SMALL MODELS OF THE HIGH SCHOOL IDENTITIES

STANLEY BURRIS AND SIMON LEE

Abstract. First we look at some easy ways to construct small models of the High School Identities. And then we prove that any model which rejects the Wilkie identity must have at least seven elements; and we show that we have such a model with fifteen elements.

In the 1960's Tarski noted that there are only eleven basic identities of the positive integers N which one learns in high school, namely

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

This collection of identities will be called HSI, as indicated above; the subset of HSI which involves only the operation symbols $+, \times, 1$ is called $\overline{\text{HSI}}$. Actually the identities of HSI were isolated in the famous 1888 work of Dedekind "Was sind und was sollen die Zahlen". He proved that they followed from the so-called Peano axioms. With such a long and famous history it is somewhat surprising that for most mathematicians the study of the fundamental identities of the natural numbers end with high school. So it might be somewhat surprising to learn that

(1) there are lots of very small models of HSI, and
(2) there are identities true of $\mathbf{N}$ which cannot be derived from HSI.

Date: May 25, 2024 (but originally 1992).
First author supported by a grant from NSERC.
Second author supported by an NSERC Undergraduate Fellowship.

An attempt to classify just the finite quotients of **N** will lead us to a fascinating problem in number theory. And, regarding (ii), Tarski asked if HSI is a basis for all the identities of **N**. This question, know as Tarski's High School Problem, was answered in the negative in 1980 by Wilkie [15]. We will prove Wilkie's result by using a finite model of HSI, a method first discovered by Gurevič in 1985.

We would like to thank Walter Taylor for bringing Wilkie's identity to our attention as a candidate for computer algebra investigation; and Ken Davidson, Denis Higgs and Peter Hoffman for their interest and contributions to this project. A summary of the results in this paper can be found in the expository article [1].

1. Basics

Definition 1.1. Let $\mathcal{L}$ be the language $\{+, \times, \uparrow, 1\}$ consisting of three binary function symbols and one constant symbol. An $\mathcal{L}$-algebra $\mathbf{A}$ which satisfies (1) – (11) will be called an HSI-*algebra.*

When writing expressions such as $x \times y$ and $x \uparrow y$ we prefer to use the more compact notation $x \cdot y$, respectively x^y.

Definition 1.2. **N** is the HSI-algebra $\langle N, +, \times, \uparrow, 1\rangle$, where N is the set of positive integers, and $+, \times, \uparrow$ are the familiar operations of addition, multiplication and exponentiation.

Definition 1.3. Let $\overline{\mathcal{L}}$ be the language $\{+, \times, 1\}$ consisting of two binary function symbols and one constant symbol. An $\overline{\mathcal{L}}$-algebra $\mathbf{A}$ which satisfies $\overline{\text{HSI}}$ will be called an $\overline{\text{HSI}}$-*algebra.*

Definition 1.4. If $\mathbf{A} = \langle A, +, \times, \uparrow, 1\rangle$ is an $\mathcal{L}$-algebra, then the *reduct* of $\mathbf{A}$ to the language $\overline{\mathcal{L}}$ is denoted by $\overline{\mathbf{A}}$, i.e., $\overline{\mathbf{A}} = \langle A, +, \times, 1\rangle$, where $+, \times$, and 1 are as in $\mathbf{A}$.

It is obvious that if $\mathbf{A}$ is an HSI-algebra then $\overline{\mathbf{A}}$ is an $\overline{\text{HSI}}$-algebra. Thus in particular $\overline{\mathbf{N}}$ is the familiar $\overline{\text{HSI}}$-algebra $\langle N, +, \times, 1\rangle$. However given an $\overline{\text{HSI}}$-algebra $\mathbf{B}$ it may not be possible to expand it to an HSI-algebra, i.e., there may not be an HSI-algebra $\mathbf{A}$ such that $\overline{\mathbf{A}} = \mathbf{B}$. Indeed we will see many examples of this soon.

Definition 1.5. Let $\mathbf{A}$ be an $\overline{\text{HSI}}$- or HSI-algebra. Then the elements in the subuniverse generated by the constant 1 are called the *integers* of $\mathbf{A}$.

Lemma 1.6. *If* $\mathbf{A}$ *is an* $\overline{\text{HSI}}$- *or* HSI-*algebra then the set of integers of* $\mathbf{A}$ *is*

$$\{\underbrace{1 + 1 + \cdots + 1}_{n} \; : \; n \in N\},$$

the set of finite sums of 1's.

Proof. Clearly each of the finite sums of 1's must be in the integers of **A**. Using $\overline{\text{HSI}}$, respectively HSI, one sees that this collection of elements is closed under the operations of **A** and includes the element 1. □

In an $\overline{\text{HSI}}$- or HSI-algebra **A** we simply write n for $\underbrace{1+1+\cdots+1}_{n}$.

2. Remarks on the Equational Theories of $\overline{\mathbf{N}}$ and $\mathbf{N}$

When working with the equational theory of $\overline{\mathbf{N}}$ we have the advantage that each $\overline{\mathcal{L}}$-term t has a simple *normal form* $\nu(t)$, called a *polynomial.* Actually, the normal forms for $\overline{\mathcal{L}}$-terms are a consequence of $\overline{\text{HSI}}$.

Theorem 2.1.

(a) *The equational theory Id($\overline{\mathbf{N}}$) of the natural numbers with addition and multiplication is decidable.*

(b) *The equational theory of $\overline{\mathbf{N}}$ is axiomatized by $\overline{\text{HSI}}$.*

Proof. An equation $t_1 \approx t_2$ holds in $\overline{\mathbf{N}}$ iff $\nu(t_1) = \nu(t_2)$ holds. Since we can effectively compute the normal forms of $\overline{\mathcal{L}}$-terms it follows that we have a decision procedure.

For part (b) let Σ be the set of $\overline{\mathcal{L}}$-equations which can be derived from $\overline{\text{HSI}}$. Then, since $\overline{\text{HSI}}$ holds in $\overline{\mathbf{N}}$ it follows that $\Sigma \subseteq \text{Id}(\overline{\mathbf{N}})$. Now let $t_1 \approx t_2$ hold in $\overline{\mathbf{N}}$. Using $\overline{\text{HSI}}$ we can find the (same) normal forms of t_1, t_2. This gives a derivation of $t_1 \approx t_2$ from $\overline{\text{HSI}}$. □

We do not have nice normal forms for $\overline{\mathcal{L}}$-terms modulo Id(**N**). So more sophisticated techniques were introduced to analyze Id(**N**). Methods from analysis (going back to G.H. Hardy) were used by Richardson [11] to show the decidability of the one-variable equational theory of **N**; and independently such methods were used by Macintyre [8] to show Id(**N**) is decidable. Gurevič[4] gives a very simple proof of the decidability of the equational consequences of HSI; and an alternate proof of the decidability of Id(**N**) based on Hovanskii's work on Pfaffian chains. Henson and Rubel [7] used Nevanlinna theory to show an interesting portion of Id(**N**) can be derived from HSI.

Wilkie's proof [15] that HSI does not axiomatize Id(**N**) uses some rather detailed proof theory. He finds an identity $W(x, y)$ which is true of **N** and is such that if HSI $\vdash W(x, y)$ then $(1) - (10) \vdash W(x, y)$. Eliminating the need for Axiom (11) is the difficult part of his proof.

After this he defines an unusual exponentiation on $\overline{\mathbf{N}}[x]$, the polynomials with coefficients from N, to give a model of (1)—(10) which does not satisfy $W(x,y)$. Later Gurevič [4] was able to find a 59 element model of HSI which does not satisfy $W(x,y)$. This is, aside from the difficulty of verifying that one does indeed have a model of HSI, the simplest proof known of Wilkie's result. And recently Gurevič [6] expanded his work to show that HSI does not have a finite basis.

3. Integer Algebras and Prime Numbers

Definition 3.1. An $\overline{\text{HSI}}$-algebra which is generated by the constant 1 is called an *integer* $\overline{\text{HSI}}$-*algebra*. Likewise, an HSI-algebra which is generated by the constant 1 is called an *integer* HSI-*algebra*.

Lemma 3.2. *If* $\mathbf{A}$ *is an integer* $\overline{\text{HSI}}$- *or* HSI-*algebra then*

$$A = \{\underbrace{1+1+\cdots+1}_{n} \ : \ n \in N\}.$$

Proof. Immediate from 1.6. □

Lemma 3.3. *In an integer* $\overline{\text{HSI}}$- *or* HSI-*algebra* $\mathbf{A}$ *we can use induction proofs, i.e., if* Φ *is a property such that* $\Phi(1)$ *holds, and* $\Phi(x) \to \Phi(x+1)$ *holds, then* $\forall x\, \Phi(x)$ *holds.*

Proof. Immediate from 3.2. □

Lemma 3.4. *The initial object (i.e., the free algebra freely generated by the empty set) in the class of* $\overline{\text{HSI}}$-*algebras is* $\overline{\mathbf{N}}$*; and in the class of* HSI-*algebras it is* $\mathbf{N}$*. Consequently the integer* $\overline{\text{HSI}}$-*algebras are (up to isomorphism) precisely the quotients of* $\overline{\mathbf{N}}$*; and the integer* HSI-*algebras are the quotients of* $\mathbf{N}$*.*

Proof. This is evident from the fact that there is only one infinite $\overline{\text{HSI}}$-algebra, respectively HSI-algebra, which is generated by the empty set. □

Definition 3.5. Let Δ_N be the identity relation on N, and for $a, k \in N$ let

$$\theta_{a,k} = \{\langle m,n\rangle \in N \times N \ : \ m = n; \text{ or } a \le m,n \text{ and } m \equiv n \bmod k\}.$$

Proposition 3.6. *The congruences of* $\overline{\mathbf{N}}$ *are precisely the relations* Δ_N *and the* $\theta_{a,k}$*, where* $a, k \in N$*.*

Proof. Clearly Δ_N and the $\theta_{a,k}$ are congruences of $\overline{\mathbf{N}}$, so we only need to show that any congruence of $\overline{\mathbf{N}}$ is of the desired form. Let θ be a congruence of $\overline{\mathbf{N}}$. Choose the smallest element $a \in N$ such that

a/θ, the equivalence class of a modulo θ, has more than one element in it; then choose the smallest $k \in N$ such that $a + k \in a/\theta$. Then $\theta = \theta_{a,k}$. □

Definition 3.7. For $a, k \in N$ let $\overline{\mathbf{N}}_{a,k}$ be the quotient algebra $\overline{\mathbf{N}}/\theta_{a,k}$.

Now have a complete description (up to isomorphism) of the integer $\overline{\text{HSI}}$-algebras, namely they are $\overline{\mathbf{N}}$ and the $\overline{\mathbf{N}}_{a,k}$ for $a, k \in N$. One can visualize the finite integer $\overline{\text{HSI}}$-algebras, namely the $\overline{\mathbf{N}}_{a,k}$, as loops with a tail (see Figure 1):

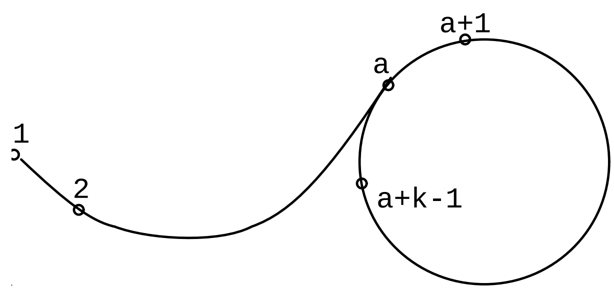

FIGURE 1. $\overline{\mathbf{N}}_{a,k}$

Now we turn to the integer HSI-algebras.

Lemma 3.8. *Any congruence of* $\mathbf{N}$ *which is not the identity relation must be one of the* $\theta_{a,k}$.

Proof. Every congruence of $\mathbf{N}$ is also a congruence of $\overline{\mathbf{N}}$. □

Definition 3.9. If $\theta_{a,k}$ is a congruence of $\mathbf{N}$ let $\mathbf{N}_{a,k}$ denote $\mathbf{N}/\theta_{a,k}$.

Lemma 3.10. $\theta_{a,k}$ *is a congruence of* $\mathbf{N}$ *iff*

$$x^a \equiv x^{a+k} \bmod k$$

holds for all $x \in N$.

