

FINITE REVERSE MATHEMATICS

Harvey M. Friedman*

Department of Mathematics

Ohio State University

friedman@math.ohio-state.edu

<http://www.math.ohio-state.edu/~friedman/>

December 22, 1999

October 19, 2001

Abstract. We present some formal systems in the language of linearly ordered rings with finite sets whose nonlogical axioms are strictly mathematical, which correspond to polynomially bounded arithmetic. With an additional strictly mathematical axiom, the systems correspond to exponentially bounded arithmetic.

1. T_0 and $I\Box_0$.

In this section, we introduce the system T_0 , and show that it corresponds to the system $I\Box_0$ of polynomially bounded arithmetic (presented below).

Let T_0 be the following system in the two sorted language with variables over integers and variables over finite sets of integers. For the integer sort, we use the language $0, 1, +, -, \cdot, <, =$ of linearly ordered rings. We use \Box between integers and sets. Equality is used only between integers. The official integer variables are x_0, x_1, \dots , and the official set variables are A_0, A_1, \dots .

The nonlogical axioms of T_0 are as follows.

1. Linearly ordered ring axioms.
2. Finite interval. $(\Box A) (\Box x) (x \Box A \Box (y < x \Box x < z))$.
3. Boolean difference. $(\Box C) (\Box x) (x \Box C \Box (x \Box A \Box \Box (x \Box B)))$.
4. Set addition. $(\Box C) (\Box x) (x \Box C \Box (\Box y) (\Box z) (y \Box A \Box z \Box B \Box x = y+z))$.
5. Set multiplication. $(\Box C) (\Box x) (x \Box C \Box (\Box y) (\Box z) (y \Box A \Box z \Box B \Box x = y \cdot z))$.
6. Least element. $(\Box x) (x \Box A) \Box (\Box x) (x \Box A \Box \Box (\Box y) (y \Box A \Box y < x))$.

The linearly ordered ring axioms are as follows.

- a. $x+0 = x$.
- b. $x+y = y+x$.
- c. $x+(y+z) = (x+y)+z$.
- d. $x+(-x) = 0$.
- e. $x \cdot 1 = x$.
- f. $x \cdot y = y \cdot x$.
- g. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- h. $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$.
- i. $(x < y \wedge y < z) \Rightarrow x < z$.
- j. $\neg(x < x)$.
- k. $x = y \iff x < y \iff y < x$.
- l. $0 < 1$.
- m. $x < y \wedge x+z < y+z$.
- n. $0 < x \wedge (y < z \wedge x \cdot y < x \cdot z)$.

We write $x-y$ for $x+(-y)$, $x > y$ for $y < x$, $x \leq y$ for $(x < y \vee x = y)$, $x \geq y$ for $y \leq x$, and $x \neq y$ for $\neg(x = y)$. Note that these ordered ring axioms suffice to prove the following.

- o. $x < y \wedge 0 < y-x$.
- p. $x < y \wedge -y < -x$.
- q. $x \cdot y = 0 \wedge (x = 0 \vee y = 0)$.
- r. $0 < x \cdot y \wedge ((0 < x \wedge 0 < y) \vee (x < 0 \wedge y < 0))$.
- s. $0 < x \wedge (y < z \wedge x \cdot y < x \cdot z)$.
- t. $x < 0 \wedge (y < z \wedge x \cdot z < x \cdot y)$.

With regard to the interval axiom, we use the notation (a,b) for $\{x: a < x \wedge x < b\}$.

With regard to set difference, we write $A \setminus B$ for $\{x: x \in A \wedge x \notin B\}$.

With regard to set addition and set multiplication, we write $A+B = \{x+y: x \in A \wedge y \in B\}$, $A \cdot B = \{x \cdot y: x \in A \wedge y \in B\}$.

We will often use scalar addition and scalar multiplication. We write $A+x = x+A = A+\{x\}$, and $A \cdot x = x \cdot A = A \cdot \{x\}$.

In Lemmas 1.1-1.27, it is understood that we are asserting provability within T_0 .

LEMMA 1.1. Let $n \geq 0$.

- i) $\neg(x < y \wedge y < x+1)$;
- ii) $[a,b], [a,b), (a,b]$ exist;
- iii) $\emptyset, \{x\}$ exists;

- iv) $x \cdot A = \{x \cdot y : y \in A\}$ exists;
- v) every nonempty set has a greatest element;
- vi) every set is included in some interval $[a, b]$;
- vii) sets are closed under pairwise union and pairwise intersection;
- viii) $\{x_1, \dots, x_n\}$ exists;
- ix) the set of all positive (negative, nonnegative, nonpositive) elements of any set exists.

Proof: For i), assume $0 < x < 1$. By axiom n, $0 = 0 \cdot x < x \cdot x < 1 \cdot x = x$. Hence there is no least y such that $0 < y < 1$. By finite interval, $(0, 1)$ exists. By least element, there is a least y such that $0 < y < 1$. This is a contradiction. So $\emptyset \cap (0 < x < 1)$. Now suppose $x < y < x+1$. Then $0 < y-x < 1$, which is a contradiction.

For ii), note that by i), $[a, b] = (a-1, b+1)$, $[a, b) = (a-1, b)$, $(a, b] = (a, b+1)$.

For iii), note that \emptyset is the interval (x, x) , and by i), $\{x\}$ is the interval $[x, x]$.

For iv), note that $x \cdot A = \{x\} \cdot A$, and apply set multiplication.

For v), Let A be nonempty. Then $-A = \{-1\} \cdot A$ has a least element x . Clearly $-x$ is the greatest element of A .

For vi), let A be given. Then $A \subseteq [\min(A), \max(A)]$.

For vii), note that $A \cap B = A \setminus (A \setminus B)$. Also note that $A \cap B = C \setminus (C \setminus A \cap C \setminus B)$, where $A, B \subseteq [\min(\min(A), \min(B)), \max(\max(A), \max(B))]$.

For viii), note that $\{x_1, \dots, x_n\} = \{x_1\} \cap \dots \cap \{x_n\}$.

For ix), let A be given. By vi), let $A \subseteq [a, b]$. Then the set of positive elements of A is $A \cap [1, b]$. The other cases are handled similarly. QED

The linearly ordered ring axioms together with $\emptyset \cap (0 < x \cap x < 1)$ is called the discrete ordered ring axioms. This is a special case of Lemma 1.1 i).

We write $-A$ for $(-1) \cdot A$, and $A-B$ for $A+(-B)$.

LEMMA 1.2. Let $d \geq 1$ and x be an integer. There exists unique q, r such that $x = dq + r$ and $0 \leq r < d$.

Proof: For uniqueness, let $x = dq + r = dq' + r'$, $0 \leq r, r' < d$. Then $d(q - q') + r - r' = 0$, $d(q - q') = r' - r$. Hence $d|q - q'| = |r' - r| < d$. So $|q - q'| < 1$, and hence $q = q'$. Therefore $0 = r' - r$, and so $r = r'$.

For existence, fix d, x as given, and first assume $x > 0$. Let $A = \{x - dq : q \in [0, x]\} = \{x\} - d \cdot [0, x]$. By Lemma 1.1 ix), let A' be the set of all nonnegative elements of A . Then A' is nonempty since $x - dq > 0$ for $q = -x$. Choose q such that $\min(A') = x - dq$. Obviously $0 \leq x - dq$ and $q \in [0, x]$.

If $q = x$ then $d = 1$ and $x - dq = 0$, in which case we are done. So we can assume that $q < x$.

Suppose $x - dq \geq d$. Then $x - d(q+1) \geq 0$ and $q+1 \in [0, x]$, contradicting the choice of q . Hence $0 \leq x - dq < d$. Set $r = x - dq$. Then $x = dq + r$ and $0 \leq r < d$.

We still have to handle the case $x \leq 0$. The case $x = 0$ is trivial, and so we assume $x < 0$. Write $-x = dq + r$, $0 \leq r < d$. Then $x = d(-q) - r$. If $r = 0$ then we are done, and so we assume $0 < r < d$. Then $x = d(-q-1) + d - r$, $0 \leq d - r < d$. QED

LEMMA 1.3. Let $k \geq 0$. The following is provable in T_0 . For all $r \geq 2$, the elements of $[0, r^{k+1})$ have unique representations of the form $n_0 r^0 + \dots + n_k r^k$, where each n_i lies in $[0, r)$. If $n_0 r^0 + \dots + n_k r^k = m_0 r^0 + \dots + m_k r^k$ and each n_i lies in $(-r/2, r/2)$, then each $n_i = m_i$.

