The Realization Theorem for S5
A Simple, Constructive Proof

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

January 10, 2008

Abstract

Justification logics are logics of knowledge in which explicit reasons are formally represented. Standard logics of knowledge have justification logic analogs. Connecting justification logics and logics of knowledge are Realization Theorems. In this paper we give a new, constructive proof of the Realization Theorem connecting S5 and its justification analog, JS5. This proof is, I believe, the simplest in the literature.

1 Introduction

Ten years ago I wrote a paper in honor of Rohit Parikh's 60^{th} birthday, [5]. Now I am honored to write another for his 70^{th}. In this paper I will make use of my paper from 10 years ago, to help provide a simple, constructive proof of the Realization Theorem for the modal logic S5. The Realization Theorem is a fundamental result in a developing area known as *justification logics*. Since these are not (yet) standard in the way that modal logics are, I will begin by sketching what justification logics are, saying why they are significant, and saying what the Realization Theorem is about. Then we can get to the more technical material, which essentially amounts to combining work from two of my earlier papers, [5] and [7].

2 Justification Logics

Modal logics are familiar things and, just as Hintikka told us, many of them can be interpreted naturally as logics of knowledge—one reads $\Box X$ as "X is known." Thus we want $\Box(X \supset Y) \supset (\Box X \supset \Box Y)$ so that we can draw conclusions from our knowledge, and we want $\Box X \supset X$ to guarantee that what we know is so. This much gives us the logic T. Or we might want to drop the latter condition and study belief instead of knowledge—the modal logic K. Then again, we might add *positive introspection*, $\Box X \supset \Box\Box X$, getting S4, or also *negative introspection*, $\neg\Box X \supset \Box\neg\Box X$, getting S5. But while this approach to (monomodal) logics of knowledge has served well these many years, logics of knowledge are somewhat blunt instruments. Typically we don't just know something, but we know it for a reason—*justifications* are involved. We can think of $\Box$ as a kind of existential quantifier, $\Box X$ says that there exists a justification for X, but the justification itself has been abstracted away.

Justification logics are modal-like logics, having a small calculus of explicit justifications as a formal part of the machinery. *Justification terms* are built up from constants and variables using certain operations. For variables we'll use x, y, x_1, x_2, ... Think of these informally as standing for information from the 'real' world, justifying knowledge we have acquired about things and events, which the logic does not further analyze. There are also basic logical truths—classical tautologies for instance—which we simply accept. We use constants to represent justifications for them, c, d, c_1, c_2, ... Here considerable flexibility is possible. We might want a single justification constant for all tautologies, or for tautology schemes, or for individual tautologies. The setup allows for all these possibilities and more.

Then we have the operation symbols. Two are standard in this area. First, we have the binary symbol $\cdot$ of *application*. The idea is that if term t justifies $X \supset Y$ and term u justifies X then $t \cdot u$ is a justification of Y. Second, we have the binary symbol $+$, representing a kind of weakening or monotonicity. The idea is that $t + u$ justifies anything that t justifies, and also anything that u justifies. We could assume $+$ is commutative, or associative, these would be reasonable assumptions, but we will not make them. We keep things as general as possible.

Finally we have operations corresponding to positive and to negative introspection, ! and ?. If t justifies X, $!t$ should justify the fact that t justifies X. And if t does not justify X, $?t$ should justify the fact that t does not justify X.

The notation that is standard here is, $t{:}X$ is a formula if t is a justification term and X is a formula, and is intended to be read "t justifies X." Here are axiomatic formulations of basic justification logics, corresponding to the modal logics mentioned above.

Axiom Schemes

1. tautologies (or enough of them)
2. $t{:}(X \supset Y) \supset (u{:}X \supset (t \cdot u){:}Y)$
3. $t{:}X \supset (t + u){:}X$ and $u{:}X \supset (t + u){:}X$
4. $t{:}X \supset X$
5. $t{:}X \supset !t{:}t{:}X$
6. $\neg t{:}X \supset ?t{:}\neg t{:}X$

Rules of Inference

1. Modus ponens, $X, X \supset Y \vdash Y$
2. Axiom necessitation, if X is an axiom and c is a constant, $\vdash c{:}X$

A *constant specification* is an assignment of axioms to constants. Each proof using the axiom system above, or a subset of it, generates a constant specification—just see what use we made of Axiom necessitation in the course of the proof. Alternately we could start with a constant specification and require that all applications of the Axiom necessitation rule be in accordance with it. Various special conditions can be put on constant specifications, but the only one we are interested in here is *injectivity.* A constant specification is *injective* if at most one axiom is associated with each constant.

The idea of justification logics, and the oldest of them, are due to Artemov [1]. The first of them was called LP, standing for *logic of proofs.* His axiomatization uses the system above without axiom 6. It was referred to as a logic of proofs because justification terms in it could be understood as representing explicit proofs in a logical system, and interpreted arithmetically as such in formal arithmetic. This made it possible to provide a constructive, arithmetic semantics for intuitionistic logic, completing a program begun by Gödel, [11]. That LP can be embedded into formal arithmetic is Artemov's *Arithmetic Completeness Theorem*, which will not concern us here.

If we take any formula of a justification logic and replace every justification term with $\Box$, we get a standard modal formula. This is called the *forgetful functor*. It is a simple matter to check that the forgetful functor turns each axiom of LP into an axiom of S4, and turns every rule application of LP into a rule application of S4. It follows that the forgetful functor turns every theorem of LP into a theorem of S4. Much more difficult to prove is that the converse also holds. Every theorem of S4 is the result of applying the forgetful functor to some theorem of LP. Actually, this holds in a stronger form, which we now state formally. Like the Arithmetic Completeness Theorem, it too is due to Artemov, [1].

