438
Notre Dame Journal of Formal Logic
Volume XX, Number 2, April 1979
NDJFAM

THE DECIDABILITY OF ONE-VARIABLE PROPOSITIONAL CALCULI

M. D. GLADSTONE

"Propositional calculus" (or "**PC**") will be defined more precisely later on. For the moment it is enough to say that the meaning is the usual one, with the qualifications

(i) the set of axioms is finite (but need not be tautologous),
(ii) the rules of inference are substitution and modus ponens, i.e., A, $A \supset B \vdash B$, where "$\supset$" *may* stand for a combination of two or more logical connectives.

Let a **PC** be *monadic* (*diadic*) iff every axiom contains at most one (two) distinct variable(s). A general discussion of such systems will be found in [1]. In [3], Hughes constructs a diadic **PC** with a non-recursive class of theorems. As we shall see, this cannot be done for monadic **PC**s. In fact the object of the present paper is to describe a single algorithm for testing theoremhood in any given monadic **PC**. Some similarity will appear between monadic **PC**s and a certain type of combinatorial system studied by Post in [5].

We begin by investigating an offshoot of Post's system to be called an **L**-*system* (**L** for "left").

Definition: **L**-*System*. An **L**-system π consists of

(i) a countable non-empty alphabet $\mathfrak{A}_\pi$;
(ii) a finite set of ordered pairs, known as *rules*, of the form (Γ, B), where Γ is a finite set of words on $\mathfrak{A}_\pi$ and B is a word on $\mathfrak{A}_\pi$; the members of Γ are the *premises* of the rule, and B is the *conclusion.*

Λ is the empty word. $\emptyset$ is the empty set.

I assume the reader is familiar with the general notion of "proof tree" (if not, see [4] for instance). In the present case we describe a finite set of words of π in tree array as a "proof tree in π" iff, for every word Z having $n\,(\geq 1)$ words immediately above it, there exist a word X and rule

Received March 29, 1977

$(\{A_1, \ldots, A_n\}, B)$ of π such that $Z = Bx$ and the words immediately above Z are $A_1X, \ldots, A_nX$, in some order. Let us call a word of π an *axiom* iff it is of the form BX where $(\emptyset, B)$ is a rule of π. For each proof tree τ in π, we define $\mathsf{H}_\pi(\tau)$ to be the set of those uppermost words of τ which are *not* axioms.

We say a proof tree in π is *pure* iff $\mathsf{H}_\pi(\tau) = \emptyset$. We write

$$\Delta \vdash_\pi X$$

to denote the fact that Δ is a set of words of π and there exists a proof tree τ in π such that

(i) X is the lowest word of τ,
(ii) $\mathsf{H}_\pi(\tau) \subseteq \Delta$.

X is a *theorem* of π iff $\emptyset \vdash_\pi X$ (usually abbreviated to "$\vdash_\pi X$").

(If the definition of **L**-system is amended to allow individual axioms and forbid all rules except single-premise ones, then we have one of the combinatorial systems studied by Post in [5]. He states there and elsewhere that theoremhood in such a system is effectively decidable, but I have not seen an actual proof in the literature.)

Lemma 1 *There exists an algorithm for deciding for an arbitrary* **L**-*system* π *and arbitrary word* X *on* $\mathfrak{A}_\pi$ *whether* $\vdash_\pi X$.

Proof: Let $\mathfrak{B}_\pi$ be the set of just those symbols of $\mathfrak{A}_\pi$ which occur in the rules of π. Clearly $\mathfrak{B}_\pi$ is finite. For each word X on $\mathfrak{A}_\pi$ let X^π be the maximal left segment of X which is a word on $\mathfrak{B}_\pi$. A useful result is that

$$\vdash_\pi X \Leftrightarrow \vdash_\pi X^\pi. \tag{\#}$$

Proof of (#): $\Rightarrow$ can be carried out by straightforward induction upon the number of rule applications in the given derivation of X, bearing in mind that if X is an immediate consequence of $Y_1, \ldots, Y_n$ by a rule of π then X^π is an immediate consequence of $(Y_1)^\pi, \ldots, (Y_n)^\pi$ by the same rule.
$\Leftarrow$ follows from the observation that if we attach the same arbitrary word to the right-hand end of every line of a pure proof tree in π, the result is still a pure proof tree in π.