Proof: It is important to note that k is treated as a standard integer.

For uniqueness, suppose $n_0 r^0 + \dots + n_k r^k = m_0 r^0 + \dots + m_k r^k$, where each $n_i, m_i \in [0, r)$. Let i be greatest such that $n_i \neq m_i$. We can assume that $n_i < m_i$. Here we think of i as a standard integer defined by a large number of cases.

Now subtract the second representation from the first. Then we obtain an inequality of the form

$$p_0 r^0 + \dots + p_{i-1} r^{i-1} \geq r^i,$$

where $p_0, \dots, p_{i-1} \in (-r, r)$.

Note that $p_0r^0 + \dots + p_{i-1}r^{i-1} \equiv (r-1)(r^0 + \dots + r^{i-1}) = r^i - 1$. This is the desired contradiction.

The second claim can be established in the same way by subtraction, since any two elements of $(-r/2, r/2)$ must differ by $< r$, and hence at most $r-1$.

For existence, we proceed by external induction on k . The case $k = 0$ is trivial. Suppose existence for all $r \geq 2$ and $x \in [0, r^{k+1})$, has been proved for a given k , where $k \geq 0$. Let $r \geq 2$ and $x \in [0, r^{k+2})$. Write $x = r^{k+1}n_{k+1} + y$, $0 \leq y < r^{k+1}$. Note that $0 \leq n_{k+1} < r$. By induction hypothesis, write $y = n_0r^0 + \dots + n_kr^k$, $n_0, \dots, n_k \in [0, r)$. Then $x = n_0r^0 + \dots + n_kr^k + r^{k+1}n_{k+1}$, $n_0, \dots, n_{k+1} \in [0, r)$. QED

Until the end of the proof of Lemma 1.12, we fix a standard integer $k > 0$.

LEMMA 1.4. For all $r > 1$, $S[r] = \{n_0r^0 + n_1r^2 + \dots + n_i r^{2i} + \dots + n_k r^{2k} : n_0, \dots, n_k \in [0, r)\}$ exists. Every element of $S[r]$ is uniquely written in the displayed form.

Proof: $S[r] = [0, r) \cdot r^0 + [0, r) \cdot r^2 + \dots + [0, r) \cdot r^{2k}$. The second claim follows immediately from Lemma 1.3. QED

For $x \in S[r]$, we write $x[i]$ for n_i in this unique representation.

LEMMA 1.5. For all $r > 1$ and $i \in [0, k]$, $\{x \in S[r] : x[i] = 0\}$ and $\{x \in S[r] : x[i] = 1\}$ exist.

Proof: The first set is

$$[0, r) \cdot r^0 + \dots + [0, r) \cdot \{r^{2i-2} + [0, r) \cdot r^{2i+2} + \dots + [0, r) \cdot r^{2k}\}.$$

The second set is

$$[0, r) \cdot r^0 + \dots + [0, r) \cdot r^{2i-2} + r^{2i} + [0, r) \cdot r^{2i+2} + \dots + [0, r) \cdot r^{2k}. \text{ QED}$$

LEMMA 1.6. For all $r > 1$ and $i, j, p \in [0, k]$, $\{x \in S[r] : x[i] + x[j] = x[p]\}$ exists.

Proof: $E = \{x: (\exists a, b \in [0, r]) (x = ar^{2i} + br^{2j} + (a+b)r^{2p})\}$
exists, since $E = \{x: (\exists a, b \in [0, r]) (x = a(r^{2i} + r^{2p}) + b(r^{2j} + r^{2p}))\} = ([0, r] \cdot (r^{2i} + r^{2p}) + [0, r] \cdot (r^{2j} + r^{2p}))$.

Let D be the sum of the sets $[0, r] \cdot r^{2q}$, where $q \in [0, k] \setminus \{i, j, p\}$. The set in question is $(E + D) \subseteq S[r]$.

To see this, obviously every element of the set in question lies in $(E + D) \subseteq S[r]$. On the other hand, let $x \in (E + D) \subseteq S[r]$. Write $x = n_0r^0 + \dots + n_kr^{2k}$ where each $n_i \in [0, r]$. Since $x \in E + D$, write $x = ar^{2i} + br^{2j} + (a+b)r^{2p} + y$, where $a, b \in [0, r]$ and $y \in D$. Both of these representations fall within the scope of the uniqueness in Lemma 1.3 with r replaced by r^2 since $a+b < r^2$. Hence these representations are identical. Therefore $a+b \in [0, r]$, and so x is in the set in question. QED

LEMMA 1.7. For all $r > 1$ and $i, j \in [0, k]$, $\{x \in S[r]: x[i] | x[j]\}$ exists.

Proof: $E = \{x: (\exists a, b \in [0, r]) (x = ar^{2i} + abr^{2j})\}$ exists, since $E = \{x: (\exists a, b \in [0, r]) (x = a(r^{2i} + br^{2j}))\} = [0, r] \cdot (r^{2i} + [0, r] \cdot r^{2j})$.

Let D be the sum of the sets $[0, r] \cdot r^{2q}$, where $q \in [0, k] \setminus \{i, j\}$. The set in question is $(E + D) \subseteq S[r]$.

To see this, obviously every element of the set in question lies in $(E + D) \subseteq S[r]$. On the other hand, let $x \in (E + D) \subseteq S[r]$. Write $x = n_0r^0 + \dots + n_kr^{2k}$ where each $n_i \in [0, r]$. Since $x \in E + D$, write $x = ar^{2i} + abr^{2j} + y$, where $a, b \in [0, r]$ and $y \in D$. Both of these representations fall within the scope of the uniqueness in Lemma 1.3 with r replaced by r^2 since $ab < r^2$. Hence these representations are identical. Therefore $ab \in [0, r]$, and so x is in the set in question. QED

LEMMA 1.8. For all $r > 1$, $i \in [0, k]$, and $A \in [0, r)$, $\{x \in S[r]: x[i] \in A\}$ exists.

Proof: Note that $\{x \in S[r]: x[i] \in A\}$ is $[0, r] \cdot r^0 + \dots + [0, r] \cdot r^{2i-2} + A \cdot r^{2i} + [0, r] \cdot r^{2i+2} + \dots + [0, r] \cdot r^{2k}$. QED

LEMMA 1.9. Let ϕ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $x_i | x_j$, $x_i \in A_j$, where $i, j, p \in [0, k]$. The following is provable in T_0 . For all $r > 1$ and $A_0, \dots, A_k \in [0, r)$

$[0, r)$, $\{x_0r^0 + \dots + x_kr^{2k} : \exists x_0, \dots, x_k \in [0, r)\}$ exists.

Proof: For atomic ϕ , this follows from Lemmas 1.4-1.8. The propositional combinations are handled by the fact that the subsets of $S[r]$ form a Boolean algebra. QED

LEMMA 1.10. For all $r > 1$, $i \in [0, k]$, and $E \in S[r]$, $\{x \in S[r] : (\exists y \in E) (\exists j \in [0, k] \setminus \{i\}) (x[j] = y[j])\}$ exists.

Proof: We first claim that $\{x \in S[r] : (\exists y \in E) (\exists j \in [0, k] \setminus \{i\}) (x[j] = y[j])\} \in E + (-r, r) \cdot r^{2i}$. To see this, suppose $x \in S[r]$, $y \in E$, and $\exists j \in [0, k] \setminus \{i\}$, $x[j] = y[j]$. Since the coefficients of r^{2i} in x and y both lie in $[0, r)$, we see that $x - y \in (-r, r) \cdot r^{2i}$.

Now let $x \in (E + (-r, r) \cdot r^{2i}) \in S[r]$. Write $x = y + z \cdot r^{2i}$, $y \in E$, $z \in (-r, r)$, and use this equation to write the obvious representation of x . In this representation, all coefficients lie in $[0, r)$ except possibly the coefficient of r^{2i} . This coefficient lies in $(-r, 2r)$. Hence this representation is subject to the uniqueness in Lemma 1.3, with r replaced by r^2 . Therefore this representation must be identical to the representation of x as an element of $S[r]$. In particular, in this common representation, the coefficients of all r^{2j} other than r^{2i} must be the same as the corresponding coefficients of y . Since $y \in A$, we see that x lies in the set in question. QED

LEMMA 1.11. Let ϕ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $x_i | x_j$, $x_i \in A_j$, where $i, j, p \in [0, k]$. Let $m \in [1, k]$. Let $\psi = (Q_m x_m \in [0, r)) \dots (Q_k x_k \in [0, r)) (\phi)$. The following is provable in T_0 . For all $A_0, \dots, A_k \in [0, r)$, $\{x_0r^0 + \dots + x_{m-1}r^{2m-2} : \exists x_0, \dots, x_{m-1} \in [0, r)\}$ exists.

