2006

TR-2006002: A Replacement Theorem for LP

Melvin Fitting

A Replacement Theorem For LP

Melvin Fitting
Dept. Mathematics and Computer Science
Lehman College (CUNY), 250 Bedford Park Boulevard West
Bronx, NY 10468-1589
e-mail: melvin.fitting@lehman.cuny.edu
web page: comet.lehman.cuny.edu/fitting

March 21, 2006

Abstract

The replacement theorem for classical and normal modal logics is a fundamental tool. It says that if A and B have been proved equivalent, occurrences of A in a formula may be replaced with occurrences of B to produce a formula equivalent to the original one. This theorem does not hold for LP, Logic of Proofs. A replacement for replacement is not simple to formulate. In this note I have provided one, along with some machinery for working with LP realizations that may prove useful for other things as well.

1 Introduction

The logic LP (logic of proofs) was introduced by Artemov, see [2]. It is a propositional modal-like logic that was introduced to help solve a problem originating with Gödel: provide a natural arithmetic foundation for intuitionistic logic, [4]. LP plays a central role in doing that. But it also proves to be an interesting logic for its own sake, a logic of explicit evidence. It is, however, a difficult logic to work with. Semantics, see [3], is more complex than that of standard modal logics, and the same applies to its proof theory. In this note I provide a proof-theoretic tool whose counterpart for more conventional logics is almost trivial. But first, a small amount of background.

LP is a modal-like language, but instead of a single modal operator it has an infinite family of them—they are called *proof polynomials*. If t is a proof polynomial and X is a formula, $t{:}X$ is another formula which can be read "t is a proof of X", or "t is a reason for X". Part of the formal machinery of the logic is a calculus on proof polynomials. LP is intended to have a close relationship with the normal modal logic S4, which in turn has a close relationship with intuitionistic logic and, as Gödel observed, S4 necessity has the properties one associates with an informal notion of provability. A formal connection between LP and arithmetic is made explicit in Artemov's Arithmetic Completeness Theorem. A formal connection between LP and S4 is Artemov's Realization Theorem. Loosely it says that each theorem of S4 can be converted into a theorem of LP that expresses the constructive content of the S4 theorem. Negative occurrences of $\Box$ become proof variables and positive occerences of $\Box$ become proof polynomials that may involve those variables. A proper statement is in Theorem 2.1. For a thorough presentation of LP, including motivation, see [2].

We commonly replace, in a formula $Z(A)$, a subfomula A with another formula B that has been proved to be equivalent to A, getting a new formula $Z(B)$, and conclude that $Z(A)$ and $Z(B)$

are themselves equivalent. This is something we do all the time. But things are not so simple in LP, where the subformula A of $Z(A)$ may be embedded in a structure of reasons, represented by proof polynomials. If A is replaced with B, reasons must be updated to reflect the original ones combined with ones embodying the passage from A to B. Further, A may be present in different parts of $Z(A)$ for different reasons. All this can lead to considerable complexities. In this note I provide a replacement for the usual replacement theorem, appropriate for LP.

One of the things accomplished in this paper is turning realizations into first-class mathematical objects—essentially functions defined on occurrences of modal operators. In order to do this conveniently, an *annotated* version of S4 is introduced, in which distinct occurrences of the necessity operator are syntactically different symbols. All this makes it easier to reason about realizations and their behavior. I think it will be found to be a useful tool.

Since Artemov's original work, the ideas of LP have been extended to a family of similar logics. Thus S4 is not the only standard modal logic that has an LP-style analysis, and various multi-modal logics have also been brought into the picture. Part of the motivation has been the desire to see proof polynomials as explicit reasons in a sense that is more general than just formal proofs, with applications to logics of knowledge. I do not address the whole family of LP-like logics here—things are complicated enough. But it is clear that my methods do extend. My purpose is simply to provide some proof-theoretic tools that make life simpler, even when reasons are made explicit.

2 The Logic LP

This section contains a brief formulation of LP axiomatically. A semantics will not be needed in this paper. The language of LP, denoted L_{LP} here, is built from the following basic machinery, which appears in [2].

1. propositional variables, P, Q, P_1, P_2, ...
2. propositional constant, $\bot$
3. logical connective, $\supset$
4. proof variables, x, y, x_1, x_2, ...
5. proof constants, c, d, c_1, c_2, ...
6. function symbols ! (monadic), $\cdot$, $+$ (binary)
7. operator symbol of the type $\langle term \rangle$:$\langle formula \rangle$

Proof polynomials are built up from proof variables and proof constants, using the function symbols. *Ground* proof polynomials are those without variables. *Formulas* are built up from propositional variables and the propositional constant using $\supset$ (with other connectives defined in the usual way), and an extra rule of formation: if t is a proof polynomial and X is a formula then $t{:}X$ is a formula.

The formula $t{:}X$ can be read: "t is a proof of X." Proof constants intuitively represent proofs of basic, assumed truths. Proof variables in a formula can be thought of as implicitly universally quantified over proofs. If t is a proof of $X \supset Y$ and u is a proof of X, we should think of $t \cdot u$, the application of t to u, as a proof of Y. The operation ! is a proof-checker: if t is a proof of X then $!t$ is a verification that t is such a proof. The operation $+$ combines proofs in the sense that $t + u$ proves all the things that t proves plus all the things that u proves.

The following axiom system for LP is from [1, 2] Axioms are specified by giving axiom schemas, and these are:

A0.	**Classical**	Classical propositional axiom schemes
A1.	**Application**	$t{:}(X \supset Y) \supset (s{:}X \supset (t \cdot s){:}Y)$
A2.	**Reflexivity**	$t{:}X \supset X$
A3.	**Proof Checker**	$t{:}X \supset\ !t{:}(t{:}X)$
A4.	**Sum**	$s{:}X \supset (s+t){:}X$
		$t{:}X \supset (s+t){:}X$

Rules of inference include modus ponens, and a version of the necessitation rule, for axioms only.

R1.	**Modus Ponens**	$\vdash Y$ provided $\vdash X$ and $\vdash X \supset Y$
R2.	**Axiom Necessitation**	$\vdash c{:}X$ where X is an axiom *A0 – A4* and c is a proof constant.

As usual, a proof is a finite sequence of formulas each of which is an axiom or comes from earlier terms by one of the rules of inference. A notion of *derivation* can be introduced, either directly, or indirectly by defining $\Gamma \vdash X$ to mean $(G_1 \wedge \ldots \wedge G_n) \supset X$ is a theorem for some finite subset $\{G_1, \ldots, G_n\}$ of Γ.