Proof. $\theta_{a,k}$ is a congruence of $\mathbf{N}$ iff it is compatible with exponentiation, i.e., if $\langle m, n\rangle \in \theta_{a,k}$ then for $s \in N$ we want the following to hold:

$$\langle m^s, n^s\rangle \in \theta_{a,k} \tag{12}$$

$$\langle s^m, s^n\rangle \in \theta_{a,k}. \tag{13}$$

Now (12) follows from the fact that $\theta_{a,k}$ is compatible with multiplication. So we only have the condition (13) to deal with; and this reduces to the special case

$$\langle s^a, s^{a+k}\rangle \in \theta_{a,k} \tag{14}$$

which can be formulated as the requirement that

$$x^a \equiv x^{a+k} \bmod k \tag{15}$$

holds for all $x \in N$. □

The following result was communicated to us by Peter Hoffman.

Lemma 3.11. *Given $a, k \in N$,*

$$x^a \equiv x^{a+k} \bmod k, \tag{16}$$

holds for all $x \in N$ iff for all primes p we have

$$p^e|k \quad \Longrightarrow \quad e \leq a, \quad \text{and} \tag{17}$$

$$p|k \quad \Longrightarrow \quad (p-1)|k. \tag{18}$$

Proof. ($\Longrightarrow$) Suppose p, a prime, and $e \in N$ are such that $p^e|k$. Then

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

This establishes (17).

Now suppose p is a prime such that $p|k$. Choose $b \in N$ such that that the order of $[b]$ in the group of units of $\mathbf{Z}_p^\star$ is $p-1$ (such is possible since this group is cyclic). Since $p|k$, and from (16), $k|b^a(b^k - 1)$, we know that $p|b^a(b^k - 1)$; and as $p \nmid b$ it follows that $p|b^k - 1$. Then $[b]^k = 1$ in $\mathbf{Z}_p^\star$, so from elementary group theory $(p-1)|k$, which is (18).

($\Longleftarrow$) If $k = 1$ the implication is trivial. So let $k > 1$, say

$$k = p_1^{e_1} \cdots p_r^{e_r}$$

where the p_i are distinct primes, and the e_i are positive integers. Then from our assumptions we have, for $1 \leq i \leq r$,

$$e_i \leq a \qquad \text{and} \qquad (p_i - 1)|k.$$

Now let us fix our attention on one of the p_i, and let $b \in N$ be given.

Case i: Suppose $p_i|b$. Then use

$$\begin{aligned} p_i|b \quad &\Longrightarrow \quad p_i^{e_i}|b^{e_i}|b^a \\ &\Longrightarrow \quad p_i^{e_i}|b^a(b^k - 1) \\ &\Longrightarrow \quad b^a \equiv b^{a+k} \bmod p_i^{e_i}. \end{aligned}$$

Case ii: Suppose $p_i \nmid b$. First observe that $\phi(p_i^{e_i})|k$, where ϕ is the Euler phi function, since $\phi(p_i^{e_i}) = p_i^{e_i-1}(p_i-1)$, and since both $p_i^{e_i-1}|k$ and $(p_i-1)|k$. Using this (for the second step below) we have

$$\begin{aligned} p_i \nmid b \quad &\Longrightarrow \quad b^{\phi(p_i^{e_i})} \equiv 1 \bmod p_i^{e_i} \\ &\Longrightarrow \quad b^k \equiv 1 \bmod p_i^{e_i} \\ &\Longrightarrow \quad b^{a+k} \equiv b^a \bmod p_i^{e_i}. \end{aligned}$$

Thus, in either case, we have $b^a \equiv b^{a+k} \bmod p_i^{e_i}$; and since this holds for each $p_i^{e_i}$ it follows that $b^a \equiv b^{a+k} \bmod k$. This proves the lemma. □

Combining these two lemmas we have our main characterization of the congruences of **N**.

Theorem 3.12. *For $a, k \in N$ the relation $\theta_{a,k}$ is a congruence of* **N** *iff for all primes p we have*

$$p^e | k \;\Rightarrow\; e \le a \tag{19}$$

$$p | k \;\Rightarrow\; (p-1)|k. \tag{20}$$

From (20) we see that the only odd k which can appear in a finite integer HSI-algebra is $k = 1$. If $k = 1$ then for any $a \in N$ we have the finite integer HSI-algebra $\mathbf{N}_{a,1}$, i.e., one simply collapses all integers greater or equal to a. Also it is easy to see that with $k = 2$ we have for any $a \in N$ the finite integer HSI-algebra $\mathbf{N}_{a,2}$.

Corollary 3.13. *Let $\mathbf{N}_{a,k}$ be a finite integer* HSI-*algebra with $k > 1$, and let $k = p_1^{e_1} \cdots p_r^{e_r}$ with $p_1 < \cdots < p_r$. Then*

$$e_i \le a \text{ for } 1 \le i \le r \tag{21}$$

$$p_1 = 2 \tag{22}$$

$$(p_i - 1) | p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} \qquad \text{for } 2 \le i \le r. \tag{23}$$

Proof. (21) follows from (19); (22) and (23) follow from (20). □

From (23) we see that p_2 is always of the form $2^m + 1$, and hence it is a Fermat prime. The next corollary gives a complete list of the five "circle" integer HSI-algebras, i.e., those with $a = 1$, and hence no "tail".

Corollary 3.14 (D. Higgs)**.** *We have a finite integer* HSI-*algebra* $\mathbf{N}_{1,k}$ *iff $k \in \{1, 2, 6, 42, 1806\}$.*

Proof. Suppose $\mathbf{N}_{1,k}$ is an integer HSI-algebra. Then by 3.13

- $k = p_1 \cdots p_r$ where $p_1 < \cdots < p_r$
- $p_1 = 2$

- $(p_i - 1)|p_1 \cdots p_{i-1}$ for $2 \le i \le r$.

Then we have each of p_2 through p_4 uniquely determined, namely

$$\begin{array}{rcl} (p_2-1)|2 & \Longrightarrow & p_2 = 3 \\ (p_3-1)|2\cdot 3 & \Longrightarrow & p_3 = 7 \\ (p_4-1)|2\cdot 3\cdot 7 & \Longrightarrow & p_4 = 43; \end{array}$$

and there is no prime $p_5 > 43$ such that $(p_5 - 1)|2\cdot 3\cdot 7\cdot 43 = 1806$. □

Jeff Shallit [3] pointed out that the sequence $2, 3, 7, 43, 1807$ occurs in a number of places in the literature, e.g., as solutions to Sylvester's recurrence equations.

Definition 3.15. 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 3.16. *Given a positive integer a, there are infinitely many integer* HSI-*algebras $\mathbf{N}_{a,k}$ (i.e., with tail having length $a-1$) iff the sequence of primes Σ_a is infinite.*

Proof. Let $\Sigma_a = (p_1, \cdots)$, and define $\Pi_a = (q_1, \cdots)$ to be the list of primes q, in increasing order, for which there exists a $k \in N$ with $q|k$ and $\theta_{a,k}$ a congruence of $\mathbf{N}$.

If Π_a is infinite then there must be arbitrarily large k such that $\theta_{a,k}$ is a congruence of $\mathbf{N}$, so there are arbitrarily large integer HSI-algebras $\mathbf{N}_{a,k}$.

On the other hand, for a given finite set S of primes one has, by 3.12, only finitely many k for which $\theta_{a,k}$ is a congruence of $\mathbf{N}$ and the primes dividing k are in S. Thus if we have infinitely many integer HSI-algebras $\mathbf{N}_{a,k}$ the sequence Π_a must be infinite. Consequently there are infinitely many $\mathbf{N}_{a,k}$ iff Π_a is infinite.

Now we want to show that $\Sigma_a = \Pi_a$. Let $p \in \Sigma_a$, say $p = p_i$. Then letting $k = (p_1 \cdots p_i)^a$ we have $\theta_{a,k}$ is a congruence of $\mathbf{N}$ by 3.12, so p_i appears in Π_a.

To show each prime of Π_a also appears in Σ_a we use a simple induction argument. First note that $p_1 = q_1 = 2$. Now suppose $p_j = q_j$ for $1 \le i \le j$. If there is a q_{i+1} then choose $k \in N$ such that $q_{i+1}|k$ and $\theta_{a,k}$ is a congruence of $\mathbf{N}$. The primes dividing k which are smaller than q_{i+1} must be among $q_1, \ldots, q_i$ (by the definition of Π_a), and thus among $p_1, \dots, p_i$. From 3.13 we see that $(q_{i+1} - 1)|(p_1 \cdots p_i)^a$, so q_{i+1} appears in the list Σ_a.

Thus $\Pi_a = \Sigma_a$, and the proposition is proved. □

As we have seen in Higgs result, $\Sigma_1 = (2, 3, 7, 43)$, a finite sequence.

Problem 1. Is Σ_a finite for $a > 1$? for some $a > 1$?

We have checked that about 20% of the primes below 1,000,000 are in $\Sigma_2 = (2, 3, 5, 7, 11, 13, 19, 23, \dots, 999667, 999727, \dots)$. Due to the slow tapering off of this sequence it appears that we will not be able to find Σ_2 by computer, if it is finite.

4. The Five 2-Element HSI-Algebras

After determining the five 2-element HSI-algebras we use them to show how one can make a large number of finite HSI-algebras from well-known algebras (like distributive lattices).

Theorem 4.1. *There are exactly five 2-element* HSI-*algebras, up to isomorphism, and they are:*

(1)

+	1	a
1	1	1
a	1	a

×	1	a
1	1	a
a	a	a

↑	1	a
1	1	1
a	a	1

(2)

+	1	a
1	1	1
a	1	a

×	1	a
1	1	a
a	a	a

↑	1	a
1	1	1
a	a	a

(3)

+	1	a
1	1	a
a	a	a

×	1	a
1	1	a
a	a	a

↑	1	a
1	1	1
a	a	a

(4)

+	1	2
1	2	2
2	2	2

×	1	2
1	1	2
2	2	2

↑	1	2
1	1	1
2	2	2

(5)

+	1	2
1	2	1
2	1	2

×	1	2
1	1	2
2	2	2

↑	1	2
1	1	1
2	2	2

Proof. First we set out to find the possible distinct 2-element HSI-algebras. Such an algebra has either one or two integers in it, so the possible cases are:

Case 1: $\boxed{2 = 1}$**:** From (6) and (9) we have

$$x + x \approx x \qquad x \cdot x \approx x.$$

Thus Cayley tables for such an HSI-algebra would look like

$+$	1	a
1	1	b
a	b	a

$\times$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	c

This gives at most 4 possibilities, namely the algebras 1,2, 3 above, and

$+$	1	a
1	1	a
a	a	a

$\times$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	1

However this last algebra fails to satisfy (9) as $a^{1+a} = a^a = 1$, but $a^1 \cdot a^a = a \cdot 1 = a$.

Case 2: $\boxed{2 \neq 1}$**:** Then all elements of the algebra are integers, i.e., we are dealing with integer HSI-algebras. There are exactly two 2-element integer HSI-algebras, namely $\mathbf{N}_{2,1}$, which is **4** above, and $\mathbf{N}_{1,2}$, which is **5** above.

Now we have narrowed the list of possible 2-element HSI-algebras to the five above; and it is easy to check that each of these does indeed satisfy HSI, and that no two are isomorphic. □

To give one indication of just how limited our knowledge is about the $\mathcal{L}$-identities of $\mathbf{N}$ we ask the following.

Problem 2. Does every 2-element HSI-algebra satisfy *all* the identities of $\mathbf{N}$?

Of course the algebras $\mathbf{N}_{2,1}$ and $\mathbf{N}_{1,2}$ satisfy $\mathrm{Id}(\mathbf{N})$ since they are quotients of $\mathbf{N}$. So the problem is concerned with the first three algebras in 4.1. From a universal algebra point of view the answer will be yes iff each of these three algebras is a homomorphic image of the subalgebra $\mathbf{F}$ of $\mathbf{N}^N$ generated by the element $\langle 1, 2, 3, \cdots \rangle$. If there is some identity $p \approx q$ true of $\mathbf{N}$ but not true of one of these 2-element algebras, then we have a very fast proof that $p \approx q$ does not follow from HSI. (Regarding Wilkie's identity, we will see that the known countermodels are rather cumbersome for careful checking by hand.)

5. Five Classes of HSI-Algebras

First some examples of $\overline{\mathrm{HSI}}$-algebras.

Lemma 5.1.

(a) *Let* $\mathbf{D} = \langle D, \vee, \wedge, 1 \rangle$ *be a distributive lattice with largest element 1. Then* $\mathbf{D}$ *is an* $\overline{\mathrm{HSI}}$*-algebra.*

(b) *Let* $\mathbf{S} = \langle S, \wedge, 1 \rangle$ *be a meet semilattice with largest element 1. Then* $\langle S, \wedge, \wedge, 1 \rangle$ *is an* $\overline{\mathrm{HSI}}$*-algebra.*

Proof. Immediate from the basic laws of distributive lattices and semilattices. ☐

Lemma 5.2. *Let* $\mathbf{A} = \langle A, +, \times, 1\rangle$ *be an* $\overline{\text{HSI}}$-*algebra. Then the expansion* $\mathbf{A}_\pi = \langle A, +, \times, \pi, 1\rangle$ *of* $\mathbf{A}$ *to an* $\mathcal{L}$-*algebra, where* π *is the first projection on* $A \times A$*, gives an* HSI-*algebra iff the operation of multiplication is idempotent, i.e.,* $x \cdot x \approx x$ *holds in* $\mathbf{A}$.

