Unification in Intuitionistic Logic

Author(s): Silvio Ghilardi

Source: *The Journal of Symbolic Logic*, Jun., 1999, Vol. 64, No. 2 (Jun., 1999), pp. 859-880

Published by: Association for Symbolic Logic

Stable URL: https://www.jstor.org/stable/2586506

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

Association for Symbolic Logic is collaborating with JSTOR to digitize, preserve and extend access to *The Journal of Symbolic Logic*

This content downloaded from 187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

THE JOURNAL OF SYMBOLIC LOGIC
Volume 64, Number 2, June 1999

UNIFICATION IN INTUITIONISTIC LOGIC

SILVIO GHILARDI

Abstract. We show that the variety of Heyting algebras has finitary unification type. We also show that the subvariety obtained by adding it De Morgan law is the biggest variety of Heyting algebras having unitary unification type. Proofs make essential use of suitable characterizations (both from the semantic and the syntactic side) of finitely presented projective algebras.

§0. Introduction. Unification under equational conditions (briefly, E-unification) is an important tool in equational reasoning whithin the point of view of automated deduction. Research on this field mainly concentates in two directions: general algorithms enumerating all E-unifiers of an E-unification problem (see, e.g., [20]) and specific algorithms for relevant special theories [1], [19]. One of the main results obtained within the second direction is the unitarity of Boolean unification [14]. This result, once translated in logical terms, says that for every formula A in classical propositional calculus, if there is a substitution making A a theorem in this calculus, then there is also 'the best' substitution with this property, i.e., there is a substitution σ such that $\sigma(A)$ is provable and any τ such that $\tau(A)$ is provable is, up to provable equivalence, an instantiation of σ.

We wonder whether the same property holds for other logical calculi. In the case of intuitionistic propositional calculus (IPC), the answer is negative, as the following simple counterexample shows. The formula $x \vee \neg x$ has unifiers (by this we mean substitutions making it a theorem in IPC)

$$\sigma_1 : x \mapsto \top, \quad \sigma_2 : x \mapsto \bot$$

(where $\top$ is 'syntactic truth' and $\bot$ is 'syntactic false') and there is no unifier more general than both because of the disjunction property of IPC. In fact, if

$$\vdash \sigma(x) \vee \neg\sigma(x)$$

then either $\vdash \sigma(x)$ (so that σ is equivalent to σ_1) or $\vdash \neg\sigma(x)$ (so that σ is equivalent to σ_2). We shall prove however in Section 3 that unification is rather nice in IPC too, because it is finitary (by this we mean that there are finitely many 'best unifiers'); the same finitarity results are obtained in [11] for some standard modal systems

Received January 22, 1997; revised September 10, 1997.
1991 *Mathematics Subject Classification.* Primary: 03B20, 68T15, Secondary: 03B55, 06D20, 08B30.
Key words and phrases. E-unification, projective Heyting algebras, exact formulas, admisssible inference rules.

© 1999, Association for Symbolic Logic
0022-4812/99/6402-0032/$3.20

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

extending K4. In Section 4, we shall also show that, by adding De Morgan law to IPC, we get a logic for which unification is unitary. Moreover, it will turn out that this logic is the smallest logic extending IPC and having unitary unification.

As unification for classical logic is the same as E-unification for Boolean algebras, unification in IPC is the same as E-unification for Heyting algebras. In fact, an arbitrary E-unification problem for the equational theory of Heyting algebras

$$A_1 =_E A_1', \ldots, A_n =_E A_n'$$

is equivalent to the E-unification problem (which is in fact a matching problem)

$$(A_1 \leftrightarrow A_1') \wedge \cdots \wedge (A_n \leftrightarrow A_n') =_E \top$$

and hence to the problem of making a single formula a theorem in the logical calculus.

We shall mainly stress here the relationship between unification and logical/algebraic aspects—algorithmic aspects will be better investigated in successive papers. In fact, the main reason for our finitarity unification results is due to an interesting syntactic property of IPC, which is emphasized in the proof of Theorems 3.5, namely the fact that any substitution making a formula A a theorem must make a theorem a formula in the projective approximation of A, which turns out to be finite. In algebraic terms, this means that any morphism

$$H \longrightarrow P$$

between finitely presented Heyting algebras having a free (or even a projective) algebra as codomain can be factored as

$$H \longrightarrow P' \longrightarrow P$$

where the first component is a surjective morphism, P' is finitely presented, projective and admitting a presentation of the same complexity as H.[1] For the special role played by projective algebras in the general theory of E-unification see [12], where in addition unification type in fragments of intuitionistic logic is characterized.

As a logical application of the finitarity results for unification, we mention the fact that an algorithm (like that described in Section 3 below) computing the finitely many maximal unifiers of a formula yields a new solution of Friedman problem [17] of recognizing admissibility of inference rules in IPC: in fact, it is sufficient to check whether the maximal unifiers for the premise are unifiers for the conclusion in order to decide whether a rule is admissible or not. This may be seen as a non-trivial example where concepts originated from computer science are useful in order to address logical problems.

We finally mention that the results from Section 2 below contain a solution to the syntactic and semantic characterization problem of exact formulas (in particular, a conjecture by De Jongh and Visser is proved to be correct).

[1] In the intuitionistic case, this result looks similar to a result by Pitts [15], [13], [23] showing (in algebraic terms) that the image factorization of a morphism between finitely presented Heyting algebras is again finitely presented. It can be shown (from the semantic characterization of projectivity given in Section 2 below) that if the codomain of the morphism is a projective algebra, then so is the image. However, the image factorization is not good enough for unification because it lacks the above mentioned property about complexity.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

The author wishes to thank A. Visser and the anonymous referee for information and suggestions.

§1. Preliminaries. Intuitionistic propositional formulas are built up from the propositional variables $x_1, x_2, \ldots, y_1, y_2, \ldots, z_1, z_2, \ldots$ by using the connectives $\top, \wedge, \bot, \vee, \rightarrow$. If A and B are formulas, $\neg A$ and $A \leftrightarrow B$ are defined as $A \rightarrow \bot$ and as $(A \rightarrow B) \wedge (B \rightarrow A)$. Strings of distinct variables are indicated by $\underline{x}, \underline{y}, \underline{z}$ and if A contains variables only from the list $\underline{x} = x_1, \ldots, x_n$, we express this fact by the notation $A(\underline{x})$ or $A(x_1, \ldots, x_n)$. $F(\underline{x})$ is the totality of formulas of the kind $A(\underline{x})$. Formulas in $F(\emptyset)$ are called ground formulas. For the description of axioms and inference rules in IPC the reader is referred to any textbook, like [8], [22]. We only recall the replacement theorem

$$A_1 \leftrightarrow B_1, \ldots, A_n \leftrightarrow B_n \vdash C(A_1/x_1, \ldots, A_n/x_n) \leftrightarrow C(B_1/x_1, \ldots, B_n/x_n)$$

(we use the notation $D_1, \ldots, D_n \vdash D$ to mean that $(D_1 \wedge \cdots \wedge D_n) \rightarrow D$ is provable in IPC, when $n = 0$ the empty conjunction is, by definition, equal to $\top$).

A *substitution* $\langle \underline{x}, \underline{y}, \sigma \rangle$ is a function

$$\sigma : \underline{x} \longrightarrow F(\underline{y}).$$

This function can be extended in the domain to $F(\underline{x})$ by (let us suppose that $\underline{x} = x_1, \ldots, x_n$)

$$\sigma(A(\underline{x})) = A(\sigma(x_1)/x_1, \ldots, \sigma(x_n)/x_n),$$

so that we often indicate a substitution by the notation $\sigma : F(\underline{x}) \longrightarrow F(\underline{y})$. In case domain and codomain can be deduced from the context, a substitution may be simply indicated by σ. The composition of the substitutions $\sigma : F(\underline{x}) \longrightarrow F(\underline{y})$ and $\tau : F(\underline{y}) \longrightarrow F(\underline{z})$ is the substitution $\tau\sigma : F(\underline{x}) \longrightarrow F(\underline{z})$ defined by $(\tau\sigma)(x) = \tau(\sigma(x))$ for all $x \in \underline{x}$. A substitution $\sigma_1 : F(\underline{x}) \longrightarrow F(\underline{y})$ is *less general* than a substitution $\sigma_2 : F(\underline{x}) \longrightarrow F(\underline{z})$ (in symbols $\sigma_1 \leq \sigma_2$) if and only if there is a substitution $\tau : F(\underline{z}) \longrightarrow F(\underline{y})$ such that for all $x \in \underline{x}$

$$\vdash \tau(\sigma_2(x)) \leftrightarrow \sigma_1(x).$$

A substitution $\sigma : F(\underline{x}) \longrightarrow F(\underline{y})$ is said to be a *unifier* for a formula $A(\underline{x})$ if and only if

$$\vdash \sigma(A).$$

A unifier σ_1 for A is *less general* than another unifier σ_2 for A if and only if σ_1 is less general than σ_2 as a substitution. A set S of unifiers for A is said to be a *complete set* of unifiers for A if every unifier for A is less general than a member of S. A complete set of unifiers for A is said to be a *basis* of unifiers for A if and only if its members are pairwise incomparable with respect to the preorder $\leq$. A unifier σ for A is said to be a *most general unifier* (mgu) for A if and only if $\{\sigma\}$ is a complete set of unifiers for A. The counterexample in the introduction shows that an mgu for A may not exist, we shall prove however in Section 3 that every *unifiable* formula A (i.e., every formula A admitting at least a unifier) admits a finite basis of unifiers. To do this it is clearly sufficient to exhibit a *finite* complete set S of unifiers for A (an algorithm producing such an S is said to be of type conformal in [19]).

