The Saga of the High School Identities

Stanley N. Burris and Karen A. Yeats

Abstract. This paper surveys and updates results and open problems related to the variety defined by the High School Identities as well as the variety generated by the positive numbers with exponentiation.

The set of eleven basic identities of the **positive** integers N with the operations $+, \times, \uparrow$ which one learns in high school are as follows (the subset not involving exponentiation is called $\widehat{\text{HSI}}$):

$$\text{HSI}\left\{\begin{array}{l}
\widehat{\text{HSI}}\left\{\begin{array}{lc}
(1) & x+y \approx y+x\\
(2) & x+(y+z) \approx (x+y)+z\\
(3) & x\cdot 1 \approx x\\
(4) & x\cdot y \approx y\cdot x\\
(5) & x\cdot(y\cdot z) \approx (x\cdot y)\cdot z\\
(6) & x\cdot(y+z) \approx (x\cdot y)+(x\cdot z)
\end{array}\right.\\
\hline
\begin{array}{lc}
(7) & 1^x \approx 1\\
(8) & x^1 \approx x\\
(9) & x^{y+z} \approx x^y\cdot x^z\\
(10) & (x\cdot y)^z \approx x^z\cdot y^z\\
(11) & (x^y)^z \approx x^{y\cdot z}.
\end{array}
\end{array}\right.$$

These can be found in Dedekind's 1888 monograph [8] *Was Sind Und Was Sollen Die Zahlen?*—they are derived from the natural numbers with the successor operation. They are among the oldest and most familiar of the equational theories in mathematics.

Our first (and perhaps most important) models of these two sets of identities are

$$\mathbf{N} = (N, +, \times, \uparrow, 1) \qquad \widehat{\mathbf{N}} = (N, +, \times, 1)$$

Obvious questions to ask about the identities of these two well known algebras concern:

- **Axioms** for their equational theories, and the
- **Decidability** of their equational theories.

Date: September 15, 2004.
Research of the first author was supported by a grant from NSERC.
Research of the second author was supported by a NSERC Undergraduate Research Grant.

It has long been known that

(a) $\widehat{\mathrm{HSI}}$ is a finite set of axioms for the equational theory of $\widehat{\mathbf{N}}$, and
(b) the equational consequences of $\widehat{\mathrm{HSI}}$, that is, the equations true of $\widehat{\mathbf{N}}$, are decidable.

One sees this by noting that every $\widehat{\mathbf{N}}$ term $t(\vec{x})$, that is, a term in the language $\{+, \times, 1\}$ of $\widehat{\mathbf{N}}$, has a **normal form**, namely a **polynomial** $p(\vec{x})$. There is a straight forward effective procedure to find this normal form, namely by multiplying out and collecting terms. By classical algebra it is clear that an equation $s(\vec{x}) \approx t(\vec{x})$ follows from $\widehat{\mathrm{HSI}}$ iff both sides have the same polynomial as their normal form. This is all one needs to prove that $\widehat{\mathrm{HSI}}$ is a basis for the equational theory of $\widehat{\mathbf{N}}$ and that this equational theory is decidable.

However when we turn to study HSI and $\mathbf{N}$ we no longer have the benefit of such normal forms, the situation becomes immensely more complicated, and there are many open questions.

1. Models of HSI

When looking for natural models of $\widehat{\mathrm{HSI}}$ one not only has the algebra $\widehat{\mathbf{N}}$ but also the familiar number systems yield models: the integers, the rationals, the reals, and the complex numbers; and one can take the nonegative [positive] integers, rationals, or reals.

However when we turn to find natural models of HSI many of these possibilities evaporate, e.g., the positive rationals are not closed under $\uparrow$. One of the most fascinating that survives (see §2) is the positive reals $\mathbf{R}^+ = (R^+, +, \times, \uparrow, 1)$.

Another natural model was found by G. Birkhoff [3] (1942)—he showed that HSI holds for the **algebra of posets**[1] where the operations are given by:

$+$ is disjoint union
$\times$ is cartesian product
$\uparrow$ is order preserving maps

Consequently they also hold for the **algebra of cardinal numbers**. Aside from some examples in topos theory[2] we know of few other natural models of HSI that have been studied.

1.1. The Smallest Submodels.

This and the next subsection draw heavily on the papers [4] (1992) and [5] (1993) of Burris and Lee.

Every model of HSI has a smallest submodel, namely the subalgebra generated by the constant 1. The elements of this submodel are just 1,2,3, etc., where

$$\begin{array}{rcl} 2 & := & 1+1 \\ 3 & := & 2+1 \\ & \text{etc.} & \end{array}$$

[1]In a footnote Birkhoff says that Tukey pointed out that HSI holds more generally for **preorders** (= reflexive + transitive).

[2]D. Higgs examined several topoi in the hopes of finding a natural countermodel to Wilkie's identity (see Section 5).

since these elements include 1 and are closed under addition, multiplication and exponentiation. We call these elements the **integers** of the model.

If the set of integers of a model of HSI is infinite then it is a copy of $\mathbf{N}$, the **free** HSI algebra freely generated by Ø. On the other hand if the set of integers is finite then it must give a submodel that looks like Fig. 1, the quotient of $\mathbf{N}$ defined by

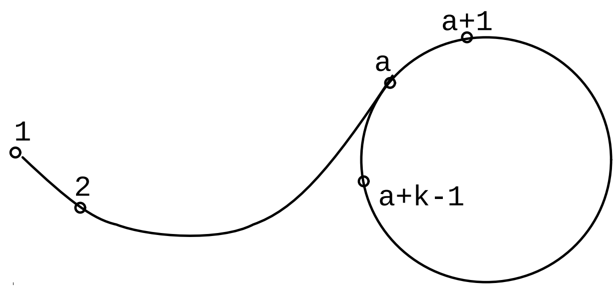

FIGURE 1. A finite quotient $\mathbf{N}_{a,k}$ of $\mathbf{N}$

$a \approx a + k$.

