Notre Dame Journal of Formal Logic
Volume 24, Number 2, April 1983

Questions Concerning Possible Shortest Single Axioms for the Equivalential Calculus: An Application of Automated Theorem Proving to Infinite Domains

L. WOS, S. WINKER, R. VEROFF,
B. SMITH and L. HENSCHEN*

1 Introduction Occasionally in mathematics, and especially in various fields of formal logic, there arise various questions of alternate axiomatization. In the equivalential calculus, for example, there are formulas that are known to be strong enough to serve as single axioms. In [15] Peterson gave various possible shortest single axioms for that calculus. With the 10 given there and the one found by Kalman [3], there arose a question concerning the existence of any additional formulas that might also be shortest single axioms. There remained seven formulas yet to be classified in that regard [15].

In this paper we show that each of the four formulas *XJL*, *XKE*, *XAK* and *BXO* is too weak to be a single axiom. Although the corresponding proof and discussion of the remaining three unclassified formulas are deferred to a later paper, we remark that *XCB* is also too weak but both *XHK* and *XHN* are each "new" shortest single axioms.

The method for obtaining both the results presented here and those that

*This work was supported in part by the Applied Mathematical Sciences Research Program (KC-04-02) of the Office of Energy Research of the U.S. Department of Energy under Contract W-31-109-Eng-38 (Argonne National Laboratory, Argonne, IL 60439) and in part by NSF grant MCS79-03870 (Northern Illinois University, DeKalb, IL 60115).

Received June 15, 1981; revised July 10, 1982

are deferred rests heavily on the use of an automated theorem-proving program. This program is a general-purpose program in that it has been and is used to study questions from various fields of mathematics and logic. Before this study was made, proofs obtained with such programs were for theorems naturally phrasible in the first-order predicate calculus. This study, on the other hand, required proving theorems of a higher order. This additional requirement resulted from the intent of examining the full set of theorems deducible from a formula in order to show that certain known theorems are absent from the set. Since, for each of the formulas under study, the set of deducible theorems is infinite, the direct examination thereof is impossible. To cope with such infinite domains and remain within the province of the existing theorem-proving program, a new methodology was developed.

For each of the four formulas, use of the program led to the discovery of a corresponding finite set of schemata. The individual sets of schemata each respectively characterize the set of theorems deducible from the particular formula under study. Although this treatment of infinite domains extends the scope of automated theorem-proving programs, its more significant aspect for the logician is its generality. Evidence of the generality of the method is provided by applications to similar problems in both the *R* and the *L* calculus [4] and is covered in a later paper.

Four aspects of the method given in this paper are worth noting. First, for those four formulas that are proved here too weak to be a single axiom, the method yields a characterization of the theorems deducible from them in terms of a finite set of schemata. Second, all formulas are treated in a uniform fashion. Third, for each of the seven formulas studied, the method is used to establish either the inadequacy or the adequacy of the formula as a single axiom. For example, *XJL* is inadequate, and *XHK* is adequate. Fourth, other than that which was required to produce the existing theorem-proving program, no programming was required to obtain the results.

In the interest of providing an understanding of the potential value of such a program and thereby suggesting possible alternate uses of the computer in the study of formal logic, we provide a brief discussion of how the program was used to obtain these results. We include the discussion of the solution of a rather different problem than that of the consideration of infinite domains. Specifically, we show how the program can be used to find shorter proofs for already proved theorems. The example chosen is *XGK*. Kalman [3] proved that *XGK* is a single axiom for the equivalential calculus. We briefly discuss the heavy use of Kalman's proof by the program in its successful attempt at obtaining an alternate proof—a proof roughly half the length of Kalman's.

The techniques given in this paper, especially when coupled with the knowledge that no additional programming is required by the researcher, may suggest the feasibility of attacking additional open questions with the assistance of an automated theorem-proving program.

2 Overview

2.1 Background The focus here is on the equivalential calculus. The elements of that calculus are the expressions that can be recursively well-formed from the variables, x, y, z, w, . . ., and the 2-place function E. The

theorems of the calculus are just those formulas in which each variable therein occurs an even number of times [14]. There are individual formulas there that are strong enough to serve alone as axioms. It has been proved [15] that the shortest possible single axiom must contain at least 11 symbols, and there are in fact formulas of that length that suffice. There are 630 formulas of length 11, i.e., that contain 11 symbols. Of these, 11 have been shown to be single axioms [3,13], but 612 have been proved too weak. Of the remaining seven, we show here that four are also too weak. In a later paper, we will show that two of the seven are addition "new" shortest single axioms and that the last of the seven is too weak. We thus disprove the conjecture [5] that no additional shortest single axioms would be found.

The standard rules of inference in this calculus are the substitution rule and the rule of detachment [17]. However, studies thereof are often conducted by means of the inference rule of condensed detachment [15]. By a remark by Kalman [16], we have the fact that all theorems in the calculus can be obtained by substitution into some formula that can in turn be obtained by condensed detachment. Since there exist single axioms for the calculus in which each variable therein occurs precisely twice, and since Lemma 2.2.1 establishes the fact that the successful condensed detachment of two formulas of this type yields a formula of the same type, we choose in this paper to confine our attention to the use of condensed detachment. We also, therefore, restrict our attention to those theorems of equivalential calculus in which each variable therein occurs twice.

Definition For the two formulas $E(A,B)$ and A, *detachment* is that inference rule that yields the formula B.

Definition For the two formulas $E(A,B)$ and A' which are assumed to have no variables in common, *condensed detachment* is that inference rule that yields the formula B'', where B'' is that which is obtained from detaching $E(A'',B'')$ and A'', and where $E(A'',B'')$ and A'' are obtained from $E(A,B)$ and A', respectively, by the most general possible substitution whose application forces A and A' to become identical. Condensed detachment is denoted by CD.

Thus condensed detachment, when it applies, takes two formulas and renames their variables so that they have no variables in common, then seeks the most general substitution that can be found whose application will permit a detachment, and finally applies detachment to the pair of formulas after the substitution has been made. For example, the condensed detachment of $E(E(E(x,x),z),z)$ with $E(E(x,y),E(y,x))$ yields $E(x,x)$ and also yields $E(x,E(E(y,y),x))$, depending on the order in which the premisses are considered.

