APPENDIX A

Denotational semantics: proofs

We show that every closed term M has a computable functional $[\![M]\!]$ as its denotation.

A.1. Unification

We show that for any two constructor terms one can decide whether there exists a unifier, and if so, compute a most general one. A solution of this problem has been given by Robinson (1965). In the formulation of the algorithm below we follow Martelli and Montanari (1982).

By a constructor term P, Q (term for short) we mean a term built from variables x, y, z and constructors C by application. A *substitution* is a finite set $\vartheta = \{P_1/x_1, \ldots, P_n/x_n\}$ of pairs of variables and terms, such that $x_i \neq x_j$ for $i \neq j$, and $P_i \neq x_i$ for all i. An element P_i/x_i of ϑ is called a *binding* (of x_i to P_i). By $P\vartheta$ we denote the result of simultaneously replacing each variable x_i in P by P_i, and call $P\vartheta$ the *instance* of P induced by ϑ. We shall use ϑ, η, ζ for substitutions. Let ε be the empty substitution. For given substitutions

$$\vartheta = \{P_1/x_1, \ldots, P_n/x_n\}$$
$$\eta = \{Q_1/y_1, \ldots, Q_m/y_m\},$$

the *composition* $\vartheta\eta$ of ϑ and η is the substitution obtained by deleting in the set

$$\{P_1\eta/x_1, \ldots, P_n\eta/x_n, Q_1/y_1, \ldots, Q_m/y_m\}$$

all bindings $P_i\eta/x_i$ such that $P_i\eta = x_i$, and also all bindings Q_j/y_j such that $y_j \in \{x_1, \ldots, x_n\}$. A substitution ϑ is *idempotent* if $\vartheta\vartheta = \vartheta$. A substitution ϑ is called *more general* than η (written $\eta \leq \vartheta$), if there is a substitution ζ such that $\eta = \vartheta\zeta$. ϑ and η are *equivalent*, if $\vartheta \leq \eta \leq \vartheta$.

It is easy to see that $(P\vartheta)\eta = P(\vartheta\eta)$, and that composition is associative.

We now come to the unification problem. By this we mean the question whether for two given terms P, Q there is a substitution ϑ "unifying" the two terms, i.e., with the property $P\vartheta = Q\vartheta$.

Let E denote finite equation systems, i.e., multisets

$$\{P_1 = Q_1, \ldots, P_n = Q_n\}$$

of equations between terms (more precisely pairs of terms). Consider $\{\bot\}$ as a (contradictory) equation system. A substitution ϑ *unifies* E, if for every equation $P = Q$ in E we have $P\vartheta = Q\vartheta$; no ϑ unifies $\{\bot\}$. ϑ is a *most general unifier (mgu)* of E, if ϑ is a unifier of E and $\eta \leq \vartheta$ for every unifier η of E.

The following characterization of idempotent mgus will be useful in the proof of the Unification Theorem below.

LEMMA (Characterization of idempotent mgu's). *Let ϑ be a unifier of E. Then ϑ is an idempotent mgu of E iff $\eta = \vartheta\eta$ for all unifiers η of E.*

PROOF. Assume that ϑ is a unifier of E.

$\rightarrow$. Let ϑ be an idempotent mgu of E, and assume that η is a unifier of E. Since ϑ is a mgu of E, we have $\eta = \vartheta\zeta$ for some substitution ζ. Hence $\eta = \vartheta\zeta = \vartheta\vartheta\zeta = \vartheta\eta$.

$\leftarrow$. Assume that $\eta = \vartheta\eta$ for all unifiers η of E. Now let η be a unifier of E. Then $\eta \leq \vartheta$; therefore ϑ is a mgu. Since ϑ is a unifier, by assumption we have $\vartheta = \vartheta\vartheta$. □

DEFINITION (Unification algorithm). $E \mapsto_\vartheta E'$ is defined by

(a) $\{P = x\} \cup E \mapsto_\varepsilon \{x = P\} \cup E$, if P is not a variable.
(b) $\{x = x\} \cup E \mapsto_\varepsilon E$.
(c) $\{\mathrm{C}P_1 \dots P_n = \mathrm{C}Q_1 \dots Q_n\} \cup E \mapsto_\varepsilon \{P_1 = Q_1, \dots P_n = Q_n\} \cup E$.
(d) $\{\mathrm{C}P_1 \dots P_n = \mathrm{C}'Q_1 \dots Q_n\} \cup E \mapsto_\varepsilon \{\bot\}$ if $\mathrm{C} \neq \mathrm{C}'$.
(e) $\{x = P, P_1(x) = Q_1(x), \dots, P_n(x) = Q_n(x)\} \mapsto_{\{P/x\}}$
$\{P_1(P) = Q_1(P), \dots P_n(P) = Q_n(P)\}$ if $x \notin \mathrm{FV}(P)$.
(f) $\{x = P\} \cup E \mapsto_\varepsilon \{\bot\}$, if $x \in \mathrm{FV}(P)$ and $P \neq x$.

PROPOSITION. *Assume $E \mapsto_\vartheta E'$.*

(a) *If η' is a unifier of E', then $\vartheta\eta'$ is a unifier of E.*
(b) *If η is a unifier of E, then $\eta = \vartheta\eta$ and η is a unifier of E'.*

PROOF. By cases according to the definition of $E \mapsto_\vartheta E'$. Clearly it suffices to treat case (e).

Let η' be a unifier of E'. Then $\{P/x\}\eta'$ is a unifier of E.