The specification of which constants are associated with which axioms for rule *R2* applications is called a *constant specification*. A constant specification is *injective* if each proof constant is used for at most one axiom. Injective constant specifications suffice, but are not required. If a proof uses an injective constant specification, I will say the proof is *injective*. In [3] constant specifications were assumed to be given beforehand, and their properties were investigated in some detail. Computational complexity is dependent on the properties of the constant specification. In [2] things were more flexible, and constants were generally assigned during the course of a proof. In this paper we use this flexible version.

The Realization Theorem plays a fundamental role for LP. If X is any theorem of LP, and we replace every proof polynomial by $\Box$ (the *forgetful* map), the result is a theorem of S4. This much is easy to see: it is clearly the case for each axiom of LP, and is preserved by the LP rules of derivation. The Realization Theorem is a converse to this.

Theorem 2.1 (Realization Theorem) *If X is a theorem of S4, there is some way of replacing $\Box$ symbols with proof polynomials to produce a theorem of LP. Moreover this can be done so that negative occurrences of $\Box$ are always replaced with distinct proof variables, and positive occurrences by proof polynomials that may involve those variables.*

Negative occurrences of proof variables can be thought of as inputs, and the proof polynomials involving them as outputs. Thus theorems of S4, in a sense, carry implicit constructive content which their embeddings into LP make explicit.

Let us say the displayed occurrence of term t in the formula $t{:}Z$ is *self-referential* if t has an occurrence in Z. It is shown in [5] that constant specifications in which proof constants have self-referential occurrences are needed for completeness. However, in what follows, I will generally need to assume that we do not have self-referentiality for 'input' variables. I do not know, but strongly suspect that the Realization Theorem can be proved in such a way that self-referentiality can be avoided for variables in negative positions. This is intuitively reasonable. A negative occurrence of a proof variable in a subformula, say $x{:}Z$, represents an input that can be freely specified. It is like saying, "let x be an arbitrary proof of Z". The formula Z should not, in turn, vary with different choices of proofs for it.

Definition 2.2 A *substitution* is a mapping, σ, from proof variables to proof polynomials. If σ is a substitution and X is a formula, I will write $X\sigma$ for the result of replacing each proof variable x in X with the proof polynomial $x\sigma$. Similarly for substitution in proof polynomials.

We will often need a special condition on substitutions—this is as good a place as any to introduce it.

Definition 2.3 A substitution σ meets the *no new variable* condition provided, for each variable x, the term $x\sigma$ contains no variables other than x.

The following is shown in [2].

Theorem 2.4 (Substitution Lemma) *If X is a theorem of LP, so is $X\sigma$. Further, if X has an injective proof, so will $X\sigma$.*

The constant specification used for proving X and that used for proving $X\sigma$ will, in general, be different, but this fact can be safely ignored for what we do here.

A fundamental result that will be used over and over in this paper is the Lifting Lemma, from [2], which says that proofs and derivations in LP can be internalized. The proof is actually algorithmic—a proof polynomial t can be explicitly constructed from any given LP derivation.

Theorem 2.5 (Lifting Lemma) *Suppose*

$$s_1{:}X_1, \ldots, s_n{:}X_n, Y_1, \ldots, Y_k \vdash Z$$

then there is a proof polynomial $t(s_1, \ldots, s_n, y_1, \ldots, y_k)$ (where the y_i are variables) such that

$$s_1{:}X_1, \ldots, s_n{:}X_n, y_1{:}Y_1, \ldots, y_k{:}Y_k \vdash t(s_1, \ldots, s_n, y_1, \ldots, y_k){:}Z.$$

Moreover, if the original derivation was injective, the same is the case for the later derivation.

Corollary 2.6 *If Z has an LP proof, then for some proof polynomial t with no proof variables, $t{:}Z$ will have an LP proof, injective if the proof of Z was injective.*

The proof polynomial t in the Corollary above can always be taken so that it does not involve the operator $+$. The standard proof, by induction on derivation length, constructively produces such a polynomial. See [2] for details. I should note that $+$ plays no role in anything shown in this report.

3 Annotations and Realizations

In this section I introduce some simple machinery to keep track of modal operator *occurrences*. But first we need modal operators in the standard sense. Let $L_\Box$ be the usual language of propositional modal logic, built up from propositional letters using $\bot$, $\supset$, and $\Box$, with other connectives and $\Diamond$ taken as defined, in the usual way.

The LP Realization Theorem treats positive and negative occurrences of modal operators differently; negatives are replaced by proof variables while positives need not be. Further, different negative occurrences in a formula are replaced with distinct variables. Generally all this has been done somewhat informally, but machinery for it is straightforward. I introduce a language intermediate between $L_\Box$ and L_{LP}—though it is much closer to $L_\Box$. As will be seen, it amounts to syntactic, and not semantic, machinery.

Definition 3.1 The language $L_\Box^a$ and its features are introduced as follows.

1. Instead of a single modal operator $\Box$, there is an infinite family, $\Box_1$, $\Box_2$, ... These will be called *indexed* modal operators. Formulas of $L_\Box^a$ are built up as in $L_\Box$, but using indexed modal operators instead of $\Box$. Formulas of $L_\Box^a$ will generally be referred to as *annotated formulas*.

2. If X is an annotated formula, and X' is the result of replacing all indexed modal operators, $\Box_n$, with $\Box$, then X' is a formula of $L_\Box$. We say X is an *annotated version* of X', and X' is an *unannotated version* of X.

3. A *properly annotated formula* is an annotated formula meeting the conditions that: no indexed modal operator occurs twice; and if $\Box_n$ occurs in a negative position n is even, and if it occurs in a positive position n is odd.

Example 3.2 The example that starts here will be continued throughout the rest of the report. Here is an annotated formula.

$$\Box_2(\Box_1 U \supset \Box_4(\Box_3 P \supset \Box_6 V)) \supset \Box_5 W \tag{1}$$

Note that this is, in fact, properly annotated.

One can think of a properly annotated formula as a bookkeeping device to keep track of occurrences of modal operators and their polarities—negative occurrences are even, positive occurrences are odd. Properly annotated formulas play a fundamental role, but it is important to note that formulas that are annotated but not properly so also arise naturally. For instance, if X is properly annotated and Y is a subformula, it may not itself be properly annotated—it will not be if Y is a negative subformula of X because polarities have been reversed in passing from X to Y. Generally we will fix a properly annotated formula X, and work with subformulas of it, all of which are annotated, and properly so when considered as subformulas of X.

Semantically, annotations are simply ignored. That is, in an S4 model $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \Vdash \rangle$ we use the following rule of evaluation:

$$\mathcal{M}, \Gamma \Vdash \Box_n X \iff \mathcal{M}, \Delta \Vdash X \text{ for every } \Delta \in \mathcal{G} \text{ with } \Gamma \mathcal{R} \Delta$$

Then in a model, an annotated formula X and its unannotated version X' behave alike at each world. As I remarked earlier, annotations are for syntactical and not for semantical purposes.