Proof. If we have an $\mathcal{L}$-algebra with the exponentiation given by $a^b = a$ then it is trivial to verify that the identities (7), (8), (10), and (11) are true. And (9) holds iff the multiplication is idempotent. ☐

We note that the $\overline{\text{HSI}}$ reducts of the algebras in 4.1 arise in this way, except for the first. Now we generalize each of the 2-element HSI-algebras.

Proposition 5.3. *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* $b \rightarrow a$.

Proof. Recall that the Heyting operation $\rightarrow$ is defined by: $a \rightarrow b = c$ iff c is the largest element such that $c \wedge a \leq b$. Since $\langle H, \vee, \wedge, 1\rangle$ is a distributive lattice with 1 it is an $\overline{\text{HSI}}$-algebra by 5.1. Now the identities (6) – (11), written with the operations of $\mathbf{H}^\star$, are

$$\begin{aligned} 1 \leftarrow x &\approx 1 \\ x \leftarrow 1 &\approx x \\ x \leftarrow (y \vee z) &\approx (x \leftarrow y) \wedge (x \leftarrow z) \\ (x \wedge y) \leftarrow z &\approx (x \leftarrow z) \wedge (y \leftarrow z) \\ (x \leftarrow y) \leftarrow z &\approx x \leftarrow (y \wedge z), \end{aligned}$$

and these are well known properties of Heyting algebras. ☐

Proposition 5.4. *Let* $\mathbf{D} = \langle D, \vee, \wedge, 1\rangle$ *be a distributive lattice with 1. Then* $\mathbf{D}_\pi = \langle D, \vee, \wedge, \pi, 1\rangle$ *is an* HSI-*algebra.*

Proof. Apply 5.1 and 5.2. $\mathbf{D}_\pi$ is isomorphic to a subdirect power of the second algebra in 4.1. ☐

$\mathbf{D}_\pi$ is isomorphic to a subdirect power of the second algebra in 4.1.

Proposition 5.5. *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.*

Proof. Apply 5.1 and 5.2. $\langle S, \wedge, \wedge, \pi, 1\rangle$ is isomorphic to a subdirect power of the third algebra in 4.1. ☐

$\langle S, \wedge, \wedge, \pi, 1\rangle$ is isomorphic to a subdirect power of the third algebra in 4.1.

Proposition 5.6. *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.*

Proof. Apply 5.2. $\langle S, f, \wedge, \pi, 1\rangle$ is isomorphic to a subdirect power of the fourth algebra in 4.1. □

$\langle S, f, \wedge, \pi, 1\rangle$ is isomorphic to a subdirect power of the fourth algebra in 4.1.

Proposition 5.7. *Let* $\mathbf{R} = \langle R, +, \times, 0, 1\rangle$ *be a Boolean ring. Then* $\langle R, +, \times, \pi, 1\rangle$ *is an* HSI-*algebra.*

Proof. Apply 5.2. $\langle R, +, \times, \pi, 1\rangle$ is isomorphic to a subdirect power of the fifth algebra in 4.1. □

$\langle R, +, \times, \pi, 1\rangle$ is isomorphic to a subdirect power of the fifth algebra in 4.1.

6. Remarks on Computational Accessibility

If A is a finite nonempty set of n elements then there are n^{n^2} possible binary functions on A; thus there are $n \cdot n^{3(n^2)}$ possible $\mathcal{L}$-algebras on A, and $n \cdot n^{2(n^2)}$ possible $\overline{\mathcal{L}}$-algebras on A. To find the 3-element HSI-algebras it seems wise (if not necessary) to turn to a computer after doing some preliminary reductions in the number of possibilities. First we apply the identities (1), (3), (4), (7) and (8) to restrict the 3-element HSI-algebras to the form

$+$	1	a	b
1	c	d	e
a	d	f	g
b	e	g	h

$\times$	1	a	b
1	1	a	b
a	a	i	j
b	b	j	k

$\uparrow$	1	a	b
1	1	1	1
a	a	l	m
b	b	n	o

The total number of algebras to test at this point would be 3^{13}, about 1,600,000. This would take a lot of computer time. To speed things up we proceed as in §4 and divide the study into cases depending on what the integers of the HSI-algebra look like. So we consider each of the five possibilities for the integers, namely $\mathbf{N}_{1,1}$, $\mathbf{N}_{1,2}$, $\mathbf{N}_{2,1}$, $\mathbf{N}_{2,2}$ $\mathbf{N}_{3,1}$.

Case 1: $\boxed{\mathbf{N}_{1,1}}$ In this case $x + x \approx x$ and $x \cdot x \approx x$ hold, and this reduces the possibilities for the Cayley tables to the following:

$+$	1	a	b
1	1	d	e
a	d	a	g
b	e	g	b

$\times$	1	a	b
1	1	a	b
a	a	a	j
b	b	j	b

$\uparrow$	1	a	b
1	1	1	1
a	a	l	m
b	b	n	o

The total number of cases to check is now $3^8 = 6,581$. By focusing on the first two Cayley tables there are $3^4 = 81$ $\overline{\mathcal{L}}$-algebras to examine, and of these only 10 turn out to be $\overline{\text{HSI}}$-algebras. Then for each of these 10 $\overline{\text{HSI}}$-algebras we have 81 possible expansions to an $\mathcal{L}$-algebra based on the third Cayley table above, so in total there are 810 $\mathcal{L}$-algebras to check in this case.

Case 2: $\boxed{\mathbf{N}_{2,1}}$ We have in this case (and the remaining cases) $x + x \approx 2 \cdot x$ and $x \cdot x \approx x^2$, which reduces the possibilities to:

$+$	1	2	b
1	1	2	e
2	2	2	g
b	e	g	h

$\times$	1	2	b
1	1	2	b
2	2	2	h
b	b	h	k

$\uparrow$	1	2	b
1	1	1	1
2	2	2	m
b	b	k	o

The total number of $\mathcal{L}$-algebras to check in this case is $3^6 = 729$.

Case 3: $\boxed{\mathbf{N}_{1,2}}$ We have

$+$	1	2	b
1	2	1	e
2	1	2	g
b	e	g	h

$\times$	1	2	b
1	1	2	b
2	2	2	h
b	b	h	k

$\uparrow$	1	2	b
1	1	1	1
2	2	2	m
b	b	k	o

The total number of $\mathcal{L}$-algebras to check in this case is also $3^6 = 729$.

Case 4: $\boxed{\mathbf{N}_{2,2}}$ The only HSI-algebra is $\mathbf{N}_{2,2}$.

Case 5: $\boxed{\mathbf{N}_{3,1}}$ The only HSI-algebra is $\mathbf{N}_{3,1}$.

At this point it is quite easy to write a program that will find the 3-element HSI-algebras. If we want to find them up to isomorphism then observe that all the algebras in Cases 2–5 are rigid, i.e., they admit only the trivial automorphism since the integers of these algebras will be fixed. Thus the HSI-algebras in Cases 2–5 appear, up to isomorphism, only once. And in Case 1 a given algebra can be isomorphic to at most one other, namely interchange the a and b elements. Thus one can rapidly determine that there are exactly 44 3-element HSI-algebras (which we give in an appendix).

We can also list all 4- and 5-element HSI-algebras in a reasonable amount of time (we didn't try finding the isomorphism types). But for six elements it seems we need about six months of CPU time on our 12 MIPS machine to exhaust the possibilities. (We ran our program on six elements for a few days to get this estimate). And for seven elements an exhaustive computer listing seems hopeless.

7. The Wilkie Identity

Definition 7.1. Let

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

In 1980 Wilkie showed that the following identity, which we call $W(x, y)$, is true of $\mathbf{N}$ but cannot be derived from HSI (where $P = P(x)$, etc):

$$(P^x + Q^x)^y \cdot (R^y + S^y)^x \approx (P^y + Q^y)^x \cdot (R^x + S^x)^y .$$

Proposition 7.2. $\mathbf{N}$ *satisfies* $W(x, y)$.

Proof. Let us define the operation $\square$ on N by

$$m \square n = \begin{cases} m - n \text{ if } m > n \\ 1 \text{ otherwise,} \end{cases}$$

and let $\mathbf{N}_\square$ be the expansion $\langle N, +, \times, \uparrow, \square, 1\rangle$ of $\mathbf{N}$. Then, with $F(x) = (1 + x^2)\square x$ we have the following holding in $\mathbf{N}_\square$:

$$\begin{aligned} R &\approx P \cdot F \\ S &\approx Q \cdot F. \end{aligned}$$

Thus $\mathbf{N}_\square$ satisfies

$$\begin{aligned} (P^x + Q^x)^y \cdot (R^y + S^y)^x &\approx F^{x \cdot y} (P^x + Q^x)^y \cdot (P^y + Q^y)^x \\ &\approx (R^x + S^x)^y \cdot (P^y + Q^y)^x \\ &\approx (P^y + Q^y)^x \cdot (R^x + S^x)^y . \end{aligned}$$

As $\mathbf{N}_\square$ satisfies $W(x, y)$, so does $\mathbf{N}$. □

$W(x, y)$ is the simplest identity known which holds on $\mathbf{N}$, but cannot be derived from HSI. As we mentioned in the introduction, Wilkie used a syntactic proof; later, in 1985, Gurevič [4] published a new proof by constructing a 59-element algebra satisfying HSIbut not $W(x, y)$.

Definition 7.3. A *Gurevič-algebra* (or *G-algebra*) is a model of HSI which does not satisfy Wilkie's identity $W(x, y)$.

In Gurevič [6], p. 30, we have the remark:

> 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.

We will show that the smallest G-algebra has at least 7 elements (see §8). A 28-element G-algebra was found by Burris in 1988, and then a 16-element example in 1990. Recently Simon Lee found the smallest such algebra known, with 15 elements, which is given in §9.

8. A Lower Bound

We will show that any HSI -algebra which does not satisfy $W(x, y)$ has at least seven elements. To achieve this we list several properties of elements a, b in an HSI-algebra $\mathbf{A}$ which guarantee $W(a, b)$ holds in $\mathbf{A}$. Avoiding this list of properties will force the size of the algebra to be at least seven.

When we write P, Q, R, respectively S without an argument then we will mean $P(x), Q(x), R(x)$, respectively $S(x)$.

Lemma 8.1.

$$\text{HSI} \vdash \forall x\, W(x, x).$$

Proof. This is obvious since both sides of $W(x, x)$ are the same. □

Lemma 8.2. *For n an integer, i.e., $n = \underbrace{1 + \cdots + 1}_{n}$, we have*

$$\text{HSI} \vdash \forall y\, W(n, y).$$

Proof. Let $m = 1 - n + n^2$, a positive integer. Then

$$\begin{aligned} \text{HSI} &\vdash P(n) \cdot m \approx R(n) \\ \text{HSI} &\vdash Q(n) \cdot m \approx S(n). \end{aligned}$$

From HSI one can carry out the derivations

$$\begin{aligned} (P(n)^n + Q(n)^n)^y \cdot (R(n)^y + S(n)^y)^n &\approx m^{n \cdot y}\, (P(n)^n + Q(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (R(n)^n + S(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (P(n)^y + Q(n)^y)^n \cdot (R(n)^n + S(n)^n)^y \,. \end{aligned}$$

Consequently

$$\text{HSI} \vdash W(n, y).$$

□

Lemma 8.3.

$$\text{HSI} \vdash P \cdot S \approx Q \cdot R.$$

Proof. This actually follows from $\overline{\text{HSI}}$; both sides are equal to $1 + x + x^2 + x^3 + x^4 + x^5$. □

Lemma 8.4. *For n an integer we have*

$$\text{HSI} \vdash \forall x\, W(x, n).$$

Proof. Using HSI we can carry out the derivations:

$$\begin{aligned}(P^x + Q^x)^n \cdot (R^n + S^n)^x &\approx \left(\sum_{i=0}^{n} \binom{n}{i} \cdot (P^x)^i \cdot (Q^x)^{n-i}\right) \cdot (R^n + S^n)^x \\ &\approx \sum_{i=0}^{n} \binom{n}{i} \cdot \left(P^i \cdot Q^{n-i} \cdot R^n + P^i \cdot Q^{n-i} \cdot S^n\right)^x;\end{aligned}$$

and

$$\begin{aligned}(P^n + Q^n)^x \cdot (R^x + S^x)^n &\approx (P^n + Q^n)^x \cdot \left(\sum_{i=0}^{n} \binom{n}{i} \cdot (R^x)^i \cdot (S^x)^{n-i}\right) \\ &\approx \sum_{i=0}^{n} \binom{n}{i} \cdot \left(P^n \cdot R^i \cdot S^{n-i} + Q^n \cdot R^i \cdot S^{n-i}\right)^x.\end{aligned}$$

Now, using 8.3, we can derive from HSI, for $0 \le i \le n$,

$$\begin{aligned}P^i \cdot Q^{n-i} \cdot R^n &\approx P^n \cdot R^i \cdot S^{n-i}; \\ P^i \cdot Q^{n-i} \cdot S^n &\approx Q^n \cdot R^i \cdot S^{n-i}.\end{aligned}$$

Thus we have a derivation from HSI of

$$(P^x + Q^x)^n \cdot (R^n + S^n)^x \approx (P^n + Q^n)^x \cdot (R^x + S^x)^n,$$

which is $W(x, n)$. □

Corollary 8.5. *If* $\mathbf{A}$ *is a G-algebra and $a, b \in A$ are such that $W(a, b)$ does not hold then a, b are distinct non-integers in A.*

Proof. Combine 8.1, 8.2, and 8.4. □

Definition 8.6. The notation $u|v$ is short for $\exists w\, (v \approx u \cdot w)$.

