

SOME WAYS OF CONSTRUCTING A PROPOSITIONAL CALCULUS OF ANY REQUIRED DEGREE OF UNSOLVABILITY⁽¹⁾

BY
M. D. GLADSTONE

1. Introduction. Let us begin by discussing exactly what is meant in this paper by *propositional calculus*. A propositional calculus P is completely specified by the following three things:

(1) *A set S of connectives.* Attached to every connective is a unique, classical, two-valued truth-function. It is emphasized that we regard a *connective*, in itself, as being merely a symbol; so different connectives may represent the same truth-function. By "a wff of P " we mean a wff built up in the usual way from the connectives of S and propositional variables. The only restriction we make on S is that its connectives must be adequate to express implication.

(2) *An expression of implication.* This means that we specify some wff of P , having x, y as sole variables, whose truth-table interpretation is "x implies y." Say the specified wff is $(x \supset y)$.

(3) *A set of tautologous wff of P , to be known as "axioms."* The theorems of P are those of its wff which can be derived from the axioms, using as rules of inference,

(i) substitution,

(ii) $a, (a \supset b) \vdash b$ (this is the " \supset " specified in property (2) above).

We shall show how to construct a propositional calculus whose decision problem is of any required recursively enumerable degree of unsolvability, in either of the following two sets of circumstances:

(A) The connectives and the specified expression of implication are given, but free choice of axioms is allowed.

(B) A propositional calculus is given, but we are allowed to add new axioms and to make use, in those axioms, of a given new connective (it does not matter which, as long as it has at least one argument-place).

We shall prove just two theorems, corresponding respectively to the above two results.

Received by the editors September 3, 1963.

⁽¹⁾ I am very much indebted to J. C. Shepherdson for supervising the work, and to the Department of Scientific and Industrial Research for a grant.

Our method, broadly speaking, is to take a decision problem of the required degree of unsolvability associated with a semi-Thue system, and translate from semi-Thue system to propositional calculus. An outline of the strategy of the proof is given in §4.

2. **Relevant literature.** Numbers in square brackets, as [1], [2], refer to works by other writers, listed at the end of the paper.

The discussion is roughly chronological.

In an abstract, [7], published in 1949, Lial and Post announce the existence of an unsolvable propositional calculus with connectives \neg (negation) and \vee (disjunction). They give a sketch proof but as far as I know the details have never been filled in.

In [4], published in 1958, Davis gives a proof of the existence of an unsolvable propositional calculus with connectives \neg (negation) and \supset (implication). Although more detailed than that of [7], his proof still does not seem quite adequate. I will enlarge on this statement, in order to underline the point of some of the detail in my own proof; I assume the reader has [4] at his side, open at pp. 139–140.

The important objection is to Lemma 4 (Lemma 1 appears to be false, but if “[$X \supset Y$]” is replaced everywhere by “[$X \vdash Y$]” we get a result which seems to be true and is strong enough for the needs of the theorem). If Lemma 4 is studied carefully it will be seen that what is actually proved is simply not as strong as what the lemma states. Furthermore, to extend the theorem by replacing “unsolvability” by “any required degree of unsolvability,” would probably involve getting a clear picture of the whole class of theorems of the propositional calculus constructed in [4]. This might be difficult. A little experimenting suggests that the class of theorems ranges over a variety of forms not easy to describe concisely. So, rather than try to improve the proof of Lemma 4, it seems better to construct a new propositional calculus with a more easily described class of theorems. This is in fact what we shall do, although the actual treatment borrows a great deal from Davis.

I understand that a satisfactory proof of the unsolvability of the propositional calculus of [4] (or one very like it) has now been provided by Singletary, although I have not seen this proof myself.

In [5], also published in 1958, Harrop discusses a type of system which he calls a *propositional calculus*, but his definition is much broader than the one I have given. His connectives are not tied to a truth-function interpretation, and he creates arbitrary rules of inference. He proves the existence of an unsolvable system of this broad type, but of course this does not necessarily imply the existence of one of the more restricted kind discussed here.

However, I am told that in 1963 Harrop submitted to the Journal of the London Mathematical Society a paper in which he shows how to construct a propositional calculus of the kind discussed here, which is unsolvable.

To conclude the account of authors in this field, I learn, again by hearsay, that Mrs. Ihrig is currently writing up a method of constructing a propositional calculus of an arbitrary degree of unsolvability.

With this exception no one, as far as I know, has strengthened the “unsolvability” result into an “arbitrary degree of unsolvability” one.

3. Notation. The small italic letters a, b, \dots, h , always denote wff; i, j, \dots, u , always denote non-negative integers; and v, w, \dots, z , always denote propositional variables.

Italic capitals are available for miscellaneous usage.

All things appertaining to a semi-Thue system, whether letters of its alphabet, words, or the system itself, will be denoted by Greek capitals, Φ, Ψ, \dots ; and Greek capitals will be used for no other purpose.

Small Greek letters $\alpha, \beta, \dots, \omega$, always denote connectives, or combinations of connectives representing truth-functions (an example of the latter is “ \supset ,” see §1.

The cumbersome phrase, *combination of connectives representing a truth-function*, is henceforward to be shortened to *complex connective*, and I shall now try to explain exactly what is meant by this. For convenience sake, now and later, let x_1, x_2, \dots , be a denumerable infinity of distinct propositional variable. Like a simple connective, each complex connective is assigned some non-negative integer n , and is then said to have “ n argument-places.” To each n -place complex connective ϕ is assigned a wff a whose distinct variables are x_1, \dots, x_n . Then, for any wff a_1, \dots, a_n ,

$$\phi(a_1, \dots, a_n)$$

denotes the wff obtained from a by substituting a_1, \dots, a_n for x_1, \dots, x_n , respectively. So complex connectives are functions defined from and onto the class of wff.

Besides standard abbreviations, such as “wff,” we introduce some of our own, notably

“arg” for “argument,”

“cc” for “complex connective,”

“vbl” for “propositional variable.”

The *equality*, $a = b$ signifies that the wff a, b are identical, not merely that they always have the same truth-values.

