Extensionality [p87 et seq.]

1. We cannot proceed to prove the adequacy statement by a straightforward induction on the structure of terms.

► Consider M to be $M_1 M_2$, $\mathbf{fix}(M')$.

2. So we proceed to prove a stronger statement that applies to terms of arbitrary types and implies adequacy.

This statement roughly takes the form:

 $\llbracket M \rrbracket \lhd_{ au} M$ for all types au and all $M \in \mathrm{PCF}_{ au}$

where the *formal approximation relations*

 $\triangleleft_{\tau} \subseteq \llbracket \tau \rrbracket \times \mathrm{PCF}_{\tau}$

are *logically* chosen to allow a proof by induction.

 $\begin{array}{c} d \triangleleft_{\tau \to \tau'} M \stackrel{\text{def}}{\Leftrightarrow} \forall e, N \ (e \triangleleft_{\tau} N \ \Rightarrow \ d(e) \triangleleft_{\tau'} M N) \\ \uparrow \\ d \in \llbracket \tau \rrbracket \twoheadrightarrow \llbracket \tau' \rrbracket \end{array}$

Given PCF terms M_1, M_2 , PCF type τ , and a type environment Γ , the relation $\Gamma \vdash M_1 \leq_{\text{ctx}} M_2 : \tau$ is defined to hold iff

- Both the typings $\Gamma \vdash M_1 : \tau$ and $\Gamma \vdash M_2 : \tau$ hold.
- For all PCF contexts C for which $C[M_1]$ and $C[M_2]$ are closed terms of type γ , where $\gamma = nat \text{ or } \gamma = bool$, and for all values $V \in PCF_{\gamma}$,

$$\mathcal{C}[M_1] \Downarrow_{\gamma} V \implies \mathcal{C}[M_2] \Downarrow_{\gamma} V$$
.

 $M_1 \cong_{dx} M_z$ if $M_2 \leqslant_{dx} M_z \leqslant_{dx} M_z$

Contextual preorder from formal approximation

Proposition. For all PCF types τ and all closed terms $M_1, M_2 \in \mathrm{PCF}_{\tau}$,

 $\llbracket M_1 \rrbracket \triangleleft_{\tau} M_2 \iff M_1 \leq_{\mathrm{ctx}} M_2 : \tau \; .$

 $M_1 \leq_{d_x} M_2 : T \Rightarrow [M_1] \leq_r M_2$ "Fundamental property" of < gives

[M] = M

$$M_{1} \leq d_{2}, M_{2}: T \Rightarrow EM_{1} \exists d_{7}, M_{2}$$

"Fundamental property" of \lhd gives

$$I M_{1} \exists d_{7}, M_{1}$$

Can also prove (by induction on T) that
if $d d_{7}, M_{1} \otimes M_{1} \leq d_{2}, M_{2}: T$, then $d d_{7}, M_{2}$
if $d d_{7}, M_{1} \otimes M_{1} \leq d_{2}, M_{2}: T$, then $d d_{7}, M_{2}$
 $M_{1} \leq d_{2}, M_{2}: Y \otimes M_{1} \forall_{Y} V \Rightarrow M_{2} \forall_{Y} V$
($\gamma = nat, bool$)
 $M_{1} \leq d_{2}, M_{2}: T \rightarrow T' \Rightarrow \forall M: T (M_{1}M \leq d_{2}, M_{2}, T')$
to prove this

•

$$M_{1} \leq_{de} M_{2}: \tau \Rightarrow \mathbb{E}M_{1} \mathbb{I} \leq_{\tau} M_{2}$$

"Fundamental property" of \lhd gives

$$\mathbb{I}M_{1} \mathbb{I} \leq_{\tau} M_{1}$$

Can also prove (by induction on τ) that
if $d \leq_{\tau} M_{1} \otimes M_{1} \leq_{dx} M_{2}: \tau$, then $d \leq_{\tau} M_{2}$
Have $d = \mathbb{E}M_{1} \mathbb{I}$ to get
 $M_{1} \leq_{dx} M_{2}: \tau \Rightarrow \mathbb{E}M_{1} \mathbb{I} \leq_{\tau} M_{2}$