In the following a claim $\text{HSI} \vdash \Sigma \to W(x, y)$ means

$$\text{HSI} \vdash \forall x\, \forall y\, [\Sigma \to W(x, y)].$$

Lemma 8.7 (Lee)**.**

$$\text{HSI} \vdash x|y \to W(x, y).$$

Proof. The following is a derivation from HSI, where the fifth step follows from 8.3. Let $y \approx u \cdot x$. Then

$$
\begin{aligned}
&(P^x + Q^x)^y \cdot (R^y + S^y)^x \\
&\quad \approx (P^x + Q^x)^{u \cdot x} \cdot (R^{u \cdot x} + S^{u \cdot x})^x \\
&\quad \approx [(P^x + Q^x)^u \cdot (R^{u \cdot x} + S^{u \cdot x})]^x \\
&\quad \approx [((P \cdot R)^x + (Q \cdot R)^x)^u + ((P \cdot S)^x + (Q \cdot S)^x)^u]^x \\
&\quad \approx [((P \cdot R)^x + (P \cdot S)^x)^u + ((Q \cdot R)^x + (Q \cdot S)^x)^u]^x \\
&\quad \approx [P^{ux} (R^x + S^x)^u + Q^{ux} (R^x + S^x)^u]^x \\
&\quad \approx [(P^{ux} + Q^{ux}) \cdot (R^x + S^x)^u]^x \\
&\quad \approx (P^y + Q^y)^x \cdot (R^x + S^x)^{ux} \\
&\quad \approx (P^y + Q^y)^x \cdot (R^x + S^x)^y .
\end{aligned}
$$

□

Now we are going to introduce one of our fundamental techniques for establishing conditions under which $W(a, b)$ holds. But first some definitions.

Definition 8.8. The Push-Pull Rules
Let Σ be a set of $\mathcal{L}$-identities. We formulate rewrite rules on 5-tuples of $\overline{\text{HSI}}$-terms as follows (the first two are thh *pull rules*, the second two the *push rules*),

$$(t,\ \bar{t} \cdot p,\ \bar{t} \cdot q,\ r,\ s) \ \longrightarrow_\Sigma\ (t \cdot \bar{t},\ p,\ q,\ r,\ s) \tag{24}$$

$$(t,\ p,\ q,\ \bar{t} \cdot r,\ \bar{t} \cdot s) \ \longrightarrow_\Sigma\ (t \cdot \bar{t},\ p,\ q,\ r,\ s) \tag{25}$$

$$(t \cdot \bar{t},\ p,\ q,\ r,\ s) \ \longrightarrow_\Sigma\ (t,\ \bar{t} \cdot p,\ \bar{t} \cdot q,\ r,\ s) \tag{26}$$

$$(t \cdot \bar{t},\ p,\ q,\ r,\ s) \ \longrightarrow_\Sigma\ (t,\ p,\ q,\ \bar{t} \cdot r,\ \bar{t} \cdot s); \tag{27}$$

and if $\Sigma \to t \approx t' \wedge p \approx p' \wedge \ldots \wedge s \approx s'$ is a consequence of $\overline{\text{HSI}}$ then

$$(t,\ p,\ q,\ r,\ s) \ \longrightarrow_\Sigma\ (t',\ p',\ q',\ r',\ s'). \tag{28}$$

Definition 8.9. Let $\longrightarrow_\Sigma^\star$ be the reflexive and transitive closure of $\longrightarrow_\Sigma$.

Lemma 8.10. *Suppose* $(t,\ p,\ q,\ r,\ s) \longrightarrow_\Sigma^\star (t',\ p',\ q',\ r',\ s')$. *Then*

$$(t,\ q,\ p,\ r,\ s) \ \longrightarrow_\Sigma^\star\ (t',\ q',\ p',\ r',\ s') \tag{29}$$

$$(t,\ p,\ q,\ s,\ r) \ \longrightarrow_\Sigma^\star\ (t',\ p',\ q',\ s',\ r') \tag{30}$$

$$(t,\ r,\ s,\ p,\ q) \ \longrightarrow_\Sigma^\star\ (t',\ r',\ s',\ p',\ q'). \tag{31}$$

Proof. These are an easy consequence of 8.8. □

Now let us look at the reasons for introducing the push-pull rules.

Lemma 8.11. *If*

$$(1,\ P,\ Q,\ R,\ S) \longrightarrow_{\Sigma}^{\star} (t,\ p,\ q,\ r,\ s)$$

then

$$\text{HSI} \vdash \Sigma \to t \cdot p \cdot s \approx t \cdot q \cdot r; \tag{32}$$

and

$$\begin{aligned} \text{HSI} \vdash \Sigma \to & \left(P^x + Q^x\right)^y \cdot \left(R^y + S^y\right)^x \\ & \approx t^{x \cdot y} \left(p^x + q^x\right)^y \cdot \left(r^y + s^y\right)^x . \end{aligned} \tag{33}$$

Proof. These are straight forward induction arguments on the length of the $\longrightarrow_{\Sigma}^{\star}$ derivation of $(t,\ p,\ q,\ r,\ s)$; the first uses 8.3 for the ground step. □

Lemma 8.12. *If*

$$(1,\ P,\ Q,\ R,\ S) \longrightarrow_{\Sigma}^{\star} (t,\ p,\ q,\ r,\ s)$$

and one of the following hold:

$$\{p, q\} = \{r, s\} \tag{34}$$

$$p = q \tag{35}$$

$$r = s \tag{36}$$

then

$$\text{HSI} \vdash \Sigma \to W(x, y).$$

Proof. **Case 1:** $\boxed{\{p, q\} = \{r, s\}}$**:** Then by (31) we have

$$(1,\ R,\ S,\ P,\ Q) \longrightarrow_{\Sigma}^{\star} (t,\ r,\ s,\ p,\ q);$$

and then from (33) we have

$$\text{HSI} \ \vdash \Sigma \to W(x, y)$$

since $\{p, q\} = \{r, s\}$ guarantees

$$\text{HSI} \ \vdash \ t^{x \cdot y} \left(p^x + q^x\right)^y \cdot \left(r^y + s^y\right)^x \ \approx \ t^{x \cdot y} \left(p^y + q^y\right)^x \cdot \left(r^x + s^x\right)^y .$$

Case 2: $\boxed{p \approx q}$**:** In this case we use the push-pull rules and 8.3 to obtain:

$$\begin{aligned} (t,\ p,\ q,\ r,\ s) & \longrightarrow_{\Sigma}^{\star} (t,\ p,\ p,\ r,\ s) \\ & \longrightarrow_{\Sigma}^{\star} (t \cdot p,\ 1,\ 1,\ r,\ s) \\ & \longrightarrow_{\Sigma}^{\star} (1,\ 1,\ 1,\ t \cdot p \cdot r,\ t \cdot p \cdot s) \\ & \longrightarrow_{\Sigma}^{\star} (1,\ 1,\ 1,\ t \cdot q \cdot r,\ t \cdot p \cdot s) \\ & \longrightarrow_{\Sigma}^{\star} (1,\ 1,\ 1,\ t \cdot q \cdot r,\ t \cdot q \cdot r) \\ & \longrightarrow_{\Sigma}^{\star} (t \cdot q \cdot r,\ 1,\ 1,\ 1,\ 1). \end{aligned}$$

But now we have

$$(1,\ P,\ Q,\ R,\ S) \longrightarrow^{\star}_{\Sigma} (t \cdot q \cdot r,\ 1,\ 1,\ 1,\ 1),$$

so we can apply the results of Case 1.

Case 3: $\boxed{r \approx s}$**:** This is handled like Case 2.

This finishes the proof. □

Lemma 8.13 (Lee)**.** *If* Σ *is one of the following conditions*

(37) $P|Q$

(38) $Q|P$

(39) $R|S$

(40) $S|R$

(41) $u \cdot P \approx R$ *and* $u \cdot Q \approx S$

(42) $P \approx u \cdot R$ *and* $Q \approx u \cdot S$

then one has

$$\text{HSI} \vdash \Sigma \rightarrow W(x,y).$$

Proof. Suppose (37) holds. Let Σ be $u \cdot P \approx Q$. Then from the push-pull rules and 8.3

$$\begin{aligned}
(1,\ P,\ Q,\ R,\ S) &\longrightarrow^{\star}_{\Sigma} (1,\ P,\ u \cdot P,\ R,\ S)\\
&\longrightarrow^{\star}_{\Sigma} (P,\ 1,\ u,\ R,\ S)\\
&\longrightarrow^{\star}_{\Sigma} (1,\ 1,\ u,\ P \cdot R,\ P \cdot S)\\
&\longrightarrow^{\star}_{\Sigma} (1,\ 1,\ u,\ P \cdot R,\ Q \cdot R)\\
&\longrightarrow^{\star}_{\Sigma} (R,\ 1,\ u,\ P,\ Q)\\
&\longrightarrow^{\star}_{\Sigma} (R,\ 1,\ u,\ P,\ u \cdot P)\\
&\longrightarrow^{\star}_{\Sigma} (R \cdot P,\ 1,\ u,\ 1,\ u),
\end{aligned}$$

so, by (34) of 8.12, $W(x,y)$ is a consequence of Σ, given HSI. The proofs of the next three cases are similar.

For the fifth case let Σ be $\{u \cdot P \approx R, u \cdot Q \approx S\}$. Then

$$\begin{aligned}
(1,\ P,\ Q,\ R,\ S) &\longrightarrow^{\star}_{\Sigma} (1,\ P,\ Q,\ u \cdot P,\ u \cdot Q)\\
&\longrightarrow^{\star}_{\Sigma} (u,\ P,\ Q,\ P,\ Q),
\end{aligned}$$

so, again by (34) of 8.12, $W(x,y)$ is a consequence of Σ, given HSI.

The sixth case is similar to the fifth case. □

Now we are ready to start establishing some lower bounds on the size of a G-algebra.

Proposition 8.14. *Let* **A** *be an* HSI*-algebra. If there is only one integer (i.e.,* $2 \approx 1$ *holds in* **A***) then* **A** *satisfies* $W(x,y)$*.*

Proof. Let Σ be the condition $1 \approx 2$. Then assuming HSI and Σ one has $Q(x) \approx 1+x+x^2 \approx 1+x+x \approx 1+2x \approx 1+x \approx P(x)$, so by (37) of 8.13 we see that HSI $\vdash \Sigma \to W(x,y)$. Thus $\mathbf{A}$ satisfies $W(x,y)$. □

Proposition 8.15 (Davidson)**.** *Let* $\mathbf{A}$ *be an* HSI*-algebra. If there are exactly two integers in* $\mathbf{A}$ *then* $\mathbf{A}$ *satisfies* $W(x,y)$*.*

Proof. We break this up into the cases where Σ is $3 \approx 1$; and $3 \approx 2$.

Case 1: $\boxed{3 \approx 1}$ Then we can derive $1+x \approx (1+x)^3 \approx 1+3x+3x^2+x^3 \approx 1+2x+x^2$, and from this we have $P(x)\cdot Q(x) \approx (1+x)(1+x+x^2) \approx 1+2x+2x^2+x^3 \approx 1+3x+2x^2 \approx (1+2x+x^2)+(x+x^2) \approx (1+x)+(x+x^2) \approx 1+2x+x^2 \approx 1+x \approx P(x)$. By (38) of 8.13 we have $\mathbf{A}$ satisfies $W(x,y)$.

