Modal unification step by step

Sam v. Gool\textsuperscript{1} and Johannes Marti\textsuperscript{2}

\textsuperscript{1} IRIF, Universit\é Paris Cit\é
\textsuperscript{2} Department of Computer Science, University of Oxford

Abstract

We propose an approach to unification in modal logics that combines duality and step-by-step constructions of terminal frames. We apply this approach to the modal logics K, Alt\textsubscript{1}, and a logic that we call KdB. For K, we show how our methods give an effective reformulation of the unifiability problem as a non-trivial decision problem involving neighborhood frames. For Alt\textsubscript{1}, we show that the problem is PSPACE-complete. For KdB, we establish that unifiability is equivalent to a problem involving de Bruijn graphs.

Introduction. The decision problem of unifiability for a normal modal logic L asks, for a given formula $\phi(p_1, \ldots, p_n)$, whether there exist formulas $\psi_1, \ldots, \psi_n$ such that the formula $\phi(\psi_1/p_1, \ldots, \psi_n/p_n)$, that is, the result of substituting $\psi_i$ for every occurrence of $p_i$, is a theorem of L. In this case, we call the substitution $p_i \mapsto \psi_i$ a unifier for $\phi$, and a ground unifier if the $\psi_i$ do not use variables. We only consider ground unifiers in this paper, which suffices for unifiability. In the case of the smallest normal modal logic, K, it is a prominent open question whether or not unifiability is decidable, see e.g. [WZ08, Je\v{r}13]. Much more is known in transitive modal logics, that is, extensions of K in which $3 \phi \rightarrow 2 \phi$ is a theorem for every formula $\phi$.

For a survey of unification problems in modal logic, with connections to description logic, we refer to [BG11], and we also refer to the introductions of [BGM+19] and [BGRT22] for more information about the modal logic side.

The main idea we pursue in this paper is that a combination of duality and step-by-step constructions gives a useful perspective on unifiability problems for modal logics beyond the transitive. Both ingredients are present in the ground-breaking series of papers on unification in transitive modal and intuitionistic logics [Ghi99, Ghi00], and the duality perspective on unification has been made more explicit since then, for example in [CM15, Ghi18, BG22]. The step-by-step approach is an algebraic way of viewing normal forms in modal logic, systematically studied in [Ghi95] and giving rise to finite model results in [Mos07]. On the semantic side of the duality, our construction is similar to the terminal sequence for a coalgebra functor, see e.g. [Bar93, Wor99], which has also been applied to prove finite model properties [Pat03].

Until further notice, we work in a propositional language with a single unary operator $\lozenge$. Recall that Alt\textsubscript{1} is defined as the extension of K by the axiom $\lozenge \phi \rightarrow \Box \phi$. Our main results are the following: (1) a general equivalence between unifiability in modal logic and a mapping problem between generalized graphs (Theorem 4), as corollary an effective reformulation of the decision problem for K (Corollary 5); (2) using the general equivalence, PSPACE-completeness of unifiability for Alt\textsubscript{1} (Theorem 7); (3) an equivalence between unifiability in a logic KdB, to be introduced below, and a mapping problem of de Bruijn graphs (Theorem 8).

A step-by-step approach: the general picture. Throughout this paper, $V$ will denote a finite set of (propositional) variables. We take $\neg, \lor, \bot$ and $\lozenge$ as primitive connectives, and other common logical symbols are considered as abbreviations. It will be convenient to borrow...
some notation from coalgebraic logic. Until further notice, we fix an arbitrary endofunctor \( \mathcal{T} \) on the category of sets and assume \( \mathcal{T} \) preserves finite sets. Recall that such an endofunctor gives rise to a coalgebraic modal logic \( L \) [Mos09], but we do not require the general definition in this paper. Instead, we will assume for now that the modal logic \( L \) associated to \( \mathcal{T} \) is described as a normal extension of \( K \) by a set of axioms \( \Gamma \), given as formulas with variables in \( V \). A reader not familiar with coalgebra may think of \( L \) as being either \( K \) or \( \text{Alt}_1 \), and of the functor \( \mathcal{T} \) as being either \( \mathcal{P} \) or \( 1 + (\cdot) \), respectively. A third instance, \( L = \text{KdB} \), will be examined later.