For the remainder of the paper, a "theorem" of equivalential calculus will be a formula in which each variable occurs twice. Such formulas will be called *pure*. The study of the calculus will thus be entirely in terms of pure formulas.

2.2 Definitions and notation We now turn to the formal treatment. We adopt the following notation and employ the following definitions.

The formulas of the equivalential calculus will be written in terms of the

2-place function, E, and the variables, $x, y, z, \ldots$. However, when two formulas are considered simultaneously (as in condensed detachment, for example), we assume that no variables are shared regardless of the syntactic form. We refer to the equivalential calculus as *EC*. Using the notation of Peterson [15], the four formulas to be studied are *XJL*, *XKE*, *XAK* and *BXO*.

Definition Two well-formed expressions (which are assumed to have no variables in common) are said to *unify* [18] if there exists a substitution that can be applied to them which makes them identical.

Definition Except for alphabetic variancy, the *most general unifier* (*MGU*) is the most general substitution that forces a pair of unifiable expressions to become identical.

Definition The *most general common instance* (*MGCI*)—within alphabetic variancy—for two unifiable expressions is that expression yielded by application of the *MGU*.

Definition If the condensed detachment of $E(A,B)$ with A' yields B'', then $E(A,B)$ is called the *major* premiss and A' the *minor* premiss.

By convention, when we say "condensed detachment of A with B", henceforth we shall mean that A is the major premiss and B is the minor.

Since the condensed detachment of $E(A,B)$ with A' requires finding the most general common instance, if any exists, of A and A', we have the following definition.

Definition If the successful unification of A with A' is represented by the set of pairs t_i/z_i where t_i are well-formed expressions and z_i are the variables in A and A', then t_i are called the *replacement terms* of unification, or simply the *replacement terms*. When $E(A,B)$ is condensed detached with A', those replacement terms t_i whose z_i are present in both A and B are called *key replacement terms*.

Thus the formula yielded by the successful condensed detachment of $E(A,B)$ with A' is obtained by replacing those z_i in B that are also in A by the corresponding key replacement terms. For example, the condensed detachment of $E(E(E(x,x),y),y)$ with $E(E(x,y),E(y,x))$ yields $E(x,x)$, where the key replacement term is $E(x,x)$.

Definition A well-formed formula of *EC* is called *pure* if each of its distinct variables occurs exactly twice.

Definition When a variable in a well-formed formula A of *EC* occurs exactly once in A, that variable is called *isolated* and is usually denoted by w.

Definition A well-formed formula of *EC* is called *almost pure* if it contains exactly one isolated variable and, except for the occurrence of the isolated variable, the formula is pure.

For example, the formula $E(E(x,x),w)$ is almost pure, and also the formula w by itself is almost pure.

Definition The *kernel(s)* of a pure formula are those (not necessarily proper) subexpressions that are pure formulas but that properly contain no pure formulas. Kernels are usually denoted by K, K', ...

Thus we have: $E(y,z)$ is not pure; $E(E(x,x),E(y,y))$ is pure, where its only kernel (exclusive of alphabetic variancy) is $E(x,x)$; and the formula, $E(E(x,y),E(y,x))$, is itself a kernel.

Definition For any formula, A, the *closure* of A, denoted by $CL(A)$, is the smallest set of formulas that contains A and that is closed under condensed detachment.

Lemma 2.2.1 *The successful condensed detachment of two pure formulas yields a pure formula.*

Proof: The proof is omitted. A similar result is found in Belnap [1] after point 12 in the proof of the lemma.

We therefore have the following remark.

Remark 2.2.1: If A is a pure formula, then all elements of $CL(A)$ are pure.

Finally, in order to study the precise nature of $CL(A)$ for the four choices of A in question, we introduce the following definitions.

Definition Let A be any pure formula of EC, and let C be any nonempty set of well-formed formulas of EC. Then C is called a *containment set* for A when: A is in C; all elements of C are pure; and C is closed under condensed detachment.

Definition Let A be any pure formula of EC, let C be any containment set for A, and let U be any nonempty set of well-formed expressions from EC. Then U is called a *unification set* for A and C when: every element of U is almost pure; every element of U contains exactly one isolated variable, which is denoted by w; and the successful unification of any element of U with any element of C yields a replacement term for w that is itself an element of C. (Although the first property of unification sets implies the second, we choose to have both given explicitly because of extensive use of isolated variables in the following sections.)

The concept of unification set is introduced because of the close connection between condensed detachment and unification. Since both particular unification sets and particular containment sets occurring in later sections are defined in terms of schemata, we do not restrict the application either of unification or condensed detachment to just the formulas of the equivalential calculus. In fact we will in most cases be concerned with application of either to various schemata. For example, if the schema $f(A) = E(E(x,A),x)$ and the schema $i(z) = E(z,z)$, the condensed detachment of $f(A)$ with $i(z)$ yields A.

We can immediately give a trivial example of these definitions. Let A be any pure formula, let C be $CL(A)$, and let U consist of the single expression, w. Then C is a containment set for A, and U is a unification set for A and C.

Although we define a "new" containment set and a "new" unification

set for each formula to be studied, we omit notationally their respective dependence on the formula in focus. A similar remark holds for the various schemata and kernels relevant to the corresponding study.

2.3 The problem and the method of solution The problem is that of considering a formula and the possibility that it may be strong enough to be a single axiom for the equivalential calculus. One can prove that the selected formula is a single axiom by merely deriving from it by repeated use of condensed detachment some known single axiom. On the other hand, if it is too weak, establishment of that fact might proceed by showing that some known theorem cannot be thereby deduced.

Since in general from a given formula one can deduce an infinite number of theorems, direct examination of that set is not possible. Thus the problem of showing a formula too weak to be a single axiom is potentially harder than proving it strong enough. With much assistance from the automated theorem-proving program [10,19,25,26], we found that a finite set of schemata exists that circumvents the difficulty of examining the infinite domain of interest. More precisely, for each of the four formulas considered here (*XJL*, *XKE*, *XAK* and *BXO*), there exists a finite set of schemata that completely characterizes the theorems deducible from the formula. Not surprisingly, the nature of the respective sets depends on the particular formula under study.

