Imperative Mutual Recursion Proof Systems

Peter Hoffman

Pure Mathematics, University of Waterloo

Abstact. *This paper extends, from one to many procedure variables, the results in* [**sing**]. *The modifications needed are fairly straightforward, but we include here every necessary detail of the changes for possible referral to in a shorter publishable version* [**submit**]. *The main 'invention' here is a pair of mildly novel rules for recursive commands, one each for partial and for total correctness, but both derivative of old basic ideas from 30 or 40 years ago. So one now has, for a rather general case of a 'pure' recursion imperative command language, a sound, Cook-complete program verification proof system, for both partial and total correctness, with* local *procedure declarations and mutual recursion in any number of procedure variables. All earlier work concentrated on the inflexible restriction that procedure declarations were strictly global with two exceptions (a minor effort without completeness considerations which avoided total correctness* [**deBa**], *and* [**Harel**]*'s system for a considerably extended command language including a vast array of nondeterministic commands to make his system work). In particular, we are now at least able to have procedures declared that themselves contain procedure declarations, which would seem to be a feature of all 'practical' programming languages. The qualification "simple" indicates that, within a mutual block of procedure declarations, "free" occurrences of only the procedure variables declared are permitted.*

As the abstract indicates, we'll describe only the modifications necessary to extend, from one to arbitrarily many procedure variables, all the results in [**sing**].

We continue to base all of it on the 1st order number theory language with the natural numbers as interpretation, trusting that whoever so wishes will be able to extend easily to arithmetical interpretations in general, and perhaps to even more general languages. All the material in building the dynamic logic language is standard, and may be referred to [**sing**]. But we must modify the command language.

1. Command Syntax and Semantics.

We call the command language which will work for all this by the name $\mathcal{R}ec\_$. It is defined by first defining $\mathcal{R}ec$ as follows:

Amplify X from [**sing**] *to a sequence of 'procedure variables' $X_1, X_2, \cdots$;*

Then by structural induction $\mathcal{R}ec$ is :

$$x \leftarrow t \;\mid\; callY \;\mid\mid\; (C;D) \;\mid\; ite(G)(C)(D) \;\mid\; \nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k \;,$$

where Y may be any X_ℓ, and where $Y_1, Y_2, \cdots, Y_k$ are mutually distinct X_ℓ's and $1 \leq j \leq k$.

The string $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$ is meant to convey the mutual recursion

$$\textsf{begin}\ declare\ Y_1\ to\ be\ C_1\ ;\ \cdots\ ;\ declare\ Y_k\ to\ be\ C_k\ ;\ doY_j\ \textsf{end}\ .$$

Note that this does not preclude occurrences, within any of the C_i, of $callX_\ell$ which are 'free' when regarded as occurrences in the entire command $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$. Here, *free* would imply the X_ℓ *not* being one of the Y_i, but it is easy and better to define it carefully by induction, since such a subcommand $callX_\ell$ would still be bound, rather than free, if it's inside a suitable 'smaller ∇-command'. We don't really need to fuss about producing an actual abstract object—the definitions below are quite adequate for doing any syntactical verifications needed—but a subcommand occurrence in C could simply be identified with a pair (k, C) for a positive integer k, where the occurrence is 'really' a consecutive string starting with the kth symbol in C. This would use various elementary facts connected with unique readability in $\mathcal{R}ec$, in particular that the natural (and more useful) inductive definition below of *subcommand occurrence* amounts to the same thing as a '*consecutive substring which happens to also be in $\mathcal{R}ec$*'.

Let us spell out in detail the inductive definition of occurrences of subcommands:

The entire command is an occurrence as a subcommand of itself, the only non-proper *one.*

The set of proper *occurrences of subcommands is empty for atomic commands, is the union of the sets of* all *occurrences of subcommands of C and D when the command is obtained from them by sequencing or ite, and is the set of* all *occurrences of subcommands of bits of $\vec{C}$ when the command is $\nabla_j \vec{C}/\vec{Y}$. Here, by the convenient phrase "bits of the sequence $[[C_1, \cdots, C_k]]$", we just mean the commands C_i.*

The inductive definition of an occurrence of $callX$ being *free* is identical, except that, if X is one of the Y_j's, its free occurrences inside any of the C_i are considered *non-free* or *bound* as occurrences in $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$. *Then $\mathcal{R}ec_-$ is the subset of those commands which have no subcommand of the form $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$ such that some $callX_\ell$ has a free occurrence as a subcommand of some C_n, and yet $X_\ell \neq Y_i$ for all i.* Equivalently, no subcommand of the form $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$ has any free occurrences of *any* $callX$. Thus $\mathcal{R}ec_-$ is virtually identical to the deterministic part of the language described on p.45 in [**Harel**]; in particular, that paper uses the word "simple" to single out the commands in $\mathcal{R}ec_-$ from those in $\mathcal{R}ec$, as we have just done.

Note also that we have changed the language from the one, which I'll name $\mathcal{R}ec_+$, suggested in [**sing**]. The present one is reasonably general. It is possible that modification of the present discussion of $\mathcal{R}ec_-$ to deal instead with $\mathcal{R}ec_+$ will not present insuperable obstructions, but let's stay on topic.

Except for the very last proof at the end of this paper, everything stated below can be made to work just as well for $\mathcal{R}ec$ as it does for $\mathcal{R}ec_-$. Thus, both soundness, and all *partial* correctness aspects of completeness, hold as stated in Section 3, but using $\mathcal{R}ec$. However, completeness for *total* correctness possibly fails without the restriction to "simple" recursion.

As for the semantics, the function m is defined much as in [**sing**], with all the free $callX_i$'s as universally diverging, and with that last command $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$ having its m-function defined as follows:

First abbreviate $\nabla_j C_1 Y_1 C_2 Y_2 \cdots C_k Y_k$ to $\nabla_j \vec{C}/\vec{Y}$.

As above, we'll write sequences with double square brackets. For example the sequence $\vec{Y}$ of procedure variables in the command above is $[[Y_1, \cdots, Y_k]]$. Whenever $\vec{C}/\vec{Y}$ is written, it is to be understood that $\vec{C} = [[C_1, \cdots, C_k]]$, i.e. the same "$k$", and each C_i is a command.

Next define

$$\overrightarrow{\nabla_* C/Y} \;:=\; [[\nabla_1 \vec{C}/\vec{Y}, \cdots, \nabla_k \vec{C}/\vec{Y}]] \;.$$

and

$$E_{\vec{D}/\vec{Y}} \;:=\; |E|^{\forall i: callY_i \to D_i} \;,$$

meaning that one simultaneously for all i substitutes D_i for free occurrences of $callY_i$ in E. The rigorous inductive definition is easy to guess. See [**submit**].

Now define a command $(\vec{C}/\vec{Y})_j^{<n>}$ for $1 \leq j \leq k$ by induction on $n \geq 0$:

$$(\vec{C}/\vec{Y})_j^{<0>} \;:=\; callY_j \quad \text{and} \quad (\vec{C}/\vec{Y})_j^{<n+1>} \;:=\; (C_j)_{\vec{D}/\vec{Y}} \;, \quad \text{where}$$

$$\vec{D} = \overrightarrow{(\vec{C}/\vec{Y})^{<n>}} \;:=\; [[(\vec{C}/\vec{Y})_1^{<n>}, \cdots, (\vec{C}/\vec{Y})_k^{<n>}]] \;.$$

As in [**sing**], we define $m(C)$ by induction on

$\mathrm{nab}(C) \;:=$ the number of distinct $\nabla_j \vec{C}/\vec{Y}$ which occur as a subcommand of C .

For fixed $\mathrm{nab}(C)$, it is then defined by structural induction on C. The only definition needed here is

$$m(\nabla_j \vec{C}/\vec{Y}) \;:=\; \bigcup_{n=0}^{\infty} m((\vec{C}/\vec{Y})_j^{<n>}) \;.$$

This is well-defined because

$$\mathrm{nab}((\vec{C}/\vec{Y})_j^{<n>}) \;\leq\; \sum_{\ell} \mathrm{nab}(C_\ell) \;=\; \mathrm{nab}(\nabla_j \vec{C}/\vec{Y}) - 1 \;.$$

See [**submit**] for more detail on this inequality, which depends on recursion being simple, though the same definitions with a slightly more subtle induction will define our straightforward input/output semantics perfectly adequately for all of $\mathcal{R}ec$.

At this point the analogues of **1** to **10** in [**sing**] all go through with no real modification needed. In particular, the substitution operation above is well-defined, the command language is deterministic, and the various other matters concerning substitution discussed in [**sing**] behave similarly here, with the additional comments four paragraphs below. Again see [**submit**] for a few extra details.

2. Proof Systems and Validity of Mutual Recursion Rules.

The system for $\vdash'$ is defined exactly as in [**sing**].

Now we present the new rule for partial correctness of recursive commands, and its validity. Using a prefix "M" to distinguish it from its baby sister in [**sing**], where the "M" stands for "mutual", the new rule is as follows, where

$\bigwedge$ denotes 'anding' together a finite set of wfs's;
e.g.

$$\bigwedge_{1\leq j\leq 2} \mathcal{A}_j = \mathcal{A}_1 \wedge \mathcal{A}_2 \ :$$

$(\mathsf{MRCS})_{[\ ]\rightarrow}$ with $\vec{D} = \overrightarrow{\nabla_* C/Y}$,

$$\frac{\vdash \bigwedge_{\mathcal{C}\in\Omega} \mathcal{C} \ \ , \ \ \Omega \ \cup \ \{\mathcal{A}_j \rightarrow [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j \mid 1 \leq j \leq k\} \ \vdash' \ \bigwedge_{1\leq j\leq k}(\mathcal{A}_j \rightarrow [(C_j)_{\vec{D}/\vec{Y}}]\mathcal{B}_j)}{\vdash \quad \bigwedge_{1\leq i\leq k}(\mathcal{A}_i \rightarrow [\nabla_i \vec{C}/\vec{Y}]\mathcal{B}_i)} \ ,$$

where :
(1) *the set* Ω *is a finite set of wfs's* ;
(2) *the object* $\vec{C}/\vec{Y}$ *is such that no* $\nabla_j \vec{C}/\vec{Y}$ *is a subcommand of any command occurring within a wfs in* Ω ;
(3) *the wfs's* $\mathcal{A}_i$ *and* $\mathcal{B}_i$ *also have no occurrences of any* $\nabla_j \vec{C}/\vec{Y}$ *in them.*

When $k = 1$, this essentially reduces to $(\mathsf{RCS})_{[\ ]\rightarrow}$ from [**sing**]. The proof of its validity is very similar, as follows.