Theorem 2.1 (Realization for S4) *Let X be a theorem of S4. Then there is some way of replacing $\Box$ operators of X with justification terms, with negative occurrences being replaced with distinct variables, and positive occurrences by terms that may involve those variables, so that the result is a theorem of LP, provable using an injective constant specification.*

The Realization Theorem plays a key role in Artemov's fulfillment of Gödel's program. Intuitionistic logic embeds in S4 via the well-known mapping that inserts $\Box$ before every subformula. Then S4 embeds in LP; the Realization Theorem is needed here. Finally, LP embeds in formal arithmetic, using the Artemov Arithmetic Completeness Theorem. But of all this, here we are only concerned with the forgetful functor and the Realization Theorem, telling us that LP serves as an explicit version of S4. The Realization Theorem, in effect, Skolemizes the existential quantifiers that are tacit in $\Box$, providing us with an analysis of the reasoning behind the validities of the logic of knowledge S4.

The logic LP can be weakened by omitting positive introspection, axiom 5 (and also modifying the Axiom Necessitation Rule, but we omit details here). Further we can create an analog of a logic of belief, by omitting axiom 4. Today these logics are known as JT and JK. Presumably LP could also be known as JS4, but the original name has been retained for historical reasons. JT and JK also have their Realization Theorems connecting them with T and K, as was also established by Artemov. The proof basically amounts to omitting parts of the full S4/LP proof. By now there are several algorithmic proofs of Realization, [1, 3, 9], and a semantic proof as well, [6].

If we have the full axiom set above, including negative introspection, axiom 6, we have a justification logic known as JS5. There is a Realization Theorem connecting it with the modal logic S5, but now the proof is more than a straightforward modification of Artemov's version for S4. The result has been established using a semantic argument, in [13], with a constructive proof in [2]. It is our intention here to give a simpler constructive argument.

To conclude this section we give a few basic results concerning justification logics. They will play a significant role later on. The first concerns substitution.

Definition 2.2 A *substitution* is a map from justification variables to justification terms. If σ is a substitution and X is a formula, we write $X\sigma$ for the result of replacing each variable x in X with the term $x\sigma$. Similarly for substitution in justification terms themselves.

The following is shown in [1] for LP, and applies, with exactly the same argument, to JS5.

Theorem 2.3 (Substitution Lemma) *If X is a theorem of LP, so is $X\sigma$. Further, if X has an injective proof, so does $X\sigma$.*

The constant specification used for proving X and that used for proving $X\sigma$ will, in general, be different, but that does not matter for our purposes.

The second fundamental result is the Lifting Lemma, also from [1], that says justification logics internalize their own proofs. Let us take $X_1, \ldots, X_n \vdash_{\mathsf{J}} Y_1, \ldots, Y_m$ to mean that $(X_1 \wedge \ldots \wedge X_n) \supset (Y_1 \vee \ldots \vee Y_m)$ is a theorem of the justification logic J. The Lifting Lemma for LP, due to Artemov [1], says that if $s_1{:}X_1, \ldots, s_n{:}X_n, Y_1, \ldots, Y_k \vdash_{\mathsf{LP}} W$, then there is a justification term $u(s_1, \ldots, s_n, y_1, \ldots, y_k)$ (where the y_i are variables) such that $s_1{:}X_1, \ldots, s_n{:}X_n, y_1{:}Y_1, \ldots, y_k{:}Y_k \vdash_{\mathsf{LP}} u(s_1, \ldots, s_n, y_1, \ldots, y_k){:}W$. The version for $\mathsf{JS5}$ is broader in that the right side of the turnstyle can have multiple formulas.

Theorem 2.4 ($\mathsf{JS5}$ Lifting Lemma) *Suppose*

$$s_1{:}X_1, \ldots, s_n{:}X_n, Y_1, \ldots, Y_k \vdash_{\mathsf{JS5}} t_1{:}Z_1, \ldots, t_m{:}Z_m, W$$

then there is a proof polynomial $u(s_1, \ldots, s_n, t_1, \ldots, t_m, y_1, \ldots, y_k)$ such that

$$s_1{:}X_1, \ldots, s_n{:}X_n, y_1{:}Y_1, \ldots, y_k{:}Y_k \vdash_{\mathsf{JS5}} t_1{:}Z_1, \ldots, t_m{:}Z_m, u(s_1, \ldots, s_n, t_1, \ldots, t_m, y_1, \ldots, y_k){:}W.$$

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

We omit the (constructive) proof of this, which is similar to that for LP except that axiom 6 plays a role. If one moves formulas $t_i{:}Z_i$ from the right of the turnstyle to the left, as $\neg t_i{:}Z_i$, things are straightforward.

3 An $\mathsf{S5}$ Gentzen System

To date, all constructive proofs of Realization Theorems make use of cut-free Gentzen system (or tableau system) proofs. The logic $\mathsf{S5}$ is an anomaly among the most common modal logics, in that it does not seem to have a simple cut-free Gentzen system. The constructive $\mathsf{S5}$ Realization Theorem proof in [2] was based on a hypersequent calculus from [12]. But in [5] we gave a cut-free tableau system for $\mathsf{S5}$ that seems to be as simple as anything in the literature. We will make use of the corresponding Gentzen system here, so in this section we present it. We begin with a standard Gentzen system for $\mathsf{S4}$. Then we explain how to modify it for $\mathsf{S5}$. We assume formulas are built up from propositional letters and $\bot$ using $\supset$ and $\Box$.