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

We recall the basic facts concerning finitary Kripke semantics of intuitionistic logic. We deal with *finite rooted posets*, i.e., finite sets P endowed with a reflexive, transitive and antisymmetric relation $\leq$ for which there exists in P a greatest element ρ_P.[2] Such finite rooted posets are usually indicated by the letters $P, Q, \ldots$ and their underlying partial order relation is usually dropped in the notation. If confusion does not arise, the root of P is indicated simply with ρ. A finite *Kripke model* over $\underline{x}$ is a triple $\langle \underline{x}, P, u \rangle$, where $\underline{x}$ is a finite list of variables, P is a finite rooted poset and $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ is a map satisfying the monotonicity requirement

$$q \leq p \Longrightarrow u(q) \supseteq u(p)$$

(thus, for instance, the value of u at ρ_P is the smallest one). We indicate a Kripke model by $u : P \longrightarrow \mathscr{P}(\underline{x})$ and if $p \in P$, u_p denotes the Kripke model obtained from $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ by restricting u in the domain to the subset $\{ q \in P \mid q \leq p \}$ (this subset is regarded as a rooted poset with respect to the partial order obtained from the partial order of P by restriction).

If $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ is a Kripke model, $A \in F(\underline{x})$ and $p \in P$, the notion of A being *true at p in u* (in symbols $u \models_p A$) is inductively defined as follows:

$$\begin{array}{lll}
u \models_p x & \text{if and only if} & x \in u(p), \\
u \models_p \top, & & \\
u \not\models_p \bot, & & \\
u \models_p A_1 \wedge A_2 & \text{if and only if} & u \models_p A_1 \text{ and } u \models_p A_2, \\
u \models_p A_1 \vee A_2 & \text{if and only if} & u \models_p A_1 \text{ or } u \models_p A_2, \\
u \models_p A_1 \to A_2 & \text{if and only if} & \forall q \leq p\ (u \models_q A_1 \Longrightarrow u \models_q A_2).
\end{array}$$

It can be easily shown by induction that '*truth is stable*', i.e., that for all $A \in F(\underline{x})$, $p, q \in P$

$$(u \models_p A \text{ and } q \leq p) \Longrightarrow u \models_q A.$$

For a formula $A \in F(\underline{x})$, let A^* be $\{ u\colon P \longrightarrow \mathscr{P}(\underline{x}) \mid u \models A \}$, where $u \models A$ means that A is true at all points of P (or, equivalently, at the root). The fundamental result about finite Kripke models is the following Completeness/Finite Model Property Theorem (see [8] or [22] for a proof):

THEOREM 1. *For all $A, B \in F(\underline{x})$, we have that $A \vdash B$ if and only if $A^* \subseteq B^*$.*

We sometimes use the terminology 'A is contained in B' in order to say that $A \vdash B$, because if we think in terms of models, which are the 'duals' of formulas, provability of implication becomes inclusion (for a duality theory and related applications, see [13]).

We need some facts connecting Kripke models with substitutions. Given a substitution $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$, we can associate with a Kripke model $u\colon P \longrightarrow \mathscr{P}(\underline{y})$ a Kripke model $\sigma^*(u)\colon P \longrightarrow \mathscr{P}(\underline{x})$ as follows:

$$x \in \sigma^*(u)(p) \quad \text{if and only if} \quad u \models_p \sigma(x)$$

for all $x \in \underline{x}$ and $p \in P$ (notice that $\sigma^*(u)$ is really a Kripke model because of the stability of truth). Notice also that the function σ^* applied to models commute

[2] In standard literature, the role played by our $\leq$ is played by $\geq$, so usually the existence of a smallest element is required.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

with restriction, i.e., for every $p \in P$

$$(\sigma^*(u))_p = \sigma^*(u_p)$$

(this is due to the fact that truth of a formula at p is determined only by the value of u at points smaller than p). We shall often use this 'commutation with restrictions' property without explicit mention in the paper.

PROPOSITION 2. *Let $A \in F(\underline{x})$ be a formula and $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$ be a substitution. We have that*:

(i) *for every Kripke model $u\colon P \longrightarrow \mathscr{P}(\underline{y})$, $\sigma^*(u) \models A$ if and only if $u \models \sigma(A)$;*

(ii) *$\vdash \sigma(A)$ if and only if $\sigma^*(u) \models A$ holds for all $u\colon P \longrightarrow \mathscr{P}(\underline{y})$;*

(iii) *for every substitution $\tau\colon F(\underline{y}) \longrightarrow F(\underline{z})$ and for every Kripke model $v\colon Q \longrightarrow \mathscr{P}(\underline{z})$, $(\tau\sigma)^*(v) = \sigma^*(\tau^*(v))$.*

PROOF. (i) is established by proving inductively that $\sigma^*(u) \models_p A$ if and only if $u \models_p \sigma(A)$ for every $p \in P$. (ii) follows from (i) and Theorem 1. (iii) is shown as follows: For all $x \in \underline{x}$ and $q \in Q$: $x \in \sigma^*(\tau^*(v))(q)$ if and only if $\tau^*(v) \models_q \sigma(x)$ if and only if (by (i)) $v \models_q \tau(\sigma(x))$ if and only if (by definition of composition of substitutions) $v \models_q (\tau\sigma)(x)$ if and only if $x \in (\tau\sigma)^*(v)(q)$. ⊣

As an easy application, we show that a formula is unifiable if and only if it is satisfiable:

PROPOSITION 3. *$A(\underline{x})$ is unifiable if and only if $A^* \neq \emptyset$.*[3]

PROOF. If $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$ is a unifier for A, then A^* is not empty because it contains any model of the kind $\sigma^*(u)$. Conversely, if A^* is not empty, it surely contains a model w whose domain is the one-point poset (by truth-stability). Take the substitution $\sigma\colon F(\underline{x}) \longrightarrow F(\emptyset)$ defined by $\sigma(x) = \top$ if and only if $w \models x$, $\sigma(x) = \bot$ if and only if $w \not\models x$, for every $x \in \underline{x}$. Then σ is a unifier for A by Proposition 2 (ii) (notice that all models of the kind $\sigma^*(u)$ are constant maps with value $w(\rho)$, hence it can be easily seen that they do not differ from w as far as truth of formulas in $F(\underline{x})$ is concerned, so they are in A^* as w is). ⊣

In case we allow extra constants in the formulas, unifiability becomes a more serious problem. The related 'solving equations' theory has been developed by V. V. Rybakov (see, e.g., [16], [18], [17]).

§2. Projective formulas. Our first step is a characterization both from the syntactic and the semantic point of view of finitely presented projective Heyting algebras.[4] From a logical point of view the related definition is the following. A formula $A(\underline{x})$ is said to be *projective* if and only if there is a unifier $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{x})$ for it such that

$$(1) \qquad \forall x \in \underline{x} \quad A \vdash x \leftrightarrow \sigma(x)$$

[3]This means that A is unifiable if and only if $\nvdash \neg A$. But intuitionistic logic and classical logic agree on provability of negated formulas by Glivenko theorem [8], hence A is unifiable in intuitionistic logic if and only if A is unifiable in classical logic. Thus, intuitionistic and classical logic do not differ as far as mere unifiability is concerned.

[4]Finite projective Heyting algebras are described in [2].

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

holds. Such σ is automatically an mgu for A, because if τ is another unifier for A, then from (1) we get $\tau(A) \vdash \tau(x) \leftrightarrow \tau(\sigma(x))$, hence $\tau \leq \sigma$ because $\tau(A)$ is a theorem in IPC (as τ unifies A).

By the replacement theorem, condition (1) above is totally equivalent to the condition[5]

$$(1') \qquad \forall B \in F(\underline{x}) \quad A \vdash B \leftrightarrow \sigma(B).$$

Notice also that substitutions $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{x})$ satisfying (1) are *closed under composition*, independently on the fact whether they unify A or not. In fact, suppose that σ_1, σ_2 are two such substitutions; we get

$$A \vdash A \leftrightarrow \sigma_1(A)$$

from (1′) applied to σ_1, hence also $A \vdash \sigma_1(A)$. From (1) applied to σ_2, we obtain

$$\sigma_1(A) \vdash \sigma_1(x) \leftrightarrow \sigma_1(\sigma_2(x))$$

for all $x \in \underline{x}$. By transitivity, we get

$$A \vdash \sigma_1(x) \leftrightarrow \sigma_1(\sigma_2(x))$$

and finally

$$A \vdash x \leftrightarrow \sigma_1(\sigma_2(x))$$

by transitivity of $\leftrightarrow$ and by (1) applied to σ_1.

We can build substitutions satisfying (1) in the following way. Let a be a subset of $\underline{x}$; the substitution $\theta^a_A\colon F(\underline{x}) \longrightarrow F(\underline{x})$ is defined as follows:

$$\theta^a_A(x) = A \to x, \quad \text{if } x \in a;$$
$$\theta^a_A(x) = A \wedge x, \quad \text{if } x \notin a.$$

Clearly θ^a_A satisfies (1) and so does any composition of such substitutions.

LEMMA 1. *Let $A \in F(\underline{x})$, $a \subseteq \underline{x}$, $x \in \underline{x}$. We have that:*

(i) $\vdash \theta^a_A(x) \leftrightarrow \theta^a_A(\theta^a_A(x))$;

(ii) *for every other $b \subseteq \underline{x}$, $A \leftrightarrow \theta^b_A(A) \vdash \theta^b_A(\theta^a_A(x)) \leftrightarrow \theta^a_A(x)$.*

PROOF. From (1′), we get $A \vdash A \leftrightarrow \theta^a_A(A)$; now it is only an easy exercise in intuitionistic deduction to get what we need for (i), i.e.,

$$\vdash \quad (A \to x) \leftrightarrow (\theta^a_A(A) \to (A \to x));$$
$$\vdash \quad (A \wedge x) \leftrightarrow (\theta^a_A(A) \wedge (A \wedge x)).$$

For (ii) we need

$$A \leftrightarrow \theta^b_A(A) \vdash (\theta^b_A(A) \to \theta^b_A(x)) \leftrightarrow (A \to x);$$
$$A \leftrightarrow \theta^b_A(A) \vdash (\theta^b_A(A) \wedge \theta^b_A(x)) \leftrightarrow (A \wedge x),$$

which easily follows from (1) applied to θ^b_A. ⊣

From the semantic side we have the following Lemma:

[5]From this, it is easy to see that projective formulas have the disjunction property (the converse is false, see Example II in the next section): if A is projective and $A \vdash A_1 \vee A_2$, then $\vdash \sigma(A_1) \vee \sigma(A_2)$, hence $\vdash \sigma(A_i)$ ($i = 1$ or 2) because of the disjunction property of IPC. But $A \vdash A_i \leftrightarrow \sigma(A_i)$ by (1′), hence $A \vdash A_i$.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

LEMMA 2. *Let* $A \in F(\underline{x})$, $a \subseteq \underline{x}$, $u: P \longrightarrow \mathscr{P}(\underline{x})$ *be a Kripke model. We have that*:

(i) *if* $u \models A$ *then* $(\theta_A^a)^*(u) = u$;
(ii) *if* $u \not\models A$ *then* $(\theta_A^a)^*(u)(\rho) \subseteq a$;
(iii) $(\theta_A^a)^*((\theta_A^a)^*(u)) = (\theta_A^a)^*(u)$;
(iv) *given another* $b \subseteq \underline{x}$, *if for all* $p \in P$

$$(\theta_A^b)^*(u_p) \models A \quad \textit{if and only if} \quad u_p \models A,$$

then $(\theta_A^a)^*((\theta_A^b)^*(u)) = (\theta_A^a)^*(u)$.