To prove that a formula A of EC is not a single axiom, it is sufficient to prove that some containment set C for A excludes a known theorem, since such a C contains all formulas deducible from A. For each of the four formulas A at hand, we do this by presenting a C such that every formula in C contains a variant of A—which is itself a kernel—or, in the case of *BXO*, a variant of A or a second kernel, namely, $E(x,E(y,E(x,y)))$. Thus in every case, C fails to contain $E(x,x)$, a known theorem. (As an aside, it can be proved that $C = CL(A)$ for all four formulas, although this equality is not crucial here.)

In each case the required C, which is infinite, is inductively defined in terms of a finite set of schemata. That C is closed under condensed detachment is proved by conducting a case analysis (based on these schemata) for the possible forms of the major premiss coupled with a study of the corresponding condensed detachments. When such a *CD* is attempted, a subformula S of the major premiss is considered for unification with the minor premiss. To study the appropriate unifications, an infinite unification set U is also inductively defined in terms of a finite set of schemata. Then various unifications of elements from C with elements from U are considered. The consideration of such unifications for these formulas often reduces to yet further unifications whose *MGCI* is smaller in length. Thus the proof that C is closed relies on an induction argument based on the length of the *MGCI*. (The schemata used to define C and U were discovered with the aid of the automated theorem-proving program by attempting unifications on partially defined C and U.)

For each of the four formulas, we first prove a lemma that shows that the unification of an element of U with an element of C yields a key replacement term that in turn is an element of C. From this, it is easy to show by case analysis that the successful *CD* of two formulas in C is also in C.

Upon its completion, this study yields the following for A, where A is respectively each of the four formulas under investigation.

1. C is closed under condensed detachment
2. C contains $CL(A)$
3. C is a containment set for A
4. U is a unification set for A and C
5. With the exception of BXO, the only kernel to be found (up to alphabetic variancy) in any element of C is A itself; for BXO a second kernel appears, namely, $E(x,E(y,E(x,y)))$
6. Among the theorems of EC, C does not contain $E(x,x)$
7. $C = CL(A)$; (A strengthening of 2 but with some detail omitted), and, because of (6),
8. A is too weak to be a (shortest) single axiom for the equivalential calculus.

Because purity of formulas is heavily relied upon throughout the treatment given here, we give the following word of warning. When defining various C and U, we implicitly assume that the various schemata employ variables distinct from those occurring in their arguments. For example, if $h(w) = E(y,E(w,y))$, then $h(h(w)) = E(z,E(E(y,E(w,y)),z))$, as occurs in BXO.

3 *Examination of four possible shortest single axioms for equivalential calculus*

3.1 Ground rules In this section we show that each of the four formulas—XJL, XKE, XAK, and BXO—is too weak to be a (shortest) single axiom for EC. For each, we are content merely to define the appropriate containment set, unification set, kernel(s), and schemata and give the necessary CD arguments in terms of unification. The proofs are contained in various tables.

Before turning to the first of the four, we give the following remark but without the tedious and straightforward details of its proof. The remark is relied upon throughout the rest of this section.

Remark 3.1.1: If $E(A,B)$ and $E(A',B')$ can be unified, where A, B, A', B' are all well-formed expressions of EC, then the pairs A,A' and B,B' can be respectively unified. Furthermore, if σ is a most general unifier of A and A', and if the most general common instance of $E(A,B)$ and $E(A',B')$ is of length p, then σB and $\sigma B'$ unify and the length of their most general common instance is strictly less than p. In addition the replacement terms that occur in the unification of σB and $\sigma B'$ are the same (except for possible variable renaming) as their correspondents that occur in the unification of $E(A,B)$ with $E(A',B')$. By symmetry, the respective roles of A and B and A' and B' can be interchanged with the corresponding remarks for a most general unifier τ.

3.2 XJL In this section we prove that

$$XJL = E(x,E(y,E(E(E(z,y),x),z)))$$

is too weak to be a single axiom for the equivalential calculus. The proof proceeds by first letting XJL be denoted by K.

The schemata to be used in the definition of C are:

1. $K = XJL = E(x,E(y,E(E(E(z,y),x),z)))$
2. $f(A) = E(y,E(E(E(z,y),A),z))$

3. $g(B,A) = E(E(E(z,B),A),z)$
4. $i(A,B) = E(A,B)$

where A and B are pure formulas and also $f(A)$, $g(B,A)$, and $i(A,B)$ are pure. Note that K is indeed a kernel.

Definition Let C_0 consist of K alone. For $i = 0, 1, 2, \ldots$, let C_{i+1} be the union of: C_i; all $f(A)$ with A in C_i; all $g(B,A)$ with A and B in C_i; and $i(A,B)$ with A and B in C_i. Then let C equal the union over i of C_i.

The schemata for U are:

1. w
2. $f(S) = E(y,E(E(E(z,y),S),z))$
3. $g(S,A) = E(E(E(z,S),A),z)$
4. $g(B,S) = E(E(E(z,B),S),z)$
5. $i(S,B) = E(S,B)$
6. $i(A,S) = E(A,S)$

where A and B are pure formulas and where S, $f(S)$, $g(S,A)$, $g(B,S)$, $i(S,B)$, and $i(A,S)$ are almost pure formulas with isolated variable w.

Definition Let U_0 consist of the expression, w, alone. For $i = 0, 1, 2, \ldots$, let U_{i+1} be the union of: U_i; all $f(S)$ for S in U_i; all $g(S,B)$ for S in U_i and B in C; all $g(B,S)$ with S in U_i and B in C; all $i(S,B)$ and all $i(B,S)$ with S in U_i and B in C. Then let U equal the union over i of U_i.