Proof: Here Q_i is \exists or \forall . Lemma 1.9 handles ϕ . Lemma 1.10 handles existential quantifiers. Universal quantifiers is taken care of by relative complementation. QED

LEMMA 1.12. Let $r > 1$, $E \in S[r]$, $i_1 < \dots < i_p \in [0, k]$, and $x_1, \dots, x_p \in [0, r)$. Then $\{y \in S[r] : y[i_1] = x_1 \wedge \dots \wedge y[i_p] = x_p\}$ exists.

Proof: Note that this set is $A \cap B_1 \cap \dots \cap B_p$, where for all $j \in [1, p]$, $B_j = \{y \in S[r] : y[i_j] = x_j\} = [0, r) \cdot r^0 + \dots + [0, r) \cdot r^{2k}$ where the term with exponent $2j$ is replaced by $x_j r^{2j}$. QED

We now release the fixed standard integer k . For formulas \square without bound set variables, and integer variables z not in \square , Let \square^z be the result of relativizing all quantifiers in \square to $[-z, z]$.

LEMMA 1.13. Let \square be a formula without bound set variables whose atomic subformulas are of the form $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $x_i | x_j$, $x_i \in A_j$. Let y, z be distinct integer variables, where z does not appear in \square . Then T_0 proves that $\{y \in [0, z]: \square^z\}$ exists. Also T_0 proves that $\{y \in [-z, z]: \square^z\}$ exists.

Proof: Officially, $x|y$ is not an atomic formula, and so we expand $x|y$ out. Also note that the conclusion should be viewed as a separation principle with parameters (represented by the free variables of \square other than y).

By changing variables, we can assume that y is x_0 , the free variables of \square are among x_0, \dots, x_{m-1} , and the quantified variables are among x_m, \dots, x_k . Also replace the relativizations to $[-z, z]$ with relativizations to $[0, z]$, by appropriately modifying the formula.

Now apply Lemma 1.11 with $r = z+1$. We obtain $\{x_0 r^0 + \dots + x_{m-1} r^{2^{m-2}}: \square' \in x_0, \dots, x_{m-1} \in [0, z]\}$. Now apply Lemma 1.12 with $i_1, \dots, i_p = 1, \dots, m-1$ and $r = z+1$. We obtain $\{x_0 \in [0, z]: \square'\} = \{y \in [0, z]: \square^z\}$.

The second claim follows from the first. QED

LEMMA 1.14. Let \square be a formula without bound set variables whose atomic subformulas are of the form $s = t$, $s < t$, $s | t$, or $t \in A_j$, where s, t are terms without \bullet . Let y, z be distinct integer variables, where z does not appear in \square . Then T_0 proves that $\{y \in [-z, z]: \square^z\}$ exists.

Proof: By inductively introducing existential quantifiers needed to unravel the terms. A bound can be placed on the existential quantifiers introduced which depends only on \square and the value of the bound z . Since the terms do not use \bullet , the expansion stays within the form in Lemma 1.13. QED

Formulas of the form in Lemma 1.14 are called special formulas.

Below we apply Lemma 1.14 together with the existence of least and greatest elements of sets in order to carry out various induction arguments that we use below.

LEMMA 1.15. $x, y \neq 0 \implies \gcd(x, y), \text{lcm}(x, y)$ exist. $x > 1 \implies x$ is divisible by a prime.

Proof: For i), let $x, y \neq 0$. By Lemma 1.14, $\{a \in [1, |xy|] : a|x \wedge a|y\}$ exists. Then $\gcd(x, y)$ is its greatest element. By Lemma 1.14, $\{a \in [1, |xy|] : x|a \wedge y|a\}$ exists. Then $\text{lcm}(x, y)$ is its least element.

For ii), let $x > 1$. By Lemma 1.14, $\{p \in [2, x] : p|x\}$ exists. Let p be the least element. Then p is a prime divisor of x . QED

LEMMA 1.16. Suppose $x, y > 1$ and $ax + by = 1$. Then there exists $cx + dy = 1$, where $c \in (0, y)$, $d \in (-x, 0)$. Suppose $x, y > 0$ and $ax + by = 1$. Then there exists $cx + dy = 1$, where $c \in [0, y]$, $d \in [-x, 0]$.

Proof: Let x, y, a, b be as given. By symmetry we can assume that $a \geq 0$.

Let $A = \{s \in [0, ax] : (\exists t \in [1-ax, 0]) (x|s \wedge y|t \wedge s + t = 1)\}$
 $= \{s \in [0, ax] : (\exists t) (x|s \wedge y|t \wedge s + t = 1)\}$. Note that A exists by Lemma 1.14, and A is nonempty since it includes $s = ax$, with $t = by$. Let c be the least element of A .

Write $cx + dy = 1$. Note that $(c-y)x + (d+x)y = 1$. By the choice of c , $\neg(0 \leq c-y < c)$, and so $c-y < 0$ or $c-y \geq c$. Hence $c \in [0, y)$.

Note that $1 = cx + dy \in xy + dy = (x+d)y$. Hence $x+d > 0$, and so $d > -x$. Hence $d \in (-x, 0]$.

Note that $c \neq 0$ and $d \neq 0$ because of $cx + dy = 1$.

For the second claim, we need only consider the case $(x = 1, y = 1)$. By symmetry, assume $x = 1$. Then take $c = 1$ and $d = 0$. QED

We say that x, y are relatively prime if and only if $x, y \neq 0$ and the only common divisors of x, y are 1 and -1.

LEMMA 1.17. Let x, y be relatively prime. Then there exists a solution to $ax + by = 1$.

Proof: We fix a positive integer t . We wish to show by induction that the following holds for every $0 < s \leq t$. For all $0 < x, y \leq s$, if x, y are relatively prime then $ax + by = 1$ has a solution.

We need to know that this last sentence can be expressed by a special formula bounded by a superscript, as in Lemma 1.14. Note that the outermost universal quantifier is already bounded to $(0, s]$. The quantifiers involved in x, y being relatively prime can be bounded to $(0, x]$, and hence to $[0, s]$. The quantifiers involved in " $ax + by = 1$ has a solution" can be bounded to $[-|xy|, |xy|]$ and hence to $[-s^2, s^2]$, according to Lemma 1.16.

The basis case $s = 1$ is trivial. Suppose true for a fixed $s \geq 1$. Let $x, y \leq s+1$ be relatively prime. We can assume $1 < y < x = s+1$. Write $x = qy + r$, $0 \leq r < y$. Since x, y are relatively prime, we have $0 < r < y$.

Note that y, r are relatively prime and positive. Hence by induction hypothesis write $cy + dr = 1$. Now $dx + (c-dq)y = 1$.

We still have to consider the case where x or y is negative. But then we can merely change the sign or signs of one or more of a, b . QED

LEMMA 1.18. Let p be a prime and suppose $p \mid xy$. Then $p \mid x$ or $p \mid y$.

Proof: Let p, x, y be as given. Suppose the contrary. Then $x, y \neq 0$, and p, x are relatively prime, and p, y are relatively prime. By Lemma 1.17, write $ap + bx = 1$, $cp + dy = 1$. Then $apcp + apdy + bxcy + bxdy = 1$. Note that p divides every summand, and so p divides 1, which is a contradiction. QED

LEMMA 1.19. Let x, y be relatively prime and let x, z be relatively prime. Suppose $x \mid yz$. Then $x = 1$ or -1 .

Proof: Let x, y, z be as given. Write $ax + by = 1$ and $cx + dz = 1$. Then $axcx + axdz + bycx + bydz = 1$. Since x divides every summand, x divides 1. Hence $x = 1$ or -1 . QED

LEMMA 1.20. Let x, y be relatively prime and $x \mid yz$. Then $x \mid z$.

Proof: Let x, y, z be as given. We can assume that $z \neq 0$. It suffices to prove this for $x, y, z > 0$.

Now $x/\gcd(x, z)$ divides $y(z/\gcd(x, z))$ via the integer factor yz/x . Also note that $x/\gcd(x, z)$ and y are relatively prime.

