THE JOURNAL OF SYMBOLIC LOGIC
Volume 41, Number 1, March 1976

TWO VARIABLE IMPLICATIONAL CALCULI OF PRESCRIBED MANY-ONE DEGREES OF UNSOLVABILITY

CHARLES E. HUGHES

Abstract. A constructive proof is given which shows that every nonrecursive r.e. many-one degree is represented by the family of decision problems for partial implicational propositional calculi whose well-formed formulas contain at most two distinct variable symbols.

Introduction. Let $p_1, p_2, \cdots$ be the set of all propositional variables in some formulation of the propositional calculus. P_n will be used to denote the class of all well-formed formulas (wffs) of the implicational propositional calculus which involve only variables among $\{p_1, p_2, \cdots, p_n\}$. An *n-adic partial implicational propositional calculus* (PIPC), I, is an inference system defined by a finite set of tautologies from P_n. Its rules of inference are modus ponens and substitution of wffs from P_n. The *decision problem* for I is the problem to decide of an arbitrary member W of P_n whether or not W is derivable (deducible) in I. We denote W being derivable in I by $\vdash_I W$. The *general decision problem for n-adic PIPC's*, denoted by $\mathscr{I}_n$, is the family of decision problems which ranges over all such systems.

n-adic PIPC's have been studied for $n = 3$ by Hughes and Singletary [3], for $n = 2$ by Wajsberg [6] and for $n = 2$ and $n = 1$ by Gladstone [1]. In [3] it was shown that every nonrecursive r.e. many-one (but not one-one) degree is represented by $\mathscr{I}_3$. In [6] it was shown that no n-adic PIPC, for $n < 3$, can derive all tautologies of the full implicational calculus where substitution of arbitrary wffs was allowable. In [1] Gladstone demonstrated that the set of all tautologies of P_1 (respectively P_2) cannot be derived by any 1-adic (respectively 2-adic) PIPC. Gladstone posed the problem as to whether or not there exists a 1-adic or 2-adic (hereafter called diadic) PIPC whose decision problem is recursively unsolvable. We address ourselves here to diadic calculi and demonstrate not only the existence of an unsolvable instance but we also precisely categorize the degree structure of the general decision problem $\mathscr{I}_2$. Our results, first announced in [2], parallel those given in [3] for $\mathscr{I}_3$. Our construction techniques are however quite different from any others previously used in the study of PIPC's in as much as we simulate halting problems for Turing machines as opposed to words problems for restrictions of Post's canonical forms (see, e.g., [7] and [5]).

Turing machines. A *Turing machine* M is a combinatorial system defined by a *tape alphabet* Σ, a *state set* Q and a *Turing table* T. For this paper the tape alphabet

Received December 5, 1973.

of all machines is $\{0, 1\}$, where 0 represents the blank symbol. The Turing table T is a set of quadruples each of the form $qaDs$ where q, $s \in Q$, and $D \in \{R, L, 0, 1\}$. Each pair qa such that $q \in Q$, $a \in \{0, 1\}$ is called a *discriminant* and at most one quadruple in T may start with qa. M possesses an infinite tape with but a finite number of 1 marks recorded on it. At any given time M is in some state $q \in Q$ and is scanning some one square of its tape. A *configuration* C of M is an instantaneous description of M's current status and is represented by a sequence of the form $b_1b_2 \cdots b_iqab_{i+1} \cdots b_{i+h}$, where $h \geq 0$, a is the scanned symbol, $i \geq 0$, q is a state symbol and $b_1b_2 \cdots b_iab_{i+1} \cdots b_{i+h}$ is the smallest segment of the tape containing all squares marked with 1 and the scanned square. If M is a configuration C, as described above, then the quadruple starting with qa, if it exists, determines the next configuration C' of M in the following manner:

$qaRs \in T$—M moves one square to the right of the current scanned square and changes state to s.
$qaLs \in T$—M moves one square to the left of the current scanned square and changes state to s.
$qabs \in T$—where $b \in \{0, 1\}$. M changes the symbol in the scanned square to b and goes to state s.

C' as determined above is then called the *immediate successor* of C in M. Any C which contains a discriminant qa such that no quadruple in T starts with qa is called *terminal* and has no immediate successor.