An \( L \)-algebra is a modal algebra \( B \) such that, for every interpretation \( f : V \to B \) of \( B \) and for every axiom \( \phi \in \Gamma \), the evaluation \( \phi[v \mapsto f(v)] \) is equal to \( \top \) in \( B \). We denote by \( F(V) \) the Lindenbaum algebra over \( V \) (for the logic \( L \)), which can be defined on the set of \( L \)-equivalence classes of formulas with variables in \( V \); in algebraic terms, \( F(V) \) is the free \( L \)-algebra over the set \( V \). By a common abuse of notation, we identify modal formulas with their corresponding class in \( F(V) \). An algebraic formulation of the unifiability problem for \( L \) is: given as input a modal formula \( \phi \) with variables in \( V \), determine whether or not there exists a homomorphism \( h : F(V) \to F(\emptyset) \) such that \( h(\phi) = \top \). Such a homomorphism is also called a (ground) unifier for \( \phi \); its depth is the maximal modal depth of the formulas \( h(p) \), for \( p \in V \).

We will make use of duality and one-step frames; we only briefly recall what we need explicitly in this abstract, for more details, see [CG12, BGJ14]. When \( S \) is a subset of a Boolean algebra \( A \), we will write \( \langle S \rangle_{\vee, \neg} \) for the Boolean subalgebra of \( A \) generated by \( S \). We define a chain of subalgebras of \( F(V) \). Let \( F_0(V) := \langle V \rangle_{\vee, \neg} \) and, for any \( n \in \mathbb{N} \), let \( F_{n+1}(V) := \langle a, \Diamond a \mid a \in F_n(V) \rangle_{\vee, \neg} \). Thus, \( F_n(V) \) contains the classes of formulas of modal depth \( \leq n \). Note that, for any \( n \in \mathbb{N} \), we have an inclusion homomorphism \( e_n : F_n(V) \to F_{n+1}(V) \) and an operator \( \varnothing_n : F_n(V) \to F_{n+1}(V) \), the restriction of the operator \( \Diamond \) on \( F(V) \) to the subalgebra \( F_n(V) \). The main idea of the step-by-step approach is that, given, for some \( n \geq 1 \), a particular "level" \( \xymatrix{ F_{n-1}(V) \ar[r]^-{\varnothing_{n-1}} & F_n(V) } \) of the approximating chain, it is possible to reconstruct the "next level" \( \xymatrix{ F_n(V) \ar[r]^-{\varnothing_n} & F_{n+1}(V) } \) without needing to refer to the global free algebra \( F(V) \).

We are thus dealing with a general construction on "levels". Any such level can be conveniently encoded as a one-step algebra for the logic \( L \). In the interest of space, we only recall the dual definition of one-step frame for the functor \( \mathcal{T} \).

A one-step \( \mathcal{T} \)-frame is a tuple \((X, Y, p, \alpha)\), where \( X, Y \) are sets and \( p : Y \to X \) and \( \alpha : Y \to TX \) are functions, and a bounded morphism \((X, Y, p, \alpha) \to (X', Y', p', \alpha')\) is a pair of functions \( f : X \to X' \), \( g : Y \to Y' \) such that \( f \circ p = p' \circ g \) and \( T f \circ \alpha = \alpha' \circ g \). We define a chain of one-step \( \mathcal{T} \)-frames. Let \( T_0(V) := 2^V \) and, for any \( n \in \mathbb{N} \), let \( T_{n+1}(V) := 2^V \times \mathcal{T} T_n(V) \). Define \( p_0 : T_1(V) \to T_0(V) \) to be the projection onto the first coordinate, and for any \( n \geq 1 \), define \( p_n : T_{n+1}(V) \to T_n(V) \) to be id_{2^V} \times \mathcal{T} p_{n-1} \). Also write, for any \( n \in \mathbb{N} \), \( \alpha_n : T_{n+1}(V) \to \mathcal{T} T_n(V) \) for the projection onto the second coordinate. We will use the notation \( C_n(V) := (T_n(V), T_{n+1}(V), p_n, \alpha_n) \) and call this the canonical one-step frame at level \( n \). In the cases that will interest us in this paper, the one-step \( \mathcal{T} \)-frame \((T_n(V), T_{n+1}(V), p_n, \alpha_n)\) is dual to \((F_n(V), F_{n+1}(V), e_n, \varnothing_n)\). What this means concretely is that one may exhibit, for every \( n \in \mathbb{N} \), a bijection \( \phi_n \) between \( T_n(V) \) and the set of atoms of \( F_n(V) \), in such a way that the function \( p_n \) corresponds to \( e_n \), and the function \( \alpha_n \) corresponds to the operator \( \varnothing_n \), under standard dual categorical equivalences between finite Boolean algebras and finite sets.