A *sequent* for $\mathsf{S4}$ is a pair of finite multisets of modal formulas, where the pair is written $\Gamma \longrightarrow \Delta$, with Γ and Δ being multisets. Using multisets avoids the need for explicit permutation rules. Axioms are the following sequents, where P is any propositional letter.

$$P \longrightarrow P \qquad\qquad \bot \longrightarrow$$

Then the rules of derivation are as follows. In stating them, Γ and Δ are multisets, X and Y are formulas, and if $\Gamma = \{Y_1, \ldots, Y_k\}$ then $\Box\Gamma = \{\Box Y_1, \ldots, \Box Y_k\}$.

$$LW \quad \frac{\Gamma \longrightarrow \Delta}{\Gamma, X \longrightarrow \Delta} \qquad RW \quad \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, X}$$

$$LC \quad \frac{\Gamma, X, X \longrightarrow \Delta}{\Gamma, X \longrightarrow \Delta} \qquad RC \quad \frac{\Gamma \longrightarrow \Delta, X, X}{\Gamma \longrightarrow \Delta, X}$$

$$L\supset \quad \frac{\Gamma, Y \longrightarrow \Delta \quad \Gamma \longrightarrow \Delta, X}{\Gamma, X \supset Y \longrightarrow \Delta} \qquad R\supset \quad \frac{\Gamma, X \longrightarrow \Delta, Y}{\Gamma \longrightarrow \Delta, X \supset Y}$$

$$L\Box \quad \frac{\Gamma, X \longrightarrow \Delta}{\Gamma, \Box X \longrightarrow \Delta} \qquad R\Box \quad \frac{\Box\Gamma \longrightarrow X}{\Box\Gamma \longrightarrow \Box X}$$

As usual, a proof of a formula X in this calculus is a proof of the sequent $\longrightarrow X$. This is a standard sequent calculus for S4, and soundness and completeness arguments are well-known in the literature.

To turn this into a proof system for propositional S5, two simple changes are needed. First, the rule $R\Box$ is replaced by a stronger version allowing multiple formulas on the right. Here is the rule we will be using for S5.

$$R\Box \quad \frac{\Box\Gamma \longrightarrow \Box\Delta, X}{\Box\Gamma \longrightarrow \Box\Delta, \Box X}$$

The system, with this new $R\Box$ rule, is sound for S5, but it is not complete when used directly. However we do have completeness in the following odd sense. *If X is a valid formula of S5, there will be a sequent proof of $\longrightarrow \Box X$.*

In order to give an example of a proof, it will be convenient to introduce negation in the usual way, $\neg X$ stands for $X \supset \bot$. It is easy to show the following are derived rules, and we will make use of them in the example. This example will be continued in Section 6.

$$L\neg \quad \frac{\Gamma \longrightarrow \Delta, X}{\Gamma, \neg X \longrightarrow \Delta} \qquad R\neg \quad \frac{\Gamma, X \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg X}$$

Example We prove $P \supset \Box\neg\Box\neg P$ in this system by giving a Gentzen derivation of the sequent $\longrightarrow \Box(P \supset \Box\neg\Box\neg P)$.

1	$P \longrightarrow P$
2	$P, \neg P \longrightarrow$
3	$P, \neg P \longrightarrow \Box\neg\Box\neg P$
4	$\neg P \longrightarrow P \supset \Box\neg\Box\neg P$
5	$\Box\neg P \longrightarrow P \supset \Box\neg\Box\neg P$
6	$\Box\neg P \longrightarrow \Box(P \supset \Box\neg\Box\neg P)$
7	$\longrightarrow \neg\Box\neg P, \Box(P \supset \Box\neg\Box\neg P)$
8	$\longrightarrow \Box\neg\Box\neg P, \Box(P \supset \Box\neg\Box\neg P)$
9	$P \longrightarrow \Box\neg\Box\neg P, \Box(P \supset \Box\neg\Box\neg P)$
10	$\longrightarrow (P \supset \Box\neg\Box\neg P), \Box(P \supset \Box\neg\Box\neg P)$
11	$\longrightarrow \Box(P \supset \Box\neg\Box\neg P), \Box(P \supset \Box\neg\Box\neg P)$
12	$\longrightarrow \Box(P \supset \Box\neg\Box\neg P)$

In this: 1 is an axiom, 2 is from 1 by $L\neg$, 3 is from 2 by RW, 4 is from 3 by $R\supset$, 5 is from 4 by $L\Box$, 6 is from 5 by $R\Box$, 7 is from 6 by $R\neg$, 8 is from 7 by $R\Box$, 9 is from 8 by LW, 10 is from 9 by $R\supset$, 11 is from 10 by $R\Box$, and 12 is from 11 by RC.

Soundness and completeness are shown in [5] for a tableau version of this system. That transfers to the present Gentzen system either by adapting the proof, or by showing that tableau proofs translate into sequent calculus proofs. Details are omitted here.

4 Annotations and Realizations

The Realization Theorem deals with *occurrences* of modal operators, and treats positive and negative occurrences differently; negatives become proof variables while positives need not. To make this formal, in [7, 8, 9] I introduced *annotated* formulas—providing syntactic machinery to keep track of $\Box$ occurrences.

For annotated formulas, instead of a single operator $\Box$ there is an infinite family, $\Box_1$, $\Box_2$, ... These are called *indexed* modal operators. Annotated formulas are built up as usual, but using indexed modal operators instead of $\Box$. If X is an annotated formula, and X' is the result of replacing all indexed modal operators, $\Box_n$, with $\Box$, we say X is an *annotated version* of X', and X' is an *unannotated version* of X.

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.

Annotations are simply 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 are fundamental, but formulas that are annotated but not properly so also arise. For instance, if $X \supset Y$ is properly annotated, the subformula Y is also, but X is not (though $\neg X$ is). Generally we will fix a properly annotated formula X and work with subformulas of it, where these may not be properly annotated.

It is easy to see that every modal formula has many properly annotated versions. But further, it is also easy to give an annotated version of the S5 proof system in Section 3. Except for the two modal rules, all the axioms and rules have exactly the same form *but formulas are now annotated.* Annotations must be preserved in moving from sequents above the line to sequents below the line. The two modal rules become the following.

$$L\Box \quad \frac{\Gamma, X \longrightarrow \Delta}{\Gamma, \Box_{2n} X \longrightarrow \Delta} \qquad R\Box \quad \frac{\Box_{2n_1} Y_1, \ldots, \Box_{2n_j} Y_j \longrightarrow \Box_{2m_1+1} Z_1, \ldots, \Box_{2m_k+1} Z_k, X}{\Box_{2n_1} Y_1, \ldots, \Box_{2n_j} Y_j \longrightarrow \Box_{2m_1+1} Z_1, \ldots, \Box_{2m_k+1} Z_k, \Box_{2p+1} X}$$

If there is a sequent proof ending with $\longrightarrow X$ (annotated or unannotated), it has one in which every formula that appears is a subformula of X; more strongly, it has one in which every formula on the left of an arrow is a negative subformula of X and every formula on the right of an arrow is a positive subformula of X.