Each of the following definitions holds throughout the paper:

(1) Γ is a semi-Thue system with alphabet $\Sigma_1, \dots, \Sigma_s$, axiom Δ_0 , and productions,

$$\Phi\Delta_i\Psi \text{ generates } \Phi\Delta_i'\Psi,$$

where $i = 1, \dots, t$.

(2) α is a certain connective; all we assume about it is that it has at least one arg-place.

(3) \supset is a two-place cc representing implication; and $(x_1 \supset x_2)$ does not contain α .

(4) \vee is a two-place cc defined by

$$(x_1 \vee x_2) = ((x_1 \supset x_2) \supset x_2).$$

(5) β_n is a one-place cc defined inductively for $n \geq 1$ by

$$\beta_1(x_1) = (x_1 \supset x_1),$$

$$\beta_{n+1}(x_1) = (x_1 \supset \beta_n(x_1)).$$

(6) γ stands ambiguously for either of two cc's, known respectively as the 1st γ -cc, and the 2nd γ -cc. Definitions follow.

1st γ -cc. $\gamma(x_1) = \beta_3(\beta_2(x_1)).$

2nd γ -cc. $\gamma(x_1) = \alpha((x_1 \supset x_1), \dots, (x_1 \supset x_1)).$

(7) $\bar{\Phi}(a)$ denotes a wff, defined for each word Φ of Γ , and each wff a , as follows;

$$\bar{\Sigma}_i(a) = \beta_i(a),$$

$$\bar{\Psi}\bar{\Sigma}_i(a) = (\bar{\Psi}(a) \vee \bar{\Sigma}_i(a)),$$

where $i = 1, \dots, s$, and Ψ is a nonvoid word of Γ .

We shall be interested in the five propositional calculi defined below. In each the expression of implication specified for the modus ponens rule is the cc \supset .

THE PROPOSITIONAL CALCULI P, Q, R, S, T .

P : All we assume about the connectives of P is that they do not contain α . The axioms are arbitrary.

Q : Q has the same connectives as P . The axioms of Q are chosen so that all tautologous wff of Q are theorems. (The existence of a propositional calculus Q , complete in this way, is established by Henkin in [6].)

R : The axioms are:

$$(R1) \ \gamma((x_1 \vee x_2) \vee x_3) \supset \gamma(x_1 \vee (x_2 \vee x_3)).$$

$$(R2) \ \gamma(x_1 \vee (x_2 \vee x_3)) \supset \gamma((x_1 \vee x_2) \vee x_3).$$

$$(R3) \ \gamma((x_1 \vee (x_2 \vee x_3)) \vee x_4) \supset \gamma(((x_1 \vee x_2) \vee x_3) \vee x_4).$$

$$(R4) \ \gamma(((x_1 \vee x_2) \vee x_3) \vee x_4) \supset \gamma((x_1 \vee (x_2 \vee x_3)) \vee x_4).$$

S : The axioms are:

$$(Si.1) \ \gamma(\bar{\Delta}_i(x_1)) \supset \gamma(\bar{\Delta}'_i(x_1)).$$

$$(Si.2) \ \gamma(x_1 \vee \bar{\Delta}_i(x_2)) \supset \gamma(x_1 \vee \bar{\Delta}'_i(x_2)).$$

$$(Si.3) \ \gamma(\bar{\Delta}_i(x_1) \vee x_2) \supset \gamma(\bar{\Delta}'_i(x_1) \vee x_2).$$

$$(Si.4) \ \gamma((x_1 \vee \bar{\Delta}_i(x_2)) \vee x_3) \supset \gamma((x_1 \vee \bar{\Delta}'_i(x_2)) \vee x_3).$$

for $i = 1, \dots, t$.

T : There is a single axiom

$$(T1) \ \gamma(\bar{\Delta}_0(x_1)).$$

The connectives of R, S, T consist of just those connectives which are contained in $(\gamma(x_1) \supset x_1)$.

Let us verify that each axiom is indeed a tautology. Anything of the form $(\gamma(a) \supset \gamma(b))$ is a tautology, whichever definition of γ is used. This takes care of all the axioms except (T1). Now, anything of the form $\gamma(a)$ is a tautology under Definition 1, but not necessarily under Definition 2. However, whenever T is mentioned we shall be using definition 1, so this does not matter.

In order to combine P, Q, R, S, T in various ways, we shall want to define the sum $(A + B)$ of two propositional calculi A, B , both having \supset as the specified expression of implication. It is simply the propositional calculus obtained by adding the connectives, and axioms, of A, B , together, and keeping \supset as the specified expression of implication.

For the semi-Thue system Γ , and any propositional calculus A , " $\vdash_{\Gamma} \Phi$ " and " $\vdash_A a$ " bear their usual meanings. " $\Phi \vdash_{\Gamma} \Psi$ " means that the word Ψ is a consequence of the word Φ through a succession of the productions of Γ , a fact which is quite independent of the axiom Δ_0 . " $a \vdash_A b$ " means that, using modus ponens as the sole rule of inference, b can be inferred from the class of wff consisting of a and the closure under substitution of the axioms of A .

We shall be interested in the inter-reducibility relations holding among the following five decision problems.

THE DECISION PROBLEMS $D1-D5$. The problems are to give general procedures for deciding

- (D1) for any given word Φ of Γ , whether $\vdash_{\Gamma} \Phi$,
- (D2) for any given words Φ, Ψ of Γ , whether $\Phi \vdash_{\Gamma} \Psi$,
- (D3) for any given wff a, b of $(R + S)$, whether $\gamma(a) \vdash_{(R+S)} \gamma(b)$,
- (D4) for any given wff a of $(R + S + T)$, whether $\vdash_{(R+S+T)} a$,
- (D5) for any given wff a of $(P + Q + R + S)$, whether $\vdash_{(P+Q+R+S)} a$.

4. Programme. There are published results (sources to be quoted later) to the effect that, as Γ ranges over all semi-Thue systems, so $D1$ and $D2$ range over all recursively enumerable degrees of unsolvability. In the light of these results our two theorems (see §1) will follow if we can reduce $D1, D4$ to each other, and $D2, D5$ to each other.