Case 2: $\boxed{3 \approx 2}$ We can proceed as follows: $R(x)^2 \approx (1+x^3)^2 \approx (1+x^2)^2 \approx 1+2x^2+x^4 \approx 1+2x^2+x^2 \approx 1+2x^2 \approx 1+x^2+x^2 \approx 1+x^2+x^4 \approx S(x)$. By (39) of 8.13 we have $\mathbf{A}$ satisfies $W(x,y)$.

□

Corollary 8.16. *If* $\mathbf{A}$ *is a G-algebra and* a,b *are such that* $W(a,b)$ *does not hold then the elements* $1,2,3,a,b$ *are distinct.*

Proof. From the last two results we see that there must be at least 3 integers of $\mathbf{A}$, and we proved in 8.5 that a,b must be two non-integers. □

Now we look at some conditions Σ which do not restrict the integers of the models, and lead to HSI $\vdash \Sigma \to W(x,y)$. These conditions will not be enough to force the size of the G-algebras above 5, so later we will turn to conditions which make assumptions about the integers.

Lemma 8.17.

(43) HSI $\vdash\ x \approx k+x \ \to\ W(x,y)$ *for* $k \geq 1$*;*

(44) HSI $\vdash\ 1 \approx k+x \ \to\ W(x,y)$ *for* $k \geq 0$*.*

Proof. For (43) first note that we have, for $n \in N$, $x^n \approx (k+x)x^{n-1} \approx kx^{n-1}+x^n$; and then $kx^n \approx x^n+(k-1)x^n \approx (kx^{n-1}+x^n)+(k-1)x^n \approx kx^{n-1}+kx^n$. Thus $R(x) \approx 1+x^3 \approx 1+(kx^2+x^3) \approx 1+(kx+kx^2)+x^3 \approx (1+x)(1+(k-1)x+x^2) \approx P(x)\cdot(1+(k-1)x+x^2)$;
$S(x) \approx 1+x^2+x^4 \approx 1+(kx+x^2)+(kx^3+x^4) \approx 1+kx+x^2+(kx^2+kx^3)+x^4 \approx 1+kx+(1+k)x^2+kx^3+x^4 \approx (1+x+x^2)(1+(k-1)x+x^2) \approx Q(x)\cdot(1+(k-1)x+x^2)$.
$W(x,y)$ follows by (41) of 8.13.

Next for (44) we use $R(x) \approx 1+x^3 \approx (k+x)+x^3 \approx k+(k+x)x+x^3 \approx k+kx+x^2+x^3 \approx (1+x)(k+x^2) \approx P(x)\cdot(k+x^2)$;

$S(x) \approx 1+x^2+x^4 \approx (k+x)+(k+x)x^2+x^4 \approx k+x+kx^2+x^3+x^4 \approx k+(k+x)x+kx^2+x^3+x^4 \approx k+kx+(k+1)x^2+x^3+x^4 \approx (1+x+x^2)(k+x^2) \approx Q(x)\cdot(k+x^2)$.
Again $W(x,y)$ follows by (41) of 8.13. □

Lemma 8.18.

$$\text{(45)} \qquad \text{HSI} \ \vdash \ x^2 \approx k+x \ \to \ W(x,y) \qquad \textit{for } k \geq 0;$$

$$\text{(46)} \qquad \text{HSI} \ \vdash \ x \approx k+x^2 \to W(x,y) \qquad \textit{for } k \geq 0.$$

Proof. For (45) $Q(x) \approx 1+x+x^2 \approx (1+k)+2x$;
$R(x) \approx 1+x^3 \approx 1+x\cdot(k+x) \approx 1+kx+x^2 \approx 1+kx+(k+x) \approx (1+k)+(1+k)x \approx (1+k)\cdot(1+x) \approx (1+k)\cdot P(x)$;
$S(x) \approx 1+x^2+x^4 \approx 1+x^2+x^2\cdot(k+x) \approx 1+(1+k)\cdot x^2+x^3 \approx 1+(1+k)\cdot x^2+x\cdot(k+x) \approx 1+kx+(2+k)x^2 \approx 1+kx+(2+k)\cdot(k+x) \approx (1+2k+k^2)+(2+2k)x \approx (1+k)\cdot[(1+k)+2x] \approx (1+k)\cdot Q(x)$.
$W(x,y)$ follows by (41) of 8.13.

Next for (46) we have the case $k=0$ covered by (45). So assume $k \geq 1$.
$R(x) \approx 1+x^3 \approx 1+x^2\cdot(k+x^2) \approx 1+kx^2+x^4 \approx 1+x^2+(k-1)\cdot x^2+x^4 \approx 1+(k+x^2)x+(k-1)\cdot x^2+x^4 \approx 1+kx+(k-1)\cdot x^2+x^3+x^4 \approx (1+(k-1)x+x^3)\cdot(1+x) \approx (1+(k-1)x+x^3)\cdot P(x)$;
$S(x) \approx 1+x^2+x^4 \approx 1+x\cdot(k+x^2)+x^4 \approx 1+kx+x^3+x^4 \approx 1+kx+x^2(k+x^2)+x^4 \approx 1+kx+kx^2+2x^4 \approx 1+kx+kx^2+x^4+x^4 \approx 1+kx+kx^2+x^3(k+x^2)+x^4 \approx 1+kx+kx^2+kx^3+x^4+x^5 \approx (1+(k-1)x+x^3)\cdot(1+x+x^2) \approx (1+(k-1)x+x^3)\cdot Q(x)$.
$W(x,y)$ follows by (41) of 8.13. □

Lemma 8.19.

$$\text{(47)} \qquad \text{HSI} \ \vdash \ x^2 \approx kx \to W(x,y) \qquad \textit{for } k \geq 1.$$

Proof. $R(x) \approx 1+x^3 \approx 1+kx^2 \approx 1+kx+(k-1)x^2 \approx (1+(k-1)x)\cdot(1+x) \approx (1+(k-1)x)\cdot P(x)$;
$S(x) \approx 1+x^2+x^4 \approx 1+kx+kx^3 \approx 1+kx+kx^2+(k-1)x^3 \approx (1+(k-1)x)\cdot(1+x+x^2) \approx (1+(k-1)x)\cdot Q(x)$.
$W(x,y)$ follows by (41) of 8.13. □

Lemma 8.20. *If Σ is any of the conditions $p \approx q$, where p marks a row, q marks a column, in the following array, and there is a $\bullet$ with coordinates (p,q), then* HSI $\vdash \Sigma \to W(x,y)$. *If there is a □ with coordinates (p,q) then we know* HSI $\nvdash \Sigma \to W(x,y)$. *A ? means we draw no conclusion.*

	1	2	3	x	$1+x$	$2+x$	$2x$	x^2	$1+x^2$	x^3
1	$\square$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$
2	$\bullet$	$\square$	$\bullet$	$\bullet$	$\square$	?	?	?	?	?
3	$\bullet$	$\bullet$	$\square$	$\bullet$	?	?	?	?	?	?
x	$\bullet$	$\bullet$	$\bullet$	$\square$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$	?
$1+x$	$\bullet$	$\square$	?	$\bullet$	$\square$	$\bullet$	?	$\bullet$	?	$\bullet$
$2+x$	$\bullet$	?	?	$\bullet$	$\bullet$	$\square$	?	?	?	?
$2x$	$\bullet$	?	?	$\bullet$	?	?	$\square$	$\bullet$	?	?
x^2	$\bullet$	?	?	$\bullet$	$\bullet$	?	$\bullet$	$\square$	$\bullet$	$\square$
$1+x^2$	$\bullet$	?	?	$\bullet$	?	?	?	$\bullet$	$\square$	?
x^3	$\bullet$	?	?	?	$\bullet$	?	?	$\square$	?	$\square$

Proof. The results relating $1, 2, 3$, and x we know from 8.16. For the remaining cases we show how to derive $W(x, y)$.

Case $\boxed{1 \approx 1 + x}$**:** $W(x, y)$ follows by (44) of 8.17.

Case $\boxed{1 \approx 2 + x}$**:** $W(x, y)$ follows by (44) of 8.17.

Case $\boxed{1 \approx 2x}$**:** Then $x|1$. $W(x, y)$ follows by 8.7.

Case $\boxed{1 \approx x^2}$**:** Then $x|1$. $W(x, y)$ follows by 8.7.

Case $\boxed{1 \approx 1 + x^2}$**:** $P(x) \approx 1 + x \approx 1 + x^2 + x \approx Q(x)$. $W(x, y)$ follows by (37) of 8.13.

Case $\boxed{1 \approx x^3}$**:** Then $x|1$. $W(x, y)$ follows by 8.7.

Case $\boxed{x \approx 1 + x}$**:** $W(x, y)$ follows by (43) of 8.17.

Case $\boxed{x \approx 2 + x}$**:** $W(x, y)$ follows by (43) of 8.17.

Case $\boxed{x \approx 2x}$**:** $Q(x) \approx 1 + x + x^2 Q(x) \approx 1 + 2x + x^2 \approx (1+x)^2 \approx P(x)^2$. $W(x, y)$ follows by (37) of 8.13.

Case $\boxed{x \approx x^2}$**:** $W(x, y)$ follows by 8.18.

Case $\boxed{x \approx 1 + x^2}$**:** $W(x, y)$ follows by (46) of 8.18.

Case $\boxed{1 + x \approx 2 + x}$**:** $Q(x) \approx 1 + x + x^2 \approx 1 + x(1 + x) \approx 1 + x(2 + x) \approx 1 + 2x + x^2 \approx (1 + x)^2 \approx P(x)^2$. $W(x, y)$ follows by (37) of 8.13.

Case $\boxed{1+x \approx x^2}$**:** $W(x,y)$ follows by (45) of 8.18.

Case $\boxed{1+x \approx x^3}$**:** $Q(x) \approx 1+x+x^2 \approx x^3+x^2 \approx x^2\cdot(1+x) \approx x^2\cdot P(x)$. $W(x,y)$ follows by (37) of 8.13.

Case $\boxed{2x \approx x^2}$**:** $W(x,y)$ follows by (47) of 8.19.

Case $\boxed{x^2 \approx 1+x^2}$**:** $Q(x) \approx 1+x+x^2 \approx x+x^2 \approx x(1+x) \approx x\cdot P(x)$. $W(x,y)$ follows by (37) of 8.13.

□

To establish 7 as a lower bound for the size of G-algebras *it suffices to consider algebras with 3 or 4 integers* (since fewer integers guarantee $W(x,y)$ holds; and since any G-algebra has at least two elements which are not integers). First we turn to the case that we have exactly 3 integers, in which case we have $4=3$ or $4=2$.

8.1. **Three Integers, with** $4=3$**.** First let it be mentioned that G-algebras do exist in this case — the smallest such example we have found has 17 elements.

Throughout this subsection we assume $\mathbf{A}$ is a G-algebra with exactly 3 integers, $4=3$, and $\mathbf{A} \not\models W(a,b)$,

Lemma 8.21. *The elements* $1,2,3,a,1+a,a^2$ *are distinct. Thus* A *has size at least 6.*

Proof. We claim that if you identify any two of the above six elements then $W(a,b)$ holds, a contradiction. Four cases are presented below — all others are covered by 8.20.

Case $\boxed{1+a=2}$**:** $Q(a) = 1+a+a^2 = 1+a(1+a) = 1+a\cdot 2 = 1+a+a = 2+a = 1+1+a = 1+2 = 3 = 4 = 2\cdot 2 = 2\cdot(1+a) = 2\cdot P(a)$. $W(a,b)$ follows by (37) of 8.13.

Case $\boxed{1+a=3}$**:** $Q(a) = 1+a+a^2 = 1+a(1+a) = 1+a\cdot 3 = 1+a+a+a = 3+a+a = 2+1+a+a = 2+3+a = 4+a = 3+1+a = 3+3 = 4 = 3 = 1+a = P(a)$. $W(a,b)$ follows by (37) of 8.13.

Case $\boxed{a^2=2}$**:** $S(a) = 1+a^2+a^4 = 1+2+4 = 1+4 = 1+a^4 = 1+a^3 = R(a)$. $W(a,b)$ follows by (39) of 8.13.

Case $\boxed{a^2=3}$**:** $S(a) = 1+a^2+a^4 = 1+3+9 = 1+9 = 1+a^4 = 1+a^3 = R(a)$. $W(a,b)$ follows by (39) of 8.13.