Proposition 4.1 *Let Z be an unannotated modal formula and X be any properly annotated version of Z. If there is an unannotated sequent proof of $\longrightarrow Z$ then there is an annotated sequent proof of $\longrightarrow X$.*

Briefly, take a proof of $\longrightarrow Z$ in the unannotated sequent calculus, and use this to construct an annotated proof of $\longrightarrow X$. Replace the final $\longrightarrow Z$ with $\longrightarrow X$, then propagate the annotations upward, from conclusions of rules to premises, until the entire sequent construction has been annotated. A formal version of this verification amounts to an induction on the number of sequents in the unannotated proof, and is omitted. An example can be found in Section 6.

Now that we have annotated formulas, realizations can be defined functionally in a natural way. A *realization function* is a mapping from positive integers to proof polynomials that maps even integers to justification variables. Moreover 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 justification variables arranged in a standardized order. If X is an annotated formulala, 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 justification logic. Now, here is a statement of the theorem we are after.

Theorem 4.2 *If Z is a theorem of S5, then for any properly annotated version X of Z there is a realization function r such that $r(X)$ is injectively provable in* JS5*.*

5 Modifying Realizations

Realizations, treated as functions, can be combined and modified in various ways, though this is not a simple process. In [7, 8, 9] several ways of doing so were presented, with the work continued in [10]. We need two of these.

The first of our results from [7, 9] has to do with the merging of different realizations for the same formula. As originally stated the theorem was for LP, but the proof only makes use of the fact that $+$ and $\cdot$ are among the available operations, and an Internalization Lemma is provable, and hence it holds for JS5 as well. Also, it applies to the merging of many realization functions—we will only need it for two of them.

Definition 5.1 Let X be an annotated formula and r_1 and r_2 be realization functions. We say a pair $\langle r, \sigma\rangle$ consisting of a realization function and a substitution *hereditarily merges* r_1 and r_2 on on X provided, for each subformula φ of X:

1. if φ is a positive subformula of X then both $r_1(\varphi)\sigma \supset r(\varphi)$ and $r_2(\varphi)\sigma \supset r(\varphi)$ are theorems, provable with an injective constant specification;

2. if φ is a negative subformula of X then both $r(\varphi) \supset r_1(\varphi)\sigma$ and $r(\varphi) \supset r_2(\varphi)\sigma$ are theorems, provable with an injective constant specification.

Theorem 5.2 (Realization Merging) *Let X be a properly annotated formula, and r_1 and r_2 be realization functions. Then there is a realization/substitution pair $\langle r, \sigma\rangle$ that hereditarily merges r_1 and r_2 on X.*

The proof of this Theorem is entirely algorithmic, but it is complex and is omitted here, as is the algorithm and verification for the next result—they can be found in detail in [7]. The second item from that paper is an analog of the replacement property of classical logic. Suppose $\psi(P)$ is a classical formula and P is a propositional letter, we write $\psi(A)$ for the result of replacing all occurrences of P in $\psi(P)$ with occurrences of the formula A. Suppose P has only positive occurrences in $\psi(P)$. Then, if $A \supset B$ is provable so is $\psi(A) \supset \psi(B)$. If P has only negative occurrences then $A \supset B$ provable yields that $\psi(B) \supset \psi(A)$ is provable. We gave a corresponding result for the justification logic LP, but it too applies to $\mathsf{JS5}$. Further, in [7] the replacement result was narrowed to be more directly applicable to the construction of realizations. In fact, we did not narrow it enough, and the realization algorithm given there appeared to be more complicated than was needed. Here we first state the appropriate item from [7], then use it to derive the narrower thing we actually need.

Definition 5.3 Let $X(P)$ be an annotated formula in which the propositional letter P has at most one positive occurrence, let A and B be annotated formulas, and let r_1 be a realization function. We say the realization/substitution pair $\langle r, \sigma\rangle$ *hereditarily replaces* $r_1(A)$ with $r_1(B)$ at P in $X(P)$ provided, for each subformula $\varphi(P)$ of $X(P)$:

1. if $\varphi(P)$ is a positive subformula of $X(P)$ then $r_1(\varphi(A))\sigma \supset r(\varphi(B))$ has a proof with an injective constant specification;

2. if $\varphi(P)$ is a negative subformula of $X(P)$ then $r(\varphi(B)) \supset r_1(\varphi(A))\sigma$ has a proof with an injective constant specification.

We actually need a very simple version of replacement, in which we jointly replace $t{:}F$ and $u{:}F$ with the weaker $(t+u){:}F$. Here is a formulation using the machinery of realization functions.

Theorem 5.4 (Realization Weakening) *Assume the following.*

S–1. *$X(P)$ is a properly annotated formula in which the propositional letter P has at most one positive occurrence;*

S–2. *$\Box_p K$ and $\Box_q K$ are both are properly annotated, there is no annotation overlap between $X(P)$ and $\Box_p K$, and $X(P)$ and $\Box_q K$, and p and q are different;*

S–3. *r_1 and r_2 are realization functions with $r_1(K) = r_2(K)$;*

S–4. *$r_1(q) = r_2(q) = r_1(p) + r_2(p)$.*

Then there is a realization/substitution pair $\langle r, \sigma\rangle$ that hereditarily replaces $r_1(\Box_p K)$ with $r_1(\Box_q K)$ at P in $X(P)$, and hereditarily replaces $r_2(\Box_p K)$ with $r_2(\Box_q K)$ at P in $X(P)$.

If we set $r_1(K) = r_2(K) = F$, $r_1(p) = t$, $r_2(p) = u$, and $r_1(q) = r_2(q) = t + u$, the theorem above provides a replacement of $t{:}F$ and $u{:}F$ with $(t + u){:}F$, as promised.