We relate our propositional calculi to the semi-Thue system Γ by giving a procedure which assigns to each wff a a unique integer $m \geq 0$, and unique m -tuple Φ_1, \dots, Φ_m of words on Γ . Suppose a is assigned words Φ_1, \dots, Φ_m as just described, and b is assigned words Ψ_1, \dots, Ψ_n .

The main result of §5 is that $\gamma(a) \vdash_{(R+S)} \gamma(b)$ iff

- (1) $m = n$, and $\Phi_i \vdash_{\Gamma} \Psi_i$ for $i = 1, \dots, m$, and
- (2) certain absolutely decidable conditions are satisfied. Using this result, we reduce $D2, D3$ to each other.

In §6, by taking the main result of §5 when $\gamma(a)$ is held fixed as (T1) (or anything obtainable from (T1) by substitution) we eventually reduce D1, D4 to each other, and so obtain Theorem 1.

In §7, we reduce D5, D3 to each other. It then follows from §5 that D2, D5, reduce to each other and so theorem 2 is obtained.

5. Inter-reducibility of D2, D3. The results of this section will hold for either definition of γ .

The first lemma says in effect that R successfully axiomatizes the associative law with respect to the two-place cc \vee . This result is announced by Jean Porte in [8]. As far as I know, no proof has yet been published, so I give one here.

LEMMA 1. Let a_1, \dots, a_n be wff, where $n \geq 1$; and let the expression,

$$a_1 \vee \dots \vee a_n$$

be capable of denoting each of the wff b, c , upon appropriate insertion of brackets. Then

$$\gamma(b) \vdash_R \gamma(c).$$

Proof. We shall say that b is *standard* iff, for some i , where $0 \leq i \leq n$, b is obtained by inserting the brackets in such a way that

(1) in the sub-expression $a_1 \vee \dots \vee a_i$, association is always to the left,

(2) in the sub-expression $a_{i+1} \vee \dots \vee a_n$, association is always to the right.

“Standard” is similarly defined for c . To clarify this, an example of a standard wff with $n = 9$ and $i = 4$, is

$$((((a_1 \vee a_2) \vee a_3) \vee a_4) \vee (a_5 \vee (a_6 \vee (a_7 \vee (a_8 \vee a_9))))).$$

Using (R1), (R2) and a succession of applications of modus ponens, we can easily show that

If b and c are both standard wff, then

$$(1) \quad \gamma(b) \vdash_R \gamma(c).$$

We now tackle the general case, where b, c are not necessarily standard, by induction upon n . For $n = 1, 2, 3$, the result is trivial. We assume the result for $3 \leq n \leq k$ and consider the case $n = k + 1$.

The first step is to prove the existence of a standard wff b'' , such that $\gamma(b) \vdash_R \gamma(b'')$. Let us suppose that b itself is not standard (otherwise the step is trivial). Then for some i , where $1 < i < k$, the expression

$$a_1 \vee \dots \vee a_{i-1} (a_i \vee a_{i+1}) \vee a_{i+2} \dots \vee a_{k+1}$$

can be made to denote b by appropriate insertion of brackets. By induction hypothesis (case $n = k$), if b' is any other wff obtained from the last expression

by the insertion of brackets, then $\gamma(b) \vdash_R \gamma(b')$. Let b be obtained by inserting the brackets in such a way that

(1) in the sub-expression $a_1 \vee \cdots \vee (a_i \vee a_{i+1})$ association is always to the left

(2) in the sub-expression $a_{i+2} \vee \cdots \vee a_{k+1}$ association is always to the right.

Then, as stated,

$$(2) \quad \gamma(b) \vdash_R (b').$$

Applying the substitution that sends $((x_1 \vee (x_2 \vee x_3)) \vee x_4)$ into b , we send (R3) into something of the form $(\gamma(b') \supset \gamma(b''))$, where b'' is standard. Combining this with result (2), we get

$$(3) \quad \gamma(b) \vdash_R \gamma(b'').$$

In a rather similar way, but this time using (R4) instead of (R3), we can find a standard wff c'' , such that,

$$(4) \quad \gamma(c'') \vdash_R \gamma(c).$$

Now, result (1) tells us that $\gamma(b'') \vdash_R \gamma(c'')$. Combining this with results (3) and (4), we conclude that $\gamma(b) \vdash_R \gamma(c)$.

The next three lemmas are devoted to showing that any given wff can be written in at most one way in the form $\Phi(a)$.

LEMMA 2. *For any wff $a, b, m \neq n$ implies $\beta_m(a) \neq \beta_n(b)$.*

Proof. Reductio ad absurdum. Suppose $\beta_m(a) = \beta_n(b)$. Then, equating the first args of the outermost \supset on each side, $a = b$. (By "the 1st and 2nd args of the outermost \supset " of a wff $(c \supset d)$, we mean c, d , respectively.) But this implies $\beta_m(a) = \beta_n(a)$, which is obviously false for $m \neq n$.

LEMMA 3. *For any wff a, b, c , and positive integer n , $\beta_n(a) \neq (b \vee c)$.*

Proof. In $\beta_n(a)$ the first arg of the outermost \supset is properly contained within the second arg, or else (in the case $n = 1$) equal to it. In $(b \vee c)$ the first arg of the outermost \supset properly contains the second arg. These two properties are clearly incompatible.

LEMMA 4. *For each wff a , there is at most one word-wff pair Φ, b , such that $a = \Phi(b)$.*

Proof. For each wff a there will be a unique expression,

$$a_1 \vee \cdots \vee a_m,$$

where m is a positive integer, and a_1, \dots, a_m are wff with the properties,

(1) by the insertion of brackets the above expression can be made to denote a ,

(2) none of a_1, \dots, a_m is of the form $(c \vee d)$.

Suppose at least one word-wff pair Φ, b , as described in the lemma exists. Bearing in mind Lemma 3, there must exist letters $\Theta_1, \dots, \Theta_m$ of Γ , such that Φ is the word $\Theta_1 \dots \Theta_m$, and

$$a_i = \overline{\Theta}_i(b) \text{ for } i = 1, \dots, m.$$

But Lemma 2 tells us that, for any a_i , there is at most one letter Θ_i such that, for some $b, a_i = \overline{\Theta}_i(b)$; and once Θ_i is fixed, b is of course determined. Hence Φ and b are unique (if they exist at all).