 $[M_1] \lhd_T M_2 \Rightarrow M_1 \leq_{d_2} M_2 : T$ "Fundamental property" of I gives [M] J J J J D M M: T-> bood M: T-> bood

 $[M_1] \lhd_{\tau} M_2 \Rightarrow M_1 \leq_{d_x} M_2 : T$ "Fundamental property" of < gives [M] JJJ M K: Z-> bood M: Z-> bood So if [[M]] J_T MZ, by definition of J_T, book we get [[M]([[M]]) J book MMZ

 $\mathbb{L}M_1\mathbb{J} \triangleleft_{\tau} \mathbb{M}_2 \implies \mathbb{M}_1 \leq_{d_2} \mathbb{M}_2 : \mathcal{T}$ "Fundamental proporty" of <>> gives [M] J_T->bod M M: T-> bod So if [M,] < T Mz, by definition of Je, book we get T -[[MM]] Jood MMZ

 $[M_1] \triangleleft_T M_2 \implies M_1 \leq_{d_2} M_2 : T$ "Fundamental property" of <> gives [M] J J T => bood M M: T => bood So if [MI] J_ Mz, by definition of J_, book we get [I MANA] JI A MANA Nre yer [[MMI] bool MMz So by definition of Joool we got V: bool (MM, thool V >> MMz thool V)

 $\mathbb{L}M_1 \mathbb{J} \triangleleft_{\tau} \mathbb{M}_2 \implies \mathbb{M}_1 \leq_{d_{\tau}} \mathbb{M}_2 : \mathcal{T}$ "Fundamental proporty" of I gives IMJJ_T->box M M: T-> box So if [MI] J_ Mz, by definition of J_z, bod we get Emmi J bool MMZ So by definition of bool we got V: bool (MM, thou V >> MM2 thool V) That hand to see this is equivalent to $M_1 \leq A_2 : 7$

Contextual preorder from formal approximation

Proposition. For all PCF types τ and all closed terms $M_1, M_2 \in \mathrm{PCF}_{\tau}$,

 $\llbracket M_1 \rrbracket \triangleleft_{\tau} M_2 \iff M_1 \leq_{\mathrm{ctx}} M_2 : \tau \; .$

Some useful constlaries of $M_1 \leq d_x M_z \iff [M_1] \lhd M_z$ • $\Omega = fix(fix:\tau.x)$ is least wrt. $\leq ctx$ $\forall M:\tau (\Omega \leq M:\tau)$

Some useful constlaries of $M_1 \leq d_x M_z \iff [M_1] \lhd M_2$ • $\Omega = fix(fix:\tau.x)$ is least wrt. $\leq dx$ $\forall M:\tau (\Omega \leq d_X M:\tau)$ because $[\Omega] = fix(\lambda d.d) = \bot \lhd_{\tau} M$

Some useful constlaries of $M_1 \leq_{ctx} M_z \iff [M_1] \lhd M_z$

• tor each $M: \tau \to \tau$, $fix(M): \tau$ is least pre-fixed point w-r.t. $\leq dx$ $\forall N: \tau (MN \leq dx N: \tau \Rightarrow fix(M) \leq dx N: \tau)$

Some useful confidences of
$$M_1 \leq_{dx} M_2 \Leftrightarrow \mathbb{I}_M_1 \supset M_2$$

• For each $M: \tau \rightarrow \tau$, $fix(M): \tau$ is least
pre-fixed point μ -r.t. \leq_{dx}
 $\forall N: \tau (MN \leq_{dx} N: \tau \Rightarrow fix(M) \leq_{dx} N: \tau)$
• Proof: use the fact that $\{d\in \mathbb{I}\tau D \mid d = \tau N\}$ is admissible.