In [7] as it has been available in pre-publication form, the proof of the Realization Theorem made use of the Realization Weakening Theorem directly. In fact, only a very narrow special case of it is needed, and this is embodied in the following Corollary. The proof of this Corollary was implicit in [7], and is made explicit here. Hopefully, the paper [7] itself can be revised before publication by incorporating the present approach into it.

Corollary 5.5 *Suppose X is a properly annotated formula with $\Box_p K$ as a positive subformula. Let r_1 be a realization function, and u be a justification term. There is a realization/substitution pair $\langle r, \sigma\rangle$ such that:*

1. *if φ is a positive subformula of X then $r_1(\varphi)\sigma \supset r(\varphi)$ is provable using an injective constant specification;*
2. *if φ is a negative subformula of X then $r(\varphi) \supset r_1(\varphi)\sigma$ is provable using an injective constant specification;*
3. *$u{:}r_1(K)\sigma \supset r(\Box_p K)$ is an injective theorem.*

The corollary above can be given an intuitive meaning consistent with what we have been saying. Suppose we write t for $r_1(p)$. Since $\Box_p K$ is a positive subformula of X conclusion 1 has, as a special case, the injective provability of

$$t{:}r_1(K)\sigma \supset r(\Box_p K)$$

while conclusion 3 asserts the injective provability of

$$u{:}r_1(K)\sigma \supset r(\Box_p K)$$

and thus we might loosely describe what is happening as: $\langle r, \sigma\rangle$ *weakens t to $t + u$ at p.*

Proof We will derive this from Theorem 5.4. We first introduce a new index q and a second realization function, r_2. Then we apply Theorem 5.4, and eliminate the index q at the end.

The formula $\Box_p K$ occurs as a positive subformula of X so it must occur exactly once, since X is properly annotated and so the index p can occur only once. Let P be a propositional letter that does not occur in X, and let $X(P)$ be like X except that the subformula $\Box_p K$ has been replaced with P. Then P must have a single positive occurrence in $X(P)$, and X is the same as $X(\Box_p K)$. Also, no index in $\Box_p K$ can occur in $X(P)$, again since $X = X(\Box_p K)$ is properly annotated.

Let q be an odd index that does not occur in X (and hence it is different than p). Then $X(P)$, $\Box_p K$, and $\Box_q K$ are properly annotated, $X(P)$ and $\Box_p K$ have no annotation overlap, and $X(P)$ and $\Box_q K$ have no annotation overlap.

Modify the definition of r_1 so that $r_1(q) = r_1(p) + u$. Since q does not occur in X this does not change the behavior of r_1 on X or its subformulas.

Define a second realization function r_2 to be the same as r_1, except that $r_2(p) = u$. Since $\Box_p K$ is a subformula of X, and X is properly annotated, p does not occur in K and hence $r_1(K) = r_2(K)$. Also by definition, $r_2(q) = r_1(q) = r_1(p) + u = r_1(p) + r_2(p)$.

Now we can apply Theorem 5.4, Realization Weakening. There is a realization/substitution pair $\langle r^*, \sigma^* \rangle$ that hereditarily replaces $r_1(\Box_p K)$ with $r_1(\Box_q K)$ at P in $X(P)$ and hereditarily replaces $r_2(\Box_p K)$ with $r_2(\Box_q K)$ at P in $X(P)$. The realization function r^* is almost the one we want—it needs one modification. Let r be like r^* except that $r(p) = r^*(q)$. We will show the realization/substitution pair $\langle r, \sigma^* \rangle$ does the job.

Let φ be an arbitrary subformula of X. Recall that $X(P)$ was like X but with $\Box_p K$ replaced with P, and so $X = X(\Box_p K)$. Since φ is a subformula of $X(\Box_p K)$ there are three possibilities. It could be that φ is a subformula of K. Otherwise φ is not a subformula of K, in which case either $\Box_p K$ is a subformula of φ (possibly not proper), or $\Box_p K$ and φ are disjoint. If $\Box_p K$ is a subformula of φ then there is a subformula $\varphi(P)$ of $X(P)$ with $\varphi = \varphi(\Box_p K)$. We can treat the case where φ and $\Box_p K$ are disjoint the same way by allowing P to occur vacuously in $\varphi(P)$. Thus we really have two cases to consider. We handle each case separately to establish conclusions 1 and 2 of the Corollary. Conclusion 3 is shown the same way in either case.

Suppose first that φ is a subformula of K. Since $r^*(K) = r_1(K)\sigma^*$ we must have $r^*(\varphi) = r_1(\varphi)\sigma^*$ Since r and r^* only differ on q, and q cannot occur in K, we have $r(\varphi) = r_1(\varphi)\sigma^*$. This gives us conclusions 1 and 2 for this case.

For the second case, let $\varphi(P)$ be a subformula of $X(P)$. Let us say it is a positive subformula—the negative subformula case is handled similarly. Since $\langle r^*, \sigma^* \rangle$ hereditarily replaces $r_1(\Box_p K)$ with $r_1(\Box_q K)$ at P in $X(P)$, we have the provability of $r_1(\varphi(\Box_p K))\sigma^* \supset r^*(\varphi(\Box_q K))$. Since $r(p) = r^*(q)$, this says we have the provability of $r_1(\varphi(\Box_p K))\sigma^* \supset r(\varphi(\Box_p K))$, and this is conclusion 1 of the Corollary.

Finally, P is a positive subformula of $X(P)$, so since $\langle r^*, \sigma^* \rangle$ also hereditarily replaces $r_2(\Box_p K)$ with $r_2(\Box_q K)$ at P in $X(P)$, we have provability of $r_2(\Box_p K)\sigma^* \supset r^*(\Box_q K)$. Again since $r^*(q) = r(p)$, this give provability of $r_2(\Box_p K)\sigma^* \supset r(\Box_p K)$. And since $r_2(p) = u$ and $r_2(K) = r_1(K)$ we have provability of $u{:}r_1(K)\sigma^* \supset r(\Box_p K)$, and this is conclusion 3 of the Corollary. ■

Now we combine the machinery presented so far, and give a proof of the Realization Theorem for S5, along the same lines as the one for S4 in [7].

