Kripke, Belnap, Urquhart and Relevant Decidability & Complexity

"Das ist nicht Mathematik. Das ist Theologie."

Jacques Riche[1] and Robert K. Meyer[2]

[1] Department of Computer Science, Katholieke Universiteit Leuven, Belgium
riche@cs.kuleuven.ac.be
[2] Automated Reasoning Project, RSISE, Australian National University, Australia
rkm@arp.anu.edu.au

Abstract. The first philosophically motivated sentential logics to be proved *undecidable* were relevant logics like **R** and **E**. But we deal here with important decidable fragments thereof, like $\mathbf{R}_{\rightarrow}$. Their decidability rests on S. Kripke's gentzenizations, together with his central combinatorial lemma. Kripke's lemma has a long history and was reinvented several times. It turns out equivalent to and a consequence of Dickson's lemma in number theory, with antecedents in Hilbert's basis theorem. This lemma has been used in several forms and in various fields. For example, Dickson's lemma guarantees termination of Buchberger's algorithm that computes the Gröbner bases of polynomial ideals. In logic, Kripke's lemma is used in decision proofs of some substructural logics with contraction. Our preferred form here of Dickson-Kripke is the Infinite Division Principle (IDP). We present our proof of IDP and its use in proving the finite model property for $\mathbf{R}_{\rightarrow}$.

1 Introduction

The Patron Saint of the Logicians Liberation League is Alasdair Urquhart, whose SECOND miracle was his proof that the major relevant logics of [AB75,ABD92] are *undecidable*. But our chief concerns in this paper are pre-Urquhart. We shall examine decidable fragments of the major relevant logics (especially **R**) and dwell on the combinatorics underlying their decision procedures, mainly the Dickson's, Kripke's and Meyer's lemmas and their ancestor, Hilbert's finite basis theorem. The main proofs in this paper are that of the IDP and the finite model property for some decidable fragments. We shall also mention briefly Urquhart's further results on the computational complexity of the decision procedures based on such principles.

The FIRST substructural logic was the system $\mathbf{R}_{\rightarrow}$ of pure relevant implication.[1] And no sooner had $\mathbf{R}_{\rightarrow}$ been seriously proposed than the question of

[1] $\mathbf{R}_{\rightarrow}$ was introduced by Moh-Shaw-Kwei and by Church circa 1950, e.g. in [Ch51]. But Došen [Do92] dug up [Or28], which basically already had relevant arrow, negation and necessity.

G. Gottlob, E. Grandjean, K. Seyr (Eds.): CSL'98, LNCS 1584, pp. 224–240, 1999.

its decidability arose. Indeed, Curry's early review [CuC53] with Craig of [Ch51] claimed (mistakenly) that decidability of $\mathbf{R}_{\rightarrow}$ was straightforward. But this was *not* confirmed by Belnap, when he successfully accepted the challenge of Robert Feys to "Gentzenize" the kindred pure calculus $\mathbf{E}_{\rightarrow}$ of entailment. For while Belnap did at that time invent the "merge" consecution calculi for various relevant logics (see [AB75]), the usual (trivial?) consequences (such as decidability) of successful Gentzenization were NOT forthcoming.

Enter then young Saul Kripke, who interested himself in these decision problems at about this time (late 1950's). He just dropped the weakening rule *K from a Gentzenization $\mathbf{LJ}_{\rightarrow}$ for pure intuitionist implication, producing one $\mathbf{LR}_{\rightarrow}$ for $\mathbf{R}_{\rightarrow}$.[2] But the usual moves from Kripke's $\mathbf{LR}_{\rightarrow}$ *failed* to produce decidability for $\mathbf{R}_{\rightarrow}$. Clearly some stronger medicine was in order. We look in succeeding sections at that medicine.

2 Gentzen and Hilbert Systems.

2.1 Gentzenizing $\mathbf{R}_{\rightarrow}$ at first

Let our first formulation $\mathbf{LR1}_{\rightarrow}$ of $\mathbf{LR}_{\rightarrow}$ be as follows:[3] We adopt the usage of [AB75] in speaking of *consecutions*, which are of the form

$$\alpha \vdash A \tag{1}$$

where α is a *multiset* of formulas and A is a formula.[4] Axioms are all formulas

(AX) $A \vdash A$

While the classical and intuitionist rule of weakening *K has been chopped from among the rules,[5] the structural rule *W of contraction remains.

(*W) $\alpha, A, A \vdash C \Longrightarrow \alpha, A \vdash C$

We state for the record what the rule *C of permutation would look like (had we chosen sequences rather than multisets as the data type of α).

[2] We follow the conventions of [Cu63] in naming rules. And we present 2 formulations of $\mathbf{LR}_{\rightarrow}$ in the next section.

[3] We also follow [Cu63] on matters notational. I.e., we use $\vdash$ as our Gentzen predicate and commas for multiset union; we associate equal connectives to the LEFT. This frees $\Longrightarrow$ for another purpose, whence we write things like "P and $Q \Longrightarrow R$" to indicate the RULE that has P and Q as premisses and R as conclusion.

[4] It is possible to follow Gentzen and Curry in taking α as a *sequence* of formulas. But in view of the rule *C of permutation for sequences it is more elegant to choose a data type that builds in *C. Multisets fill the bill, as we suggested with McRobbie in [MM82] and implemented with him and Thistlewaite in [TMM88].

[5] *K is the rule $\alpha \vdash C \Longrightarrow \alpha, A \vdash C$.

(*C) $\alpha, A, B, \beta \vdash C \Longrightarrow \alpha, B, A, \beta \vdash C$

Operational rules *→* introduce → on left and right respectively.

(*→) $\beta \vdash A$ and $\alpha, B \vdash C \Longrightarrow \alpha, A \rightarrow B, \beta \vdash C$

(→ *) $\alpha, A \vdash B \Longrightarrow \alpha \vdash A \rightarrow B$

The VALID CONSECUTIONS of $\mathbf{LR}_{\rightarrow}$ are just those that may be obtained from (AX) using rules from among *W and *→*. The following CUT rule is moreover admissible:

(CUT) $\beta \vdash A$ and $\alpha, A \vdash C \Longrightarrow \alpha, \beta \vdash C$

Using CUT, it is straightforward to establish the equivalence of $\mathbf{LR}_{\rightarrow}$ and the Hilbert-style axiomatic version of $\mathbf{R}_{\rightarrow}$ set out in [Ch51] and below.