First we must define $|D|^{\forall i:\nabla_i \vec{C}/\vec{Y}\rightarrow E_i}$ in the obvious way (simultaneously for all i substituting of command E_i for each occurrence of $\nabla_i \vec{C}/\vec{Y}$), and prove:

Theorem M11. *Suppose* $\Gamma \vdash' \mathcal{A}$. *Then* $|\Gamma|^{\forall i:\nabla_i \vec{C}/\vec{Y}\rightarrow E_i} \vdash' |\mathcal{A}|^{\forall i:\nabla_i \vec{C}/\vec{Y}\rightarrow E_i}$ *for any* $\vec{C}/\vec{Y}$ *and* $\vec{E}$ *for which all the program variables in* $\vec{E}$ *already occur as program variables in* $\vec{C}$.

Then the following are the appropriate analogues to get the required validity of the above 'partial correctness recursive command rule' $(\mathsf{MRCS})_{[\ ]\rightarrow}$.

In all of **M12** to **M17**, the objects $\vec{C}/\vec{Y}$, Ω , $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$ and $\vec{D}$ are as specified in the statement of $(\mathsf{RCN})_{[\ ]}$.

Corollary M12.

$$\Omega \cup \{\mathcal{A}_j \rightarrow [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j \mid 1 \leq j \leq k\} \ \vdash' \bigwedge_{1\leq j\leq k} (\mathcal{A}_j \rightarrow [(C_j)_{\vec{D}/\vec{Y}}]\mathcal{B}_j) \ \textit{ implies that}$$

$$\Omega \ \cup \ \{\mathcal{A}_j \rightarrow [E_j]\mathcal{B}_j \mid 1 \leq j \leq k\} \ \vdash' \bigwedge_{1\leq j\leq k} (\mathcal{A}_j \rightarrow [(C_j)_{\vec{E}/\vec{Y}}]\mathcal{B}_j)$$

for all $\vec{E}$ *all of whose program variables are also program variables in* $\vec{C}$.

Proof. The conditions imply that there is only the one (very visible) occurrence of $\nabla_j \vec{C}/\vec{Y}$ on each side of $\vdash'$ for which to substitute the command E_j, so this is immediate from **M11**.

Corollary M13. *With assumption as in* **M12**, *for all* $n \geq 0$ *we have*

$$\Omega \cup \{\mathcal{A}_j \to [(\vec{C}/\vec{Y})_j^{<n>}]\mathcal{B}_j \mid 1 \leq j \leq k\} \vdash' \bigwedge_{1 \leq j \leq k} (\mathcal{A}_j \to [(\vec{C}/\vec{Y})_j^{<n+1>}]\mathcal{B}_j) \ .$$

Proof. Take $E_j = (\vec{C}/\vec{Y})_j^{<n>}$ in **M12** , noting that $(C_j)_{\vec{E}/\vec{Y}} = (\vec{C}/\vec{Y})_j^{<n+1>}$ and that $(\vec{C}/\vec{Y})_j^{<n>}$ has all its program variables occurring in $\vec{C}$ also as program variables.

Theorem M14. *The* $\vdash'$*-proof system is sound. That is, if* $\Gamma \vdash' \mathcal{A}$, *and if* $\mathcal{B}$ ttN *for each* $\mathcal{B} \in \Gamma$, *then* $\mathcal{A}$ ttN.

The proofs of validity for its rules are well-known. See Theorem 14 in [**sing**].

Corollary M15. *With the conditions on* $\vec{C}/\vec{Y}$, $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$, $\vec{D}$ *and* Ω *stated in* $(\mathsf{RCN})_{[\ ]}$, *if*

$$\Omega \cup \{\mathcal{A}_j \to [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j \mid 1 \leq j \leq k\} \vdash' \bigwedge_{1 \leq j \leq k} (\mathcal{A}_j \to [(C_j)_{\vec{D}/\vec{Y}}]\mathcal{B}_j)$$

where all wfs's in Ω *are* ttN, *then* $(\mathcal{A}_j \to [(\vec{C}/\vec{Y})_j^{<n>}]\mathcal{B}_j)$ ttN *for all* j *and all* $n \geq 0$.

Proof. Proceed by induction on n. Since $(\vec{C}/\vec{Y})_j^{<0>} = \mathit{call} Y_j$ which never converges, clearly $(\mathcal{A} \to [(\vec{C}/\vec{Y})_j^{<0>}]\mathcal{B})$ ttN for *any* $\mathcal{A}$ and $\mathcal{B}$. For the inductive step, simply use **M13**, and the soundness of $\vdash'$ from **M14**.

Lemma M16. *If, for all* $n \geq 0$, $(\mathcal{A}_j \to [(\vec{C}/\vec{Y})_j^{<n>}]\mathcal{B}_j)$ ttN, *then* $(\mathcal{A}_j \to [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j)$ ttN (where j is irrelevant as a subscript on $\mathcal{A}$ and $\mathcal{B}$).

The proof is straightforward from the definitions of $m(\nabla_j \vec{C}/\vec{Y})$, of ttN, and of $[D]\mathcal{B}$.

Corollary M17. *With the conditions on* $\vec{C}/\vec{Y}$, $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$, $\vec{D}$ *and* Ω *stated in* $(\mathsf{RCN})_{[\ ]}$, *if*

$$\Omega \cup \{\mathcal{A}_j \to [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j \mid 1 \leq j \leq k\} \vdash' \bigwedge_{1 \leq j \leq k} (\mathcal{A}_j \to [(C_j)_{\vec{D}/\vec{Y}}]\mathcal{B}_j)$$

where all wfs's in Ω *are* ttN*, then* $(\mathcal{A}_j \to [\nabla_j \vec{C}/\vec{Y}]\mathcal{B}_j)$ ttN *for all* j .

The proof is immediate from **M15** and **M16**, and gives the validity of $(\mathsf{RCN})_{[\ ]}$.

Next comes the obvious generalization of a rule to which we'll give the same name as in [**sing**]:

$$(\mathsf{AX})_{<\nabla>} \qquad \text{with } \vec{D} = \overrightarrow{\nabla_* C/Y}\ ,$$

$$\emptyset\ /\ (< (C_j)_{\vec{D}/\vec{Y}} > \mathcal{A} \iff < \nabla_j \vec{C}/\vec{Y} > \mathcal{A})\ .$$

Proof of validity is entirely parallel to the case of a single procedure variable. See [**submit**] for details. There is again an exceptionally simple proof that its twin, $(\mathsf{AX})_{[\nabla]}$, is derivable.

As in [**sing**], the systems for $\vdash''$, and for $\vdash^w$ respectively, are defined by adding this rule to the list of rules for $\vdash'$, and then respectively restricting the use of the variable w in five of the earlier rules.

Now we can give the new rule for total correctness of recursive commands, and discuss its validity. Again using a prefix "M" to distinguish it from its baby sister in [**sing**], the new rule is as follows:

$(\mathsf{MRCS})_{<\ >}$

$$\frac{\vdash \bigwedge_{1\le j\le k} \neg|\mathcal{A}_j|^{w\mapsto 0}\ ,\ \vdash \bigwedge_{\mathcal{C}\in\Omega} \mathcal{C}\ ,\ \Omega \cup \{\ \mathcal{A}_j \to \mathcal{B}_j \mid 1 \le j \le k\}\ \vdash^w\ \bigwedge_{1\le j\le k}(|\mathcal{A}_j|^{w\mapsto w+1} \to \mathcal{B}_j\ )}{\vdash\ \bigwedge_{1\le i\le k}(\mathcal{A}_i \to \mathcal{B}_i)}\ ,$$

for all variables w*, all wfs's* $\mathcal{A}_j$ *(recall that, because of the substitution,* w *cannot be a* program *variable in any of* $\mathcal{A}_j$*'s subcommands), all finite sets* Ω *of wfs's, and all wfs's* $\mathcal{B}_j$ in which w does not occur at all.

When $k = 1$. this essentially reduces to $(\mathsf{RCS})_{<\ >}$ from [**sing**]. The proof of its validity is very similar, as follows. It again uses the characteristic semantic property of $\vdash^w$, namely that it preserves truth at the set of all states with a fixed value for w (i.e. Lemma 24 in [**sing**]).

Assuming the truth in **N** of the antecedents, we prove by induction on ℓ, as required, that, for all ℓ,

$$(\mathcal{A}_i \to \mathcal{B}_i)\ \mathsf{tt@}s_{w\mapsto\ell}\ \text{ for all } s\ ,$$

where i might as well be fixed.

For $\ell = 0_{\mathbf{N}}$, we have $|\mathcal{A}_i|^{w\mapsto 0}$ $\mathsf{ff}@s$ for all s, and so $\mathcal{A}_i$ $\mathsf{ff}@s_{w\mapsto 0_{\mathbf{N}}}$ for all s, and so $(\mathcal{A}_i \to \mathcal{B}_i)$ $\mathsf{tt}@s_{w\mapsto 0_{\mathbf{N}}}$ for all s.

For the inductive step, both $\mathcal{A}_j \to \mathcal{B}_j$ for all j by the inductive assumption, and all wfs's in Ω are $\mathsf{tt}@s_{w\mapsto \ell}$ for all s. Thus by the semantic property referred to just above, the $\vdash^w$-antecedent shows that

$$|\mathcal{A}_i|^{w\mapsto w+1} \to \mathcal{B}_i \ , \text{ which equals } |\mathcal{A}_i \to \mathcal{B}_i|^{w\mapsto w+1} \ ,$$

is also $\mathsf{tt}@s_{w\mapsto \ell}$ for all s. But that last statement amounts to $\mathcal{A}_i \to \mathcal{B}_i$ being $\mathsf{tt}@(s_{w\mapsto \ell})_{w\mapsto s_{w\mapsto \ell}(w+1)}$ for all s. But the latter state is simply $s_{w\mapsto \ell +_{\mathbf{N}} 1_{\mathbf{N}}}$, as required.

So now one can define, and be sure of the soundness of, the 'ultimate' (to coin a highly original adjective) system, for $\vdash$, just as in [**sing**], using all the rules for $\vdash''$ plus the two new mutual recursion rules discussed and proved valid in this section. The general specification of this system, and of what one means by a $\vdash$-derivation, and by justifying the lines in such a derivation, are almost identical to the details given in [**sing**]. See [**submit**] for more explicit formulations.

It may be worth reminding the reader that we have no need for various ad-hoc devices such as *counting variables, auxiliary variables, adaptation rules, contexts, correctness phrases, conversion of Hilbert systems to Gentzen systems to make sense of soundness,* etc. which always seem to crop up in the (in my opinion) unnatural languages where all the procedure variables have fixed meanings (i.e. only global declarations involved) and where one is denied the flexibility provided by the language of dynamic logic.