Later on we shall establish a correspondence between words of Γ and certain wff. This will help link the decision problems associated with Γ with those associated with P, Q, R, S, T . From each wff a we shall now show how to construct an expression $E(a)$, so arranged that the words (if any) corresponding to a are readily extracted.

THE EXPRESSION $E(a)$. The first step is to construct from a the expression,

$$a_1 \vee \dots \vee a_m,$$

with properties (1) and (2) as described during the proof of Lemma 4. Next, list every sub-expression of the form,

$$a_p \vee a_{p+1} \vee \dots \vee a_{p+q}, \quad \text{where } 1 \leq p < p + q \leq m,$$

with the properties that, for some b ,

(1) each of a_p, \dots, a_{p+q} belongs to the set

$$\{\overline{\Sigma}_1(b), \dots, \overline{\Sigma}_s(b)\},$$

(2) neither of a_{p-1}, a_{p+q+1} (if these are defined) belongs to the set just mentioned.

It follows from the sort of argument used in Lemma 4, that no two of the above sub-expressions can overlap. We make each of these sub-expressions denote a wff by inserting brackets in it with association to the left. This will transform $a_1 \vee \dots \vee a_m$ into an expression,

$$b_1 \vee \dots \vee b_n, \quad \text{where } 1 \leq n \leq m,$$

and where b_1, \dots, b_n are wff; and it is this last expression which we write as $E(a)$.

We note that, for each b_i of $E(a)$, either (1) there exists a unique word-wff pair Φ, c such that $b_i = \overline{\Phi}(c)$, or (2) b_i is not of the form $(d \vee e)$. The words of Γ introduced under category (1) form a finite set associated with a .

Below we define the wff-relation \succ . It will be found that the statement " $a \succ b$ " asserts certain derivability-in- Γ relations between the words associated with a and those associated with b .

THE RELATION \succ . Let a, b be any wff. We write " $a \succ b$ " iff all the following conditions hold:

(1) For some m ,

$$E(a) = a_1 \vee \cdots \vee a_m,$$

$$E(b) = b_1 \vee \cdots \vee b_m,$$

where a_1, \dots, b_m are wff.

(2) For each i , where $1 \leq i \leq m$, either (i) $a_i = b_i$, or (ii) there exist a wff c , and words Φ, Ψ of Γ , such that $a_i = \overline{\Phi}(c)$ and $b_i = \overline{\Psi}(c)$.

(3) In each case of (2) (ii), $\Phi \vdash_{\Gamma} \Psi$.

It would not be difficult in principle to find an effective procedure for deciding whether a, b satisfy conditions (1) and (2), and, if so, constructing the words Φ, Ψ in all cases of (2) (ii). We would then merely need to test condition (3) in a finite number of cases, a task which is reduced to (D2) as it stands. Having done all this we could answer the question, Does $a \succ b$? Hence we have

LEMMA 5. *The problem of deciding, for any given wff a, b , whether $a \succ b$, reduces to (D2).*

In the course of the next seven lemmas we gradually reduce (D3) to the problem of deciding whether $a \succ b$, by showing that $\gamma(a) \vdash_{(R+S)} \gamma(b)$ iff $a \succ b$.

LEMMA 6. *If $a \succ b$, then $\gamma(a) \vdash_{(R+S)} \gamma(b)$.*

Proof. We define a wff-relation \succ_{-1} , solely for the purposes of the present lemma. Its definition can be obtained from that of \succ by adding the following restriction: There is at most one wff-pair $\{a_1, b_1\}$ which does not come under category (2)(i), and if Φ, Ψ are the words appropriate to such a pair, then Ψ is an immediate consequence of Φ by one of the productions of Γ .

We first prove the lemma with \succ replaced by \succ_{-1} . Our notation is the same as that used during the definition of \succ .

We may take it that, for some integers i, j , wff c , and words Θ, K of Γ ,

$$a_i = \overline{\Theta \Delta_j K}(c) \quad \text{and} \quad b_i = \overline{\Theta \Delta'_j K}(c).$$

We tackle the most complicated case, when neither of Θ, K is void, and $1 < i < m$. Let d, e be wff obtained by inserting brackets in, respectively, $a_1 \vee \cdots \vee a_{i-1}$ and $a_{i+1} \vee \cdots \vee a_m$ (it does not matter how the brackets are inserted).

The first and third of the following results arise from Lemma 1, and the second from (Sj.4):

$$(1) \quad \gamma(a) \vdash_{(R+S)} \gamma(((d \vee \overline{\Theta}(c)) \vee \overline{\Delta_j}(c)) \vee (K(c) \vee e)),$$

$$(2) \quad \gamma(((d \vee \overline{\Theta}(c)) \vee \overline{\Delta_j}(c)) \vee (K(c) \vee e)) \\ \vdash_{(R+S)} \gamma(((d \vee \overline{\Theta}(c)) \vee \overline{\Delta_j}(c)) \vee (K'(c) \vee e)),$$

$$(3) \quad \gamma(((d \vee \overline{\Theta}(c)) \vee \overline{\Delta'_j}(c)) \vee (K(c) \vee e)) \vdash_{(R+S)} \gamma(b).$$

Combining (1), (2) and (3), we get

$$(4) \quad \gamma(a) \vdash_{(R+S)} \gamma(b).$$

When i is 1 or m , or when one of Θ, K is void, the proof runs along similar lines, except that it may be necessary to use one of (Sj.1), (Sj.2), (Sj.3), instead of (Sj.4).

Now let us return to the general case when we are given simply $a \succ b$. It is easily seen that, for some n , wff c_1, \dots, c_n can be constructed, such that,

$$(5) \quad \begin{array}{l} a \succ \neg c_1, \\ c_1 \succ \neg c_2, \\ \dots, \\ c_n \succ \neg b. \end{array}$$

It follows from result (4) that we can replace $\succ \neg$ by $\vdash_{(R+S)}$ throughout (5). Hence we have

$$\gamma(a) \vdash_{(R+S)} \gamma(b).$$

To obtain the converse of Lemma 6, we want to be able to draw, for any given wff $\gamma(a)$, a picture of the class of wff b which satisfy $\gamma(a) \vdash_{(R+S)} b$. Fortunately in this class of wff the variety of form is very restricted, in consequence of the properties of γ proved in the following two lemmas.