We claim that $x/\gcd(x, z)$ and $z/\gcd(x, z)$ are relatively prime. To see this, suppose they have a common factor $u > 1$. Then $\gcd(x, z)u$ is a factor of x and also a factor of z , contradicting that $\gcd(x, z)$ is the greatest common factor of x, z .

By Lemma 1.19, $x/\gcd(x, z) = 1$. I.e., $\gcd(x, z) = x$. So $x|z$. QED

LEMMA 1.21. Let a, b be relatively prime. Then the least positive common multiple of a, b is ab .

Proof: Let a, b be as given, and let x be a positive common multiple of a, b . Write $x = ay$.

Since $b|ay$, by see by Lemma 1.20 that $b|y$. Hence $b \leq y$. Therefore $x = ay \geq ab$ as required. QED

LEMMA 1.22. There is a special formula \square with free variables among x, y such that the following is provable in T_0 . For all z there exists $z' > z$ such that $(\square_{x, y \in [-z, z]}) (x = y^2 \square \square^{z'})$.

Proof: Let \square express $x+y = \text{lcm}(y, y+1)$. Let z be given. If $y \in [-1, 0]$ then $\gcd(y, y+1) = 1$, and hence by Lemma 1.10, $\text{lcm}(y, y+1) = y(y+1)$. Therefore $(\square_{x, y \in [-z, z] \setminus [-1, 0]}) (\square \square x+y = y(y+1))$. Hence $(\square_{x, y \in [-z, z] \setminus [-1, 0]}) (\square \square x = y^2)$. The quantifiers in \square can be bounded to an integer z' that depends only on z .

We still have to modify \square in order to handle $[-1, 0]$. Take \square' to be $(\square \square_{x, y \in [-1, 0]}) \quad x = y = 0 \quad (x = 1 \square y = -1)$. QED

LEMMA 1.23. There is a special formula \square with free variables among u, v, w , such that the following is provable in T_0 . For all z there exists $z' > z$ such that $(\square_{u, v, w \in [-z, z]}) (u \cdot v = w \square \square^{z'})$.

Proof: Let $\square = (\square_{x, y, a, b}) (x = y^2 \square y = u+v \square a = u^2 \square b = v^2 \square 2w = x-a-b)$. Let z be given. Then $(\square_{u, v, w \in [-z, z]}) (u \cdot v = w$

\square \square). Use the \square from Lemma 1.22 to remove the first, third, and fourth displayed equations, to make \square special. The quantifiers can be bounded to $z' > z$, where z' depends only on z . QED

We now extend Lemma 1.14.

LEMMA 1.24. Let \square be a formula without bound set variables whose atomic subformulas are of the form $x_i = 0$, $x_i = 1$, $x_i + x_j = z$, $x_i \cdot x_j = x_p$, $x_i \in A_j$. Let y, z be distinct integer variables, where z does not appear in \square . Then T_0 proves that $\{y \in [-z, z]: \square^z\}$ exists.

Proof: Let \square be as given. Replace each atomic subformula of the form $x \cdot y = z$ by the \square of Lemma 1.23, with an appropriate change of variables. Call this expansion \square . Let z be given. Then there exists $z' > z$ depending only on z such that for all $y \in [-z, z]$, $\square^z \in \square^{z'}$. By Lemma 1.14, $\{y \in [-z', z']: \square^{z'}\}$ exists. Hence $\{y \in [-z', z']: \square^z\}$ exists. Hence $\{y \in [-z, z]: \square^z\}$ exists. QED

LEMMA 1.25. Let \square be a formula without bound set variables. Let y, z be distinct integer variables, where z does not appear in \square . Then T_0 proves that $\{y \in [-z, z]: \square^z\}$ exists.

Proof: Let \square be as given, and let z be given. Expand the terms appearing in \square using existential quantifiers. Apply Lemma 1.24 with appropriately chosen z' , where z' depends only on z and the terms that appear. QED

We now define the class of bounded formulas of T_0 .

- i) every atomic formula of T_0 is a bounded formula of T_0 ;
- ii) if \square, \square are bounded formulas of T_0 then so are $\square \square$, $\square \in \square$, $\square \in \square$, $\square \in \square$, $\square \in \square$;
- iii) if \square is a bounded formula of T_0 , x is an integer variable, s, t are integer terms, x not in s, t , then $(\exists x \in [s, t]) (\square)$ and $(\exists x \in [s, t]) (\square)$ are bounded formulas of T_0 .

LEMMA 1.26. Let \square be a bounded formula of T_0 . Let x_1, \dots, x_k be an enumeration without repetition of at least the free variables of \square . The following is provable in T_0 . Let $r > 1$. Then $\{x_1 r^1 + \dots + x_k r^k: x_1, \dots, x_k \in [0, r) \cap \square\}$ exists.

Proof: By induction on \square . Let \square be atomic. Then this follows from Lemma 1.25. Suppose this is true for the bounded

formulas of T_0 , φ, ψ . Let φ be among $\varphi\psi, \varphi \vee \psi, \varphi \wedge \psi, \varphi \rightarrow \psi, \varphi \leftrightarrow \psi, \exists x \varphi$. Then obviously this holds for φ .

Now suppose this holds for the bounded formulas of T_0 , φ , and $\psi = (\exists x \varphi [s, t]) (\theta)$. Let x_1, \dots, x_k be an enumeration without repetition of at least the free variables of φ . Then x_1, \dots, x_k, x is an enumeration without repetition of at least the free variables of ψ .

We want to show that

$$A = \{x_1 r^1 + \dots + x_k r^k : x_1, \dots, x_k \in [0, r) \wedge (\exists x \varphi [s, t]) (\theta)\}$$

provably exists for all $r > 1$. We know that

$$B = \{x_1 r^1 + \dots + x_k r^k + x r^{k+1} : x_1, \dots, x_k, x \in [0, r) \wedge \theta\}$$

provably exists for all $r > 1$. We can define A from B appropriately so that we can simply apply Lemma 1.25. QED

LEMMA 1.27. Let φ be a bounded formula of T_0 . Let z be an integer variable that does not appear in φ . Then T_0 proves that $\{y \in [-z, z] : \varphi\}$ exists.

Proof: From Lemmas 1.25 and 1.26. QED

THEOREM 1.28. T_0 can be axiomatized as follows.

1. Linearly ordered ring axioms.
2. $(\exists A) (\exists x) (x \in A \wedge (y < x \wedge x < z \wedge \varphi))$, where φ is a bounded formula of T_0 and A is not free in φ .
3. Least element.

Proof: Axiom scheme 2 is derivable from T_0 by Lemma 1.27. For the other direction, first note that we can derive $(\exists A) (\neg A \text{ exists})$. Hence every set has a greatest element. Then it is easy to see that finite interval, Boolean difference, set addition, and set multiplication are special cases of axiom scheme 2 above. QED

We now introduce the system K_0 based on integers only. The language of K_0 is the same as that of T_0 , except no set variables are allowed.

A bounded formula of K_0 is a bounded formula of T_0 that has no set variables.

The nonlogical axioms of K_0 are as follows.

1. Linearly ordered ring axioms.
2. $(\exists [x/0] \wedge (\forall x \geq 0) (\exists \square \wedge \square[x/x+1])) \wedge (x \geq 0 \wedge \square)$, where \square is a bounded formula of K_0 .

THEOREM 1.29. T_0 and K_0 prove the same formulas without set variables.

Proof: By Theorem 1.28, K_0 is a subsystem of T_0 . For the other direction, it suffices to show that any model of K_0 can be expanded by attaching sets to form a model of T_0 . Take the sets to be of the form $\{x \in [-r, r] : \square\}$, where \square is a bounded formula in the language of K_0 , and r is an integer in the model. Then the resulting expansion satisfies the three axioms in Theorem 1.28. QED

We now introduce the system $I\mathbb{N}_0$ based on nonnegative integers only. See [HP98], p. 62.

The language of $I\mathbb{N}_0$ has variables over nonnegative integers, $0, S, +, \cdot, \square, =$.

The \mathbb{N}_0 formulas are the formulas of $I\mathbb{N}_0$ defined as follows.

- i) every atomic formula of $I\mathbb{N}_0$ is \mathbb{N}_0 ;
- ii) if \square, \square are \mathbb{N}_0 then so are $\square \wedge \square, \square \vee \square, \square \rightarrow \square, \square \leftrightarrow \square, \forall \square, \exists \square$;
- iii) if \square is \mathbb{N}_0 , x is a variable, s, t are terms, x not in s, t , then $(\forall x \square t) (\square)$ and $(\exists x \square t) (\square)$ are \mathbb{N}_0 .