Let C_1 and C_2 be arbitrary configurations of M. Then C_2 is said to be *derivable* from C_1 if there exists some sequence $S_1, \cdots, S_m$, $m \geq 1$, of configurations such that $S_1 = C_1$, $S_m = C_2$ and if $m > 1$, S_{i+1} is the immediate successor S_i, for $1 \leq i < m$. A configuration C_1 is said to be *mortal* if there exists a terminal configuration C_2 such that C_2 is derivable from C_1. The *halting problem* for M is the problem to decide for an arbitrary configuration C of M whether or not C is mortal. The *general halting problem for Turing machines*, denoted $\mathscr{H}$, is then the class of all such problems.

Reduction of $\mathscr{H}$ to $\mathscr{I}_2$. Let M be an arbitrary Turing machine with tape alphabet $\{0, 1\}$, state set $Q = \{q_1, \cdots, q_n\}$ and Turing table T. From the description of M we shall now construct a diadic PIPC, D, whose decision problem is of the same many-one degree as the halting problem for M. Prior to demonstrating D we have need of the following abbreviations for certain classes of wffs.

$I(p)$ is defined to abbreviate the wff $[p \supset p]$.
$\Phi_0(p)$ is $[p \supset I(p)]$, i.e., $[p \supset [p \supset p]]$.
$\Phi_1(p)$ is $[p \supset \Phi_0(p)]$.
$\xi_1(p)$ is $[p \supset \Phi_1(p)]$.
$\xi_2(p)$ is $[p \supset \xi_1(p)]$.
$\xi_3(p)$ is $[p \supset \xi_2(p)]$.
$\Psi_1(p)$ is $[p \supset \xi_3(p)]$.
$\Psi_2(p)$ is $[p \supset \Psi_1(p)]$.
$\vdots$
$\Psi_n(p)$ is $[p \supset \Psi_{n-1}(p)]$.

Now let $C = a_{i_1} \cdots a_{i_h} q_m a_{j_1} \cdots a_{j_k}$ be an arbitrary configuration of M. Then define C^* to be the wff $[\Psi_m \Phi_{j_1} \cdots \Phi_{j_k} I(p_1) \vee \Phi_{i_h} \cdots \Phi_{i_1} I(p_1)]$, where $[A \vee B]$ abbreviates $[[A \supset B] \supset B]$, for any wffs A and B. We shall construct D in such a manner that $\vdash_D C^*$ iff C is a mortal configuration of M.

The axioms of D are as below, where the outer set of brackets are standardly omitted in order to better expose premise and conclusion. In studying these axioms the reader should be aware of the following intent. Axiom sets 1 through 8 are designed to effect the derivation of the tautology C^* iff C is a terminal configuration of M. The remainder of the axioms are specified in such a way as to cause C_2^* to be derived from C_1^* by a single application of modus ponens iff C_1 is the immediate successor of C_2 in M, that is to say, they cause D to simulate M in reverse. This, of course, implies that, for C a configuration of M, $\vdash_D C^*$ iff C is mortal. The reader should also note that any wff which may be abbreviated as C^*, for some configuration C of M, has a unique such abbreviation.

1. $[\xi_1 I(p_1) \vee I(p_1)]$.
2. $[\xi_1 I(p_1) \vee I(p_1)] \supset [\xi_1 I(p_1) \vee \Phi_1 I(p_1)]$.
3. $[\xi_1 I(p_1) \vee \Phi_i(p_2)] \supset [\xi_1 I(p_1) \vee \Phi_j \Phi_i(p_2)]$, $\forall i, j \in \{0, 1\}$.
4. $[\xi_1 I(p_1) \vee p_2] \supset [\xi_2 \Phi_1 I(p_1) \vee p_2]$.
5. $[\xi_1 I(p_1) \vee p_2] \supset [\xi_3 \Phi_i I(p_1) \vee p_2]$, $\forall i \in \{0, 1\}$.
6. $[\xi_2 \Phi_i(p_1) \vee p_2] \supset [\xi_2 \Phi_j \Phi_i(p_1) \vee p_2]$, $\forall i, j \in \{0, 1\}$.
7. $[\xi_2 \Phi_i(p_1) \vee p_2] \supset [\xi_3 \Phi_j \Phi_i(p_1) \vee p_2]$, $\forall i, j \in \{0, 1\}$.
8. $[\xi_3 \Phi_i(p_1) \vee p_2] \supset [\Psi_k \Phi_i(p_1) \vee p_2]$, whenever $q_k a_i$ is a terminal discriminant of M.
9. $[\Psi_k \Phi_i(p_1) \vee p_2] \supset [\Psi_h \Phi_j(p_1) \vee p_2]$, whenever $q_h a_j a_i q_k \in T$.