Let η be a unifier of E. Then $x\eta = P\eta$, hence $\eta = \{P/x\}\eta$ (since both substitutions coincide on all variables), and moreover

$$P_i\{P/x\}\eta = P_i\eta = Q_i\eta = Q_i\{P/x\}\eta.$$

Hence η is a unifier of E'. □

COROLLARY. *Assume*

$$E_1 \mapsto_{\vartheta_1} E_2 \mapsto_{\vartheta_2} \dots E_n \mapsto_{\vartheta_n} E_{n+1}.$$

(a) *If ϑ is a unifier of E_{n+1}, then $\vartheta_1 \dots \vartheta_n\vartheta$ is a unifier of E_1.*

(b) *If η is a unifier of E_1, then $\eta = \vartheta_1 \dots \vartheta_n \eta$ and η is a unifier of E_{n+1}.*

PROOF. The first part clearly follows from the first part of the Proposition. The second part is proved by induction on n. For $n = 0$ there is nothing to show. In the step we split the assumption into

$$E_1 \mapsto_{\vartheta_1} E_2 \quad \text{and} \quad E_2 \mapsto_{\vartheta_2} \dots E_n \mapsto_{\vartheta_n} E_{n+1}.$$

By the second part of the Proposition we have that $\eta = \vartheta_1 \eta$ is a unifier of E_2. Hence by IH $\eta = \vartheta_2 \cdots \vartheta_n \eta$ is a unifier of E_{n+1}. Moreover we have $\eta = \vartheta_1 \eta = \vartheta_1 \vartheta_2 \dots \vartheta_n \eta$. □

UNIFICATION THEOREM. *Let E be a finite equation system. Then every sequence*

$$E = E_1 \mapsto_{\vartheta_1} E_2 \mapsto_{\vartheta_2} \dots$$

terminates with $E_{n+1} = \emptyset$ or $E_{n+1} = \{\bot\}$. In the first case E is unifiable, and $\vartheta_1 \dots \vartheta_n$ is an idempotent mgu of E. In the second case E is not unifiable.

PROOF. We first show termination using the lexicographic ordering of $\mathbf{N}^3$. To every $E = \{P_1 = Q_1, \dots, P_n = Q_n\}$ assign a triple $(n_1, n_2, n_3) \in \mathbf{N}^3$ by

$n_1 :=$ number of variables in E,

$n_2 :=$ number of occurrences of variables and constructors in E,

$n_3 :=$ number of equations $P = x$ in E such that P is not a variable.

In every step $E \mapsto_\vartheta E'$ the assigned triple decreases w.r.t. the lexicographic ordering of $\mathbf{N}^3$. This can be verified easily by considering the different cases: For (a), n_1, n_2 remain unchanged, and n_3 decreases. For (b), (c), (d) and (f), n_2 decreases, and n_1 does not increase. For (e), n_1 decreases. Hence our given sequence $E_1 \mapsto_{\vartheta_1} E_2 \mapsto_{\vartheta_2} \dots$ terminates with $E_n \mapsto_{\vartheta_n} E_{n+1}$. Then it is easy to see that either $E_{n+1} = \emptyset$ or $E_{n+1} = \{\bot\}$.

Case $E_{n+1} = \emptyset$. By the Corollary $\vartheta_1 \dots \vartheta_n$ is a unifier of E, and by the Proposition we have $\eta = \vartheta_1 \dots \vartheta_n \eta$ for every unifier η of E. Hence by the characterization of idempotent mgu's $\vartheta_1 \dots \vartheta_n$ is an idempotent mgu of E.

Case $E_{n+1} = \{\bot\}$. Then by the proposition E is not unifiable. □

A.2. Ideals as denotations of terms

Recall the definition of the relation $(\vec{U}, a) \in [\![\lambda_{\vec{x}} M]\!]$ in Section 2.3

The *height* of a derivation of $(\vec{U}, a) \in [\![\lambda_{\vec{x}} M]\!]$ is defined as usual, by adding 1 at each rule. We define its *D-height* similarly, where only rules (D) count.

We begin with some simple consequences of this definition. The following transformations preserve D-height:

$$\vec{V} \vdash \vec{U} \to (\vec{U}, a) \in [\![\lambda_{\vec{x}} M]\!] \to (\vec{V}, a) \in [\![\lambda_{\vec{x}} M]\!], \tag{12}$$

$$(\vec{U}, V, a) \in [\![\lambda_{\vec{x},y} M]\!] \leftrightarrow (\vec{U}, a) \in [\![\lambda_{\vec{x}} M]\!] \quad \text{if } y \notin \mathrm{FV}(M), \tag{13}$$

$$(\vec{U}, V, a) \in [\![\lambda_{\vec{x},y}(My)]\!] \leftrightarrow (\vec{U}, V, a) \in [\![\lambda_{\vec{x}} M]\!] \quad \text{if } y \notin \mathrm{FV}(M), \tag{14}$$

$$(\vec{U}, \vec{V}, a) \in [\![\lambda_{\vec{x},\vec{y}}(M(\vec{P}(\vec{y})))]\!] \leftrightarrow (\vec{U}, \vec{P}(\vec{V}), a) \in [\![\lambda_{\vec{x},\vec{z}}(M(\vec{z}))]\!]. \tag{15}$$

Proof. (12) and (13) are both proved by easy inductions on the respective derivations.

(14). Assume $(\vec{U}, V, a) \in [\![\lambda_{\vec{x},y}(My)]\!]$. By (A) we then have W such that $(\vec{U}, V, W) \subseteq [\![\lambda_{\vec{x},y} y]\!]$ (i.e., $V \vdash W$) and $(\vec{U}, V, W, a) \in [\![\lambda_{\vec{x},y} M]\!]$. By (12) from the latter we obtain $(\vec{U}, V, V, a) \in [\![\lambda_{\vec{x},y} M]\!]$. Now since $y \notin \mathrm{FV}(M)$, (13) yields $(\vec{U}, V, a) \in [\![\lambda_{\vec{x}} M]\!]$, as required. Conversely, assume $(\vec{U}, V, a) \in [\![\lambda_{\vec{x}} M]\!]$. Since $y \notin \mathrm{FV}(M)$, (13) yields $(\vec{U}, V, V, a) \in [\![\lambda_{\vec{x}} M]\!]$. Clearly we have $(\vec{U}, V, V) \subseteq [\![\lambda_{\vec{x},y} y]\!]$. Hence by (A) $(\vec{U}, V, a) \in [\![\lambda_{\vec{x},y}(My)]\!]$, as required. Notice that the D-height did not change in these transformations.