Now that we have annotated formulas, realizations can be defined functionally in a natural way.

Definition 3.3 Realization functions and related notions are defined as follows.

1. A *realization function* is a mapping from positive integers to proof polynomials that maps even integers to LP variables. It is assumed that all realization functions behave the same on the even integers, specifically, if r is any realization function, $r(2n) = x_n$, where $x_1, x_2, \ldots$ is the list of proof variables arranged in a standardized order.

2. If X is a formula of $L_\Box^a$, an annotated formula, and r is a realization function, by $r(X)$ is meant the result of replacing each modal operator $\Box_i$ in X with the proof polynomial $r(i)$. The result, $r(X)$ is formula of LP.

3. Let X be an annotated formula. We say the realization function r is *non self-referential on variables in* X provided, for each subformula $\Box_{2n} Y$ of X the variable $r(2n) = x_n$ does not occur in $r(Y)$.

Example 3.4 Let r be a realization function such that the following holds, where f, g, h, and k are particular proof polynomials that need not be fully specified for present purposes, and the behavior of r on other inputs is not specified.

$$\begin{array}{rclcrcl} r(1) & = & g(x_2, x_3, x_5) & \quad & r(4) & = & x_2 \\ r(2) & = & x_1 & & r(5) & = & h(x_1, x_2, x_3) \\ r(3) & = & f(x_3) & & r(6) & = & x_3 \end{array} \tag{2}$$

Let $X(P)$ be formula (1) from Example 3.2 (later on P will play a special role, though it does not at the moment). Then we have the following. Note that r is non self-referential on variables in $X(P)$.

$$r(X(P)) = x_1{:}[g(x_2, x_3, x_5){:}U \supset x_2{:}(f(x_3){:}P \supset x_3{:}V)] \supset h(x_1, x_2, x_3){:}W \tag{3}$$

Finally, here is our official definition of a realization. In practice we will be working with realization functions that are non self-referential on variables, but this has not been built into the definition.

Definition 3.5 If X is a formula of $L_\Box$, a conventional modal formula, a *realization* of X is any formula of LP of the form $r(X')$ where r is a realization function and X' is any properly annotated version of X.

4 The Replacement Theorem

In $\mathsf{S4}$ (and in normal modal logics generally) one can prove a replacement result: If $A \equiv B$ is provable, and $X(B)$ is like $X(A)$ except that some subformula occurrences of A have been replaced with B, then $X(A) \equiv X(B)$ is also provable. Equivalence plays a central role here, and this has its problems for LP. If $A \equiv B$ is expanded into a formula in conjunctive normal form, one sees that A occurs both positively and negatively. Since positive and negative occurrences of modal operators play different roles when realized in LP, any LP analog of the replacement result in a form that uses equivalence should not be expected. There is, however, a version of replacement for normal modal logics that is less problematic. If $X(B)$ is like $X(A)$ except that some *positive* occurrences of A have been replaced with B, then if $A \supset B$ is provable so is $X(A) \supset X(B)$. Here is a formal statement of it, in a version that introduces notation that is useful for its proof.

Proposition 4.1 *Let $\varphi(P)$ be a formula of $L_\Box$ in which the propositional letter P has only positive occurrences. Let $\varphi(Z)$ be the result of replacing occurrences of P with occurrences of the $L_\Box$ formula Z. Then, if $A \supset B$ is provable in $\mathsf{S4}$, so is $\varphi(A) \supset \varphi(B)$.*

In this form, Replacement respects polarity of subformula occurrence. There is one more minor problem before we get to the serious ones for an LP analog. The Proposition allows for the replacement of several occurrences of A with occurrences of B. We will be interested in using properly annotated formulas. But if $\varphi(P)$ and A are both properly annotated, and A actually contains indexed modal operators, $\varphi(A)$ can never be properly annotated if P occurs more than once in $\varphi(P)$. Very simply, the requirement on proper annotations that no indexed modal operator occurs more than once would be violated in $\varphi(A)$. So we must restrict ourselves to the replacement of single occurrences of subformulas. Of course multiple replacements can be done sequentially.

Now we get to the serious matters. Proof polynomials represent reasons. If A is replaced with B inside a more complex LP formula, reasons for A must be adjusted to incorporate reasons for the passage from A to B, reasons for subformulas containing reasons for A need adjustment, and so on up. A version of Replacement for LP is not simple to formulate. In this section I do provide such a result, and prove it.

In order to state a version of Replacement for LP in a way that is not too complex to be comprehended, I will make use of annotated formulas and realization functions. After all, every LP formula with distinct variables in negative positions can be expressed as $r(X)$ for some realization function r and some properly annotated formula X. Indeed, if we drop the requirement that X be *properly* annotated, every LP formula is of the form $r(X)$ for suitable r and X.

There is one more piece of complexity that should be discussed before launching into the formal details. We care about *proper* annotation but, as noted earlier, subformulas of a properly annotated formula need not be properly annotated. In order to deal with this, we fix a formula X that is properly annotated, and work with subformulas of X which are properly annotated within X, but may not be when considered on their own.

In what follows, if $\varphi(P)$ is an annotated formula and P is a propositional letter, $\varphi(A)$ is the result of replacing all occurrences of P in $\varphi(P)$ with occurrences of the annotated formula A.

Definition 4.2 Let $X(P)$ be an annotated formula in which the propositional letter P has one positive occurrence, let A and B be annotated formulas, let r be a realization function, and let $\varphi(P)$ be a subformula of $X(P)$. For a realization function r_φ and a substitution σ_φ, we say $\langle r_\varphi, \sigma_\varphi\rangle$ *replaces* $r(A)$ *with* $r(B)$ *at* P *in* $\varphi(P)$ *within* $X(P)$ provided:

1. if $\varphi(P)$ is a positive subformula of $X(P)$ then $r(\varphi(A))\sigma_\varphi \supset r_\varphi(\varphi(B))$ has an injective LP proof;

2. if $\varphi(P)$ is a negative subformula of $X(P)$ then $r_\varphi(\varphi(B)) \supset r(\varphi(A))\sigma_\varphi$ has an injective LP proof;

3. $r(B) = r_\varphi(B)$

Theorem 4.3 (Replacement For LP) *Assume the following.*

1. *$X(P)$ is an annotated formula in which the propositional letter P has one positive occurrence, A and B are annotated formulas;*

2. *$X(B)$ is properly annotated;*

3. *r is a realization function that is non self-referential on variables in $X(A)$;*

4. *$r(A) \supset r(B)$ has an injective LP proof.*

Then for each subformula $\varphi(P)$ of $X(P)$ there is some $\langle r_\varphi, \sigma_\varphi\rangle$ that replaces $r(A)$ with $r(B)$ at P in $\varphi(P)$ within $X(P)$.