3. Discussion of the main results.

These have exactly the same statements as in [**sing**], but we will number them by adding an **M** (for 'mutual') to indicate that the results are talking about the dynamic logic based on the command language here :

Theorem M19. (Soundness of the $\vdash$-system)
If $\vdash \mathcal{A}$, *then* $\mathcal{A}$ $\mathtt{ttN}$.

We have essentially proved all the 'new' stuff needed for this in the last section.

Theorem M20. (Cook-completeness of the $\vdash$-system)
If $\mathcal{A}$ $\mathtt{ttN}$, *then* $\vdash \mathcal{A}$.

The proof is split into three pieces just below, the first due to Harel, as in [**sing**].

Theorem M21. (essentially in [**Harel**]) *To prove* **M20**, *it suffices to prove the following two cases, for* $1^{\underline{\text{st}}}$*order* F *and* G, *and any command* D :
(i) $(F \to [D]G)$ $\mathtt{ttN} \implies \vdash (F \to [D]G)$ *; and*
(ii) $(F \to\!< D >\! G)$ $\mathtt{ttN} \implies \vdash (F \to\!< D >\! G)$.

This is proved as in [**sing**]..

Theorem M22. *For all* F, D *and* G, *statement* **M21***(i) holds.*

Theorem M23. *For all* F, D *and* G, *statement* **M21***(ii) holds.*

These two are proved in the next two sections, respectively, where we again use the same numbering as in [**sing**], but this time state the results and immediately prove them in 'logical' order, with the proofs of the two theorems just above coming at the ends of the sections. Note that all these proofs are very straightforward modifications of the ones for a single procedure variable in [**sing**], and a few times are exactly the same, but it seems more helpful to have them all here in one place.

4. Technical results and all proofs re partial correctness.

The proofs below will make many referrals to rules in the $\vdash'$-system, not named and specified here, but rather in **[sing]**.

Lemma M22.0.
(a) *For each command C, and $1^{\underline{\text{st}}}$order formula F, there is a $1^{\underline{\text{st}}}$order formula $A(C,F)$—("A" for "after" rather than "post")—such that*

$$A(C,F)\ \mathsf{tt}@s' \quad \Longleftrightarrow \quad \exists s \text{ with } F\ \mathsf{tt}@s \text{ and } (s,s') \in m(C)\ .$$

And so, $A(C,F)$ is the 'universal' A for which $(F \to [C]A)$ ttN. That is, for all $1^{\underline{\text{st}}}$order K,

$$F \to [C]K\ \ \mathsf{ttN} \ \Longleftrightarrow\ \ A(C,F) \to K\ \ \mathsf{ttN}\ .$$

(b) *For any wfs $\mathcal{H}$, there is a $1^{\underline{\text{st}}}$order formula H, whose free variables are from the variables occurring in $\mathcal{H}$, with $H \leftrightarrow \mathcal{H}$ true in $\mathbf{N}$.*

The proof is the same as in **[sing]**, depending only on the effectiveness of the command language $\mathcal{R}ec_{-}$ and its semantics.

Lemma M22.5. *If D is a command, and Γ is a set of wfs's, define the phrase "Γ der $[D]$" to mean*

$$\mathsf{for\ all}\ 1^{\underline{\text{st}}}\ \mathsf{order\ formulas}\ F\ \mathsf{and}\ G, \quad (F \to [D]G)\,\mathsf{ttN} \implies \Gamma\ \vdash'\ (F \to [D]G)\,.$$

Assume Γ_1 der $[D_1]$ and Γ_2 der $[D_2]$. Then $\Gamma_1 \cup \Gamma_2$ der $[(D_1;D_2)]$; and similarly, with H any quantifier-free $1^{\underline{\text{st}}}$order formula, we also have

$$\Gamma_1 \cup \Gamma_2\ \ \mathsf{der}\ \ [ite(H)(D_1)(D_2)]\ .$$

Proof of M22.5. For the sequencing command, given F and G such that $F \to [(D_1;D_2)]G$ ttN, by **M22.0**(b), choose a $1^{\underline{\text{st}}}$order J such that $J \longleftrightarrow [D_2]G$ ttN. Then $\Gamma_2 \vdash' J \to [D_2]G$ since Γ_2 der $[D_2]$, so

$$\Gamma_2\ \vdash'\ [D_1]J \to [D_1][D_2]G \qquad\qquad (I)$$

by $(\mathsf{UNAR})_{[\ ]}$. Since

$$(F \to [D_1]J)\ \longleftrightarrow\ (F \to [D_1][D_2]G)\quad \mathsf{ttN}\ ,$$

and $(F \to [D_1][D_2]G)$ ttN, we get

$$\Gamma_1 \ \vdash' \ F \to [D_1]J \qquad\qquad (II)$$

since Γ_1 der $[D_1]$. Now $(I), (II)$ and (HYSY) give

$$\Gamma_1 \cup \Gamma_2 \ \vdash' \ F \to [D_1][D_2]G \ .$$

Then $(\mathsf{AX})_{[;]}$ plus (HYSY) allow one to change $[D_1][D_2]$ to $[(D_1; D_2)]$ in the last display, as required.

For 'if-then-else', given F and G with $F \to [ite(H)(D_1)(D_2)]G$ ttN, it follows from the validity of $(\mathsf{AX})_{[ite]}$ that

$$F \ \to \ (H \to [D_1]G) \wedge (\neg H \to [D_2]G) \quad \mathsf{ttN} \ .$$

And so both the following are true in $\mathbf{N}$:

$$F \wedge H \ \to \ [D_1]G \quad \text{and} \quad F \wedge \neg H \ \to \ [D_2]G \ .$$

But then the two Γ_i der $[D_i]$ guarantee that these two can be derived from $\Gamma_1 \cup \Gamma_2$. The rules $(\mathsf{P})_1$ and $(\mathsf{P})_2$ now handily establish

$$\Gamma_1 \cup \Gamma_2 \ \vdash' \ F \ \to \ (H \to [D_1]G) \wedge (\neg H \to [D_2]G) \ .$$

But $(\mathsf{AX})_{[ite]}$ and $(\leftrightarrow)$ show

$$\vdash' \ (H \to [D_1]G) \wedge (\neg H \to [D_1]G) \quad \longrightarrow \quad [ite(H)(D_1)(D_2)]G \ ,$$

so (HYSY) applied to the last two displays finishes the job.

In many places in the rest of this paper,

$$\vec{x} \approx \vec{z} \quad \text{is short for} \quad x_1 \approx z_1 \ \wedge \ \cdots \ \wedge \ x_\ell \approx z_\ell,$$

for various ℓ , where the two matching (i.e. same length) lists of distinct variables are always disjoint from each other.

Lemma M22.4. *For any* $1^{\underline{\text{st}}}$*order* F *and* G*, command* C'*, and matching disjoint lists* $\vec{x}$ *and* $\vec{z}$ *of pairwise distinct variables such that all variables from* C' *are in* $\vec{x}$*, if* $(F \to [C']G)$ ttN *, then we have*

$$(A(C', \vec{x} \approx \vec{z}) \ \wedge \ |F|^{\vec{x} \to \vec{z}} \ \to \ G) \quad \mathsf{ttN} \ .$$

Proof of M22.4. Assume $A(C', \vec{x} \approx \vec{z}) \wedge |F|^{\vec{x}\to\vec{z}}\ \mathsf{tt}@s'$. Then, for some s we have

$$(s, s') \in m(C') \quad , \quad \vec{x} \approx \vec{z}\ \mathsf{tt}@s \quad , \quad F\ \mathsf{tt}@s'_{\vec{x}\mapsto s'(\vec{z})} \ .$$

Now $s'_{\vec{x}\mapsto s'(\vec{z})}(\vec{x}) = s'(\vec{z}) = s(\vec{z}) = s(\vec{x})$. The last equality comes from the truth of $\vec{x} \approx \vec{z}$ indicated in the previous display. The equality before that is because all the variables in C' are from $\vec{x}$—none are from $\vec{z}$.

Also $s'_{\vec{x}\mapsto s'(\vec{z})}(\vec{z}) = s'(\vec{z}) = s(\vec{z})$. All states here obviously agree on variables other than those in $\vec{x}$ and $\vec{z}$.

Thus $s'_{\vec{x}\mapsto s'(\vec{z})} = s$. And so $F\ \mathsf{tt}@s$. Combined with $(s, s') \in m(C')$ and $F \to [C']G\ \mathsf{tt}@s$, we get $G\ \mathsf{tt}@s'$, as required.

Lemma M22.3. *With hypotheses as in* **22.4**,

$$\{\vec{x} \approx \vec{z}\ \to\ [C']A(C', \vec{x} \approx \vec{z})\}\ \ \vdash'\ \ (F \to [C']G) \ .$$

Proof of that M22.4 implies M22.3. First we prove the special case when no $\vec{z}$-variables occur in F nor G. Here is a derivation, shortening $A(C', \vec{x} \approx \vec{z})$ to just A :

$\vec{x} \approx \vec{z}\ \to\ [C']A$	(premiss)
$\|F\|^{\vec{x}\to\vec{z}} \to [C']\|F\|^{\vec{x}\to\vec{z}}$	$(\mathsf{AX})_{disj}$
$\vec{x} \approx \vec{z} \wedge \|F\|^{\vec{x}\to\vec{z}} \to [C'](A \wedge \|F\|^{\vec{x}\to\vec{z}})$	(AND)
$A \wedge \|F\|^{\vec{x}\to\vec{z}} \to G$	(ORAC) and **M22.4**
$[C'](A \wedge \|F\|^{\vec{x}\to\vec{z}}) \to [C']G$	$(\mathsf{UNAR})_{[\ ]}$
$\vec{x} \approx \vec{z} \wedge \|F\|^{\vec{x}\to\vec{z}} \to [C']G$	(HYSY)
$\vec{x} \approx \vec{x} \wedge F \to [C']G$	$(\mathsf{SUB})_2^{\vec{z}\to\vec{x}}$
$F \to\ \vec{x} \approx \vec{x} \wedge F$	(ORAC)
$F \to [C']G$	(HYSY)

Line 7 uses that no z_i is in G or F, since then $||F|^{\vec{x}\to\vec{z}}|^{\vec{z}\to\vec{x}} = F$ and $|G|^{\vec{z}\to\vec{x}} = G$.