Alas, it is also easy to see why decidability remains a problem. For consider a candidate consecution, say $A \vdash C$. Of course this could have come by *W from $A, A \vdash C$, and, continuing in this vein, we are clearly "off to the races".

If we are to get a decision procedure for $\mathbf{LR}_{\rightarrow}$, some combinatorial insight is in order. But we are pleased nonetheless by Kripke's invention of $\mathbf{LR1}_{\rightarrow}$, which we take to agree with the philosophical motivation for dropping the "thinning" rule *K. The mate of *K in the Hilbert-style axiomatization of $\mathbf{R}_{\rightarrow}$ is the Positive Paradox axiom A7 below.

2.2 Automating the search for an *associative* operation.

One main early use of theorem proving techniques in relevant logics was related to the decision problem for **R**, a logically important, technically difficult and long open problem. The full system **LR**, closely related to **R**, was known to be decidable. There were reasons to think that **R** was undecidable and there were reasons to think that a theorem prover based on **LR** could help to establish this negative solution for the decision problem of **R**.
For more on relevant automated reasoning, see [TMM88].[6] The leading idea for showing **R** undecidable relied on a technique suggested by Meyer for coding the word problem for semigroups into **R**. The hope was that, since the former is undecidable, so also is the latter.[7] Translating the semigroup operations into the **R** connectives, the problem reduced to finding a binary connective $\oplus$ corresponding to semigroup multiplication which is *freely* associative. That is, the

[6] This book is based on the ANU Ph.D. thesis of Paul Thistlewaite, in which with McRobbie and Meyer he describes his computer program *KRIPKE*. The program was so named by McRobbie, because it implements Kripke's decision procedure for $\mathbf{R}_{\rightarrow}$ and other systems related to **LR**.

[7] The hope has *paid off*, though not quite as envisaged. For the argument of [Ur84] eventually finds an undecidable semigroup hidden in **R**. But Urquhart found it *more deeply* hidden than Meyer ever supposed.

subalgebra of the Lindenbaum algebra of **R** generated by the first n (congruence classes of) propositional variables under $\oplus$ was to be the *free* semigroup with n generators. Of course the $\oplus$ thus found cannot be commutative nor idempotent, nor have any other special properties beyond associativity.
Possible definitions of such a connective were generated. Those proved in decidable **LR** could not define the free connective wanted for **R**. The remaining candidates had then to be checked to see whether they define an associative connective in **R**. The theorem prover *KRIPKE* had already proved associative 16 candidate definitions of such a connective in **LR**. But then A. Urquhart's proof of undecidability of **R** suspended this specific research and made of **R**, as Urquhart notes, the first independently motivated undecidable propositional logic.
Nevertheless, the technical problem of defining an associative connective (i.e. to automatically prove associativity of all candidates in **LR** and **R**) still remains a challenge for the automated theorem proving community. Granted, it is important not to miss the *point* of the exercise. But Urquhart, who did see its point, continues to hold it an interesting question whether a freely associative operation is definable in **R**. He, and we, do not know.

2.3 Tuning $\mathbf{LR}_{\rightarrow}$ for decidability.

When its authors put together [BW65], they extended to the system with negation work that Kripke had done for the pure system $\mathbf{E}_{\rightarrow}$. While this extension is itself non-trivial,[8] the hardest and most imaginative part of [BW65] seems to us the work reported in [Kr59].

We shall mainly follow the Kripke-Belnap-Wallace strategy here, "building *W into the rules" to set out a consecution calculus $\mathbf{LR2}_{\rightarrow}$, with the same theorems as $\mathbf{LR1}_{\rightarrow}$. This is the weather that we know how to control, along the lines that we set out with Thistlewaite and McRobbie in [TMM88].

$\mathbf{LR2}_{\rightarrow}$ is our second formulation of $\mathbf{LR}_{\rightarrow}$. It will have NO structural rules. Though in order to ensure that $\mathbf{LR2}_{\rightarrow}$ will have the same theorems as $\mathbf{LR1}_{\rightarrow}$ (and so of $\mathbf{R}_{\rightarrow}$, on interpretation), clearly *W will have to be *admissible*. First, we leave the axioms and the rule $\rightarrow$* as they were in $\mathbf{LR1}_{\rightarrow}$. In compensation we complicate *$\rightarrow$. The clear invertibility of $\rightarrow$* enables us to insist that the *succedent C of the conclusion* of *$\rightarrow$ shall be a *propositional variable* p in $\mathbf{LR2}_{\rightarrow}$.[9] Then we state the rule for building in contraction with a care that we hope is optimal. A useful theft from [TMM88] is a counting function c, which keeps track of the *number of occurrences* of each formula D in the multiset γ. I.e.,

Unit: c(D;D) = 1.
Zero: If D does not occur in γ, c(D;γ) = 0.

[8] It involves what Meyer dubs "Belnap's Crazy Interpretation Theorem," in order to show that the Gentzen system is in an appropriate sense a subsystem of the Hilbert system for $\mathbf{E}_{\rightarrow}$.

[9] We borrow this trick from Kit Fine, who used in another context with E. P. Martin something similar.

Union: Let γ be the *multiset union* of γ_1 and γ_2. Then c(D;γ) = c(D;γ_1) + c(D;γ_2).