A few words before we start the proof. Loosely the theorem says that if we replace a positive occurrence of $r(A)$ in $r(\varphi(A))$ with an occurrence of $r(B)$, and if $r(A)$ implies $r(B)$, we get a provable implication, not between $r(\varphi(A))$ and $r(\varphi(B))$, but between formulas that are similar to these, but with adjusted proof polynomials. As will be seen, positive and negative proof polynomials are adjusted separately; the substitution σ_φ takes care of negative polynomial occurrences (proof variables) while the realization function r_φ takes care of positive polynomial occurrences.

Example 4.4 We continue Example 3.4. Suppose we take A to be $\Box_7 R$ and B to be $\Box_9\Box_{11}R$, so that we have the following.

$$A \supset B \quad \text{is} \quad \Box_7 R \supset \Box_9\Box_{11} R \tag{4}$$

Note that with $X(P)$ from (1) we have

$$X(A) \quad \text{is} \quad \Box_2(\Box_1 U \supset \Box_4(\Box_3\Box_7 R \supset \Box_6 V)) \supset \Box_5 W \tag{5}$$
$$X(B) \quad \text{is} \quad \Box_2(\Box_1 U \supset \Box_4(\Box_3\Box_9\Box_{11} R \supset \Box_6 V)) \supset \Box_5 W \tag{6}$$

and both are properly annotated. Also let us specify more of the realization function r that was partly given in (2).

$$\begin{aligned} r(7) &= k(x_3) \\ r(9) &= !k(x_3) \\ r(11) &= k(x_3) \end{aligned} \tag{7}$$

Then r is non self-referential on variables in $X(A)$, and we have the following.

$$r(X(A)) = x_1{:}[g(x_2, x_3, x_5){:}U \supset x_2{:}(f(x_3){:}k(x_3){:}R \supset x_3{:}V)] \supset h(x_1, x_2, x_3){:}W \tag{8}$$

Also $r(A) \supset r(B)$ is $k(x_3){:}R \supset !k(x_3){:}k(x_3){:}R$ and this has an injective LP proof.

The proof of Theorem 4.3 is lengthy and detailed, but it actually does something stronger than is stated: it provides an algorithm for the construction of the pair $\langle r_\varphi, \sigma_\varphi\rangle$. This algorithm is rather straightforward; the bulk of the proof is devoted to showing the correctness of the algorithm. It should be noted that the operations + and ! play no role here.

Proof Let $X(P)$ be a given formula, and assume conditions 1 – 4 hold. The result will be shown by an induction on the complexity of $\varphi(P)$, but actually something slightly stronger must be established, and for this we need some terminology. Let Z be an annotated formula; we say a substitution σ *lives on* Z provided the only variables that σ changes are x_i where $\Box_{2i}$ occurs in Z. Now, call a subformula $\varphi(P)$ of $X(P)$ *good* provided there is some $\langle r_\varphi, \sigma_\varphi\rangle$ that replaces $r(A)$ with $r(B)$ at P in $\varphi(P)$ within $X(P)$, and where σ_φ lives on $\varphi(P)$; we also say $\langle r_\varphi, \sigma_\varphi\rangle$ is a *witness* to the goodness of $\varphi(P)$. We will show every subformula of $X(P)$ is good.

Let $\varphi(P)$ be a subformula of $X(P)$, and suppose that all its proper subformulas are good—we show $\varphi(P)$ itself is good. There are several cases to consider.

Case: P does not occur in $\varphi(P)$, so that $\varphi(P) = \varphi(A) = \varphi(B)$. In this case we do not actually need the induction hypothesis. Set $r_\varphi = r$ and σ_φ to be the identity substitution, which lives on *every* formula. Then both $[r(\varphi(A))]\sigma_\varphi \supset r_\varphi(\varphi(B))$ and $r_\varphi(\varphi(B)) \supset [r(\varphi(A))]\sigma_\varphi$ are simply $r(\varphi(P)) \supset r(\varphi(P))$, which certainly has an injective LP proof. And $r_\varphi(B) = r(B)$ by definition. So $\langle r_\varphi, \sigma_\varphi\rangle$ is a witness to the goodness of $\varphi(P)$.

Case: $\varphi(P)$ is atomic and P occurs. Then $\varphi(P)$ is just P, and must be a positive subformula of $X(P)$, since the only occurrence of P is positive. Again set $r_\varphi = r$ and σ_φ to be the identity substitution, which lives on every formula. We have $r_\varphi(B) = r(B)$ by definition, again. We also need the injective provability of $[r(\varphi(A))]\sigma_\varphi \supset r_\varphi(\varphi(B))$. But this is just $r(A) \supset r(B)$, and this has an injective proof, by hypothesis. So, $\langle r_\varphi, \sigma_\varphi\rangle$ is a witness to the goodness of $\varphi(P)$ in this case. Again the induction hypothesis is not used.

Case: $\varphi(P)$ is $\Box_i\theta(P)$, this is a positive subformula of $X(P)$, and P occurs. By hypothesis $\theta(P)$ is good, say $\langle r_\theta, \sigma_\theta\rangle$ is a witness to its goodness. In particular, $r(\theta(A))\sigma_\theta \supset r_\theta(\theta(B))$ has an injective proof.

By the Lifting Lemma, for some ground proof polynomial u, $u{:}[r(\theta(A))\sigma_\theta \supset r_\theta(\theta(B))]$ has an injective proof. To keep notation somewhat under control, say $r(i)$ is t. Then, using the LP Application Axiom, the following has an injective proof: $(t\sigma_\theta){:}[r(\theta(A))\sigma_\theta] \supset (u\cdot t\sigma_\theta){:}r_\theta(\theta(B))$. Now let r_φ be like r_θ except that $r_\varphi(i) = u \cdot t\sigma_\theta$. Let $\sigma_\varphi = \sigma_\theta$. We claim that $\langle r_\varphi, \sigma_\varphi\rangle$ is a witness to the goodness of $\Box_i\theta(P)$.

In verifying our claim we need to show the injective provability of $r(\Box_i\theta(A))\sigma_\varphi \supset r_\varphi(\Box_i(\theta(B))$. Since $r(i)\sigma_\varphi = t\sigma_\varphi = t\sigma_\theta$, equivalently, this is $(t\sigma_\theta){:}r(\theta(A))\sigma_\theta \supset r_\varphi(i){:}r_\varphi(\theta(B))$, which is $(t\sigma_\theta){:}r(\theta(A))\sigma_\theta \supset (u \cdot t\sigma_\theta){:}r_\varphi(\theta(B))$. But this is $(t\sigma_\theta){:}r(\theta(A))\sigma_\theta \supset (u \cdot t\sigma_\theta){:}r_\theta(\theta(B))$, since $X(B)$ is *properly* annotated so $\Box_i$ cannot occur in $\theta(B)$ and hence r_θ and r_φ agree on $\theta(B)$.