(15). By induction on $\vec{P}$, with a side induction on M. We distinguish cases on M. The cases x_i, C and D are follow immediately from (13). In case MN the following are equivalent by induction hypothesis:

$$(\vec{U}, \vec{V}, a) \in [\![\lambda_{\vec{x},\vec{y}}((MN)(\vec{P}(\vec{y})))]\!]$$
$$\exists_W((\vec{U}, \vec{V}, W) \subseteq [\![\lambda_{\vec{x},\vec{y}}(N(\vec{P}(\vec{y})))]\!] \wedge (\vec{U}, \vec{V}, W, a) \in [\![\lambda_{\vec{x},\vec{y}}(M(\vec{P}(\vec{y})))]\!])$$
$$\exists_W((\vec{U}, \vec{P}(\vec{V}), W) \subseteq [\![\lambda_{\vec{x},\vec{y}}(N(\vec{z}))]\!] \wedge (\vec{U}, \vec{P}(\vec{V}), W, a) \in [\![\lambda_{\vec{x},\vec{y}}(M(\vec{z}))]\!])$$
$$(\vec{U}, \vec{P}(\vec{V}), a) \in [\![\lambda_{\vec{x},\vec{y}}((MN)(\vec{z}))]\!].$$

The final case is where M is z_i. Then we have to show

$$(\vec{U}, \vec{V}, a) \in [\![\lambda_{\vec{x},\vec{y}}(P(\vec{y}))]\!] \leftrightarrow P(\vec{V}) \vdash a.$$

We distinguish cases on $P(\vec{y})$. If $P(\vec{y})$ is y_j, then both sides are equivalent to $V_j \vdash a$. In case $P(\vec{y})$ is $(\mathrm{C}\vec{Q})(\vec{y})$ the following are equivalent, using the induction hypothesis for $\vec{Q}(\vec{y})$

$$(\vec{U}, \vec{V}, a) \in [\![\lambda_{\vec{x},\vec{y}}((\mathrm{C}\vec{Q})(\vec{y}))]\!]$$
$$(\vec{U}, \vec{V}, a) \in [\![\lambda_{\vec{x},\vec{y}}(\mathrm{C}\vec{Q}(\vec{y}))]\!]$$
$$(\vec{U}, \vec{Q}(\vec{V}), a) \in [\![\lambda_{\vec{x},\vec{u}}(\mathrm{C}\vec{u})]\!]$$
$$(\vec{U}, \vec{Q}(\vec{V}), a) \in [\![\lambda_{\vec{x}}\mathrm{C}]\!] \quad \text{by (14)}$$
$$\exists_{\vec{a^*}}(a = \mathrm{C}\vec{a^*} \wedge \vec{Q}(\vec{V}) \vdash \vec{a^*})$$

$$\mathrm{C}\vec{Q}(\vec{V}) \vdash a. \qquad \square$$

Let $\sim$ denote the equivalence relation on formal neighborhoods generated by entailment, i.e., $U \sim V$ means $(U \vdash V) \wedge (V \vdash U)$.

(16) If $\vec{U} \vdash \vec{P}(\vec{V})$, then there are $\vec{W}$ such that $\vec{U} \sim \vec{P}(\vec{W})$ and $\vec{W} \vdash \vec{V}$.

Proof. By induction on $\vec{P}$. The cases x and $\langle\rangle$ are clear, and in case $\vec{P}, Q$ we can apply the induction hypothesis. It remains to treat the case $\mathrm{C}\vec{P}(\vec{x}\,)$. Since $U \vdash \mathrm{C}\vec{P}(\vec{V})$ there is a $\vec{b_0^*}$ such that $\mathrm{C}\vec{b_0^*} \in U$. Let

$$U_i := \{\, a \mid \exists_{\vec{a^*}}(\mathrm{C}\vec{a^*} \in U \wedge a = a_i^*) \,\}.$$

For the constructor pattern $\mathrm{C}\vec{x}$ consider $\mathrm{C}\vec{U}$. By definition

$$\mathrm{C}\vec{U} = \{\, \mathrm{C}\vec{a^*} \mid a_i^* \in U_i \text{ if } U_i \neq \emptyset, \text{ and } a_i^* = * \text{ otherwise} \,\}.$$

We first show $U \sim \mathrm{C}\vec{U}$. Assume $\mathrm{C}\vec{a^*} \in \mathrm{C}\vec{U}$. For each i, if $U_i \neq \emptyset$, then there is an $\vec{a_i^*}$ such that $\mathrm{C}\vec{a_i^*} \in U$ and $a_{ii}^* = a_i^*$, and if $U_i = \emptyset$ then $a_i^* = *$. Hence

$$U \supseteq \{\, \mathrm{C}\vec{a_i^*} \mid U_i \neq \emptyset \,\} \cup \{\mathrm{C}\vec{b_0^*}\} \vdash \mathrm{C}\vec{a^*}.$$

Conversely assume $\mathrm{C}\vec{a^*} \in U$. We define $\mathrm{C}\vec{b^*} \in \mathrm{C}\vec{U}$ by $b_i^* = a_i^*$ if $a_i^* \neq *$, $b_i^* = *$ if $U_i = \emptyset$, and otherwise (i.e., if $a_i^* = *$ and $U_i \neq \emptyset$) take an arbitrary $b_i^* \in U_i$. Clearly $\{\mathrm{C}\vec{b^*}\} \vdash \mathrm{C}\vec{a^*}$.