PROOF. (i) and (ii) are trivial; (iii) and (iv) can be easily reduced to Lemma 1(i) and (ii), respectively through Proposition 2 (i) of Section 1 (it is not hard, however, to check them directly). For instance, in the case of (iv), the hypothesis 'for all $p \in P$, $(\theta_A^b)^*(u_p) \models A$ if and only if $u_p \models A$' implies $u \models \theta_A^b(A) \leftrightarrow A$, hence by Lemma 1 (ii) we have that for all $x \in \underline{x}$,

$$u \models \theta_A^b(\theta_A^a(x)) \leftrightarrow \theta_A^a(x),$$

i.e., $(\theta_A^a)^*((\theta_A^b)^*(u)) = (\theta_A^a)^*(u)$. ⊣

A Kripke model $u': P \longrightarrow \mathscr{P}(\underline{x})$ is said to be a *variant* of a Kripke model $u: P \longrightarrow \mathscr{P}(\underline{x})$ if and only if $u'(p) = u(p)$ holds for all $p \in P$ different from the root of P.

LEMMA 3. *Let* $A(\underline{x})$ *be a formula and let* $u: P \longrightarrow \mathscr{P}(\underline{x})$ *be a Kripke model such that* $u \not\models A$ *and such that* $u_p \models A$ *holds for all* $p \in P$ *different from* ρ_P. *If there is a variant* u' *of* u *which is a model of* A, *then for some* $a \subseteq \underline{x}$ *we have both* $(\theta_A^a)^*(u) \models A$ *and* $(\theta_A^a)^*(u)(\rho) = a$.

PROOF. Take $a = u'(\rho)$. We have $(\theta_A^a)^*(u_p) = u_p$ for all p different from the root by Lemma 2 (i). Moreover, for $x \in a$, $u \models A \to x$ (as $a \subseteq u'(p) = u(p)$ for all $p \neq \rho$, by the monotonicity of Kripke models) and for $x \notin a$, $u \not\models A \wedge x$. Hence $(\theta_A^a)^*(u) = u'$ and the Lemma is proved. ⊣

We now define a substitution θ_A as a suitable composition of the θ_A^a's. Let $a_1, \ldots, a_s$ be an ordering of all subsets of $\underline{x}$ satisfying the requirement:

$$a_i \subseteq a_j \Longrightarrow i \leq j \tag{2}$$

(we can easily get such ordering, starting, e.g., by $\emptyset$, then taking singletons, then pairs, etc.). We put $\theta_A = \theta_A^{a_s} \ldots \theta_A^{a_1}$. Notice that, by Proposition 2 (iii) of Section 1, we have $\theta_A^*(u) = (\theta_A^{a_1})^* \ldots (\theta_A^{a_s})^*(u)$ for every Kripke model u over $\underline{x}$. The reason why we took such an order in the composition is that we want the following property to hold:

LEMMA 4. *Let* $A(\underline{x})$ *be a formula and let* $u: P \longrightarrow \mathscr{P}(\underline{x})$ *be a Kripke model such that* $\theta_A^*(u) \models A$. *Let* $i = 1, \ldots, s$ *be such that* $a_i \subseteq \theta_A^*(u)(\rho)$. *Then we have that* $(\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \models A$.

PROOF. Suppose not; in this case let $1 \leq j < i$ be the maximum index such that $(\theta_A^{a_j})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \models A$ holds (such j exists because $\theta_A^*(u) \models A$). By Lemma 2 (ii) and (i), $\theta_A^*(u)(\rho) \subseteq a_j$, yielding $a_i \subseteq a_j$ in contrast to (2). ⊣

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

A class K of Kripke models over $\underline{x}$ is said to have the *extension property* if and only if for every Kripke model $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ such that $u_p \in K$ for all $p \in P$ different from ρ_P, there is a variant u' of u which belongs to K.

THEOREM 5. *For a formula $A(\underline{x})$ the following conditions are equivalent*:

(i) *θ_A is a unifier for A*;
(ii) *A is projective*;
(iii) *A^* has the extension property.*

PROOF. (i) $\Longrightarrow$ (ii) follows from the fact that θ_A satisfies (1), as a composition of substitutions satisfying (1).

In order to prove that (ii) $\Longrightarrow$ (iii), suppose that σ is a unifier for A satisfying (1) and take a Kripke model $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ such that $u_p \in A^*$ for all p different from the root. We have that $\sigma^*(u) \in A^*$ because σ is a unifier for A (recall Proposition 2 (ii) from Section 1). It is sufficient to show that $\sigma^*(u)$ is a variant of u: this follows from the fact that $\sigma^*(u)_p = \sigma^*(u_p)$ for all $p \in P$ and from the fact that if $w \in A^*$ then $\sigma^*(w) = w$ for every Kripke model $w\colon Q \longrightarrow \mathscr{P}(\underline{x})$ (in fact, for every $q \in Q$, $x \in \underline{x}$, $x \in \sigma^*(w)(q)$ if and only if $w_q \models \sigma(x)$ if and only if $w_q \models x$ because w is a model of A and because σ satisfies (1)).

Let us finally show that (iii) $\Longrightarrow$ (i): suppose that $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ is a Kripke model. Our aim consists in showing that $\theta_A^*(u) \models A$ (see Proposition 2 (ii) of Section 1). Suppose not. We can freely assume that $\theta_A^*(u_p) \models A$ holds for all p different from the root because our posets are finite (indeed, if this is not the case for u, it will be the case for some restriction of u to some point of P). As A^* has the extension property, by Lemma 3 there is $i = 1, \ldots, s$ such that $(\theta_A^{a_i})^*(\theta_A^*(u)) \models A$ and $a_i = (\theta_A^{a_i})^*(\theta_A^*(u))(\rho)$, hence $a_i \subseteq \theta_A^*(u)(p)$ for all p different from the root because Kripke models are monotonic and because of Lemma 2 (i). By Lemma 4,

$$(\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u_p) \models A$$

for all p different from the root of P. Now we can repeatedly apply the hypothesis of Lemma 2 (iv) to all Kripke models

$$(\theta_A^{a_j})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \quad (1 < j \leq i)$$

relatively to $\theta_A^a = \theta_A^{a_i}$ and $\theta_A^b = \theta_A^{a_{j-1}}$ (in fact, A is true at points different from the root and false at the root both for $(\theta_A^{a_j})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u)$ and for $(\theta_A^{a_{j-1}})^*(\theta_A^{a_j})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u)$). We get:

$$\begin{aligned}
(\theta_A^{a_i})^*(\theta_A)^*(u) &= (\theta_A^{a_i})^*(\theta_A^{a_1})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \\
&= (\theta_A^{a_i})^*(\theta_A^{a_2})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \\
&= (\theta_A^{a_i})^*(\theta_A^{a_3})^* \ldots (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \\
&\vdots \\
&= (\theta_A^{a_i})^*(\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \\
&= (\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u)
\end{aligned}$$

because of Lemma 2 (iii). So from $(\theta_A^{a_i})^*\theta_A^*(u) \models A$ and the above equations, we get $(\theta_A^{a_i})^* \ldots (\theta_A^{a_s})^*(u) \models A$, hence also $\theta_A^*(u) \models A$ by Lemma 2 (i), contradiction. ⊣

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

Theorem 5 shows that in order to decide whether A is projective, it is sufficient to check whether θ_A is a unifier for it (notice that in this case, as θ_A satisfies (1), it is automatically an mgu for A). In many concrete cases (but not always) it is sufficient to apply θ_A^a for a single suitably chosen $a \subseteq \underline{x}$ in order to get a unifier showing that A is projective. Kripke models may be of some help in guessing such a.

EXAMPLE 1. $A = \bigwedge_{i=1}^n (x_i \to A_i)$ is projective and has $\theta_A^\emptyset$ as mgu ($\theta_A^\emptyset(A)$ is equal to $\bigwedge_{i=1}^n (x_i \wedge A \to \theta_A^\emptyset(A_i))$, which is a theorem in IPC by (1′)). This is related to the fact that if for a Kripke model u, we have that $u_p \models A$ for all p different from the root, then we can get a variant u' of u which is a model of A by putting $u'(\rho) = \emptyset$.

EXAMPLE 2. $A = \bigwedge_{i=1}^n (A_i \to x_i)$ is projective and has mgu $\theta_A^{\{x_1,\dots,x_n\}}$: in fact, $\theta_A^{\{x_1,\dots,x_n\}}(A)$ is equal to

$$\bigwedge_{i=1}^n \left(\theta_A^{\{x_1,\dots,x_n\}}(A_i) \to (A \to x_i)\right),$$

which is a theorem in IPC by (1′). An observation like the above one holds for the related Kripke models (this time, we put $x_i \in u'(\rho)$, 'whenever possible').

EXAMPLE 3. $A = (\neg y \to (x \wedge z_1)) \wedge (x \to (z_1 \vee z_2))$ is projective and it can be checked that it has mgu $\theta_A^{\{x,z_1\}}\theta_A^\emptyset$; no single θ_A^a is sufficient in order to unify A. Moreover, $\theta_A^\emptyset\theta_A^{\{x,z_1\}}$ is not a unifier for A (this shows that the order in the composition can be essential).