LEMMA 7. For any wff a, b, c we have $\gamma(a) \neq (\gamma(b) \supset \gamma(c))$.

Proof for 1st γ -cc. The first args of the outermost \supset 's of $\gamma(a), (\gamma(b) \supset \gamma(c))$ are, respectively, $\beta_2(a), \beta_3(\beta_2(b))$. But, by Lemma 2, $\beta_2(a) \neq \beta_3(\beta_2(b))$.

Proof for 2nd γ -cc. Since \supset does not contain α , the two wff have different outermost connectives.

LEMMA 8. Let *modus ponens* be applied to two members of the class of those wff which are of either of the two forms,

- (1) $\gamma(a)$,
- (2) $(\gamma(b) \supset \gamma(c))$.

Then the first and second premises must be of forms (1) and (2), respectively.

Proof for 1st γ -cc. The first arg of the outermost \supset of $\gamma(a)$ is $\beta_2(a)$. Using Lemma 2, we can show that this is of neither of forms (1), (2). Hence $\gamma(a)$ cannot be the second premise. This leaves only the possibility described in the lemma.

Proof for 2nd γ -cc. Since $\gamma(a)$ is not of the form $(d \supset e)$, it cannot be the second premise. This leaves only the possibility described in the lemma.

I pause here to remark that, if we allowed ourselves to introduce new connectives at will, we could replace γ by a new one-place connective. Lemmas 7 and 8 would then follow trivially. Similarly we could bring in a new two-place connective for \vee , and individual constants for $\bar{\Sigma}_1(a), \dots, \bar{\Sigma}_s(a)$. This would simplify the notation and render Lemmas 2-4 trivial.

The next lemma indicates how the properties of γ described in Lemmas 7 and 8, restrict the class of wff derivable from $\gamma(a)$ in $(R + S)$.

LEMMA 9. *If $\gamma(a) \vdash_{(R+S)} \gamma(b)$ (where $a \neq b$), then, for some m , there exist wff c_1, \dots, c_m , such that,*

$$\begin{aligned} &(\gamma(a) \supset \gamma(c_1)), \\ &(\gamma(c_1) \supset \gamma(c_2)), \\ &\quad \dots \quad \dots \\ &(\gamma(c_m) \supset \gamma(b)), \end{aligned}$$

all proceed directly by substitution from axioms of $(R + S)$.

Proof. It follows from Lemmas 7 and 8 that, if $\gamma(a) \vdash_{(R+S)} d$, then exactly one of the following two cases must hold:

(1) d is of the form $\gamma(e)$,

(2) d is of the form $(\gamma(e) \supset \gamma(f))$ and proceeds directly by substitution from an axiom of $(R + S)$.

The desired result now follows by induction upon the length of the derivation of $\gamma(b)$ from $\gamma(a)$.

LEMMA 10. *If $(\gamma(a) \supset \gamma(b))$ proceeds directly by substitution from an axiom of $(R + S)$, then $a \succ b$.*

Proof. For axioms of R the result is trivial since then $E(a) = E(b)$.

To illustrate the method of proof for axioms of S we take the most complicated case, that of $(Sj.4)$, by way of example. Suppose that the substitution which sends this axiom into $(\gamma(a) \supset \gamma(b))$, sends x_2 into c . Then, for certain words (possibly void) Φ, Ψ of Γ , and expressions X, Y we have either

$$E(a) = X \vee \overline{\Phi \Delta_j \Psi}(c) \vee Y,$$

and

$$E(b) = X \vee \overline{\Phi \Delta_j \Psi}(e) \vee Y,$$

or else one of the three possibilities obtainable from the above by deleting one, or both, of " $X \vee$," " $\vee Y$."

Since $\Phi \Delta_j \Psi \vdash_{\Gamma} \Phi \Delta_j \Psi$, we have $a \succ b$.

LEMMA 11. *If $\gamma(a) \vdash_{(R+S)} \gamma(b)$, then $a \succ b$.*

Proof. Ignoring the trivial case $a = b$, we learn from Lemmas 9 and 10 that, for some m , there exist wff c_1, \dots, c_m , such that,

$$\begin{aligned} &a \succ c_1, \\ &c_1 \succ c_2, \\ &\quad \dots \quad , \\ &c_m \succ b. \end{aligned}$$

Since the relation \succ is transitive, (this follows from Lemma 4 and the transitivity of \vdash_r), we have $a \succ b$.

Combining Lemmas 6 and 11, we have

LEMMA 12. $\gamma(a) \vdash_{(R+S)} \gamma(b)$ iff $a \succ b$.

From the last lemma and Lemma 5, we get

LEMMA 13. (D3) reduces to (D2).

Conversely, we have

LEMMA 14. (D2) reduces to (D3).

Proof. $\Phi \vdash \Psi$ iff $\bar{\Phi}(x_1) \succ \bar{\Psi}(x_1)$ (from definition of \succ), i.e., iff $\gamma(\bar{\Phi}(x_1)) \vdash_{(R+S)} \gamma(\bar{\Psi}(x_1))$ (Lemma 12).

Lemmas 13 and 14 give us

LEMMA 15. (D2) and (D3) are of the same degree of unsolvability.

6. Inter-reducibility of (D1), (D4). In this section, Definition 1 of γ applies throughout. Hence (T1) is a tautology. The next three lemmas draw a picture of the class of theorems of $(R + S + T)$.

LEMMA 16. Every theorem of $(R + S + T)$ falls into exactly one of the following two classes:

- (1) wff of the form $\gamma(a)$;
- (2) wff of the form $(\gamma(a) \supset \gamma(b))$, which proceed directly by substitution from axioms of $(R + S)$.

Proof. Almost at once from Lemmas 7 and 8.