Now in the general case, let $\vec{u}$ be a matching list of pairwise distinct variables, disjoint from $\vec{x}$ and $\vec{z}$. Define F_1 to be $|F|^{\vec{z}\to\vec{u}}$ and let $G_1 := |G|^{\vec{z}\to\vec{u}}$, so F_1 and G_1 have no $\vec{z}$-variables. Since the validity of $(\mathsf{SUB})_1^{\vec{z}\to\vec{u}}$ entails that

the truth of $F \to [C']G$ in $\mathbf{N}$ also guarantees $\mathsf{tt}\mathbf{N}$ for the wfs $F_1 \to [C']G_1$, the special case above yields

$$\{\vec{x} \approx \vec{z} \ \to \ [C']A(C', \vec{x} \approx \vec{z})\} \quad \vdash' \quad (F_1 \to [C']G_1) \ .$$

But now application of $(\mathsf{SUB})_1^{\vec{u} \to \vec{z}}$ allows us the erase the subscript on F and G in this last display, as required.

Recall that by "bits of $[[C_1, \cdots, C_k]]$", we just mean the commands C_i, and also recall the definition of *subcommand* given at the beginning of the paper.

Lemma M22.2. *Suppose given a command D_1, and $1^{\underline{\text{st}}}$order formulas F and G, such that $(F \to [D_1]G)$ $\mathsf{tt}\mathbf{N}$. For each subcommand $\nabla_j \vec{C}'/\vec{Y}'$ of D_1, choose a pair of matching disjoint lists $\vec{x}$ and $\vec{z}$ of pairwise distinct variables, such that all the variables in $\vec{C}'$ are in $\vec{x}$. Let Γ_{D_1} be the* (finite!) *set of all formulas (one for each such $\nabla_j \vec{C}'/\vec{Y}'$)*

$$\vec{x} \approx \vec{z} \ \to \ [\nabla_j \vec{C}'/\vec{Y}']A(\nabla_j \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}) \ .$$

Then $\Gamma_{D_1} \ \vdash' \ (F \to [D_1]G)$.

Proof that (M22.3 plus M22.5) imply M22.2. Proceed by induction on D_1.

When $D_1 = callX_i$: By $(\mathsf{AX})_{[call]}$ and $(\mathsf{P})_4$, we have $\vdash' \ (F \to [callX_i]G)$ (for *any* F and G).

When $D_1 = y \leftarrow\!\!\div t$: By the soundness of $(\mathsf{AX})_{\leftarrow\!\!\div}$, we see that

$$(F \to [y \leftarrow\!\!\div t]G) \ \mathsf{tt}\mathbf{N} \quad \Longrightarrow \quad (F \to |G|^{y \to t}) \ \mathsf{tt}\mathbf{N} \ .$$

So here's a little derivation doing the job :

$F \to |G|^{y \to t}$ $\quad (\mathsf{ORAC})$

$|G|^{y \to t} \leftrightarrow \ [y \leftarrow\!\!\div t]G$ $\quad (\mathsf{AX})_{[\leftrightarrow]}$

$|G|^{y \to t} \to \ [y \leftarrow\!\!\div t]G$ $\quad (\leftrightarrow)$

$F \to [y \leftarrow\!\!\div t]G$ $\quad (\mathsf{HYSY})$

When $D_1 = \nabla_i \vec{C}/\vec{Y}$: The set $\Gamma_{\nabla_i \vec{C}/\vec{Y}}$ from **M22.2** contains the element $\vec{x} \approx \vec{z} \ \to \ [\nabla_i \vec{C}/\vec{Y}]A$, so **M22.3** with $C' = \nabla_i \vec{C}/\vec{Y}$ gives the result.

When $D_1 = (D;E)$ or $ite(H)(D)(E)$: Apply **M22.5** with $\Gamma_1 = \Gamma_D$ and $\Gamma_2 = \Gamma_E$, noting that $\Gamma_{D_1} = \Gamma_D \cup \Gamma_E$ for both types of D_1 here. Use the inductive hypotheses for D and E as the hypotheses in **M22.5**. The latter's conclusions are exactly the required results.

Lemma M22.1. *For all $\vec{C}/\vec{Y}$ and matching disjoint lists $\vec{x}$ and $\vec{z}$ of pairwise distinct variables such that all variables from $\vec{C}$ are in $\vec{x}$, the finite set Ω below, of wfs's which are*

(i) all ttN*; and*

(ii) involve only commands which occur as subcommands of $\vec{C}$;

is such that, with $\vec{D} = \overrightarrow{\nabla_* C/Y}$,

$$\Omega \ \cup \ \{ \ \vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_j \vec{C}/\vec{Y}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z}) \mid 1 \leq j \leq k \ \} \quad \vdash'$$

$$\bigwedge_{1 \leq j \leq k} (\vec{x} \approx \vec{z} \ \rightarrow \ [(C_j)_{\vec{D}/\vec{Y}}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z})) \ .$$

The useful Ω here is the set of all $(\vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_i \vec{C}'/\vec{Y}']A(\nabla_i \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}))$ as $\nabla_i \vec{C}'/\vec{Y}'$ ranges over all subcommands, of bits of $\vec{C}$, which have that form.

To dramatize the contrast between $\vdash'$ and $\vdash''$, note that $(\mathsf{AX})_{[\nabla]}$ gives a completely trivial derivation to witness

$$\vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_j \vec{C}/\vec{Y}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z}) \ \vdash'' \ (\vec{x} \approx \vec{z} \ \rightarrow \ [(C_j)_{\vec{D}/\vec{Y}}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z})) \ ,$$

and lots more.

Proof that M22.2 implies M22.1. We'll fix $j = \ell$ on the right-hand side of $\vdash'$, and show

$$\Omega \ \cup \ \{ \ \vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_j \vec{C}/\vec{Y}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z}) \mid 1 \leq j \leq k \ \} \quad \vdash'$$

$$(\vec{x} \approx \vec{z} \ \rightarrow \ [(C_\ell)_{\vec{D}/\vec{Y}}]A(\nabla_\ell \vec{C}/\vec{Y}, \vec{x} \approx \vec{z})) \ .$$

In **M22.2**, take $F = \vec{x} \approx \vec{z}$ and $G = A(\nabla_\ell \vec{C}/\vec{Y}, \vec{x} \approx \vec{z})$ and $D_1 = (C_\ell)_{\vec{D}/\vec{Y}}$. To see that $(F \rightarrow [D_1]G)$ is true in **N**, the validity of $(\mathsf{AX})_{[\nabla]}$ reduces it to showing that $(F \rightarrow [\nabla_\ell \vec{C}/\vec{Y}]G)$ ttN. The latter is immediate from the definition of A in **M22.0**. So we can apply **M22.2** and get

$$\Gamma_{(C_\ell)_{\vec{D}/\vec{Y}}} \ \vdash' \ (F \rightarrow [D_1]G) \ .$$

Thus it remains only to show that

$$\Gamma_{(C_\ell)_{\vec{D}/\vec{Y}}} \ \subset \ \Omega \cup \{\ \vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_j \vec{C}/\vec{Y}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z}) \mid 1 \leq j \leq k \ \}\ .$$

This amounts to the fact that, for fixed $\vec{C}/\vec{Y}$, if $\nabla_i \vec{C}'/\vec{Y}'$ is a subcommand of $(C_\ell)_{\vec{D}/\vec{Y}}$ where $\vec{D} = \overrightarrow{\nabla_* C/Y}$, then either

(i) $\nabla_i \vec{C}'/\vec{Y}' \ = \ \nabla_j \vec{C}/\vec{Y}$ for some j; or

(ii) $\nabla_i \vec{C}'/\vec{Y}'$ is a subcommand of a bit of $\vec{C}$.

For this, combine the definition of *subcommand* with the inductive definition of $C_{\vec{D}/\vec{Y}}$ for general $\vec{D}/\vec{Y}$ and C to prove that, *for any commands B, C and D, if B is a subcommand of $C_{\vec{D}/\vec{Y}}$, then it must be : $C_{\vec{D}/\vec{Y}}$; or a subcommand of C ; or a subcommand of a bit of $\vec{D}$.* The inductive proof (on C) is entirely mechanical.

N.B. Just above, it is important to use the case $D_1 = (C_\ell)_{\vec{D}/\vec{Y}}$ from **22.2**, not just the case $D_1 = \nabla_j \vec{C}/\vec{Y}$. We cannot use the extra rule $(\mathsf{AX})_{[\nabla]}$ (which is needed for $\vdash''$) when doing a $\vdash'$-derivation, or the trick of 'substituting for $\nabla_j \vec{C}/\vec{Y}$' could lead to an unsound system—i.e. **M11** would fail; see its proof, which is that of Theorem 11 in [**sing**] with notational changes.

Deduction of Theorem M22 from M22.1 and M22.2. Proceed by induction on D_1 to show $\vdash (F \rightarrow [D_1]G)$ from its truth in **N**. Since $\vdash'$ is stronger than $\vdash$, we have $\Gamma_{D_1} \vdash (F \rightarrow [D_1]G)$ for the set Γ_{D_1} in **22.2**. It remains to prove that $\vdash \mathcal{D}$ for each $\mathcal{D} \in \Gamma_{D_1}$.

Any such $\mathcal{D}$ has the form $F_2 \rightarrow [D_2]G_2$ for $1^{\underline{\text{st}}}$order F_2 and G_2, is $\mathsf{tt}\mathbf{N}$, and D_2 has the form $\nabla_j \vec{C}/\vec{Y}$ and is a subcommand of D_1. Thus in all but one case, the induction on D_1 gives $\vdash \mathcal{D}$ as required.

In that case, for some j, $D_1 = D_2 = \nabla_j \vec{C}/\vec{Y}$ and

$$\mathcal{D} = (\vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_j \vec{C}/\vec{Y}]A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z}))\ .$$

Do all j simultaneously. This is done by applying the instance of $(\mathsf{MRCS})_{[\ ]\rightarrow}$ for which $\mathcal{A}_j = \vec{x} \approx \vec{z}$, $\mathcal{B}_j = A(\nabla_j \vec{C}/\vec{Y}, \vec{x} \approx \vec{z})$ and

$$\Omega = \{\ \vec{x} \approx \vec{z} \ \rightarrow \ [\nabla_i \vec{C}'/\vec{Y}']A(\nabla_i \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}) \mid \nabla_i \vec{C}'/\vec{Y}' \text{ is a subcommand of a bit of } \vec{C}\ \}\ .$$

Verifying the main antecedent in this instance $(\mathsf{MRCS})_{[\ ]\rightarrow}$ consists merely of noting the conclusion of **M22.1**.

All $\mathcal{C} \in \Omega$ are true in $\mathbf{N}$ and have the form $F_3 \to [D_3]G_3$ in which D_3 is a *proper* subcommand of D_1 (because $D_3 = \nabla_i \vec{C}'/\vec{Y}'$, a subcommand of a bit of $\vec{C}$, and $D_1 = \nabla_j \vec{C}/\vec{Y}$). And so we have $\vdash \mathcal{C}$ for all $\mathcal{C} \in \Omega$ by the inductive hypothesis, giving the other antecedent, and completing the proof.