Lemma 3.2.1 *If the pair S in U and B_0 in C are unifiable, then the key replacement term t for the isolated variable w in S occurring in the unification is itself an element of C.*

Proof: Let S be an element of U and B_0 be an element of C. If S and B_0 are not unifiable, there is nothing to prove. Now assume that S and B_0 are unifiable. Then S and B_0 have a most general common instance. The proof is one of induction on the length of this most general common instance, where length is defined as the symbol count. If the length, p, is one, the lemma holds vacuously since all elements of C have length at least eleven. Next, assume by induction that the lemma holds for all unifiable pairs whose *MGCI* is of length less than p, and let S and B_0 be unifiable with *MGCI* of length p. The proof is one of case analysis on the possible forms for both S and B_0. The results of this case analysis are given in a table below in terms of schemata rather than in terms of formulas. The columns are indexed by the possible forms for S, while the rows are indexed by those for B_0.

Each entry in the table reflects the outcome of consideration of a pair of schemata for unification. There are three possible outcomes:

1. the unification fails
2. the unification succeeds, and the key replacement term is in C and is found in the corresponding table entry
3. the attempted unification reduces to the attempted unification of another pair of schemata, where the pair is found in the corresponding table entry.

In this third case, the length of the *MGCI* of the formulas represented by the second pair is strictly less than that of the formulas represented by the original pair under consideration. Remark 3.1.1 comes into play. If this third case terminates with successful unification, we appeal to the induction hypothesis to prove that the key replacement term is in C.

Before presenting the table, we cite one example, taken from the table, to illustrate each of the three cases.

1. Consider $S = f(T) = E(y,E(E(E(x,y),T),x))$ and $B_0 = g(B,D) = E(E(E(z,B),D),z)$. Clearly, y must become $E(E(z,B),D)$. But z must then unify with a term containing z itself, which is impossible.
2. Suppose $S = w$ and $B_0 = K$. Then the key replacement term is K itself.
3. Now suppose that $S = f(T)$ and $B_0 = f(B)$. The unification question immediately reduces to one for T and B. Recall that we are assuming purity of $f(B)$, almost purity of $f(T)$, and disjointness of the sets of variables for $f(T)$ and $f(B)$.

XJL	K	$f(B)$	$g(B,D)$	$i(B,D)$
w	K	$f(B)$	$g(B,D)$	$i(B,D)$
$f(T)$	failure	$T;B$	failure	$g(B,T);D$
$g(T,A)$	failure	failure	$T;B$	$i(i(D,T),A);B$
$g(A,T)$	failure	failure	$T;D$	$i(i(D,A),T);B$
$i(T,A)$	$f(T);A$	$g(T,B);A$	$T;i(i(A,B),D)$	$T;B$
$i(A,T)$	$T;f(A)$	$T;g(A,B)$	$i(i(T,B),D);A$	$T;D$

Examination of the table completes the proof.

Lemma 3.2.1 establishes that U is a unification set for XJL and C. More importantly, this lemma enables us to prove the following theorem that in turn shows XJL too weak to be a single axiom for EC.

Theorem 3.2.1 *The set, C, of formulas is closed under condensed detachment, and the only kernel, within alphabetic variancy, to be found in any element of C is K = XJL.*

Proof: The proof is one of case analysis. We focus attention on the possible forms for the major premiss of the various cases of condensed detachment:

Case 1. Assume the major premiss is $K = XJL$ itself. (To conform to the definition of the various schemata under consideration, we assume throughout the proof that purity is present.) The condensed detachment of K with any A of EC yields $f(A)$. Since, by definition, $f(A)$ is in C whenever A is, closure is preserved in this case.

Case 2. Let the major premiss be $f(A)$ with A in C. It is trivial to verify that the condensed detachment of $f(A)$ and any B is $g(B,A)$. As above, if A and B are in C, then $g(B,A)$ is also.

Case 3. Let $g(B,A)$ with B,A in C be the major premiss. For an arbitrary choice of D from the equivalential calculus as minor premiss, the condensed detachment question can be settled by considering the unification question

for $E(E(w,B),A)$ with D. If the unification is successful, the inference of interest is determined by the key replacement term, the term to be substituted for w. That $E(E(w,B),A)$ is in U can be seen by letting $S_2 = w$, $S_1 = i(S_2,B)$, and noting that $i(S_1,A)$ is in U. When D is restricted to be an element of C, Lemma 3.2.1 forces the key replacement term in question, say D', to be in C. Since the CD of $g(B,A)$ and D will be just D' itself, C is closed under this set of condensed detachments.

Case 4. Let $E(A,B)$ be the major premiss for some A and B in C. Since A and B are by definition assumed to have no variables in common, the condensed detachment with some D in C will either fail or yield B, and again closure is preserved. This completes the proof of closure for C.

That the only kernel to be found in any element of C is K follows from the definition of the classes of elements comprising C, which completes the proof of the theorem.

3.3 XKE In this section we prove that

$$XKE = E(x,E(y,E(E(x,E(z,y)),z)))$$

is too weak to be a single axiom for the EC. The proof proceeds as that for XJL.

The schemata to be used in the definition of C are:

1. $K = XKE = E(x,E(y,E(E(x,E(z,y)),z)))$
2. $f(A) = E(y,E(E(A,E(z,y)),z))$
3. $g(B,A) = E(E(B,E(z,A)),z)$
4. $i(A,B) = E(A,B)$

where A and B are pure formulas and also $f(A)$, $g(A,B)$, and $i(A,B)$ are pure. C is the minimal set generated by K and closed under the operations of f, g, i, which is just the analogue of the definition of the corresponding C for XJL.

The schemata for U are:

1. w
2. $f(S) = E(y,E(E(S,E(z,y)),z))$
3. $g(S,A) = E(E(S,E(z,A)),z)$
4. $g(B,S) = E(E(B,E(z,S)),z)$
5. $i(S,B) = E(S,B)$
6. $i(A,S) = E(A,S)$

where A and B are pure formulas and where S, $f(S)$, $g(S,A)$, $g(B,S)$, $i(S,B)$, and $i(A,S)$ are almost pure formulas with isolated variable w. Essentially, U is the set generated by w and closed under the operations represented by schemata 2 through 6 above, which is just the analogue of the definition of the corresponding U for XJL.

For this C and this U, both dependent on XKE, we can prove the analogue to Lemma 3.2.1.