LEMMA 17. $\vdash_{(R+S+T)} \gamma(a)$ iff there exists some wff b , such that $\gamma(\bar{\Delta}_0(b)) \vdash_{(R+S)} \gamma(a)$.

Proof. The "iff" part is trivial, so we go straight to the "only if" part.

By a standard result, the derivation of $\gamma(a)$ can be carried out in two successive phases, the first consisting exclusively of substitutions, and the second exclusively of applications of modus ponens. Take such a derivation of $\gamma(a)$. We proceed by induction upon n , the number of applications of modus ponens.

For $n = 0$, the result is trivial. Assume the result for $0 \leq n \leq k$, and consider the case $n = k + 1$. Let the first premise in the $(k + 1)$ st application of modus ponens be $\gamma(c)$ (Lemma 8). The second premise must proceed immediately by substitution from an axiom of $(R + S)$ (Lemmas 8 and 16). Hence

$$\gamma(c) \vdash_{(R+S)} \gamma(a).$$

By induction hypothesis, there exists a wff b , such that

$$\gamma(\bar{\Delta}_0(b)) \vdash_{(R+S)} \gamma(c).$$

Therefore $\gamma(\bar{\Delta}_0(b)) \vdash_{(R+S)} \gamma(a)$, as required.

LEMMA 18. $\vdash_{(R+S+T)} \gamma(a)$ iff there exist a word Θ of Γ , and wff b , such that (1) $E(a) = \bar{\Theta}(b)$, and (2) $\vdash_{\Gamma} \Theta$.

Proof. Applying Lemma 12 to Lemma 17, $\vdash_{(R+S+T)} \gamma(a)$ iff, for some wff b , $\bar{\Delta}_0(b) \prec a$.

Bearing in mind the fact that $E(\bar{\Delta}_0(b)) = \bar{\Delta}_0(b)$, this gives us the required result. From this last lemma and Lemma 4, it follows that $\vdash_{\Gamma} \Phi$ iff $\vdash_{(R+S+T)} \gamma(\bar{\Phi}(x_1))$. Hence we have

LEMMA 19. (D1) reduces to (D4).

Conversely, we have

LEMMA 20. (D4) reduces to (D1).

Proof. An answer to the question:

(X) Is the wff a a theorem of $(R + S + T)$?

can be obtained by carrying out the following instructions in the order given:

(1) Ask, Does a proceed immediately by substitution from an axiom of $(R + S)$? If the answer is Yes, then so is the answer to (X). If the answer is No, proceed to (2).

(2) Ask, Is a of the form $\gamma(b)$? if the answer is No, then so is the answer to (X) (Lemma 16). If the answer is Yes, construct b and proceed to (3).

(3) Ask, Is $E(b)$ of the form $\gamma(c)$? If the answer is No, then so is the answer to (X) (Lemma 18). If the answer is Yes, construct Φ (it is unique by Lemma 4) and proceed to (4).

(4) Ask, Is Φ a theorem of Γ ? The answer to (X) is the same as the answer to this last question (Lemma 18).

This completes the procedure. It would be simple in principle to make every stage effective, except for (4), which is already reduced to (D1) as it stands.

Combining Lemmas 19 and 20, we have

LEMMA 21. (D1), (D4) are of the same degree of unsolvability.

We are now in a position to prove

THEOREM 1. *Given the expression of implication to be used in the modus ponens rule, and restricting ourselves to the connectives appearing in this expression, we can choose a finite set of axioms so as to obtain a propositional calculus of any required recursively enumerable degree of unsolvability.*

Proof. We exhibit $(R + S + T)$ as a propositional calculus with the required properties. It is sufficient to show that, as Γ varies over all semi-Thue systems, so $(D4)$ ranges over all recursively enumerable degrees of unsolvability. It follows from Clapham's main result in [3], (also found in [2]) that, as Γ ranges over all semi-Thue systems, so $(D1)$ ranges over all recursively enumerable degrees of unsolvability. The theorem now follows from Lemma 21.

7. Inter-reducibility of $(D3)$, $(D5)$. Throughout this section, Definition 2 of γ holds. We shall look for a method of deciding whether any given wff is a theorem of $(P + Q + R + S)$. It is clear that difficulties will arise only if the given wff contains α . For, if it does not contain α , then it is a theorem iff it is a tautology (due to the completeness of Q). We shall give a method depending upon $(D3)$ for constructing from any given wff a of $(P + Q + R + S)$ a wff a^* of Q , with the property that a is a theorem of $(P + Q + R + S)$ iff a^* is.

THE *-NOTATION. Take any wff a . Let the number of occurrences in it of wff with outermost connective α , which do not take place within the scope of any other α , be n . Replace the i th such occurrence (reading from left to right in a) by y_i , for $i = 1, \dots, n$; where y_1, \dots, y_n are the first n vbls of the series x_1, x_2, \dots , which do not appear in a .

Let the wff thus replaced by y_1, \dots, y_n be a_1, \dots, a_n ; and let the wff thus obtained from a^* be a^\dagger .

Let $\{b_1, \dots, b_m\}$ be the set of all wff,

$$(y_i \supset y_j) \quad (\text{where } 1 \leq i \leq n, 1 \leq j \leq n, \text{ and } i \neq j)$$

for which, $a_i \vdash_{(R+S)} a_j$ (the exact ordering of b_1, \dots, b_m does not matter). Then we define

$$a^* = (b_1 \supset (b_2 \supset \dots (b_m \supset a^\dagger) \dots)).$$

If the set $\{b_1, \dots, b_m\}$ is void, $a^* = a^\dagger$.

Lemmas 22–25 will be devoted to proving that, if a is a theorem of $(P + Q + R + S)$, then so is a^* .

LEMMA 22. *If c^* and $(c \supset d)^*$ are theorems of $(P + Q)$, then so is d^* .*

Proof. Writing $a = (c \supset d)$, and following the notation used in the definition of a^* just above, we have

$$(1) \quad \vdash_{(P+Q)} (b_1 \supset (b_2 \supset \dots (b_m \supset a^\dagger) \dots)).$$

Since \supset does not contain α , a^\dagger will be of the form $(c^x \supset d^x)$, where c^x, d^x differ from c^\dagger, d^\dagger only in the naming of the vbls.