In iii), the expressions are treated as abbreviations.

The nonlogical axioms of $I\mathbb{N}_0$ are as follows.

1. The axioms of \mathbb{Q} .
2. $(\exists [x/0] \wedge (\forall x) (\exists \square \wedge \square[x/Sx])) \wedge \square$, where \square is \mathbb{N}_0 .

The nonlogical axioms of \mathbb{Q} are

- Q1. $\square Sx = 0$.
- Q2. $Sx = Sy \wedge x = y$.
- Q3. $x \neq 0 \wedge (\forall y) (x = Sy)$.
- Q4. $x + 0 = x$.
- Q5. $x + Sy = S(x + y)$.
- Q6. $x \cdot 0 = 0$.

- Q7. $x \cdot Sy = (x \cdot y) + x$.
 Q8. $x \leq y \iff (\exists z)(z + x = y)$.

This presentation is slightly different than that given in [HP98]. There \leq is not taken as a primitive, but instead is defined by Q8. Also there the terms t in bounded quantification are required to be variables.

The equivalence between $I\mathbb{N}_0$ and K_0 is extremely strong.

THEOREM 1.30. A sentence in the language of $I\mathbb{N}_0$ is provable in $I\mathbb{N}_0$ if and only if the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in K_0 (or T_0).

Proof: For the forward direction, first note that the indicated interpretation sends the universal closure of each instance of axiom 2 of $I\mathbb{N}_0$ to a theorem of K_0 . To see this, note that the indicated interpretation of any \mathbb{N}_0 formula of $I\mathbb{N}_0$ is a bounded formula of K_0 . It now suffices to show that the indicated interpretation sends the universal closure of each axiom of Q to a theorem of K_0 . For this, we only need only the linearly ordered group axioms with $\leq (0 < x < 1)$.

For the reverse direction, let ϕ be a sentence in the language of $I\mathbb{N}_0$ whose indicated interpretation ϕ' is a theorem of K_0 . Note that there is an obvious interpretation $*$ from the language of K_0 into the language of $I\mathbb{N}_0$ such that $\phi' * \phi$ is provable in $I\mathbb{N}_0$. (This obvious interpretation $*$ is according to the usual way of developing the linearly ordered ring of integers out of the linearly ordered semiring of natural numbers).

We now have that $(\phi' * \phi)$ is provable in K_0 . Hence $\phi' * \phi$ is provable in K_0 , and therefore ϕ' is provable in K_0 .

Now looking at this obvious interpretation $*$, we see that it sends sentences provable in K_0 to sentences provable in $I\mathbb{N}_0$. Hence $\phi' * \phi$ is provable in K_0 . Since $\phi' * \phi$ is provable in $I\mathbb{N}_0$, we see that ϕ' is provable in $I\mathbb{N}_0$. Since $\phi' * \phi$ is provable in $I\mathbb{N}_0$, we see that ϕ is provable in $I\mathbb{N}_0$. QED

Note that Theorem 1.30 also gives a criterion for determining provability of sentences in K_0 in terms of provability of sentences in $I\mathbb{N}_0$. This is because the provability of any sentence in K_0 is equivalent to the provability of an obvious

associated sentence in K_0 which is itself the indicated interpretation (in Theorem 1.30) of a unique sentence in the language of $I\mathbb{Q}_0$.

In fact, from the proof of Theorem 1.30, it is easily seen that we have given a rather strong form of what is called synonymy of $I\mathbb{Q}_0$ and K_0 . See [Bo65].

2. T_1 and $I\mathbb{Q}_0(\text{exp})$.

We now consider the system T_1 whose nonlogical axioms are

1. The axioms of T_0 .
2. Multiples. $(\exists y)(0 < y \wedge (\forall z)((0 < z \wedge z < x) \rightarrow (\exists w)(y = z \cdot w)))$.

Informally, axiom 2 asserts that for all integers x , the positive integers $1, \dots, x$ have a common positive multiple. This axiom can be viewed as mathematically essential since it is an immediate consequence of having a usable discrete factorial function.

An obvious consequence of T_1 is

- 2'. $(\exists y)(y \neq 0 \wedge (\forall z)((z \neq 0 \wedge z \in A) \rightarrow (\exists w)(y = z \cdot w)))$.

Informally, 2' asserts that the nonzero elements of any finite set have a nonzero common multiple.

LEMMA 2.1. The following is provable in T_1 . Let $n > 1$ and t be the least positive common multiple of $1, \dots, n$. Then $t+1, 2t+1, \dots, nt+1$ are relatively prime in pairs.

Proof: Suppose $it+1$ and $jt+1$, $1 \leq i < j \leq n$, are not relatively prime. Let p be the least positive common divisor of $it+1$ and $jt+1$.

Since $p \mid it+1$, we see that $p > n$. Hence $p \mid i-j$ is false.

Now $p \mid (jt+1) - (it+1)$, and so $p \mid (j-i)t$. By Lemma 1.18, $p \mid t$. This contradicts $p \mid it+1$. QED

LEMMA 2.2. The following is provable in T_1 . Let $n, t > 1$ and $t+1, 2t+1, \dots, nt+1$ be relatively prime in pairs. For each $1 \leq i \leq n$, the least common multiple of $t+1, \dots, (i+1)t+1$ is at

least $(i+1)^{t+1}$ times the least common multiple of $t+1, \dots, it+1$.

Proof: Let n, t be as given. The common multiples in question exist by axiom 2 of T_1 . Let $1 \leq i \leq n$ and x be the least common multiple of $t+1, \dots, it+1$. Let y be any common multiple of $t+1, \dots, (i+1)^{t+1}$. Let $z = y/(i+1)^{t+1}$.

We claim that z is still a common multiple of $t+1, \dots, it+1$. To see this, let $1 \leq j \leq i$. Then $j^{t+1} | z((i+1)^{t+1})$. Now j^{t+1} and $(i+1)^{t+1}$ are relatively prime by Lemma 2.1. Hence by Lemma 1.20, $j^{t+1} | z$.

By the choice of x , we see that $z \geq x$. I.e., $y/(i+1)^{t+1} \geq x$. So $y \geq x((i+1)^{t+1})$. QED

LEMMA 2.3. There is a Π_0 formula $\text{Exp}(x, y, z)$ with only the free variables shown such that the following is provable in $I\Pi_0$.

- i) $\text{Exp}(x, 0, z) \leftrightarrow z = 1$;
- ii) $\text{Exp}(x, y+1, z) \leftrightarrow (\exists v) (\text{Exp}(x, y, v) \leftrightarrow z = vx)$.

Proof: See [HP98], p. 299. QED

LEMMA 2.4. There is a bounded formula $\text{Exp}'(x, y, z)$ with only the free variables shown such that the following is provable in K_0 .

- i) $\text{Exp}'(x, 0, z) \leftrightarrow (z = 1 \wedge x \geq 0)$;
- ii) $\text{Exp}'(x, y+1, z) \leftrightarrow ((\exists v) (\text{Exp}'(x, y, v) \leftrightarrow z = vx) \wedge x \geq 0)$.

Proof: Immediate from Lemma 2.1 and Theorem 1.30. QED

We fix a formula $\text{Exp}'(x, y, z)$ provided by Lemma 2.4.

LEMMA 2.5. T_1 proves $(\exists n \geq 0) (\exists r) (\text{Exp}'(n, n, r))$.

Proof: Fix $n > 1$. By Lemma 2.1, let $t \geq n$ be such that $t+1, 2t+1, \dots, nt+1$ are relatively prime in pairs. By Lemma 2.2, for each $1 \leq i \leq n$, $\text{lcm}(t+1, \dots, (i+1)^{t+1}) \geq ((i+1)^{t+1}) \text{lcm}(t+1, \dots, it+1) \geq n \text{lcm}(t+1, \dots, it+1)$. Let $x = \text{lcm}(t+1, \dots, nt+1)$.

It is straightforward to prove by induction on $1 \leq i \leq n$ that $(\exists z \leq y \leq x) (y = \text{lcm}(t+1, \dots, it+1) \wedge \text{Exp}'(n, i, z))$. QED

LEMMA 2.6. T_1 proves $(\exists n, m \geq 0) (\exists r) (\text{Exp}'(n, m, r))$.