For each word X on $\mathfrak{A}_\pi$ let its *length*, written $|X|$, be the number of occurrences of symbols of $\mathfrak{A}_\pi$ in it. Let us call a rule (Γ, B) *positive* iff, for all $A \in \Gamma$, $|A| < |B|$. If all the rules of π are positive then the decision procedure is obvious; if a word of length n cannot be derived in $\leqslant n$ rule applications then it cannot be derived at all.

For the remainder of the lemma let π be an arbitrary **L**-system. It will be described how to construct from π an **L**-system π^* such that

(i) π^* has the same theorems as π,
(ii) all rules of π^* are positive.

Assuming that π has at least one rule (otherwise the whole thing is trivial) we define

$$\mathsf{k} = \text{maximum length of a conclusion of a rule of } \pi.$$

Let S_π be the set of all $\mathbf{L}$-systems Σ such that

(i) $\mathfrak{A}_\Sigma = \mathfrak{A}_\pi$,
(ii) every rule of Σ is positive, the premises and conclusion are words on $\mathfrak{B}_\pi$, and length of conclusion $\leqslant \mathsf{k}$.

Clearly S_π is finite. For each $\Sigma \in S_\pi$ let $\Phi(\Sigma)$ be Σ plus every rule (Δ, Z) which is not already a rule of Σ and satisfies the following conditions:

(i) Z and the words of Δ are all on $\mathfrak{B}_\pi$,
(ii) $\max\{|X|: X \in \Delta\} < |Z| \leqslant \mathsf{k}$,
(iii) there exist a rule (Γ, B) of π and word Y such that

(a) $Z = BY$,
(b) for each $A \in \Gamma$, $\Delta \vdash_{\Sigma} AY$.

Note that there are only finitely many ordered pairs (Δ, Z) satisfying (i) and (ii), and that the rules of Σ are positive; therefore the construction of $\Phi(\Sigma)$ from Σ is effective. Clearly $\Phi(\Sigma) \in S_\pi$.

Now let Σ be the $\mathbf{L}$-system with alphabet $\mathfrak{A}_\pi$ and no rules. Each $\mathbf{L}$-system in the sequence Σ, $\Phi(\Sigma)$, $\Phi^2(\Sigma)$, . . . is at least as strong as its predecessor. Therefore, since S_π is finite, there must be a member of the sequence which is equal to its successor and hence to all succeding members of the sequence. We define π^* to be this eventual fixed value of the sequence. Clearly π^* is effectively recognisable. Note that π^* has the property $\Phi(\pi^*) = \pi^*$.

The lemma will now follow if we show

$$\vdash_{\pi} X \Leftrightarrow \vdash_{\pi^*} X.$$

Since every rule of π^* is a derived rule of π, it follows at once that

$$\vdash_{\pi} X \Leftarrow \vdash_{\pi^*} X.$$

Now let π^0 have alphabet $\mathfrak{A}_\pi$ and as rules the union of those of π and those of π^*. Clearly it will be enough to show

$$\vdash_{\pi^0} X \Rightarrow \vdash_{\pi^*} X.$$

Now suppose $\vdash_{\pi^0} X$. We lose no generality in making the following 2 assumptions:

(i) X is the lowest line of a pure proof tree in π^0 in which the only application of a rule $\notin \pi^*$ is the final step;
(ii) X is a word on $\mathfrak{B}_\pi$.

See result (#) above.

Let (Γ, B) be the rule applied in the final step referred to in (i), above. The treatment splits into two cases.

Case 1: $|X| \leqslant \mathsf{k}$. There exists a word Y such that $X = BY$ and, for every $A \in \Gamma$, $\vdash_{\pi^*} AY$. Therefore $(\emptyset, X)$ is a rule of π^* and so $\vdash_{\pi^*} X$.

Case 2: $|X| = m > \mathsf{k}$. There exist words Y, Z such that

(i) $X = BYZ$,
(ii) $|BY| = \mathsf{k}$,
(iii) for every $A \in \Gamma$, $\vdash_{\overline{\pi^*}} AYZ$.

For each $A \in \Gamma$, AYZ must be the lowest word of some pure proof tree τ_A in π^*. Let τ'_A be obtained from τ_A by deleting every word having a word of length $< m$ below it. It is easily seen that each word in τ'_A is of the form WZ for some word W, and, in any rule application leading from WZ and other words on the same level to a word immediately below WZ, the premise appropriate to WZ is a left segment of W, i.e., the right segment Z is "passive". Thus if we delete the right segment Z from every word in τ'_A, the result is still a proof tree in π^*. Let

$$\Omega = \{W\colon\ WZ \text{ is an uppermost line of } \tau'_A \text{ for some } A \in \Gamma \,\&\, |W| < \mathsf{k}\}.$$

So any uppermost line of τ'_A not contributing to Ω, must be the conclusion of a no-premise rule of π^*.