For example, in the case where \( L \) is the modal logic \( K \), we have \( \mathcal{T} = \mathcal{P} \), and it is well-known [Ghi05, Mos07] that the bijections may be described as follows. Given \( a \in T_0(V) = 2^V \), define the modal depth 0 formula \( \phi_0(a) := \bigwedge_{a(p) = 1} \Diamond p \land \bigwedge_{a(p) = 0} \neg p \). Then \( \phi_0 \) gives a bijection between \( T_0(V) \) and the set of atoms of \( F_0(V) \). Inductively, assuming a bijection \( \phi_n \) between \( T_n(V) \) and
the atoms of $F_n(V)$ has already been defined, we may define, for $a \in 2^V$ and $S \in \mathcal{PT}_n(V)$, the formula $\phi_{n+1}(a,S)$ as $\phi_0(a) \land \bigvee \{ \chi \phi_{n}(S) \land \bigwedge_{s \in S} \chi \phi_{n}(s) \}$.

Towards formulating the unifiability problem for $L$ using one-step frames, we now observe that we may restrict to formulas of depth at most 1, at the expense of a polynomial increase in the number of propositional variables; this is known as flattening, see e.g. [CG12, Remark 3.1].

If $\phi$ is a formula with variables in $V$, let $V'$ be the disjoint union of $V$ with a set of fresh proposition letters $q_\psi$, where $\psi$ ranges over the set $S(\phi)$ of subformulas of $\phi$. For every $\psi \in S(\phi)$, define a formula $\chi_\psi$ with variables in $V'$ as follows. If $\psi = \bot$ or $\psi = p$ then $\chi_\psi = q_\psi \leftrightarrow \psi$. If $\psi = \psi_1 \land \psi_2$ then $\chi_\psi = q_{\psi_1} \land q_{\psi_2}$. If $\psi = \neg \theta$ then $\chi_\psi = q_\psi \leftrightarrow \neg q_\theta$. Finally, if $\psi = \diamond \theta$ then $\chi_\psi = q_\psi \leftrightarrow \diamond q_\theta$. Note that, when $\theta$ is the identity functor, $\mathcal{T}$-graphs are just directed graphs, and when $\theta = \mathcal{P}$, $\mathcal{T}$-graphs are known as neighborhood frames, but our morphisms are not the same as the usual ones in that context.

We may thus assume that $\phi \in F_1(V)$. By duality, the finite Boolean algebra $F_1(V)$ is isomorphic to the algebra on $\mathcal{PT}_1(V)$; write $\widehat{\phi} \subseteq T_1(V)$ for the subset corresponding to $\phi$. Define the one-step frame $P(\phi) := (T_0(V), \widehat{\phi}, \phi')$, where $\phi'$ are the restrictions of $r_0$ and $p_0$, respectively, to $\phi$. Then duality between one-step algebras and one-step frames gives the following.

**Proposition 1.** Let $\phi \in F_1(V)$. For any $n \geq 0$, the set of functions $f : V \to F_n(\emptyset)$ such that $\phi(f(p) / p) = \top$ is in bijection with the set of bounded morphisms $C_n(\emptyset) \to P(\phi)$.