By definition $\vec{U} \vdash \vec{P}(\vec{V})$. Hence by induction hypothesis there are $\vec{W}$ such that $\vec{U} \sim \vec{P}(\vec{W})$ and $\vec{W} \vdash \vec{V}$. Therefore $U \sim \mathrm{C}\vec{U} \sim \mathrm{C}\vec{P}(\vec{W})$. $\square$

Lemma (Unification). *If $\vec{P}_1(\vec{V}_1) \sim \cdots \sim \vec{P}_n(\vec{V}_n)$, then $\vec{P}_1, \ldots, \vec{P}_n$ are unifiable with a most general unifier ϑ and there exists $\vec{W}$ such that*

$$(\vec{P}_1\vartheta)(\vec{W}) = \cdots = (\vec{P}_n\vartheta)(\vec{W}) \sim \vec{P}_1(\vec{V}_1) \sim \cdots \sim \vec{P}_n(\vec{V}_n).$$

Proof. Assume $\vec{P}_1(\vec{V}_1) \sim \cdots \sim \vec{P}_n(\vec{V}_n)$. Then $\vec{P}_1(\vec{V}_1), \ldots, \vec{P}_n(\vec{V}_n)$ are componentwise consistent and hence $\vec{P}_1, \ldots, \vec{P}_n$ are unifiable with a most general unifier ϑ. We now proceed by induction on $\vec{P}_1, \ldots, \vec{P}_n$. If they are either all empty or all variables the claim is trivial. In the case $(\vec{P}_1, P_1), \ldots, (\vec{P}_n, P_n)$ it follows from the linearity condition on variables that a most general unifier of $(\vec{P}_1, P_1), \ldots, (\vec{P}_n, P_n)$ is the union of most general unifiers of $\vec{P}_1, \ldots, \vec{P}_n$ and of $P_1, \ldots, P_n$. Hence the induction hypothesis applies. In the case $\mathrm{C}\vec{P}_1, \ldots, \mathrm{C}\vec{P}_n$ the assumption $\mathrm{C}\vec{P}_1(\vec{V}_1) \sim \cdots \sim \mathrm{C}\vec{P}_n(\vec{V}_n)$ implies $\vec{P}_1(\vec{V}_1) \sim \cdots \sim \vec{P}_n(\vec{V}_n)$ and hence again the induction hypothesis applies. The remaining case is when some are variables and the other ones of the form $\mathrm{C}\vec{P}_i$, say $x, \mathrm{C}\vec{P}_2, \ldots, \mathrm{C}\vec{P}_n$. By assumption

$$V_1 \sim \mathrm{C}\vec{P}_2(\vec{V}_2) \sim \cdots \sim \mathrm{C}\vec{P}_n(\vec{V}_n).$$

By induction hypothesis we obtain the required $\vec{W}$ such that

$$(\vec{P}_2\vartheta)(\vec{W}) = \cdots = (\vec{P}_n\vartheta)(\vec{W}) \sim \vec{P}_2(\vec{V}_2) \sim \cdots \sim \vec{P}_n(\vec{V}_n). \qquad \square$$

We need a final preparation before we can tackle consistency of $[\![\lambda_{\vec{x}}M]\!]$. The information systems $\boldsymbol{C}_\rho$ enjoy the pleasant property of *coherence*, which amounts to the possibility to locate inconsistencies in two-element sets of data objects. Generally, an information system $\boldsymbol{A} = (A, \mathrm{Con}, \vdash)$ is *coherent* if it satisfies: $U \subseteq A$ is consistent if and only if all of its two-element subsets are.

LEMMA. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be information systems. If $\boldsymbol{B}$ is coherent, then so is $\boldsymbol{A} \to \boldsymbol{B}$.*

PROOF. Let $\boldsymbol{A} = (A, \mathrm{Con}_A, \vdash_A)$ and $\boldsymbol{B} = (B, \mathrm{Con}_B, \vdash_B)$ be information systems, and consider $\{(U_1, b_1), \ldots, (U_n, b_n)\} \subseteq \mathrm{Con}_A \times B$. Assume

$$\forall_{1\le i<j\le n}(\{(U_i, b_i), (U_j, b_j)\} \in \mathrm{Con}).$$

We have to show $\{(U_1, b_1), \ldots, (U_n, b_n)\} \in \mathrm{Con}$. Let $I \subseteq \{1, \ldots, n\}$ and $\bigcup_{i\in I} U_i \in \mathrm{Con}_A$. We must show $\{\, b_i \mid i \in I \,\} \in \mathrm{Con}_B$. Now since $\boldsymbol{B}$ is coherent by assumption, it suffices to show that $\{b_i, b_j\} \in \mathrm{Con}_B$ for all $i, j \in I$. So let $i, j \in I$. By assumption we have $U_i \cup U_j \in \mathrm{Con}_A$, and hence $\{b_i, b_j\} \in \mathrm{Con}_B$. $\square$

By a similar argument we can prove

LEMMA (Coherence). *The information systems $\boldsymbol{C}_\rho$ are all coherent.*

PROOF. By induction of the height $|U|$ of consistent finite sets of tokens in $\boldsymbol{C}_\rho$, as defined in parts (c) and (d) of the definition in 2.1.5. $\square$

LEMMA (Consistency). *$[\![\lambda_{\vec{x}}M]\!]$ is consistent.*

PROOF. Let $(\vec{U}_i, a_i) \in [\![\lambda_{\vec{x}}M]\!]$ for $i = 1, 2$. By coherence it suffices to prove that $(\vec{U}_1, a_1)$ and $(\vec{U}_2, a_2)$ are consistent. We shall prove this by induction on the maximum of the D-heights and a side induction on the maximum of the heights.

Case (V). Let $(\vec{U}_1, a_1), (\vec{U}_2, a_2) \in [\![\lambda_{\vec{x}}x_i]\!]$, and assume that $\vec{U}_1$ and $\vec{U}_2$ are componentwise consistent. Then $U_{1i} \vdash a_1$ and $U_{2i} \vdash a_2$. Since $U_{1i} \cup U_{2i}$ is consistent, a_1 and a_2 must be consistent as well.

Case (C). For $i = 1, 2$ we have

$$\frac{\vec{V}_i \vdash \vec{a_i^*}}{(\vec{U}_i, \vec{V}_i, \mathrm{C}\vec{a_i^*}) \in [\![\lambda_{\vec{x}}\mathrm{C}]\!]}.$$

Assume $\vec{U}_1, \vec{V}_1$ and $\vec{U}_2, \vec{V}_2$ are componentwise consistent. The consistency of $\mathrm{C}\vec{a_1^*}$ and $\mathrm{C}\vec{a_2^*}$ follows from $\vec{V}_i \vdash \vec{a_i^*}$ and the consistency of $\vec{V}_1$ and $\vec{V}_2$.