Not every positive a and k gives a quotient of $\mathbf{N}$ as pictured in Fig. 1—each picture does support addition and multiplication, but not necessarily exponentiation. It is routine to show that the congruences of $\widehat{\mathbf{N}}$ are the relations $\equiv_{a,k}$ defined by $(i, j) \in\equiv_{a,k}$ iff $i = j$, or $i, j \geq a$ and $i \equiv j \mod k$. We want to know the a, k for which $\equiv_{a,k}$ is a congruence of $\mathbf{N}$, that is, when is $\equiv_{a,k}$ compatible with exponentiation. This is equivalent to the condition $x^a \equiv_{a,k} x^{a+k}$ holds for $x \in N$, which leads to the fascinating divisibility conditions in the following theorem (for a complete proof see [4]).

Theorem 1.1. *The finite quotients of* $\mathbf{N}$ *are the* $\mathbf{N}_{a,k}$ *where* $a, k \in N$ *satisfy (for all primes* p*):*

$$\begin{aligned} p^e | k \quad &\Rightarrow \quad e \leq a \\ p | k \quad &\Rightarrow \quad (p-1) | k. \end{aligned}$$

The next corollary gives a complete list of the five "circle" integer HSI-algebras, i.e., those with $a = 1$, and hence no "tail". These give the examples of **rings** $\mathbf{Z}/(k)$ that support exponentiation (with $0^0 = 0$).

Corollary 1.2. $\mathbf{N}_{1,k}$ *is a quotient of* $\mathbf{N}$ *iff* $k \in \{1, 2, 6, 42, 1806\}$.

Already in the most elementary study of the quotients of $\mathbf{N}$, the $\mathbf{N}_{a,k}$, we run into an interesting question in the theory of numbers. Given $a \in N$ define the sequence of primes $\Sigma_a = (p_1, p_2, \cdots)$ by

- $p_1 = 2$;
- given $p_1, \ldots, p_i$, let p_{i+1} be the smallest prime p which is greater than p_i and such that $(p-1) | (p_1 \cdots p_i)^a$, assuming such a p exists. If no such p exists then Σ_a terminates with p_i.

Proposition 1.3. *Given a positive integer a, there are infinitely many $\mathbf{N}_{a,k}$ iff the sequence of primes Σ_a is infinite.*

Note that $\Sigma_1 = (2, 3, 7, 43)$, a finite sequence.

Problem 1. Is Σ_a finite for all (any) $a > 1$?

About 20% of the primes below 10,000,000 are in

$$\Sigma_2 = (2, 3, 5, 7, 11, 13, 19, 23, \dots, 9999749, 9999973, \dots).$$

So even if Σ_2 is finite, a computer enumeration does not look feasible.

Conjecture 1. Σ_a is infinite for $a > 1$, with asymptotic density zero in the set of primes.

To show the first part of the conjecture holds it suffices to show Σ_2 is infinite as $\Sigma_a \subsetneq \Sigma_{a+1}$.

1.2. The Five Two-Element Models of HSI. It is a routine exercise to verify that there are exactly five two-element models of HSI, and they are:

$$(1) \quad \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & 1 \\ a & 1 & a \end{array} \qquad \begin{array}{c|cc} \times & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \qquad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & 1 \end{array}$$

$$(2) \quad \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & 1 \\ a & 1 & a \end{array} \qquad \begin{array}{c|cc} \times & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \qquad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & a \end{array}$$

$$(3) \quad \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \qquad \begin{array}{c|cc} \times & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \qquad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & a \end{array}$$

$$(4) \quad \begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 2 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{c|cc} \times & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \qquad \mathbf{N_{2,1}}$$

$$(5) \quad \begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 1 \\ 2 & 1 & 2 \end{array} \qquad \begin{array}{c|cc} \times & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \qquad \mathbf{N_{1,2}}$$

Clearly algebras (4) and (5) satisfy all the identities of $\mathbf{N}$ as they are quotients of $\mathbf{N}$. It is astonishing that we did not know until the recent proof of Asatryan [2] that all five of the two-element algebras satisfy all of the identities of $\mathbf{N}$, answering a question posed more than a decade ago in [4].

By taking the variety generated by each of these two-element models of HSI we easily have many other recognizable models of HSI. In four of the cases below exponentiation is the *first projection* function π (defined by $\pi(a, b) = a$).

- Let $\mathbf{H} = \langle H, \vee, \wedge, \rightarrow, 0, 1\rangle$ be a Heyting algebra.
  Then $\mathbf{H}^\star = \langle H, \vee, \wedge, \leftarrow, 1\rangle$ is an HSI-algebra, where $a \leftarrow b$ is defined to be $b \rightarrow a$.
- Let $\mathbf{D} = \langle D, \vee, \wedge, 1\rangle$ be a distributive lattice with 1.
  Then $\langle D, \vee, \wedge, \pi, 1\rangle$ is an HSI-algebra.

- Let $\mathbf{S} = \langle S, \wedge, 1\rangle$ be a semilattice with 1.
  Then $\langle S, \wedge, \wedge, \pi, 1\rangle$ is an HSI-algebra.
- Let $\mathbf{S} = \langle S, \wedge, 0, 1\rangle$ be a semilattice with 0,1.
  Then $\langle S, f, \wedge, \pi, 1\rangle$ is an HSI-algebra, where f is the binary constant map whose value is always 0.
- Let $\mathbf{R} = \langle R, +, \times, 0, 1\rangle$ be a Boolean ring.
  Then $\langle R, +, \times, \pi, 1\rangle$ is an HSI-algebra.