To analyze unification problems combinatorially, it is useful to replace one-step frames by single-sorted structures, which in several concrete cases below will become directed graphs with some additional structure. We define a $\mathcal{T}$-graph to be a pair $(X, \rho)$, where $X$ is a set and $\rho : X \to \mathcal{PT}X$ is a function. A $\mathcal{T}$-graph homomorphism from $(X, \rho)$ to $(X', \rho')$ is a function $f : X \to X'$ such that $P(T f)(p(x)) \subseteq \rho'(f(x))$ for all $x \in X$.\footnote{For any function $g : Y \to Y'$ between sets, we use the notation $P(g)$ for the direct image map $P(Y) \to P(Y')$.} Note that, when $\mathcal{T}$ is the identity functor, $\mathcal{T}$-graphs are just directed graphs, and when $\mathcal{T} = \mathcal{P}$, $\mathcal{T}$-graphs are known as neighborhood frames, but our morphisms are not the same as the usual ones in that context.

We will now show that we can toggle between $\mathcal{T}$-graphs and one-step $\mathcal{T}$-frames by means of an adjoint pair of functors, as we shall briefly describe now. When $(X', \rho')$ is a $\mathcal{T}$-graph, define the associated one-step $\mathcal{T}$-frame $\Phi(X', \rho') := (X', \rho'^1, \rho'^2)$, where $\rho'^1 := \{(w, v) \in X' \times T(X') \mid v \in \rho'(w)\}$, and $\rho'^1$ and $\rho'^2$ are the restrictions to $\rho'^1$ of the projection maps on $X'$ and $T(X')$, respectively. Conversely, when $\mathcal{F} = (X, Y, p, \alpha)$ is a one-step $\mathcal{T}$-frame, the associated $\mathcal{T}$-graph is defined as $\Gamma \mathcal{F} := (X, P \rho \circ p^{-1})$. Note that if $(f, g) : \mathcal{F} \to \Phi(X', \rho')$ is a bounded morphism, then in particular $f$ is a $\mathcal{T}$-graph homomorphism $\Gamma \mathcal{F} \to (X', \rho')$.

**Proposition 2.** Let $(X, Y, p, \alpha)$ be a one-step $\mathcal{T}$-frame and let $(X', \rho')$ be a $\mathcal{T}$-graph. For any $\mathcal{T}$-graph homomorphism $f : \Gamma(X, Y, p, \alpha) \to (X', \rho')$, there is a unique function $g$ such that $(f, g) : (X, Y, p, \alpha) \to \Phi(X', \rho')$ is a bounded morphism.

For any one-step $\mathcal{T}$-frame $\mathcal{F} = (X, Y, p, \alpha)$, we have that $\Phi \Gamma \mathcal{F} = (X, R, \pi_1, \pi_2)$, where $R = \{(x, \alpha(y)) \mid x \in X, y \in p^{-1}(x)\}$. We thus get a natural one-step morphism $\eta_\mathcal{F} := (id_X, g) : \mathcal{F} \to \Phi \Gamma \mathcal{F}$, where $g(y) := (p(x), \alpha(y))$ for every $y \in Y$.

**Proposition 3.** For any modal formula $\phi \in F_1(V)$, the one-step morphism $\eta_{P(\phi)} : P(\phi) \to \Phi \Gamma (P(\phi))$ is an isomorphism of one-step $\mathcal{T}$-frames.

Combining Propositions 1, 2, and 3, we obtain the following.

**Theorem 4.** Let $\phi$ be a modal formula of depth $\leq 1$. For any $n \geq 0$, there is a bijection between the set of ground $L$-unifiers of $\phi$ of depth $\leq n$ and the set of $\mathcal{T}$-graph homomorphisms $f : \Gamma(C_n(\emptyset)) \to \Gamma(P(\phi))$. 
Corollary 5. The unifiability problem for $K$ is equivalent to the problem which asks, given a modal formula $\phi \in F_1(V)$, whether or not there exist $n \geq 0$ and a $P$-graph homomorphism $f : \Gamma(C_n(\emptyset)) \to \Gamma(P(\phi))$.