Then (Ω, BY) is a rule of π^*; moreover, for each $W \in \Omega$, $\vdash_{\overline{\pi^*}} WZ$. Therefore $\vdash_{\overline{\pi^*}} BYZ$, and the lemma follows.

Definition: *Propositional Calculus*. I take the general notion of **PC** (propositional calculus) for granted (see [4] for instance). We restrict the general notion here by stipulating that **P** is a **PC** iff it consists of

(i) A finite set of logical connectives, none of which is an individual constant, and a countable infinity of propositional variables, from which *wffs* (well-formed formulae) are built up in the usual way; for future use we specify 2 particular variables of **P**, say $p_{\mathbf{P}}$, $q_{\mathbf{P}}$;
(ii) A specified finite set of wffs of **P**, to be known as *axioms*;
(iii) A specified wff of **P**, in which the variables occurring are precisely $p_{\mathbf{P}}$, $q_{\mathbf{P}}$; we shall write the result of substituting A, B for $p_{\mathbf{P}}$, $q_{\mathbf{P}}$, respectively, in the specified wff as "$A \supset_{\mathbf{P}} B$".

Note that condition (iii) ensures that **P** has at least one logical connective having $\geqslant 2$ argument-places. Let us say that a **PC** **P** is *monadic* iff the only variable appearing in the axioms is $p_{\mathbf{P}}$. In practice the suffix **P** will often be omitted from $p_{\mathbf{P}}$, $q_{\mathbf{P}}$, $\supset_{\mathbf{P}}$.

A finite array τ of wffs of a **PC** **P** in tree form is a *proof tree in* **P** iff for every non-uppermost wff x, *either*

(i) there is precisely one wff Y immediately above X, and X is a substitution instance of Y,

or

(ii) there are precisely 2 wffs immediately above X, and they are of the form Y, $Y \supset X$, for some Y.

We define $\mathsf{H}_{\mathbf{P}}(\tau)$ to be the set of those uppermost wffs of τ which are not substitution instances of axioms. A proof tree in **P** is *pure* iff

$\mathsf{H_P}(\tau) = \emptyset$. We write

$$\Delta \vdash_{\mathbf{P}} X$$

to denote the fact that Δ is a set of wffs of **P** and there exists a proof tree τ in **P** such that

(i) X is the lowest wff of τ,
(ii) $\mathsf{H_P}(\tau) \subseteq \Delta$.

X is a *theorem* of **P** iff $\emptyset \vdash_{\mathbf{P}} X$ (usually abbreviated to "$\vdash_{\mathbf{P}} X$").

Definitions: Prime wffs, p-wffs, rank, etc.

A wff is a *p-wff* iff p is the only variable occurring in it.

Suppose that A is a p-wff and B is a wff; then

$$A \cdot B, \text{ or just } AB,$$

denotes the result of substituting B for p in A. It is easily seen that if C is also a p-wff then

$$(AC)B = A(CB),$$

so henceforward we omit brackets when using this notation.

The rank of a wff A is the number of connective—occs (occurrences) in A plus the number of variable-occs in A.

For the remainder of the paper, "wff" means "wff of some monadic **PC**", i.e., individual constants are excluded. Hence, for any wff A, rank $A = 1$ iff A is a variable.

A wff A is said to be *prime* iff rank $A > 1$ and there exist *no* p-wff B and wff C, each of rank > 1, such that $A = BC$.

We write the fact that X is a subwff of the wff Y as $X \subseteq Y$.

There follow 2 technical lemmas on the foregoing concepts.

Lemma 2 *Let A, B be p-wffs and let C be a wff. Then $AC = BC \Rightarrow A = B$.*

Proof: Suppose rank $C > 1$, otherwise the result is trivial. The substitution $p \to C$ destroys all the original variable-occs (occurrences) in A. Now each C-occ in AC contains at least one variable-occ and hence replaces a p-occ in A. Let θ be the operation of simultaneously replacing all C-occs by p-occs (e.g., if $C = (p \supset p)$, then $\theta((q \supset q) \supset ((p \supset p) \supset (p \supset p))) = ((q \supset q) \supset (p \supset p))$.). Then

$$A = \theta(AC) = \theta(BC) = B.$$

Note that Lemma 2, like some later results, would not be valid if individual constants were allowed.