Let $\{c_1, \dots, c_p\}$ be that subset of $\{b_1, \dots, b_m\}$ which has no vbls except those found in c^x ; and let $\{d_1, \dots, d_m\}$ be that subset of $\{b_1, \dots, b_m\}$ which has no vbls

except those found in d^X . If the two subsets just defined are suitably ordered, then c^* , d^* will differ from, respectively

$$(c_1 \supset (c_2 \supset \dots (c_p \supset c^X) \dots)),$$

$$(d_1 \supset (d_2 \supset \dots (d_q \supset d^X) \dots)),$$

only in the naming of some of the vbls. Hence

$$(2) \quad \vdash_{(P+Q)} (c_1 \supset (c_2 \supset \dots (c_p \supset c^X) \dots)).$$

In view of the completeness of Q , results (1) and (2) lead to

$$(3) \quad \vdash_{(P+Q)} (b_1 \supset (b_2 \supset \dots (b_m \supset d^X) \dots)).$$

Because of the transitivity of the relation $\vdash_{(R+S)}$, we have:

$$(4) \quad \text{If } (x_i \supset x_j) \text{ and } (x_j \supset x_k) \text{ both belong to } \{b_1, \dots, b_m\},$$

then so does $(x_i \supset x_k)$, unless $i = k$.

Take any assignment of truth-values to the vbls of $\{d_1, \dots, d_q\}$, in which all of d_1, \dots, d_q are "true." Extend this by assigning truth-values to the remaining vbls of $\{b_1, \dots, b_m\}$, in such a way that,

x_i is "true," if there exists some vbl x_j of $\{d_1, \dots, d_q\}$, such that x_j is "true," and $(x_j \supset x_i)$ belongs to $\{b_1, \dots, b_m\}$;
 x_i is "false" otherwise.

Because of result (4), all of b_1, \dots, b_m must be "true" under this assignment. So we have:

Every assignment of truth-values to the vbls of $\{d_1, \dots, d_q\}$ in which all q of these wff are "true," is part of an assignment of truth-values to *all* vbls, in which all of b_1, \dots, b_m are "true."

Now, result (3) tells us that d^X is "true" in any assignment of truth-values in which all of b_1, \dots, b_m are true. Hence, by result (5), d^X is "true" in any assignment of truth-values under which all of d_1, \dots, d_q are true.

Therefore $(d_1 \supset (d_2 \supset \dots (d_q \supset d^X) \dots))$ is a tautology and hence, because of the completeness of Q , it is a theorem of $(P + Q)$.

Hence, by a substitution which simply re-names some of the vbls, $\vdash_{(P+Q)} d^*$.

LEMMA 23. *If a proceeds directly by substitution from an axiom of $(P + Q)$, then $\vdash_{(P+Q)} a^*$.*

Proof. Again we follow the notation used during the definition of a^* from a .

Let c be an axiom of $(P + Q)$ which generates a by the substitution, say, in which x_1, \dots, x_p are replaced by c_1, \dots, c_p . Since c does not contain α , every wff-occurrence which, in going from a to a^\dagger , is replaced by a new vbl, must have been introduced into a by virtue of being contained in one of c_1, \dots, c_p . By replacing

each such wff-occurrence by the appropriate vbl (that which replaces the wff-occurrence in a), obtain the wff c'_1, \dots, c'_p from c_1, \dots, c_p .

Then a^\dagger is obtained from c by the substitution which replaces x_1, \dots, x_p by c'_1, \dots, c'_p . Therefore a^\dagger is a theorem of $(P + Q)$, and hence so is a^* .

LEMMA 24. *If a proceeds directly by substitution from an axiom of $(R + S)$, then $\vdash_{(P+Q)} a^*$.*

Proof. It is sufficient to observe that a^* must be of one of the following three tautologous forms:

$$\begin{aligned} & ((y_1 \supset y_2) \supset (y_1 \supset y_2)), \\ & ((y_2 \supset y_1) \supset ((y_1 \supset y_2) \supset (y_1 \supset y_2))), \\ & ((y_1 \supset y_2) \supset ((y_2 \supset y_1) \supset (y_1 \supset y_2))), \end{aligned}$$

for some vbls y_1, y_2 .

LEMMA 25. *If $\vdash_{(P+Q+R+S)} a$, then $\vdash_{(P+Q)} a^*$.*

Proof. By a standard result, the derivation of any theorem a of $(P + Q + R + S)$ can be carried out in two successive phases, the first consisting exclusively of substitutions, and the second exclusively of applications of modus ponens. Viewing this mode of derivation in the light of Lemmas 22–24, we conclude that $\vdash_{(P+Q)} a^*$.

The next two lemmas are concerned with proving the converse of Lemma 25.

LEMMA 26. *If a, b both have α as their outermost connective, and $a \vdash_{(R+S)} b$, then*

- (1) *either $a = b$, or there exist wff c, d , such that $a = \gamma(c)$ and $b = \gamma(d)$,*
- (2) $\vdash_{(P+Q+R+S)} (a \supset b)$.

Proof. Suppose $a \neq b$. Since b does not proceed directly by substitution from an axiom of $(R + S)$ (because of its outermost connective), there must be at least one application of modus ponens in its derivation. Consider the very first such application. a cannot act as second premise, being of the wrong form. Therefore the second premise must proceed by substitution from an axiom of $(R + S)$; in which case the only way for there to be a first premise available is for a to be of the form $\gamma(c)$. It then follows from Lemma 8 that b must be of the form $\gamma(d)$.

Now we tackle the second part of the lemma. By the first part of the present lemma, and Lemma 9, there exist wff e_1, \dots, e_m , for some m , such that,

$$\begin{aligned} & \vdash_{(R+S)} (a \supset \gamma(e_1)), \\ & \vdash_{(R+S)} (\gamma(e_1) \supset \gamma(e_2)), \\ & \quad \dots \quad \dots \\ & \vdash_{(R+S)} (\gamma(e_m) \supset b). \end{aligned}$$

Also we have

$$\vdash_Q ((x_1 \supset x_2) \supset ((x_2 \supset x_3) \supset (x_1 \supset x_3))).$$

Substituting several times into this last line, and applying modus ponens to it and the $(m + 1)$ lines just above, we get

$$\vdash_{(P+Q+R+S)} (a \supset b).$$

We could have obtained this last result in the case $a = b$, simply by substituting into the theorem $(x_1 \supset x_1)$ of Q .