Theorem 5.6 *If Z_0 is a theorem of S5, there is a realization of Z_0 that is an injectively provable theorem of* JS5. *More precisely, if Z_0 is a theorem of S5, then for any properly annotated version Z of Z_0 there is a realization function r such that $r(Z)$ is injectively provable in* JS5.

Proof Assume Z_0 is a theorem of S5, and Z is a properly annotated version of Z_0. There is a sequent proof $\mathcal{P}$ of $\rightarrow \Box Z$ in the annotated Gentzen calculus of Section 3. We will show that, in a suitable sense, every sequent in $\mathcal{P}$ is realizable. It will follow that $\Box Z$ is realizable, and then so is Z, using Axiom Scheme 4 from Section 2.

There is a standard connection between sequents and formulas. Here it is, for the record. For each sequent S of annotated formulas, an annotated formula $\|S\|$ is defined.

1. $\|X_1, \ldots, X_n \longrightarrow Y_1, \ldots, Y_m\| = [(X_1 \wedge \ldots \wedge X_n) \supset (Y_1 \vee \ldots \vee Y_m)]$.

2. $\|X_1, \ldots, X_n \rightarrow \| = [(X_1 \wedge \ldots \wedge X_n) \supset \bot]$.

3. $\| \longrightarrow Y_1, \ldots, Y_k\| = [(Y_1 \vee \ldots \vee Y_k)]$.

We now show that for every sequent S in proof $\mathcal{P}$, there is a realization function r such that $r(\|S\|)$ is injectively provable in JS5. The final sequent is $\longrightarrow \Box Z$, and $\| \longrightarrow \Box Z\|$ is simply $\Box Z$, and the existence of a realization function for Z follows. We show axioms in $\mathcal{P}$ are realized, and that realization is preserved by the rules of derivation.

Sequents that are axioms have no modal operators, so for these we can take any realization function.

With two exceptions, if r realizes the premise of a rule, it also realizes the conclusion. The two exceptions are $L\supset$ (which has two premises), and $R\Box$. We concentrate on these two cases, and leave the others to you—the arguments are straightforward.

The two hard cases are handled more-or-less the same way that worked for the S4 Realization Theorem in [7], so here we only sketch the ideas.

We begin with $L\supset$. Suppose both $\Gamma, Y \longrightarrow \Delta$ and $\Gamma \longrightarrow \Delta, X$ are realized, though different realization functions may be involved. Say $r_1(\|\Gamma, Y \longrightarrow \Delta\|)$ and $r_2(\|\Gamma \longrightarrow \Delta, X\|)$ both have injective S5 proofs. By the Realization Merging Theorem 5.2, there is a realization/substitution pair $\langle r, \sigma\rangle$ that hereditarily merges r_1 and r_2 on Z. Then $r(\|\Gamma, X \supset Y \longrightarrow \Delta\|)$ is injectively provable, as we now verify.

Suppose φ is an annotated formula on the left in one of the premise sequents, so φ is in Γ or is Y itself. Then φ is a negative subformula of Z, so both $r(\varphi) \supset r_1(\varphi)\sigma$ and $r(\varphi) \supset r_2(\varphi)\sigma$ are injectively provable. Similarly if φ on the right, a member of Δ or X itself, it is a positive subformula of Z and so both $r_1(\varphi)\sigma \supset r(\varphi)$ and $r_2(\varphi)\sigma \supset r(\varphi)$ are injectively provable. Either way, it is easy to see that $r_1(\|\Gamma, Y \to \Delta\|)\sigma \supset r(\|\Gamma, Y \to \Delta\|)$ and $r_2(\|\Gamma \to \Delta, X\|)\sigma \supset r(\|\Gamma \to \Delta, X\|)$ are injectively provable. Since $r_1(\|\Gamma, Y \longrightarrow \Delta\|)$ is injectively provable, by the Substitution Lemma 2.3 so is $r_1(\|\Gamma, Y \longrightarrow \Delta\|)\sigma$. Similarly $r_2(\|\Gamma \longrightarrow \Delta, X\|)\sigma$ is injectively provable. It follows that both $r(\|\Gamma, Y \to \Delta\|)$ and $r(\|\Gamma \to \Delta, X\|)$ are injectively provable. Now we have a single realization function, r, for both sequents and it is easy to show that $r(\|\Gamma, X \supset Y \longrightarrow \Delta\|)$ is injectively provable.

Finally we consider the case $R\Box$. Suppose

$$\Box_{n_1} Y_1, \ldots, \Box_{n_j} Y_j \longrightarrow \Box_{p_1} Z_1, \ldots, \Box_{p_k} Z_k, X \tag{1}$$

is realized, say using the realization function r_1. In this each n_1 is even, being in a negative position, and each p_i is odd, being in a positive position. We show

$$\Box_{n_1} Y_1, \ldots, \Box_{n_j} Y_j \longrightarrow \Box_{p_1} Z_1, \ldots, \Box_{p_k} Z_k, \Box_p X \tag{2}$$

is realized, where p is odd. It is assumed that (1) and (2) occur in proof $\mathcal{P}$.

Since r_1 realizes (1), there is a JS5 proof of the following (where $r_1(n_i)$ is a variable for each n_i).

$$[r_1(\Box_{n_1} Y_1) \wedge \ldots \wedge r_1(\Box_{n_j} Y_j)] \supset [r_1(\Box_{p_1} Z_1) \wedge \ldots \wedge r_1(\Box_{p_k} Z_k) \wedge r_1(X)] \tag{3}$$

Using (3) and the Lifting Lemma, Theorem 2.4, there is a justification term, call it u, such that

$$[r_1(\Box_{n_1} Y_1) \wedge \ldots \wedge r_1(\Box_{n_j} Y_j)] \supset [r_1(\Box_{p_1} Z_1) \wedge \ldots \wedge r_1(\Box_{p_k} Z_k) \wedge u{:}r_1(X)] \tag{4}$$

is injectively provable.