2. G.H. Hardy's "Orders of Infinity"

One of the most important tools for studying the identities of $\mathbf{N}$ has been G.H. Hardy's monograph [15] (1921) on the partial functions defined by the terms of the partial algebra on the reals R that we call $\mathbf{R}_H$:

$$\mathbf{R}_H \;=\; \big(R,\, +,\, -,\, \times,\, \div,\, (\sqrt[n]{\ })_{n\in N},\, \exp,\, \log,\, (r)_{r\in R}\big).$$

Let $\mathcal{H}$ be the set of partial functions defined by $\mathbf{R}_H$ terms $t(x)$, and let $\mathcal{H}_\infty$ be the set of $f \in \mathcal{H}$ such that f is eventually defined on the reals, that is, defined for sufficiently large values of x. (He called $\mathcal{H}_\infty$ the set of *logarithmico-exponential* functions.) Hardy considered the following relation $\prec$ between functions that are eventually defined on the reals:

$f \prec g$ means f is eventually less than g,

and proved the following fundamental result.

Theorem 2.1 (Hardy [15], Theorem 13)**.** *Given $f, g \in \mathcal{H}_\infty$ either $f \prec g$ or $g \prec f$ or f is eventually equal to g.*

Thus two distinct $\mathcal{H}_\infty$-functions cannot weave back and forth infinitely often, that is, we cannot have the situation suggested by Fig. 2. Note that this almost

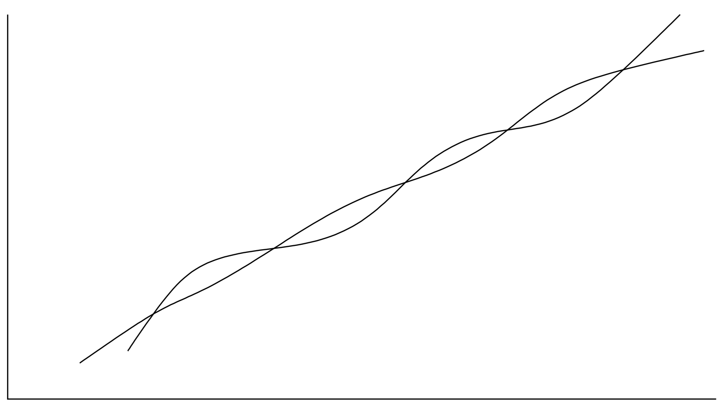

Figure 2. Two functions repeatedly intersecting

says $\prec$ defines a linear order on $\mathcal{H}$. However two partial functions from $\mathcal{H}_\infty$ that eventually agree need not agree everywhere they are defined.

To prove the ordering result Hardy introduced the following concepts:

(1) The **order** of an $\mathcal{R}_H$ term is the maximal number of nested exponentials and logs in it.
(2) An **integral** $\mathcal{R}_H$ term of order at most n is one of the form

$$\sum_i \alpha_i(x) \cdot e^{\beta_i(x)} \cdot \prod_j \log \gamma_{ij}(x)$$

where the $\alpha_i(x)$, $\beta_i(x)$ and $\gamma_{ij}(x)$ are of order at most $n-1$.

Usual induction over formulas does not seem to yield Theorem 2.1. Instead Hardy uses multi-stage induction to show:

an $\mathcal{H}_\infty$-function with arbitrarily large roots is eventually zero.

He uses the fact:

every $\mathcal{H}_\infty$-function of order at most n is an algebraic expression in integral functions of order at most n.

One of his most important ways of reducing a case to the induction hypothesis is to differentiate, noting that Rolle's Theorem guarantees:

$f(x)$ has arbitrarily large roots implies $f'(x)$ has arbitrarily large roots (see Fig. 3).

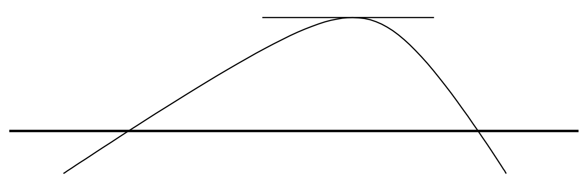

FIGURE 3. The derivative of f has a root between two roots of f

Corollary 2.2. *If $f, g \in \mathcal{H}_\infty$ are both defined on (a, ∞) but do not define the same function on (a, ∞) then either $f \prec g$ or $g \prec f$.*

Proof. This follows from the fact that f and g each have power series expansions in some neighborhood of any $b \in (a, \infty)$, so if they are eventually equal then they are equal on (a, ∞). $\square$

To connect Hardy's work with $\mathbf{R}^+$ we first define a translation of terms:

given any term $t(\vec{x})$ in the language of $\mathbf{R}^+$ let $t^*(\vec{x})$ be the term obtained by replacing subterms of the form u^v in t by $\exp(v \log u)$.

Then we observe that

for t a term in the language of $\mathbf{R}^+$ each t^* gives a partial function of $\mathbf{R}_H$ that is defined whenever all arguments are positive reals, and for such arguments it agrees with the term function of $\mathbf{R}^+$ defined by t.

As an immediate corollary we see that the term functions f, g of $\mathbf{R}^+$ as well as of $\mathbf{N}$ satisfy the hypothesis of Corollary 2.2, so $\prec$ defines a *linear order* on each of these sets. The set of term functions of $\mathbf{N}$ is called Sk (for the set of **Skolem functions**). We know more about the ordering on the term functions of $\mathbf{N}$.

Theorem 2.3 (Ehrenfeucht [9] (1973))**.** *The set* Sk *is well-ordered by* $\prec$.

The exact order type of Sk under $\prec$ is not known.

Conjecture 2. (See [13], p. 8) ϵ_0 is the order type of (Sk, $\prec$).

Using Corollary 2.2 we have the following result.

Theorem 2.4 (Macintyre [18] (1981))**.** $V(\mathbf{N}) = V(\mathbf{R}^+)$.

Proof. As $\mathbf{N}$ is a subalgebra of $\mathbf{R}^+$ it suffices to show that each identity of $\mathbf{N}$ is also an identity of $\mathbf{R}^+$.