EXAMPLE 4. Negated formulas $A = \neg B$ are all projective (provided they are satisfiable): they have as mgu any θ_A^a such that the one-point poset with value a is a model for A. In fact, notice that for every Kripke model u, $u \models A$ if and only if $u \models_p A$ holds for all minimal points p in the domain of u. Consequently, $(\theta_A^a)^*(u)$ is always a model of A, so that $\vdash \theta_A^a(A)$.

REMARK ([12] (on Boolean unification)). The unitarity of Boolean unification is due to the fact that all satisfiable (i.e., unifiable) formulas in classical logic are projective (this is the same as the algebraic fact that all non-degenerated finitely presented Boolean algebras are projective). A proof of this statement can be deduced from Example 4 above, together with the obvious observation that all formulas are equivalent in classical logic to a negated formula (notice that formulas which are projective in IPC are projective in classical propositional calculus too, although not conversely). Alternatively, it is possible to show syntactically that θ_A^a unifies A in classical logic, in case the two-valued assignement giving value 1 to the variables in a and 0 to the variables not in a satisfies A (use (1′) and conjunctive normal forms to check it). Notice that the formula for most general unifiers in classical logic given in [14] through 'Löwenheim approach' is exactly our θ_A^a (the only apparent difference lies in a dual formulation of the unification problems).

REMARK (on exact formulas). Exact formulas were introduced in [3]. Following [5], [4], we say that a formula $A(\underline{x})$ is *exact* (with respect to IPC) if and only if there is a unifier $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$ for A such that for all $B(\underline{x})$, $\vdash \sigma(B)$ implies $A \vdash B$. In other words, A is exact if and only if it represents the theory of a substitution.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

By Pitts Theorem [15], any substitution σ, seen as an order-preserving map

$$\sigma\colon \langle F(\underline{x}), \vdash\rangle \longrightarrow \langle F(\underline{y}), \vdash\rangle,$$

has a left adjoint $\exists_\sigma$, consequently it immediately follows from the definition of adjoint that exact formulas are just formulas of the kind $\exists_\sigma(\top)$, for some substitution σ. Clearly projective formulas are exact, because if A is projective and σ is a unifier for A satisfying (1), then $\vdash A \leftrightarrow \exists_\sigma(\top)$. On the other hand, by the duality theory of [13], for any substitution $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$, $(\exists_\sigma(\top))^*$ is the sheaf image of σ^* (alternatively, following [23], it is the bisimulation closure of the class $\{\sigma^*(u) \mid u\colon P \longrightarrow \mathscr{P}(\underline{y})\}$), hence it is easily seen that it has the extension property.[6] Thus, *exact formulas are the same as projective formulas* by Theorem 2.5. Condition 2.5 (i) gives a syntactic characterization and a decision procedure, whereas condition 2.5 (iii) gives the corresponding semantic characterization, thus solving positively a conjecture by de Jongh and Visser.[7]

§3. **Intuitionistic unification.** The (implicational) complexity $c(A)$ of a formula A is defined inductively as follows:

- $c(A) = 0$, if A is a propositional variable or $\bot$ or $\top$,
- $c(A_1 * A_2) = \max\big(c(A_1), c(A_2)\big)$ for $* = \wedge, \vee$,
- $c(A_1 \to A_2) = 1 + \max\big(c(A_1), c(A_2)\big)$.

It is evident that the number of non provably equivalent formulas in the variables $\underline{x}$ and whose complexity is less or equal to a fixed natural number is finite. However, the number of such non provably equivalent formulas grows quite fast in dependence on the complexity of the formula. No precise upper bound is known, better than the obvious tower of exponentials. A direct description in terms of the dual poset of the finite lattice of equivalence classes of formulas of bounded complexity is given in [21], [10].

We shall prove, for every formula $A(\underline{x})$, that each unifier σ for A is also a unifier for a projective formula $B(\underline{x})$ contained in A[8] and such that $c(B) \leq c(A)$, so that σ is *less general than an mgu for* B (which is also a unifier for A, as $B \vdash A$). From this and Theorem 2.5 it immediately follows that unification is finitary in intuitionistic logic and that complete sets of unifiers can be effectively computed.

We need some extra basic information about Kripke models, in order to relate them to complexity of formulas. We shall remind a necessary and sufficient criterion in order to recognize for every $n \geq 0$ whether a class of Kripke models is of the form A^* for a formula A whose complexity does not exceed n.

The notion of n-equivalence (*bounded bisimulation*) between two Kripke models $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ and $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$ was introduced in modal logic by K. Fine [6], [7] by imitating Ehrenfeucht games. Here you are the related version for

[6]This last statement is checked during the proof of Theorem 3.5 below. The notion of bisimulation is also recalled in Section 3.

[7]In his original paper [3], deJongh introduced an apparently different notion, namely exactness with respect to Heyting arithmetic HA. In earlier work by deJongh and Visser, it was established that: (i) IPC-exactness implies HA-exactness; (ii) the class of Kripke models of an HA-exact formula has the extension property. Thus, by Theorem 2.5, *a formula is HA-exact if and only if it is IPC-exact.*

[8]Recall from Section 1 that 'B is contained in A' means $B \vdash A$.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

intuitionistic logic. Define:

$$\begin{aligned} u \sim_0 v \quad & \text{if and only if} \quad u(\rho) = v(\rho); \\ u \sim_{n+1} v \quad & \text{if and only if} \quad \forall p \in P\ \exists q \in Q\ u_p \sim_n v_q \text{ and vice versa}; \\ u \leq_0 v \quad & \text{if and only if} \quad u(\rho) \supseteq v(\rho); \\ u \leq_{n+1} v \quad & \text{if and only if} \quad \forall p \in P\ \exists q \in Q\ u_p \sim_n v_q. \end{aligned}$$

From the definition, it is clear that for every $n \geq 0$, $\sim_n$ is an equivalence relation and that $\leq_n$ is a preorder (i.e., reflexive and transitive) relation. Notice that $u \sim_{n+k} v$ implies $u \sim_n v$ for all n, k (for $n = 0$, use the fact that Kripke models are monotonic maps). Notice also that $u \sim_n v$ is equivalent to the conjunction of $u \leq_n v$ and $v \leq_n u$. Finally, it is easily established, by induction on n, that there are only finitely many non n-equivalent Kripke models over $\underline{x}$ for every $n \geq 0$. Next two Propositions can be found, e.g., in [13], [23].

PROPOSITION 1. *Fix $n \geq 0$ and two Kripke models $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ and $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$. We have that $v \leq_n u$ if and only if for all formulas $A(\underline{x})$ such that $c(A) \leq n$ ($u \models A$ implies $v \models A$).*

PROOF. The left-to-right side is a quite simple induction on n. For the right-to-left side, it is sufficient to introduce for every n, $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ a formula X_u^n (called the n-character of u) of complexity less or equal to n such that

$$v \models X_u^n \quad \text{if and only if} \quad v \leq_n u \tag{1}$$

holds for every Kripke model $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$. This is done as follows: while defining X_u^n, we simultaneously check that $X_{u_1}^n$ is equal to $X_{u_2}^n$ in case $u_1 \sim_n u_2$. For $n = 0$, X_u^0 is $\bigwedge_{x \in u(\rho)} x$: clearly (1) is satisfied. Now put

$$X_u^{n+1} = \bigwedge_{\{\, u' \mid \forall p \in P\ u' \not\sim_n u_p \,\}} \left(X_{u'}^n \to \bigvee_{\{\, w \mid u' \not\leq_n w \,\}} X_w^n \right). \tag{2}$$

Notice that all conjunctions and disjunctions involved are finite, because there are only finitely many non n-equivalent Kripke models and because n-equivalent Kripke models have the same n-character (it is understood that in (2), we do not write down twice an identical conjunct or disjunct).[9] Moreover, if $u_1 \sim_{n+1} u_2$, then $X_{u_1}^{n+1}$ is equal to $X_{u_2}^{n+1}$ because the index sets of the conjunction in (2) are the same. We finally prove (1) for X_u^{n+1} (we assume it holds for $X_{u'}^n$ for all u'). Suppose that $v \leq_{n+1} u$ and take u' such that for every point p in the domain of u, $u' \not\sim_n u_p$. We show that

$$v \models X_{u'}^n \to \bigvee_{\{\, w \mid u' \not\leq_n w \,\}} X_w^n.$$

To check it, take a point q in the domain of v and suppose that $v_q \models X_{u'}^n$, i.e., that that $v_q \leq_n u'$. Now from $v \leq_{n+1} u$ we conclude that there exists p such that

[9] More explicitly: $\bigvee_{\{\, w \mid u' \not\leq_n w \,\}} X_w^n$ is a finite disjunction for each u'. Moreover, if $u_1' \sim_n u_2'$, then $X_{u_1'}^n \to \bigvee_{\{\, w \mid u_1' \not\leq_n w \,\}} X_w^n$ is equal to $X_{u_2'}^n \to \bigvee_{\{\, w \mid u_2' \not\leq_n w \,\}} X_w^n$, so there are only finitely many conjuncts in (2).

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

$v_q \sim_n u_p$. Consequently, $u' \not\leq_n v_q$ (otherwise $v_q \sim_n u'$ and so $u' \sim_n u_p$, which contradicts the choice of u') and so

$$v_q \models \bigvee_{\{ w | u' \not\leq_n w \}} X^n_w,$$

by induction hypothesis applied to v_q. Vice versa, suppose that $v \not\leq_{n+1} u$. It follows that there is a point q in the domain of v such that for every point p in the domain of u, $v_q \not\sim_n u_p$. We check that

$$v \not\models X^n_{v_q} \rightarrow \bigvee_{\{ w | v_q \not\leq_n w \}} X^n_w.$$

This is clear as (by induction hypothesis applied to v_q) $v_q \models X^n_{v_q}$ and $v_q \not\models \bigvee_{\{ w | v_q \not\leq_n w \}} X^n_w$. ⊣

PROPOSITION 2. *A class K of Kripke models over $\underline{x}$ is of the form A^* for a formula $A(\underline{x})$ such that $c(A) \leq n$ if and only if it satisfies the following $\leq_n$-closure condition:*

$$(u \in K \text{ and } v \leq_n u) \Longrightarrow v \in K,$$

for all Kripke models u, v over $\underline{x}$.