5. Technical results and all proofs re total correctness.

Lemma M23.0. *For all $\vec{C}/\vec{Y}$, all commands D, $1^{\underline{\text{st}}}$order formulas G, and variables $w \notin \vec{C} \cup D \cup G$, there is a $1^{\underline{\text{st}}}$order formula $B(w, \vec{C}/\vec{Y}, D, G)$—("$B$" for "before" rather than "pre")—such that*

$$B(w, \vec{C}/\vec{Y}, D, G)\ \mathsf{tt}@s \iff < D_{\vec{E}/\vec{Y}} > G\ \mathsf{tt}@s \quad \text{with} \quad \vec{E} = \overrightarrow{(\vec{C}/\vec{Y})^{<s(w)>}}.$$

We don't here use the notation $F(t)$, elsewhere denoting F with all free occurrences of some-or-other variable replaced by the term t. The "w" in $B(w, \vec{C}/\vec{Y}, D, G)$ is there for a different reason: to tell us which variable is the 'special one', playing a 'counting role' in its semantics, as defined by the display in the lemma.

It follows from that semantics (though not directly utilized here) that

$$\exists w B(w, \vec{C}/\vec{Y}, D, G) \ \rightarrow \ < D_{\vec{E}_1/\vec{Y}} > G \quad \mathbf{ttN} \quad \text{with} \quad \vec{E}_1 = \overrightarrow{\nabla C/Y}.$$

In fact, $\exists w B(w, \vec{C}/\vec{Y}, D, G)$ is the 'universal' $1^{\underline{\text{st}}}$order formula J for which we have $(J \rightarrow < D_{\vec{E}_1/\vec{Y}} > G)\ \mathbf{ttN}$, in the sense that $(J \rightarrow \exists w B(w, \vec{C}/\vec{Y}, D, G))\ \mathbf{ttN}$ for any such J. Summarizing, for all J,

$$J \rightarrow < D_{\vec{E}_1/\vec{Y}} > G\ \ \mathbf{ttN} \iff J \rightarrow \exists w B(w, \vec{C}/\vec{Y}, D, G)\ \ \mathbf{ttN}\ .$$

Note that the command $D_{\vec{E}_1/\vec{Y}}$ would be the standard simulation for

$$\mathsf{begin}\ \textit{declare}\ Y_1\ \textit{to be}\ C_1\ ;\ \cdots\ ;\ \textit{declare}\ Y_k\ \textit{to be}\ C_k\ ;\ \textit{do}D\ \mathsf{end}\ .$$

In each of **M23.1** to **M23.4** below, a $\vec{C}/\vec{Y}$, a variable w, and variable strings $\vec{x},\ \vec{z}$ are involved.

Let us just use $B(\vec{C}/\vec{Y}, j)$ to denote $B(w, \vec{C}/\vec{Y}, callY_j, \vec{x} \approx \vec{z})$.

This notation is only used with $\vec{x}$ and $\vec{z}$ disjoint strings of distinct variables, with all variables in $\vec{C}$ from $\vec{x}$, and with one more new variable w, but it occurs about 40 times below!

Remark. The definition of $B(\vec{C}/\vec{Y}, j)$ and the semantics of $B(w, \vec{C}/\vec{Y}, D, G)$ in general yield

$$B(\vec{C}/\vec{Y}, j)\ \mathsf{tt}@s \iff \text{for some } s',\ \text{we have } (s, s') \in m((\vec{C}/\vec{Y})_j^{<s(w)>}) \text{ and } s'(\vec{x}) = s'(\vec{z})\ .$$

Thus, from the semantics of $\nabla_j \vec{C}/\vec{Y}$,

$\exists w\ B(\vec{C}/\vec{Y}, j)\ \mathsf{tt}@s \iff$ for some s', we have $(s, s') \in m(\nabla_j \vec{C}/\vec{Y})$ and $s'(\vec{x}) = s'(\vec{z})$.

So the following is true in **N**:

$$\exists w\ B(\vec{C}/\vec{Y}, j) \longleftrightarrow\ < \nabla_j \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\ .$$

Deriving the '→-half' of that wfs looms large just ahead.

Lemma M23.5. *This is identical to* **M22.5** *except for replacing* $[C]$ *by* $< C >$ *for each command* C*, and replacing* $\vdash'$ *by* $\vdash^w$*.*

The proof is virtually identical also.

Proof of M23.5. Just change every [ ] to < > in the proof of **M22.5.**

Lemma M23.4. *Under the conditions listed below, each of the following four* $1^{\underline{\text{st}}}$*order formulas is true in* **N***.*

(i)(a) $F \ \rightarrow\ \exists \vec{z}((\exists w B(\vec{C}/\vec{Y}, i)) \wedge |G|^{\vec{x}\mapsto\vec{z}})$;

(b) $B(w, \vec{C}/\vec{Y}, E, G) \ \rightarrow\ \exists \vec{z}(B(w, \vec{C}/\vec{Y}, E, \vec{x} \approx \vec{z}) \wedge |G|^{\vec{x}\mapsto\vec{z}})$;

(ii) $\neg |B(\vec{C}/\vec{Y}, i)|^{w\mapsto 0}$;

(iii) $|B(\vec{C}/\vec{Y}, i)|^{w\mapsto w+1} \ \rightarrow\ B(w, \vec{C}/\vec{Y}, C_i, \vec{x} \approx \vec{z})$.

<u>*Assumptions:*</u> *We are given* $\vec{C}/\vec{Y}$*, and matching disjoint lists* $\vec{x}$ *and* $\vec{z}$ *of pairwise distinct variables such that all variables in* $\vec{C}$ *are from* $\vec{x}$*, plus a variable* w *not from* $\vec{x} \cup \vec{z}$*. In* (i)(a)*, assume* $F \rightarrow < \nabla_i \vec{C}/\vec{Y} > G$ *is true in* **N***, with no variables from* $\vec{z}$ *in the* $1^{\underline{\text{st}}}$*order formulas* F *and* G *in both parts of* (i)*, and* E *any command in* (i)(b)*.*

Proof of M23.4(i)(a) Assume that

$$\exists \vec{z}((\exists w B(\vec{C}/\vec{Y}, i)) \wedge |G|^{\vec{x}\mapsto\vec{z}})\ \ \mathsf{ff}@s\ .$$

Then $F\ \mathsf{ff}@s$ follows, as required, by showing $< \nabla_i \vec{C}/\vec{Y} > G\ \mathsf{ff}@s$, using that $(F \rightarrow < \nabla_i \vec{C}/\vec{Y} > G)\ \mathsf{tt}@s$.
Now the displayed formula, with $\exists \vec{z}$ erased, is $\mathsf{ff}@s_1$, for all s_1 which agree with s except possibly on $\vec{z}$. Fix such an s_1. Then either $|G|^{\vec{x}\mapsto\vec{z}}\ \mathsf{ff}@s_1$ or

the $\exists w B$-part part of the displayed formula is $\mathsf{ff}@s_1$. So one of the following must hold:
(I) $|G|^{\vec{x}\to\vec{z}}\ \mathsf{ff}@s_1$; or
(II) for some s_1', $(s_1, s_1') \in m(\nabla_i \vec{C}/\vec{Y})$ but $s_1'(\vec{x}) \neq s_1'(\vec{z})$; or
(III) $\nabla_i \vec{C}/\vec{Y}$ 'diverges' at input s_1 .

The deduction of (II) or (III) from the falsity of the '$\exists w$-part' of the displayed formula is a straightforward consequence of the semantic definition of B in **M23.0** and that of the m-function on $\nabla_i \vec{C}/\vec{Y}$.
But (III) $\implies$ $< \nabla_i \vec{C}/\vec{Y} > G\ \mathsf{ff}@s_1$ $\implies$ $< \nabla_i \vec{C}/\vec{Y} > G\ \mathsf{ff}@s$, as required, the latter $\implies$ because neither $\vec{C}$ nor G has any variable from $\vec{z}$. So we may assume:

(IV) $\nabla_i \vec{C}/\vec{Y}$ 'converges' at input s_1 for *all* s_1 which agree with s except possibly at $\vec{z}$.
This last statement with $s_1 = s$ gives us an s' with $(s, s') \in m(\nabla_i \vec{C}/\vec{Y})$. Use it to define $s_2 := s_{\vec{z}\mapsto s'(\vec{x})}$. Then s_2 is one such s_1, so (IV) with $s_1 = s_2$ gives us an s_2' with $(s_2, s_2') \in m(\nabla_i \vec{C}/\vec{Y})$. Now

$$s_2'(\vec{z}) \ = \ s_2(\vec{z}) \ = \ s'(\vec{x}) \ = \ s_2'(\vec{x}) \ ,$$

so (II) fails when $s_1 = s_2$, forcing (I) to hold for s_2. But that fact [namely, $|G|^{\vec{x}\to\vec{z}}\ \mathsf{ff}@s_2$] forces $G\ \mathsf{ff}@s'$, because $s_2(\vec{z}) \ = \ s'(\vec{x})$. Since $\nabla_i \vec{C}/\vec{Y}$ converges at input s to s', we now have $< \nabla_i \vec{C}/\vec{Y} > G\ \mathsf{ff}@s$, completing the proof.

Proof of M23.4(i)(b). Assume the line displayed just below. We have

$$B(w, \vec{C}/\vec{Y}, E, G)\ \mathsf{tt}@s$$
$$\iff \quad < E_{\vec{D}/\vec{Y}} > G\ \mathsf{tt}@s \qquad \text{for } \vec{D} = \overrightarrow{(\vec{C}/\vec{Y})^{<s(w)>}}$$
$$\iff \quad \exists s' \text{ with } (s, s') \in m(E_{\vec{D}/\vec{Y}}) \text{ and } G\ \mathsf{tt}@s' \ .$$

Now let $\bar{s} := s_{\vec{z}\mapsto s'(\vec{x})}$. We'll show that $B(w, \vec{C}/\vec{Y}, E, \vec{x} \approx \vec{z})$ and $|G|^{\vec{x}\to\vec{z}}$ are both $\mathsf{tt}@\bar{s}$. Since $\bar{s}$ agrees with s except at $\vec{z}$, this shows as required that

$$\exists \vec{z}(B(w, \vec{C}/\vec{Y}, E, \vec{x} \approx \vec{z}) \wedge |G|^{\vec{x}\to\vec{z}})\mathsf{tt}@s \ .$$

As for the latter,

$$|G|^{\vec{x}\to\vec{z}}\ \mathsf{tt}@\bar{s} \iff G\ \mathsf{tt}@\bar{s}_{\vec{x}\mapsto\bar{s}(\vec{z})} \ .$$

But $\bar{s}_{\vec{x}\mapsto\bar{s}(\vec{z})}$ and s' agree except at $\vec{z}$, no variables in G are from $\vec{z}$, and $G\ \mathsf{tt}@s'$, so that does it.

