Logique & Analyse **155-156** (1996), 379-387

LINEAR ARITHMETIC DESECSED

John K. SLANEY, Robert K. MEYER and Greg RESTALL

Abstract

In classical and intuitionistic arithmetics, any formula implies a true equation, and a false equation implies anything. In weaker logics fewer implications hold. In this paper we rehearse known results about the relevant arithmetic $\mathbf{R}^{\#}$, and we show that in linear arithmetic $\mathbf{LL}^{\#}$ by contrast false equations never imply true ones. As a result, linear arithmetic is *desecsed*. A formula A which entails $0 = 0$ is a *secondary equation*; one entailed by $0 \neq 0$ is a *secondary unequation*. A system of formal arithmetic is *secsed* if every extensional formula is either a secondary equation or a secondary unequation. We are indebted to the program MaGIC for the simple countermodel **SZ7**, on which $0 = 1$ is not a secondary formula. This is a small but significant success for automated reasoning.

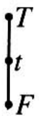
Question: when does one equation between natural numerals imply another? Answer: it depends on your logic. Keeping the purely arithmetical part of number theory fixed, it is part of the function of logic to confer a sense upon 'imply', so that changes in logic may change the implication relation between extensional propositions such as equations. In this paper we show that for a range of substructural logics including all subsystems of the linear logic of [3] numerical equations *never* imply other equations unless the two equations are rather trivially equivalent.

In order to fix the discussion, let us focus on first order theories of arithmetic couched in a language $\mathbf{L}^{\#}$ which is built up as usual from numerals including 0 (zero) and variables with term-forming operators $'$ (successor), + (plus) and . (times), one binary predicate symbol = to form equations between terms, universal and existential quantifiers $\forall x_i$ and $\exists x_i$ respectively and the standard logical connectives $\wedge$ (and), $\vee$ (or), $\rightarrow$ (implies) and $\circ$. This last connective is the multiplicative (intensional) 'and' known in the linear logic literature as tensor product and in the relevant logical literature as fusion. An arithmetical theory $\mathbf{S}^{\#}$ is based on a logic $\mathbf{S}$ whose theorems are at least closed under the rules of detachment for $\rightarrow$, adjunction for $\wedge$ and generalisation for $\forall$. In addition to the logical theorems, and to closure under the primitive logical rules of inference, arithmetic has the special postulates:

(Id=)	$x = x$
(Sym=)	$x = y \rightarrow y = x$
(Tr=)	$x = y \rightarrow (y \doteq z \rightarrow x = z)$
(Sfun)	$x = y \rightarrow x' = y'$
(Sinj)	$x' = y' \rightarrow x = y$
(Succ)	$x' \neq 0$
(0+)	$x + 0 = x$
(S+)	$x + y' = (x + y)'$
(0×)	$x.0 = 0$
(S×)	$x.y' = x.y + x$
(Rul-**MI**)	from $A(0)$ and $\forall x(A(x) \rightarrow A(x'))$ to infer $A(x)$

These are just the normal Peano-Dedekind axioms and rules for first order natural arithmetic, expressed in a form which allows some freedom to vary the logical basis.

Classically and intuitionistically, of course, the answer to our opening question is trivial: $a = b \rightarrow c = d$ is a theorem of arithmetic if and only if either a and b are distinct numerals or c and d are not. In various substructural logics, however, matters are more interesting. It has long been known that in the relevant arithmetic $\mathbf{R}^{\#}$ such an implication is provable iff $|a - b|$ divides $|c - d|$, though to the best of our knowledge no proof has been published.



A	$\sim A$
F	T
t	t
T	F

$\circ$	F	t	T
F	F	F	F
t	F	t	T
T	F	T	T

$\rightarrow$	F	t	T
F	T	T	T
t	F	t	T
T	F	F	T

Figure 1: RM3 matrix and Hasse diagram

In one direction it is obvious in virtue of the theorem $x = y \rightarrow k.x = k.y$ for constant k. For the other direction, let the absolute difference between a and b be m and let that between c and d be n. Suppose m does not divide n. Then consider the propositional structure characteristic of the logic RM3, as given in Figure 1. We may interpret $\mathbf{R}^{\#}$ in this structure by letting the domain consist of the integers modulo m, letting the true equations (modulo m) take the value **t** and the false ones the value **F**. It is reasonably well known that this gives a model of $\mathbf{R}^{\#}$ (see for example [10]). Of course, the model verifies some contradictions, such as the assertion that 0 both is and is not a successor, but the propositional structure provides a paradoxical value $\mathbf{t}$ which is a fixed point for negation and so appropriate for such assertions. Whatever we might make metaphysically of that, note that *some* equations at least are not verified, among them $c = d$ since c and d are not congruent mod m. Since $a = b$ gets the value $\mathbf{t}$ which does not imply $\mathbf{F}$, the implication $a = b \rightarrow c = d$ is falsified.