We need that $r_\varphi(B) = r(B)$. We have that $r_\theta(B) = r(B)$ since $\langle r_\theta, \sigma_\theta\rangle$ witnesses the goodness of $\theta(P)$. But B is a subformula of $\theta(B)$, and not vacuously, since P occurs in $\Box_i\theta(P)$. Since r_θ and r_φ agree on $\theta(B)$, they must agree on B.

Finally σ_θ lives on $\theta(P)$, so of course it lives on $\Box_i\theta(P)$, and $\sigma_\varphi = \sigma_\theta$. This completes verification that $\langle r_\varphi, \sigma_\varphi\rangle$ witnesses the goodness of $\Box_i\theta(P)$.

Case: $\varphi(P)$ is $\Box_i\theta(P)$, this is a negative subformula of $X(P)$, and P occurs. In this case i is even, say it is $2j$. By hypothesis, $\theta(P)$ is good, say $\langle r_\theta, \sigma_\theta\rangle$ is a witness. Then $r_\theta(\theta(B)) \supset r(\theta(A))\sigma_\theta$ has an injective proof.

As in the previous case, by the Lifting Lemma there is a ground proof polynomial u such that $u{:}[r_\theta(\theta(B)) \supset r(\theta(A))\sigma_\theta]$ has an injective proof. Then by the LP Application Axiom, there is an injective proof of $x_j{:}r_\theta(\theta(B)) \supset (u \cdot x_j){:}r(\theta(A))\sigma_\theta$. Let σ_φ be like σ_θ except that $\sigma_\varphi(x_j) = u \cdot x_j$. Let $r_\varphi = r_\theta$. We claim that $\langle r_\varphi, \sigma_\varphi\rangle$ is a witness to the goodness of $\Box_i\theta(P)$, that is, of $\Box_{2j}\theta(P)$.

Of course $r_\varphi(B) = r(B)$ since $r_\varphi = r_\theta$ and $\langle r_\theta, \sigma_\theta\rangle$ witnesses the goodness of $\theta(P)$. We need to show the injective provability of $r_\varphi(\Box_i\theta(B)) \supset r(\Box_i\theta(A))\sigma_\varphi$. Equivalently, this is $x_j{:}r_\varphi(\theta(B)) \supset (x_j\sigma_\varphi){:}r(\theta(A))\sigma_\varphi$ (recall, all realization functions agree on the even indexes). And this is just $x_j{:}r_\theta(\theta(B)) \supset (u\cdot x_j){:}r(\theta(A))\sigma_\varphi$, so we are finished if we have that $r(\theta(A))\sigma_\varphi = r(\theta(A))\sigma_\theta$. But we do have this, because r is non self-referential on variables in $X(A)$, $\Box_{2j}\theta(A)$ is a subformula, hence x_j cannot occur in $r(\theta(A))$, and so σ_θ and σ_φ agree on $r(\theta(A))$.

Finally, σ_θ lives on $\theta(P)$. The substitution σ_φ is like σ_θ except that it changes x_j. But then σ_φ lives on $\Box_{2j}\theta(P)$. This finishes verification that $\langle r_\varphi, \sigma_\varphi\rangle$ witnesses the goodness of $\Box_{2j}\theta(P)$.

Case: $\varphi(P)$ is an implication, and this is a subformula of $X(P)$ in which P occurs. Since there is at most one occurrence of P in $X(P)$ it must be in the antecedent or in the consequent of the implication. Let us write $\theta(P)$ for whichever it is of antecedent or consequent that contains the occurrence of P, and η for the other. Then there are four cases to consider depending on whether $\varphi(P)$ is $\theta(P) \supset \eta$ or $\eta \supset \theta(P)$, and whether $\varphi(P)$ is a positive or a negative subformula of $X(P)$. The construction is the same in all four cases, though the justification differs a bit. I'll begin with what is common.

By hypothesis, $\theta(P)$ is good. Assume $\langle r_\theta, \sigma_\theta\rangle$ is a witness to the goodness of $\theta(P)$. Define a function r_φ by setting $r_\varphi(i) = r(i)\sigma_\theta$ if $\Box_i$ occurs in η, and $r_\varphi(i) = r_\theta(i)$ otherwise. Set $\sigma_\varphi = \sigma_\theta$. We claim $\langle r_\varphi, \sigma_\varphi\rangle$ witnesses the goodness of $\varphi(P)$.

It must be checked that r_φ is actually a realization function, $r_\varphi(2i) = x_i$ for all i. Since r_θ is a realization function, $r_\theta(2i) = x_i$ so the only part that needs verification is where $\Box_{2i}$ occurs in η. Since $\langle r_\theta, \sigma_\theta\rangle$ is a witness to the goodness of $\theta(P)$, σ_θ lives on $\theta(P)$, and hence must be the identity on x_i such that $\Box_{2i}$ does not occur in $\theta(P)$. Then, if $\Box_{2i}$ occurs in η it cannot occur in $\theta(P)$, since $X(P)$ is properly annotated, so in this case we have $r_\varphi(2i) = r(2i)\sigma_\theta = x_i\sigma_\theta = x_i$.

$X(B)$ is properly annotated, $\theta(B)$ and η are distinct subformulas, and B actually occurs as a subformula of $\theta(B)$ since P has an occurrence in $\theta(P)$. Then no index in B can occur in η, so $r_\varphi(B) = r_\theta(B)$. And $r_\theta(B) = r(B)$ since $\langle r_\theta, \sigma_\theta\rangle$ witnesses the goodness of $\theta(P)$, so $r_\varphi(B) = r(B)$.

Finally the argument divides into the four cases mentioned above. Let us consider the case where $\varphi(P)$ is a positive subformula of $X(P)$ of the form $\theta(P) \supset \eta$; the other three cases are similar and are omitted. In the case being considered, we need to show the injective provability of $r(\varphi(A))\sigma_\varphi \supset r_\varphi(\varphi(B))$, that is, of $[r(\theta(A) \supset \eta)\sigma_\theta] \supset [r_\varphi(\theta(B) \supset \eta)]$. Since $\theta(P)$ is a negative subformula of $X(P)$, $r_\theta(\theta(B)) \supset r(\theta(A))\sigma_\theta$ has an injective proof. Now,

$$\begin{aligned} r(\theta(A) \supset \eta)\sigma_\theta &= r(\theta(A))\sigma_\theta \supset r(\eta)\sigma_\theta & (9)\\ &= r(\theta(A))\sigma_\theta \supset r_\varphi(\eta) & (10)\end{aligned}$$

and

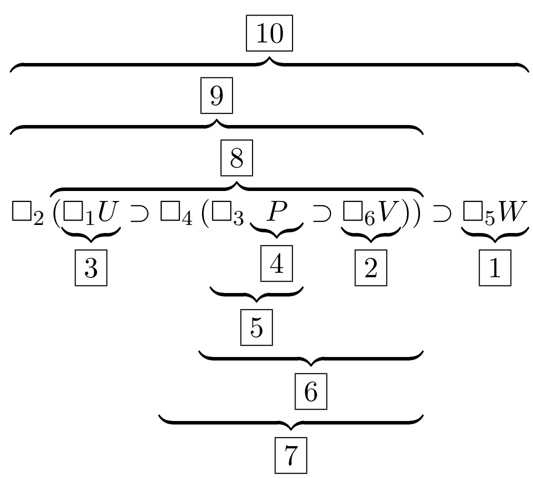
$$\begin{aligned} r_\varphi(\theta(B) \supset \eta) &= r_\varphi(\theta(B)) \supset r_\varphi(\eta) & (11)\\ &= r_\theta(\theta(B)) \supset r_\varphi(\eta) & (12)\end{aligned}$$