Now we build in *W *very carefully* for maximal efficiency into *→. So here is the rule for $\mathbf{LR2}_{\rightarrow}$.

$$(^*\!\!\rightarrow) \quad \alpha \vdash A \text{ and } \beta, B \vdash p \Longrightarrow \gamma, A \rightarrow \ B \vdash p,$$

where p is a propositional variable and the multiset γ is subject to the following constraints:[10]
We require for each formula D, if D $\neq A \rightarrow B$,

1. c(D;γ) = 0 iff c(D;α) = 0 and c(D;β) = 0
2. if c(D;γ) = 1 then either
   (a) c(D;α) = 0 and c(D;β) = 1, or
   (b) c(D;α) = 1 and c(D;β) = 0, or
   (c) c(D;α) = 1 and c(D:β) = 1
3. if c(D;γ) > 1 then c(D;γ) = c(D;α) + c(D;β)

For the particular formula $A \rightarrow B$, if c(A→B;γ) = 0 then either

1. c(A→B;α) = 0 and c(A→B;β) = 0, or
2. c(A→B;α) = 1 and c(A→B;β) = 0, or
3. c(A→B;α) = 0 and c(A→B;β) = 1, or
4. c(A→B;α) = 1 and c(A→B;β) = 1

To be sure, A→B may occur PROPERLY in the multiset γ which is part of the CONCLUSION of the revised *→ rule of $\mathbf{LR2}_{\rightarrow}$. But it is then one of the formulas D already considered above, and is subject to the corresponding constraints there laid down.[11]

2.4 Relevant Hilbert systems.

We are mainly interested in the Relevant system $\mathbf{R}_{\rightarrow}$. But we also mention some other *pure implicational* fragments of Relevant (and related) Logics. These may be axiomatized as follows. (The letter following the name of an axiom is its corresponding combinator.) $\mathbf{T}_{\rightarrow}$: $A1-A4$; $\mathbf{E}_{\rightarrow}$: $A1-A5$; $\mathbf{R}_{\rightarrow}$: $A1-A6$. $\mathbf{J}_{\rightarrow}$: $A1-A7$. **BCK** and **BCI** (using combinatory axioms B, C, K and I to characterize them)

[10] The purpose of these constraints is to render *W admissible while stoutly resisting *K.

[11] Note that we are here treating *→ in $\mathbf{LR2}_{\rightarrow}$ EXACTLY ANALOGOUSLY to how Po'' is treated on p. 53ff. of [TMM88]. So the proof that exactly the same consecutions $\alpha \vdash A$ are provable in $\mathbf{LR1}_{\rightarrow}$and $\mathbf{LR2}_{\rightarrow}$ will be analogous as well to Thistlewaite's proof in [TMM88] that the formulations $L1$ and $L5$ of **LR** are deductively equivalent.

are other well known systems.[12]

Axioms.

A1.	$A \to A$	Identity (I)
A2.	$(A \to B) \to ((B \to C) \to (A \to C))$	Suffixing (B')
A3.	$(A \to B) \to ((C \to A) \to (C \to B))$	Prefixing (B)
A4.	$(A \to (A \to B)) \to (A \to B)$	Contraction (W)
A5.	$((A \to A) \to B) \to B$	Specialized assertion (CII)
A6.	$(A \to (B \to C)) \to (B \to (A \to C))$	Permutation (C)
A7.	$A \to (B \to A)$	Positive Paradox (K)

and the deduction rule schema:

R1. $\vdash A \to B$ and $\vdash A \implies \vdash B$ Modus Ponens

The axiomatic and consecution formulations of the system $\mathbf{R}_{\to}$ are equivalent. A formula is provable in the Gentzen system iff it is provable in the axiomatic system.
Note that the consecution formulations of the systems $\mathbf{E}_{\to}$ and $\mathbf{T}_{\to}$ impose some restrictions on the rules.

3 Decidability.

As we have indicated, the decision problem for the implicational fragments of **E** and **R** is difficult.[13] We briefly summarize the main steps of the procedure, which were worked out via a "combinatorial lemma" and that underlay the claims of [Kr59]. See also [BW65], [AB75], [Du86], [TMM88].

Suppose that a given formula A is to be proved. Applying the rules (in reverse), a proof search tree for $\vdash A$ is constructed in $\mathbf{LR2}_{\to}$. The basic idea of this formulation of $\mathbf{LR}_{\to}$ is to restrict the application of the contraction rule.

[12] **BCI** corresponds to the implicational fragment of Linear Logic. And we note for the reader's logical pleasure that he/she/it may achieve fame and fortune by solving the *decision problem* for $\mathbf{T}_{\to}$. Having been around since *circa* 1960, this is the most venerable problem in all of relevant logic. And a clue would appear to lie in the principle of commutation of antecedents. $\mathbf{R}_{\to}$, which admits the principle, is decidable; even $\mathbf{E}_{\to}$ admits *enough* commutativity to be decidable. $\mathbf{T}_{\to}$ would seem to have *some* useful permutation of antecedents; e.g., the B and B' axioms result from each other by permutation. But these facts have not yet proved enough to apply to $\mathbf{T}_{\to}$ the Kripke methods that work for other pure relevant logics.

[13] There are *simpler* related problems. For example, the first-degree entailment fragment in which the formulas are of type $A \to B$, where A, B are of degree zero, has a simple decision procedure: there is a four-valued Smiley matrix which is characteristic for the fragment. The zero-degree fragment of **R** and **E** is strictly equivalent to classical propositional logic with truth-values as characteristic model.

And we say that a multiset β *reduces* to γ if γ can be obtained from β by a series of applications of the rule of contraction. Similarly we may say that a consecution $\beta \vdash B$ reduces to one $\gamma \vdash B$ iff β reduces to γ. We have so formulated $\mathbf{LR2}_{\rightarrow}$ that the following lemma of [Cu50] is provable:

Lemma 1 (Curry, 1950). *Suppose a consecution $\beta \vdash C$ reduces to $\gamma \vdash C$, where the former is provable in n steps. Then there is a number $m \leq n$ such that the latter is provable in m steps.*

Let us now follow [BW65] (who were adapting Kripke) in calling a derivation of a consecution $\beta \vdash B$ *irredundant* if no earlier step in its proof tree reduces to any later step. We then have

Theorem 1. *Every provable consecution of* $\mathbf{LR2}_{\rightarrow}$ *has an irredundant derivation.*

Proof. Proof by Curry's lemma.

This clears the ground for Kripke's beautiful combinatorial lemma, which he worked out as a lad. Call two multisets *cognate* if the same *wffs* occur in both of them. And call the *cognation class* of a multiset the class of multisets that are cognate to it. By the subformula property, any formula occurring in the derivation of a given consecution is a subformula of some formula in the conclusion of that derivation. Upshot: only finitely many cognation classes have members in a proof search tree for an $\mathbf{LR}_{\rightarrow}$ consecution. Further upshot: every irredundant $\mathbf{LR2}_{\rightarrow}$ proof search is *finite*. For, by Kripke's lemma (K)

Lemma 2 (Kripke 1959). *Every irredundant sequence of cognate consecutions is finite.*

Proof. Proof by transposition. Suppose that there exists an infinite sequence $\alpha_i \vdash B$ of cognate consecutions. Show by induction on the number of formulas in the (common) cognation class of the α_i that the sequence is redundant; whence, contraposing, any cognate irredundant sequence must be finite.