Lemma 3.3.1 *If the pair S in U and B_0 in C are unifiable, then the key replacement term t for the isolated variable w in S occurring in the unification is itself an element of C.*

Proof: As in Lemma 3.2.1, this proof is by induction on the length of the most general common instance of S and B_0. Remark 3.1.1 again comes into play.

XKE	K	$f(B)$	$g(B,D)$	$i(B,D)$
w	K	$f(B)$	$g(B,D)$	$i(B,D)$
$f(T)$	failure	$T;B$	failure	$g(T,B);D$
$g(T,A)$	failure	failure	$T;B$	$i(T,i(D,A));B$
$g(A,T)$	failure	failure	$T;D$	$i(A,i(D,T));B$
$i(T,A)$	$f(T);A$	$g(B,T);A$	$T;i(B,i(A,D))$	$T;B$
$i(A,T)$	$T;f(A)$	$T;g(B,A)$	$i(B,i(T,D));A$	$T;D$

The proof of Lemma 3.3.1 is thus obtained.

Lemma 3.3.1 establishes that U is a unification set for XKE and C. More importantly, we can prove Theorem 3.3.1 which shows XKE too weak to be a single axiom for EC.

Theorem 3.3.1 *C (which is dependent on XKE) is closed under condensed detachment, and the only kernel (within alphabetic variancy) to be found in any element of C is $K = XKE$.*

Proof: As in Theorem 3.2.1, we proceed by case analysis by focusing attention on the forms for the major premiss of the various cases of condensed detachment.

The following summary suffices. The condensed detachment of K as major premiss with any A of EC is $f(A)$. The CD of $f(A)$ for any A in C with any B of EC is $g(A,B)$. The CD of $g(A,B)$ for A,B in C with some D in C reduces to the unification question of $E(A,E(w,B))$ with D, and Lemma 3.3.1 applies since this $E(A,E(w,B))$ is in U. And finally, the CD of $i(A,B)$ with D for A and B and D in C either fails or is B.

Examination of the definition of C shows that $K = XKE$ is the only kernel therein, which completes the proof.

One can immediately see that C contains $CL(XKE)$ but does not contain $E(x,x)$. So XKE is too weak to be a single axiom for the equivalential calculus.

3.4 XAK The formula,

$$XAK = E(x,E(E(E(E(y,z),x),z),y)),$$

is too weak to be a single axiom. This result can be established by defining a C and a U, each dependent on XAK, and proceeding as with XJL and XKE.

The schemata to be used in the definition of C, which is shown to be a containment set for XAK by examining the following tables, are:

1. $K = XAK = E(x,E(E(E(E(y,z),x),z),y))$
2. $f(A) = E(E(E(E(y,z),A),z),y)$
3. $g(A,B) = E(E(E(A,z),B),z)$
4. $i(A,B) = E(A,B)$

where A and B are pure formulas and also $f(A)$, $g(A,B)$, and $i(A,B)$ are pure.

C is the minimal set generated by K and closed under the operations of f, g, i, which is just the analogue of the definitions of the corresponding C for XJL and XKE.

The schemata for U, which is shown to be a unification set, are:

1. w
2. $f(S) = E(E(E(E(y,z),S),z),y)$
3. $g(S,A) = E(E(E(S,z),A),z)$
4. $g(B,S) = E(E(E(B,z),S),z)$
5. $i(S,B) = E(S,B)$
6. $i(A,S) = E(A,S)$

where A and B are pure formulas and where S, $f(S)$, $g(S,A)$, $g(B,S)$, $i(S,B)$, and $i(A,S)$ are almost pure formulas with isolated variable w. Essentially, U is the set generated by w and closed under the operations represented by schemata 2 through 6 above, which is just the analogue of the definitions of the corresponding U for XJL and XKE.

Unification table for U and C:

XAK	K	$f(B)$	$g(B,D)$	$i(B,D)$
w	K	$f(B)$	$g(B,D)$	$i(B,D)$
$f(T)$	failure	$T;B$	$i(T,D);B$	$g(D,T);B$
$g(T,A)$	failure	$T;i(B,A)$	$T;B$	$i(i(T,D),A);B$
$g(A,T)$	failure	$i(B,T);A$	$T;D$	$i(i(A,D),T);B$
$i(T,A)$	$f(T);A$	$T;g(A,B)$	$T;i(i(B,A),D)$	$T;B$
$i(A,T)$	$T;f(A)$	$g(T,B);A$	$i(i(B,T),D);A$	$T;D$

Condensed detachment table for XAK:

Major premiss	Condensed detachment with D in C reduces to
K	$f(D)$
$f(A)$	unification of $g(w,A)$ with D
$g(A,B)$	unification of $i(i(A,w),B)$ with D
$i(A,B)$	B (if A and D unify; failure otherwise)

This concludes the discussion of XAK.

3.5 BXO We now come (in this paper) to the last of the four candidates for the status of shortest single axiom for EC, namely,

$$BXO = E(E(E(E(x,E(y,z)),z),y),x).$$

(In a second paper we dispatch the remaining three candidates, XCB, XHK, and XHN. This task is accomplished by extending the method described herein.)

BXO is rather more interesting than its three predecessors in that immediately one infers $E(x,E(y,E(x,y)))$ from the condensed detachment of BXO with itself. Thus a second kernel is quickly present. What may be surprising is the fact that no further kernels arise. Hence we can conclude that BXO is

also too weak to be a single axiom for EC, although the case analysis is somewhat more complicated.

The schemata to be used in the definition of C, which is shown to be a containment set for BXO, are:

1. $K = BXO = E(E(E(E(x,E(y,z)),z),y),x)$
2. $f(A) = E(E(E(A,E(y,z)),z),y)$
3. $g(A,B) = E(E(A,E(B,z)),z)$
4. $i(A,B) = E(A,B)$
5. $K' = E(x,E(y,E(x,y)))$
6. $h(A) = E(y,E(A,y))$
7. $j(A) = E(E(z,E(E(A,z),y)),y)$
8. $n(A,B) = E(z,E(E(A,z),B))$

where A and B are pure formulas and also $f(A)$, $g(A,B)$, $h(A)$, $i(A,B)$, $n(A,B)$, and $j(A)$ are pure. C is the minimal set generated by K and K' and closed under the operations of f, g, h, i, j, n, which is just the analogue of the definitions of the corresponding C for XJL, XKE, and XAK.