Proof: Fix $t \geq 0$. We prove $(\exists n, m \leq [0, t]) (\exists r) (\text{Exp}'(n, m, r))$ as follows. By Lemma 2.5, let $\text{Exp}'(t, t, x)$. Fix $n \leq [0, t]$. Then prove by induction on $0 \leq m \leq t$ that $(\exists r \leq y \leq x) (\text{Exp}'(t, t, y) \leq \text{Exp}'(n, m, r))$. QED

We now introduce the system K_1 . We augment the language of K_0 with the binary function symbol $*$. We wish to use only total functions, so the intended interpretation is that if either argument is negative then the value is 0 by default.

The bounded formulas of K_1 are defined as follows.

- i) every atomic formula of K_1 is a bounded formula of K_1 ;
- ii) if ϕ, ψ are bounded formulas of K_1 then so are $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$, $\phi \leftrightarrow \psi$;
- iii) if ϕ is a bounded formula of K_1 , x is an integer variable, s, t are terms of $K_0(\text{exp})$, x not in s, t , then $(\exists x \leq [s, t]) (\phi)$ and $(\exists x \leq [s, t]) (\neg \phi)$ are bounded formulas of $K_0(\text{exp})$.

The nonlogical axioms of K_1 are as follows.

1. Linearly ordered ring axioms.
2. $x, y \geq 0 \rightarrow (x * 0 = 1 \rightarrow x * (y + 1) = x * y + x)$;
3. $(x < 0 \vee y < 0) \rightarrow x * y = 0$;
4. $(\exists [x/0] \rightarrow (\exists x \geq 0) (\phi \rightarrow \phi[x/x+1])) \rightarrow (x \geq 0 \rightarrow \phi)$, where ϕ is a bounded formula in the language of K_1 .

THEOREM 2.7. T_1 and K_1 prove the same formulas without set variables and $*$.

Proof: We can interpret the language of K_1 in the language of T_1 as follows. Preserve the integers and the ordered ring operations. Interpret $*$ by

$$x * y = z \rightarrow ((x < 0 \vee y < 0) \rightarrow z = 0) \rightarrow \text{Exp}'(x, y, z).$$

By Lemma 2.6, T_1 proves that this provably defines a total binary function, and also the interpretations of axioms 2, 3 of K_1 .

For axiom 4 of K_1 , let $(\exists [x/0] \rightarrow (\exists x \geq 0) (\phi \rightarrow \phi[x/x+1])) \rightarrow (x \geq 0 \rightarrow \phi)$ be given, where ϕ is a bounded formula in the language of K_0 . Let

$$(\phi' [x/0] \rightarrow (\exists x \geq 0) (\phi' \rightarrow \phi' [x/x+1])) \rightarrow (x \geq 0 \rightarrow \phi')$$

be its interpretation into the language of T_1 . Note that the terms in ϕ are unraveled with existential quantifiers under this interpretation. Let $r \geq 0$ be arbitrary. We can prove

$$(\phi' [x/0] \wedge (\exists x \geq 0) (\phi' \wedge \phi' [x/x+1])) \wedge (x \in [0, r] \wedge \phi')$$

by induction on $x \in [0, r]$ within T_1 . This is because we can bound all of the quantifiers in this formula by a number depending only on r and the subterms of ϕ . That number corresponds to the value of a single term of K_1 in r and the free variables of ϕ . By Lemma 2.6, this bound provably exists in T_1 . Thus the induction on $x \in [0, r]$ becomes an induction with respect to a bounded formula of T_0 , and hence is available in T_1 .

For the other direction, it suffices to show that any model of K_1 can be expanded by attaching sets to form a model of T_1 . Take the sets to be of the form $\{x \in [-r, r] : \phi\}$, where ϕ is a bounded formula of K_1 , and r is an integer in the model. Then the resulting expansion satisfies the axioms of T_1 . QED

We now give two standard systems involving only nonnegative integers with correspond to K_1 . These are $I\mathbb{N}_0 + \text{exp}$ and $I\mathbb{N}_0(\text{exp})$. See [HP98], p. 272, and p. 37, respectively.

$I\mathbb{N}_0 + \text{exp}$ has the same language as $I\mathbb{N}_0$. The nonlogical axioms are

1. The axioms of $I\mathbb{N}_0$.
2. $(\exists x, y) (\exists z) (\text{Exp}(x, y, z))$.

Here we rely on any formula given by Lemma 2.3. It can be easily shown that any such formula leads to the same system.

$I\mathbb{N}_0(\text{exp})$ is to $I\mathbb{N}_0$ as K_1 is to K_0 . We add the binary function symbol $*$. The $\mathbb{N}_0(\text{exp})$ formulas are defined as follows.

- i) every atomic formula of $I\mathbb{N}_0$ is $\mathbb{N}_0(\text{exp})$;
- ii) if ϕ, ψ are $\mathbb{N}_0(\text{exp})$ then so are $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$, $\phi \leftrightarrow \psi$;
- iii) if ϕ is $\mathbb{N}_0(\text{exp})$, x is an integer variable and t is a term of $I\mathbb{N}_0(\text{exp})$, x not in s, t , then $(\exists x \in t) (\phi)$ and $(\forall x \in t) (\phi)$ are $\mathbb{N}_0(\text{exp})$.

The nonlogical axioms of $I\mathbb{N}_0(\text{exp})$ are as follows.

1. The axioms of Q .
2. $x \cdot 0 = 1, x \cdot (y+1) = x \cdot y + x$.
3. $(\exists [x/0] \exists (\exists x \geq 0) (\exists \exists [x/x+1])) \rightarrow (x \geq 0 \rightarrow \exists)$, where \exists is $\exists_0(\text{exp})$.

It is well known that $I\exists_0(\text{exp})$ and $I\exists_0 + \text{exp}$ prove the same formulas that do not mention $*$.

THEOREM 2.8. A sentence in the language of $I\exists_0(\text{exp})$ is provable in $I\exists_0(\text{exp})$ if and only if the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in K_1 . A sentence in the language of $I\exists_0$ is provable in $I\exists_0 + \text{exp}$ if and only if the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in T_1 .

Proof: The first claim is proved analogously to the proof of Theorem 1.30. The second claim follows from the first claim and Theorem 2.7. QED

We can elegantly axiomatize T_1 by adding the factorial function. The language of $T_1(!)$ is the same as the language of T_1 with the addition of a unary function symbol $!$.

The nonlogical axioms of $T_1(!)$ are

1. The axioms of T_0 .
2. $0! = 1$.
3. $x > 0 \rightarrow x! = x \cdot (x-1)!$.
4. $0 < x < y \rightarrow (\exists z) (0 < z \rightarrow z \cdot (x!) = y!)$.

THEOREM 2.9. T_1 is a subsystem of $T_1(!)$. T_1 and $T_1(!)$ prove the same formulas that do not mention $!$.

Proof: It is obvious that Multiples is derivable from axiom 4 of T_0 . We now interpret $T_1(!)$ in T_1 by using the same integers, and the same ordered ring primitives. Since we have the \exists_0 formula $\text{Exp}'(x, y, z)$ with $(\exists x, y) (\exists z) (\text{Exp}'(x, y, z))$ available in T_1 , we can code finite sequences using the Gödel \exists function. We can then build codes for the finite sequences $(0!, 1!, \dots, n!)$, $n \geq 0$, using bounds coming from iterating $(\exists x, y) (\exists z) (\text{Exp}'(x, y, z))$ just a few times. QED

3. Some Variants.

T_2 has the same language as T_0 . The nonlogical axioms of T_2 are as follows.

1. Linearly ordered ring axioms.
2. Finite interval.
3. Boolean difference.
4. Duplicate set addition. $(\exists B)(\exists x)(x \in B \wedge (\exists y)(\exists z)(y \in A \wedge z \in A \wedge x = y+z))$.
5. Duplicate set multiplication. $(\exists B)(\exists x)(x \in B \wedge (\exists y)(\exists z)(y \in A \wedge z \in A \wedge x = y \cdot z))$.
6. Every set has a least and greatest element.

Axiom 4 asserts the existence of $A+A$, and axiom 5 asserts the existence of $A \cdot A$.

Lemmas 3.1 - 3.8 refer to provability in T_2 .

LEMMA 3.1. i)-iii),v)-ix) of Lemma 1.1.

Proof: Straightforward. QED

LEMMA 3.2. Let $A \subseteq [-x, x]$, $x \geq 0$, and $|y| > 3x$. Then $A+y$ exists.