PROOF. One side is clear from the easy part of the previous Proposition; for the other one, suppose that K is $\leq_n$-closed, take $A = \bigvee_{v \in K} X^n_v$ (which is a finite disjunction, provided we do not write down many times the same disjunct) and apply (1) in order to show that $K = A^*$. ⊣

For a class K of Kripke models over $\underline{x}$, put

$$\langle K \rangle_n = \{ v \colon Q \longrightarrow \mathscr{P}(\underline{x}) \mid \exists u \in K \; v \leq_n u \}.$$

It is obvious that $\langle K \rangle_n$ is the smallest $\leq_n$-closed class of Kripke models over $\underline{x}$ extending K.

A class K of Kripke models over $\underline{x}$ is called *stable* if and only if for all $u \colon P \longrightarrow \mathscr{P}(\underline{x})$

$$u \in K \Longrightarrow u_p \in K$$

for all $p \in P$. If $\{w_i \colon P_i \longrightarrow \mathscr{P}(\underline{x})\}_i$ is a finite set of Kripke models, the Kripke model $(\sum_i w_i)^+$ is so defined: we take the disjoint union of the P_i's, we add it a new root (this poset is indicated with $(\sum_i P_i)^+$) and then we extend the w_i's by giving the new root the value $\emptyset$.

LEMMA 3. *Let K be a stable class of Kripke models over $\underline{x}$. If K has the extension property, so does $\langle K \rangle_n$ for every $n \geq 0$.*

PROOF. We show separately the case $n = 0$. Notice that if K has the extension property, then the set

$$\{ b \subseteq \underline{x} \mid \exists v \in K \; v(\rho) = b \}$$

has a smallest element a: to show it, recall the monotonicity of Kripke models and simply consider a variant in K of $(\sum_b v^b)^+$, where the index set is

$$\{ b \subseteq \underline{x} \mid \exists v \in K \; v(\rho) = b \}$$

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

and v^b is any chosen Kripke model in K such that $v^b(\rho) = b$. It turns out that $\langle K\rangle_0 = \{ u \mid u(\rho) \supseteq a \}$ and this class obviously has the extension property.

Let us now turn to the more interesting case $n > 0$. Let $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ be such that $u_p \in \langle K\rangle_n$ for all p different from the root of P. We look for a variant of u belonging to $\langle K\rangle_n$. According to the definition of $\langle K\rangle_n$, for every $p \in P$ different from the root, u_p is n-less or equal to a Kripke model in K, hence in particular, as K is stable, for every $p \in P$ different from the root there is $w^p\colon Q^p \longrightarrow \mathscr{P}(\underline{x})$ in K such that $u_p \sim_{n-1} w^p$. Now take $(\sum_p w^p)^+$: surely a variant w' of this model belongs to K as K has the extension property. Define a variant u' of u by putting $u'(\rho) = w'(\rho)$: notice that this definition really gives a Kripke model, because the monotonicity requirement is fullfilled (for every point $p \in P$ different from the root, $u_p \sim_{n-1} w^p$, hence $u(p) = w^p(\rho) \supseteq w'(\rho) = u'(\rho)$). We show that $u' \leq_n w'$, hence $u' \in \langle K\rangle_n$. By construction, it is clearly sufficient to show that $u' \sim_{n-1} w'$. We prove that

$$u' \sim_k w'$$

for all $k = 0, \ldots, n-1$ by induction on k. For $k = 0$, $u' \sim_0 w'$ holds by the definition of u'. For $k > 0$, we must show that:

(i) for all $p \in P$ there is $q \in (\sum_p Q^p)^+$ such that $u'_p \sim_{k-1} w'_q$;

(ii) for all $q \in (\sum_p Q^p)^+$ there is $p \in P$ such that $u'_p \sim_{k-1} w'_q$.

(i) is trivial: if $p = \rho$ we take $q = \rho$ and apply induction; if $p \neq \rho$, then $u'_p = u_p \sim_{n-1} w^p$, so we can take q equal to the root of Q^p (recall that $n - 1 \geq k - 1$).

(ii) is established as follows: if $q = \rho$, we again take $p = \rho$. If $q < \rho$, then $q \in Q^{p'}$ for some $p' \in P$ different from the root. But $w^{p'} \sim_{n-1} u_{p'}$, hence there is $p \leq p'$ such that

$$w'_q = (w^{p'})_q \sim_{n-2} (u_{p'})_p = u_p = u'_p.$$

This p is a good choice as $n - 2 \geq k - 1$. ⊣

For $u\colon P \longrightarrow \mathscr{P}(\underline{x})$, $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$, put $u \sim_\infty v$ (*u bisimulates v*) if and only if for all $n \geq 0$, $u \sim_n v$.

LEMMA 4. *Let $u\colon P \longrightarrow \mathscr{P}(\underline{x})$ and $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$ be Kripke models.*

(i) *$u \sim_\infty v$ if and only if for every $p \in P$ there is $q \in Q$ such that $u_p \sim_\infty v_q$ and vice versa;*

(ii) *$u \sim_\infty v$ if and only if ($u \sim_0 v$ and for every $p \in P$ different from the root there is $q \in Q$ such that $u_p \sim_\infty v_q$ and vice versa).*

PROOF. (i) is because our posets are finite. The left-to-right side of (ii) follows from (i) and the right-to-left side is easily obtained by showing by induction on n that $u \sim_n v$. ⊣

THEOREM 5. *Each unifiable formula $A(\underline{x})$ admits a finite complete set of unifiers.*

PROOF. Let $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$ be a unifier for A and let $n = c(A)$. As we mentioned above, the Theorem is proved once we show that there is a projective formula $B(\underline{x})$ such that $B \vdash A$, $c(B) \leq n$ and σ is a unifier for B.

Take

$$K = \{ v\colon Q \longrightarrow \mathscr{P}(\underline{x}) \mid \exists u\colon P \longrightarrow \mathscr{P}(\underline{y}) \text{ s.t. } v \sim_\infty \sigma^*(u) \}.$$

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

K is stable by Lemma 4 (i):[10] in fact, if $v \sim_\infty \sigma^*(u)$, then for all q in the domain of v there is p in the domain of u such that $\sigma^*(u_p) = \sigma^*(u)_p \sim_\infty v_q$.

We show that K also has the extension property. Suppose that for $v\colon Q \longrightarrow \mathscr{P}(\underline{x})$ we have that $v_q \in K$ for all $q \in Q$ different from the root. For all such q there are Kripke models $u^q\colon P^q \longrightarrow \mathscr{P}(\underline{y})$ such that $\sigma^*(u^q) \sim_\infty v_q$. Now take the Kripke model $u = (\sum_q u^q)^+$ and define a variant v' of v by putting $v'(\rho) = \sigma^*(u)(\rho)$: notice that this is really a Kripke model (i.e., a monotonic map), because for all $q \neq \rho_Q$, $v_q \sim_\infty \sigma^*(u^q)$ and $\sigma^*(u^q)$ is equal to $\sigma^*(u)$ restricted to the root of P^q, hence $v(q) = \sigma^*(u^q)(\rho) \supseteq \sigma^*(u)(\rho)$. We use Lemma 4 (ii) in order to show that $v' \sim_\infty \sigma^*(u)$: in fact they agree at the root. Moreover, if we pick $q \in Q$ different from the root, by construction there is $p \in (\sum_q P^q)^+$ (namely the root of P^q) such that

$$v'_q = v_q \sim_\infty \sigma^*(u^q) = \sigma^*(u_p) = \sigma^*(u)_p.$$

Conversely, each $p \in (\sum_q P^q)^+$ different from the root is less or equal to the root of $P^{q'}$ for some $q' \in Q$ different from the root of Q, hence as $v_{q'} \sim_\infty \sigma^*(u^{q'})$, by Lemma 4 (i) there is $q \leq q'$ such that

$$v'_q = v_q \sim_\infty \sigma^*(u^{q'})_p = \sigma^*((u^{q'})_p) = \sigma^*(u_p) = \sigma^*(u)_p.$$

This shows that $v' \in K$, so that K has the extension property.

The hypotheses of Lemma 3 can be applied to K, hence $\langle K\rangle_n$ has the extension property. By Proposition 2, $\langle K\rangle_n = B^*$ for some formula B whose complexity is less or equal to n and which is also projective by Theorem 5 of Section 2. Moreover σ is a unifier for B because for every $u\colon P \longrightarrow \mathscr{P}(\underline{y})$, $\sigma^*(u) \in K \subseteq B^*$. It remains to show that $B \vdash A$.

As σ is a unifier for A, we have that $\sigma^*(u) \models A$ for every Kripke model $u\colon P \longrightarrow \mathscr{P}(\underline{y})$, consequently $K \subseteq A^*$ (in fact, A^* is $\leq_n$-closed, contains all $\sigma^*(u)$ and hence also all models infinitely equivalent to those of the kind $\sigma^*(u)$); as $c(A) \leq n$, $\langle K\rangle_n \subseteq A^*$ because $\langle K\rangle_n$ is the smallest $\leq_n$-closed class containing K. We so have that $B^* \subseteq A^*$, that is $B \vdash A$ by Theorem 1 of Section 1. ⊣

According to the above proof of Theorem 5, given any unifiable formula $A(\underline{x})$, one gets a complete set of unifiers for A by taking $\{\theta_C \mid C \in S_A\}$, where

$$S_A = \{C \in F(\underline{x}) \mid C \vdash A,\ C \text{ is projective and } c(C) \leq c(A)\}.$$

$\{\theta_C \mid C \in S_A\}$ is usually not a basis of unifiers for A. In fact it is not difficult to show, by using (1′) of Section 2, that if $B_1(\underline{x})$, $B_2(\underline{x})$ are both projective, then[11]

$$B_1 \vdash B_2 \quad \text{if and only if} \quad \theta_{B_1} \leq \theta_{B_2}. \tag{3}$$

Thus, if two elements of S_A are $\vdash$-comparable, their corresponding most general unifiers are comparable too. This suggests the following definition. For a formula

[10] It can be shown that K is of the form C^* for some formula C (the related argument, which is not immediate, is in [13], [23]). However, the complexity of such C can be very high and depends on the complexity of σ.