The schemata for U, which is shown to be a unification set, are:

1. w
2. $f(S) = E(E(E(S,E(y,z)),z),y)$
3. $g(S,A) = E(E(S,E(A,z)),z)$
4. $g(B,S) = E(E(B,E(S,z)),z)$
5. $i(S,B) = E(S,B)$
6. $i(A,S) = E(A,S)$
7. $h(S) = E(y,E(S,y))$
8. $j(S) = E(E(z,E(E(S,z),y)),y)$
9. $n(S,A) = E(z,E(E(S,z),A))$
10. $n(B,S) = E(z,E(E(B,z),S))$

where A and B are pure formulas and where S, $f(S)$, $g(S,A)$, $g(B,S)$, $i(S,B)$, $i(A,S)$, $h(S)$, $j(S)$, $n(S,A)$, and $n(B,S)$ are almost pure formulas with isolated variable w. Essentially, U is the set generated by w and closed under the operations represented by schemata 2 through 10 above, which is just the analogue of the definitions of the corresponding U for XJL, XKE, and XAK.

Unification table for U and C:

BXO	K	$f(B)$	$g(B,D)$	$i(B,D)$
w	K	$f(B)$	$g(B,D)$	$i(B,D)$
$f(T)$	$T;K'$	$T;B$	$i(T,h(D));B$	$g(T,D);B$
$g(T,A)$	$T;j(A)$	$T;i(B,h(A))$	$T;B$	$i(T,i(A,D));B$
$g(A,T)$	$j(T);A$	$i(B,h(T));A$	$T;D$	$i(A,i(T,D));B$
$i(T,A)$	$T;f(A)$	$T;g(B,A)$	$T;i(B,i(D,A))$	$T;B$
$i(A,T)$	$f(T);A$	$g(B,T);A$	$i(B,i(D,T));A$	$T;D$
$h(T)$	failure	failure	failure	$i(T,B);D$
$j(T)$	failure	failure	$i(T,B);D$	$n(T,D);B$
$n(T,A)$	failure	failure	failure	$i(i(T,B),A);D$
$n(A,T)$	failure	failure	failure	$i(i(A,B),T);D$

BXO	K'	$h(B)$	$j(B)$	$n(B,D)$
w	K'	$h(B)$	$j(B)$	$n(B,D)$
$f(T)$	failure	failure	failure	failure
$g(T,A)$	failure	failure	$i(B,T);A$	failure
$g(A,T)$	failure	failure	$T;i(B,A)$	failure
$i(T,A)$	$h(T);A$	$i(B,T);A$	$T;n(B,A)$	$i(i(B,T),D);A$
$i(A,T)$	$T;h(A)$	$T;i(B,A)$	$n(B,T);A$	$T;i(i(B,A),D)$
$h(T)$	failure	$T;B$	failure	$T;i(B,D)$
$j(T)$	failure	failure	$T;B$	failure
$n(T,A)$	$h(T);A$	$i(T,A);B$	failure	$T;B$
$n(A,T)$	$T;h(A)$	$i(A,T);B$	failure	$T;D$

Condensed detachment table for BXO:

Major premiss	Condensed detachment with D in C reduces to
K	unification of $f(w)$ with D
$f(A)$	unification of $g(A,w)$ with D
$g(A,B)$	unification of $i(A,i(B,w))$ with D
$i(A,B)$	B (if A and D unify; failure otherwise)
K'	$h(D)$
$h(A)$	$i(A,D)$
$j(A)$	unification of $n(A,w)$ with D
$n(A,B)$	$i(i(A,D),B)$

This concludes the discussion of BXO except for one important point, namely, there are two kernels present in the theorems deducible from BXO instead of just one as in the other cases. They are BXO itself, which is usual for this study, and $E(x,E(y,E(x,y)))$. It is the presence of this second kernel that makes this study of BXO rather more interesting.

4 Use of an automated theorem-proving program At this point, we touch briefly on the methodology and also on aspects of the automated theorem-proving program employed in obtaining our results. The assistance of such a program was invaluable in completing this study. A more complete treatment of the method and use of the program can be found in [26]. Examination of the following material may suggest to the logician other uses for such a program.

The language required by the program is a modified first-order predicate calculus. For the problem at hand, we use a one-place predicate P to represent "is deducible", and "$-$" to represent "not". Thus the wff $P(E(x,x))$ states that $E(x,x)$ is deducible. The conjunct

$$-P(E(x,y)) \quad -P(x) \quad P(y)$$

states the rule of condensed detachment: for any x and y, if $E(x,y)$ and x are both deducible, then y is also deducible. Although the first inference rule of note was binary resolution [18], which combines substitution with a generalization of modus ponens and syllogism, a number of inference rules are now

extant in the program. One of these, *UR*-resolution [9], actually performs condensed detachment when supplied with the encoding of condensed detachment given above. When seeking to prove that a particular formula is a single axiom, the program generates formulas by repeated application of condensed detachment. These formulas are continually compared to a list of known single axioms. The object is that of noting when a known single axiom has been derived. Because of the need to avoid examination of the myriad of formulas that would naturally arise, various powerful strategies must be used to guide the search. We now briefly describe certain of these.

One strategy is to key on certain formulas. This strategy is especially useful in seeking shorter proofs of known theorems (see Appendix). Examination of the work of Kalman [3] and that of Peterson [15] reveals that certain formulas that occur while attempting to establish that a formula is a single axiom are exceedingly powerful. Examples are:

1. the given formula under study and the one immediately deducible from it by a single application of *CD*
2. formulas that have certain structural properties, such as the occurrence of a variable as the first argument of a formula
3. certain formulas that arise repeatedly in related proofs found in the literature.

The program can be instructed to place these formulas on special lists [19], and/or it can be instructed to assign them high priority by means of "weighting" [10]. Such an instruction enables the program to prefer such a formula as a premiss for *CD*. One can thus "build in" one's intuition and/or take advantage of known structure when using the program.