Since relevant logic is a supertheory of linear logic, this divisibility condition is also necessary for linear implication between equations. It is not sufficient, however, as the following model demonstrates. Let $\mathfrak{Z}^*$ be the integers together with an upper bound $\top$ and a lower bound $\bot$. The operations of addition and subtraction are easily extended to the infinite elements. Where x, a and b are elements of $\mathfrak{Z}^*$ such that $a \neq \bot$ and $b \neq \top$:

$$\begin{array}{lclcl} x + \bot & = & \bot & = & \bot + x \\ a + \top & = & \top & = & \top + a \\ \top - x & = & \top & = & x - \bot \\ b - \top & = & \bot & = & \bot - a \end{array}$$

This is a complete lattice under the usual (total) numerical order, and thus a lattice ordered monoid under the extended addition. The logical connectives may be interpreted very naturally in this structure: $\wedge$ and $\vee$ as lattice meet and join, $\circ$ as addition, and $x \rightarrow y$ as $y - x$. Taking the true propositions to be those elements in the positive cone (0 or greater), this is a model of the additive and multiplicative fragment of linear logic. For this purpose, negation may be defined by selecting an arbitrary integer to interpret $\mathbf{f}$ and defining $\sim x$ as $x \rightarrow \mathbf{f}$. Regardless of the value of $\mathbf{f}$ this makes negation a dual automorphism of period 2 on the lattice, as required by the negation postulates of linear logic. Canonically, $\mathbf{f}$ may be identified with $\mathbf{t}$ (that is, with 0) but this is not mandatory.[1]

We may interpret arithmetic in the standard model on this propositional structure, letting each numeral designate its proper number and interpreting successor, addition and multiplication as what they should be. We assign the value $-|a - b|$ to the equation $a = b$. It is clear (subject to the usual leap of faith concerning (Rul-**MI**)) that all postulates of linear arithmetic are satisfied in this model, provided $\mathbf{f} \geq -1$, and that $a = b \rightarrow c = d$ is true therein iff $|a - b| \geq |c - d|$. Put together with the earlier observation concerning relevant logic, this entails that an implication between *false* equations $a = b$ and $c = d$ holds only if $|a - b| = |c - d|$.

[1] The use of the integers as a propositional structure is explored in detail in [11].

The status of *true* equations, however, is still special. Since every number divides zero, $\mathbf{R}^{\#}$ has the property that all equations imply all true equations, and in particular that they imply the paradigm true equation $0 = 0$. The model of linear arithmetic just exhibited also validates the implication $x = y \rightarrow 0 = 0$, prompting the question of how far into the weaker substructural logics this property extends.

A logic needs to have this property if arithmetics based on that logic are to be "secsed". That is, if their zero-degree formulas are secondary formulas. Recall that a zero-degree formula as defined in [1] is one in which $\rightarrow$ and $\circ$ do not occur. Secondary formulas are defined as follows:

(SEQ) A is a *secondary equation* of $\mathbf{S}^{\#}$ iff $\mathbf{S}^{\#} \vdash A \rightarrow 0 = 0$
(SUQ) A is a *secondary unequation* of $\mathbf{S}^{\#}$ iff $\mathbf{S}^{\#} \vdash 0 \neq 0 \rightarrow A$
(SEC) A is a *secondary formula* of $\mathbf{S}^{\#}$ iff it is either a secondary equation or a secondary unequation of $\mathbf{S}^{\#}$

Then we say that $\mathbf{S}^{\#}$ is secsed provided that all zero-degree formulas of $\mathbf{L}^{\#}$ are secondary formulas; otherwise $\mathbf{S}^{\#}$ is desecsed. Note that the Peano arithmetic of any logic which allows weakening

(**K**) $A \rightarrow (B \rightarrow A)$
(**K**~) $A \rightarrow ({\sim}A \rightarrow B)$

is secsed, just because $0 = 0$ is a theorem and $0 \neq 0$ is the negation of a theorem.