Meyer had a bit of a problem at this point. He *knew* that the conclusion was true, because Belnap had shown his fellow students and him Kripke's sound argument. But he *did not believe* it. Visions of irredundant infinite cognate sequences fluttered through his dreams. And so he wanted an argument that he did believe.

More of that below! Meanwhile let us draw the immediate conclusion.

Theorem 2 (Kripke 1959). $\mathbf{R}_{\rightarrow}$ *is decidable. So is* $\mathbf{E}_{\rightarrow}$ *.*

Proof. We omit all arguments for $\mathbf{E}_{\rightarrow}$. The interested reader may look up valid ones, e.g., in [AB75]).[14] For $\mathbf{R}_{\rightarrow}$ we argue as follows: construct a proof search tree

[14] It seems that Kripke wrote up his original argument re $\mathbf{E}_{\rightarrow}$ at most in private communications to Anderson and Belnap. In addition to Kripke's Lemma, he had an *interpretation* of his Gentzen system for $\mathbf{E}_{\rightarrow}$ in the axiomatic formulation which, he has written to us, "is quite straightforward". He told us that Dunn has gone through something similar. And he pronounced it "marginally simpler than Belnap's approach, though his is not too complicated."

for the theorem candidate $\vdash A$ in $\mathbf{LR2}_{\rightarrow}$. Only the finitely many subformulas of A are relevant to the (cut-free) proof search; and, by Curry, we may keep that search irredundant. Suppose (curse our luck!) that the proof search tree is infinite. Since the tree has the finite fork property (inasmuch as there are only finitely many things to try to deduce a candidate consecution at any point in the search tree), it follows by König's lemma that there must be some infinite branch. But there are only finitely many cognation classes whose representatives may appear on the bad branch. Accordingly there is an infinite irredundant subbranch of *cognate* $\alpha_i \vdash B$. This contradicts Kripke's lemma, and refutes the hypothesis that we must curse our luck. For there are but finitely many nodes in our proof search tree for the theorem candidate. End of proof.

3.1 Relevant Divisibility.

Decidability is guaranteed by Kripke's lemma, but this lemma itself is not immediately obvious. [Me73,Me98] summarize the main results obtained in trying to fully understand S. Kripke's insights. One of them is an equivalent formulation of Kripke's lemma in terms of a *relevant divisibility principle*.

The "use" criterion for relevance in Relevant Logics says that in a deduction the premisses must be effectively used in the derivation of a conclusion. Let us now consider ordinary divisibility. *Obviously* it involves fallacies of relevance. For consider the suspicious claim that 2 divides 12. There is a factor of 12, namely 3, which is *not used* in performing the division. We rest for now with this observation that ordinary divisibility has a *less than upright character*, whence we slantily write "/" for it thus:

$$m/n \text{ iff } m \text{ divides } n \tag{2}$$

Relevant divisibility $|$ will by contrast have an *upright* character.[15] We define first a function *primeset*, whose application to any positive integer n yields the *set* of the prime divisors of n.
For example, $\mathit{primeset}(2) = \{2\}$ but $\mathit{primeset}(6) = \mathit{primeset}(12) = \{2, 3\}$. Then our definition of $|$ will go like this:

$$m|n \text{ iff } (i)\ m/n \text{ and } (ii)\ \mathit{primeset}(m) = \mathit{primeset}(n) \tag{3}$$

We adapt Kripke's terminology by introducing the following

Definition. We call m and n *cognate* iff $\mathit{primeset}(m) = \mathit{primeset}(n)$.

And it is now clear that ordinary and relevant division coincide on cognate pairs of numbers. Moreover, since a division performed with unused factors is as reprehensible as an argument with unused premisses, we trust that all good relevantists and true will stick henceforth to *vertebrate, relevant* division.

[15] We confess that we have *reversed* the conventions of [Me98], on which $|$ was ordinary and $/$ was relevant divisibility.

4 Kripke, Dickson and Meyer Lemmas.

Let $I\!N_n$ be the free commutative monoid generated by the first n primes. Then, **Kripke's lemma** (K) can be formulated in the following way:
Let a_i be any sequence of members of $I\!N_n$ and suppose that for all i, j, if $i < j$ then $a_i \not| a_j$. Then a_i is finite.

We prove (K) in the form of the **Infinite Division Principle** (IDP):

Lemma 3 (Meyer). *Let A_n be any infinite subset of $I\!N_n$. Then there is an infinite subset A'_n of A_n and a member a of A'_n s.t. for all $b \in A'_n$, $a|b$.*

Proof. We call the element a which divides infinitely many members of A an *infinite divisor for A*. We prove that every infinite A has an infinite divisor by induction on n.

Base case: If $n = 1$, we have an isomorphic copy of $I\!N$ with the natural order. Every non-empty subset $A \subseteq I\!N$ has a least element m, which (reversing the isomorphism) will divide all other elements of A.

Inductive case: Suppose then that the lemma holds for all $m < n$. We show that it holds for n.
Let A_n be an infinite subset of $I\!N_n$. Partition A_n into *cognation classes* by setting
(i) $c \sim d$ iff $primeset(c) = primeset(d)$. There are only finitely many equivalence classes under (i) since there is exactly one such class for each subset of the set of the first n primes. A_n being infinite, one of the classes is infinite. Call it B_n.

Subcase 1: B_n is *bounded by x* on some coordinate m.[16] Let m be the coordinate in question, and let x be the least bound. W.l.o.g. we may take m to be n. Then B_n is the *union* of the *finitely many* cognation classes $B_n^0, \ldots, B_n^x$, whose values on the n^{th} coordinate are respectively $0, \ldots, x$. Since the infinite set B_n is the union of finitely many sets, one of these sets B_n^i is itself infinite. On inductive hypothesis this set, and hence B_n, and hence A_n has an infinite divisor.