Unification for $Alt_1$ step by step. In this section we apply the step-by-step approach to the modal logic $Alt_1$. This logic can be described as the coalgebraic modal logic for the endofunctor $T = 1 + (-)$ on the category of sets, which sends any set $X$ to the set $1 + X := \{\star\} \sqcup X$. One can show that the the canonical one-step frame at level $n$, when constructed from this functor $T$ as described above, is dual to the one-step algebras of formulas of depth $n$ in $Alt_1$. A $T$-graph for this functor $T$ is a pair $(X, \rho)$ with $\rho : X \to P(1 + X)$. Because $P(1 + (-)) \cong 2 \times P(-)$, these can be viewed concretely as graphs $(X, S, E)$ consisting of a set $X$ with a binary relation $S \subseteq X \times X$ and a set $E \subseteq X$. $T$-graph homomorphisms are then structure homomorphisms in the usual sense, meaning functions that preserve the relation $S$ and the labeling $E$.

To get an idea of how our approach applies, note that the set $T_n(V)$ is in bijection with the set of atoms in $F_n(V)$. In $Alt_1$ the corresponding formulas can be described concretely by the same bijection $\phi_0$ as in the case of $K$ above, and then, for any $n \in \mathbb{N}$, $a \in 2^V$, $s \in 1 + T_n(V)$, $\phi_{n+1}(a, s) := \phi_0(a) \land \Box \bot$ if $s = \star$ and $\phi_{n+1}(a, s) := \phi_0(a) \land \Diamond \phi_n(s)$ if $s \in T_n(V)$. In Figure 1a, we depict the initial part of the sequence of sets $T_n(\emptyset)$, with each element labeled by the corresponding formula, and the functions $p_n : T_{n+1}(\emptyset) \to T_n(\emptyset)$ and $\alpha_n : T_{n+1}(\emptyset) \to TT_n(\emptyset)$. Figure 1b shows the graphs $\Gamma(C_n)$ that are derived from the canonical frames as described in the previous section. For $Alt_1$, for any $n \in \mathbb{N}$, $\Gamma(C_n)$ is an $S$-chain of length $n$, where the first vertex is $S$-reflexive and the last vertex is the only vertex that satisfies $E$. Combining this observation with Theorem 4 leads to the following characterization of unification in $Alt_1$:

Theorem 6. For every formula $\phi$ of depth $\leq 1$ and $n \geq 0$ the ground $Alt_1$-unifiers of $\phi$ with depth $\leq n$ are in bijection with paths in the graph $\Gamma(P(\phi))$ that are of the form $v_0Sv_1S \ldots Sv_n$, where $v_0Sv_0$ and $v_n \in E$.

Using the characterization from Theorem 6 we obtain the following complexity result.

Theorem 7. The unifiability problem for $Alt_1$ is PSPACE-complete.

From Proposition 6.1 in [BT16] it is already known that unifiability for $Alt_1$ is in PSPACE. Our analysis shows that finding a unifier corresponds to finding a particular kind of path in the
introduce a set $M$ of Turing machine configurations of the graph $\Gamma(P(\phi))$. The vertices of the graph $\Gamma(P(\phi))$, on input $\phi$, can be represented in polynomial space and the relation $S$ and subset $E$ can be computed in polynomial time. The existence of such a path in $\Gamma(P(\phi))$ can be determined with a nondeterministic polynomial space algorithm that successively guesses the vertices on the path. Because PSPACE = NPSPACE this yields the PSPACE upper bound.