The result now follows from (10) and (12) because we have the injective provability of $r_\theta(\theta(B)) \supset r(\theta(A))\sigma_\theta$.

We have established that $\langle r_\varphi, \sigma_\varphi\rangle$ witnesses the goodness of $\varphi(P)$ in this case.

■

Example 4.5 We continue Example 4.4 and work with formula $X(P)$ from (1). It is $\Box_2(\Box_1 U \supset \Box_4(\Box_3 P \supset \Box_6 V)) \supset \Box_5 W$. It will be useful to introduce numbers to designate subformulas, which we do in the following.



As in (4), take $A \supset B$ to be $\Box_7 R \supset \Box_9\Box_{11} R$, and take r as given in (2) and (7). We follow the algorithm specified in the proof above, to compute $\langle r_\varphi, \sigma_\varphi\rangle$ for each subformula φ of $X(P)$.

[1], [2], [3] If i is any of 1, 2, or 3, $r_i = r$ and σ_i is the identity substitution, because P does not occur.

$\boxed{4}$ In this case too we have $r_4 = r$ and σ_4 is the identity substitution.

$\boxed{5}$ This is $\Box_3\boxed{4}$ and is a positive subformula. There is a proof polynomial c with no variables such that $c{:}[r(\boxed{4}(A))\sigma_4 \supset r_4(\boxed{4}(B))]$ has an injective proof. That is, $c{:}[r(A) \supset r(B)]$, or $k(x_3){:}R \supset !k(x_3){:}k(x_3){:}R$, has an injective proof. Then, set r_5 to be like r_4 except that $r_5(3) = [c \cdot r(3)]\sigma_4 = c \cdot f(x_3)$. Also $\sigma_5 = \sigma_4$ and so is the identity.

$\boxed{6}$ This is $\boxed{5} \supset \boxed{2}$. Take r_6 to be the same as r_5 except that $r_6(6) = r(6)\sigma_5 = x_3\sigma_5 = x_3$. Also $\sigma_6 = \sigma_5$ is the identity.

$\boxed{7}$ This is $\Box_4\boxed{6}$ and is a negative subformula. There is a variable free proof polynomial d such that $d{:}[r_6(\boxed{6}(B)) \supset r(\boxed{6}(A))\sigma_6]$ has an injective proof. Then σ_7 is like σ_6 except that $\sigma_7(x_2) = d \cdot x_2$, and $r_7 = r_6$.

$\boxed{8}$ This is $\boxed{3} \supset \boxed{7}$, where the consequent has the occurrence of P. Set r_8 to be the same as r_7 except that $r_8(1) = r(1)\sigma_7 = g(x_2, x_3, x_5)\sigma_7 = g(d \cdot x_2, x_3, x_5)$, and set $\sigma_8 = \sigma_7$.

$\boxed{9}$ This is $\Box_2\boxed{8}$ and is a negative subformula. There is a ground proof polynomial e such that $e{:}[r_8(\boxed{8}(B)) \supset r(\boxed{8}(A))\sigma_8]$ has an injective proof. Set σ_9 to be like σ_8 except that $\sigma_9(x_1) = e \cdot x_1$, and set $r_9 = r_8$.

$\boxed{10}$ This is $\boxed{9} \supset \boxed{1}$, where $\boxed{9}$ has the occurrence of P. Set r_{10} to be the same as r_9 except that $r_{10}(5) = r(5)\sigma_9 = h(x_1, x_2, x_3)\sigma_9 = h(e \cdot x_1, d \cdot x_2, x_3)$, and set $\sigma_{10} = \sigma_9$.

With all this put together, we have the following.

$$\begin{array}{lcllcl} r_{10}(1) & = & g(d \cdot x_2, x_3, x_5) & r_{10}(6) & = & x_3 \\ r_{10}(2) & = & e \cdot x_1 & r_{10}(7) & = & k(x_3) \\ r_{10}(3) & = & c \cdot f(x_3) & r_{10}(9) & = & !k(x_3) \\ r_{10}(4) & = & x_2 & r_{10}(11) & = & k(x_3) \\ r_{10}(5) & = & h(e \cdot x_1, d \cdot x_2, x_3) & & & \end{array} \tag{13}$$

And σ_{10} is the identity substitution except that $\sigma_{10}(x_1) = e \cdot x_1$ and $\sigma_{10}(x_2) = d \cdot x_2$. The formula $r(X(A))\sigma_{10}$ is

$$x_1{:}(g(d \cdot x_2, x_3, x_5){:}U \supset (d \cdot x_2){:}(f(x_3){:}k(x_3){:}R \supset x_3{:}V)) \supset h(e \cdot x_1, d \cdot x_2, x_3){:}W$$

and $r_{10}(X(B))$ is

$$x_1{:}(g(d \cdot x_2, x_3, x_5){:}U \supset x_2{:}((c \cdot f(x_3)){!}k(x_3){:}k(x_3){:}R \supset x_3{:}V)) \supset h(e \cdot x_1, d \cdot x_2, x_3){:}W$$

and I leave it to you to verify that there is an injective proof of $r(X(A))\sigma_{10} \supset r_{10}(X(B))$.

5 A Strengthened Version

The Replacement Theorem for LP asserts the existence of an $\langle r_\varphi, \sigma_\varphi \rangle$ for each subformula φ of $X(P)$ when appropriate conditions are met. As noted earlier, a stronger result has been shown—an algorithm for constructing $\langle r_\varphi, \sigma_\varphi \rangle$ has been given. The proof really amounts to stating this algorithm and showing its correctness. In fact, the proof actually shows a still stronger result. I did not give the strengthened form because doing so requires keeping track of many details, and I thought it better for the reader to see the basic structure in a clear way first. With that accomplished, here is the stronger version. I would say that part 1 is the most significant. The proof of Theorem 4.3 gives, for each subformula $\varphi(P)$ of $X(P)$, a pair $\langle r_\varphi, \sigma_\varphi \rangle$ that carries out a replacement for that subformula. Part 1 below says this can be done uniformly, for all subformulas.