Lemma 3 *Let A be a wff of* rank > 1; *then there exists a unique sequence of prime wffs, say $A_1, \ldots, A_n$, such that $A_1, \ldots, A_{n-1}$ are p-wffs and*

$$A = A_1 \ldots A_n.$$

Proof: Obviously A has an expression as described but is it unique? Let $A_1 \ldots A_n$, $B_1 \ldots B_k$ be two such expressions for A. We take rank $A_n \leq$

rank B_k. Now every variable-occ in A lies within an A_n-occ and also within a B_k-occ. On the principle that if two wff-occs overlap then one contains the other, we conclude that $A_n \subseteq B_k$ and every variable-occ in B_k lies within an A_n-occ. Let θ be the operation of simultaneously replacing all A_n-occs by p-occs. Then $\theta(B_k)$ is a p-wff and

$$B_k = \theta(B_k) \cdot A_n.$$

Since B_k is prime it follows that $\theta(B_k) = p$ and so $B_k = A_n$. Hence, by Lemma 2,

$$A_1 \ldots A_{n-1} = B_1 \ldots B_{k-1}.$$

Making the harmless assumption that $n \leqslant k$, and repeating the above argument a further $n - 1$ times, we get

$$A_i = B_{i+k-n}, \text{ for } i = 1, \ldots, n,$$

and

$$p = B_1 \ldots B_{k-n}.$$

Therefore $k = n$ and the lemma follows.

Lemma 3 establishes the soundness of the definitions which follow.

Definitions: Prime factor, left segment, etc.

Let $A = A_1 \ldots A_n$, where $A_1, \ldots, A_n (n \geqslant 1)$ are prime wffs and $A_1, \ldots, A_{n-1}$ are p-wffs. Then $A_1, \ldots, A_n$ are said to be *prime factors* of A, and A_1 (A_n) is the *leftmost* (*rightmost*) *prime factor* of A.

For $1 \leqslant i \leqslant n$, we say that $A_1 \ldots A_i$ ($A_i \ldots A_n$) is a *left* (*right*) *segment* of A.

We now proceed to label certain entities arising from an analysis of "$\supset_\mathrm{P}$". Strictly speaking, each of these labels, k_0, $\square$, etc. should bear the suffix **P**, but we omit it.

Definitions: A_0, B_0, C_0, $\square$, k_0, m_0, n_0.

By Lemma 3, there exist a unique p-wff C_0 and a unique prime wff X, such that

$$p \supset q = C_0 X.$$

Let A_0 (B_0) be the maximal p-wff such that every p-occ (q-occ) in X lies within an occ of A_0 ($B_0 q$). Let Y be the result of simultaneously replacing in X all A_0-occs by p and all $B_0 q$-occs by q. Let us write the wff obtained by applying the substitution $(p,q) \to (W,Z)$ to Y as

$$W \square Z.$$

Then

$$p \supset q = C_0(A_0 \square B_0 q).$$

Let

$$\mathsf{k}_0 = \mathsf{rank}\,(p \,\Box\, q),$$
$$\mathsf{m}_0 = \mathsf{max}\,(\mathsf{rank}\ A_0,\ \mathsf{rank}\ B_0),$$
$$\mathsf{n}_0 = \mathsf{max}\{\mathsf{rank}\ Z\colon Z \text{ is an axiom of } \mathbf{P}\}.$$

Lemma 4 *Let A, B be wffs and let r be a variable not occurring in A or B. Then any one of the following* 3 *conditions is sufficient to ensure that $A \,\Box\, B$ is prime:*

(a) *A, B have distinct rightmost prime factors;*
(b) *A is a variable and $B \not\subseteq A \,\Box\, r$;*
(c) *B is a variable and $A \not\subseteq r \,\Box\, B$.*

Proof: There exist a p-wff C and prime wff D, such that

$$A \,\Box\, B = CD.$$

Case (a): We first show that $D \not\subseteq A$. Suppose $D \subseteq A$. Let θ be the operation of simultaneously replacing all D-occs by r. Then every occ in $\theta(A) \,\Box\, B$ of a variable other than r must lie within an occ of B, and also must continue to lie within a D-occ. There follows the contradictory result that D is the rightmost prime factor of B (B cannot be a proper right segment of D, because D is prime) and also of A. Therefore, $D \not\subseteq A$. Similarly, $D \not\subseteq B$.