As for the former, copying the first set of displays with G specialized, and s changed to $\bar{s}$,

$$B(w,\vec{C}/\vec{Y},E,\vec{x}\approx\vec{z})\ \mathsf{tt}@\bar{s} \iff < E_{\vec{D}/\vec{Y}} > \vec{x}\approx\vec{z}\ \ \mathsf{tt}@\bar{s}$$

$$\iff \exists \bar{s}' \text{ with } (\bar{s},\bar{s}')\in m(E_{\vec{D}/\vec{Y}}) \text{ and } \vec{x}\approx\vec{z}\ \ \mathsf{tt}@\bar{s}' \ .$$

But $\bar{s}(w)=s(w)$, and the unique $\bar{s}'$ with $(\bar{s},\bar{s}')\in m(E_{\vec{D}/\vec{Y}})$ is $s'_{\vec{z}\mapsto s'(\vec{x})}$, where clearly $\vec{x}\approx\vec{z}$ is tt, so we are done.

Proof of M23.4(ii). For a contradiction, assume

$$\neg|B(\vec{C}/\vec{Y},i)|^{w\mapsto 0}\ \ \mathsf{ff}@s \ ,$$

so that $|B(\vec{C}/\vec{Y},i)|^{w\mapsto 0}\ \mathsf{tt}@s$. Thus

$$B(\vec{C}/\vec{Y},i)\ \ \mathsf{tt}@s_{w\mapsto 0} \ .$$

Then, from the general definition of B,

$$< (callY_i)_{\vec{D}/\vec{Y}} > G\ \mathsf{tt}@s_{w\mapsto 0} \qquad \text{for } \vec{D}=\overrightarrow{(\vec{C}/\vec{Y})^{<s_{w\mapsto 0}(w)>}}=\overrightarrow{(\vec{C}/\vec{Y})^{<0>}}$$

i.e.

$$< (\vec{C}/\vec{Y})_i^{<0>} > G\ \mathsf{tt}@s_{w\mapsto 0}\ , \quad \text{or equivalently} \quad < callY_i > G\ \mathsf{tt}@s_{w\mapsto 0}\ ,$$

which contradicts the emptiness of $m(callY_i)$.

Proof of M23.4(iii). Let $s_+ := s_{w\mapsto s(w)+_{\mathbf{N}}1_{\mathbf{N}}}$. Then the statements in following list are all logically equivalent :

$$|B(\vec{C}/\vec{Y},i)|^{w\mapsto w+1}\ \mathsf{tt}@s \ \ ; \ \ B(\vec{C}/\vec{Y},i)\ \mathsf{tt}@s_+ \ \ ;$$

$$< (\vec{C}/\vec{Y})_i^{<s_+(w)>} > \vec{x}\approx\vec{z}\ \mathsf{tt}@s_+ \ \ ; \ \ < (\vec{C}/\vec{Y})_i^{<s(w)+_{\mathbf{N}}1_{\mathbf{N}}>} > \vec{x}\approx\vec{z}\ \mathsf{tt}@s \ \ ;$$

$$< (C_i)_{\vec{D}/\vec{Y}} > \vec{x}\approx\vec{z}\,\mathsf{tt}@s \text{ with } \vec{D}=\overrightarrow{(\vec{C}/\vec{Y})^{<s(w)>}} \ ; \ B(w,\vec{C}/\vec{Y},C_i,\vec{x}\approx\vec{z})\ \mathsf{tt}@s \ .$$

The 2nd and 5th 'semicolons' appeal to the definition of B; the 3rd to the fact that s and s_+ agree except on w, which does not occur in $\vec{C}$ nor in $\vec{x}\approx\vec{z}$; and the 4th to the inductive definition of $(\vec{C}/\vec{Y})_i^{<n>}$.

Thus we have proved the stronger result (not needed later), where the symbol $\rightarrow$ in **M23.4**(iii) is replaced with $\leftrightarrow$.

Lemma M23.3. *For any* $1^{\underline{\text{st}}}$*order* F *and* G*, any* $\vec{C}/\vec{Y}$*, and matching disjoint lists* $\vec{x}$ *and* $\vec{z}$ *of pairwise distinct variables such that all variables from* $\vec{C}$ *are in* $\vec{x}$*, if* $(F \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G)$ ttN *, then*

$$\{(\exists w\ B(\vec{C}/\vec{Y}, i)) \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\} \quad \vdash^w \quad (F \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G)\ .$$

Proof that M23.4(i) **implies M23.3.** First we prove the special case when no $\vec{z}$-variables occur in F nor in G. Here is a slightly abbreviated $\vdash^w$-derivation for that :

$(\exists w\ B(\vec{C}/\vec{Y}, i)) \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}$ (premiss)

$\exists w\ B(\vec{C}/\vec{Y}, i) \wedge |G|^{\vec{x}\rightarrow\vec{z}} \ \rightarrow\ \ < \nabla_i \vec{C}/\vec{Y} > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}})$
$(\mathsf{AX})_{<\rightarrow>}$ and (MP)

$\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}} \ \rightarrow\ G$ (ORAC)

$< \nabla_i \vec{C}/\vec{Y} > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}}) \ \rightarrow\ \ < \nabla_i \vec{C}/\vec{Y} > G$ $(\mathsf{UNAR})_{<\ >}$

$\exists w B(\vec{C}/\vec{Y}, i) \wedge |G|^{\vec{x}\rightarrow\vec{z}} \ \rightarrow\ \ < \nabla_i \vec{C}/\vec{Y} > G$ (HYSY)

$\exists \vec{z}(\exists w B(\vec{C}/\vec{Y}, i) \wedge |G|^{\vec{x}\rightarrow\vec{z}}) \ \rightarrow\ \ < \nabla_i \vec{C}/\vec{Y} > G$ $(\mathsf{PRE})^{\vec{z}}$

$F \rightarrow\ \exists \vec{z}(\exists w B(\vec{C}/\vec{Y}, i) \wedge |G|^{\vec{x}\rightarrow\vec{z}})$ (ORAC) and **M23.4**(i)(a)

$F \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G$ (HYSY)

Now in the general case, let $\vec{u}$ be a matching list of pairwise distinct variables, disjoint from $w, \vec{x}$ and $\vec{z}$. Define F_1 to be $|F|^{\vec{z}\rightarrow\vec{u}}$ and let G_1 be $|G|^{\vec{z}\rightarrow\vec{u}}$, so F_1 and G_1 have no $\vec{z}$-variables. Since the validity of $(\mathsf{SUB})_1^{\vec{z}\rightarrow\vec{u}}$ entails that the truth of $F \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G$ in $\mathbf{N}$ also guarantees the truth in $\mathbf{N}$ for the wfs $F_1 \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G_1$, the special case above assures us that

$$\{(\exists w\ B(\vec{C}/\vec{Y}, i)) \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\} \quad \vdash^w \quad (F_1 \rightarrow\!< \nabla_i \vec{C}/\vec{Y} > G_1)\ .$$

But now application of $(\mathsf{SUB})_1^{\vec{u}\rightarrow\vec{z}}$ (and that doesn't violate the $\vdash^w$-restrictions!) allows us the erase the subscripts on F and G in the last display, as required.

Lemma M23.2. *Suppose given a command D_1, and $1^{\underline{\text{st}}}$order formulas F and G, such that $(F \rightarrow\!< D_1 > G)$ $\mathsf{tt}\mathbf{N}$. For each i and $\vec{C}/\vec{Y}$ such that $\nabla_i\vec{C}/\vec{Y}$ is a sub-command of D_1, choose a pair of matching disjoint lists $\vec{x}$ and $\vec{z}$ of pairwise distinct variables, and variable $w \notin \vec{x} \cup \vec{z}$, such that all the variables in $\vec{C}$ are in $\vec{x}$. Let the set Λ_{D_1} consist of all formulas (one for each such i and $\vec{C}/\vec{Y}$)*

$$(\exists w\ B(\vec{C}/\vec{Y}, i)) \ \rightarrow \ \ < \nabla_i\vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\ .$$

Then $\Lambda_{D_1} \ \vdash^w \ (F \rightarrow\!< D_1 > G)$.

Proof that (M23.3 plus M23.5) imply M23.2. This proceeds by induction on commands D_1, which we shall re-name as just D, since there is no danger here (only in the proof of **M23**!) of confusing it with the D in **23.1**.

When $D = callX_j$: By validity of $(\mathsf{AX})_{<call>}$, the wfs $< callX_j > G$ $\mathsf{ff}@s$ for all s. So the truth in $\mathbf{N}$ of $F \rightarrow\!< callX_j > G$ gives us that F $\mathsf{ff}@s$, and so $\neg F$ $\mathsf{tt}@s$, for all s. Now (ORAC) and $(\mathsf{P})_3$ give us a 2-line derivation witnessing $\vdash^w (F \rightarrow\!< callX_j > G)$, as required.

When $D = y \leftarrow\!\!\div t$: By the soundness of $(\mathsf{AX})_{<\leftrightarrow>}$, we see that

$$(F \rightarrow\!< y \leftarrow\!\!\div t > G)\ \mathsf{tt}\mathbf{N} \quad \Longrightarrow \quad (F \rightarrow |G|^{y \rightarrow t})\ \mathsf{tt}\mathbf{N}\ .$$

So here's a little derivation doing the job :

$F \rightarrow \lvert G\rvert^{y \rightarrow t}$	(ORAC)
$\lvert G\rvert^{y \rightarrow t} \leftrightarrow \ \ < y \leftarrow\!\!\div t > G$	$(\mathsf{AX})_{<\leftrightarrow>}$
$\lvert G\rvert^{y \rightarrow t} \rightarrow \ \ < y \leftarrow\!\!\div t > G$	$(\leftrightarrow)$
$F \rightarrow\!< y \leftarrow\!\!\div t > G$	(HYSY)

When $D = \nabla_i\vec{C}/\vec{Y}$: The set Λ_D in this case contains the element

$$(\exists w\ B(\vec{C}/\vec{Y}, i)) \ \rightarrow \ \ < \nabla_i\vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\ ,$$

so **23.3** gives the result immediately.

When $D = (D'; D'')$ or $ite(H)(D')(D'')$: Apply **23.5** with $\Gamma_1 = \Lambda_{D'}$ and $\Gamma_2 = \Lambda_{D''}$, noting that $\Lambda_D = \Lambda_{D'} \cup \Lambda_{D''}$ for both types of D here. Use the inductive hypotheses for D' and D'' as the hypotheses in **23.5**. The latter's conclusions are exactly the required results.

