760
Notre Dame Journal of Formal Logic
Volume XX, Number 4, October 1979
NDJFAM

A GENERALIZED THEOREM CONCERNING A RESTRICTED RULE OF SUBSTITUTION IN THE FIELD OF PROPOSITIONAL CALCULI

CHARLES H. LAMBROS

Sobociński [1] proves that certain axiomatized systems of the propositional calculus having the rule of simultaneous substitution are not weakened in their deductive power by restricting the application of the substitution rule to the axioms alone. In his proof it is shown how a proof sequence employing only the rule of substitution and a rule of detachment may be uniquely and constructively replaced by a proof sequence to the same effect employing only the restricted rule. When the rule of detachment is the classical one, since classical systems require for their completeness no more than these two rules, Sobociński's result is already a general one for classical systems. We further generalize the theorem to apply to any system (classical or not) containing any rules whatsoever. The only stipulation made (which we will express in a precise way at the appropriate time) is that such rules are "schematically representable".

Theorem *If* $\mathbf{T}$ *is an axiom system in the propositional calculus such that it contains*

1. *a rule of simultaneous substitution,* R_s
2. *other schematically representable rules of inference* $R_1, R_2, \ldots, R_k$ *(none of which are* R_s*)*
3. *an axiom set* A,

and if $\{a_1, a_2, \ldots, a_m\}$ *is a finite sequence of axioms and* $\{a_1, a_2, \ldots, a_m, b_1, \ldots, b_n\}$ *constitutes a proof sequence in* $\mathbf{T}$ *of* b_n*, then that proof sequence where none of* $b_1, \ldots, b_n$ *is in* A *may be replaced by a proof sequence in* $\mathbf{T}$ *of* b_n *which restricts the applications of* R_s *to* $\{a_1, a_2, \ldots, a_m\}$.

Before presenting the proof, we give the following terminological remarks. When $b_1, \ldots, b_n, c$ are formulas such that c follows from $b_1, \ldots, b_n$ by some rule R of $\mathbf{T}$, we shall write $\{b_1, \ldots, b_n\} \vdash_{\overline{R}} c$. Where a_i, $1 \leqslant i \leqslant m$, is in A, and $\{a_1, \ldots, a_m, \ldots, b\}$ constitutes a proof sequence of b in $\mathbf{T}$, $\{a_1, \ldots, a_m\}$ shall be represented by "α", the rest of the sequence by

Received June 15, 1975

"βb", and the entire sequence by "$\alpha;\beta b$". Classes will be designated by the variables "γ", "δ", . . . and by "(. . .)".

Proof: By induction on the length of proof sequences, where the "length" of the proof sequence $\{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ is n.

Base step: $n = 1$. Then the theorem follows immediately.

Induction step: Suppose the theorem holds for all sequences of length $n \leqslant p$. It will be shown that it then holds for all sequences of length $p + 1$. Consider an arbitrary proof sequence of length $p + 1$, $\{a_1, \ldots, a_m, b_1, \ldots, b_p, b_{p+1}\}$.

Case 1. In $\alpha;\ \beta_{b_{p+1}}$, b_{p+1} follows from earlier lines $c_1, \ldots, c_n$ by some R_i, $1 \leqslant i \leqslant k$, (and R_i is not R_s). Then there are proof sequences (sub-sequences of $\alpha;\ \beta_{b_{p+1}}$)

$$\alpha;\ \beta_{c_1},\ \alpha;\ \beta_{c_2},\ \ldots,\ \alpha;\ \beta_{c_n}$$

such that each sequence is of length no greater than p. But then by the induction hypothesis, each may be replaced by sequences to the same effect but which restrict the application of R_s to α. Call these replacements

$$\alpha;\ \beta^*_{c_j},\ 1 \leqslant j \leqslant n.$$

Now form the sequence

$$\alpha;\ \beta^*_{c_1};\ \beta^*_{c_2};\ \ldots;\ \beta^*_{c_n}.$$

Such a sequence contains each of $c_1, c_2, \ldots, c_n$ and restricts R_s to α. Now annex $\{b_{p+1}\}$ to form

$$\alpha;\ \beta^*_{c_1};\ \beta^*_{c_2};\ \ldots;\ \beta^*_{c_n};\ \{b_{p+1}\}$$

and, since $\{c_1, \ldots, c_n\} \vdash_{\overline{R_i}} b_{p+1}$, the theorem holds.