□

Lemma 8.22. *The set* $U = \{1,2,3,a,1+a,a^2\}$ *is not a subuniverse of* $\overline{\mathbf{A}}$. *Thus* A *has at least seven elements in it.*

Proof. Consider the element a^3. We know a^3 is not 1 or $1+a$ by 8.20. The following arguments show that U is not closed under $+, \times$.

Case $\boxed{a^3 = 2}$**:** $2 = a^3 = a^6 = (a^3)^2 = 2^2 = 4 = 3$. This contradicts our assumption that we have three integers.

Case $\boxed{a^3 = 3}$**:** $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 4 + a^2 = 7 + a^2 = 1 + a^2 + 2a^3 = 1 + a^2 + a^3 + a^3 = 1 + a^2 + a^3 + a^5 = (1+a^3)(1+a^2) = R(a) \cdot (1+a^2)$. $W(a,b)$ follows by (39) of 8.13.

Case $\boxed{a^3 = a}$**:** $P(a) = 1+a = 1+a^3 = R(a); Q(a) = 1+a+a^2 = 1+a^2+a^3 = 1+a^2+a^4 = S(a)$. $W(a,b)$ follows by (41) of 8.13.

Thus if a^3 is in U then it must be the element a^2.

Case $\boxed{a^3 = a^2}$**:** We will now show that this implies $1 + a^2$ is not in U. First we see that $1 + a^2$ is distinct from $1, a, a^2$ by 8.20.

Subcase $\boxed{1 + a^2 = 2}$ $R(a) = 1 + a^3 = 1 + a^2 = 2; S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 1 + 2a^2 = 1 + a^2 + a^2 = 2 + a^2 = 1 + (1 + a^2) = 3 = 4 = 2^2 = R(a)^2$. $W(a,b)$ follows by (39) of 8.13.

Subcase $\boxed{1 + a^2 = 3}$ $R(a) = 1 + a^3 = 1 + a^2 = 3; S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 1 + 2a^2 = 1 + a^2 + a^2 = 3 + a^2 = 5 = 3 = R(a)$. $W(a,b)$ follows by (39) of 8.13.

Subcase $\boxed{1 + a^2 = 1 + a}$ $P(a) = 1+a = 1+a^2 = 1+a^3 = R(a); Q(a) = 1+a+a^2 = 1+a^2+a^2 = 1+a^2+a^3 = 1+a^2+a^4 = S(a)$. $W(a,b)$ follows by (41) of 8.13.

□

8.2. **Three Integers, with** $4 = 2$**.** In this case we do not know if there is an a G-algebra.

Throughout this subsection we assume $\mathbf{A}$ is a G-algebra with exactly 3 integers, $4 = 2$, and $\mathbf{A} \not\models W(a,b)$.

Lemma 8.23. *The elements* $1, 2, 3, a, 1 + a$ *are distinct.*

Proof. In view of 8.20 we only need to check that $1+a$ is distinct from 2 and 3.

Case $\boxed{2 = 1 + a}$**:** $Q(a) = 1 + a + a^2 = 1 + a \cdot (1 + a) = 1 + 2 \cdot a = 1 + a + a = 2 + a = 3; P(a) = 1 + a = 2 = 2 \cdot 3 = 2 \cdot Q(a)$. $W(a,b)$ follows by (38) of 8.13.

Case $\boxed{3 = 1 + a}$**:** $Q(a) = 1 + a + a^2 = 1 + a(1 + a) = 1 + 3 \cdot a = 3 + 2 \cdot a = 7 = 3; P(a) = 1 + a = 3 = Q(a)$. $W(a,b)$ follows by (37) of 8.13.

□

Lemma 8.24. *$a^2 \neq 2+a$, and either a^2 or $2+a$ is not in $\{1, 2, 3, a, 1+a\}$.*

Proof. $a^2 \neq 2 + a$ by 8.20. If $\{a^2, 2 + a\} \subseteq \{1, 2, 3, a, 1 + a\}$ then from 8.20 a^2 is either 2 or 3; and likewise $2 + a$ is either 2 or 3. But then we can use (45) of Proposition 8.18 to show $W(a, b)$ holds. □

Thus we need only show that adding a^2 or $2 + a$ to $\{1, 2, 3, a, 1 + a\}$ does not give a subuniverse of $\overline{\mathbf{A}}$ to conclude that A has at least seven elements.

Lemma 8.25. *The set $U = \{1, 2, 3, a, 1+a, 2+a\}$ is not a subuniverse of $\overline{\mathbf{A}}$.*

Proof. Suppose U is a subuniverse of $\mathbf{A}$. As we observed above, a^2 could only be 2 or 3. Under either of these assumptions we will show that $3 + a \notin U$. First observe that $3 + a \notin \{1, a\}$ by 8.17. Also $3 + a \notin \{2, 3\}$ by (45) of 8.18 (since $a^2 \in \{2, 3\}$). So it only remains to show that $3 + a \notin \{1 + a, 2 + a\}$.

Case $\boxed{2 = a^2}$**:**

Subcase $\boxed{3 + a = 1 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 2 = 3 + a = 1 + a = P(a)$. $W(a, b)$ follows by (37) of 8.13.

Subcase $\boxed{3 + a = 2 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 2 = 3 + a = 2 + a = a^2 + a = a(1 + a) = a \cdot P(a)$. $W(a, b)$ follows by (37) of 8.13.

Case $\boxed{3 = a^2}$**:**

Subcase $\boxed{3 + a = 1 + a}$ $Q(a) = 1 + a + a^2 = 4 + a = 2+a$; $P(a) = 1+a = 3+a = 7+a = 4+a+a^2 = 4+a(1+a) = 4 + a(3 + a) = 4 + 3a + a^2 = 2 + 3a + a^2 = (2 + a) \cdot (1 + a) = Q(a) \cdot (1 + a)$. $W(a, b)$ follows by (38) of 8.13.

Subcase $\boxed{3 + a = 2 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 3 = 4 + a = 2 + a = 3 + a = a^2 + a = a(1 + a) = a \cdot P(a)$. $W(a, b)$ follows by (37) of 8.13.

Thus the assumption that U is a subuniverse of $\overline{\mathbf{A}}$ leads, through several cases, to a contradiction. □

Lemma 8.26. *The set $U = \{1, 2, 3, a, 1 + a, a^2\}$ is not a subuniverse of $\overline{\mathbf{A}}$.*

Proof. Assume that U is a subuniverse of $\overline{\mathbf{A}}$. We will proceed to show $W(a, b)$ holds, which gives a contradiction.

First consider the element $2a$. From 8.20 we know that $2a \notin \{1, a, a^2\}$. In the next two cases we show that $2a \in \{3, 1 + a\}$ leads to $W(a, b)$.

Case $\boxed{2a = 3}$**:** $3 = 2a = 4a = 2 \cdot 2a = 2 \cdot 3 = 2$. This contradicts our assumption that we have three integers.

Case $\boxed{2a = 1 + a}$**:** $P(a) = 1 + a = 2a$;
$Q(a) = 1 + a + a^2 = 2a + a^2 = a + a(1 + a) = a + a(2a) = a(1 + a) + a^2 = a(2a) + a^2 = 3a^2$;
$S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + a \cdot 2a = 1 + a \cdot (1 + a) = 1 + a + a^2 = 2a + a^2 = a + a(1 + a) = a + a(2a) = a(1 + a) + a^2 = a(2a) + a^2 = 3a^2$.

With this information about $P(a)$, $Q(a)$ and $S(a)$ we can carry out a push-pull argument to show $W(a, b)$ holds:

$$\begin{aligned}
(1, P(a), Q(a), R(a), S(a)) &\rightarrow (1, 2a, 3a^2, 1 + a^3, 3a^2) \\
&\rightarrow (a, 2, 3a, 1 + a^3, 3a^2) \\
&\rightarrow (1, 2, 3a, a + a^4, 3a^3) \\
&\rightarrow (1, 2, 3a, a + a^2, 3a^3) \\
&\rightarrow (1, 2, 3a, 2a^2, 3a^3) \\
&\rightarrow (a, 2, 3a, 2a, 3a^2) \\
&\rightarrow (1, 2a, 3a^2, 2a, 3a^2).
\end{aligned}$$

$W(a, b)$ follows by (34) of 8.12.

Thus U is a subuniverse of $\overline{\mathbf{A}}$ implies $\boxed{2a = 2.}$

Next we determine the possible values of $2 + a$. We see from 8.17 that $2 + a \notin \{1, a, 1 + a\}$, and $2 + a \neq a^2$ by 8.18. The next case shows that $2 + a \neq 2$.

Case $\boxed{2 + a = 2}$**:** $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + (2 + a)a^2 = 1 + 2a^2 + a^3 = 1 + (2 + a)a^2 + a^3 = 1 + 2a^2 + 2a^3 = 1 + (2 + a)a^2 + 2a^3 = 1 + (2 + a)a^2 + 2a^3 = 1 + 2a^2 + 3a^3 = (1 + a^2 + a^3) \cdot (1 + a^3) = (1 + a^2 + a^3) \cdot R(a)$. $W(a, b)$ follows by (39) of 8.13.

Consequently our assumption that U is a subuniverse of $\overline{\mathbf{A}}$ forces $\boxed{2 + a = 3}$.

Finally we look at the possible values of $1 + a^2$ and a^3 in U. From 8.20 we see that $1 + a^2 \notin \{1, a, a^2\}$.

Case $\boxed{1 + a^2 = 3}$**:** $2 = 4 = 1 + (1 + a^2) = 2 + a^2 = 2a + a^2 = a(2 + a) = a \cdot 3 = 2a + a = 2 + a = 3$. This contradicts our assumption that we have three integers.

Thus $\boxed{1 + a^2 \in \{2, 1 + a\}}$.

We also have from 8.20 that $a^3 \notin \{1, 1 + a\}$. The next two cases show $a^3 \notin \{2, 3\}$.

Case $\boxed{a^3 = 2}$**:** $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + a^3 \cdot a^2 = 1 + a^5 = 1 + a^3 = R(a)$. $W(a, b)$ follows by (39) of 8.13.

Case $\boxed{a^3 = 3}$**:** $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + 6a^2 = 1 + 6a^6 = 1 + 2 \cdot 3a^3 \cdot a^3 = 1 + 2 \cdot 3 \cdot 3 \cdot 3 = 1 + 2 = 3$; $R(a) = 1 + a^3 = 1 + 3 = 2 = 2 \cdot 3 = 2 \cdot S(a)$. $W(a, b)$ follows by (40) of 8.13.

Consequently our assumption that U is a subuniverse of $\overline{\mathbf{A}}$ forces $\boxed{a^3 \in \{a, a^2\}}$.

Combining the possibilities for $1 + a^2$ and a^3 we have four cases to analyze.

Case $\boxed{1 + a^2 = 2 \textbf{ and } a^3 = a}$**:** $R(a) = 1+a^3 = 1+a = P(a); S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 2 + a^2 = 3 = 2 + a = 1 + a^2 + a = Q(a)$. $W(a, b)$ follows by (41) of 8.13.

Case $\boxed{1 + a^2 = 2 \textbf{ and } a^3 = a^2}$**:** $S(a) = 1 + a^2 + a^4 = 2 + a^2 = 3; R(a) = 1 + a^3 = 1 + a^2 = 2 = 2 \cdot 3 = 2 \cdot S(a)$. $W(a, b)$ follows by (40) of 8.13.

Case $\boxed{1 + a^2 = 1 + a \textbf{ and } a^3 = a}$**:** $R(a) = 1 + a^3 = 1 + a = P(a); S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 1 + a + a^2 = Q(a)$. $W(a, b)$ follows by (41) of 8.13.

Case $\boxed{1 + a^2 = 1 + a \textbf{ and } a^3 = a^2}$**:** $R(a) = 1 + a^3 = 1 + a^2 = 1 + a = P(a); S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 1 + a + a^2 = Q(a)$. $W(a, b)$ follows by (41) of 8.13.

So the assumption that U is a subuniverse of $\overline{\mathbf{A}}$ leads, through several cases, to a contradiction. □

Proposition 8.27. *The size of a G-algebra* $\mathbf{A}$ *is at least seven if* $\mathbf{A}$ *has exactly three integers.*

8.3. **Four Integers.** Throughout this subsection we assume $\mathbf{A}$ is a G-algebra with exactly 4 integers, and $\mathbf{A} \not\models W(a, b)$. There are two possibilities: either $3 = 5$ or $4 = 5$.

We give a 15-element example of such an algebra in the last section, with $4 = 5$. (No example is known for $3 = 5$.)

