)

For every $n \times k$-matrix A over $\mathbb{C}$, there exists a unique $k \times n$-matrix $A^\dagger$ such that

$$AA^\dagger A = A,\ A^\dagger AA^\dagger = A^\dagger,\ (A^\dagger A)^* = A^\dagger A,\ (AA^\dagger)^* = AA^\dagger.$$

Here * stands for the usual Hermitian conjugation.

Now let $K = \mathbb{C}$, the field of complex numbers.

Theorem (Penrose, 1955)

For every $n \times k$-matrix A over $\mathbb{C}$, there exists a unique $k \times n$-matrix $A^\dagger$ such that

$$AA^\dagger A = A, \; A^\dagger AA^\dagger = A^\dagger, \; (A^\dagger A)^* = A^\dagger A, \; (AA^\dagger)^* = AA^\dagger.$$

Here * stands for the usual Hermitian conjugation.

The matrix $A^\dagger$ is called the Moore–Penrose inverse of A. (Moore defined the same generalized inverse in a completely different way in 1920.)

Moore–Penrose Inverse

Now let $K = \mathbb{C}$, the field of complex numbers.

Theorem (Penrose, 1955)

For every $n \times k$-matrix A over $\mathbb{C}$, there exists a unique $k \times n$-matrix $A^\dagger$ such that

$$AA^\dagger A = A, \ A^\dagger AA^\dagger = A^\dagger, \ (A^\dagger A)^* = A^\dagger A, \ (AA^\dagger)^* = AA^\dagger.$$

Here * stands for the usual Hermitian conjugation.

The matrix $A^\dagger$ is called the Moore–Penrose inverse of A. (Moore defined the same generalized inverse in a completely different way in 1920.) This is an important concept of both theoretical and applied value.

Now let $K = \mathbb{C}$, the field of complex numbers.

Theorem (Penrose, 1955)

For every $n \times k$-matrix A over $\mathbb{C}$, there exists a unique $k \times n$-matrix $A^\dagger$ such that

$$AA^\dagger A = A,\ A^\dagger AA^\dagger = A^\dagger,\ (A^\dagger A)^* = A^\dagger A,\ (AA^\dagger)^* = AA^\dagger.$$

Here * stands for the usual Hermitian conjugation.

The matrix $A^\dagger$ is called the Moore–Penrose inverse of A. (Moore defined the same generalized inverse in a completely different way in 1920.) This is an important concept of both theoretical and applied value. For instance, if $Ax = b$ is a system of simultaneous linear equations (which may be inconsistent), then $A^\dagger b$ is its "least square" solution: $\|Ax - b\| \geq \|A(A^\dagger b) - b\|$ for every vector x.

Identities Involving Moore–Penrose Inverse

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, ^*, ^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*, ^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, ^*, ^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, ^*, ^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*, ^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, ^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, ^*, ^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Theorem

$(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ is nonfinitely based.

The result is surprising and even counter-intuitive. It is easy to see that $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$ is finitely based and Penrose's four laws uniquely determine $A^\dagger$—this suggests that a finite basis for the identities of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ can be obtained by adding Penrose's laws to a finite basis of $(\mathrm{M}_2(\mathbb{C}); \cdot, {}^*)$. Our theorem shows that this is not the case.

We do not know whether or not $(\mathrm{M}_n(\mathbb{C}); \cdot, {}^*, {}^\dagger)$ with $n > 2$ is finitely based. None of our present methods allow us to approach this case.

Conclusion

Studying matrices from the viewpoint of the FBP for their identities involving multiplication and natural one-place operations reveals a variety of results some of which are quite surprising.

This study has required new techniques that have found many further applications—see our sequel papers:
K. Auinger, I. Dolinka, MV., Equational theories of semigroups with involution, J. Algebra 369 (2012) 203–225;
K. Auinger, I. Dolinka, T. V. Pervukhina, MV., Unary enhancements of inherently nonfinitely based semigroups, Semigroup Forum 89 (2014) 41–51.

There still remain challenging open problems in the area.

Look at `http://csseminar.kadm.usu.ru/volkov/` for details (and these slides).

Conclusion

Studying matrices from the viewpoint of the FBP for their identities involving multiplication and natural one-place operations reveals a variety of results some of which are quite surprising.

This study has required new techniques that have found many further applications—see our sequel papers:
K. Auinger, I. Dolinka, MV., Equational theories of semigroups with involution, J. Algebra 369 (2012) 203–225;
K. Auinger, I. Dolinka, T. V. Pervukhina, MV., Unary enhancements of inherently nonfinitely based semigroups, Semigroup Forum 89 (2014) 41–51.

There still remain challenging open problems in the area.

Look at `http://csseminar.kadm.usu.ru/volkov/` for details (and these slides).

Conclusion

Studying matrices from the viewpoint of the FBP for their identities involving multiplication and natural one-place operations reveals a variety of results some of which are quite surprising.

This study has required new techniques that have found many further applications—see our sequel papers:
K. Auinger, I. Dolinka, MV., Equational theories of semigroups with involution, J. Algebra 369 (2012) 203–225;
K. Auinger, I. Dolinka, T. V. Pervukhina, MV., Unary enhancements of inherently nonfinitely based semigroups, Semigroup Forum 89 (2014) 41–51.

There still remain challenging open problems in the area.

Look at http://csseminar.kadm.usu.ru/volkov/ for details (and these slides).

Conclusion

Studying matrices from the viewpoint of the FBP for their identities involving multiplication and natural one-place operations reveals a variety of results some of which are quite surprising.

This study has required new techniques that have found many further applications—see our sequel papers:
K. Auinger, I. Dolinka, MV., Equational theories of semigroups with involution, J. Algebra 369 (2012) 203–225;
K. Auinger, I. Dolinka, T. V. Pervukhina, MV., Unary enhancements of inherently nonfinitely based semigroups, Semigroup Forum 89 (2014) 41–51.

There still remain challenging open problems in the area.

Look at `http://csseminar.kadm.usu.ru/volkov/` for details (and these slides).