Hence A, B are proper subwffs of D. (1)

Without loss of generality we may now take $\mathsf{rank}\ A \leqslant \mathsf{rank}\ B$. Can there be a B-occ in $A \,\Box\, r$? If so, every variable-occ lying within such a B-occ would also lie within an A-occ. Hence A would be a right segment of B, and it would follow that A, B have the same rightmost prime factor.

Therefore, there is no B-occ in $A \,\Box\, r$. (2)

Let $\lambda(\mu)$ be the operation of simultaneously replacing all B-occs (A-occs) by $r(p)$. Then, by result (2),

$$\mu\lambda(A \,\Box\, B) = \mu(A \,\Box\, r) = p \,\Box\, r.$$

And, by result (1),

$$\mu\lambda(A \,\Box\, B) = C \,.\, \mu\lambda(D).$$

Therefore, $p \,\Box\, r = C \cdot \mu\lambda(D)$. It then follows from the definition of "$\Box$" that $C = p$, and so

$$A \,\Box\, B = D \text{ (prime)}.$$

Case (b): Let λ be as in Case (a). Since $B \not\subseteq A \,\Box\, r$, it follows that

$$\lambda(A \,\Box\, B) = A \,\Box\, r.$$

Now, if $B \not\subseteq D$ then any D-occ in $A \,\Box\, B$ not lying within a B-occ is unaffected by λ. Therefore, every occ of the variable A in $A \,\Box\, r$ must lie within a D-occ. But this contradicts the maximality of A_0 in the definition of "$\Box$". Therefore, $B \subseteq D$. Hence, $\lambda(A \,\Box\, B) = C \cdot \lambda(D)$. Hence, $A \,\Box\, r =$

$C \cdot \lambda(D)$. It follows from the definition of "$\Box$" that $C = p$. Therefore $A \Box B = D$ (prime).

Case (c): Similar to Case (b).

Lemma 5 *Let A, B, D, E be p-wffs, with D prime, such that*

(i) $A \supset B = C_0 DE$,
(ii) *A, B have no common rightmost prime factor.*

Then: rank $E \leqslant k_0^2\, m_0$.

Proof: $A \supset B = C_0(A_0 A \Box B_0 B)$. Therefore, $DE = A_0 A \Box B_0 B$.

Case 1: A, B have distinct rightmost prime factors. It follows from Lemma 4 that $A_0 A \Box B_0 B$ is prime. Hence E is p and of rank 1.

Case 2: At least one of A, B, say A, is p. Let Z be the maximal right segment common to both A_0 and $B_0 B$. Then there exist p-wffs X, Y such that

$$A_0 = XZ \quad \text{and} \quad B_0 B = YZ.$$

Clearly.

$$\text{rank } Z \leqslant m_0. \tag{1}$$

Subcase 2.1: Neither of X, Y is p. Then X, Y have distinct rightmost prime factors and hence by Lemma 4 $X \Box Y$ is prime. Now,

$$DE = (X \Box Y)Z.$$

Therefore, $E = Z$ and the required result follows from result (1).

Subcase 2.2: At least one of X, Y, say X, is p, and $Y \not\subseteq p \Box q$. Again, by Lemma 4, $X \Box Y$ is prime, and the argument proceeds as in Subcase 2.1.

Subcase 2.3: At least one of X, Y, say X, is p, and $Y \subseteq p \Box q$. Then

$$\begin{aligned} \text{rank } E &\leqslant \text{rank } DE \\ &= \text{rank}(X \Box Y)Z \\ &\leqslant \text{rank}(X \Box Y) \times \text{rank } Z \\ &\leqslant \text{rank}(p \Box q) \times \text{rank } Y \times \text{rank } Z \\ &\leqslant (\text{rank}(p \Box q))^2 \times \text{rank } Z \\ &\leqslant k_0^2 \times m_0. \end{aligned}$$

This concludes the proof of Lemma 5.

The purpose of the next two lemmas is to "normalize" certain proof trees.

Lemma 6 *Let* **P** *be a monadic* **PC** *and let* $\vdash_{\mathbf{P}} X$. *Then there exists a p-wff W such that* $\vdash_{\mathbf{P}} W$ *and X is a substitution instance of W.*

Proof: Obviously the required property of X holds when X is an axiom and is preserved under substitution. It remains to show that it is preserved under modus ponens. Suppose that Y, $Y \supset X$ have the required property.