Subcase 2: B_n is unbounded on every coordinate m. Let $h = I\!N_n \longrightarrow I\!N_{n-1}$ be the *truncation* function defined on $I\!N_n$ with values in $I\!N_{n-1}$. In particular, let $h(A_n) = A_{n-1}$. A_{n-1} is either finite or infinite. But since $n > 1$ it cannot be finite (or else we would be in Subcase 1). So A_{n-1} is infinite. Apply the inductive hypothesis. There is an infinite subset $B_{n-1} \subseteq A_{n-1}$ and an $a' \in B_{n-1}$ such that $a'|b', \forall b' \in B_{n-1}$.
Let $B_n = \{c : c \in A_n \text{ and } h(c) \in B_{n-1}\}$.
B_n is infinite since all elements in B_{n-1} are images under h of at least one member of A_n. In particular, the infinite divisor a' is such an image. Pick

[16] Where $C \subseteq A_n$ we say that x bounds C on m iff for all $c \in C$ the m^{th} coordinate $c_m \leq x$. Otherwise we say that C is *unbounded* on m.

the member a'' of B_n that is least on coordinate n among the members of B_n such that $h(a) = a'$.
Is a'' an infinite divisor for B_n? If the answer is "Yes," we are through. So suppose that it is "No." At any rate we know that $a' = h(a'')$ is an infinite divisor for B_{n-1}. So since a'' has *failed* infinitely often to divide members of B_n, on our remaining hypothesis, the reason must be that its n^{th} coordinate is too great. But now we simply fall back on the strategy that has several times already proved successful, setting $C_n = \{c \in B_n : a'|h(c) \text{ and not } a''|c\}$. But the infinite set C_n is built from elements all of which are bounded by a'' on the n^{th} coordinate. This means again that there will be an infinite C_n^i for a particular value i on the last coordinate, whence the inductive hypothesis delivers the theorem in this case also, ending the proof of the IDP.

It can be shown moreover that the IDP is equivalent to K and to **Dickson's lemma** (D) stated in the following form:

Lemma 4. *Let $A_n \subseteq I\!N_n$ and suppose that for all $a, b \in A_n$, if $a|b$ then $a = b$. Then A_n is finite.*

The proof is left as an exercise.

5 Finitizing the Commutative Monoid Semantics for $\mathbf{R}_\rightarrow$.

Building on ideas of Urquhart, Routley, Dunn and Fine, [Me73,MO94,Me98] develop an operational semantics for $\mathbf{R}_\rightarrow$ in terms of *commutative monoids*. Kripke's lemma is then applied to deliver an *effective* finite model property for $\mathbf{R}_\rightarrow$ and some of its supersystems on that semantics. Referring readers to the cited papers for details, we summarize some main points.

Let S be the sentential variables of $\mathbf{R}_\rightarrow$ and F the set of formulas built from S in the usual way. Let $\mathbf{M}$ be an arbitrary partially ordered square-increasing commutative monoid.[17] A *possible interpretation* I in such an $\mathbf{M}$ is a function $I : F \times \mathbf{M} \longrightarrow \{T, F\}$ that satisfies the following truth condition: for all $A, B \in F$, and for all $a \in \mathbf{M}$, $I(A \rightarrow B, a) = T$ iff for all $x \in \mathbf{M}$, if $I(A, x) = T$ then $I(B, ax) = T$. And A is *verified* on I iff $I(A, 1) = T$.

A problem with $\mathbf{R}_\rightarrow$ is that not all of its theorems are verified on arbitrary interpretations. In particular, the Contraction axiom A4 above is not verified. To solve the problem, the set of possible interpretations is restricted by imposing a hereditary condition: an interpretation is *hereditary* if for all $\mathbf{M}$, for all $A \in F$ and for all $a, b \in \mathbf{M}$, if $a \leq b$ and $I(A, b) = T$ then $I(A, a) = T$.

It is shown in [Me98] that the only model you'll ever need for $\mathbf{R}_\rightarrow$ is the *free* one. Specifically, take this to be $I\!N_+$, the positive integers, with *primes* as free generators, 1 as monoid identity, multiplication as monoid operation and relevant division $|$ as the square-increasing ordering relation. For the completeness proof for $\mathbf{R}_\rightarrow$ assures that every non-theorem is refuted on an appropriate hereditary

[17] I.e., satisfying conditions (i), (ii) and (iv) that we set out in [AB75], p. 376.

interpretation I at 1 in some appropriate **M**. And there is then an equivalent I', i.e. an interpretation verifying exactly the same formulas, in the monoid $\mathbb{N}_+$, of which **M** is a homomorphic image.

But if you want the finite model property, you had better be more careful. First, to refute a given non-theorem A, freely generate a commutative monoid **M** from the subformulas of A. W.l.o.g. we may take this **M** to be $\mathbb{N}_n$, where n is the number of subformulas of A. This technique thus transforms infinitely long vectors with no finite bound into vectors of uniform length n. Hence, the property transforms the cardinality of the primes required for a refutation of a non-theorem A.
Kripke's lemma and the finite generator property suffice for decidability. But we can go further and prove the Finite Model Property.

5.1 The Finite Model Property.

Taking the monoid generated by the primes as characteristic presents another difficulty because arbitrarily high exponents are allowed on any particular prime. This is solved by placing bounds on the exponents which are relevant to a refutation of a formula A. I.e. we *shrink* $\langle \mathbb{N}^k, +, 0\rangle$ to $\mathbf{i}^k = \langle i^k, \oplus, 0\rangle$ where $i, k \in \mathbb{N}_+$. Our additive commutative monoid will be $\langle i, \oplus, 0\rangle$, where $i = \{n : 0 \leq n < i\}$ and $\oplus$ is defined as follows: for $0 \leq m, n < i$, if $m + n \geq i$ then $m \oplus n = i - 1$, otherwise, $m \oplus n = m + n$. That is, $\mathbf{i}$ is the 1-generator commutative monoid $\langle \mathbb{N}, +, 0\rangle$ bounded at $i - 1$, and the elements of i^k are the k-place sequences of natural numbers $< i$ on every coordinate. Shrinking $\mathbb{N}^k$ to $\mathbf{i}^k$ is guaranteed by the natural homomorphism $h : \mathbb{N}^k \to \mathbf{i}^k$ whose effect on the jth coordinate of each element $a \in \mathbb{N}^k$ is s.t. if $a_j \geq i, (h(a_j)) = i - 1$, else $(h(a_j)) = a_j$. In this way, the coordinates of elements that are greater than $i - 1$ are all reduced to $i - 1$.