First consider a one variable identity $s(x) \approx t(x)$. If this fails in $\mathbf{R}^+$ then the term functions that $s(x)$ and $t(x)$ define on $\mathbf{R}^+$ are eventually distinct. Hence they eventually disagree on the integers. So the identity also fails in $\mathbf{N}$.

Now a simple induction on the number of variables shows that every identity of $\mathbf{N}$ is an identity of $\mathbf{R}^+$. □

Thus in studying the identities of $\mathbf{N}$ it is natural to consider switching to the identities of $\mathbf{R}^+$ and make use of the tools of analysis.

3. Decidability

Hardy's investigations of the asymptotic behaviour of $\mathcal{H}_\infty$-functions provided the starting point for investigations into the decidability of the equational theory of $\mathbf{N}$. D. Richardson [23] (1969) built on Hardy's work to show that the *one variable* equational theory of $\mathbf{N}$ is decidable, that is, one can decide which identities $s(x) \approx t(x)$ hold in the natural numbers. Richardson's method was to study the validity of equations in $\mathbf{R}_H$. However, before one can even talk about decidability of equations it is necessary to to have a countable language, to eliminate the continuum many real constants available in Hardy's formulation. If we replace the constants $(r)_{r\in R}$ in the model $\mathbf{R}_H$ by just the two constants $0, 1$ then the language is countable, and furthermore any partial function in Hardy's set $\mathcal{H}$ is defined by a term in the reduced language with the help of real parameters, i.e., it is defined by an expression $t(x, \vec{r})$ where $t(x, \vec{y})$ is a term using only the two constants 0 and 1, and $\vec{r}$ is a sequence of reals.

Richardson modified Hardy's language a bit further, dropping the radicals and changing the log function to the log of the absolute value. So Richardson was working with the structure

$$\widetilde{\mathbf{R}}_H \;=\; \big(R, +, -, \times, \div, \exp, \log|\;|, 0, 1\big).$$

Let $\widetilde{\mathcal{H}}$ be the set of partial functions defined by the $\widetilde{\mathbf{R}}_H$ terms $t(x, \vec{r})$ with real parameters r, and let $\widetilde{\mathcal{H}}_\infty$ be the set of $f \in \widetilde{\mathcal{H}}$ for which f is eventually defined.

It is easy to see that $\widetilde{\mathcal{H}} \subseteq \mathcal{H}$, so Hardy's Theorem holds for $\widetilde{\mathcal{H}}_\infty$. Furthermore any partial function in $\mathcal{H}$ which can be defined without using radicals is also in $\widetilde{\mathcal{H}}$. In particular, all the term functions of $\mathbf{R}^+$ appear as restrictions (to the positive reals) of members of $\widetilde{\mathcal{H}}_\infty$.

Now that we have a countable language it is possible to formulate a number of open questions concerning decision problems. In the following we write $s \prec t$ for terms s and t if the corresponding partial functions are in the relation $\prec$.

Problem 2 (Eventually Defined)**.** Can one decide if a one variable $\widetilde{\mathbf{R}}_H$ term $t(x)$ is eventually defined?

Problem 3 (Root Size)**.** Given that an $\widetilde{\mathbf{R}}_H$ term $t(x)$ is eventually defined and eventually nonzero, can one give an effective bound on (the size of) the roots of $t(x)$?

A special case of this is formulated for $\mathbf{N}$.

Problem 4 (Intersection Size)**.** Given that two $\mathbf{N}$ terms $s(x)$ and $t(x)$ do not define the same function on $\mathbf{N}$ (this is decidable—see Theorem 3.3), can one give an effective bound on the size of the n for which s and t agree?

Problem 5 (Dominance for $\widetilde{\mathcal{H}}$)**.** Given $t(x)$, an $\widetilde{\mathbf{R}}_H$ term that is eventually defined, can one decide if $0 \prec t(x)$?

A special case of the Dominance problem is formulated for $\mathbf{N}$.

Problem 6 (Dominance for Sk)**.** Is there a decision procedure for $s(x) \prec t(x)$, where $s(x), t(x)$ are terms in the language of $\mathbf{N}$?

Richardson showed that if a decision procedure for Problem 6 exists then one can decide *equality* for the so-called **exponential constants**, that is, for the variable free terms in the language $+, \times, \div, \uparrow, 1$.

Gurevič [14] (1986) showed that if one considers only $s(x), t(x) \prec 2^{x^2}$ then Problem 6 is decidable.

3.1. Richardson's Proof. Note that if $t(x, \vec{y})$ is an $\widetilde{\mathbf{R}}_H$ term and $\vec{b} \in \mathbb{R}$ are such that $t(x, \vec{b})$ is defined on an interval I, then $t(x, \vec{b})$ defines a function in $C^\infty(I)$. Richardson's main idea was to associate with each $\widetilde{\mathbf{R}}_H$ term t a finite sequence of $\widetilde{\mathbf{R}}_H$ terms

$$t_0, \ldots, t_k$$

which give important information about the number of distinct zeros of $t(x, \vec{b})$ in any interval of definition.

Let us say that a term $t(x, \vec{y})$ has the property $\mathcal{R}(x, k)$ if there is a sequence of $\widetilde{\mathbf{R}}_H$ terms

$$t_0(x, \vec{y}),\ \ldots,\ t_k(x, \vec{y})$$

such that

$$(1)\quad t_0(x, \vec{y}) = t(x, \vec{y}) \quad \text{and} \quad \frac{\partial}{\partial x} t_k(x, \vec{y}) = 0$$

(2) For every interval $I \subseteq \mathbb{R}$ and every tuple $\vec{b} \in \mathbb{R}^n$, if $t(x, \vec{b})$ is defined on I then, for each $a \in I$ and each $i < k$, $t_{i+1}(a, \vec{b})$ is defined and

$$t_{i+1}(a, \vec{b}) = 0 \qquad \Leftrightarrow \qquad \frac{\partial}{\partial x} t_i(a, \vec{b}) = 0.$$

The simplest example is when $t(x)$ is a polynomial.