Some useful constlaries of
$$M_1 \leq d_x M_z \Leftrightarrow \mathbb{I}M_1 \mathbb{I} \supset M_z$$

• For each $M: \tau \rightarrow \tau$, $fix(M): \tau$ is least
pre-fixed point w-r.t. $\leq d_x$
 $\forall N: \tau (MN \leq d_x N: \tau \Rightarrow fix(M) \leq d_x N: \tau)$
• Proof: use the fact that $\{d \in \mathbb{I} \tau D \mid d \supset_{\tau} N\}$ is admissible.
 $d \leq_{\tau} N \Rightarrow \mathbb{I}M \mathbb{I}(d) \supset_{\tau} MN$ since $\mathbb{I}M \mathbb{I} \supset M$

Some useful constlaries of
$$M_1 \leq d_X M_Z \Leftrightarrow \mathbb{I}M_1 \supset M_Z$$

• For each $M: \tau \rightarrow \tau$, $fix(M): \tau$ is least
pre-fixed point w-r.t. $\leq d_X$
 $\forall N: \tau (MN \leq d_X N: \tau \Rightarrow fix(M) \leq d_X N: \tau)$
• Proof: use the fact that $\{d \in \mathbb{I} : D \mid d \lhd_{\tau} N \}$ is admissible.
 $d \leq_{\tau} N \Rightarrow \mathbb{I}MJ(d) \supset_{\tau} MN$ since $\mathbb{I}MJ \supset M$
 $\Rightarrow \mathbb{I}MJ(d) \supset_{\tau} N$ since $MN \leq d_X N$

Some useful constlaries of
$$M_1 \leq ct_X M_z \Leftrightarrow \mathbb{I}M_1 \mathbb{J} \supset M_z$$

• For each $M: \tau \rightarrow \tau$, $fix(M): \tau$ is least
pre-fixed point w-r.t. $\leq ct_X$
 $\forall N: \tau (MN \leq ct_X N: \tau \Rightarrow fix(M) \leq ct_X N: \tau)$
> Proof: use the fact that $\{deltald_{\tau}N\}$ is admissible.
 $d \leq_{\tau} N \Rightarrow \mathbb{I}MJ(d) \supset_{\tau} MN$ since $[M] \lhd M$
 $\Rightarrow \mathbb{I}MJ(d) \supset_{\tau} N$ since $MN \leq ct_X N$
So $\mathbb{L}fix(M)J = fix(\mathbb{I}MJ) \supset_{\tau} N$ by Suft Induction.

Some useful constlaries of
$$M_1 \leq_{dx} M_2 \Leftrightarrow [M_1] \lhd M_2$$

• For each $M: \tau \rightarrow \tau$, $fix(M): \tau$ is least
pre-fixed point w-r.t. \leq_{dx}
 $\forall N: \tau (MN \leq_{dx} N: \tau \Rightarrow fix(M) \leq_{dx} N: \tau)$
• Proof: use the fact that $\{deltald_{\tau}N\}$ is admissible.
 $d \leq_{\tau} N \Rightarrow IMJ(d) \leq_{\tau} MN$ since $[M] \lhd M$
 $\Rightarrow IMJ(d) \leq_{\tau} N$ since $MN \leq_{dx} N$
So $Lfix(M)J = fix(IMJ) =_{\tau} N$ by Suft Induction.
Hence $fix(M) \leq_{dx} N: \tau$ $Q, \in P$

At a ground type $\gamma \in \{bool, nat\}$,

 $M_1 \leq_{ ext{ctx}} M_2: \gamma$ holds if and only if

 $\forall V \in \mathrm{PCF}_{\gamma} (M_1 \Downarrow_{\gamma} V \implies M_2 \Downarrow_{\gamma} V) .$