Henceforth, by the *index* of a formula A we mean simply its number k of subformulas. And for every non-theorem A of $\mathbf{R}_\to$ there is a procedure that yields a refutation of A in $\mathbb{N}^k = \langle \mathbb{N}^k, +, 0\rangle$ or in the isomorphic $\langle \mathbb{N}_k, \cdot, 1\rangle$. Suppose now that we have a refuting interpretation I for such an A. We single out some elements $b \in \mathbb{N}^k$ as *critical* for A. Specifically, b is critical if it is a "first falsehood" for some subformula B of A. Even more specifically, suppose I fixed.

Then b is critical iff there is a subformula B of A s.t.

1. $I(B, b) = F$
2. for all $c \in \mathbb{N}^k$, if $c|b$, then $I(B, c) = T$.

That is, each subformula B of A gives rise to a family of critical elements. And b is critical iff it is *minimal* in the ordering induced by $|$ in the subset of elements of $\mathbb{N}^k$ at which B is false.

Every formula A has finitely many subformulas B. And we can then apply Dickson's lemma to assure that the non-theorem A gives rise, at most, to finitely many critical elements. And we then apply the shrinking operation to transform a refutation of A in $\mathbb{N}^k$ into a refutation of A in $\mathbf{i}^k$. So

Theorem 3 (Meyer 1973). $\mathbf{R}_{\rightarrow}$ *has the* FMP.

Proof. Let A be a non-theorem of $\mathbf{R}_{\rightarrow}$ of index k. A is refutable in $\langle I\!N^k, +, 0\rangle$ on a hereditary interpretation I. It suffices to find an interpretation I' in $\mathbf{i}^k$ refuting A and such that I' is hereditary. Apply the procedure just sketched. $\mathbf{i}^k$ being finite, A is refuted in a finite model. End of proof.

6 Partial orders.

Kripke's lemma in its number-theoretic form is about order induced by divisibility on the positive integers. The theory of partial order not only illuminates its significance, but it also guarantees the truth of the lemma and of its equivalent formulations for the free commutative monoid $\langle I\!N_k, \cdot, 1\rangle$.

Let $\langle X, \leq\rangle$ be a *partially ordered* set; i.e. the ordering relation $\leq$ is reflexive, transitive and antisymmetric.
Then, X satisfies the IDP if for all infinite $A \subseteq X$, there is a $a \in A' \subseteq A \subseteq X$ s.t. A' is infinite and for all $a' \in A'$, $a \leq a'$.

Let $A \subseteq X$. Then, A_{min}, the set of A-*minimal* elements is the set of $a \in A$ s.t. for all $y \in A$, $y \not< a$.
Then, X satisfies the *finite minimum condition* (FMC) iff, for all $A \subseteq X$, A_{min} is finite. Then, D says that, for $n \in I\!N_+$, $\langle I\!N_n, |\rangle$ and $\langle I\!N_n, /\rangle$ satisfy the FMC.

As in [Bi67] X satisfies the *Ascending Chain Condition* (ACC) iff all strictly ascending chains are finite. Dually, it satisfies the DCC iff all strictly descending chains are finite.

An alternative way of showing that $IDP \equiv D \equiv K$ and that all of these hold in the free commutative monoid $I\!N^k$ partially ordered by divisibility can be based on these definitions.[18] We first note that for *any* partially-ordered set A, the conditions "*A satisfies the IDP*" and "*A satisfies both the DCC and the FMC*" are equivalent.

7 More about Dickson's Lemma.

In addition to the Birkhoff exercise cited above, we also discovered that Higman's lemma [Hi52] states and proves some equivalent formulations of *K, D, IDP*. The property we are interested in is that of a *well-partial-ordering*.

7.1 Higman's Lemma.

There are various ways to characterise a well-partial-order or a well-quasi-order. We concentrate here on the former. Most often the associated proof techniques rely on the notion of *minimal bad sequences*.
Definition. Let $\mathbf{a} = a_1, a_2, \ldots, a_n, \ldots$ be an infinite sequence of elements of a partially ordered set A. Then, $\mathbf{a}$ is called *good* if there exist positive integers i, j such that $i < j$ and $a_i \leq a_j$. Otherwise, the sequence $\mathbf{a}$ is called *bad*.

[18] In fact, these equivalences were suggested by an exercise in Birkhoff [Bi67].

Then,

Definition. Let A be a *partially ordered* set. Then A is *well-partially-ordered*, if every infinite sequence of elements of A is good or, equivalently, if there are no infinite bad sequences. Also equivalently, A is *well-partially-ordered* if it does not contain an infinite descending chain (i.e. $a_0 > a_1 > \cdots > \cdots$), nor an infinite anti-chain (i.e. a set of pairwise incomparable elements).

To be well-partially-ordered is also equivalent to having a finite basis:

Definition. Let A be a *partially ordered* set and $B \subset A$. The *closure* of B, $Cl(B) = \{a \in A | \exists b \in B, b \leq a\}$. And B is closed iff $B = Cl(B)$. A has the *finite basis property* if every subset of A is the closure of a finite set.

All the properties expressed in the preceding definitions are proved equivalent to the well-partial-ordering or to the finite basis property in **Higman's lemma** [Hi52] :

Let A be a *partially ordered* set. Then the following conditions on A are equivalent:

1. every closed subset of A is the closure of a finite subset;
2. the ascending chain condition holds for the closed subsets of A;
3. if B is any subset of A, there is a finite set B_0 such that $B_0 \subset B \subset Cl(B_0)$
4. every infinite sequence of elements of A has an infinite ascending subsequence;
5. if $a_1, a_2, \ldots$ is an infinite sequence of elements of A, there exist integers i, j such that $i < j$ and $a_i \leq a_j$;
6. there exists neither an infinite strictly descending sequence in A (well-founded-ness), nor an infinite antichain, that is, an infinity of mutually incomparable elements of A.

7.2 Hilbert's Finite Basis and Gordan's lemma.

In [Di13], Dickson remarks that his lemma can be obtained from Hilbert's theorem [Hi90].