Case (A). For $i = 1, 2$ we have

$$\frac{(\vec{U}_i, V_i, a_i) \in [\![\lambda_{\vec{x}} M]\!] \qquad (\vec{U}_i, V_i) \subseteq [\![\lambda_{\vec{x}} N]\!]}{(\vec{U}_i, a_i) \in [\![\lambda_{\vec{x}}(MN)]\!]}.$$

Assume $\vec{U}_1$ and $\vec{U}_2$ are componentwise consistent. By the side induction hypothesis for the right premises $V_1 \cup V_2$ is consistent. Hence by the side induction hypothesis for the left hand sides a_1 and a_2 are consistent.

Case (D). For $i = 1, 2$ we have

$$\frac{(\vec{U}_i, \vec{V}_i, a_i) \in [\![\lambda_{\vec{x},\vec{y}_i} M_i(\vec{y}_i)]\!] \qquad \vec{W}_i \vdash \vec{P}_i(\vec{V}_i)}{(\vec{U}_i, \vec{W}_i, a_i) \in [\![\lambda_{\vec{x}} D]\!]}(D)$$

for computation rules $D\vec{P}_i(\vec{y}_i) = M_i(\vec{y}_i)$. Assume $\vec{U}_1, \vec{W}_1$ and $\vec{U}_2, \vec{W}_2$ are componentwise consistent; we must show that a_1 and a_2 are consistent. Since $\vec{W}_1 \cup \vec{W}_2 \vdash \vec{P}_i(\vec{V}_i)$ for $i = 1, 2$, by (16) there are $\vec{V}_1', \vec{V}_2'$ such that $\vec{V}_i' \vdash \vec{V}_i$ and $\vec{W}_1 \cup \vec{W}_2 \sim \vec{P}_i(\vec{V}_i')$. Then by the unification lemma there are $\vec{W}$ such that $(\vec{P}_1\vartheta)(\vec{W}) = (\vec{P}_2\vartheta)(\vec{W}) \sim \vec{P}_i(\vec{V}_i') \vdash \vec{P}_i(\vec{V}_i)$ for $i = 1, 2$, where ϑ is the most general unifier of $\vec{P}_1$ and $\vec{P}_2$. But then also

$$(\vec{y}_i\vartheta)(\vec{W}) \vdash \vec{V}_i,$$

and hence by (12) we have

$$(\vec{U}_i, (\vec{y}_i\vartheta)(\vec{W}), a_i) \in [\![\lambda_{\vec{x},\vec{y}_i} M_i(\vec{y}_i)]\!]$$

with lesser D-height. Now (15) gives

$$(\vec{U}_i, \vec{W}, a_i) \in [\![\lambda_{\vec{x},\vec{z}} M_i(\vec{y}_i)\vartheta]\!]$$

without increasing the D-height. Notice that $M_1(\vec{y}_i)\vartheta = M_2(\vec{y}_i)\vartheta$ by our condition on computation rules. Hence the induction hypothesis applied to $(\vec{U}_1, \vec{W}, a_1), (\vec{U}_2, \vec{W}, a_2) \in [\![\lambda_{\vec{x},\vec{z}} M_1(\vec{y}_1)\vartheta]\!]$ implies the consistency of a_1 and a_2, as required. □

Lemma (Deductive closure). $[\![\lambda_{\vec{x}} M]\!]$ *is deductively closed, i.e., if* $W \subseteq [\![\lambda_{\vec{x}} M]\!]$ *and* $W \vdash (\vec{V}, b)$*, then* $(\vec{V}, b) \in [\![\lambda_{\vec{x}} M]\!]$.

Proof. By induction on the maximum of the D-heights and a side induction on the maximum of the heights of $W \subseteq [\![\lambda_{\vec{x}} M]\!]$. We distinguish cases on the last rule of these derivations (which is determined by M).

Case (V). For all $(\vec{U}, a) \in W$ we have

$$\frac{U_i \vdash a}{(\vec{U}, a) \in [\![\lambda_{\vec{x}} x_i]\!]}.$$

We must show $V_i \vdash b$. By assumption $W \vdash (\vec{V}, b)$, hence $W\vec{V} \vdash b$. It suffices to prove $V_i \vdash W\vec{V}$. Let $c \in W\vec{V}$; we show $V_i \vdash c$. There are $\vec{U}$ such that $\vec{V} \vdash \vec{U}$ and $(\vec{U}, c) \in W$. But then by the above $U_i \vdash c$, hence $V_i \vdash U_i \vdash c$.

Case (A). Let $W = \{(\vec{U}_1, a_1), \ldots, (\vec{U}_n, a_n)\}$. For each $(\vec{U}_i, a_i) \in W$ there is U_i such that

$$\frac{(\vec{U}_i, U_i, a_i) \in [\![\lambda_{\vec{x}} M]\!] \qquad (\vec{U}_i, U_i) \subseteq [\![\lambda_{\vec{x}} N]\!]}{(\vec{U}_i, a_i) \in [\![\lambda_{\vec{x}}(MN)]\!]}.$$

Define $U := \bigcup\{\, U_i \mid \vec{V} \vdash \vec{U}_i \,\}$. We first show that U is consistent. Let $a, b \in U$. There are i, j such that $a \in U_i$, $b \in U_j$ and $\vec{V} \vdash \vec{U}_i, \vec{U}_j$. Then $\vec{U}_i$ and $\vec{U}_j$ are consistent; hence by the consistency of $[\![\lambda_{\vec{x}} N]\!]$ proved above a and b are consistent as well.