At a function type au
ightarrow au',

 $M_1 \leq_{\operatorname{ctx}} M_2: au o au'$ holds if and only if

 $\forall M \in \mathrm{PCF}_{\tau} (M_1 M \leq_{\mathrm{ctx}} M_2 M : \tau') .$

At a ground type $\gamma \in \{bool, nat\}$,

$$\begin{split} M_1 \leq_{\mathrm{ctx}} M_2 : \gamma \text{ holds if and only if} \\ & \swarrow \\ \forall V \in \mathrm{PCF}_{\gamma} \left(M_1 \Downarrow_{\gamma} V \implies M_2 \Downarrow_{\gamma} V \right) \,. \end{split}$$

At a function type au
ightarrow au',

 $M_1 \leq_{\operatorname{ctx}} M_2: au o au'$ holds if and only if

 $\forall M \in \mathrm{PCF}_{\tau} (M_1 M \leq_{\mathrm{ctx}} M_2 M : \tau') .$

If $M_1 \leq ctx M_2$: nat, then taking C = [-] we get $M_1 = C[M_1] \downarrow_{rat} V \Rightarrow C[M_2] \downarrow_{rat}$ C[m] Unat V ⇒ M2 Inat V

At a ground type $\gamma \in \{bool, nat\},\$

 $M_1 \leq_{\mathrm{ctx}} M_2 : \gamma$ holds if and only if

 $\forall V \in \mathrm{PCF}_{\gamma} (M_1 \Downarrow_{\gamma} V \implies M_2 \Downarrow_{\gamma} V) .$

At a function type au ightarrow au',

 $M_1 \leq_{\mathrm{ctx}} M_2 : \tau \to \tau'$ holds if and only if

 $\forall M \in \operatorname{PCF}_{\tau} (M_1 M \leq_{\operatorname{ctx}} M_2 M : \tau') .$

If $M_1 \leq_{ctx} M_2 : T \rightarrow T'$, then $\mathcal{C}[M_1M] \Downarrow_{\mathcal{V}} V \Rightarrow \mathcal{C}'[M_1] \amalg_{\mathcal{V}} V$ where $\mathcal{C}' = \mathcal{C}[-M]$ $\rightarrow \mathcal{C}'[M_2] \not \downarrow_{\mathcal{V}} \mathcal{V}$ $\Rightarrow \simeq [M_2 M] \downarrow_{\gamma} V$

If $M_1 \leq_{ctx} M_2 : T \rightarrow T'$, then $\mathcal{C}[M_1M] \downarrow_{\mathcal{V}} \vee \Rightarrow \mathcal{C}'[M_1] \downarrow_{\mathcal{V}} \vee \text{ where}$ $\mathcal{C}' = \mathcal{C}[-M]$ $\rightarrow \mathcal{C}'[M_2] \Downarrow_{\mathcal{V}} \mathcal{V}$ ⇒>C[M2M] Jfy V

So $M_1 M \leq_{U_X} M_2 M : Z'$

At a ground type $\gamma \in \{bool, nat\}$,

 $M_{1} \leq_{\mathrm{ctx}} M_{2} : \gamma \text{ holds if and only if}$ $(\forall V \in \mathrm{PCF}_{\gamma} (M_{1} \Downarrow_{\gamma} V \implies M_{2} \Downarrow_{\gamma} V).$

At a function type au
ightarrow au',

 $M_1 \leq_{\operatorname{ctx}} M_2: au o au'$ holds if and only if

 $\forall M \in \mathrm{PCF}_{\tau} (M_1 M \leq_{\mathrm{ctx}} M_2 M : \tau') .$

If
$$\forall V: nat (M_1 \Downarrow_{nat} V \Longrightarrow M_2 \amalg_{nat} V)$$

putting $d = [M_1] \in M_1$
if $d \neq l$ then $[M_1] = d = [lsucc(0)]$
so $M_1 \Downarrow_{nat} succ(0)$ (adequacy)

If $\forall V: nat(M_1 \Downarrow nat V \implies M_2 \amalg nat V)(*)$ putting $d = [M,] \in M_{\perp}$ if $d \neq \bot$ then $[m_1] = d = [[succ(0)]]$ Mi Unat Succd(0) 50 M_2 Unat Succ^d(0) (by (*)) 20