10a. $[\Psi_k \Phi_0 I(p_1) \vee I(p_1)] \supset [\Psi_h \Phi_0 I(p_1) \vee I(p_1)]$,
 b. $[\Psi_k \Phi_1 I(p_1) \vee I(p_1)] \supset [\Psi_h \Phi_0 I(p_1) \vee \Phi_1(p_1)]$,
 c. $[\Psi_k \Phi_i I(p_1) \vee \Phi_j(p_2)] \supset [\Psi_h \Phi_0 I(p_1) \vee \Phi_i \Phi_j(p_2)]$,
 d. $[\Psi_k \Phi_0 \Phi_0 \Phi_i(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_0 \Phi_i(p_1) \vee I(p_2)]$,
 e. $[\Psi_k \Phi_1 \Phi_0 \Phi_i(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_0 \Phi_i(p_1) \vee \Phi_1 I(p_2)]$,
 f. $[\Psi_k \Phi_i \Phi_0 \Phi_j(p_1) \vee \Phi_m(p_2)] \supset [\Psi_h \Phi_0 \Phi_j(p_1) \vee \Phi_i \Phi_m(p_2)]$,
 $\forall i, j, m \in \{0, 1\}$ whenever $q_h 0 L q_k \in T$.

11a. $[\Psi_k \Phi_0 \Phi_1(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_1(p_1) \vee I(p_2)]$,
 b. $[\Psi_k \Phi_1 \Phi_1(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_1(p_1) \vee \Phi_1 I(p_2)]$,
 c. $[\Psi_k \Phi_i \Phi_1(p_1) \vee \Phi_j(p_2)] \supset [\Psi_h \Phi_1(p_1) \vee \Phi_i \Phi_j(p_2)]$,
 $\forall i, j \in \{0, 1\}$ whenever $q_k 1 L q_k \in T$.

12a. $[\Psi_k \Phi_0 I(p_1) \vee I(p_1)] \supset [\Psi_h \Phi_0 I(p_1) \vee I(p_1)]$,
 b. $[\Psi_k \Phi_0 I(p_1) \vee \Phi_0 \Phi_i(p_2)] \supset [\Psi_h \Phi_0 I(p_1) \vee \Phi_i(p_2)]$,
 c. $[\Psi_k \Phi_1(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_0 \Phi_1(p_1) \vee I(p_2)]$,
 d. $[\Psi_k \Phi_0 \Phi_i(p_1) \vee I(p_2)] \supset [\Psi_h \Phi_0 \Phi_0 \Phi_i(p_1) \vee I(p_2)]$,
 e. $[\Psi_k \Phi_0 \Phi_i(p_1) \vee \Phi_0 \Phi_j(p_2)] \supset [\Psi_h \Phi_0 \Phi_0 \Phi_i(p_1) \vee \Phi_j(p_2)]$,
 f. $[\Psi_k \Phi_1(p_1) \vee \Phi_0 \Phi_i(p_2)] \supset [\Psi_h \Phi_0 \Phi_1(p_1) \vee \Phi_i(p_2)]$,
 $\forall i, j \in \{0, 1\}$ whenever $q_h 0 R q_k \in T$.

13a. $[\Psi_k \Phi_0 I(p_1) \vee \Phi_1(p_2)] \supset [\Psi_h \Phi_1 I(p_1) \vee p_2]$,
 b. $[\Psi_k \Phi_1(p_1) \vee \Phi_1(p_2)] \supset [\Psi_h \Phi_1 \Phi_1(p_1) \vee p_2]$,
 c. $[\Psi_k \Phi_0 \Phi_i(p_1) \vee \Phi_1(p_2)] \supset [\Psi_h \Phi_1 \Phi_0 \Phi_i(p_1) \vee p_2]$
 $\forall i \in \{0, 1\}$ whenever $q_h 1 R q_k \in T$.

We shall now set about proving that the halting problem for M and the decision problem for D are equivalent in the sense of many-one degrees. We do this through a series of relatively simple lemmas.

LEMMA 1. *If C is a mortal configuration of M then $\vdash_D C^*$.*

PROOF. This may be seen by observing the axioms of D in order to verify the following which was noted previously:

(a) $\vdash_D C_1^*$, whenever C_1 is a terminal configuration of M, and

(b) $\vdash_D C_2^*$, whenever $C_2 \vdash_M C_1$ and $\vdash_D C_1^*$.