Lemma M23.1. *For each $\vec{C}/\vec{Y}$, pair of matching disjoint lists $\vec{x}$ and $\vec{z}$ of pairwise distinct variables such that all variables from $\vec{C}$ are in $\vec{x}$, and variable $w \notin \vec{x} \cup \vec{z}$, the finite set Ω of wfs's below, which are all* ttN*, is such that, for all* $1^{\underline{\text{st}}}$*order formulas G and subcommands D of bits of $\vec{C}$, we have*

$$\Omega \ \cup \ \{ \ B(\vec{C}/\vec{Y}, i) \rightarrow < \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z} \mid 1 \leq i \leq k \ \} \ \ \vdash^w$$

$$B(w, \vec{C}/\vec{Y}, D, G) \rightarrow < D_{\vec{E}/\vec{Y}} > G \ , \ \ \text{where } \vec{E} = \overrightarrow{\nabla_* C/Y} \ .$$

The Ω which usefully does the trick is the set of all wfs's
$B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}) \rightarrow \ \ < (\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}} > \vec{x} \approx \vec{z}$ *, as j and $\vec{C}'/\vec{Y}'$ range over all pairs for which $\nabla_j \vec{C}'/\vec{Y}'$ is a subcommand of a bit of $\vec{C}$.*

The lemma above will only be used in the case $D = C_j$ and $G = \vec{x} \approx \vec{z}$; but the general case seems needed for seeing how to prove it—namely, by induction on D, and with one inductive case really needing general G. Note that the subscript in $(\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}}$ isn't needed as long as we are working with simple recursion, since then, $\nabla_j \vec{C}'/\vec{Y}'$ has no free occurrences of $callX$ for any procedure variable X, much less any of the form $callY_i$ for which to substitute E_i. (They are all of the non-free form $callY_j'$.) But we'll leave the lemma as above, showing that, along with everything else so far, we could just as well be working in $\mathcal{R}ec$ as in $\mathcal{R}ec_-$.

Proof of M23.1. Inductively there will be six cases:

When $D = y \leftarrow\!\!\!\div t$: For any D with no free $callY_j$-subcommands, and twice using that $D_{\vec{E}/\vec{Y}} = D$ for such D and *any* $\vec{E}$, for a certain $\vec{E}_0$ we have

$$(I) \ \ B(w, \vec{C}/\vec{Y}, D, G)\, \mathsf{tt@}s \iff \ < D_{\vec{E}_0/\vec{Y}} > G\, \mathsf{tt@}s \iff \ < D > G\, \mathsf{tt@}s \ ;$$

and

$$(II) \ \ D_{\vec{E}/\vec{Y}} \ = \ D \ .$$

For D here, since $< D > G \longleftrightarrow |G|^{y \rightarrowtail t}$ is ttN, we can take $B(w, \vec{C}/\vec{Y}, D, G)$ to be $|G|^{y \rightarrowtail t}$ by (I), and, by (II), we only need to establish

$$\vdash^w \ (|G|^{y \rightarrowtail t} \rightarrow \ \ < y \leftarrow\!\!\!\div t > G) \ ,$$

which is immediate from $(\mathsf{AX})_{<\leftrightarrow>}$.

When $D = callX_i$ where $X_i \neq Y_j$ for any j: Here again $D_{\vec{E}/\vec{Y}} = D$, so what must be derived has the form $F \rightarrow\!< callX_i > G$. But $\neg < callX_i > G$ is immediately derivable from $(\mathsf{AX})_{<call>}$, so we then can propositionally derive $F \rightarrow\!< callX_i > G$.

This last case won't actually occur if we are allowing only *simple* recursion, but we'll include it to show that, along with everything else so far, we could just as well be working in $\mathcal{R}ec$ as in $\mathcal{R}ec_{-}$.

The next two cases are done in a manner which is very nearly the same as the proof of **M23.3**. But, for safety in a subject whose literature is infested with subtle errors, we will write down every detail.

When $D = callY_j$: First we prove the special case when no $\vec{z}$-variables occur in G. Here is a slightly abbreviated $\vdash^w$-derivation as required:

$B(\vec{C}/\vec{Y}, j) \rightarrow\!< \nabla_j \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}$ (premiss)

$B(\vec{C}/\vec{Y}, j) \wedge |G|^{\vec{x}\rightarrow\vec{z}} \rightarrow < \nabla_j \vec{C}/\vec{Y} > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}})$
$(\mathsf{AX})_{<\rightarrow>}$ and (MP)

$\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}} \rightarrow G$ (ORAC)

$< \nabla_j \vec{C}/\vec{Y} > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\rightarrow\vec{z}}) \rightarrow < \nabla_j \vec{C}/\vec{Y} > G$ $(\mathsf{UNAR})_{< >}$

$B(\vec{C}/\vec{Y}, j) \wedge |G|^{\vec{x}\rightarrow\vec{z}} \rightarrow < \nabla_j \vec{C}/\vec{Y} > G$ (HYSY)

$\exists \vec{z}(B(\vec{C}/\vec{Y}, j) \wedge |G|^{\vec{x}\rightarrow\vec{z}}) \rightarrow < \nabla_j \vec{C}/\vec{Y} > G$ $(\mathsf{PRE})^{\vec{z}}$

$B(w, \vec{C}/\vec{Y}, callY_j, G) \rightarrow \exists \vec{z}(B(\vec{C}/\vec{Y}, j) \wedge |G|^{\vec{x}\rightarrow\vec{z}})$
(ORAC) and **M23.4**(i)(b) with $E = callY_j$

$B(w, \vec{C}/\vec{Y}, callY_j, G) \rightarrow\!< \nabla_j \vec{C}/\vec{Y} > G$ (HYSY)

This last line is what we want, since $(callY_j)_{\vec{E}/\vec{Y}} = \nabla_j \vec{C}/\vec{Y}$.

Now in the general case, let $\vec{u}$ be a matching list of pairwise distinct variables, disjoint from $w, \vec{x}$ and $\vec{z}$. Let G_1 be $|G|^{\vec{z}\rightarrow\vec{u}}$, so G_1 has no $\vec{z}$-variables. The case above assures us that

$$\{(\exists w\ B(\vec{C}/\vec{Y}, j)) \rightarrow\!< \nabla_j \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\} \quad \vdash^w$$
$$(B(w, \vec{C}/\vec{Y}, callY_j, G_1) \rightarrow\!< \nabla_j \vec{C}/\vec{Y} > G_1) \ .$$

But now application of $(\mathsf{SUB})_1^{\vec{u}\to\vec{z}}$ (and that doesn't violate the $\vdash^w$-restrictions!) allows us the erase the subscript on G in the last display, as suffices.

When $D = \nabla_j \vec{C}'/\vec{Y}'$: It suffices to prove

$$B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}) \to \ < (\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}} > \vec{x} \approx \vec{z} \vdash^w$$

$$B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', G) \to \ < (\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}} > G \ ,$$

since on the left of the $\vdash^w$ we have an element of Ω. (This is where D being a subcommand of a bit of $\vec{C}$ is used.) Temporarily abbreviate $(\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}}$ to just C_0 and $B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z})$ to just B_0.

First we prove the special case when no $\vec{z}$-variables occur in G. Here is a slightly abbreviated $\vdash^w$-derivation as required:

$B_0 \to \ < C_0 > \vec{x} \approx \vec{z}$ (premiss)

$B_0 \wedge |G|^{\vec{x}\to\vec{z}} \ \to \ < C_0 > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\to\vec{z}})$
$(\mathsf{AX})_{<\to>}$ and (MP)

$\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\to\vec{z}} \ \to \ G$ (ORAC)

$< C_0 > (\vec{x} \approx \vec{z} \wedge |G|^{\vec{x}\to\vec{z}}) \ \to \ < C_0 > G$ $(\mathsf{UNAR})_{< >}$

$B_0 \wedge |G|^{\vec{x}\to\vec{z}} \ \to \ < C_0 > G$ (HYSY)

$\exists \vec{z}(B_0 \wedge |G|^{\vec{x}\to\vec{z}}) \ \to \ < C_0 > G$ $(\mathsf{PRE})^{\vec{z}}$

$B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', G) \to \ \exists \vec{z}(B_0 \wedge |G|^{\vec{x}\to\vec{z}})$
(ORAC) and $\mathbf{M23.4}$(i)(b) with $E = \nabla_j \vec{C}'/\vec{Y}'$

$B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', G) \to < C_0 > G$ (HYSY)

Now in the general case, let $\vec{u}$ be a matching list of pairwise distinct variables, disjoint from $w, \vec{x}$ and $\vec{z}$. Let G_1 be $|G|^{\vec{z}\to\vec{u}}$, so G_1 has no $\vec{z}$-variables. The case above assures us that

$$B_0 \to \ < C_0 > \vec{x} \approx \vec{z} \ \vdash^w \ B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', G_1) \to \ < C_0 > G_1) \ .$$

But now application of $(\mathsf{SUB})_1^{\vec{u}\to\vec{z}}$ (and that doesn't violate the $\vdash^w$-restrictions!) allows us the erase the subscripts on G in the last display, as required.

In the last two cases below, we have many subscripts $\vec{E}/\vec{Y}$. Every time this happens, $\vec{E} = \overrightarrow{\nabla_* C/Y}$, as in the statement of **M23.1**.