If $\forall V: nat(M_1 \Downarrow nat V \Longrightarrow M_2 \amalg nat V)$ putting $d = [M, J \in M_{\perp}]$ if $d \neq \bot$ then $[m_i] = d = [[succ(0)]]$ So Mi Unat Succa(0) So M_2 Unat Succ^d(0) By definition of Inat, this means d Jrat M2 $[M, J] \leq nat M_2 \\ M_1 \leq dx M_2 : nat$ So (slide 68) Sð

At a ground type $\gamma \in \{bool, nat\}$,

 $M_1 \leq_{ ext{ctx}} M_2: \gamma$ holds if and only if

 $\forall V \in \mathrm{PCF}_{\gamma} (M_1 \Downarrow_{\gamma} V \implies M_2 \Downarrow_{\gamma} V) .$

At a function type au ightarrow au',

 $M_1 \leq_{\mathrm{ctx}} M_2: au o au'$ holds if and only if

$$\forall M \in \mathrm{PCF}_{\tau} (M_1 M \leq_{\mathrm{ctx}} M_2 M : \tau') .$$

If $\forall M:\tau(M_1M \leq_{ctx} M_2M:\tau')$ then $d \lhd_{\tau} M \Rightarrow [[M_1](d) \lhd_{\tau}, M_1 M (since [[M_1]] \lhd_{\tau}, M_1)]$

 $I \forall M:\tau (M_1 M \leq_{ctx} M_2 M : \tau') (t)$ then $d \triangleleft_{\tau} M \Rightarrow [[M_1](d) \triangleleft_{\tau}, M_1 M$ $\Rightarrow [[M_{i}](d) \triangleleft_{\tau}, M_{2}M(by(\mathcal{H}))$

 $\mathcal{I} \mathcal{F} \forall \mathcal{M} : \tau \left(\mathcal{M}_{1} \mathcal{M} \leq_{\mathcal{O} \mathcal{K}} \mathcal{M}_{2} \mathcal{M} : \tau' \right)$ then $d \triangleleft_{\tau} M \Rightarrow [[M_1](d) \triangleleft_{\tau}, M_1 M$ $\Rightarrow [[M,](d) \triangleleft_{\tau}, M_2M]$ So by definition of dis, this means $[M_1] \triangleleft_{\tau \to \tau}, M_2$ $M_1 \leq c_{\text{tx}} M_z : \tau \rightarrow \tau'$ (slide 68) So

We've seen

Compositionality + soundness + adequacy \Rightarrow $[M_1] = [M_2] \in [\tau] \Rightarrow M_1 \cong d_X M_2 : \tau$

Similarly $[M_1] \subseteq [M_2] \text{ in } [T] \Rightarrow M_1 \leq_{d_X} M_2 : T$

We've seen Compositionality + soundness + adequacy \Rightarrow $[M_1] = [M_2] \in [T_1] \Rightarrow M_1 \cong ct_X M_2 : T$ Similarly $[M_1] \subseteq [M_2] \text{ in } [T] \implies M_1 \leq d_X M_2 : 7$ What about the converse implications?

Full abstraction

A denotational model is said to be *fully abstract* whenever denotational equality characterises contextual equivalence.

At type nat $M_1 \leq_{ctx} M_2$: nat $\implies \forall n \in IN(M_1 \Downarrow Succ^2(0)) \Rightarrow$ $M_2 \Downarrow Succ^2(0))$

At type nat

 $M_1 \leq_{ctx} M_2 : nat \iff \forall n \in IN(M_1 \Downarrow_{nat} Succ^{n}_{O}) \Rightarrow$ $M_2 \Downarrow_{nat} Succ^{n}_{O})$ soundness $\stackrel{\checkmark}{\Longrightarrow} \forall n \in \mathbb{N} \left(\mathbb{E} \mathbb{M}_{1} \mathbb{I} = n \Rightarrow \mathbb{I} \mathbb{M}_{2} \mathbb{I} = n \right)$ adequacy