Case 2. In $\alpha;\ \beta_{b_{p+1}}$, b_{p+1} follows from some earlier line μ by R_s. There are three subcases.

Case 2a. μ appears in α. Then replace $\alpha;\ \beta_{b_{p+1}}$ by $\alpha;\ \{b_{p+1}\}$ and the theorem holds.

Case 2b. μ appears in β_p and μ follows from some earlier line ν by R_s. Then there must be some substitution in ν which yields b_{p+1} directly. So drop μ from β_p and add b_{p+1}. Such a sequence is of length no greater than p, and so by the induction hypothesis the theorem holds.

Before proceeding to Case 2c, we shall first provide a precise sense to the statement that a rule is "schematically representable", and then prove a lemma. The intuitive idea behind a "schematically representable" rule is that the applicability of the rule depends only on the structure of a sequence of formulas, not on the occurrence of any particular propositional variables. We begin by providing a way of characterizing all the possible logical structures of the formulas of the language of **T**.

Suppose that the formulas of the language of **T** are unambiguous, i.e., that there is but one predominant logical operator in each formula, and that each operator is a function on at most two formulas, yielding a new formula with those as component parts.[1] Then all the operators appearing in an arbitrary formula A may be indexed in a binary branch notation. For example, we will write "${}_AL_{RRLR}$" to designate the logical operator which is dominant in the right-hand component (formula) of the left-hand component of the right-hand component of the right-hand component of A. (If the language of **T** includes operators which function on a single formula, we shall call that formula, arbitrarily, the left-hand component, and there is no right-hand component of the formula in which that operator dominates.) The following ordered sequence then will include a designation for every logical sign occurring in A (though some of them may designate nothing which occurs in A): ${}_AL$ (which designates the dominant operator of A itself), ${}_AL_L$, ${}_AL_R$, ${}_AL_{LL}$, ${}_AL_{LR}$, ${}_AL_{RL}$, ${}_AL_{RR}$, ${}_AL_{LLL}$, ${}_AL_{LLR}$, ${}_AL_{LRL}$, ${}_AL_{LRR}$, ${}_AL_{RLL}$, and so on. Let us index this ordered sequence by the sequence of prime numbers beginning with 2, i.e., as $P_1(=2)$, $P_2(=3)$, $P_3(=5)$, . . ., P_i, ... Now suppose that there are n logical signs in the language of **T**. Index these as 1, 2, 3, ... Then we may assert that A has the logical operator indexed by i in the position indexed by P_m by "$S_A((P_m)^i)$" (read "A has the structure P_m to the exponent i"). In general, that A has the logical operators indexed by $i, j, \ldots, k$ in the positions indexed by P_m, P_n, . . ., P_o will be expressed by "$S_A((P_m)^i \cdot (P_n)^j \cdot \ldots \cdot (P_o)^k)$". In this way, the logical structure of A is completely and uniquely characterized by "$S_A(p)$", where p is some number with a unique prime factor decomposition, where each prime factor designates a position in A, and the number of times that factor appears designates which operator appears in that position. If $S_A(p)$, we call (p) the "structural mode of A". Also, when $S_A(p)$, and some q $(\neq 1)$ divides p evenly with quotient r, and where none of the prime factors of q are factors of r, (q) is also a structural mode of A. Finally, we shall say of a sequence of formulas $\{d_1, d_2, \ldots, d_k\}$ that it has the structural mode $S = (S_{d_1}(m), S_{d_2}(n), \ldots, S_{d_k}(o))$. If some d_i, $1 \leqslant i \leqslant k$, does not appear as a subscript in S, this means that S leaves the logical structure of d_i unspecified.