If the index p has no occurrences in the sequent (1) then things are simple since what we do with p has no effect on what we have already done. Define a realization function r to be like r_1 except that $r(p) = u$. Then it follows immediately from (4) that r realizes (2).

The simple case just discussed may not always happen—the index p may already occur in (1) and so $r_1(p)$ may already be playing an important role in realizing (1). In such event, in realizing (2) we realize $\Box_p$ not with u itself, but with $r_1(p) + u$. We now establish that this works.

Apply Corollary 5.5 of the Realization Weakening Theorem. (Recall, $\Box_p X$ must be a positive subformula of Z since it occurs on the right of the arrow in the Gentzen proof $\mathcal{P}$ of Z.) There is a realization/substitution pair $\langle r, \sigma\rangle$ that meets the following conditions

1. if φ is a positive subformula of Z then $r_1(\varphi)\sigma \supset r(\varphi)$ is an injective theorem;

2. if φ is a negative subformula of Z then $r(\varphi) \supset r_1(\varphi)\sigma$ is an injective theorem;

3. $u{:}r_1(X)\sigma \supset r(\Box_p X)$ is an injective theorem.

From (4) and the Substitution Lemma, Theorem 2.3, we have provability of the following.

$$[r_1(\Box_{n_1} Y_1)\sigma \wedge \ldots \wedge r_1(\Box_{n_j} Y_j)\sigma] \supset [r_1(\Box_{p_1} Z_1)\sigma \wedge \ldots \wedge r_1(\Box_{p_k} Z_k)\sigma \wedge u{:}r_1(X)\sigma] \tag{5}$$

Using this, we will now show that

$$[r(\Box_{n_1} Y_1) \wedge \ldots \wedge r(\Box_{n_j} Y_j)] \supset [r(\Box_{p_1} Z_1) \wedge \ldots \wedge r(\Box_{p_k} Z_k) \wedge r(\Box_p X)] \tag{6}$$

has a proof, and thus (2) is realized.

Consider one of the formulas on the left of sequent (2), say $\Box_{n_i} Y_i$. This is a negative subformula of Z and hence $r(\Box_{n_i} Y_i) \supset r_1(\Box_{n_i} Y_i)\sigma$ is provable. We thus have provability of the following.

$$[r(\Box_{n_1} Y_1) \wedge \ldots \wedge r(\Box_{n_j} Y_j)] \supset [r_1(\Box_{n_1} Y_1)\sigma \wedge \ldots \wedge r_1(\Box_{n_j} Y_j)\sigma] \tag{7}$$

Next consider a formula on the right of sequent (2) of the form $\Box_{p_i} Z_i$. This is a positive subformula of Z and so $r_1(\Box_{p_i} Z_i)\sigma \supset r(\Box_{p_i} Z_i)$ is provable. So we have provability of the following.

$$[r_1(\Box_{p_1} Z_1)\sigma \wedge \ldots \wedge r_1(\Box_{p_k} Z_k)\sigma] \supset [r(\Box_{p_1} Z_1) \wedge \ldots \wedge r(\Box_{p_k} Z_k)] \tag{8}$$

Finally, by conclusion 3 of the Corollary,

$$u{:}r_1(X)\sigma \supset r(\Box_p X) \tag{9}$$

is provable.

Now, simply combining (7), (5), (8), and (9), we immediately have (6). ■

6 A Realization Example

We produce a realization for the S5 theorem $P \supset \Box\neg\Box P$, where P is a propositional letter. In Section 3 we gave a Gentzen system proof for this, which amounted to constructing a sequent proof for $\Box(P \supset \Box\neg\Box P)$. We build on that.

To begin, we need a properly annotated version of $\Box(P \supset \Box\neg\Box P)$. We use $\Box_1(P \supset \Box_3\neg\Box_2\neg P)$. And next we need an annnotated sequent proof of this. One can be created by starting with the unannotated proof, annotating the last sequent, and propagating the annotations upward. The result is the following.

1	$P \longrightarrow P$
2	$P, \neg P \longrightarrow$
3	$P, \neg P \longrightarrow \Box_3 \neg \Box_2 \neg P$
4	$\neg P \longrightarrow P \supset \Box_3 \neg \Box_2 \neg P$
5	$\Box_2 \neg P \longrightarrow P \supset \Box_3 \neg \Box_2 \neg P$
6	$\Box_2 \neg P \longrightarrow \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
7	$\longrightarrow \neg \Box_2 \neg P, \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
8	$\longrightarrow \Box_3 \neg \Box_2 \neg P, \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
9	$P \longrightarrow \Box_3 \neg \Box_2 \neg P, \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
10	$\longrightarrow (P \supset \Box_3 \neg \Box_2 \neg P), \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
11	$\longrightarrow \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P), \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$
12	$\longrightarrow \Box_1 (P \supset \Box_3 \neg \Box_2 \neg P)$

Next, we follow the algorithm embodied in the proof of Theorem 5.6, and show each sequent above is realizable in JS5. In doing this we make use of Corollary 5.5 which, in turn, uses the Realization Weakening Theorem 5.4. The proof of this theorem is algorithmic, and the algorithm can be found in [7]—here we simply give the results of the application of the algorithm.