Axioms sets 1 through 8 are used to achieve (a). Axiom set 9 simulates prints in reverse, 10 and 11 left moves in reverse and 12 and 13 right moves in reverse.

LEMMA 2. *A wff of the form $[[A_1 \vee B] \supset [A_2 \vee B]]$ can take the form $[X \vee Y]$, where A_1, A_2, B, C, X and Y are wffs, iff B is $A_2 \vee C$.*

PROOF. By definition $[[A_1 \vee B] \supset [A_2 \vee C]]$ is an abbreviation of

$$[[[A_1 \supset B] \supset B] \supset [A_2 \vee C]]$$

and $[X \vee Y]$ is an abbreviation of $[[X \supset Y] \supset Y]$. But then Y must be identified with both B and $A_2 \vee C$ and hence B must be $A_2 \vee C$.

LEMMA 3. *Every theorem of D may be abbreviated into a substitution instance of one of the following forms:*

Form 1. *Axioms contained in axiom sets* 2 *through* 13.

Form 2. *C^*, where C is a mortal configuration of M.*

Form 3. $[\xi_1 I(p_1) \vee \Phi_{j_1} \cdots \Phi_{j_x} I(p_1)]$, *where* $x \geq 0$, $j_m \in \{0, 1\}$ *for* $m \in (1, \cdots, x - 1)$, *and* $j_x = 1$.

Form 4. $[\xi_2 \Phi_{i_1} \cdots \Phi_{i_y} I(p_1) \vee \Phi_{j_1} \cdots \Phi_{j_x} I(p_1)]$, *where* $y \geq 1$, $x \geq 0$, $i_m \in \{0, 1\}$ *for* $m \in (1, \cdots, y - 1)$, $i_y = 1$, $j_m \in \{0, 1\}$ *for* $m \in (1, \cdots, x - 1)$, *and* $j_x = 1$.

Form 5. $[\xi_3 \Phi_{i_1} \cdots \Phi_{i_y} I(p_1) \vee \Phi_{j_1} \cdots \Phi_{j_x} I(p_1)]$, *where* $y \geq 1$, $x \geq 0$, $i_m \in \{0, 1\}$ *for* $m \in \{1, \cdots, y\}$, $i_y = 0$ *only if* $y = 1$, $j_m \in \{0, 1\}$ *for* $m \in \{1, \cdots, x - 1\}$, *and* $j_x = 1$.

PROOF. Our proof is by induction on m, the number of lines in the proof of a theorem B of D. Let $B_1, B_2, \cdots, B_m$ be a proof of B, where B_m is B and each B_j is either a substitution instance of an axiom or is obtained by modus ponens with minor premise B_q and major premise B_r, q, $r < m$.

Case 1. $m = 1$. But then B_m is either of Form 1, or of Form 3 with $x = 0$.

Case 2. $m > 1$. Assume the conclusion holds for all positive integers less than m.

Case 2a. B_m is a substitution instance of an axiom. Then the result follows from Case 1.

Case 2b. B_q is of Form 2 and B_r is of Form 1. Then B_r must be a substitution instance of an axiom in 9, 10, 11, 12, or 13 and B_m is of Form 2.

Case 2c. B_q is of Form 3 and B_r is of Form 1. Then B_r must be a substitution instance of an axiom in 2, 3, 4 or 5 and B_m is

(i) of Form 3 if B_r is an instance of 2 or 3;
(ii) of Form 4 if B_r is an instance of 4; or
(iii) of Form 5 if B_r is an instance of 5.

Case 2d. B_q is of Form 4 and B_r is of Form 1. Then B_r must be a substitution instance of an axiom in 6 or 7 and B_m is

(i) of Form 4 if B_r is an instance of 6; or

(ii) of Form 5 if B_r is an instance of 7.

Case 2e. B_q is of Form 5 and B_r is of Form 1. Then B_r must be a substitution instance of an axiom in 8 and B_m is of Form 2 where C is a terminal configuration of M.

The above 5 cases are exhaustive since a theorem of Form 1 may not interact with another of this form nor may a theorem of Form 2, 3, 4 or 5 interact with another of these kinds. This is seen to be true in light of Lemma 2.

LEMMA 4. *Every wff which can be abbreviated into a substitution instance of any of the forms of Lemma* 3 *is a theorem of* D.

PROOF. The lemma is established by considering each form separately.

Form 1. Trivially true since all substitution instances of axioms are theorems.

Form 2. This was established in Lemma 1.