The relevant Peano arithmetics $\mathbf{R}^{\#}$ and $\mathbf{E}^{\#}$, and their "true" extensions $\mathbf{R}^{\#\#}$, $\mathbf{E}^{\#\#}$, and $\mathbf{TE}^{\#}$ [4, 5, 7, 9] are also secsed. We show this by structural induction on zero-degree formulas, noting first that all equations $u = v$ entail $0 = 0$, satisfying (SEQ); whence by contraposition their negations (i.e., the unequations) satisfy (SUQ); by induction this result extends to all zero-degree formulas.[2]

But the base step of this induction depends ineluctably on contraction. Here is the argument for $\mathbf{R}^{\#}$:

(1) $x = y \rightarrow (x = y \rightarrow x = x)$ Symmetry & transitivity of =
(2) $x = y \rightarrow x = x$ (1), Contraction, $\rightarrow$ E
(3) $x = x \rightarrow 0 = 0$ Subtraction
(4) $x = y \rightarrow 0 = 0$ (2), (3), Transitivity of provable $\rightarrow$

[2] In the relevant arithmetics, unlike the classical and intuitionist cases, it does not extend to *all* formulas. For instance, $0 = 1 \rightarrow 0 = 1$ is not a secondary formula in $\mathbf{R}^{\#}$.

The fact that $\mathbf{R}^{\#}$ in particular is secsed was used in [5,6] to obtain useful results on the strength of relevant arithmetic. In particular, we can provide an exact translation τ from classical Peano arithmetic $\mathbf{P}^{\#}$ into $\mathbf{R}^{\#}$ by setting $\tau(u = v)$ to be $(u = v) \vee (0 \neq 0)$ and by keeping the interpretation of the extensional connectives fixed (so $\tau(A \wedge B)$ is $\tau(A) \wedge \tau(B)$ and so on). Then it can be shown that $\tau(A)$ is provable in $\mathbf{R}^{\#}$ if and only if A is provable in $\mathbf{P}^{\#}$, essentially because $\tau(A)$ is equivalent either to $(A \wedge \mathbf{t}) \vee \mathbf{f}$ or to $(A \vee \mathbf{f}) \wedge \mathbf{t}$, and because the rule γ of material detachment is admissible for formulas of these forms.

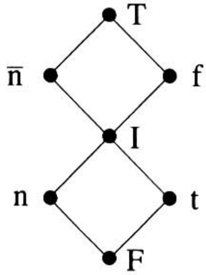


Figure 2: DeMorgan lattice underlying **SZ7**

Restall hastily conjectured that the argument could be fixed to work in contraction-free systems, such as those studied in [14, 12, 13]. Meyer doubted that a contraction-free proof could be found to get from step (1) to step (2). When he mentioned this to Slaney he was greeted with, "Let's find a countermodel."[3] Here is the result of that conversation.

Consider the DeMorgan lattice shown in Figure 2. The partial order $\leq$ and the lattice connectives $\wedge$ and $\vee$ are determined on this lattice by the Hasse diagram just exhibited. We define the implication $\rightarrow$ and fusion $\circ$ of the associated propositional structure **SZ7** by the tables shown in Figure 3, taking negation $\sim x$ as $x \rightarrow \mathbf{f}$. **SZ7** was found by the program MaGIC [15], as a simplification of a 10 element matrix that Slaney and Meyer had found by hand.

[3] Meyer views such greetings with great respect. While still a student at Pitt, he conjectured to Belnap that such-and-such a formula was a non-theorem of **R**. "Let's make up a matrix to refute it," continued Belnap. And he did (to Meyer's amazement, since it had not occurred to him that even a graduate student could make up a matrix of his very own; these days, even a computer can, again thanks in part to Belnap).

$\rightarrow$	F	n	t	I	f	$\bar{n}$	T
F	T	T	T	T	T	T	T
n	F	t	n	I	$\bar{n}$	f	T
$*t$	F	n	t	I	f	$\bar{n}$	T
$*I$	F	F	F	I	I	I	T
$*f$	F	F	F	F	t	n	T
$*\bar{n}$	F	F	F	F	n	t	T
$*T$	F	F	F	F	F	F	T

$\circ$	F	n	t	I	f	$\bar{n}$	T
F	F	F	F	F	F	F	F
n	F	t	n	I	$\bar{n}$	f	T
$*t$	F	n	t	I	f	$\bar{n}$	T
$*I$	F	I	I	I	T	T	T
$*f$	F	$\bar{n}$	f	T	T	T	T
$*\bar{n}$	F	f	$\bar{n}$	T	T	T	T
$*T$	F	T	T	T	T	T	T