At type nat

$M_1 \leq_{ctx} M_2: nat \iff \forall n \in IN(M_1 \#_{nat} \#_{ncc}) \Rightarrow M_2 \#_{nat} \#_{ncc})$ $\iff \forall n \in \mathbb{N} \left(\mathbb{E} M_1 \mathbb{J} = n \implies \mathbb{I} M_2 \mathbb{J} = n \right)$ $def! f \subseteq for IN_{\perp}$ $\longrightarrow [M_1] \subseteq [M_2] \text{ in } N_1$

So E& Edx coincide at type nat

At type nat-nat

$[[M_1] \subseteq [[M_2]] \text{ in } [[nat \rightarrow nat]] = [N_1 \rightarrow N_1]$ iff $\forall d \in [N_1] ([[M_1](d)] \subseteq [[M_2](d)))$

At type nat-nat



At type nat-nat

$[[M, J \subseteq [[M_z]] \text{ in } [[nat \rightarrow nat]] = N_1 \rightarrow N_1$ iff $\forall M: nat([[M_1], [[M_1]]) \subseteq [[M_z]([[M_1]))$

At type nat-nat

$[[M_1] \sqsubseteq [[M_2]] \text{ in } [[nat \rightarrow nat]] = [N_1 \rightarrow N_1]$ iff $\forall M: nat([[M_1, M_1]) \subseteq [[M_2, M_1]))$

At type nat-nat

$$\begin{bmatrix} M_{1} \end{bmatrix} \equiv \begin{bmatrix} M_{2} \end{bmatrix} \text{ in } \begin{bmatrix} \text{nat} \rightarrow \text{nat} \end{bmatrix} = \begin{bmatrix} M_{1} \rightarrow N_{1} \end{bmatrix}$$

iff $\forall M: \text{nat} (\begin{bmatrix} M_{1} & M \end{bmatrix}) \subseteq \begin{bmatrix} M_{2} & M \end{bmatrix})$
iff $\forall M: \text{nat} (M_{1} & M \leq_{ctx} M_{2} & M: \text{nat})$
Since we now know $\subseteq \& \leq_{ctx}$
coincide at type nat

At type nat-nat

$$\begin{bmatrix} M_{1} \end{bmatrix} \equiv \begin{bmatrix} M_{2} \end{bmatrix} \text{ in } \begin{bmatrix} \text{nat} \rightarrow \text{nat} \end{bmatrix} = \begin{bmatrix} M_{1} \rightarrow M_{1} \\ \text{iff} \quad \forall M: \text{nat} (\begin{bmatrix} M_{1} & M_{1} \end{bmatrix}) \subseteq \begin{bmatrix} M_{2} & M_{2} \end{bmatrix}) \\ \text{iff} \quad \forall M: \text{nat} (M_{1} & M_{1} \leq \text{ctx} & M_{2} & \text{mat}) \\ \text{iff} \quad M_{1} \leq \text{ctx} & M_{2}: \text{nat} \rightarrow \text{nat} & (\text{by slide 69}) \\ \text{so} \quad \equiv \& \leq_{\text{ctx}} & \text{coincide at type } \text{nat} \rightarrow \text{nat} \\ \end{bmatrix}$$

At type not
$$\rightarrow$$
 not $\subseteq \& \leq ct_X$ coincide,
essentially because of
 $[M, J \subseteq [M_Z]$ in $[Inat \rightarrow not] = N_1 \rightarrow N_1$
if $\forall d \in N_1 ([M, J(d) \subseteq [M_Z](d))$
 $\forall d \in N_1 ([M, J(d) \subseteq [M_Z](d))$
But every $d \in [N_1]$ is of the form
 $d = [M_J]$ for some $M: nat$

a PCF term. (Ditto for bool.)