To avoid trivialities we may assume

(i) both p and q occur in X,
(ii) Y is not a variable (otherwise $\vdash_{\mathbf{P}} p$ and the lemma follows trivially).

Then there exist unique p-wffs X', Y', Z', and prime wffs X'', Y'', Z'', such that

$$X = X'X'', \; Y = Y'Y'', \; Y \supset X = Z'Z''.$$

Now, by hypothesis, there exists a p-wff Z^* such that $\vdash_{\mathbf{P}} Z^*$ and $Y \supset X$ is a substitution instance of Z^*. $Z^* \neq Y \supset X$ because both p and q occur in the latter. Therefore, Z^* is a left segment of Z', i.e., Z' is a substitution instance of Z^*. Therefore,

$$\vdash_{\mathbf{P}} Z'. \tag{1}$$

Again, by hypothesis, there exists a p-wff Y^* such that $\vdash_{\mathbf{P}} Y^*$ and Y is a substitution instance of Y^*. Studying the proof of result (1), we see that

$$\text{If both } p \text{ and } q \text{ occur in } Y, \text{ then } \vdash_{\mathbf{P}} Y'. \tag{2}$$

The treatment now splits into 2 cases.

Case 1: $X'' = Y''$. From result (2),

$$\vdash_{\mathbf{P}} Y'. \tag{3}$$

Now, $Z'Z'' = (Y' \supset X')X''$, hence $Z'' = X''$ and $Z' = Y' \supset X''$; so, from result (1),

$$\vdash_{\mathbf{P}} Y' \supset X'. \tag{4}$$

Applying modus ponens to results (3) and (4), we get $\vdash_{\mathbf{P}} X'$, and clearly X is a substitution instance of X'.

Case 2: $X'' \neq Y''$.

$$Y \supset X = C_0(A_0 Y \,\square\, B_0 X),$$

where $A_0 Y \,\square\, B_0 X$ is prime, by Lemma 4, and hence equal to Z''. Therefore, $Z' = C_0$. Hence, by result (1),

$$\vdash_{\mathbf{P}} C_0.$$

Applying the substitution $p \to A_0 Y^* \,\square\, B_0 X'$, we obtain

$$\vdash_{\mathbf{P}} Y^* \supset X'.$$

Hence, by modus ponens, $\vdash_{\mathbf{P}} X'$.

Lemma 7 *Let* **P** *be a monadic* **PC**, *let X be a p-wff of* **P**, *and let* $\vdash_{\mathbf{P}} X$. *Then there exists a pure proof tree in* **P** *such that*

(i) *X is the lowest wff;*
(ii) *for every non-uppermost wff W, there exists a Y such that the wffs immediately above W are Y, $Y \supset W$;*
(iii) *every wff is a p-wff.*

Proof: It is a well-known and easily-proved result that there exists a pure proof tree τ satisfying conditions (i) and (ii). If every variable in τ is replaced by p we have the required proof tree.

Definition: $\pi(\mathbf{P})$. Corresponding to each monadic **PC P** we define an **L**-system $\pi(\mathbf{P})$ as follows.

(i) *Alphabet.* This is $\{\overline{X}$: X is a prime p-wff of $\mathbf{P}\}$, each "$\overline{X}$" being regarded as an individual symbol. It will be convenient to extend the bar notation by defining

$$\overline{p} = \Lambda \text{ (the empty word)},$$

and $\overline{X} = \overline{A}_1 \ldots \overline{A}_n$, for each p-wff X whose factorization into primes is $A_1 \ldots A_n$ $(n \geqslant 1)$.

(ii) *Rules.* The rules of $\pi(\mathbf{P})$ are just those implied by the following two schemes.

(a) If A is an axiom of **P**, then

$$(\emptyset, \overline{A})$$

is a rule of $\pi(\mathbf{P})$.

(b) If A, B are p-wffs of **P** such that

(i) A, B have no common rightmost prime factor,
(ii) rank of leftmost prime factor of $A_0A \,\square\, B_0B \leqslant \mathrm{j}_0$, where

$$\mathrm{j}_0 = \max\{\mathrm{k}_0\mathrm{m}_0\mathrm{n}_0,\ \mathrm{k}_0^2\mathrm{m}_0\},$$

then

$$(\{\overline{A}, \overline{A \supset B}\}, \overline{B})$$

is a rule of $\pi(\mathbf{P})$. (Note that it follows from Lemma 5 that there can be only finitely many rules under scheme (b).)