Sequents 1, 2, 3, 4, 5 To realize 1, any realization function will do. Then this is also the case for 2, 3, 4, and 5, which follow using rules $L\neg$, RW, $R \supset$, and $L\Box$ respectively. We must have $r_1(2) = x_1$ and, to be specific, let us say $r_1(3) = a$. Then 5 is realized by the following justification formula, provable in JS5.

$$x_1{:}\neg P \supset [P \supset a{:}\neg x_1{:}\neg P]$$

Sequents 6, 7 Sequent 6 follows from 5 by $R\Box$, and since the index 1 does not occur in sequent 5 things are simple. By the Lifting Lemma there is a justification term q such that $x_1{:}\neg P \supset q{:}[P \supset a{:}\neg x_1{:}\neg P]$ is a theorem of JS5. The proof of the Lifting Lemma is constructive, but here we will not explicitly produce q. We simply note that such a term can be produced. Now, a realization function for 6 is r_2 where $r_2(1) = q$, $r_2(2) = x_1$, and $r_2(3) = a$. The same realization function works for sequent 7 since the rule $R\neg$ is involved. Thus we have JS5 provability of the following.

$$\neg x_1{:}\neg P \vee q{:}[P \supset a{:}\neg x_1{:}\neg P]$$

Sequents 8, 9, 10 Sequent 8 follows from 7 by $R\Box$, and index 3 already occurs in 7 so we are in a more complex situation. Since we have JS5 provability of the formula given above, realizing sequent 7, by the Lifting Lemma there is a justification term r such that $r{:}\neg x_1{:}\neg P \wedge q{:}(P \supset a{:}\neg x_1{:}\neg P)$ is provable. The idea is to have realization function r_3 come from r_2 using Corollary 5.5, weakening $a = r_2(3)$ to $a + r$. Working this out produces a realization function such that $r_3(1) = s \cdot q$, $r_3(2) = x_1$, and $r_3(3) = a + r$, where s internalizes a proof of the JS5 theorem $(P \supset a{:}\neg x_1{:}\neg P) \supset (P \supset (a + r){:}\neg x_1{:}\neg P)$. That is, we have JS5 provability of

s:$[(P \supset a{:}\neg x_1{:}\neg P) \supset (P \supset (a+r){:}\neg x_1{:}\neg P)]$. The same realization function works for sequents 9 and 10. Then, sequent 10 has the following realization.

$$(P \supset (a+r){:}\neg x_1{:}\neg P) \vee (s \cdot q){:}(P \supset (a+r){:}\neg x_1{:}\neg P)$$

Sequents 11, 12 Sequent 11 is from 10 by $R\Box$, and the index 1 occurs in 10, so we again have a complex situation. The formula above, realizing sequent 10, is provable so by the Lifting Lemma, again, there is a justification term t such that $t{:}(P \supset (a+r){:}\neg x_1{:}\neg P) \vee (s \cdot q){:}(P \supset (a+r){:}\neg x_1{:}\neg P)$ is provable. Now Corollary 5.5 comes into play again, and we arrive at the following. Let r_4 be like r_3 except that $r_4(1) = r_3(1) + t$. That is, $r_4(1) = (s \cdot q) + t$, $r_4(2) = x_1$, and $r_4(3) = a + r$. This realizes sequent 11, and also sequent 12. We thus have the $\mathsf{JS5}$ provability of the following.

$$(s \cdot q + t){:}(P \supset (a+r){:}\neg x_1{:}\neg P)$$

Conclusion Now we use axiom 4 and modus ponens with the formula above. The following is provable in $\mathsf{JS5}$:

$$P \supset (a+r){:}\neg x_1{:}\neg P \tag{10}$$

where a is arbitrary, and r is a justification term such that $r{:}\neg x_1{:}\neg P \wedge q{:}(P \supset a{:}\neg x_1{:}\neg P)$ is provable, where q in turn is a justification term such that $x_1{:}\neg P \supset q{:}[P \supset a{:}\neg x_1{:}\neg P]$ is provable. Notice that q itself has disappeared from (10) except insofar as it has been incorporated into r. It is (10) that realizes the $\mathsf{S5}$ theorem $P \supset \Box\neg\Box\neg P$.

References

[1] S. Artemov. Explicit provability and constructive semantics. *The Bulletin for Symbolic Logic*, 7(1):1–36, 2001.

[2] S. Artemov, E. Kazakov, and D. Shapiro. On logic of knowledge with justifications. Technical Report CFIS 99-12, Cornell University, 1999.

[3] V. Brezhnev and R. Kuznets. Making knowledge explicit: How hard it is. *Theoretical Computer Science*, 357(1-3):23–34, 2006.

[4] S. Feferman, editor. *Kurt Gödel Collected Works*. Oxford, 1986-2003. Five volumes.

[5] M. C. Fitting. A simple propositional S5 tableau system. *Annals of Pure and Applied Logic*, 96:107–115, 1999. Originally in *The Parikh Project, Seven papers in honour of Rohit*, Uppsala Prints and Reprints in Philosophy, 1996 Number 18.

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

[7] M. C. Fitting. Realizations and LP. Available at `http://comet.lehman.cuny.edu/fitting/`, 2006.

[8] M. C. Fitting. A replacement theorem for LP. Technical Report TR-2006002, CUNY Ph.D. Program in Computer Science, 2006. `http://www.cs.gc.cuny.edu/tr/`.

[9] M. C. Fitting. Realizations and LP. In S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science — New York '07*. Springer-Verlag, 2007. Lecture Notes in Computer Science, 4514.

[10] M. C. Fitting. Realizing substitution instances of modal theorems. Technical Report TR-2007006, CUNY Ph.D. Program in Computer Science, 2007. `http://www.cs.gc.cuny.edu/tr/`.

[11] K. Gödel. Eine Interpretation des intuistionistischen Aussagenkalkuls. *Ergebnisse eines mathematischen Kolloquiums*, 4:39–40, 1933. Translated as *An interpretation of the intuitionistic propositional calculus* in [4] I, 296-301.

[12] G. Mints. Lewis' systems and system T. In *Selected papers in proof theory (1965-1973)*. Bibliopolis, 1992.

[13] N. Rubtsova. Evidence reconstruction of epistemic modal logic S5. In D. Grigoriev, J. Harrison, and E. A. Hirsch, editors, *Computer Science — Theory and Applications*, Lecture Notes in Computer Science, vol 3967, pages 313–321. Springer-Verlag, 2006.