When a formula A has formulas as proper parts, we call these the components of A. The branch sequence ${}_AC$ (which is A itself), ${}_AC_L$, ${}_AC_R$, ${}_AC_{LL}$, ${}_AC_{LR}$, and so on, contains a designation for each component of A. We index this ordered sequence by the sequence of primes. Consider an arbitrary sequence of length k of formulas $d_1, \ldots, d_k$. Let us index this sequence with the first k primes. If d_m, $1 \leqslant m \leqslant k$, indexed by the m-th prime P_m, has a component indexed by P_i which is identical to the component at P_j in the formula (d_n) indexed by P_n, $1 \leqslant n \leqslant k$, we say that the sequence, D_k, has the "component identity mode" $((P_i)^{P_m} \cdot (P_j)^{P_n})$; and in general if in D_k d_m has a component at P_s which is identical to the component P_t in d_p, and d_n has a component at P_u which is identical to the component at P_v in d_q, . . ., and d_o has a component at P_w which is identical to the component at P_x in d_r, we shall write "$C_{D_k}((P_s)^{P_m} \cdot (P_t)^{P_p}, (P_u)^{P_n} \cdot (P_v)^{P_q}, \ldots, (P_w)^{P_o} \cdot (P_x)^{P_r})$". Thus for a sequence of length k a component identity mode may be uniquely and effectively expressed by "$C_{D_k}((p), (q), \ldots, (r))$", where $p, q, \ldots, r$ have a prime factor decomposition. If for some s, m $(P_s)^{P_m}$ is a factor of none of $p, q, \ldots, r$, then the component of d_m at P_s need not be identical to any other component of any other formula in the sequence in order for the sequence to have that identity mode. Finally, if $C_D\gamma$ and $\delta \subseteq \gamma$, then $C_D\delta$.

We are now in a position to give a precise sense to the term "schematically representable". We shall call a rule "schematically representable" if and only if a complete expression of R may be given by the specification of a structural mode $S = (S_{d_1}(m), \ldots, S_{d_k}(o))$ and a component identity mode $C = C_{D_k}((p), (q), \ldots, (r))$. To say that R is a rule of inference means that when S and C are modes of any sequence of length k, $\{d_1, d_2, \ldots, d_{k-1}, d_k\}$, then $\{d_1, d_2, \ldots, d_{k-1}\} \vdash_{\overline{R}} d_k$.

We now prove the following:

Lemma *If R_i is schematically representable, $\{c_1, \ldots, c_n\} \vdash_{\overline{R_i}} \mu$, and $\{\mu\} \vdash_{\overline{R_s}} b_{p+1}$, then there will be substitutions in $c_1, \ldots, c_n$ such that $\{c_1\} \vdash_{\overline{R_s}} c'_1$, $\{c_2\} \vdash_{\overline{R_s}} c'_2, \ldots, \{c_n\} \vdash_{\overline{R_s}} c'_n$, and $\{c'_1, \ldots, c'_n\} \vdash_{\overline{R_i}} b_{p+1}$.*

Proof: Consider the substitutions in μ such that $\{\mu\} \vdash_{\overline{R_s}} b_{p+1}$. Among the propositional variables occurring in μ, some or all are simultaneously and in every one of their occurrences replaced by some formula of the language of **T**. Suppose the variables of μ which are changed in this way are $q_1, q_2, \ldots, q_h$, and the formulas which replace them are $Q_1, Q_2, \ldots, Q_h$ respectively. (In order to facilitate the proof μ is renamed "c_o".) Now wherever $q_1, \ldots, q_h$ appear in $c_1, \ldots, c_n, c_o$ make those same substitutions, the rest of the variables remaining the same. Call the resulting formula $c'_1, \ldots, c'_n, c'_o$. Since only individual variables have been replaced, all of the logical signs appearing in any of $c_1, \ldots, c_n, c_o$ also appear in $c'_1, \ldots, c'_n, c'_o$ and in the same branch positions. Consequently, if (p) is a structural mode of $\{c_1, \ldots, c_n, c_o\}$, it is also a structural mode of $\{c'_1, \ldots, c'_n, c'_o\}$. Now suppose that C is some component identity mode of $\{c_1, \ldots, c_n, c_o\}$. We shall show that it is also a component identity mode $\{c'_1, \ldots, c'_n, c'_o\}$. Suppose that $(P_s)^{P_m} \cdot (P_t)^{P_p}$ is in C. (If C is empty, then any sequence of length 0 has the component identity mode specified in R.) Then the component in c_m at P_s is identical to the component in c_p at P_t. If none of $q_1, \ldots, q_h$ appear in either component, then these components are unchanged after the substitution and remain in the same branch position in $\{c'_1, \ldots, c'_n, c'_o\}$. In this case, $(P_s)^{P_m} \cdot (P_t)^{P_p}$ is a component identity mode of the latter. If any of $q_1, \ldots, q_h$ do appear, then, since the substitutions for these are simultaneous and uniformly replace every occurrence of the variables, the component of c'_m at P_s must take the same form of the component of c'_p at P_t. Consequently $(P_s)^{P_m} \cdot (P_t)^{P_p}$ is also a component identity mode of $\{c'_1, \ldots, c'_n, c'_o\}$.