Proof: Let A, x be as given. By Lemma 3.1, let $B = A \cup \{y\}$. Then $B+B$ is composed of three parts: $A+A$, $A+y$, $\{2y\}$. We don't know yet that the second part is a set. Note that $A+A \subseteq [-2x, 2x]$ and $A+y \subseteq [-x+y, x+y]$.

First assume $y > 0$. Note that $2x < -x+y$ and $x+y < 2y$. Hence these three parts are pairwise disjoint. Since $B+B$ and the first and third parts exist, clearly the second part exists.

Now assume $y < 0$. Note that $-2x > x+y$ and $-x+y > 2y$. Hence these three parts are pairwise disjoint. So the second part exists. QED

LEMMA 3.3. Let $A \subseteq [7z/8, 9z/8]$, $z > 0$, $w < -z/2$. Then $A+w$ exists.

Proof: Let A, z, w be as given. Let $B = A \cup \{w\}$. Then $B+B$ is composed of three parts: $A+A$, $A+w$, $\{2w\}$. Note that $A+A \subseteq [7z/4, 9z/4]$ and $A+w \subseteq [7z/8 + w, 9z/8 + w]$.

Note that $9z/8 + w < 7z/4$. Hence the first two parts are disjoint. Therefore $A+w$ is among $B+B \setminus A+A$, $B+B \setminus A+A \setminus \{2w\}$, $B+B \setminus A+A \setminus \{2w\}$. Hence $A+w$ exists. QED

LEMMA 3.4. $A+y$ exists.

Proof: Let $A \subseteq [-x, x]$, $x > 0$, and y be given. We can assume that y is nonzero. Write $y = z+w$, where $z > 3x$, $A+z \subseteq [7z/8, 9z/8]$, $w < -z/2$. By Lemma 3.2, $A+z$ exists. By Lemma 3.3, $A+z+w$ exists. But $A+z+w = A+y$.

It remains to show how z, w can be chosen. Set $z = 9\max(x, |y|)$. Set $w = y - z = y - 9\max(x, |y|)$. Note that $A+z \subseteq [-x+z, x+z] \subseteq [7z/8, 9z/8]$.

We have only to verify that $w < -z/2$. I.e., $y - 9\max(x, |y|) < -9\max(x, |y|)/2$, which is $y < 9\max(x, |y|)/x$. This follows from $x > 0$ and $y \neq 0$. QED

LEMMA 3.5. $A+B$ exists.

Proof: Let A, B be given. Let $A, B \subseteq [-x, x]$, $x \geq 0$. By Lemma 3.2, let $C = B+4x$. Consider $A \setminus C + A \setminus C$. This is composed of three parts: $A+A$, $A+C$, $C+C$. We don't know yet that the second part is a set.

Note that $A+A \subseteq [-2x, 2x]$, $A+C \subseteq [3x, 5x]$, $C+C \subseteq [6x, 10x]$. Hence these three parts are pairwise disjoint. Since $A \setminus C + A \setminus C$ and the first and third parts exist, clearly the second part exists. I.e., $A+C$ exists.

Observe that $A+C = A+B+4x$, and so $A+B = A+C-4x$, which exists by Lemma 3.4. QED

LEMMA 3.6. $-A$ exists.

Proof: Let A be given. First assume that $A \subseteq [1, x]$, $x > 1$. Let $B = A \setminus \{-1\}$. Note that $B \cdot B = A \cdot A \setminus \{1\} \setminus -A$, where we don't know yet that $-A$ exists. However, $-A$ is disjoint from $A \cdot A \setminus \{1\}$. Hence $-A$ exists.

Now assume that $A \subseteq [-x, -1]$, $x > 1$. Using Lemmas 3.1 and 3.4, let $B = A + x^3$. Consider $B \setminus \{-1\} \cdot B \setminus \{-1\}$. This is composed of three parts: $B \cdot B$, $-B$, $\{1\}$, where we don't know yet that $-B$ exists. Note that $B \cdot B \subseteq [x^3+1)^2, (x^3+x)^2]$, $-B \subseteq [1+x^3, x+x^3]$.

Hence the three parts are pairwise disjoint. Therefore $-B$ exists.

Finally, let A be arbitrary. Write $A = A^+ \sqcup A^- \sqcup A^0$, where A^+ is the positive part of A , A^- is the negative part of A , and A^0 is the 0 part of A , which is $\{0\}$ if $0 \in A$ and \emptyset if $0 \notin A$.

Note that $-A = -(A^+) \sqcup -(A^-) \sqcup A^0$, and so $-A$ exists. QED

LEMMA 3.7. $A \cdot x$ exists.

Proof: First assume $A \subseteq [y^2, y^3]$, $y > x > 1$. Consider $A \sqcup \{x\} \cdot A \sqcup \{x\}$. This is composed of three parts: $A \cdot A$, $A \cdot x$, $\{x^2\}$, where we don't know yet that $A \cdot x$ exists. Note that $A \cdot A \subseteq [y^4, y^6]$, $A \cdot x \subseteq [xy^2, xy^3]$. Hence the three parts are pairwise disjoint. Therefore $A \cdot x$ exists.

Now assume A is arbitrary and $x > 1$. We can choose $y > x$ such that $B \subseteq [y^2, y^3]$, where B is a translation of A . Then $B \cdot x$ exists.

Let $A = B + c$. Then $A \cdot x = (B + c) \cdot x = B \cdot x + \{cx\}$. Therefore $A \cdot x$ exists.

The case $x = 0$ is trivial. Finally suppose A is arbitrary and $x < -1$. Then $A \cdot x = -(A \cdot -x)$, and $-x > 1$. Therefore $A \cdot x$ exists. QED

LEMMA 3.8. $A \cdot B$ exists.

Proof: Let A, B be given. We first assume that $A, B \subseteq [1, x]$, $x > 1$. Let $C = A \sqcup -B$. Then $C \cdot C$ exists. Its negative part is obviously $A \cdot -B$, which therefore exists. Note that $A \cdot B = -(A \cdot -B)$, and therefore $A \cdot B$ exists.

For the general case, write $A = A^+ \sqcup A^- \sqcup A^0$, $B = B^+ \sqcup B^- \sqcup B^0$. Then $A \cdot B$ is the union of the nine obvious crossproducts. There are only three of them that we have to check exist, the other six obviously existing. These are $A^+ \cdot B^-$, $A^- \cdot B^+$, $A^- \cdot B^-$. However, it is easy to see that these are, respectively, $-(A \cdot B)$, $-(A \cdot B)$, $A \cdot B$, and therefore exist. QED

Recall that T_1 is T_0 with Multiples. Let T_3 be T_2 with Multiples.

THEOREM 3.9. T_0 and T_2 are equivalent. T_1 and T_3 are equivalent.

Proof: By Lemmas 3.5 and 3.8. QED

We now present another variant of T_0 . Here we replace $A \bullet B$ in favor of scalar multiplication and squares.

The language of T_4 is the same as the language of T_0 . The nonlogical axioms of T_4 are as follows.

1. Linearly ordered ring axioms.
2. Finite interval.
3. Boolean difference.
4. Duplicate set addition.
5. Scalar multiplication. $(\exists B) (\exists x) (x \in B \wedge (\exists y) (y \in A \wedge x = y \bullet z))$.
6. Squares. $(\exists A) (\exists x) (x \in A \wedge (\exists y) (0 < y \leq y < z \wedge x = y^2))$.
7. Least element.

Axiom 5 asserts that each $c \bullet A$ exists. Axiom 6 asserts that each $\{1^2, 2^2, \dots, n^2\}$, $n \geq 0$, exists.

Lemmas 3.10 - 3.27 refer to provability in T_4 .

LEMMA 3.10. i)-ix) of Lemma 1.1. $A+B$ exists.

Proof: For the first claim, we need only observe that by scalar multiplication, $-A$ exists. From this we obtain that every nonempty set has a greatest element. For the second claim, we can repeat the proof of Lemma 3.5. QED

To show that T_4 is equivalent to T_0 , it suffices to prove that $A \bullet B$ exists in T_4 . We do not know a clean way of doing this. Instead, we recast the proof of Lemma 1.23 for T_4 in order to derive that $A \bullet B$ exists. Much of the proof will be the same. The key point is to avoid use of $|$ in the auxiliary languages, and instead use a monadic predicate for "being a square".

LEMMA 3.11. Let $d \geq 1$ and x be an integer. There exists unique q, r such that $x = dq + r$ and $0 \leq r < d$.