To prove PSPACE-hardness, we show that the language of an arbitrary polynomial space Turing machine $M$ reduces to the unification problem. Fix $M$. For every input $x$ of $M$, we introduce a set $V$ of size polynomial in the size of $x$, and we will compute in polynomial time a formula $\phi_x \in F(V)$ such that the accepting computations of $M$ on input $x$ correspond to paths in the graph $\Gamma(P(\phi_x))$ of the kind described in Theorem 6. We briefly describe the construction of $\phi_x$. The idea is to let the vertices of $\Gamma(P(\phi_x))$, which are by definition elements of $2^V$, encode configurations of $M$, whose size is bounded by a polynomial in the size of the input $x$. The formula $\phi_x$ can be defined in such a way that the following hold in $\Gamma(P(\phi_x))$ for all distinct $a, b \in 2^V$: (1) $aSa$ iff $a$ encodes the initial configuration of $M$ on input $x$. (2) $aSb$ iff $b$ encodes a successor configuration of the configuration encoded by $a$. (3) $a \in E$ iff $a$ encodes an accepting configuration. Requirement (2) can be expressed by a modal formula of polynomial size because it suffices to describe for each of the polynomially many individual cells on the tape how its content is updated when moving to the successor configuration.

Unification for $KdB$ step by step. The modal logic $KdB$ is an extension of the modal logic $KD!$, where we recall that $KD!$ is defined by extending $Alt_1$ with the axiom $\Box \phi \rightarrow \Diamond \phi$. Every ground formula in $KD!$ is equivalent to either $\top$ or $\bot$, so $KD!$-unification is trivially decidable. To make the unification problem more interesting we add a single constant $c$ to the language, which acts syntactically as a propositional letter but cannot be replaced by substitutions. The modal depth of the formula $c$ is stipulated to be 1. We define $KdB$ to be the logic resulting from adding the constant $c$ to $KD!$, without any additional axioms. The notions of one-step algebra and one-step frame can be extended to provide an interpretation for $c$.

One can view $KdB$ as the coalgebraic modal logic for the functor $T = 2 \times (-)$. The notions of one-step $T$-frame and $T$-graph are adequate for our framework to apply. Because of the natural isomorphism $\mathcal{P}(2 \times X) \cong \mathcal{P}(X + X) \cong \mathcal{P}X \times \mathcal{P}X$, one can represent $T$-graphs as structures $(X, R_0, R_1)$ for a set $X$ and two relations $R_0, R_1 \subseteq X \times X$. Graph homomorphisms are required to preserve the label $i \in \{0, 1\}$ of the binary relation $R_i$.

The graph $\Gamma(C_n(0))$, for $n \geq 1$, is isomorphic to the so-called de Bruijn graph $B(n) = (2^n, S_0, S_1)$ of dimension $n$ over the alphabet $2 = \{0, 1\}$ [dB46]. It is defined such that for $b \in 2$ and $w, v \in 2^n$ it holds that $wS_0v$ iff $w = ba$ and $v = ua$ for some $u \in 2^{n-1}$ and $a \in 2$. Following Theorem 4, we obtain the following characterization of the unification problem:

**Theorem 8.** For every formula $\phi$ of depth $\leq 1$ and $n \geq 0$ the ground $KdB$-unifiers of $\phi$ with depth $\leq n$ are in bijection with the graph homomorphisms from $B(n)$ to $\Gamma(P(\phi))$.

We have not yet been able to determine whether, given a $T$-graph of the form $\Gamma(P(\phi))$, it is decidable if there exist $n \geq 0$ and a homomorphism from $B(n)$ to $\Gamma(P(\phi))$.

Conclusion. We have shown that unifiability problems in non-transitive modal logics are equivalent to the existence of homomorphisms between certain graph-like structures. In the case of $Alt_1$, this analysis allowed us to prove the new result that the unifiability problem is PSPACE-hard. We also exhibit a new logic $KdB$, seemingly less complex than $K$, but for which unifiability is still not easily seen to be decidable.
While duality has previously been used in the context of unification problems, the main novelty here is to combine it with step by step approaches, which, as one reviewer noted, in particular avoids having to make explicit use of the profinite topology inherent to these problems (although we took crucial inspiration from the existing literature that is framed in the infinite topological setting).

As future work, we are interested in investigating how our approach can be adapted to normal modal logics that are not coalgebraic logics for some endofunctor. We also note that for the purposes of this paper we decided to focus only on the question of unifiability, but, as one of the reviewers suggested, it is natural to ask whether the methods outlined here might also be useful for determining unification type.

We hope that this paper can serve as a first step towards new methods for unification for non-transitive modal logics.

References