Now since $\{c_1, \ldots, c_n\} \vdash_{\overline{R_i}} c_o$, then the sequence $\{c_1, \ldots, c_n, c_o\}$ has the modes S and C specified in the expression of R_i. But then so does $\{c'_1, c'_2, \ldots, c'_n, c'_o\}$. Thus $\{c'_1, \ldots, c'_n\} \vdash_{\overline{R_i}} c'_o$, where c'_o is just $c_o\,(\mu)$ except that where $q_1, \ldots, q_h$ appeared in μ, $Q_1, \ldots, Q_h$ now appear in c'_o. But then c'_o is just b_{p+1}.

Case 2c. μ appears in β_p and μ follows from earlier lines $c_1, \ldots, c_n$ by some R_i, $1 \leqslant i \leqslant k$, and R_i is not R_s. In this case, there are proof sequences for each of $c_1, \ldots, c_n$, $\alpha; \beta_{c_1}$, $\alpha; \beta_{c_2}, \ldots, \alpha; \beta_{c_n}$, such that none are of length greater than $p - 1$. By the lemma, since $\{c_1, \ldots, c_n\} \vdash_{R_i} \mu$ and $\{\mu\} \vdash_{R_s} b_{p+1}$, there are substitutions in $c_1, \ldots, c_n$ resulting in $c_1', \ldots, c_n'$ such that $\{c_1', \ldots, c_n'\} \vdash_{R_i} b_{p+1}$. Form the sequences

$$\alpha;\ \beta_{c_1};\ \{c_1'\},\quad \alpha;\ \beta_{c_2};\ \{c_2'\},\ \ldots,\ \alpha;\ \beta_{c_n};\ \{c_n'\}$$

and represent these as

$$\alpha;\ \beta'_{c_i},\ 1 \leqslant i \leqslant n,\ \text{respectively.}$$

Since each of $\alpha; \beta_{c_i}$, $1 \leqslant i \leqslant n$, is of length no greater than $p - 1$, none of $\alpha; \beta'_{c_i}$, $1 \leqslant i \leqslant n$, is of length greater than p. So by the induction hypothesis each may be replaced by a sequence $\alpha; \beta^{*\prime}_{c_i}$ which is a proof sequence of c_i', respectively, employing R_s only in the restricted way. Now form the sequence

$$\alpha;\ \beta^*c_1';\ \beta^*c_2';\ \ldots;\ \beta^*c_n'.$$

This contains each of $c_1', \ldots, c_n'$, and employs R_s only upon α. Now annex $\{b_{p+1}\}$ to form

$$\alpha;\ \beta^*c_1';\ \beta^*c_2';\ \ldots;\ \beta^*c_n';\ \{b_{p+1}\}$$

and, since $\{c_1', \ldots, c_n'\} \vdash_{R_i} b_{p+1}$, the theorem holds.

NOTE

1. If there are operators which function on more than two component formulas, say, n components, then the branch notation sequence will need to be n-ary instead of binary as in the text. Aside from this, the proof remains the same.

REFERENCE

[1] Şobociński, Bolesław, "A theorem concerning a restricted rule of substitution in the field of propositional calculi, I, II," *Notre Dame Journal of Formal Logic*, vol. XV (1974), pp. 465-476 and 589-597.

State University of New York at Buffalo
Buffalo, New York