Certain other formulas, like $E(E(x,y),t)$ for any t other than $E(y,x)$, if felt to be unnecessary (because they did not occur in proofs of other single axioms) can be avoided (as in searching for a different or shorter proof, see Appendix). These formulas can be removed from consideration by assigning them low priority or by subsumption (the removal of formulas that are either less general than or identical to ones already present [18]). For example, to prevent the program from finding the same proof of *XGK* as given by Kalman [3], certain formulas of his proof were put on a special list that was not used for *CD*. If any of these formulas were generated by the program, they were discarded by subsumption. Thus certain steps in Kalman's proof were blocked. With such a mechanism one can easily explore a wide variety of alternate proofs.

A major use of the program was that of gathering information on the structure of formulas derivable from the one being studied. The purpose of many runs was not to generate a proof, but rather to identify patterns in the formulas and to formulate conjectures about the space of derivable theorems. In one instance, we had the program generate a number of the derivable theorems from *XAK*, the formula then under study.

To aid in the examination of the derived formulas, we employed a standard mathematical approach—that of using notation to simplify the form of the formulas. When using the program, one has access to such simplifying notation by means of demodulation [24]. For example, when the equality

$$E(x,E(E(E(E(y,z),x),z),y)) = K$$

($XAK = K$) is adjoined, the program automatically replaces every occurrence of XAK by the single constant K. Examination of the transformed formulas generated by the program led directly to the conjecture that all theorems derivable from XAK by CD contain a variant of XAK as a kernel. Use of demodulation coupled with a series of program runs alternated with analyses of the runs then led to the discovery of the various schemata used in completing the proof of the conjecture.

Before the given study was completed, it was necessary to refute a number of conjectures about the structure of the derivable theorems which, although natural, were easily rejected only because of access to the program. These conjectures required counting various symbol occurrences and also classifying formulas according to their structure—that briefly alluded to in 2 above. Although we could have used tedious hand counting or could have written yet another program, instead this study led to the formulation of new uses of demodulation. The new uses include scanning formulas as they are derived, counting symbol occurrences, and classifying formulas [23].

Finally, once the schemata had been discovered, the program was used to study the interaction of these schemata under CD. This led almost immediately to the case analysis given earlier and presented in tabular form. An alternate and, as it turned out, pointless case analysis had been pursued for some time. It was found wanting and was thus terminated because of information derived directly from use of the program. Of equal importance, the results obtained with the program pointed the way to the correct nature of the case analysis and the corresponding induction argument.

The techniques of this section, especially the use of demodulation and weighting, have proven to be applicable to many areas of study.

*5 **Conclusions*** We have proved here that each of the four formulas, XJL, XKE, XAK, and BXO, is too weak to be a shortest single axiom for the equivalential calculus. Each of the corresponding proofs exemplifies a method that studies the set of theorems deducible therein. We were able with this method to examine the infinite domain of deducible theorems in each of the four cases by finding a finite presentation. We in fact found, for each of the four, a finite set of schemata that proved that certain well-known theorems of the calculus are not present even as subexpressions of any of the theorems deducible from the formula. These studies were conducted by relying heavily on a general-purpose automated theorem-proving program. Furthermore, the information was obtained without recourse to any special programming, which suggests that the system in its present state may prove useful to those interested in conducting various types of research but without the burden of programming.

Among the kinds of questions that one might consider attacking with this automated theorem-proving program are the following. What is the full set of theorems deducible from a given formula or set of formulas? For a given set of formulas and a given domain, does that set axiomatize the domain? Are the elements of the set independent? Can an alternate and/or a shorter proof than that which is known be found for a specified theorem? Can a proof be found for a purported theorem? Can a counterexample be found for a given

conjecture? Can a model, especially a small finite model, be generated for a set of axioms?

Since we have succeeded in answering questions of the listed types with the system [20,21,22], we are encouraged to ask for additional open questions on which to work.

We have included here at least some details relevant to the theorem-proving techniques for accomplishing the above tasks. We hope thereby to further suggest uses of the system. For example, both the concept of kernel and the corresponding conjectures for the four formulas studied here resulted directly from the use of the procedure of demodulation in its function of simplification.

Finally, we wish to dispel the possible notion that the method employed in Section 3 relies on the weakness of the formulas therein. We shall in fact show in a succeeding paper that the method can be applied to both sides of the question, that is, it can also be used to prove a formula strong enough to be a single axiom when that is the case. In fact two new shortest single axioms for the equivalential calculus have been found. The method, together with the automated theorem-proving program, has also been used to answer certain open questions in both the R-calculus and L-calculus. Thus, at least in this context, the method has the property of correctly establishing either adequacy or inadequacy for the property of being a single axiom.

The nature of the methodology presented in this paper leads one to conjecture that in no way is it dependent specifically on the equivalential calculus. The successful examination of infinite domains gives rise to the thought that a number of the techniques may well apply to other areas of formal logic and perhaps to other areas of mathematics.

Appendix: A shorter proof The following proof, employing condensed detachment, establishes that XGK is a shortest single axiom for the equivalential calculus. The standard approach is used, namely, we show that PYO [13,15], one of the known single axioms for EC, is derivable by condensed detachment from XGK. The following proof is roughly half the length of that given by Kalman [3].

Proof:

1			$E(x,E(E(y,E(z,x)),E(z,y)))$
2	1	1	$E(E(x,E(y,E(z,E(E(u,E(v,z)),E(v,u))))),E(y,x))$
3	2	1	$E(E(E(E(x,E(y,z)),E(y,x)),E(z,u)),u)$
4	3	3	$E(x,x)$
5	1	4	$E(E(x,E(y,E(z,z))),E(y,x))$
6	5	1	$E(E(x,E(x,y)),y)$
7	2	6	$E(x,E(y,E(y,E(x,E(z,E(E(u,E(v,z)),E(v,u)))))))$
8	5	6	$E(x,E(y,E(y,E(x,E(z,z)))))$
9	2	8	$E(x,E(y,E(y,x)))$
10	1	9	$E(E(x,E(y,E(z,E(u,E(u,z))))),E(y,x))$
11	2	7	$E(x,E(E(E(y,E(z,u)),E(z,y)),E(u,x)))$
12	5	11	$E(E(E(x,E(y,z)),E(y,x)),z)$
13	1	12	$E(E(x,E(y,E(E(E(z,E(u,v)),E(u,z)),v))),E(y,x))$