[11] On one side, suppose that $B_1 \vdash B_2$: as $B_2 \vdash x \leftrightarrow \theta_{B_2}(x)$ for all $x \in \underline{x}$, we get $\theta_{B_1}(B_2) \vdash \theta_{B_1}(x) \leftrightarrow \theta_{B_1}(\theta_{B_2}(x))$, so $\theta_{B_1} \leq \theta_{B_2}$ because $\theta_{B_1}(B_2)$ is a theorem in IPC. On the other side, if $\theta_{B_1} \leq \theta_{B_2}$, then there is σ such that θ_{B_1} is equivalent to $\sigma\theta_{B_2}$. In particular, we have that $\vdash \theta_{B_1}(B_2) \leftrightarrow \sigma(\theta_{B_2}(B_2))$, that is $\vdash \theta_{B_1}(B_2)$. By (1′) of Section 2, we can conclude $B_1 \vdash B_2$.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

$A(\underline{x})$, a *projective approximation* of A is any subset Π_A of S_A satisfying the two conditions:

- if $C_1, C_2 \in \Pi_A$ and $C_1 \vdash C_2$, then $C_1 = C_2$;
- for any $D \in S_A$ there is $C \in \Pi_A$ such that $D \vdash C$.

In other words, a projective approximation of A is obtained by picking exactly one formula from each $\vdash$-maximal class of provably equivalent formulas in S_A.[12] For this reason, the projective approximation Π_A of A is unique, up to provable equivalences. In conclusion, by (3) above, we have that $\{ \theta_C \mid C \in \Pi_A \}$ *is a basis of unifiers for each unifiable formula* A. This observation gives a (quite heavy) algorithm in order to compute a basis of unifiers for a given formula A; next examples show that in concrete cases it is often possible, by using Kripke models, to avoid the expensive check of projectivity for all the formulas of complexity less or equal to the complexity of A.

EXAMPLE 1. $A = x \vee \neg x$ is not projective; it can be shown that if B is projective and $B \vdash A$, then ($B \vdash x$ or $B \vdash \neg x$): in fact, suppose not, then by the Completeness Theorem there are Kripke models v_1, v_2 of B such that $v_1 \not\models x$ and $v_2 \not\models \neg x$. As B is projective, there must be a model of B which is a variant of $(v_1 + v_2)^+$, but this is in contrast to $B \vdash A$. So $\{x, \neg x\}$ is the projective approximation of A, that is x and $\neg x$ are the maximal projective formulas contained in A and A has a basis of unifiers consisting on the mgu's of x and $\neg x$, which are $x \mapsto \top$ and $x \mapsto \bot$, respectively.

EXAMPLE 2. $A = \neg x \to (y \vee z)$ has projective approximation given by $\{A_1, A_2\}$, where $A_1 = \neg x \to y$ and $A_2 = \neg x \to z$ (the argument is similar to the above one). So by Example 2 of Section 2, A has a basis of unifiers given by $\theta_{A_1}^{\{y\}}$ and $\theta_{A_2}^{\{z\}}$. Notice that A is not projective, but has the disjunction property, because for every Kripke models v_1, v_2 of A, there is a Kripke model of A which is a variant of $(v_1 + v_2 + w)^+$ for a suitable $w \in A^*$.

EXAMPLE 3. Here we show an example of a formula A which is not projective but admits a most general unifier. Let

$$A_1 = x \to \bigvee_{i=1}^{3} y_i$$

$$A_2 = \bigwedge_{i=1}^{3} \left(\neg y_i \to \bigvee_{j \neq i} y_j \right) \wedge \bigwedge_{i=1}^{3} \left(y_i \to \bigwedge_{j \neq i} \neg y_j \right)$$

$$A = A_1 \vee A_2$$

A is not projective because it does not have the disjunction property, as $A \vdash A_1 \vee A_2$ but $A \nvdash A_1$, $A \nvdash A_2$ (this is shown by exhibiting suitable Kripke models). We know from Example 1 in Section 2 that A_1 is projective. By making use of Kripke models it is possible to show that if B is projective and $B \vdash A_2$, then $B \vdash \bigvee_{i=1}^{3} y_i$ (the

[12] To be $\vdash$-maximal in this set is the same as to be $\vdash$-maximal in the set (which usually is infinite, however, even after identification of provably equivalent formulas) $\{ C \in F(\underline{x}) \mid C \vdash A$ and C is projective $\}$, because if $C(\underline{x})$ is projective and $C \vdash A$, then θ_C is a unifier for A, hence it is less general than the mgu $\theta_{C'}$ for some projective $C'(\underline{x})$ contained in A and such that $c(C') \leq c(A)$. But $\theta_C \leq \theta_{C'}$ implies that $C \vdash C'$ (see (3) above).

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

argument is of the same kind as the above ones, although the details are a little longer). As projective formulas have the disjunction property and as $\bigvee_{i=1}^{3} y_i \vdash A_1$, we can conclude that if B is projective and $B \vdash A$, then $B \vdash A_1$. So A does have an mgu, the same as the mgu of A_1 computed in Section 2, Example 1.

REMARK (on admissibility of inference rules). An inference rule $A_1(\underline{x})/A_2(\underline{x})$ is said to be *admissible* in IPC if and only if every unifier for A_1 is also a unifier for A_2. From the information we obtained, it follows that *the rule* $A_1(\underline{x})/A_2(\underline{x})$ *is admissible in* IPC *if and only if all formulas belonging to the projective approximation of* A_1 *are contained in* A_2. In fact, if this condition is satisfied then the rule is admissible, because we know from the proof of Theorem 5 that each unifier σ for the premise A_1 is also a unifier for a projective formula $B \in \Pi_{A_1}$, thus from $B \vdash A_2$ we can conclude that σ unifies the conclusion A_2. Vice versa, suppose that the rule is admissible and take a formula $B(\underline{x})$ in the projective approximation of A_1. As θ_B unifies B and consequently also A_1, we must have that $\theta_B(A_2)$ is a theorem in IPC. But $B \vdash \theta_B(A_2) \leftrightarrow A_2$ by (1′) of Section 2, hence $B \vdash A_2$, as claimed. We can summarize the content of the present remark by saying that the inclusion $\langle F(\underline{x}), \vdash\rangle \hookrightarrow \langle F(\underline{x}), \vdash_a\rangle$ has a left adjoint, namely the disjunction of the formulas in the projective approximation (here $A_1 \vdash_a A_2$ means that the rule A_1/A_2 is admissible).

§4. Unification with De Morgan axiom. An *intermediate logic* (briefly, a *logic*) L is a set of formulas containing all theorems of IPC and closed under modus ponens rule ($A \in L$ and $A \to B \in L$ imply $B \in L$) and substitution rule ($A \in L$ implies $\sigma(A) \in L$ for all substitutions σ). By $A \vdash_L B$ we mean that $A \to B \in L$. We recall that the cardinality of intermediate logics has the power of the continuum. Among them, we have *De Morgan logic* (or *weak excluded middle logic*) DM, which is axiomatized by adding to IPC one of the two following equivalent axiom schemata

$$\neg(A \wedge B) \to (\neg A \vee \neg B), \qquad \neg A \vee \neg\neg A.$$

We can define projective formulas in every logic, hence also in De Morgan logic: the definition is the same as in Section 2, with $\vdash$ replaced by $\vdash_{DM}$.[13] From a semantic point of view, all the results from Section 1 still hold [8], provided we limit ourselves to Kripke models $v : Q \longrightarrow \mathscr{P}(\underline{x})$ such that $v(m_1) = v(m_2)$ for all minimal points of Q.[14] From now on, by a Kripke model, we always mean a Kripke model satisfying this additional requirement. Let us consider the totality of Kripke models over $\underline{x}$: for every $a \subseteq \underline{x}$, the ath *connected component* C_a is defined as

$$\{\, v\colon Q \longrightarrow \mathscr{P}(\underline{x}) \mid v(m) = a \text{ for all minimal points of } Q \,\},$$

or equivalently as

$$\left\{ v \mid v \models \bigwedge_{x \in a} \neg\neg x \wedge \bigwedge_{x \notin a} \neg x \right\}.$$

[13] Formulas which are projective in IPC are also projective in De Morgan logic, but the converse does not hold (see Example 1 below). Notice that in De Morgan logic projective formulas need not to have the disjunction property: for instance $\top$ is projective, but $\top \not\vdash_{DM} \neg x$ and $\top \not\vdash_{DM} \neg\neg x$, although $\top \vdash_{DM} \neg x \vee \neg\neg x$.

[14] Another equivalent possibility is to restrict to posets having a minimum element.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

Notice that each Kripke model over $\underline{x}$ belongs to exactly one connected component.

Most of the results of the previous sections can be restated with the same proof in De Morgan logic. Among them, we have Theorem 5 of Section 2. However, the meaning of this theorem has a little changed now and in particular there is an argument we often used in Section 3 that is not available anymore. If a class of Kripke models K has the extension property and if $v_1, \ldots, v_k \in K$, there may be no variant of $(\sum_i v_i)^+$ in K, unless all the v_i's are in the same connected component: otherwise, $(\sum_i v_i)^+$ is not itself a Kripke model, according to the new definition (recall that 'K has the extension property' means that K contains a variant of every model—in the new sense!—whose restrictions to all points different from the root are in K). Notice however that if $v_1 \leq_2 v_2$, then v_1 and v_2 lie in the same connected component. This observation is sufficient to get Lemma 3, Section 3, provided we limit ourselves to $n \geq 2$ in the statement (this is an inessential changement, we can always suppose that a formula has complexity less or equal to n for some $n \geq 2$). The remaining results in Section 3 are still valid, except Theorem 5 (the proof of Theorem 5 does not work, because the class K used in it need not have anymore the extension property). So we assume all results from Sections 1–3 for De Morgan logic, except Theorem 5 of Section 3 and we restart our investigations from that point.