Lemma 8.28. *The five elements* $1, 2, 3, 4, a$ *are distinct, and they do not form a subuniverse of* $\overline{\mathbf{A}}$*.*

Proof. These elements are distinct by 8.2. If they form a subuniverse of $\overline{\mathbf{A}}$ then consider first what value $1 + a$ has. From 8.20 $1 + a \notin \{1, x\}$.

Case $\boxed{1 + a = 3}$**:** $P(a) = 1 + a = 3; Q(a) = 1 + a + a^2 = 1 + a(1 + a) = 1 + 3a = 7$. $W(a, b)$ follows by (37) of 8.13 (since $3|7$).

Case $\boxed{1+a=4}$**:** $P(a) = 1+a = 4; Q(a) = 1+a+a^2 = 1+a(1+a) = 1+4a = 13 = 3$. Again $W(a,b)$ follows by (38) of 8.13.

Thus the only possibility is $\boxed{1+a=2}$. Next consider the possibilities for the value of a^2. From 8.20 we have $a^2 \notin \{1, a\}$. Thus $\boxed{a^2 \in \{2,3,4\}}$. But then there is a $k \geq 1$ such that $k + a = a^2$. Now apply (45) of 8.18 to see that $W(a,b)$ holds, which is a contradiction. □

Definition 8.29. Let U_a be the subuniverse of $\overline{\mathbf{A}}$ generated by a.

Lemma 8.30. *U_a has six elements implies* $\mathbf{A}$ *has at least seven elements.*

Proof. Assume U_a has exactly six elements. Since $U = \{1, 2, 3, 4, a\}$ is not a subuniverse of $\overline{\mathbf{A}}$ it follows that at least one of $1+a, 2a, a^2$ is not in U; and hence provides the sixth element of U_a. If the sixth element is $2a$ or a^2 then b could not be in U_a as b cannot be an integer or be divisible by a by 8.5 and Lemma 8.7.

Finally suppose $U_a = \{1, 2, 3, 4, a, 1+a\}$. From 8.20 we know $a^2 \notin \{1, a, 1+a\}$, and thus $a^2 \in \{2, 3, 4\}$. Also from 8.17 $2+a \notin \{a, 1+a\}$, so $2 + a \in \{1, 2, 3, 4\}$. Also $a^2 \neq k + a$ for any non-negative k by (45) of 8.18, so $\boxed{2+a \in \{3,4\}}$ and $\boxed{a^2 \in \{2,3\}}$. Now we split into the two possible cases for four integers.

Case $\boxed{5=3}$**:** Then $a^2 = 2$ and $2 + a \in \{3, 4\}$ by (45) of 8.18. Consequently $S(a) = 1 + a^2 + a^4 = 1 + 2 + 4 = 3; R(a) = 1 + a^3 = 1 + 2a$. Now if $2a$ is an integer then $S(a)|R(a)$, so apply (40) of 8.13 to get $W(a,b)$. Thus $2a$ is not an integer, so by 8.20 $2a = 1+a$. Then $R(a) = 1+a^3 = 1+2a = 2+a \in \{3, 4\}$. So again $S(a)|R(a)$, yielding $W(a,b)$ by (40) of 8.13.

Case $\boxed{5=4}$**:** Let $a^2 = m \in \{2, 3, 4\}$. Then $R(a) = 1 + a^3 = 1 + ma; S(a) = 1 + a^2 + a^4 = 4 = 4 + 4 = 4a^4 + 4ma^5 = 4a^4(1+ma) = 4a^4 \cdot R(a)$. Apply (39) of 8.13 to obtain $W(a,b)$. □

Proposition 8.31. *If there are exactly four integers in a G-algebra* $\mathbf{A}$ *then the size of* $\mathbf{A}$ *is at least seven.*

Proof. We know there are at least six elements in U_a by 8.28; and if there are exactly six elements in U_a then $\mathbf{A}$ has at least seven elements by 8.30. □

Theorem 8.32. *A G-algebra must have at least seven elements.*

Proof. Just combine 8.5 and 8.16 with 8.27 and 8.31. □

Problem 3. Is there a finite G-algebra $\mathbf{A}$ with the integers of $\mathbf{A}$ isomorphic to $\mathbf{N}_{a,k}$ for some $k > 1$?

9. Simon Lee's Fifteen Element Example

```
From simon@shire.math.columbia.edu
To: snburris@turing.math.uic.edu
Subject: The 15 element model

Here is the 15 element model:
```

Let $\mathbf{C}$ be the following algebra.

+	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
1	2	3	4	4	2	3	e	3	4	4	4	4	4	4	4
2	3	4	4	4	3	4	3	4	4	4	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	4	4	4	4	4	4
a	2	3	4	4	c	3	c	3	4	4	4	4	4	4	4
c	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
d	e	3	4	4	c	3	c	3	4	4	4	4	4	4	4
e	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
f	4	4	4	4	4	4	4	4	4	h	4	4	4	4	4
g	4	4	4	4	4	4	4	4	h	4	4	j	4	4	4
h	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
i	4	4	4	4	4	4	4	4	4	j	4	4	4	4	4
j	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
k	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
b	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

·	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
1	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
2	2	4	4	4	c	4	c	4	4	4	4	4	4	4	4
3	3	4	4	4	3	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
a	a	c	3	4	d	c	d	c	4	g	4	4	4	4	4
c	c	4	4	4	c	4	c	4	4	4	4	4	4	4	4
d	d	c	3	4	d	c	d	c	4	g	4	4	4	4	4
e	e	4	4	4	c	4	c	4	4	4	4	4	4	4	4
f	f	4	4	4	4	4	4	4	4	4	4	k	4	4	4
g	g	4	4	4	g	4	g	4	4	4	4	4	4	4	4
h	h	4	4	4	4	4	4	4	4	4	4	4	4	4	4
i	i	4	4	4	4	4	4	4	k	4	4	4	4	4	4
j	j	4	4	4	4	4	4	4	4	4	4	4	4	4	4
k	k	4	4	4	4	4	4	4	4	4	4	4	4	4	4
b	b	4	4	4	4	4	4	4	4	4	4	4	4	4	4

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

It will be shown that $\mathbf{C}$ is a G-algebra, yielding a proof of Wilkie's theorem. This is the smallest G-algebra known; furthermore it is such that $W(x, y)$ fails only for the pair $(x, y) = (a, b)$.

Define $S_1 = \{1, a, d\}$, $S_2 = \{2, c, e\}$, $S = \{2, 3, 4, c, e, h, j\}$, $R = C \backslash S_1$.

Lemma 9.1. *Let α, $\beta \in \mathbf{C}$. Then*

(1) $\alpha + \beta \in S_2$ *iff* α, $\beta \in S_1$.
(2) $\alpha + \beta = 3$ *iff one is in* S_1 *and the other is in* S_2.
(3) $\alpha\beta = 3$ *iff one is equal to 3 and the other is in* S_1.
(4) $\alpha\beta = g$ *iff one is* g *and the other is in* S_1.
(5) $RS = \{4\}$, $R \uparrow S = \{4\}$, $RC = R$, $R + R = \{4, h, j\}$.
(6) $C + C = S$

Proof. These statements are obvious from the tables. □

Define $T_1 = \{a, d\}$ and $M = \{3, 4, c, d, g, k\}$.

Lemma 9.2. *Let α, $\beta \in \mathbf{C} \backslash \{1\}$ and $\gamma \in T_1$. Then*

(1) $\alpha + \beta = c$ *iff* $\alpha, \beta \in T_1$.
(2) $\alpha\beta = c$ *iff one is in* T_1 *and the other is in* S_2.
(3) $\alpha\beta = d$ *iff both are in* T_1.
(4) $\alpha\beta \in T_1$ *iff both are in* T_1.
(5) $(C \backslash \{1\}) \cdot (C \backslash \{1\}) = M$.
(6) $\delta \in S_1$ *iff* $\gamma\delta \in T_1 \subset S_1$.
(7) $\delta \in S_2$ *iff* $\gamma\delta \in S_2$.

Proof. Again, these statements are obvious from the tables. □

Theorem 9.3. **C** *is a HSI-algebra.*

Proof. HSI identities (1), (3), (4), (7), and (8) are clearly true in **C**. The other identities are also true:

(2): From the first lemma, $y+z \in S$. By considering the addition table, we see that $x + (y + z) \in \{3, 4\}$ (In fact, the sum of any three elements must be either 3 or 4). Because the sum of two element can never be in S_1, we have the following.

$$\begin{aligned} x + (y + z) = 3 \quad & \text{iff } x \in S_1 \text{ and } y + z \in S_2 \\ & \text{iff } x, y, z \in S_1 \\ & \text{iff } x + y \in S_2 \text{ and } z \in S_1 \\ & \text{iff } (x + y) + z = 3. \end{aligned}$$

(5): Note that if $1 \in \{x, y, z\}$ then we are done. So assume that $x, y, z \neq 1$. The product of any two elements ($\neq 1$) must be in M so the product of three elements ($\neq 1$) is in $\{3, 4, c, d, g\}$.

$$\begin{aligned} x(yz) = 3 \quad & \text{iff } x \in T_1,\ yz = 3 \text{ or } x = 3,\ yz \in T_1 \\ & \text{iff exactly one variable} = 3, \text{ others in } T_1 \\ & \text{iff } (xy)z = 3 \text{ (by symmetry)}. \end{aligned}$$

$$\begin{aligned} x(yz) = c \quad & \text{iff } x \in T_1,\ yz \in S_2 \text{ or } x \in S_2,\ yz \in T_1 \\ & \text{iff exactly one variable} \in S_2, \text{ others in } T_1 \\ & \text{iff } (xy)z = c \text{ (by symmetry)}. \end{aligned}$$

$$\begin{aligned} x(yz) = d \quad & \text{iff } x, yz \in T_1 \\ & \text{iff } x, y, z \in T_1 \\ & \text{iff } (xy)z = d \text{ (by symmetry)}. \end{aligned}$$

$$\begin{aligned} x(yz) = g \quad & \text{iff } x \in T_1,\ yz = g \text{ or } x = g,\ yz \in T_1 \\ & \text{iff exactly one variable} = g, \text{ others in } T_1 \\ & \text{iff } (xy)z = g \text{ (by symmetry)}. \end{aligned}$$

(6): If $x = 1$, we are done. Now suppose $x \neq 1$. If $x \in R$ then $x(y + z) \in RS = \{4\}$. Now $(xy) + (xz) \in RC + RC = R + R = \{4, h, j\}$. However, only $f + g = g + f = h$ and $g + i = i + g = j$ and $\nexists x$ such that $\{f, g\} \subseteq xC$ or $\{i, g\} \subseteq xC$ so $(xy) + (xz) = 4 = x(y + z)$.

Now suppose $x \in T_1$. Then $x(y + z) \in T_1S = \{3, 4, c\}$ and $(xy) + (xz) \in T_1C + T_1C$. As $T_1C = \{a, 3, 4, c, d, g\}$, $T_1C + T_1C = \{3, 4, c\}$.

$$\begin{aligned} x(y + z) = 3 \quad & \text{iff } y + z = 3 \\ & \text{iff exactly one of } y, z \in S_1 \text{ and the other is in } S_2 \\ & \text{iff exactly one of } xy, xz \in S_1 \text{ and the other is in } S_2 \\ & \text{iff } (xy) + (xz) = 3. \end{aligned}$$

$$\begin{aligned} x(y+z)=c \quad & \text{iff } y+z \in S_2 \\ & \text{iff } y,z \in S_1 \\ & \text{iff } xy, xz \in T_1 \\ & \text{iff } (xy)+(xz)=c. \end{aligned}$$

(9): If $x=1$, we are done. Note that for $x \in R$, $x \uparrow S = \{4\}$ so $x^{y+z}=4$. Since $\forall\alpha, 4\alpha=4$ and $\alpha\alpha=4$, we need only check products of powers of x for which $x^w \neq 4$ for at least two distinct $w \in C$. But $2\cdot 9 = 3\cdot 10 = 8\cdot 12 = 11\cdot 12 = 13\cdot 9 = 4$. Hence, $(x^y)(x^z) = 4 = x^{y+z}$. Now for $x \in T_1$, $x^{y+z} \in x \uparrow S = \{d\}$. Also $x^y, x^z \in x \uparrow C = T_1$ so $(x^y)(x^z) \in T_1T_1 = \{d\}$ so this identity holds.