Next we show $(\vec{V}, U) \subseteq [\![\lambda_{\vec{x}} N]\!]$. Let $a \in U$; we show $(\vec{V}, a) \in [\![\lambda_{\vec{x}} N]\!]$. Fix i such that $a \in U_i$ and $\vec{V} \vdash U_i$, and let $W_i := \{\, (\vec{U}_i, b) \mid b \in U_i \,\} \subseteq [\![\lambda_{\vec{x}} N]\!]$. Since by the side induction hypothesis $[\![\lambda_{\vec{x}} N]\!]$ is deductively closed it suffices to prove $W_i \vdash (\vec{V}, a)$, i.e., $\{\, b \mid b \in U_i \wedge \vec{V} \vdash \vec{U}_i \,\} \vdash a$. But the latter set equals U_i, and $a \in U_i$.

Finally we show $(\vec{V}, U, b) \subseteq [\![\lambda_{\vec{x}} M]\!]$. Let

$$W' := \{(\vec{U}_1, U_1, a_1), \ldots, (\vec{U}_n, U_n, a_n)\} \subseteq [\![\lambda_{\vec{x}} M]\!].$$

By side induction hypothesis it suffices to prove that $W' \vdash (\vec{V}, U, b)$, i.e., $\{\, a_i \mid \vec{V} \vdash \vec{U}_i \wedge U \vdash U_i \,\} \vdash b$. But by definition of U the latter set equals $\{\, a_i \mid \vec{V} \vdash \vec{U}_i \,\}$, which in turn entails b because by assumption $W \vdash (\vec{V}, b)$.

Now we can use (A) to infer $(\vec{V}, b) \in [\![\lambda_{\vec{x}} M]\!]$, as required.

Case (C). Assume $W \subseteq [\![\lambda_{\vec{x}} C]\!]$. Then W consists of $(\vec{U}, \vec{U}', \mathrm{C}\vec{a^*})$ such that $\vec{U}' \vdash \vec{a^*}$. Assume further $W \vdash (\vec{V}, \vec{V}', b)$. Then

$$\{\, \mathrm{C}\vec{a^*} \mid \exists_{\vec{U}, \vec{U}'}((\vec{U}, \vec{U}', \mathrm{C}\vec{a^*}) \in W \wedge \vec{V} \vdash \vec{U} \wedge \vec{V}' \vdash \vec{U}') \,\} \vdash b.$$

By definition of entailment b has the form $\mathrm{C}\vec{b^*}$ such that

$$W_i := \{\, a \mid \exists_{\vec{U}, \vec{U}', \vec{a^*}}(a = a_i^* \wedge (\vec{U}, \vec{U}', \mathrm{C}\vec{a^*}) \in W \wedge \vec{V} \vdash \vec{U} \wedge \vec{V}' \vdash \vec{U}') \,\} \vdash b_i^*.$$

We must show $(\vec{V}, \vec{V}', \mathrm{C}\vec{b^*}) \in [\![\lambda_{\vec{x}} \mathrm{C}]\!]$, i.e., $\vec{V}' \vdash \vec{b^*}$. It suffices to show $V_i' \vdash W_i$, for every i. Let $a \in W_i$. Then there are $\vec{U}, \vec{U}', \vec{a^*}$ such that $a = a_i^*$, $(\vec{U}, \vec{U}', \mathrm{C}\vec{a^*}) \in W$ and $\vec{V}' \vdash \vec{U}'$. Hence $V_i' \vdash U_i' \vdash a_i^* = a$.

Case (D). Let $W = \{(\vec{U}_1, \vec{U}_1'', a_1), \ldots, (\vec{U}_n, \vec{U}_n'', a_n)\}$. For every i there is an $\vec{U}_i'$ such that

$$\frac{(\vec{U}_i, \vec{U}_i', a_i) \in [\![\lambda_{\vec{x}, \vec{y_i}} M_i(\vec{y_i})]\!] \qquad \vec{U}_i'' \vdash \vec{P}_i(\vec{U}_i')}{(\vec{U}_i, \vec{U}_i'', a_i) \in [\![\lambda_{\vec{x}} D]\!]}$$

for $D\vec{P}_i(\vec{y_i}) = M_i(\vec{y_i})$ a computation rule. Assume $W \vdash (\vec{V}, \vec{V}'', b)$. We must prove $(\vec{V}, \vec{V}'', b) \in [\![\lambda_{\vec{x}} D]\!]$. Let

$$I := \{\, i \mid 1 \leq i \leq n \wedge \vec{V} \vdash \vec{U}_i \wedge \vec{V}'' \vdash \vec{U}_i'' \,\}.$$

Then $\{\, a_i \mid i \in I \,\} \vdash b$, hence $I \neq \emptyset$. For $i \in I$ we have $\vec{V}'' \vdash \vec{U}_i'' \vdash \vec{P}_i(\vec{U}_i')$, hence by (16) there are $\vec{V}_i'$ such that $\vec{V}'' \sim \vec{P}_i(\vec{V}_i')$ and $\vec{V}_i' \vdash \vec{U}_i'$. In particular for $i, j \in I$

$$\vec{V}'' \sim \vec{P}_i(\vec{V}_i') \sim \vec{P}_j(\vec{V}_j').$$

To simplify notation assume $I = \{1, \ldots, m\}$. Hence by the unification lemma $\vec{P}_1, \ldots, \vec{P}_m$ are unifiable with a most general unifier ϑ and there exists $\vec{W}$ such that

$$(\vec{P}_1\vartheta)(\vec{W}) = \cdots = (\vec{P}_m\vartheta)(\vec{W}) \sim \vec{P}_1(\vec{V}_1') \sim \cdots \sim \vec{P}_m(\vec{V}_m').$$

Let $i, j \in I$. Then by the conditions on computation rules $M_i\vartheta = M_j\vartheta$. Also $(\vec{y}_i\vartheta)(\vec{W}) \vdash \vec{V}_i' \vdash \vec{U}_i'$. Therefore by (12)

$$(\vec{V}, (\vec{y}_i\vartheta)(\vec{W}), a_i) \in [\![\lambda_{\vec{x},\vec{y_i}} M_i(\vec{y_i})]\!]$$

and hence by (15)

$$(\vec{V}, \vec{W}, a_i) \in [\![\lambda_{\vec{x},\vec{y_i}} M_i(\vec{y}_i\vartheta)]\!].$$