Our strategy is the following: first, we show that all *disjunctions of projective formulas* have a most general unifier in De Morgan logic and then we show that if σ is a unifier for an arbitrary formula A, then it is a unifier for the disjunction of all projective formulas contained in A and having at most the same complexity as A. It will turn out that every unifiable formula admits a most general unifier in De Morgan logic.

Formulas $A_1(\underline{y}), \ldots, A_m(\underline{y})$ are called a *partition* if and only if $\vdash_{DM} A_1 \vee \cdots \vee A_m$ and $\vdash_{DM} \neg(A_i \wedge A_j)$ for $i \neq j$. Intuitionistic logic admits only trivial partitions because of the disjunction property; the situation is different for De Morgan logic:

LEMMA 1. *Let* $\underline{y} = y_1, \ldots, y_k$; *for* $i = 1, \ldots, k$, *put*

$$\Pi_i(\underline{y}) = \neg\neg y_i \wedge \bigwedge_{i \neq j} \neg y_j.$$

Put also

$$\Pi_0 = \left(\bigwedge_{i=1}^{k} \neg y_i\right) \vee \bigvee_{i \neq j} (\neg\neg y_i \wedge \neg\neg y_j).$$

Then $\Pi_0, \Pi_1, \ldots, \Pi_k$ *are a partition.*

PROOF. Apply distributivity to $\vdash_{DM} \bigwedge_{i=1}^{k} (\neg y_i \vee \neg\neg y_i)$. ⊣

If $v\colon Q \longrightarrow \mathscr{P}(\underline{x}, \underline{y})$ is a Kripke model, its restriction to $\underline{x}$ is the Kripke model $v_{\underline{x}}\colon Q \longrightarrow \mathscr{P}(\underline{x})$ defined by $v_{\underline{x}}(q) = v(q) \cap \underline{x}$ for all $q \in Q$.

LEMMA 2. *Suppose that* $B_1(\underline{x}), \ldots, B_k(\underline{x})$ *are projective formulas in De Morgan logic* ($k \geq 1$). *Then* $B_1 \vee \cdots \vee B_k$ *admits a most general unifier.*

PROOF. Let $\sigma_i\colon F(\underline{x}) \longrightarrow F(\underline{x})$ $(i = 1, \ldots, k)$ be a unifier for B_i such that

$$B_i \vdash_{DM} \sigma_i(x) \leftrightarrow x \tag{1}$$

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

for all $x \in \underline{x}$. Let $\sigma_0 \colon F(\underline{x}) \longrightarrow F(\emptyset)$ be a ground unifier for $B_1 \vee \cdots \vee B_k$ (we can get σ_0 for instance by instantiating $\underline{x}$ by $\bot$ or $\top$ in σ_1). Let $\underline{y} = y_1, \ldots, y_k$ be propositional variables not contained in $\underline{x}$. Define $\sigma \colon F(\underline{x}) \longrightarrow F(\underline{x}, \underline{y})$ by putting

$$\sigma(x) = \bigvee_{i=0}^{k} (\Pi_i(\underline{y}) \wedge \sigma_i(x)),$$

for every $x \in \underline{x}$. We show that σ is an mgu for $B_1 \vee \cdots \vee B_k$.

First, we show that σ is indeed a unifier for $B_1 \vee \cdots \vee B_k$, i.e., that for every Kripke model $v \colon Q \longrightarrow \mathscr{P}(\underline{x}, \underline{y})$, $\sigma^*(v) \models B_i$ for some $i = 1, \ldots, k$. As $\Pi_0, \Pi_1, \ldots, \Pi_k$ are a partition by Lemma 1, there is exactly one $i = 0, 1, \ldots, k$ such that $v \models \Pi_i$. Hence $\sigma^*(v) = \sigma_i^*(v_{\underline{x}})$, which is a model of B_i because σ_i unifies B_i (if $i = 0$, $\sigma(v) = \sigma_0(v_\emptyset)$ which is also a model of $B_1 \vee \cdots \vee B_k$ because σ_0 unifies it).

Now suppose that $\tau \colon F(\underline{x}) \longrightarrow F(\underline{z})$ is another unifier for $B_1 \vee \cdots \vee B_k$: we show that τ is less general than σ, i.e., that there is $\theta \colon F(\underline{x}, \underline{y}) \longrightarrow F(\underline{z})$ such that for every $x \in \underline{x}$

$$\vdash_{DM} \theta(\sigma(x)) \leftrightarrow \tau(x). \tag{2}$$

Before defining θ and proving (2), we need a preliminary remark.

Let $C_{a_1}, \ldots, C_{a_s}$ be the connected components of Kripke models over $\underline{z}$. We claim that for every $i = 1, \ldots, s$ there is $h(i) = 1, \ldots, k$ such that for every $u \colon P \longrightarrow \mathscr{P}(\underline{z})$

$$u \in C_{a_i} \Longrightarrow \tau^*(u) \models B_{h(i)}. \tag{3}$$

If not, there is $i = 1, \ldots, s$ such that for all $j = 1, \ldots, k$ there is u_j such that

$$u_j \in C_{a_i} \quad \text{and} \quad \tau^*(u_j) \not\models B_j.$$

As $u_1, \ldots, u_k$ are all in the same connected component, we can take into consideration $u = (\sum_j u_j)^+$ and realize that $\tau^*(u) \not\models B_1 \vee \cdots \vee B_k$, contrary to the fact that τ is a unifier for $B_1 \vee \cdots \vee B_k$. So (3) is proved.

Define θ by:

$$\theta(y_j) = \bigvee_{\{i \mid h(i)=j\}} \left(\bigwedge_{z \in a_i} z \wedge \bigwedge_{z \notin a_i} \neg z \right),$$
$$\theta(x) = \tau(x),$$

for all $j = 1, \ldots, k$ and $x \in \underline{x}$. Notice that for all $u \colon P \longrightarrow \mathscr{P}(\underline{z})$,

$$\theta^*(u) \models \Pi_{h(i)}$$

where a_i is the connected component of u. In fact

$$u \models \bigwedge_{z \in a_i} \neg\neg z \wedge \bigwedge_{z \notin a_i} \neg z,$$

so that $\theta^*(u) \models \neg\neg y_{h(i)}$ and moreover $\theta^*(u) \models \neg y_l$ for $l \neq h(i)$. As $\Pi_0, \Pi_1, \ldots, \Pi_k$ are a partition, the fact that $\theta^*(u) \models \Pi_{h(i)}$ implies that $\theta^*(u) \not\models \Pi_j$ for $j \neq h(i)$. We so obtained that

$$\theta^*(u) \models \Pi_j \quad \text{if and only if} \quad h(i) = j, \tag{4}$$

where a_i is the connected component of u.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

We can finally prove (2). Take $u\colon P \longrightarrow \mathscr{P}(\underline{z})$; let a_i be its connected component and let $j = h(i)$; according to (4), $\theta^*(u) \models \Pi_k$ if and only if $k = j$. This implies

$$\theta^*(u) \models \sigma(x) \quad \text{if and only if} \quad \theta^*(u) \models \sigma_j(x);$$

this relation can be extended to all models u_p (for $p \in P$), because all u_p lie in the same connected component as u. We consequently have that

$$u \models \theta(\sigma(x)) \leftrightarrow \theta(\sigma_j(x)). \tag{5}$$

According to (3), $\tau^*(u) \models B_j$ and by (1), $\tau^*(u) \models x \leftrightarrow \sigma_j(x)$, i.e.,

$$u \models \tau(x) \leftrightarrow \tau(\sigma_j(x)).$$

But $\sigma_j(x)$ does not contain the $\underline{y}$'s, hence $\tau(\sigma_j(x)) = \theta(\sigma_j(x))$ according to the definition of θ. We get

$$u \models \tau(x) \leftrightarrow \theta(\sigma_j(x)). \tag{6}$$

(5) and (6) together yield (2) as u is arbitrary. ⊣

THEOREM 3. *Each unifiable formula admits a most general unifier in De Morgan logic.*

PROOF. Let $A(\underline{x})$ be a unifiable formula such that $c(A) \leq n$ for $n \geq 2$ (we take $n \geq 2$ in order to be able to use Lemma 3 from Section 3, cf. the remark at the beginning of this section). We show that if $\sigma\colon F(\underline{x}) \longrightarrow F(\underline{y})$ is a unifier for A, then it is also a unifier for $B_1 \vee \cdots \vee B_k$, where $B_1, \ldots, B_k$ are all the projective formulas contained in A and having complexity at most n (consequently, σ is less general than the mgu of $B_1 \vee \cdots \vee B_k$, which exists by Lemma 2 and which is also a unifier for A, as $B_1 \vee \cdots \vee B_k \vdash A$).

It is sufficient to show that for every $u\colon P \longrightarrow \mathscr{P}(\underline{y})$ there is B such that $B \vdash_{DM} A$, $c(B) \leq n$, B is projective and $\sigma^*(u) \models B$. Let C_a be the connected component of u. Take

$$K_a = \{\, v \mid \exists w \in C_a \text{ such that } \sigma^*(w) \sim_\infty v \,\}.$$

By the same argument used in the proof of Theorem 5, Section 3, we can prove that K_a is stable and has the extension property (the latter is possible because the w appearing in the definition of K_a are all in the same connected component). Hence, by Lemma 3 of Section 3, we can take any B such that $\langle K_a \rangle_n = B^*$, in order to complete the proof of the Theorem. ⊣

EXAMPLE 1. $A = x \vee \neg x$ is projective in De Morgan logic and has most general unifier $\theta_A^{\{x\}}$. This substitution is equivalent to the substitution $x \mapsto \neg\neg x$.