Corollary 5.1 (Replacement For LP, Strong Form) *Let $X(P)$, A, B, and r meet conditions 1 – 4 of Theorem 4.3. Then the algorithm described in the proof produces an $\langle r_X, \sigma_X \rangle$ that replaces $r(A)$ with $r(B)$ at P in $X(P)$ within $X(P)$, that is, this replacement applies to the entire of $X(P)$. For this $\langle r_X, \sigma_X \rangle$ we have the following properties.*

1. *For each subformula $\varphi(P)$ of $X(P)$, $\langle r_X, \sigma_X \rangle$ replaces $r(A)$ with $r(B)$ at P in $\varphi(P)$ within $X(P)$ (call this* hereditary replacement*).*
2. *σ_X meets the condition that, for each variable x the proof polynomial $x\sigma_X$ contains at most x as a variable (call this the* no new variable condition*).*
3. *If r is non self-referential on variables in $X(B)$ then so is r_X.*
4. *If W is a subformula of $X(P)$ that does not contain the occurrence of P, then $r_X(W) = r(W)\sigma_X$.*
5. *If $\Box_{2i}$ occurs in a subformula of $X(P)$ that does not contain the occurrence of P, then $x_i\sigma_X = x_i$.*

Proof We show these items one at a time, by establishing that the proof of Theorem 4.3 already proves them. In that proof, for each subformula $\varphi(P)$ of $X(P)$, a witness to its goodness is constructed—I will continue to denote the witness constructed for $\varphi(P)$ by $\langle r_\varphi, \sigma_\varphi \rangle$.

1. We analyze each of the cases of the proof of Theorem 4.3 and show that for each subformula $\varphi(P)$ of $X(P)$, $\langle r_\varphi, \sigma_\varphi \rangle$ not only is a witness to the goodness of $\varphi(P)$, but to the goodness of all its subformulas as well. We refer to this property as being an *hereditary* witness. The case where $\varphi(P) = X(P)$ establishes the stated result.

   Suppose P does not occur in $\varphi(P)$. In this case $\langle r_\varphi, \sigma_\varphi \rangle$ is defined in a way that is independent of φ, and so is a witness to the goodness of *every* subformula of $X(P)$ not containing P and this includes the subformulas of $\varphi(P)$.

   If $\varphi(P)$ is P, there are no proper subformulas, so this case is trivial.

   Suppose $\varphi(P)$ is $\Box_i\theta(P)$, where this is positive in $X(P)$ and P occurs. In the proof algorithm, r_φ differs from r_θ only on the index i, and $\Box_i$ does not occur in $\theta(B)$, hence r_φ and r_θ agree on $\theta(B)$. Also σ_φ and σ_θ are the same, and so if $\langle r_\theta, \sigma_\theta \rangle$ is an hereditary witness to the goodness of $\theta(P)$, $\langle r_\varphi, \sigma_\varphi \rangle$ must be an hereditary witness to the goodness of $\varphi(P) = \Box_i\theta(P)$.

   Suppose $\varphi(P)$ is $\Box_{2j}\theta(P)$, where this is negative in $X(P)$ and P occurs. Then σ_φ differs from σ_θ only on x_j, and x_j does not occur in $r(\theta(A))$ because r is non self-referential on variables in $X(A)$, hence σ_φ and σ_θ agree on $r(\theta(A)$. Also $r_\varphi = r_\theta$. Then if $\langle r_\theta, \sigma_\theta \rangle$ is an hereditary witness to the goodness of $\theta(P)$ in this case, $\langle r_\varphi, \sigma_\varphi \rangle$ will be an hereditary witness to the goodness of $\Box_{2j}\theta$.

   Finally suppose $\varphi(P)$ is an implication, and P occurs. I will only consider the case where $\varphi(P)$ occurs positively in $X(P)$, and is of the form $\theta(P) \supset \eta$, where P occurs in $\theta(P)$ but not in η. According to the implication case construction, r_φ agrees with r_θ everywhere except on η. Also $\sigma_\varphi = \sigma_\theta$. Then if $\langle r_\theta, \sigma_\theta \rangle$ is an hereditary witness to the goodness of $\theta(P)$, so is

$\langle r_\varphi, \sigma_\varphi\rangle$. $\langle r_\varphi, \sigma_\varphi\rangle$ is a witness to the goodness of $\varphi(P)$; it must still be shown that $\langle r_\varphi, \sigma_\varphi\rangle$ is an hereditary witness to the goodness of η. Recall that if $\Box_i$ occurs in η then $r_\varphi(i) = r(i)\sigma_\theta$. Now let W be a subformula of η—say it is a positive subformula of $X(P)$, the case where it is negative is similar. We need to establish the injective provability of $r(W)\sigma_\varphi \supset r_\varphi(W)$. But $r(W)\sigma_\varphi = r(W)\sigma_\theta$ by definition of σ_φ. And $r_\varphi(W) = r(W)\sigma_\theta$ by definition of r_φ, so we need the injective provability of $r(W)\sigma_\theta \supset r(W)\sigma_\theta$, and this is obvious.

2. We show that for each subformula $\varphi(P)$ of $X(P)$, σ_φ meets the no new variable condition, again by considering cases in the proof of Theorem 4.3.

   If $\varphi(P)$ does not contain P, or if $\varphi(P)$ is P itself, the result is immediate since in these cases σ_φ is the identity substitution.

   Suppose $\varphi(P)$ is $\Box_i\theta(P)$ and the result is known for $\theta(P)$. If $\varphi(P)$ is a positive subformula of $X(P)$ then σ_φ is the same as σ_θ and we are done. If $\varphi(P)$ is a negative subformula then σ_φ is like σ_θ except that for $j = i/2$ we have $\sigma_\varphi(x_j) = u \cdot x_j$, where u contains no variables. Then obviously σ_φ again meets the no new variable condition.

   Suppose, finally, that $\varphi(P)$ is $\theta(P) \supset \eta$, a positive subformula of $X(P)$, and the result is known for $\theta(P)$. The other implication cases are similar, and are omitted. In this case σ_φ is just σ_θ, and we are done.

3. Assume r is non self-referential on variables in $X(B)$. We show that for each subformula $\varphi(P)$ of $X(P)$, r_φ is non self-referential on variables in $X(B)$ (note that the assumption concerns $X(B)$ and not $\varphi(B)$). Of course this involves checking each case in the proof of Theorem 4.3.

   Suppose P does not occur in $\varphi(P)$, or $\varphi(P)$ is P itself. In both of these cases, $r_\varphi = r$ so we simply appeal to the assumption that r is non self-referential on variables in $X(B)$.