But $M_i(\vec{y}_i\vartheta) = M_i\vartheta = M_1\vartheta = M_1(\vec{y_1}\vartheta)$ and hence for all $i \in I$

$$(\vec{V}, \vec{W}, a_i) \in [\![\lambda_{\vec{x},\vec{y_i}} M_1(\vec{y_1}\vartheta)]\!].$$

Therefore $X := \{\, (\vec{V}, \vec{W}, a_i) \mid i \in I \,\} \subseteq [\![\lambda_{\vec{x},\vec{y_i}} M_1(\vec{y_1}\vartheta)]\!]$. Since $\{\, a_i \mid i \in I \,\} \vdash b$, we have $X \vdash (\vec{V}, \vec{W}, b)$ and hence the induction hypothesis implies $(\vec{V}, \vec{W}, b) \in [\![\lambda_{\vec{x},\vec{y_i}} M_1(\vec{y_1}\vartheta)]\!]$. Using (15) again we obtain $(\vec{V}, (\vec{y}_i\vartheta)(\vec{W}), b) \in [\![\lambda_{\vec{x},\vec{y_i}} M_1(\vec{y_1})]\!]$. Since $\vec{V}'' \sim \vec{P}_1(\vec{V}_1') \sim \vec{P}_1((\vec{y_1}\vartheta)(\vec{W}))$ we obtain $(\vec{V}, \vec{V}'', b) \in [\![\lambda_{\vec{x}} D]\!]$, by (D). □

Corollary. *$[\![\lambda_{\vec{x}} M]\!]$ is an ideal.*

A.3. Preservation of values

We now prove that our definition above of the denotation of a term is reasonable in the sense that it is not changed by an application of the standard (β- and η-) conversions or a computation rule. For the β-conversion part of this proof it is helpful to first introduce a more standard notation, which involves variable environments.

Definition. Assume that all free variables in M are among $\vec{x}$. Let $[\![M]\!]^{\vec{U}}_{\vec{x}} := \{\, b \mid (\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!] \,\}$ and $[\![M]\!]^{\vec{u},\vec{V}}_{\vec{x},\vec{y}} := \bigcup_{\vec{U} \subseteq \vec{u}} [\![M]\!]^{\vec{U},\vec{V}}_{\vec{x},\vec{y}}$.

From (13) we obtain $[\![M]\!]^{\vec{U},V}_{\vec{x},y} = [\![M]\!]^{\vec{U}}_{\vec{x}}$ if $y \notin \mathrm{FV}(M)$, and similarly for ideals $\vec{u}, v$ instead of $\vec{U}, V$. We have a useful monotonicity property, which follows from the deductive closure of $[\![\lambda_{\vec{x}} M]\!]$.

LEMMA. (a) *If* $\vec{V} \vdash \vec{U}$, $a \vdash b$ *and* $a \in [\![M]\!]^{\vec{U}}_{\vec{x}}$, *then* $b \in [\![M]\!]^{\vec{V}}_{\vec{x}}$.
(b) *If* $\vec{v} \supseteq \vec{u}$, $a \vdash b$ *and* $a \in [\![M]\!]^{\vec{u}}_{\vec{x}}$, *then* $b \in [\![M]\!]^{\vec{v}}_{\vec{x}}$.

PROOF. (a) $\vec{V} \vdash \vec{U}$, $a \vdash b$ and $(\vec{U}, a) \in [\![\lambda_{\vec{x}} M]\!]$ together imply $(\vec{V}, b) \in [\![\lambda_{\vec{x}} M]\!]$, by the deductive closure of $[\![\lambda_{\vec{x}} M]\!]$. (b) follows from (a). □

LEMMA. (a) $[\![x_i]\!]^{\vec{U}}_{\vec{x}} = \overline{U}_i$ *and* $[\![x_i]\!]^{\vec{u}}_{\vec{x}} = u_i$.
(b) $[\![\lambda_y M]\!]^{\vec{U}}_{\vec{x}} = \{\, (V,b) \mid b \in [\![M]\!]^{\vec{U},V}_{\vec{x},y} \,\}$ *and* $[\![\lambda_y M]\!]^{\vec{u}}_{\vec{x}} = \{\, (V,b) \mid b \in [\![M]\!]^{\vec{u},V}_{\vec{x},y} \,\}$.
(c) $[\![MN]\!]^{\vec{U}}_{\vec{x}} = [\![M]\!]^{\vec{U}}_{\vec{x}} [\![N]\!]^{\vec{U}}_{\vec{x}}$ *and* $[\![MN]\!]^{\vec{u}}_{\vec{x}} = [\![M]\!]^{\vec{u}}_{\vec{x}} [\![N]\!]^{\vec{u}}_{\vec{x}}$.

PROOF. (b) It suffices to prove the first part. But $(V,b) \in [\![\lambda_y M]\!]^{\vec{U}}_{\vec{x}}$ and $b \in [\![M]\!]^{\vec{U},V}_{\vec{x},y}$ are both equivalent to $(\vec{U}, V, b) \in [\![\lambda_{\vec{x},y} M]\!]$.