Example 3.1. Let $t(x)$ be a polynomial of degree k. Then

$$t(x),\ t'(x),\ \ldots,\ t^{(k)}$$

is a sequence that shows $t(x)$ has $\mathcal{R}(x, k)$.

In this case the length of the sequence is just the degree of the polynomial. However the sequences quickly become more complicated:

Example 3.2. If $p(x)$ is a polynomial of degree k and $q(x)$ is a polynomial of degree ℓ, then for $t(x) = \exp(p(x)/q(x)) - 1$ let $r(x) = p(x)q'(x) - q(x)p'(x)$. The sequence

$$e^{p(x)/q(x)} - 1,\ r(x),\ r'(x),\ \ldots,\ r^{(k+\ell-1)}(x)$$

shows that $t(x)$ has the property $\mathcal{R}(x, k + \ell - 1)$.

Suppose that $t(x, \vec{y})$ is an $\widetilde{\mathbf{R}}_H$ term that has property $\mathcal{R}(x, k)$. It is easy to show that for any interval I and any tuple $\vec{b}$, if $t(x, \vec{b})$ is defined in I then

either $t(x, \vec{b}) = 0$ on I, or $t(x, \vec{b})$ has at most k distinct roots in I.

Richardson's main result is that for each $\widetilde{\mathbf{R}}_H$ term $t(\vec{x})$ and each variable x_i from $\vec{x}$

there is an effective procedure to find a nonnegative integer k such that $t(\vec{x})$ has property $\mathcal{R}(x_i, k)$.

It is amazing that one is able to effectively bound the *number* of roots of $t(x, \vec{b})$ on any interval I for which it is defined but not identically 0, but we do not know how to effectively bound the *size* of the roots in the interval I. (See Problems 3 and 4.)

From Richardson's result one immediately has:

Theorem 3.3 (Richardson [23] (1969))**.** *The one variable identities* $s(x) \approx t(x)$ *of* $\mathbf{N}$ *are decidable.*

3.2. Macintyre's Proof.

Macintyre, initially unaware of Richardson's work, tackled the decidability of the identities of $\mathbf{N}$ by refining Hardy's work, but using the language of $\widetilde{\mathbf{R}}_H$. At each step of Hardy's induction proof in which $t(x, \vec{b})$ is not identically 0 on an interval I, Macintyre effectively computed an upper bound on the number of roots of $t(x, \vec{b})$ in I. This allows him to prove the decidability of one variable equations, and then a simple inductive argument gives:

Theorem 3.4 (Macintrye, [18] (1981))**.** *The identities* $s(\vec{x}) \approx t(\vec{x})$ *of* $\mathbf{N}$ *are decidable.*

We note that Macintyre's proof of the one variable case requires an excursion into the complex plane, something that the other two published proofs do not.

3.3. Gurevič's Proof. Another proof of the decidability of the equational theory of $\mathbf{N}$ was given by Gurevič [11] (1985) using ideas of A. G. Khovanskii. This proof has a resemblance to that of Richardson, with the emphasis on building a *chain of terms* $t_0, \ldots, t_k$ linked in some fashion by differentiation. In Gurevič's paper the t_i must satisfy

$$t_0 = T, \quad t_k \in Q, \quad \frac{\partial t_j}{\partial x} \;=\; \frac{\beta_j t_j + t_{j+1}}{\alpha_j}$$

By solving these linear differential equations one sees that the number of roots in I can drop by at most one when passing from t_j to t_{j+1}, in any given interval of definition I of t_0 in which $t_j(x, \vec{b})$ is not identically 0,

In the same paper Gurevič examines the equational consequences of any finite set Σ of identities true of $\mathbf{N}$ that contains the identities

$$1^x \approx 1, \qquad x^1 \approx 1 \cdot x \approx x \cdot 1 \approx x. \tag{3.1}$$

He gives a decision procedure that takes as input any such Σ and identity $s \approx t$ and determines if $\Sigma \vdash s \approx t$. The method is to describe a congruence of the term algebra generated by the finitely many variables of Σ, s and t, that yields a finite quotient whose size is effectively bounded and in which $s \approx t$ will fail if it is not a consequence of Σ. Thus

Theorem 3.5 (Gurevič [11] (1985))**.** *If Σ is a finite set of identities including* (3.1) *and true of $\mathbf{N}$ then the equational consequences of Σ form a decidable set of identities.*

Corollary 3.6 (Gurevič [11] (1985))**.** *The equational consequences of HSI are decidable.*

4. The Study of $\mathbf{R}_{\exp}$

Our understanding of the first-order theory of

$$\mathbf{R}_{\exp} \;=\; (R, +, -, \times, \exp, 0, 1, <)$$

has made great strides in the last two decades. The interest in this structure was motivated by the famous result of Tarski that showed the ordered field

$$\mathbf{R} \;=\; (R, +, \times, -, 0, 1, <)$$

has a decidable first-order theory, a result proved by the method of elimination of quantifiers. There are three results that we want to mention here:[3]

- $\mathbf{R}_{\exp}$ is O-minimal.
- $\mathbf{R}_{\exp}$ has a model-complete theory.
- If Schanuel's conjecture holds then $\mathbf{R}_{\exp}$ has a decidable first-order theory.

---

[3]We are indebted to Charles Steinhorn for an enlightening conversation on the importance of these results.

To see that the study of the first-order theory of $\mathbf{R}_{\exp}$ impacts our understanding of $\mathbf{N}$ we only need to note that $y \approx \log x$ is first-order definable by $x \approx \exp y$. Thus one can define $z \approx x \uparrow y$ for positive x, y by

$$(0 < x)\&(0 < y)\&\exists u\big((x \approx \exp u)\&z \approx \exp(yu)\big).$$

Then one can see that all term functions of $\mathbf{R}^+$ are first-order definable in $\mathbf{R}_{\exp}$.