Figure 3: Implication and fusion matrices for **SZ7**

The countermodel in **SZ7** has as domain the integers mod 2, with atomic sentences interpreted under the function I as follows:

(It) $I(0 = 0) = I(1 = 1) = \mathbf{t}$

(In) $I(0 = 1) = I(1 = 0) = \mathbf{n}$

I is then extended to all sentences on the obvious homomorphism. Note that, mod 2, we can interpret the quantifiers by simple substitution; i.e.,

(I∀) $\mathrm{I}(\forall xAx) = I(A0) \wedge I(A1)$

(I∃) $\mathrm{I}(\exists xAx) = I(A0) \vee I(A1)$

On this interpretation I, we refute the universal generalization of (2) because

(2I) $I(0 = 1 \rightarrow 0 = 0) = \mathbf{n} \rightarrow \mathbf{t} = \mathbf{n}$, which fails because **n** is undesignated. On the other hand readers may amuse themselves by verifying (Sym=) and (Tr=) for all values of x,y,z in $\{0,1\}$.

Evidently contraction-free arithmetics $\mathbf{S}^\#$ are desecsed, provided that the function I just defined in **SZ7** provides a sound interpretation. Sufficient for this is that axioms and rules of $\mathbf{S}^\#$ be taken from the arithmetical ones given above and any among the following:[4]

(**LL**)	Any theorems of linear logic.
(Ax$\wedge\vee$)	$A \wedge (B \vee C) \rightarrow (A \wedge B) \vee (A \wedge C)$
(Ax**BWW**)	$(A \rightarrow (A \rightarrow (A \rightarrow B))) \rightarrow (A \rightarrow B)$[5]
(Ax$\vee{\sim}$)	$A \vee {\sim}A$
(Ax$\circ\vee$**F**)	$(A \circ A) \vee (A \rightarrow B)$
(Ax$\vee\rightarrow{\sim}$)	$(A \rightarrow {\sim}A) \vee ({\sim}A \rightarrow A)$
(Ax$\wedge\vee{\sim}$)	$A \wedge {\sim}A \rightarrow B \vee {\sim}B$
(Ax$\wedge\exists$)	$A \wedge \exists xB \rightarrow \exists x(A \wedge B)$, if x is not free in A
(Ax$\forall\vee$)	$\forall x(A \vee B) \rightarrow A \vee \forall xB$, if x is not free in A
(Rul-ω)	From $A0, A1 \ldots An \ldots$ for all numerals n, to infer $\forall xAx$
(**Uneq**)	Any unequations of the form $t \neq u$.

We note that all universal closures of the suggested axioms take designated values on I in **SZ7**, and that the suggested rules preserve this property. Moreover, we can accomodate a Girard style necessity ('of course') operator '!' and possibility ('why not') operator '?' on interpretation in **SZ7** as follows:

(I!)	If $\mathbf{t} \leq I(A)$ then $I(!A) = \mathbf{t}$ else $I(!A) = \mathbf{F}$
(I?)	If $I(A) \leq \mathbf{f}$ then $I(?A) = \mathbf{f}$ else $I(?A) = \mathbf{T}$

Note that these schemes make the following axiom schemes and rules also valid on I

(Ax!**K**)	$A \rightarrow (!B \rightarrow A)$
(Ax!**W**)	$(!A \rightarrow (!A \rightarrow B)) \rightarrow (!A \rightarrow B)$

[4] Conventions for reading formulas are as follows: unary operators have minimal scope; binary connectives are ranked $\wedge$, $\circ$, $\vee$, $\rightarrow$, in order of increasing scope.

[5] (Ax**BWW**) is as close to contraction as we can get while staying valid in **SZ7**. Its deductive equivalent in **LL** is $A \rightarrow A \circ A \circ A$. We note incidentally that the strong near-contraction postulate $A \circ B \rightarrow A \circ A \circ B \vee A \circ B \circ B$ which is not valid in **SZ7** may nonetheless be added to $\mathbf{LL}^\#$ without secsing the system.