(10): If $1 \in \{x,y,z\}$, we are done so suppose none of them are 1. Then $(xy)^z \in \{4,d,g\}$ since $2,j,e,h$ are never nontrivial products so $(xy)^z$ cannot be f or i. $(x^z)(y^z) \in \{4,d,f,g,i\}\{4,d,f,g,i\} = \{4,d,g,k\}$; however, k is not attainable since $\nexists z$ such that $\{x^z,y^z\}=\{f,i\}$.

$$\begin{aligned} (xy)^z=d \quad & \text{iff } xy \in T_1 \\ & \text{iff } x,y \in T_1 \\ & \text{iff } x^z, y^z = d \\ & \text{iff } (x^z)(y^z)=d. \end{aligned}$$

$$\begin{aligned} (xy)^z=g \quad & \text{iff } xy=3 \text{ and } z \in a,b \\ & \text{iff one of } x,y=3, \text{ other in } T_1 \text{ and } z \in a,b \\ & \text{iff one of } x^z,y^z=d, \text{ other} = g \\ & \text{iff } (x^z)(y^z)=g. \end{aligned}$$

(11): If $1 \in \{x,y,z\}$, we are done so suppose none of them are 1. $(x^y)^z \in \{4,d\}$ since $2,3,e,h,j$ are not nontrivial powers which means that f,g,i cannot be attained. Similarly, $x^{(yz)} \in \{4,d\}$ since a,b are not nontrivial products.

$$\begin{aligned} (x^y)^z=d \quad & \text{iff } xy=d \\ & \text{iff } x \in T_1 \\ & \text{iff } x^{(yz)}=d. \end{aligned}$$

□

Theorem 9.4. **C** *is a G-algebra.*

Proof. Consider $W(a,b)$. $P(a)=1+a=2$, $Q(a)=1+a+a^2=3$, $R(a)=1+a^3=e$, and $S(a)=1+a^2+a^4=3$. The LHS of $W(a,b)$ then is:

$$\begin{aligned}
\text{LHS} &= (2^a+3^a)^b \cdot (e^b+3^b)^a \\
&= (f+g)^b \cdot (i+g)^a \\
&= h^b \cdot j^a \\
&= i \cdot f \\
&= k.
\end{aligned}$$

But the RHS is:

$$\begin{aligned}
\text{RHS} &= (2^b+3^b)^a \cdot (e^a+3^a)^b \\
&= (4+g)^a \cdot (4+g)^b \\
&= 4^a \cdot 4^b \\
&= 4 \cdot 4 \\
&= 4.
\end{aligned}$$

Since W(x,y) does not hold on the HSI-algebra C, C is a G-algebra.

□

To find such small models of HSI which reject $W(x,y)$ we used the computer to help search for *cores*. Let us briefly describe this procedure. First settle on the integers you wish to work with, in this case $\mathbf{N}_{4,1}$ (boxed off in the above tables). Let $\overline{\mathbf{N}}_{4,1}[x]$ be the algebra which consists of all polynomials $a_0 + a_1x + \cdots + a_sx^s$ with coefficients from $\overline{\mathbf{N}}_{4,1}$. Addition and multiplication in $\overline{\mathbf{N}}_{4,1}[x]$ are defined in the obvious manner:

$$\begin{aligned}
(a_0 + a_1x + \cdots) + (b_0 + b_1x + \cdots +) &= (a_0+b_0) + (a_1+b_1)x + \cdots \\
(a_0 + a_1x + \cdots) \cdot (b_0 + b_1x + \cdots +) &= (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0)x + \cdots,
\end{aligned}$$

where the coefficients on the right hand sides are calculated in $\overline{\mathbf{N}}_{4,1}$. It is easy to see that $\overline{\mathbf{N}}_{4,1}[x]$ is a model of $\overline{\text{HSI}}$ — indeed it is the free algebra on one generator in the variety defined by $\overline{\text{HSI}} \cup \{4 \approx 5\}$. Now let $\overline{\mathbf{Q}}_{4,1}$ be $\overline{\mathbf{N}}_{4,1}[x]/\Theta(x^4, x^5)$, also a model of $\overline{\text{HSI}}$. The elements of $\overline{\mathbf{Q}}_{4,1}$ can be thought of as polynomials of the form

$$a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4,$$

with coefficients in $\overline{\mathbf{N}}_{4,1}$ — however the multiplication is not the same as in $\overline{\mathbf{N}}_{4,1}[x]$. For our example we have $5^5 - 1 = 3,124$ polynomials (in $\overline{\mathbf{Q}}_{4,1}$).

The key idea is to look for quotients (called *cores*) $\overline{\mathbf{Q}}_{4,1}[x]/\theta$ which can be a subreduct (subalgebra of a $\overline{\mathcal{L}}$-reduct) of a G-algebra $\mathbf{A}$ with the property that the element x/θ and some other element b will fail the Wilkie identity. For this purpose we wrote three routines for interactive computing:

- find $\Theta(p,q)$ for and p,q in $\overline{\mathbf{Q}}_{4,1}$

- check if $\forall y W(x/\theta, y)$ follows from $\overline{\mathbf{Q}}_{4,1}/\theta$ using push-pull derivations, etc., for θ a congruence of $\overline{\mathbf{Q}}_{4,1}$
- calculate $\theta_1 \vee \theta_2$ for any two congruences of $\overline{\mathbf{Q}}_{4,1}$

The computer was used (in an interactive mode) first to find small quotients of $\overline{\mathbf{N}}_{4,1}[x]/\theta$, starting with the θ being principal congruences, and then forming joins of such to get successively smaller quotients; and the computer was used to make sure they did not satisfy any of our conditions which would guarantee that

> any HSI-algebra $\mathbf{A}$ for which they were a subreduct would satisfy $W(x/\theta, y)$, for every y.

In particular push-pull derivations were analyzed (in $\overline{\mathbf{N}}_{4,1}/\theta$), starting from

$$(1, P(x/\theta), Q(x/\theta), R(x/\theta), S(x/\theta)),$$

by computer. Using this technique we were able to find the 8-element core indicated in the first two of the above tables (consisting of the elements 1,2,3,4,a,c,d,e); and we knew that this was a minimal candidate in the sense that any quotient of this core could not be a subreduct of a G-algebra which rejects Wilkie at $\langle x/\theta, y\rangle$, for some y.

Having found the 8-element quotient which "passed" all the push-pull tests, etc., there still remained the question of whether it could be extended, and then expanded, to an HSI-algebra, especially to one which rejects Wilkie. For this we have no algorithm which can be implemented on a computer. The remaining 8 elements, and the filling out of the tables, were done by hand, by trial and error. The only strategy was to try to keep the new elements as "free" as possible; and after having obtained an algebra slightly larger than 15 elements further collapsing led to this model. This part of our search looks too ad hoc to program.

In summary we have proved that the smallest G-algebra has between 7 and 15 elements. We are reasonably confident that with substantially more effort we could raise the 7 to 8. However finding G-algebras with less than 15 elements seems to be a matter of sheer good fortune at this point.

Problem 4. Find a smallest HSI-algebra which does not satisfy Wilkie's identity. (Is it unique?)

Problem 5. If $\mathbf{A}$ is an HSI-algebra with an element a such that a generates $\overline{\mathbf{A}}$ (i.e., every element of A is a polynomial in a), does it follow that $\mathbf{A} \models \forall y\, W(a, y)$?

Proposition 8.7 is a step toward answering this problem. An affirmative answer to this last question would help in pushing up the lower bound on the size of G-algebras, namely it would guarantee that a core $\mathbf{N}_{a,k}[x]/\theta$ would have to be augmented by at least one element to get a G-algebra for which $W(x/\theta, y)$ fails for some y.

Appendix A. The 44 Three-Element HSI-algebras

(1)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	1	1
b	b	1	1

(2)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	1	1
b	b	b	1

(3)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	1	1
b	b	b	b

(4)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	1
b	b	a	1

(5)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	1
b	b	b	1

(6)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	1
b	b	b	b

(7)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	a	a

(8)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	a

(9)

$+$	1	a	b
1	1	1	1
a	1	a	a
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	b

(10)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	b	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	1	a
b	b	1	a

(11)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	b	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	1	a
b	b	1	b

(12)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	b	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	1	b

(13)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	b	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	b

(14)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	b	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	b	a
b	b	b	b

(15)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	1	b	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	b

(16)

$+$	1	a	b
1	1	1	b
a	1	a	b
b	1	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	b
b	b	b	b

(17)

$+$	1	a	b
1	1	a	a
a	a	a	a
b	a	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	1
b	b	b	1

(18)

$+$	1	a	b
1	1	a	a
a	a	a	a
b	a	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	1
b	b	b	b

(19)

$+$	1	a	b
1	1	a	a
a	a	a	a
b	a	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	a

(20)

$+$	1	a	b
1	1	a	a
a	a	a	a
b	a	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	b

(21)

$+$	1	a	b
1	1	a	a
a	a	a	a
b	a	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	b
b	b	b	b

$\uparrow$	1	a	b
1	1	1	1
a	a	b	b
b	b	b	b

(22)

$+$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	a	a

(23)

$+$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	a	b

(24)

$+$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\times$	1	a	b
1	1	a	b
a	a	a	a
b	b	a	b

$\uparrow$	1	a	b
1	1	1	1
a	a	a	a
b	b	b	b

(25)

$+$	1	2	b
1	2	1	1
2	1	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	1

(26)

$+$	1	2	b
1	2	1	1
2	1	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	b

(27)

$+$	1	2	b
1	2	1	1
2	1	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	2

(28)

$+$	1	2	b
1	2	1	1
2	1	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(29)

$+$	1	2	b
1	2	1	b
2	1	2	b
b	b	b	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(30)

$+$	1	2	b
1	2	1	b
2	1	2	b
b	b	b	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	b
b	b	b	b

(31)

$+$	1	2	b
1	2	2	1
2	2	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	1

(32)

$+$	1	2	b
1	2	2	1
2	2	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	b

(33)

$+$	1	2	b
1	2	2	1
2	2	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	2

(34)

$+$	1	2	b
1	2	2	1
2	2	2	2
b	1	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(35)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	2

$\times$	1	2	b
1	1	2	b
2	2	2	2
b	b	2	2

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	2	2

(36)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	2

$\times$	1	2	b
1	1	2	b
2	2	2	2
b	b	2	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(37)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	1

(38)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	1
b	b	b	b

(39)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	2

(40)

$+$	1	2	b
1	2	2	2
2	2	2	2
b	2	2	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(41)

$+$	1	2	b
1	2	2	b
2	2	2	b
b	b	b	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	2
b	b	b	b

(42)

$+$	1	2	b
1	2	2	b
2	2	2	b
b	b	b	b

$\times$	1	2	b
1	1	2	b
2	2	2	b
b	b	b	b

$\uparrow$	1	2	b
1	1	1	1
2	2	2	b
b	b	b	b

(43)

$+$	1	2	3
1	2	3	2
2	3	2	3
3	2	3	2

$\times$	1	2	3
1	1	2	3
2	2	2	2
3	3	2	3

$\uparrow$	1	2	3
1	1	1	1
2	2	2	2
3	3	3	3

(44)

$+$	1	2	3
1	2	3	3
2	3	3	3
3	3	3	3

$\times$	1	2	3
1	1	2	3
2	2	3	3
3	3	3	3

$\uparrow$	1	2	3
1	1	1	1
2	2	3	3
3	3	3	3

References

[1] S. Burris and S. Lee, Tarski's High School Identities. To appear in the Amer. Math. Monthly.

[2] S. Burris and H.P. Sankappanavar, A Course in Universal Algebra. Grad. Texts in Math. **78**, Springer-Verlag, 1981. Springer

[3] J.L. Davison and J.O. Shallit, Continued Fractions for Some Alternating Series. Monatshefte Math. **111** (1991), 119-126.

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

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

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

[7] 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.

[8] A. Macintyre, The laws of exponentiation. Springer LNM **890** (1981), 185–197.

[9] C. Martin, Equational theories of natural numbers and transfinite ordinals, Ph.D. Thesis, U. Cal. Berkeley, 1973.

[10] G. McNulty, An equational logic sampler. in *Rewriting Techniques and Applications, RTA-89 Proceedings*, ed. N. Dershowitz, Springer Lecture Notes in Computer Science **335** (1989), 234–262.

[11] D. Richardson, Solution of the identity problem for integral exponential function. Zeitschr. f. math. Logik u. Grund. d. Math. **15** (1969), 333–340.

[12] D. Richardson, The simple exponential constant problem. Zeitschr. f. math. Logik u. Grund. d. Math. **17** (1971), 133–136.

[13] J.J. Sylvester, On a point in the theory of vulgar fractions. Amer. J. Math. **3** (1880), 332–335.

[14] J.J. Sylvester, Postscript to a note on a point in vulgar fractions. Amer. J. Math. **3** (1880), 388–389.

[15] A.J. Wilkie, On exponentiation — a solution to Tarski's high school algebra problem. Preprint, Oxford University 1980.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada, N2L 3G1

Department of Mathematics
Columbia University
New York, NY 10027