14	10	1	$E(E(E(x,E(x,y)),E(y,z)),z)$
15	14	11	$E(x,E(y,E(y,E(E(z,E(u,x)),E(u,z)))))$
16	13	1	$E(E(x,E(E(E(y,E(z,x)),E(z,y)),u)),u)$
17	16	1	$E(x,E(y,E(x,y)))$
18	17	17	$E(x,E(E(y,E(z,E(y,z))),x))$
19	1	18	$E(E(x,E(y,E(z,E(E(u,E(v,E(u,v))),z)))),E(y,x))$
20	19	15	$E(E(x,y),E(y,x))$
21	1	20	$E(E(x,E(y,E(E(z,u),E(u,z)))),E(y,x))$
22	21	1	$E(E(E(x,y),E(E(y,x),z)),z)$
23	22	11	$E(x,E(E(y,z),E(z,E(y,x))))$
24	2	23	$E(E(E(x,E(y,z)),z),E(y,x)) = PYO.$

REFERENCES

[1] Belnap, N., "The two-property," *Relevance Logic Newsletter 1*, (1976), pp. 173-180.

[2] Kalman, J., "Computer studies of $T\rightarrow - W - I$," *Relevance Logic Newsletter 1*, (1976), pp. 181-188.

[3] Kalman, J., "A shortest single axiom for the classical equivalential calculus," *Notre Dame Journal of Formal Logic*, vol. 19, no. 1 (1978), pp. 141-144.

[4] Kalman, J., "Substitution-and-detachment systems related to Abelian groups," with an appendix by C. A. Meredith, pp. 22-31 in *A Spectrum of Mathematics, Essays presented to H. G. Forder*, Auckland University Press, Auckland, New Zealand, 1971.

[5] Kalman, J., private communication.

[6] Łukasiewicz, J., "Der Aquivalenzenkalkul," *Collectanea Logica*, vol. 1 (1939), pp. 145-169. English translation in [8], pp. 88-115 and in [7], pp. 250-277.

[7] Łukasiewicz, J., *Jan Łukasiewicz: Selected Works*, ed., L. Borkowski, North-Holland Publishing Company, Amsterdam, 1970.

[8] McCall, S., *Polish Logic, 1920-1939*, Clarendon Press, Oxford, 1967.

[9] McCharen, J., R. Overbeek, and L. Wos, "Problems and experiments for and with automated theorem proving programs," *IEEE Transactions on Computers*, vol. C-25 (1976), pp. 773-782.

[10] McCharen, J., R. Overbeek, and L. Wos, "Complexity and related enhancements for automated theorem-proving programs," *Computers and Mathematics with Applications*, vol. 2 (1976), pp. 1-16.

[11] Meredith, C., "Single axioms for the systems (C,N), (C,O) and (A,N) of the two-valued propositional calculus," *The Journal of Computing Systems*, vol. 1, no. 3 (1953), pp. 155-164.

[12] Meredith, C. and A. Prior, "Notes on the axiomatics of the propositional calculus," *Notre Dame Journal of Formal Logic*, vol. 4 (1963), pp. 171-187.

[13] Peterson, J., "Shortest single axioms for the equivalential calculus," *Notre Dame Journal of Formal Logic*, vol. 17 (1976), pp. 267-271.

[14] Peterson, J., "Single axioms for the classical equivalential calculus," *Auckland University Department of Mathematics Report Series No. 78*, 1976.

[15] Peterson, J., "The possible shortest single axioms for *EC*-tautologies," *Auckland University Department of Mathematics Report Series No. 105*, 1977.

[16] Peterson, J., "An automatic theorem prover for substitution and detachment systems," *Notre Dame Journal of Formal Logic*, vol. 19 (1978), pp. 119-122.

[17] Prior, A. N., *Formal Logic*, 2nd Ed., Clarendon Press, Oxford, 1962.

[18] Robinson, J., "A machine-oriented logic based on the resolution principle," *Journal of the Association for Computing Machinery*, vol. 12 (1965), pp. 23-41.

[19] Smith, B., "Reference manual for the environmental theorem prover," to be published as an Argonne National Laboratory technical report.

[20] Winker, S. and L. Wos, "Automated generation of models and counterexamples and its application to open questions in ternary Boolean algebra," pp. 251-256 in *Proceedings of the Eighth International Symposium on Multiple-Valued Logic*, Rosemont, Illinois, 1978.

[21] Winker, S., L. Wos, and E. Lusk, "Semigroups, antiautomorphisms, and involutions: a computer solution to an open problem, I," *Mathematics of Computation*, vol. 37 (1981), pp. 533-545.

[22] Winker, S., "Generation and verification of finite models and counterexamples using an automated theorem prover answering two open questions," *Journal of the Association for Computing Machinery*, vol. 29 (1982), pp. 273-284.

[23] Winker, S. and L. Wos, "Procedure implementation through demodulation and related tricks," *6th Conference on Automated Deduction*, vol. 138, *Lecture Notes in Computer Science* (1982), pp. 109-131.

[24] Wos, L., G. Robinson, D. Carson, and L. Shalla, "The concept of demodulation in theorem proving," *Journal of the Association for Computing Machinery*, vol. 14 (1967), pp. 698-709.

[25] Wos, L., S. Winker, and E. Lusk, "An automated reasoning system," *AFIPS Conference Proceedings*, vol. 50 (1981), National Computer Conference, Chicago, Illinois, 1981, AFIPS Press, pp. 697-702.

[26] Wos, L., S. Winker, R. Veroff, B. Smith, and L. Henschen, "A new use of an automated reasoning assistant: open questions in equivalential calculus and the study of infinite domains," submitted for publication.

L. Wos, S. Winker, and B. Smith

Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439

L. Henschen

Computer Science Department
Northwestern University
Evanston, Illinois 60201

R. Veroff

Department of Computer Science
University of New Mexico
Albuquerque, New Mexico 87131