4.1. O-minimal. An ordered structure $\mathbf{A}$ is said to be *O-minimal* if every set defined by a first-order formula $\phi(x, \vec{a})$ with parameters $\vec{a}$ from $\mathbf{A}$ is just a union of finitely many open intervals and finitely many points. In particular this says that a definable subset is either bounded above or contains an interval (a, ∞).

Tarski's elimination of quantifiers for $\mathbf{R}$ easily yields the result that $\mathbf{R}$ is O-minimal—after all, a quantifier free formula in a single variable with parameters $\vec{a}$ is (effectively equivalent to) a Boolean combination of atomic formulas of the form $p(x, \vec{a}) \approx 0$, where p is a polynomial.

However we do not have elimination of quantifiers for $\mathbf{R}_{\exp}$. According to [28], Charbonnel presented an incomplete proof of the O-minimality of $\mathbf{R}_{\exp}$ in 1991—the gaps were filled by Wilkie.

Hardy's Theorem from Section 2 is an easy corollary of O-minimality of $\mathbf{R}_{\exp}$ since any two $\mathbf{R}_H$ terms $s(x)$ and $t(x)$ can be expressed by first-order formulas of $\mathbf{R}_{\exp}$ with real parameters, and thus the set of points where $s(x)$ is less than $t(x)$ is definable by a first-order formula of $\mathbf{R}_{\exp}$ with real parameters.

By O-minimality one also sees that the set of points where a term of $\mathbf{R}_H$, or a term of $\widetilde{\mathbf{R}}_H$, is undefined is a union of finitely many open sets and finitely many points.

4.2. Model Completeness. A first-order theory is *model complete* if every submodel of a model of the theory is an elementary submodel. Although not obvious, this is equivalent to requiring that every first-order formula be equivalent to an existential formula. Hence one can view model completeness as a step toward quantifier elimination. Wilkie [29] (1996) proved that the first-order theory of $\mathbf{R}_{\exp}$ is model complete. This does not have an immediate bearing on our study of HSI, but it led to the next topic.

4.3. Decidability and Schanuel's Conjecture. Schanuel's conjecture says that if $z_1, \ldots, z_n$ are linearly independent complex numbers over the field $\mathbf{Q}$ of rationals then the field extension $\mathbf{Q}\big(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}\big)$ has transcendence degree over Q at least n. (This conjecture is widely believed to be correct.) The Schanuel Conjecture for the Reals means his conjecture with $z_1, \ldots, z_n$ restricted to the reals.

Theorem 4.1 (Macintyre and Wilkie [19] (1996))**.** *If Schanuel's Conjecture for the Reals holds then the first-order theory of* $\mathbf{R}_{\exp}$ *is decidable.*

Since the term functions of $\mathbf{R}^+$ are definable by first-order formulas of $\mathbf{R}_{\exp}$, it follows that the problems posed at the beginning of Section 3 have positive answers if Schanuel's conjecture holds.

Corollary 4.2. *If Schanuel's Conjecture [for the reals] holds then the Eventually Defined Problem and the Dominance Problem are decidable, and one effectively has a bound on the Root Size for $t(x)$ for any interval I in which $t(x)$ is defined but not identically zero.*

5. Exotic identities of N

By the 1960s there was an interest in determining if HSI actually axiomatizes the equational theory of **N**. Although the identities were known to be decidable, this did not give a way to determine if there are any exotic identities of **N**, that is, identities not following from HSI.

5.1. The Wilkie Identity. In 1981 Wilkie circulated a manuscript[4] [27] showing that the identity

$$\begin{aligned}&\big((1+x)^y + (1+x+x^2)^y\big)^x \cdot \big((1+x^3)^x + (1+x^2+x^4)^x\big)^y \\ &\quad\approx \big((1+x)^x + (1+x+x^2)^x\big)^y \cdot \big((1+x^3)^y + (1+x^2+x^4)^y\big)^x,\end{aligned}$$

which we call $W(x,y)$, is indeed an exotic identity of **N**.

Wilkie's proof was purely syntactic, using an induction on the length of a supposed derivation of $W(x,y)$ from HSI. This proof was soon augmented by a model theoretic proof of Gurevič [11] (1985). Using the subterms of $W(x,y)$, and a little tweaking, Gurevič constructed a 59-element algebra satisfying HSI but not $W(x,y)$. In Gurevič [12] (1990) we find the following remark (p. 33):

> C.W. Henson once asked if there are countermodels to Tarski's question (whether all valid identities in signature $(+,\cdot,\uparrow)$ were derivable) of a very small size, say, 5. Currently I don't know; my own record was 33 elements and I heard a rumour that someone had pushed the record further to 28 elements.

Since then there has been considerable progress in the search for a smallest counterexample to $W(x,y)$. The second column gives the size of a counterexample that has been found, the third column a lower bound on the size of any counterexample.

R. Gurevič	59 elements		[11] (1985)
	⋮		
R. Gurevič	33 elements		($\leq$ 1990)
S. Burris	28 elements		(1988)
	⋮		
S. Burris	16 elements		(1990)
S. Lee	15 elements		(1991)
S. Burris, S. Lee	15 elements	$\geq$ 7 elements	[4] (1992)

[4]This manuscript was not put in final form and published until 2002.

M. Jackson	14 elements	≥ 8 elements	[17] (1996)
S. Burris, K. Yeats	13 elements		(2001)
S. Burris, K. Yeats	12 elements		Fig. 4 (2001)

Conjecture 3. The 12 element algebra in Fig. 4 is a smallest counterexample to Wilkie's identity.

5.2. How We Found the 12-Element Example. The method used first a lengthy search for possible *cores* of such an example. If $W(x, y)$ fails in a model of HSI at (a, b) then we call the $\widehat{\text{HSI}}$-subalgebra generated by $\{a\}$ a core of the model. Burris and Lee [4] (1992) state a number of conditions that cores must satisfy, for example, there must be at least three integers.