LEMMA 27. *If $\vdash_{(P+Q)} a^*$, then $\vdash_{(P+Q+R+S)} a$.*

Proof. We follow the notation used in the original definition of a^* from a . By hypothesis,

$$\vdash_{(P+Q)} (b_1 \supset (b_2 \supset \cdots (b_m \supset a^\dagger) \cdots)).$$

Applying the substitution which sends y_1, \dots, y_n into a_1, \dots, a_n , we get

$$(1) \quad \vdash_{(P+Q)} (c_1 \supset (c_2 \supset \cdots (c_m \supset a) \cdots)),$$

where c_i is the result of applying the foregoing substitution to b_i , for $i = 1, \dots, m$.

Now, each c_i is of the form $(a_j \supset a_k)$, where $a_j \vdash_{(R+S)} a_k$, and both of a_j, a_k have α as outermost connective. Hence, by Lemma 26,

$$(2) \quad \vdash_{(P+Q+R+S)} c_i, \text{ for } i = 1, \dots, m.$$

From results (1) and (2), by m applications of modus ponens, we get

$$\vdash_{(P+Q+R+S)} a.$$

Combining Lemmas 25 and 27, we have

LEMMA 28. $\vdash_{(P+Q+R+S)} a$ iff $\vdash_{(P+Q)} a^*$.

We are now in a position to prove

LEMMA 29. *(D5) reduces to (D3).*

Proof. Consider the question:

(X) Is a a theorem of $(P + Q + R + S)$?

Our first step is to construct a^* . The only part of the construction that might prove ineffective consists in answering in a finite number of cases the question:

(Y) Does $b \vdash_{(R+S)} c$?

where b, c both have α as outermost connective. An answer to (Y) is obtained by carrying out the following instructions in the order given:

(1) Ask, Does $b = c$? If the answer is Yes, then so is the answer to (Y) . If the answer is No, proceed to (2).

(2) Ask, Do there exist wff d, e , such that $b = \gamma(d)$ and $c = \gamma(e)$? If the answer is No, then so is the answer to (Y) (Lemma 26). If the answer is Yes, construct d, e and proceed to (3).

(3) Ask, Does $\gamma(d) \vdash_{(R+S)} \gamma(e)$? The answer to this is the answer to (Y) .

Each stage in the procedure is easily made effective, except for (3), which is reduced to (D3) as it stands.

Once a^* is constructed, the rest of the procedure is effective. It is only necessary to ask: Is a^* a tautology? The answer to this will be the answer to (X) (Lemma 28). (A qualification is needed here. If Q has infinitely many connectives, and the task of finding out the truth-function associated with each of these is linked to an unsolvable decision problem, then the problem of deciding whether any given a^* is a tautology may be unsolvable. However, I propose to ignore this rather artificial situation.)

LEMMA 30. (D3) reduces to (D5).

Proof. $\gamma(a) \vdash_{(R+S)} \gamma(b)$ iff $(\gamma(a) \supset \gamma(b))^*$ is a tautology (by consideration of the possible forms of the latter—there are only three):

i.e., iff $\vdash_{(P+Q)} (\gamma(a) \supset \gamma(b))^*$ (completeness of Q).

i.e., iff $\vdash_{(P+Q+R+S)} (\gamma(a) \supset \gamma(b))$ (Lemma 28).

Combining Lemmas 29 and 30, we have

LEMMA 31. (D3), (D5) are of the same degree of unsolvability.

We are now in a position to prove

THEOREM 2. *Every propositional calculus can be embedded in one of an arbitrary recursively enumerable degree of unsolvability, by bringing in any given new connective (as long as it has at least one arg-place) and some axioms containing it. If the given calculus has finitely many connectives, it is sufficient to add a finite number of axiom s.*

Proof. Take the given propositional calculus to be A and the given new connective to be α . It is sufficient to show that as Γ varies over all semi-Thue systems so the decision problem of $(P + Q + R + S)$ ranges over all recursively enumerable degree of unsolvability. The remark about the case when P has finitely many connectives, follows from the fact that Q is then finitely axiomatizable (proved by Henkin in [6]).

As Γ ranges over all semi-Thue systems, so (D2) ranges over all recursively enumerable degrees of unsolvability. This result is given by Boone in [1] (abstract);

alternatively it can be deduced from a similar result for groups proved by Clapham in [2] and [3].

The theorem now follows from Lemmas 15 and 32.

BIBLIOGRAPHY

1. W. W. Boone, *Thue system with word problem of any preassigned recursively enumerable degree of unsolvability*, Abstracts of Short Communications, Internat. Congr. of Mathematicians, Stockholm, Almqvist, Uppsala, 1962.
2. C. R. J. Clapham, *Some investigations in abstract algebra*, Doctoral Thesis, Oxford Univ., Oxford, 1962.
3. ———, *The existence of finitely-presented groups with word problems of arbitrary degrees of unsolvability*, Proc. London Math. Soc. (to appear).
4. Martin Davis, *Computability and unsolvability*, McGraw-Hill, New York, 1958.
5. R. Harrop, *Finite models and decision procedures for propositional calculi*. I, Proc. Cambridge Philos. Soc. **54** (1958), 1–13.
6. Leon Henkin, *Fragments of the propositional calculus*, J. Symbolic Logic **14** (1949), 42–48.
7. S. Linial and E. L. Post, *Recursive unsolvability of the deducibility, Tarski's completeness and independence of axiom problems of the propositional calculus*, Abstract 38, Bull. Amer. Math. Soc. **55** (1949), 50.
8. Jean Porte, *An associativity lemma*, Abstracts of Short Communications, Internat. Congr. of Mathematicians, Stockholm, Almqvist and Wiksells, Uppsala, 1962.

UNIVERSITY OF BRISTOL,
BRISTOL, ENGLAND