In its modern reading, Hilbert's theorem says that *if a ring R is Noetherian, then the polynomial ring in n commuting indeterminates $R[X_1, \ldots, X_n]$ is Noetherian*[19].

And a ring R is Noetherian if one the following conditions holds:
(i) every ideal in R is finitely generated,
(ii) any ascending chain of ideals is finite,
(iii) every ideal in R has a maximal element.

Historically, Hilbert's theorem originated in the old and now forgotten invariant theory. A short note on this theorem is not without interest since it throws some light on the ancestry of our D, K and IDP principles.

[19] A *ring* R is an additive commutative group together with an associative and distributive multiplication operation. If I is an additive subgroup of R such that for all $a \in I$, for all $r \in R$, $ar, ra \in I$, then I is an *ideal*

In the middle of the nineteenth century, Cayley had studied "quantics", i.e. homogeneous polynomials with arbitrary constant coefficients of degree n in m independent variables. Gordan proved constructively the existence of finite fundamental invariants and covariants for systems of binary quantics (see [Be45]). His theorem shows that *the number of irreducible solutions in positive integers of a system of homogeneous linear equations is finite.*

Hilbert [Hi90] gave a more general proof of the theorem which applies to any number of variables. But, unlike Gordan's proof, Hilbert's proof gives no indication as to the actual determination of the finite system. It is a mere existence proof, provoking the Gordan quotation which we have adopted as our slogan for the paper—"This is not mathematics, it is theology".

Interestingly, Gordan later found a much simplified proof of Hilbert's theorem. The proof is reproduced in Grace and Young [GY03]. We consider only **Gordan's lemma**:

Let S be a set of products of the form $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ such that the α_i satisfy some condition. Although the number of products that satisfy these conditions may be infinite, a finite number can be chosen so that every other is divisible by one at least of this finite number.

This lemma is often used in proofs of Dickson's lemma, it is even sometimes called Dickson's lemma (see [CLO92]). This is not surprising when it is compared to the original formulation of **Dickson's lemma**:

Any set S of functions of type (1), $F = a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_r^{\alpha_r}$ contains a finite number of functions $F_1,\ldots,F_k$ such that each function F of S can be expressed as a product F_if where f is of the form (1) but is not necessarily in the set S.

Finally, let us note that König [Kö36](XI, §3, α) uses a lemma that expresses one of the equivalent properties of Higman's lemma: *if two elements of a set M of ordered sequences of positive integers are incomparable, then M is finite.* And he remarks in a note that Gordan's theorem follows from this lemma.

8 Complexity.

With the Dickson-Kripke lemma we have a finiteness or termination condition. But finite can be arbitrarily large. We turn to complexity results for relevant logics, which are all due to A.Urquhart [Ur90,Ur97]. He shows that the decision problem for the conjunction-implication fragment of the logics between T and R is $EXPSPACE$-hard under log-lin reducibility. This result relies on the $EXPSPACE$-completeness of the word problem for commutative semigroups.

Urquhart also shows that Kripke's decision procedure for $R_{\rightarrow}$ is, as an *upper* bound, *primitive recursive in the Ackermann function*. His result is based on the study of decision procedures for Petri Nets and vector addition systems where a lemma essentially equivalent to Kripke's lemma is used to show that the reachability tree of a vector addition system is finite. For each k in a k-dimensional vector addition system, or a k-place Petri Net, the k-finite containment problem has a primitive recursive decision procedure. And in the unbounded case, the procedure is *primitive recursive in the Ackermann function*.

Urquhart sharpens his result in [Ur97] by showing that for the decidable extension of $\mathbf{R}_{\to}$ called **LR** in [TMM88], the lower and upper bounds converge. This result suggests that the logics decided by a procedure based on *K, D, IDP* are primitive recursive in the Ackermann function.[20]

S. Kripke had conjectured that the proof that $\mathbf{R}_{\to}$ is decidable might itself be undemonstrable in elementary recursive arithmetic [TMM88]. That is, Kripke conjectured that powerful arithmetical principles were required for his demonstration that proof search trees for $\mathbf{R}_{\to}$ and its kin are invariably finite. Results originating in the program of 'Reverse Mathematics' [Si88] confirm that conjecture for *primitive* recursive arithmetic. They show that none of the properties expressed by Dickson's lemma, Higman's lemma or Hilbert's theorem are provable in primitive recursive arithmetics.[21]

9 Conclusion.

The idea of the surprising property expressed by Dickson's lemma was in the air at the turn of the century due to Gordan and Hilbert. The property reappeared from time to time. In Logic, well-quasi-orders were used by Y. Gurevich in his early work on Hilbert's *Entscheidungsproblem* to show that some classes of first-order formulae are decidable [BGG97]. In Relevant Logics, it reappeared in Kripke and in Meyer. Its interpretation in terms of infinite divisibility, its proof in the *IDP* form and its application in the decision procedure that are reported here allow one to see similarities to the theory of Gröbner bases, especially as it has been worked out via the Buchberger algorithm.
Now, Dickson's lemma and its mates may appear quite obvious to some. To us, they did not. Is the proof presented here *yet another* proof of Dickson's lemma? It is the proof that satisfies us. And not all purported proofs of the principle do so.[22] In a concluding conclusion, we return to our slogan. For after Gordan had

[20] This "suggestion" is not yet a proof. And Urquhart calls our attention in correspondence to the fact that "actually, I proved a non-primitive-recursive lower bound for all implication-conjunction logics between T and R. So for implication and conjunction, the later results are a strict improvement on the old. The only result in the old paper that is not improved in the later is that $\mathbf{R}_{\to}$ is $EXSPACE$-hard. The true complexity of $\mathbf{R}_{\to}$ is a very interesting open problem, and might be worth mentioning."

[21] It is interesting to note that primitive recursive arithmetic, a finitary and constructive system, corresponds to Hilbert's notion of finitism.