So first we searched for possible cores. Then we tried to expand the core candidates to models of HSI that failed $W(x, y)$. Again we had some conditions that b must satisfy if $W(a, b)$ is to fail, for example b cannot be in the core generated by a (Jackson [17] (1996)). C-programs were written and a few months of computing needed ...

5.3. The Search for Natural Counterexamples to Wilkie's Identity. The counterexamples to Wilkie that we know are quite intricate and certainly not easy to remember. One can hope for a natural counterexample along the lines of Birkhoff's algebra of posets. The natural HSI-algebras that we have constructed from relational structures or topologies share features of Birkhoff's algebra that lead to $W(x, y)$ being satisfied, namely:

(a) elements of the algebra are structures that decompose into sums of components,
(b) exponentiation is given by certain maps, and such decompose into maps on the components, and
(c) product is given by Cartesian product.

Problem 7. Is there is natural counterexample to $W(x, y)$?

Fiore, Di Cosmo and Balat [10] have answered Problem 7 in the negative within the context of cartesian closed categories with finite coproducts.[5]

Problem 8. Is there a natural HSI-algebra that is not in $V(\mathbf{N})$? In particular, is the algebra of [finite] posets in $V(\mathbf{N})$?

Problem 9. Is there an algebra with fewer than 12 elements that satisfies HSI but is not in the variety generated by $\mathbf{N}$?

[5]We are indebted to Sergei Soloviev for bringing this developement to our attention.

$+$	1	2	3	4	a	b	c	d	e	f	g	h
1	2	3	4	4	2	3	d	3	3	3	3	4
2	3	4	4	4	3	4	3	4	4	4	4	4
3	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4
a	2	3	4	4	b	4	b	3	h	3	3	4
b	3	4	4	4	4	4	4	4	4	4	4	4
c	d	3	4	4	b	4	b	3	3	3	3	4
d	3	4	4	4	3	4	3	4	4	4	4	4
e	3	4	4	4	h	4	3	4	4	3	h	4
f	3	4	4	4	3	4	3	4	3	4	3	4
g	3	4	4	4	3	4	3	4	h	3	4	4
h	4	4	4	4	4	4	4	4	4	4	4	4

$\times$	1	2	3	4	a	b	c	d	e	f	g	h
1	1	2	3	4	a	b	c	d	e	f	g	h
2	2	4	4	4	b	4	b	4	4	4	4	4
3	3	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	b	4	4	c	b	c	b	h	4	4	4
b	b	4	4	4	b	4	b	4	4	4	4	4
c	c	b	4	4	c	b	c	b	4	4	4	4
d	d	4	4	4	b	4	b	4	4	4	4	4
e	e	4	4	4	h	4	4	4	4	4	h	4
f	f	4	4	4	4	4	4	4	4	4	4	4
g	g	4	4	4	4	4	4	4	h	4	4	4
h	h	4	4	4	4	4	4	4	4	4	4	4

$\uparrow$	1	2	3	4	a	b	c	d	e	f	g	h
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	4	4	4	4	4	4	f	4	4	4
3	3	4	4	4	e	4	4	4	g	4	e	h
4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	c	c	c	c	c	c	c	c	c	c	c
b	b	4	4	4	4	4	4	4	4	4	4	4
c	c	c	c	c	c	c	c	c	c	c	c	c
d	d	4	4	4	f	4	4	4	4	4	4	4
e	e	4	4	4	4	4	4	4	h	4	4	4
f	f	4	4	4	4	4	4	4	4	4	4	4
g	g	4	4	4	h	4	4	4	4	4	h	4
h	h	4	4	4	4	4	4	4	4	4	4	4

FIGURE 4. A Twelve-Element Counterexample to Wilkie's Identity

5.4. The Smallest Exotic Identity. If $s(x) \approx t(x)$ is a one-variable equation that holds in $\mathbf{N}$ then both sides of the equation define the same Skolem function on N. Thus given two such identities $s_i(x) \approx t_i(x)$, $i = 1, 2$, we say that *the first identity is smaller than the second identity* if $s_1(x) \prec s_2(x)$ holds. Ehrenfeucht's Theorem says that the set of Skolem functions of $\mathbf{N}$ are well-ordered by $\prec$, so one can ask:

Problem 10. What is the smallest one variable exotic identity?

Conjecture 4 (Gurevič [12] (1990), p. 29)**.** The smallest exotic identity is

$$(P^x + Q^x)^{2^x} \cdot (R^{2^x} + S^{2^x})^x \;=\; (P^{2^x} + Q^{2^x})^x \cdot (R^x + S^x)^{2^x}$$

where

$$\begin{aligned} P &= 1 + x \\ Q &= 2 + x \\ R &= 2 + x + x^3 \\ S &= 4 + x^2 + x^3. \end{aligned}$$

5.5. The Search for Non-Exotic Identities. Considerable effort has been expended to find nice sets S of terms such that any equation true of $\mathbf{N}$ that has both sides from S will be a consequence of HSI. C.W. Henson and L.A. Rubel used Nevanlinna theory in [16] (1984) to show that S can be the set of terms that only use exponentiation of variables or constants. Gurevič [13] (1993) extended this work by showing that one can allow exponentiation of polynomials.

6. The Equational Theory of N is not Finitely Axiomatizable

Gurevič [12] (1990) showed that there is no finite set of identities that axiomatize the identities of $\mathbf{N}$. Indeed the following collection of Wilkie style identities in one variable x are true of $\mathbf{N}$ but cannot all be derived from any finite subset of the identities true of $\mathbf{N}$ (n is odd in the following):

$$(P^x + Q_n^x)^{2^x} \cdot (R_n^{2^x} + S_n^{2^x})^x \;=\; (P^{2^x} + Q_n^{2^x})^x \cdot (R_n^x + S_n^x)^{2^x}$$

where

$$\begin{aligned} P &= 1 + x \\ Q_n &= 1 + x + \cdots + x^{n-1} \\ R_n &= 1 + x^n \\ S_n &= 1 + x^2 + \cdots + x^{2n-2}. \end{aligned}$$

Although much of his proof of the non-finitely axiomatizable result is an elementary study of the forms in which terms and equational proofs can be expressed, at one point he needs to go into the complex plane and examine analytic continuations of complex functions around singularities.