When $D = (D_1; D_2)$: Firstly, letting $B_* := B(w, \vec{C}/\vec{Y}, D_1, B(w, \vec{C}/\vec{Y}, D_2, G))$, we'll show that we may take

$$B(w, \vec{C}/\vec{Y}, (D_1; D_2), G) \;=\; B_* \;,$$

by showing

$$B(w, \vec{C}/\vec{Y}, (D_1; D_2), G) \;\longleftrightarrow\; B_* \quad \mathsf{tt}\mathbf{N} \;.$$

This is immediate from the following logical equivalences:

$$B(w, \vec{C}/\vec{Y}, (D_1; D_2), G)\,\mathsf{tt}@s \iff \;<(D_1; D_2)_{\vec{E}'/\vec{Y}} > G\,\mathsf{tt}@s \;\text{ with }\; \vec{E}' = \overrightarrow{(\vec{C}/\vec{Y})^{<s(w)>}}$$

$$\iff \;<(D_{1_{\vec{E}'/\vec{Y}}}; D_{2_{\vec{E}'/\vec{Y}}}) > G \;\; \mathsf{tt}@s \iff \;< D_{1_{\vec{E}'/\vec{Y}}} >< D_{2_{\vec{E}'/\vec{Y}}} > G \;\; \mathsf{tt}@s$$

$$\iff \;< D_{1_{\vec{E}'/\vec{Y}}} > B(w, \vec{C}/\vec{Y}, D_2, G)\;\mathsf{tt}@s \iff B_*\;\mathsf{tt}@s \;.$$

It remains then to establish, with

$$\Delta \;:=\; \Omega \;\cup\; \{\; B(\vec{C}/\vec{Y}, i) \to < \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z} \mid 1 \le i \le k \;\} \;,$$

that

$$\Delta \;\; \vdash^w \;\; (B_* \to < D_{\vec{E}/\vec{Y}} > G) \;.$$

By the inductive assumption re D_1, we have

$$\Delta \;\; \vdash^w \;\; B_* \to < D_{1_{\vec{E}/\vec{Y}}} > B(w, C, D_2, G) \qquad (I)$$

(Here $B(w, C, D_2, G)$ plays the usual role of G, so this is where 'general G' is needed.) The inductive assumption re D_2 gives

$$\Delta \;\; \vdash^w \;\; B(w, \vec{C}/\vec{Y}, D_2, G) \to < D_{2_{\vec{E}/\vec{Y}}} > G \qquad (II)$$

Combining $(\mathsf{UNAR})_{<\,>}$ and $(\mathsf{AX})_{<;>}$ allows us to $\vdash^w$-derive

$$< D_{1_{\vec{E}/\vec{Y}}} > B(w, \vec{C}/\vec{Y}, D_2, G) \to < (D_{1_{\vec{E}/\vec{Y}}}; D_{2_{\vec{E}/\vec{Y}}}) > G$$

from the RHS of (II). Using (HYSY) to combine the latter with (I) then yields the required result, since $D_{\vec{E}/\vec{Y}} = (D_{1_{\vec{E}/\vec{Y}}}; D_{2_{\vec{E}/\vec{Y}}})$.

Note that the use of $(\mathsf{UNAR})_{<\,>}$ is fine for $\vdash^w$ here, because w does not occur in $D_{1_{\vec{E}/\vec{Y}}}$, all of whose variables are from $\vec{x}$.

When $D = ite(H)(D_0)(D_1)$: In this case, letting

$$B_* \;:=\; (H \to B_+) \wedge (\neg H \to B_-) \;,$$

where

$$B_+ \;:=\; B(w, \vec{C}/\vec{Y}, D_0, G) \;\text{ and }\; B_- \;:=\; B(w, \vec{C}/\vec{Y}, D_1, G) \;,$$

we'll first show that we may take

$$B(w, \vec{C}/\vec{Y}, D, G) \;=\; B_* \;,$$

by showing

$$B(w, \vec{C}/\vec{Y}, D, G) \;\longleftrightarrow\; B_* \qquad \mathsf{ttN} \;.$$

This is immediate from the following logical equivalences:

$$B(w, \vec{C}/\vec{Y}, D, G) \;\; \mathsf{tt}@s \iff$$

$$< D_{\vec{E}'/\vec{Y}} > G \;\; \mathsf{tt}@s \quad \text{with} \;\; \vec{E}' = \overrightarrow{(\vec{C}/\vec{Y})^{<s(w)>}} \iff$$

$$< ite(H)(D_{0_{\vec{E}'/\vec{Y}}})(D_{1_{\vec{E}'/\vec{Y}}}) > G \;\; \mathsf{tt}@s \iff$$

$$(H \to < D_{0_{\vec{E}'/\vec{Y}}} > G) \wedge (\neg H \to < D_{1_{\vec{E}'/\vec{Y}}} > G) \;\; \mathsf{tt}@s \iff$$

$$(H \to B(w, \vec{C}/\vec{Y}, D_0, G)) \wedge (\neg H \to B(w, \vec{C}/\vec{Y}, D_1, G)) \;\; \mathsf{tt}@s \;.$$

It remains then to establish, with

$$\Delta \;:=\; \Omega \;\cup\; \{\; B(\vec{C}/\vec{Y},i) \rightarrow\!< \nabla_i\vec{C}/\vec{Y} > \vec{x} \approx \vec{z} \mid 1 \leq i \leq k \;\}\;,$$

that

$$\Delta \quad \vdash^w \quad (B_* \rightarrow\!< D_{\vec{E}/\vec{Y}} > G)\;.$$

The inductive hypotheses re D_j for $j = 0, 1$ give

$$\Delta \quad \vdash^w \quad B_{(-1)^j} \rightarrow\!< D_{j_{\vec{E}/\vec{Y}}} > G\;.$$

Simple propositional arguments plus $(\mathsf{AX})_{<ite>}$ give that $B_* \rightarrow\!< D_{\vec{E}/\vec{Y}} > G$ can be $\vdash^w$-derived from

$$\{(B_* \rightarrow (H \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G)) \wedge (B_* \rightarrow (\neg H \rightarrow\!< D_{1_{\vec{E}/\vec{Y}}} > G))\}\;,$$

using that $D_{\vec{E}/\vec{Y}} \;=\; ite(H)(D_{0_{\vec{E}/\vec{Y}}})(D_{1_{\vec{E}/\vec{Y}}})$. So we just need to 'fill in the middle', showing both

$$\{B_+ \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G\} \quad \vdash^w \quad B_* \rightarrow (H \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G)$$

and

$$\{B_- \rightarrow\!< D_{1_{\vec{E}/\vec{Y}}} > G\} \quad \vdash^w \quad B_* \rightarrow (\neg H \rightarrow\!< D_{1_{\vec{E}/\vec{Y}}} > G)\;.$$

A derivation for the second is exactly parallel (by changing subscript 0 to 1, $+$ to $-$, and H to $\neg H$) to the following (purely propositional) derivation for the first, so that will do it.

$B_+ \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G$	(premiss)
$(H \rightarrow B_+) \wedge H \rightarrow B_+$	(TAUT)
$(H \rightarrow B_+) \wedge H \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G$	(HYSY)
$B_* \wedge H \rightarrow (H \rightarrow B_+) \wedge H$	(TAUT)
$B_* \wedge H \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G$	(HYSY)
$B_* \rightarrow (H \rightarrow\!< D_{0_{\vec{E}/\vec{Y}}} > G)$	$(\mathsf{P})_1$

Deduction of Theorem M23 from M23.1, M23.2 and (ii) **,** (iii) **of M23.4**. To show $\vdash (F \to\!< D_1 > G)$ from its truth in **N**, by **M23.2** it suffices to establish $\vdash \mathcal{D}$ for all $\mathcal{D} \in \Lambda_{D_1}$. Proceed by induction on D_1. By (PRE), it suffices to prove

$$\vdash (B(\vec{C}/\vec{Y}, \ell) \ \to \ \ < \nabla_\ell \vec{C}/\vec{Y} > \vec{x} \approx \vec{z})$$

whenever $\nabla_\ell \vec{C}/\vec{Y}$ is a subcommand of D_1. We only need that 'subcommand fact' for one ℓ, and then we can prove the display simultaneously for all ℓ by taking the instance of $(\mathsf{MRCS})_{<\ >}$ in which

$$\mathcal{A}_\ell = B(\vec{C}/\vec{Y}, \ell) \ \text{ and } \ \mathcal{B}_\ell =< \nabla_\ell \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\,.$$

Now we verify that rule's antecedents in the order presented in its 'numerator', and specify which Ω will be employed.

(i) By **M23.4**(ii), the oracle gives a derivation of $\neg|\mathcal{A}_j|^{w\mapsto 0}$, which is $\neg|B(\vec{C}/\vec{Y}, j)|^{w\mapsto 0}$.

(ii) Taking

$$\Omega \ := \ \{\, B(w, \vec{C}/\vec{Y}, \nabla_j \vec{C}'/\vec{Y}', \vec{x} \approx \vec{z}) \to \ \ < (\nabla_j \vec{C}'/\vec{Y}')_{\vec{E}/\vec{Y}} > \vec{x} \approx \vec{z} \,|$$

$$\nabla_j \vec{C}'/\vec{Y}' \text{ subcommand of bits of } \vec{C}\ ; \vec{E} = \overrightarrow{\nabla_* C/Y}\,\}\ ,$$

we have $\vdash \mathcal{C}$ for all $\mathcal{C} \in \Omega$ by the inductive hypothesis, because all these wfs's have the form $F_0 \to\!< \nabla_j \vec{C}'/\vec{Y}' > G_0$ (this is precisely where we need to use the assumption that only simple recursion is allowed, so the subscript $\vec{E}/\vec{Y}$ is irrelevant!) for $1^{\underline{\text{st}}}$order F_0 and G_0, are true in **N**, and because $\nabla_j \vec{C}'/\vec{Y}'$ being a subcommand of a bit of $\vec{C}$, and $\nabla_\ell \vec{C}/\vec{Y}$ a subcommand of D_1, the first is a *proper* subcommand of the last.

(iii) Finally, we need, for each j, that

$$\Omega \ \cup \ \{\ B(\vec{C}/\vec{Y}, i) \to\!< \nabla_i \vec{C}/\vec{Y} > \vec{x} \approx \vec{z} \mid 1 \le i \le k\ \} \ \ \vdash^w$$

$$|B(\vec{C}/\vec{Y}, j)|^{w\to w+1} \to\!< \nabla_j \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}\,.$$

Now Ω is the correct one for applying **M23.1**, in which we take $D = C_j$ and $G = \vec{x} \approx \vec{z}$, so at least it gives a $\vdash^w$-derivation of

$$B(w, \vec{C}/\vec{Y}, C_j, \vec{x} \approx \vec{z}) \ \to \ \ < (C_j)_{\vec{E}/\vec{Y}} > \vec{x} \approx \vec{z}\,, \ \ \text{where } \vec{E} = \overrightarrow{\nabla_* C/Y}\ .$$

By $(\mathsf{AX})_{<\nabla>}$, we can replace $< (C_j)_{\vec{E}/\vec{Y}} > \vec{x} \approx \vec{z}$ by $< \nabla_j \vec{C}/\vec{Y} > \vec{x} \approx \vec{z}$, which is half the battle. The other half is immediate from (HYSY), the oracle, and **M23.4**(iii). It replaces

$$B(w, \vec{C}/\vec{Y}, C_j, \vec{x} \approx \vec{z}) \text{ by } |B(\vec{C}/\vec{Y}, j)|^{w \mapsto w+1} .$$

So that's it.

Reference

[**deBa**] deBaaker, Jaco *Mathematical Theory of Program Correctness.* Prentice/Hall International, 1980.

[**Harel**] Harel, David *First-Order Dynamic Logic.* Lecture Notes in CS # 68, Springer, 1979. See also *Correctness of regular deterministic programs.* Theor. Comp. Sci. 12(1980) 61-81

[**sing**] Hoffman, P. *Deterministic Dynamic Logic Imperative Recursive Programming Proof Systems.* (this website).

[**submit**] Hoffman, P. *A Proof System for Recursive Programming with Local Declarations .* (this website).