Lemma 8 *For any p-wff X of a monadic* **PC P**,

$$\vdash_{\mathbf{P}} X \Leftrightarrow \vdash_{\pi(\mathbf{P})} \overline{X}.$$

Proof: $\Leftarrow$. Take any pure proof tree τ for $\overline{X}$ in $\pi(\mathbf{P})$ ("for $\overline{X}$" means "having lowest entry $\overline{X}$"). Replace every word $\overline{Y}$ by the wff Y, and the result is a pure proof tree for X in **P**, with axioms translating into substitution instances of axioms, and applications of Scheme (b) translating into applications of modus ponens.

$\Rightarrow$. Let us say that a proof tree in **P** is *normal* iff it is pure and satisfies conditions (ii) and (iii) of Lemma 7. Let us say that a normal proof tree τ in **P** is *good* iff, for every wff $A \supset B$ acting as 2nd premise in an application of modus ponens, the rank of the leftmost prime factor of $A_0A \,\square\, B_0B \leqslant \mathrm{j}_0$; otherwise we say τ is *bad*.

Some preliminary results will be proved about the concepts of "normal" and "good", after which the rest follows easily. Firstly we show:

The replacement of every wff Y by the word $\overline{Y}$ transforms every good normal proof tree in **P** *into a pure proof tree in* $\pi(\mathbf{P})$. (1)

The only part of this result that is at all doubtful is the effect of the transformation upon applications of modus ponens. Consider $A \supset B$, where the rank of the leftmost prime factor of $A_0 A \,\square\, B_0 B \leqslant \mathrm{j}_0$. Let Z be the maximal right segment common to A, B. Then there exist p-wffs A', B' such that $A = A'Z$ and $B = B'Z$. Clearly, $(\overline{A'}, \overline{A' \supset B'}, \overline{B'})$ is a rule of $\pi(\mathbf{P})$, and by this rule $\overline{B'} \cdot \overline{Z}$ is a consequence of $\overline{A'} \cdot \overline{Z}, \overline{A' \supset B'} \cdot \overline{Z}$, i.e., $\overline{B}$ is a consequence of $\overline{A}$, $\overline{A \supset B}$.

Another useful result is:

Let X, Y, Z be p-wffs, with Y prime and of rank $> \mathrm{j}_0$, *and let* τ *be a good normal proof tree in P for XYZ; then there exists a good normal proof tree in* **P** *for X.* (2)

Result (2) will be proved by induction upon the number of wffs in τ. Suppose that XYZ is a substitution instance of an axiom W. Then W is a left segment of XYZ, and, since Y is of too high a rank to be a prime factor of W, we deduce that W is a left segment of X. Therefore X is a substitution instance of the axiom W.

There remains the case that XYZ is a consequence by modus ponens of two wffs immediately above it, say A and $A \supset B$. Let C be the maximal right segment common to A, B. Then there exist p-wffs A', B', such that

$$A = A'C \quad \text{and} \quad B = B'C.$$

Now let F be the maximal right segment common to $A_0 A'$, $B_0 B'$. Then there exist p-wffs A'', B'' such that

$$A_0 A' = A'' F \quad \text{and} \quad B_0 B' = B'' F.$$

Thus, $A_0 A' \,\square\, B_0 B' = (A'' \,\square\, B'')F$. By Lemma 4, at least one of the following 3 cases holds:

(i) $A'' \,\square\, B''$ is prime, in which case it is the leftmost prime factor of $A_0 A \,\square\, B_0 B$, and hence (because τ is good normal) of rank $\leqslant \mathrm{j}_0$;
(ii) B'' is a variable;
(iii) $B'' \subseteq r \,\square\, s$, for appropriate variables r, s, and hence rank $B'' \leqslant \mathrm{k}_0$.

In all cases, rank $B'' \leqslant \mathrm{j}_0$. Also, by Lemma 5, rank $\mathrm{F} \leqslant \mathrm{k}_0^2 \mathrm{m}_0 \leqslant \mathrm{j}_0$. Therefore, $B''F$ has no prime factor of rank $> \mathrm{j}_0$. Hence, neither has B'. But $B = B'C = XYZ$. So YZ must be a right segment of C, i.e., there exists a p-wff C' such that

$$C = C'YZ.$$

Noting that $A \supset B = (A'C' \supset B'C')YZ$, it follows from the induction hypothesis that there exist good normal proof trees in **P** for

$$A'C' \quad \text{and} \quad A'C' \supset B'C'.$$

Combining these two proofs trees via an application of modus ponens, we obtain a good normal proof tree for $B'C' = X$.