Form 3. Axiom 1 is of Form 3 where $x = 0$. Form 3, for $x = 1$, is derived by one application of modus ponens with minor premise axiom 1 and major premise axiom 2. If all instances of Form 3 for $x < m$ are derivable then axiom set 3 allows us to derive all instances for $x = m$.

Form 4. All instances of Form 4 for $y = 1$ are derivable from one application of modus ponens with an instance of Form 3 as minor premise and an instance of axiom 4 as major premise. Successive applications of instances of axiom 6 may be used to derive instances of Form 4 where $y > 1$.

Form 5. All instances for $y = 1$ are derivable from one application of modus ponens with an instance of Form 3 as minor premise and an instance of axiom 5 as major premise. For $y > 1$ the desired result is achieved with an instance of Form 4 as minor premise and an instance of axiom 7 as major premise.

LEMMA 5. *The halting problem for* M *is of the same many-one degree as the decision problem for* D.

PROOF. Let C be an arbitrary configuration of M. Then C is mortal in M iff $\vdash_D C^*$. This follows from Lemmas 1 and 4. Hence the many-one degree of the halting problem for M is less than or equal to that of the decision problem for D.

Next let B be a wff of the diadic implicational calculus. By Lemmas 3 and 4, B is a theorem of D iff B is of one of Forms 1 through 5. One can easily check to see if B is of Form 1, 3, 4, or 5. If not, then we can determine if B is a theorem as follows. First determine if there exists a configuration C of M such that B is C^*. If not, B is not a theorem. If so, then B is a theorem iff C is mortal. (*Note.* If such a C exists it may be seen to be unique.) But then the decision problem for D is of a many-one degree less than or equal to the degree of the halting problem for M. Hence the lemma is proved.

THEOREM. (I) *The general halting problem for Turing machines over the alphabet* $\{0, 1\}$ *is many-one reducible to the general decision problem for diadic partial implicational propositional calculi* ($\mathscr{I}_2$).

(II) *Every nonrecursive r.e. many-one degree is represented by* $\mathscr{I}_2$.

(III) *Every nonrecursive r.e. one-one degree is not represented by* $\mathscr{I}_2$.

PROOF. (I) follows from Lemma 5 and the fact that M was chosen arbitrarily. (II) is a consequence of (I) and Overbeek's Turing machine results [4]. (III) was shown in [3] for all $\mathscr{I}_n$, $n \geq 1$, hence for $\mathscr{I}_2$.

Partial equivalence propositional calculi. *A partial equivalence propositional calculus* (PEPC) is a system similar to a PIPC except that its one connective is equivalence, denoted by the symbol $\equiv$, and in place of modus ponens it has the analogous rule of inference: if A and $A \equiv B$ then B. The results presented in this paper for diadic PIPC's may also be shown for diadic PEPC's. This may be done by parallelling the constructions and proofs presented in the previous section with the one change of replacing each occurrence of $\supset$ by $\equiv$ and interpreting $A \vee B$ as $(A \equiv B) \equiv B$.

Acknowledgements. The author wishes to express his sincere appreciation to Justin C. Walker of the National Bureau of Standards for his constructive criticisms of the work presented here and most importantly for his insight in finding flaws in a number of previous unsuccessful attacks on the problem.

REFERENCES

[1] M. D. GLADSTONE, *On the number of variables in the axioms*, ***Notre Dame Journal of Formal Logic,*** vol. 11 (1970), pp. 1–15.

[2] C. E. HUGHES, *Two variable implicational calculi*, this JOURNAL, vol. 39 (1974), p. 403. Abstract.

[3] C. E. HUGHES and W. E. SINGLETARY, *Triadic partial implicational propositional calculi*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 21 (1975), pp. 21–28.

[4] ROSS OVERBEEK, *The representation of many-one degrees by decision problems of Turing machines*, ***Proceedings of the London Mathematical Society*** (3), vol. 26 (1973), pp. 167–183.

[5] W. E. SINGLETARY, *Recursive unsolvability of a complex of problems proposed by Post*, ***Journal of the Mathematical Society of Japan,*** vol. 14 (1967), pp. 25–58.

[6] M. WAJSBERG, *Axiomatization of the three-valued propositional logic*, ***Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie Classe II,*** vol. 24 (1931).

[7] M. K. YNTEMA, *A detailed argument for the Post-Linial theorems*, ***Notre Dame Journal of Formal Logic,*** vol. 5 (1964), pp. 37–51.

UNIVERSITY OF TENNESSEE
KNOXVILLE, TENNESSEE 37916