(c) For the first part we argue as follows.

$$\begin{aligned}
c \in [\![M]\!]^{\vec{U}}_{\vec{x}} [\![N]\!]^{\vec{U}}_{\vec{x}} &\leftrightarrow \exists_{V \subseteq [\![N]\!]^{\vec{U}}_{\vec{x}}} ((V,c) \in [\![M]\!]^{\vec{U}}_{\vec{x}}) \\
&\leftrightarrow \exists_V ((\vec{U}, V) \subseteq [\![\lambda_{\vec{x}} N]\!] \wedge (\vec{U}, V, c) \in [\![\lambda_{\vec{x}} M]\!]) \\
&\leftrightarrow (\vec{U}, c) \in [\![\lambda_{\vec{x}} (MN)]\!] \quad \text{by } (A) \\
&\leftrightarrow c \in [\![MN]\!]^{\vec{U}}_{\vec{x}}.
\end{aligned}$$

The second part is an easy consequence:

$$\begin{aligned}
c \in [\![M]\!]^{\vec{u}}_{\vec{x}} [\![N]\!]^{\vec{u}}_{\vec{x}} &\leftrightarrow \exists_{V \subseteq [\![N]\!]^{\vec{u}}_{\vec{x}}} ((V,c) \in [\![M]\!]^{\vec{u}}_{\vec{x}}) \\
&\leftrightarrow \exists_{V \subseteq [\![N]\!]^{\vec{u}}_{\vec{x}}} \exists_{\vec{U} \subseteq \vec{u}} ((V,c) \in [\![M]\!]^{\vec{U}}_{\vec{x}}) \\
&\leftrightarrow \exists_{\vec{U}_1 \subseteq \vec{u}} \exists_{V \subseteq [\![N]\!]^{\vec{U}_1}_{\vec{x}}} \exists_{\vec{U} \subseteq \vec{u}} ((V,c) \in [\![M]\!]^{\vec{U}}_{\vec{x}}) \\
&\leftrightarrow^{(*)} \exists_{\vec{U} \subseteq \vec{u}} \exists_{V \subseteq [\![N]\!]^{\vec{U}}_{\vec{x}}} ((V,c) \in [\![M]\!]^{\vec{U}}_{\vec{x}}) \\
&\leftrightarrow \exists_{\vec{U} \subseteq \vec{u}} (c \in [\![M]\!]^{\vec{U}}_{\vec{x}} [\![N]\!]^{\vec{U}}_{\vec{x}}) \\
&\leftrightarrow \exists_{\vec{U} \subseteq \vec{u}} (c \in [\![MN]\!]^{\vec{U}}_{\vec{x}}) \quad \text{by the first part} \\
&\leftrightarrow c \in [\![MN]\!]^{\vec{u}}_{\vec{x}}.
\end{aligned}$$

Here is the proof of the equivalence marked $(*)$. The upward direction is obvious. For the downward direction we use monotonicity. Assume $\vec{U}_1 \subseteq \vec{u}$, $V \subseteq [\![N]\!]^{\vec{U}_1}_{\vec{x}}$, $\vec{U} \subseteq \vec{u}$ and $(V,c) \in [\![M]\!]^{\vec{U}}_{\vec{x}}$. Let $\vec{U}_2 := \vec{U}_1 \cup \vec{U} \subseteq \vec{u}$. Then by monotonicity $V \subseteq [\![N]\!]^{\vec{U}_2}_{\vec{x}}$ and $(V,c) \in [\![M]\!]^{\vec{U}_2}_{\vec{x}}$. □

COROLLARY. $[\![\lambda_y M]\!]^{\vec{u}}_{\vec{x}} v = [\![M]\!]^{\vec{u},v}_{\vec{x},y}$.

PROOF.

$$\begin{aligned} b \in [\![\lambda_y M]\!]^{\vec{u}}_{\vec{x}} v &\leftrightarrow \exists_{V \subseteq v}((V,b) \in [\![\lambda_y M]\!]^{\vec{u}}_{\vec{x}}) \\ &\leftrightarrow \exists_{V \subseteq v}(b \in [\![M]\!]^{\vec{u},V}_{\vec{x},y}) \quad \text{by the lemma, part (b)} \\ &\leftrightarrow b \in [\![M]\!]^{\vec{u},v}_{\vec{x},y}. \end{aligned}$$ □

LEMMA (Substitution). $[\![M(z)]\!]^{\vec{u},[\![N]\!]^{\vec{u}}_{\vec{x}}}_{\vec{x},z} = [\![M(N)]\!]^{\vec{u}}_{\vec{x}}$.

PROOF. By induction on M, and cases on the form of M.
Case $\lambda_y M$. For readability we leave out $\vec{x}$ and $\vec{u}$.

$$\begin{aligned} [\![\lambda_y M(z)]\!]^{[\![N]\!]}_{z} &= \{\, (V,b) \mid b \in [\![M(z)]\!]^{[\![N]\!],V}_{z,y} \,\} \\ &= \{\, (V,b) \mid b \in [\![M(N)]\!]^{V}_{y} \,\} \quad \text{by induction hypothesis} \\ &= [\![\lambda_y M(N)]\!] \quad \text{by the last lemma, part (b)} \\ &= [\![(\lambda_y M)(N)]\!]. \end{aligned}$$

The other cases are easy. □

LEMMA (Preservation of values, β). $[\![(\lambda_y M(y))N]\!]^{\vec{u}}_{\vec{x}} = [\![M(N)]\!]^{\vec{u}}_{\vec{x}}$.

PROOF. Again we leave out $\vec{x}$, $\vec{u}$. By the last two lemmata and the corollary, $[\![(\lambda_y M(y))N]\!] = [\![\lambda_y M(y)]\!][\![N]\!] = [\![M(y)]\!]^{[\![N]\!]}_{y} = [\![M(N)]\!]$. □

LEMMA (Preservation of values, η). $[\![\lambda_y(My)]\!]^{\vec{u}}_{\vec{x}} = [\![M]\!]^{\vec{u}}_{\vec{x}}$ *if* $y \notin \mathrm{FV}(M)$.

PROOF.

$$\begin{aligned} (V,b) \in [\![\lambda_y(My)]\!]^{\vec{u}}_{\vec{x}} &\leftrightarrow \exists_{\vec{U} \subseteq \vec{u}}((\vec{U},V,b) \in [\![\lambda_{\vec{x},y}(My)]\!]) \\ &\leftrightarrow \exists_{\vec{U} \subseteq \vec{u}}((\vec{U},V,b) \in [\![\lambda_{\vec{x}} M]\!]) \quad \text{by (14)} \\ &\leftrightarrow (V,b) \in [\![M]\!]^{\vec{u}}_{\vec{x}}. \end{aligned}$$ □