The last of the preliminary results to be proved is:

If there exists a bad normal proof tree in **P**, *then there exists a good normal proof tree for p in* **P**. (3)

Let τ be a bad normal proof tree in **P** having the fewest possible wffs. Then the two lowest lines of τ are of the form

$$\frac{A \qquad A \supset B}{B},$$

where the leftmost prime factor of $A_0 A \,\square\, B_0 B$ is of rank $> \mathrm{j}_0$, and the subtree subtending $A \supset B$ is good normal. By result (2), there exists a good normal proof tree, say τ', for C_0. Let E be an axiom of **P** (one exists, otherwise there would be no normal proof trees). Apply the substitution

$$p \to A_0 E \,\square\, B_0$$

to every wff of τ'. The result, say τ'', is a good normal proof tree for $E \supset p$. Make the obvious application of modus ponens and we have a normal proof tree for p which is good because

$$\mathrm{rank}\ A_0 E \,\square\, B_0 p \leqslant \mathrm{rank}\ E \times \mathrm{m}_0 \times \mathrm{k}_0 \leqslant \mathrm{j}_0.$$

The rest of the proof of the lemma splits into two cases.

Case 1: $\vdash_{\mathbf{P}} p$. Then for every p-wff X of **P**, $\vdash_{\mathbf{P}} X$. Clearly, there will exist bad normal proof trees in **P**. Therefore, by result (3), there exists a good normal proof tree for p in **P**. Therefore, by result (1), there exists a pure proof tree, say τ, for $\wedge$ in $\pi(\mathbf{P})$. Take any p-wff X of **P**. Attach $\overline{X}$ to the right-hand side of every word in τ. The result is a pure proof tree for $\overline{X}$ in $\pi(\mathbf{P})$. Therefore, for every p-wff X of **P**, $\vdash_{\overline{\pi(\mathbf{P})}} \overline{X}$.

Case 2: Not - $\vdash_{\mathbf{P}} p$. Suppose $\vdash_{\mathbf{P}} X$, where X is a p-wff. Then X has a normal proof tree in **P** (Lemma 8) and by result (3) this proof tree must be good. Therefore, by result (1), $\vdash_{\overline{\pi(\mathbf{P})}} \overline{X}$.

Theorem *There exists an algorithm for deciding for an arbitrary monadic propositional calculus* **P**, *and arbitrary wff X of* **P**, *whether* $\vdash_{\mathbf{P}} X$.

Proof: Let X be a given wff of a given monadic **PC P**. Let S_X be the set of p-wffs of which X is a substitution instance. Clearly S_X is finite and effectively constructible. By Lemma 6, $\vdash_{\mathbf{P}} X \Longleftrightarrow$ there exists some $Y \in S_X$ such that $\vdash_{\mathbf{P}} Y$. Lemmas 1 and 8 furnish us with an obvious algorithm for determining the truth of the right-hand condition.

It will be noticed that our algorithm extends trivially to answer such problems as whether a given **PC** is consistent, and whether two given monadic **PC**s have the same theorems.

The algorithm was obtained *despite* the "diadic" nature of the modus ponens rule. Reviewing other possible "polyadic" rules, I imagine that some (e.g., $A \supset B, B \supset C \vdash A \supset C$?) would preserve decidability, whereas others (e.g., $\Psi(A,B) \vdash X(A,B)$?) might not, but the boundary does not seem clear.

I presume that the theorem still holds if individual constants are allowed, but I do not have a proof of this.

Finally, I remark that I do not know whether every monadic **PC** has the finite model property (defined for instance in [2]).

REFERENCES

[1] Gladstone, M. D., "On the number of variables in the axioms," *Notre Dame Journal of Formal Logic*, vol. XI (1970), pp. 1-15.

[2] Harrop, R., "Finite models and decision procedures for propositional calculi," *Proceedings of the Cambridge Philosophical Society*, vol. 54, Part I (1958), pp. 1-13.

[3] Hughes, C. E., "Two variable implicational calculi of prescribed many-one degrees of unsolvability," *The Journal of Symbolic Logic*, vol. 41 (1976), pp. 39-44.

[4] Mendelson, E., *Introduction to Mathematical Logic*, Van Nostrand (1964).

[5] Post, E. L., "Formal reductions of the general combinatorial decision problem," *American Journal of Mathematics*, vol. 65 (1943), pp. 197-215.

University of Bristol
Bristol, England