(Ax!E)	$!A \rightarrow A$
(Ax!!I)	$!A \rightarrow\ !!A$
(Ax!$\rightarrow$)	$!(A \rightarrow B) \rightarrow (!A \rightarrow\ !B)$
(Rul!I)	From A to infer $!A$

Of course (and indeed why not) many non-theorems of **LL**$^{\#}$ are also validated by **SZ7** and therefore do not resecs arithmetic. These include:

(Ax!$\wedge$)	$!A \wedge\ !B \rightarrow\ !(A \wedge B)$
(Ax?$\vee$)	$?(A \vee B) \rightarrow\ ?A \vee\ ?B$
(Ax!$\forall$)	$!\forall xA \leftrightarrow \forall x!A$
(Ax?$\exists$)	$?\exists xA \leftrightarrow \exists x?A$
(Ax?)	$?A$
(Ax!~)	$!(0 = 1) \rightarrow A$

The result is the desecsing of all of linear arithmetic, in the sense that any formal arithmetic got by adding axioms and rules from the above lists to **LL**$^{\#}$ will contain zero-degree formulas that are not secondary formulas. Indeed, we may strengthen the logic far beyond **LL**, as noted above. Our crucial matrix **SZ7** was found by a computer program; MaGIC confirms that there is no way to improve on it, in the sense that there is no smaller matrix satisfying the postulates of **LL**$^{\#}$ while remaining desecsed.

We must add just a little book-keeping before resting from our labours. Our countermodel showed that $0 = 1 \rightarrow 0 = 0$ fails in **LL**$^{\#}$ and related systems. It also shows that $n = m \rightarrow 0 = 0$ fails whenever n and m differ by an odd number. But it is easy to check that $n = m \rightarrow 0 = 0$ is true when n and m differ by an even number. However this was an artefact of how we constructed the model out of the integers mod 2. Consider instead, the integers mod k, and define $I(m = n) = \mathbf{t}$ when $m = n$, and $I(m = n) = \mathbf{n}$ otherwise. The rest of the evaluation is just as before: the universal quantifier is a long, finite, conjunction, and each of the arithmetic axioms and rules holds under this interpretation. And now, $I(n = m \rightarrow z = z) = \mathbf{n} \rightarrow \mathbf{t} = \mathbf{n}$ whenever $m \neq n$ mod k. As a result, *no* false equation implies any true equation. Linear logic is therefore *thoroughly desecsed*, in that no false equation is a secondary equation, and dually, no true unequation is a secondary unequation. The same goes for any weaker system. In all such arithmetics, $a = b$ implies $c = d$ iff $|a — b| = |c — d|$.[6]

[6] Thanks to many past and present colleagues in the ANU automated reasoning project, and its predecessor the ANU logic group; we are especially indebted to Dunn, Belnap, Martin, Mortensen, Priest, and Sylvan. Thanks too to Surendonk for help in preparing the manuscript.

REFERENCES

[1] Anderson, A. R., N. D. Belnap, Jr., and J. M. Dunn, *Entailment, vol. II*. Princeton, 1992.

[2] Curry, H. B., *Foundations of mathematical logic*. New York, 1963.

[3] Girard, J.-Y., Linear logic. *Theoretical Computer Science* 50 (1987) 1-102.

[4] Meyer, R. K., Intuitionism, Entailment, Negation. Leblanc (ed) *Truth, Syntax and Modality*. Amsterdam, 1973, 168-198.

[5] Meyer, R. K., Arithmetic Formulated Relevantly. Canberra, 1976. (Some of the results appear in [1].)

[6] Meyer, R. K., The Consistency of Arithmetic. Canberra, 1976.

[7] Meyer, R. K., Relevant arithmetic (abstract). *Bulletin of the section of logic* 5 (1976) 133-137.

[8] Meyer, R. K., $\supset$E is admissible in "true" relevant arithmetic. *Journal of Philosophical Logic* forthcoming.

[9] Meyer, R. K., and G. Restall, "Strenge" arithmetics. Canberra, 1996.

[10] Meyer, R. K. and C. E. Mortensen, Inconsistent Models for Relevant Arithmetics. *Journal of Symbolic Logic* 49 (1984) 917-929.

[11] Meyer, R. K., and J. K. Slaney, Abelian Logic (from A to Z). Priest, Routley and Norman (eds), *Paraconsistent Logic: Essays on the Inconsistent*. Munich, 1989, 245-288.

[12] Restall, G., Arithmetic and truth in Lukasiewicz's infinitely valued logic. *Logique et Analyse* 139-140 (1992) 303-312.

[13] Restall, G., *Logics without contraction*. PhD thesis, University of Queensland, 1994.

[14] Slaney, J. K., The square root of 2 is irrational (and no funny business). Typescript, 1982.

[15] Slaney, J. K., *MaGIC, Matrix Generator for Implication Connectives: release 2.1 notes and guide*. Technical Report TR-ARP-11-95, ANU, Canberra, 1995, ftp://arp.anu.edu.au/pub/techreports.