Proof: See Lemma 1.2. QED

LEMMA 3.12. Let $k \geq 0$. The following is provable in T_4 . For all $r \geq 2$, the elements of $[0, r^{k+1})$ have unique representations of the form $n_0 r^0 + \dots + n_k r^k$, where each n_i lies in $[0, r)$. If $n_0 r^0 + \dots + n_k r^k = m_0 r^0 + \dots + m_k r^k$ and each n_i lies in $(-r/2, r/2)$, then each $n_i = m_i$.

Proof: See Lemma 1.3. QED

Until the end of the proof of Lemma 3.21, we fix a standard integer $k > 0$.

LEMMA 3.13. For all $r > 1$, $S[r] = \{n_0 r^0 + n_1 r^2 + \dots + n_i r^{2i} + \dots + n_k r^{2k} : n_0, \dots, n_k \in [0, r)\}$ exists. Every element of $S[r]$ is uniquely written in the displayed form.

Proof: See Lemma 1.4. QED

LEMMA 3.14. For all $r > 1$ and $i \in [0, k]$, $\{x \in S[r] : x[i] = 0\}$ and $\{x \in S[r] : x[i] = 1\}$ exist.

Proof: See Lemma 1.5. QED

LEMMA 3.15. For all $r > 1$ and $i, j, p \in [0, k]$, $\{x \in S[r] : x[i] + x[j] = x[p]\}$ exists.

Proof: See Lemma 1.6. QED

Note that we cannot use Lemma 1.7 here since it involves multiplication of sets, as opposed to just scalar multiplication of sets.

LEMMA 3.16. For all $r > 1$, $i \in [0, k]$, and $A \in [0, r)$, $\{x \in S[r] : x[i] \in A\}$ exists.

Proof: See Lemma 1.8. QED

LEMMA 3.17. For all $r > 1$ and $i \in [0, k]$, $\{x \in S[r] : x[i] \text{ is a square}\}$ exists.

Proof: Use Lemma 3.16 with $A = \{1^2, \dots, r^2\}$. QED

LEMMA 3.18. Let ϕ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $\text{Sq}(x_i)$, $x_i \in A_j$, where $i, j, p \in [0, k]$. The following is provable in T_4 . For all $A_0, \dots, A_k \in [0, r)$, $\{x_0 r^0 + \dots + x_k r^{2k} : \phi \wedge x_0, \dots, x_k \in [0, r)\}$ exists.

Proof: See Lemma 1.9. $Sq(x_i)$ means " x_i is a square". QED

LEMMA 3.19. For all $r > 1$ and $i \in [0, k]$ and $E \in S[r]$, $\{x \in S[r]: (\exists y \in E) (\exists j \in [0, k] \setminus \{i\}) (x[j] = y[j])\}$ exists.

Proof: See Lemma 1.10. QED

LEMMA 3.20. Let ϕ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $Sq(x_i)$, $x_i \in A_j$, where $i, j, p \in [0, k]$. Let $m \in [1, k]$. Let $\psi = (Q_m x_m \in [0, r]) \dots (Q_k x_k \in [0, r]) (\phi)$. The following is provable in T_4 . For all $A_0, \dots, A_k \in [0, r]$, $\{x_0 r^0 + \dots + x_{m-1} r^{2^{m-2}}: \psi \wedge x_0, \dots, x_{m-1} \in [0, r]\}$ exists.

Proof: See Lemma 1.11. QED

LEMMA 3.21. Let $r > 1$, $E \in S[r]$, $i_1 < \dots < i_p \in [0, k]$, and $x_1, \dots, x_p \in [0, r]$. Then $\{y \in S[r]: y[i_1] = x_1 \wedge \dots \wedge y[i_p] = x_p\}$ exists.

Proof: See Lemma 1.12. QED

We now release the fixed standard integer k .

LEMMA 3.22. Let ϕ be a formula without bound set variables whose atomic subformulas are of the form $x_i = 0$, $x_i = 1$, $x_i + x_j = x_p$, $Sq(x_i)$, $x_i \in A_j$. Let y, z be distinct integer variables, where z does not appear in ϕ . Then T_4 proves that $\{y \in [0, z]: \phi^z\}$ exists. Also T_4 proves that $\{y \in [-z, z]: \phi^z\}$ exists.

Proof: See Lemma 1.13. QED

LEMMA 3.23. Let ϕ be a formula without bound set variables whose atomic subformulas are of the form $s = t$, $s < t$, $Sq(t)$, or $t \in A_j$, where s, t are terms without \cdot . Let y, z be distinct integer variables, where z does not appear in ϕ . Then T_4 proves that $\{y \in [-z, z]: \phi^z\}$ exists.

Proof: See Lemma 1.14. QED

We call the formulas given in Lemma 3.23 good formulas.

LEMMA 3.24. Let $x = y^2$, $y \geq 0$. Then the next square after x is $(y+1)^2$, and this is at most $3x+1$.

Proof: Suppose $y^2 < z^2 < (y+1)^2$. We can assume $z \geq 0$. Clearly $y < z < y+1$ since squaring is strictly increasing on the nonnegative integers. For the second claim, first note that $y \leq x$. Then observe that $(y+1)^2 = y^2 + 2y + 1 = x + 2y + 1 \leq 3x + 1$. QED

LEMMA 3.25. $x = y^2$ if and only if x is a square and the next square after x is $x + 2y + 1$. The next square after x is at most $2x + 1$.

Proof: The forward direction is by Lemma 3.24. For the reverse direction, let x be a square and the next square after x is $x + 2y + 1$. Let $x = z^2$. Then the next square after x is $(z+1)^2$. So $(z+1)^2 = z^2 + 2y + 1 = z^2 + 2z + 1$. Hence $y = z$. QED

LEMMA 3.26. There is a good formula ϕ with at most the free variables among x, y , such that the following is provable in T_4 . For all z there exists $z' > z$ such that $(\exists x, y \in [-z, z]) (x = y^2 \wedge \phi^{z'})$.

Proof: Let z be given. We can assume that $z \geq 0$. Let $\phi(x, y)$ be $(y \geq 0 \wedge \text{Sq}(x) \wedge \text{Sq}(x + 2y + 1) \wedge (\exists w) (\text{Sq}(w) \wedge (x < w < x + 2y + 1)))$. Note that ϕ expresses that x is a square, $y \geq 0$, and $x + 2y + 1$ is the next square after x . Note also that when bounded to $[-3z + 1, 3z + 1]$, the meaning remains unchanged. This works for $x, y \in [0, z]$, and can be easily modified to work for $x, y \in [-z, z]$. QED

LEMMA 3.27. There is a good formula ψ with at most the free variables u, v, w , such that the following is provable in T_4 . For all z there exists $z' > z$ such that $(\exists x, y, z \in [-z, z]) (u \cdot v = w \wedge \psi^{z'})$.

Proof: Let z be given. As in the proof of Lemma 1.23, use $\phi = (\exists x, y, a, b) (x = y^2 \wedge y = u + v \wedge a = u^2 \wedge b = v^2 \wedge 2w = x - a - b)$ and Lemma 3.26. We can easily bound the quantifiers to an appropriately chosen $[-z', z']$. QED

Let T_5 be T_4 with Multiples.

THEOREM 3.28. T_0 and T_4 are equivalent. T_1 and T_5 are equivalent.

Proof: It suffices to show that $A \cdot B$ exists within T_4 . Let A, B be given, where $A, B \in [-z, z]$. Then $A \cdot B \in [-z^2, z^2]$, but we don't know yet that $A \cdot B$ exists.

Let z' be according to Lemma 3.27 for z^2 . Then $A \bullet B = \{y \in [-z^2, z^2] : (\exists u, v, w) (u \in A \wedge v \in B \wedge \varphi^{z'})\} = \{y \in [-z^2, z^2] : (\exists u, v, w) (u \in A \wedge v \in B \wedge \varphi)^{z'}\}$ which exists by Lemma 3.23.

The second claim follows immediately from the first. QED

REFERENCES

[Bo65] Karel de Bouvere, *Synonymous theories*, in: *The Theory of Models*, ed. Addison, Henkin, Tarski, North-Holland, 1965, p. 402-406.

[HP98] P. Hajek, P. Pudlak, *Metamathematics of First-Order Arithmetic, Perspectives in Mathematical Logic*, Springer, 1998.

*This research was partially supported by NSF Grant DMS-9970459.