References

[1] Chris Arbuthnott, Master's Thesis, University of Waterloo, 2002.

[2] Gurgen R. Asatryan, *A solution to identities problem in 2-element HSI-algebras.* MLQ Math. Log. Q. **50** (2004), no. 2, 175–178.

[3] Garrett Birkhoff, *Generalized Arithmetic.* Duke Math. J. **9** (1942), 283–302.

[4] S. Burris and S. Lee, *Small models of the High School Identities.* Internat. J. Algebra Comput. **2** (1992), 139–178.

[5] S. Burris and S. Lee, *Tarski's High School Identities.* Amer. Math. Monthly **100** (1993), 231–236.

[6] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra.* Grad. Texts in Math. **78**, Springer-Verlag, 1981. [Now available online from *www.thoralf.uwaterloo.ca*]

[7] Bernd I. Dahn, *Fine structure of the integral exponential functions below* 2^{2^x}. Trans. Amer. Math. Soc. **297** (1986), 707–716.

[8] Richard Dedekind, *Was sind und was sollen die Zahlen?* 8te unveränderte Aufl. Friedr. Vieweg & Sohn, Braunschweig 1960. [English Translation: *What are numbers and what should they be?* Revised, edited, and translated from the German by H. Pogorzelski, W. Ryan and W. Snyder. RIM Monographs in Mathematics. Research Institute for Mathematics, Orono, ME, 1995.]

[9] A. Ehrenfeucht, *Polynomial functions with exponentiation are well ordered.* Alg. Universalis **3** (1973), 261-349.

[10] Marcelo Fiore, Roberto Di Cosmo and Vincent Balat, *Remarks on isomorphisms in typed lambda calculi with empty and sum types.* IEEE Symposium LICS 2002. Copenhagen, Denmark, July 2002.

[11] R. Gurevič, *Equational theory of positive numbers with exponentiation.* Proc. Amer. Math. Soc. **94** (1985), 135–141.

[12] R. Gurevič, *Equational theory of positive numbers with exponentiation is not finitely axiomatizable.* Annal of Pure and Applied Logic **49** (1990), 1–30.

[13] R.H. Gurevič, *Detecting algebraic (in)dependence of explicitly presented functions (some applications of Nevanlinna theory to mathematical logic).* Trans. Amer. Math. Soc. **336** (1993), 1–67.

[14] R.H. Gurevič, *Transcendental numbers and eventual dominance of exponential functions.* Bull. London. Math. Soc. **18** (1986), 560–570.

[15] G.H. Hardy, *Orders of Infinity, the 'Infinitar' Calcul of Paul Du Bois-Reymond.* Cambridge University Press. [first ed. 1921] 2nd ed. 1954.

[16] C.W. Henson and L.A. Rubel, *Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions.* Trans. Amer. Math. Soc. **282** (1984), 1–32.

[17] M.G. Jackson, *A note on HSI-identities and counterexamples to Wilkie's identity.* Algebra Universalis **36** (1996), 528–535.

[18] A. Macintyre, *The laws of exponentiation.* Model theory and arithmetic. (Paris, 1979-1980) Lecture Notes in Math. **890**, 185–197. Springer, 1981.

[19] Angus Macintrye and A.J. Wilkie, *On the decidability of the real exponential field.* Kreiseliana: about and around Georg Kreisel, ed. by P. Olfreddi, 441–467, A.K. Peters, 1996.

[20] David Marker, *Khovanskii's theorem.* Algebraic Model Theory, eds. Bradd T. Hart, Alistair H. Lachlan and Matthew A. Valeriote, 181–193, Kluwer Academic Publ., 1997.

[21] Anand Pillay and Charles Steinhorn, *Definable sets in ordered structures. I* Trans. Amer. Math. Soc. **295** (1986), 565–592.

[22] Julia F. Knight, Anand Pillay and Charles Steinhorn, *Definable sets in ordered structures. II* Trans. Amer. Math. Soc. **295** (1986), 593–605.

[23] D. Richardson, *Solution of the identity problem for integral exponential functions.* Zeitschr. f. math. Logik und Grundlagen d. Math. **15** (1969), 333–340.

[24] John Shackell, *Growth estimates for exp-log functions.* J. Symbolic Computation **10** (1990), 611–632.

[25] Lou van den Dries, *A completeness theorem for trigonometric identities and various results on exponential functions.* Proc. Amer. Math. Soc. **96** (1986), 345–352.

[26] Lou van den Dries, Hilbert Levitz, *On Skolem's exponential functions below* 2^{2^x}. Trans. Amer. Math. Soc. **286** (1984), 339–349.

[27] A.J. Wilkie, *On exponentiation — a solution to Tarski's high school algebra problem.* Quaderni di Matematica (to appear).

[28] A.J. Wilkie, *O-Minimality.* Documenta Mathematica, Extra Volume ICM 1998, **1** 633–636.

[29] A.J. Wilkie, *Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function.* J. Amer. Math. Soc. **4** (1996), 1051–1094.

[30] A.J. Wilkie, *Schanuel's conjecture and the decidability of the real exponential field.* Algebraic Model Theory, eds. Bradd T. Hart, Alistair H. Lachlan and Matthew A. Valeriote, 223–230, Kluwer Academic Publ., 1997.

Dept. of Pure Mathematics, University of Waterloo, Waterloo, Ont., Canada N2L 3G1

E-mail address: snburris@thoralf.uwaterloo.ca

Department of Mathematics and Statistics at Boston University 111 Cummington Street, Boston, MA 02215

E-mail address: kayeats@math.bu.edu