EXAMPLE 2. $A = \neg x \to (y \vee z)$ is still not projective in De Morgan logic, but is provably equivalent in this logic to $(\neg x \to y) \vee (\neg x \to z)$, which is a disjunction of projective formulas. These two projective formulas have mgu's σ_1, σ_2 given by:

$$\begin{array}{ll} x \overset{\sigma_1}{\mapsto} x & x \overset{\sigma_2}{\mapsto} x \\ y \overset{\sigma_1}{\mapsto} (\neg x \to y) \to y & y \overset{\sigma_2}{\mapsto} y \\ z \overset{\sigma_1}{\mapsto} z & z \overset{\sigma_2}{\mapsto} (\neg x \to z) \to z \end{array}$$

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

(these two mgu's are a little more simple, but of course equivalent to those computed in Section 2, Example 2). We take σ_0 given by

$$x \overset{\sigma_0}{\mapsto} \top$$
$$y \overset{\sigma_0}{\mapsto} \bot$$
$$z \overset{\sigma_0}{\mapsto} \bot$$

and get an mgu σ for A by

$$\begin{aligned} x &\overset{\sigma}{\mapsto} ((\neg\neg y_1 \wedge \neg\neg y_2) \vee (\neg y_1 \wedge \neg y_2)) \\ &\qquad \vee (x \wedge \neg\neg y_1 \wedge \neg y_2) \vee (x \wedge \neg y_1 \wedge \neg\neg y_2); \\ y &\overset{\sigma}{\mapsto} (\neg\neg y_1 \wedge \neg y_2 \wedge ((\neg x \to y) \to y))) \\ &\qquad \vee (\neg y_1 \wedge \neg\neg y_2 \wedge y); \\ z &\overset{\sigma}{\mapsto} (\neg y_1 \wedge \neg\neg y_2 \wedge ((\neg x \to z) \to z))) \\ &\qquad \vee (\neg\neg y_1 \wedge \neg y_2 \wedge z). \end{aligned}$$

The peculiarity of De Morgan logic within the lattice of intermediate logics with respect to unification type is explained in the following Theorem:

THEOREM 4. *Let L be an intermediate logic in which all unifiable formulas have a most general unifier. Then De Morgan logic is included in L.*

PROOF. $x \vee \neg x$ is unifiable and hence has a most general unifier $\mu\colon F(x) \longrightarrow F(\underline{z})$ in L. In particular

$$\vdash_L \mu(x) \vee \neg\mu(x) \tag{7}$$

and there are two ground substitutions $\sigma_1\colon F(\underline{z}) \longrightarrow F(\emptyset)$ and $\sigma_2\colon F(\underline{z}) \longrightarrow F(\emptyset)$ such that

$$\vdash_L \sigma_1(\mu(x)) \leftrightarrow \top \quad \text{and} \quad \vdash_L \sigma_2(\mu(x)) \leftrightarrow \bot. \tag{8}$$

Notice that all ground formulas are provably equivalent to $\top$ or to $\bot$ in IPC (hence also in L), so we can freely assume that σ_1, σ_2 associates either $\top$ or $\bot$ with every $z \in \underline{z}$. Define a substitution $\sigma\colon F(\underline{z}) \longrightarrow F(x)$ by

$$\begin{aligned} \sigma(z) &= x, && \text{if } \sigma_1(z) = \top \text{ and } \sigma_2(z) = \bot \\ \sigma(z) &= \neg x, && \text{if } \sigma_1(z) = \bot \text{ and } \sigma_2(z) = \top \\ \sigma(z) &= \top, && \text{if } \sigma_1(z) = \top \text{ and } \sigma_2(z) = \top \\ \sigma(z) &= \bot, && \text{if } \sigma_1(z) = \bot \text{ and } \sigma_2(z) = \bot. \end{aligned}$$

for all $z \in \underline{z}$. By induction it can be seen (by using only axioms and rules of IPC) that for all $A(\underline{z})$

$$\begin{aligned} x \vee \neg x &\vdash_L x \leftrightarrow \sigma(A), && \text{if } \vdash_L \sigma_1(A) \leftrightarrow \top \text{ and } \vdash_L \sigma_2(A) \leftrightarrow \bot \\ x \vee \neg x &\vdash_L \neg x \leftrightarrow \sigma(A), && \text{if } \vdash_L \sigma_1(A) \leftrightarrow \bot \text{ and } \vdash_L \sigma_2(A) \leftrightarrow \top \\ x \vee \neg x &\vdash_L \top \leftrightarrow \sigma(A), && \text{if } \vdash_L \sigma_1(A) \leftrightarrow \top \text{ and } \vdash_L \sigma_2(A) \leftrightarrow \top \\ x \vee \neg x &\vdash_L \bot \leftrightarrow \sigma(A), && \text{if } \vdash_L \sigma_1(A) \leftrightarrow \bot \text{ and } \vdash_L \sigma_2(A) \leftrightarrow \bot. \end{aligned}$$

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

In particular, by (8), we have that

$$x \vee \neg x \vdash_L x \leftrightarrow \sigma(\mu(x)).$$

By deduction in IPC, we get

$$x \vee \neg x \vdash_L \neg x \leftrightarrow \neg\sigma(\mu(x)),$$

hence also

$$\neg\neg(x \vee \neg x) \vdash_L \neg\neg(\neg x \leftrightarrow \neg\sigma(\mu(x))$$

and finally

$$\vdash_L \neg x \leftrightarrow \neg\sigma(\mu(x)).$$

By (7), we have

$$\vdash_L \neg\sigma(\mu(x)) \vee \sigma(\mu(x)),$$

hence also

$$\vdash_L \neg\sigma(\mu(x)) \vee \neg\neg\sigma(\mu(x)).$$

By the replacement theorem, we get

$$\vdash_L \neg x \vee \neg\neg x,$$

showing that De Morgan logic is included in L. ⊣

The converse of Theorem 4 does not hold: in [9], we shall exhibit some easily built extensions of De Morgan logic in which unification is not even finitary. A quick algebraic proof of Theorem 4 can be obtained as follows through the methods and results of [12]: first notice that in any variety V of Heyting algebras for which unification is unitary the product of two finite projective algebras must be projective[15] and then observe that $\mathbf{2} \times \mathbf{2}$ cannot be projective in V in case V contains the algebra whose splitting is De Morgan variety.

REFERENCES

[1] F. Baader and J. H. Siekmann, *Unification theory*, ***Handbook of logic in artificial intelligence and logic programming*** (D. M. Gabbay, C. J. Hogger, and J. A. Robinson, editors), Oxford University Press, 1993, pp. 41–125.

[2] R. Balbes and A. Horn, *Injective and projective Heyting algebras*, ***Transactions of the American Mathematical Society***, vol. 148 (1970), pp. 549–559.

[3] D. de Jongh, *Formulas of one propositional variable in intuitionistic arithmetic*, ***The L. E. J. Brouwer centenary symposium*** (A. Troelstra and D. van Dalen, editors), North-Holland, 1982, pp. 51–64.

[4] D. de Jongh and A. Visser, *Embeddings of Heyting algebras*, ***Logic: from foundations to applications*** (W. Hodges, M. Hyland, C. Steinhorn, and J. Truss, editors), Clarendon Press, Oxford, 1996, pp. 187–213.

[5] de Jongh D. and L. A. Chagrova, *The decidability of dependency in intuitionistic propositional logic*, this Journal, vol. 60 (1995), pp. 498–504.

[6] K. Fine, *Logics containing K4, Part I*, this Journal, vol. 34 (1974), pp. 31–42.

[7] ———, *Logics containing K4, Part II*, this Journal, vol. 50 (1985), pp. 619–651.

[8] D. M. Gabbay, ***Semantical investigations in Heyting intuitionistic logic***, Sinthese Library, no. 148, Reidel, 1981.

[15] This is quite general, it follows only from the fact that finite Heyting algebras are finitely presented (recall that the signature of Heyting algebras is finite): to see it, consider any unifier, in the algebraic sense of [12], which is more general than the two projections.

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms

[9] S. GHILARDI, *E-unification in some varieties of Heyting algebras*, in preparation.

[10] ———, *Free Heyting algebras as bi-Heyting algebras*, ***Mathematical Reports of the Academy of Sciences of Canada***, vol. XIV (1992), no. 6, pp. 240–244.

[11] ———, *Unification and projectivity in propositional logic*, ***Quaderno n. 58/96***, Dipartimento di Matematica, Università degli Studi, Milano, 1996.

[12] ———, *Unification through projectivity*, ***Journal of Logic and Computation***, vol. 7 (1997), no. 6, pp. 733–752.

[13] S. GHILARDI and M. ZAWADOWSKI, *A sheaf representation and duality for finitely presented Heyting algebras*, this JOURNAL, vol. 60 (1995), no. 3, pp. 911–939.

[14] U. MARTIN and T. NIPKOW, *Boolean unification—the story so far*, ***Journal of Symbolic Computation***, vol. 7 (1989), pp. 275–293.

[15] A. M. PITTS, *On an interpretation of second order quantification in first order intuitionistic propositional logic*, this JOURNAL, vol. 57 (1992), no. 1, pp. 33–52.

[16] V. V. RYBAKOV, *Equations in a free topoboolean algebra and substitution problem*, ***Soviet Math. Dokl.***, vol. 33 (1986), no. 2, pp. 428–431.

[17] ———, *Rules of inference with parameters for intuitionistic logic*, this JOURNAL, vol. 57 (1992), no. 3, pp. 912–923.

[18] ———, *The universal theory of the free pseudo-Boolean algebra in extended signature*, ***Contemporary Mathematics***, vol. 131 (1992), no. 3, pp. 645–656.

[19] J. SIEKMANN, *Unification theory*, ***Journal of Symbolic Computation***, vol. 7 (1989), pp. 207–274.

[20] W. SNYDER, ***A proof theory for general unification***, Birkhäuser, 1991.

[21] A. URQUHART, *Free Heyting algebras*, ***Algebra Universalis***, vol. 3 (1973), pp. 94–97.

[22] D. VAN DALEN, *Intuitionistic logic*, ***Handbook of philosophical logic*** (Gabbay and Günther, editors), vol. III, Reidel, 1986, pp. 225–339.

[23] A. VISSER, *Bisimulations, model descriptions and propositional quantifiers*, ***Logic Group Preprint Series 161***, Department of Philosophy, Utrecht University, Utrecht, 1996.

DIPARTIMENTO DI SCIENZE DELL' INFORMAZIONE
UNIVERSITA 'DEGLI' STUDI DI MILANO
VIA COMELICO 39/41
20135 MILANO, ITALY
E-mail: ghilardi@dsi.unimi.it

This content downloaded from
187.255.252.12 on Tue, 04 May 2021 00:39:10 UTC
All use subject to https://about.jstor.org/terms