[22] For example, consider the proof of T. Becker *et al.,* in [BWK93] which tries to avoid the use of the (questionable to some) axiom of choice (AC). There, the proof of Proposition 4.49 (Dickson's lemma) does not convince us. They claim, independently of AC, that if $\langle M, \leq \rangle$ is a well-quasi-ordered set, then so also is the direct product $\langle M \times N, \leq' \rangle$, where N is the natural numbers and $\leq'$ is the product ordering. To show this, they assume that S is a non-empty subset of $\langle M \times N, \leq' \rangle$. They let, for each $n \in N$, $M_n = \{a \in M \mid \langle a, n \rangle \in S\}$. Because M is well-quasi-ordered, they deduce correctly that each M_n has a finite basis B_n. They then form $\bigcup_{n \in N} B_n$, and

adapted [Hi90] for his own purposes, he conceded that "I have convinced myself that theology also has its merits."

References

AB75. Anderson, A. R. and Belnap, N. D., *Entailment I. The Logic of Relevance and Necessity.* Princeton, Princeton Un. Press, 1975. 224, 225, 225, 229, 230, 233

ABD92. Anderson, A. R., Belnap, N. D. and Dunn, J. M., *Entailment II. The Logic of Relevance and Necessity.* Princeton, Princeton Un. Press, 1992. 224

BWK93. Becker, T., Weispfenning, V. and Kredel, H., *Gröbner Bases. A Computational Approach to Commutative Algebra,* New York, Springer-Verlage, 1993. 238

Be45. Bell, E, T., *The Development of Mathematics*, New York, McGraw-Hill, 1945. 237

BW65. N.D. Belnap, N.D. and Wallace, J.R., A Decision Procedure for the System E_I of Entailment with Negation. *Zeitschr. f. math. Logik und Grundlagen d. Math.* 11 (1965), 277-289. 227, 227, 229, 230

Bi67. Birkhoff, G., *Lattice Theory*, 3rd edition. Providence, AMS, 1967. 235, 235

BGG97. Börger, E., Grädel, E. and Gurevich, Y., *The Classical Decision Problem*, New York, Springer Verlag, 1997. 238

CLO92. Cox, D., Little, J. and O'Sheen, D., *Ideals, Varieties, and Algorithms.* New York, Springer Verlag, 1992. 237

Ch51. Church, A., The Weak Theory of Implication, In: *Kontrolliertes Denken, Untersuchungen zum Logikkalkül und zur Logik der Einzelwissenschaften*, ed., A. Menne et al., Karl Albert Verlag, 1951, pp. 22-37. 224, 225, 226, 239

Cu50. Curry, H.B., *A Theory of Formal Deducibility*, Ann Arbor, 1950. 230

Cu63. Curry, H.B., *Foundations of Mathematical Logic*, New York, 1963. 225, 225

CuC53. Curry, H.B. and Craig, W., Review of [Ch51], *J. Symb. Logic* 18 (1953) pp. 177-8. 225

Di13. Dickson, L.E., Finiteness of the Odd Perfect Primitive Abundant Numbers with n Distinct Prime Factors. *Am. J. Math.* 35 (1913) 413-422.

Do92. Došen, K., The First Axiomatization of Relevant Logic *J. Phil. Log.* 21 (1992), 339-56.

Du86. Dunn, J. M., Relevance Logic and Entailment. In: *Handbook of Philosophical Logic*, Vol.III, D. Gabbay and F. Guenthner (eds.), Dordrecht, D. Reidel, 1986, pp. 117-224. 224 229

GY03. Grace, J.H. and Young, A., *The Algebra of Invariants.* Cambridge University Press, 1903. (Repub. New York, Chelsea Pub. Comp.). 237

Hi52. Higman, G., Ordering by Divisibility in Abstract Algebras. *Proc. London. Math. Soc.* 2, (1952) 326-336. 235, 236

Hi90. Hilbert, D., Über die Theorie des algebraischen Formen. *Math. Annalen* 36 (1890) 473-534. 236, 239

again deduce correctly that there is a finite basis $C \subseteq \bigcup_{n\in N} B_n$. They let $r \in N$ be s.t. $C \subseteq \bigcup_{i=1}^{r} B_i$, and set $B = \{\langle a, i\rangle \in M \times N \mid 1 \leq i \leq r, a \in B_i\}$. They claim that B is a finite basis for S. But, according to us, they *overlook* that not all elements $\langle a, i\rangle$, $i \leq r$, need belong to S. So while B is certainly finite, it is *not necessarily* a basis for S.

Kö36. König, D., *Theorie der endlichen und unendlichen Graphen,* 1936. (Repub. New York, Chelsea Pub. Comp.) 237

Kr59. Kripke, S., The Problem of Entailment, (Abstract). *J. Symb. Logic* 24 (1959) 324. 227, 229

Me73. Meyer, R. K., Improved Decision Procedures for Pure Relevant Logics. Unpublished, 1973. 231, 233

Me98. Meyer, R. K., Improved Decision Procedures for Pure Relevant Logics. t.a. In: *A. Church's Festschrift.* 231, 231, 233, 233

MO94. Meyer, R. K and Ono, H., The Finite Model Property for BCK and BCIW. *Studia Logica*, 53, 1 (1994),107-118. 233

MM82. Meyer, R. K. and McRobbie, M. A., Multisets and Relevant Implication I and II. *Australasian J. of Philosophy* 60 (1982), 107-139 and 265-281. 225

Or28. Orlov, I. E., The Calculus of Compatibility of Propositions, (in Russian). *Matematicheskiĭ sbornik* 35 (1928), 263-286. 224

Si88. Simpson, S.G., Ordinal Numbers and the Hilbert Basis Theorem. *J. Symb. Logic* 53, 3 (1988) 961-974. 238

TMM88. Thistlewaite, P., McRobbie, M. and Meyer, R.K., *Automated Theorem-Proving in Non-Classical Logics,* John Wiley, New York, 1988. 225, 226, 227, 227, 228, 228, 229, 238, 238

Ur84. Urquhart, A., The Undecidability of Entailment and Relevant Implication, *J. Symb. Logic*, 40 (1984), pp. 1059-1073. 226

Ur90. Urquhart, A., The Complexity of Decision Procedures in Relevance Logic. In: J.M. Dunn and A. Gupta (eds), *Truth or Consequences, Essays in Honor of Nuel Belnap.*, Dordrecht, Kluwer Academic Publishers, 1990, pp. 61-76. 237

Ur97. Urquhart, A., The Complexity of Decision Procedures in Relevance Logic II. (t.a.) 237, 238