   Suppose $\varphi(P)$ is $\Box_i\theta(P)$, P occurs, and the result is known for $\theta(P)$. If $\varphi(P)$ is a negative subformula of $X(P)$ then $r_\varphi = r_\theta$ and we are done. Now suppose $\varphi(P)$ is a positive subformula of $X(P)$. Then r_φ is the same as r_θ except on i, so if r_φ failed to be non self-referential on variables in $X(B)$ it must be that $\Box_i\theta(B)$ is a subformula of some $\Box_{2n}Z(B)$ in $X(B)$, and the variable x_n occurs in $r_\varphi(i)$. But $r_\varphi(i) = u \cdot (r(i)\sigma_\theta)$, where u has no variables. Since σ_θ meets the no new variable condition, $r(i)\sigma_\theta$ has the same variables as $r(i)$. But this violates the condition that r is non self-referential on variables in $X(B)$.

   Finally suppose $\varphi(P)$ is $\theta(P) \supset \eta$ where P occurs in $\theta(P)$, and the result is known for $\theta(P)$, that is, r_θ is non self-referential on variables in $X(B)$. As usual, the other implication cases are similar and are omitted. In this case $r_\varphi(i) = r(i)\sigma_\theta$ if $\Box_i$ occurs in η, and otherwise r_φ agrees with r_θ. We derive a contradiction from the assumption that r_φ fails to be non self-referential on variables in $X(B)$. So, suppose $\Box_{2i}W$ is a subformula of $X(B)$ and x_i occurs in $r_\varphi(W)$. Then x_i occurs in $r_\varphi(j)$ for some $\Box_j$ in W. Now either $\Box_j$ is not part of η or it is. If it is not part of η, $r_\varphi(j) = r_\theta(j)$, and the assumption that r_θ is non self-referential on variables in $X(B)$ is violated. If $\Box_j$ is part of η then $r_\varphi(j) = r(j)\sigma_\theta$. If x_i occurs in this, it must also occur in $r(j)$ since σ_θ meets the no new variable condition. But this violates the assumption that r is non self-referential on variables in $X(B)$.

4. and 5. These items are shown simultaneously. Let W be a subformula of $X(P)$ that does not contain P. We show by an analysis of the cases in the proof of Theorem 4.3 that for each subformula $\varphi(P)$ of $X(P)$ with W as a subformula, and for the corresponding $\langle r_\varphi, \sigma_\varphi\rangle$, $r_\varphi(W) = r(W)\sigma_\varphi$ and if $\Box_{2i}$ occurs in W then $x_i\sigma_\varphi = x_i$. Then the results stated in the Theorem are the special case where $\varphi(P)$ is $X(P)$.

First consider the case where P does not occur in $\varphi(P)$. Then σ_φ is the identity substitution, and $r_\varphi = r$. Then of course $r_\varphi(W) = r(W)\sigma_\varphi$, and $x_i\sigma_\varphi = x_i$ whether or not $\Box_{2i}$ is in W.

For the remaining cases, assume P occurs in $\varphi(P)$.

If $\varphi(P)$ is P, there is no subformula W not containing P.

Suppose $\varphi(P)$ is $\Box_i\theta(P)$, a positive subformula of $X(P)$. In this case, r_φ agrees with r_θ except on i, and $\sigma_\varphi = \sigma_\theta$. Suppose also that the result is known for $\theta(P)$. Since W is a subformula of $\varphi(P)$ not containing P, while $\varphi(P)$ does contain P, W must be a proper subformula, and hence a subformula of $\theta(P)$. In particular, W does not contain $\Box_i$. Then $r_\varphi(W) = r(W)\sigma_\varphi$ since $r_\theta(W) = r(W)\sigma_\theta$. And if $\Box_{2k}$ occurs in W, $x_k\sigma_\varphi = x_k$, because $x_k\sigma_\theta = x_k$.

Suppose $\varphi(P)$ is $\Box_{2j}\theta(P)$, a negative subformula of $X(P)$. In this case $r_\varphi = r_\theta$, and σ_φ agrees with σ_θ except on x_j. And suppose the result is known for $\theta(P)$. Again since W does not contain P but is a subformula of $\varphi(P)$ which does contain P, it must be a proper subformula, and hence a subformula of $\theta(P)$. Then $r_\theta(W) = r(W)\sigma_\theta$. Since r is non self-referential on variables in $X(A)$, x_j cannot occur in $r(W)$, and so $r_\varphi(W) = r(W)\sigma_\varphi$. Also if $\Box_{2k}$ occurs in W, since $X(B)$ is properly annotated, $k \neq j$, so $x_k\sigma_\varphi = x_k\sigma_\theta = x_k$.

Finally suppose $\varphi(P)$ is an implication. As usual we only consider the case where $\varphi(P)$ is $\theta(P) \supset \eta$, P occurs in $\theta(P)$ but not in η, and this is a positive subformula of $X(P)$. And we suppose the result is known for $\theta(P)$ and for η. The definition of $\langle r_\varphi, \sigma_\varphi\rangle$ in the present case is as follows. If $\Box_i$ occurs in η then $r_\varphi(i) = r(i)\sigma_\theta$ and $r_\varphi(i) = r_\theta(i)$ otherwise. And $\sigma_\varphi = \sigma_\theta$.

Since W is a subformula that does not contain P, while $\varphi(P)$ does contain P, W must be a proper subformula, and hence is either a subformula of $\theta(P)$ or of η. If W is a subformula of $\theta(P)$ then since $X(P)$ is properly annotated, $r_\varphi(W) = r_\theta(W) = r(W)\sigma_\theta = r(W)\sigma_\varphi$, using the fact that the result is known for $\theta(P)$. And if W is a subformula of η then $r_\varphi(W) = r(W)\sigma_\theta = r(W)\sigma_\varphi$, by definition of r_φ. Finally, if $\Box_{2i}$ occurs in W, then since the result is known for both $\theta(P)$ and η, then $x_i\sigma_\varphi = x_i\sigma_\theta = x_i$.

■

Example 5.2 I leave it to you to check that the replacement r_{10} and the substitution σ_{10} constructed in Example 4.5 do meet the conditions given in this theorem.

References

[1] S. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, December 1995.

[2] S. Artemov. Explicit provability and constructive semantics. *The Bulletin for Symbolic Logic*, 7(1):1–36, 2001. `http://www.cs.gc.cuny.edu/~sartemov/publications/BSL.ps`.

[3] M. C. Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132:1–25, 2005.

[4] K. Gödel. Eine Interpretation des intuitionistischen Aussagenkalküls. *Ergebnisse eines mathematischen Kolloquiums*, 4:39–40, 1933. English translation in [**?**].

[5] R. Kuznets. On self-referentiality in modal logic. 2005.