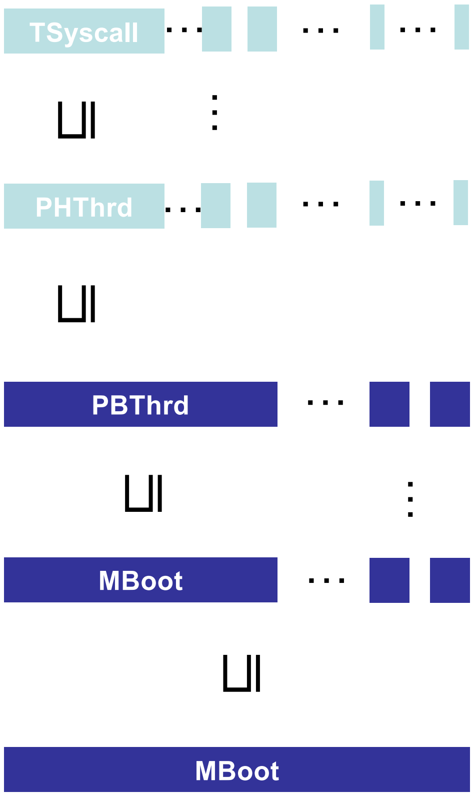


$$[\![\mathbf{Tsyscall}[\mathit{tid}, \varepsilon'_{\mathrm{thrd}}]\langle \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$$

(2) $\sqsubseteq$

$$[\![\mathbf{PHThrd}[\mathit{tid}, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$$

(3) $\sqsubseteq$

$$\left[\!\left[\mathbf{PBThrd}\left[\mathit{cid}, \varepsilon'_{\mathrm{cpu}}\right]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle\right]\!\right]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

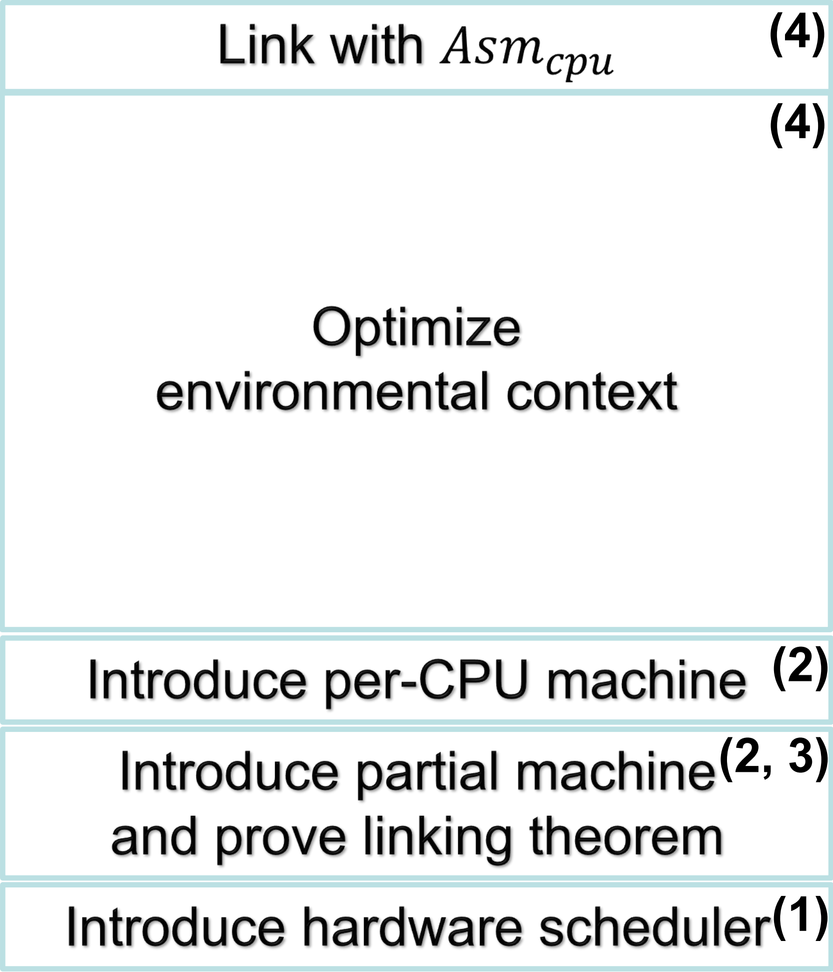
(1) $\sqsubseteq$

$$\left[\!\left[\mathbf{MBoot}\left[\mathit{cid}, \varepsilon_{\mathrm{cpu}}\right]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle\right]\!\right]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

(4) $\sqsubseteq$

$$[\![\mathbf{MBoot}\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{x86}}}$$

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



Link with Asm_{cpu} **(4)**

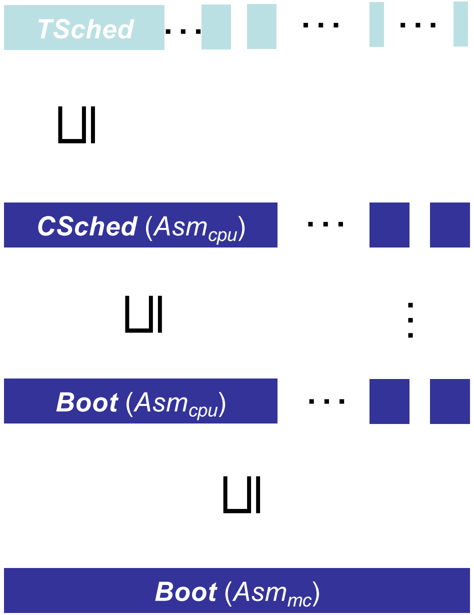
(4) Optimize environmental context

Introduce per-CPU machine **(2)**

Introduce partial machine and prove linking theorem **(2, 3)**

Introduce hardware scheduler **(1)**

$$\begin{array}{c}
Asm_{cpu}(Boot[cid, \varepsilon_{cpu}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{sep}(Boot[cid, \varepsilon_{sep}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{reorder}(Boot[cid, \varepsilon'_{reorder}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{reorder}(Boot[cid, \varepsilon_{reorder}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{split}(Boot[cid, \varepsilon]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{big2}(Boot[cid, \varepsilon]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{big}(Boot[cid, \varepsilon]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{single}(Boot[cid, \varepsilon]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{env}(Boot[cid, \varepsilon]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{env}(\|_{i \in CoreSet}\ Boot[CoreSet, \varepsilon_{CoreSet}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{oracle}(Boot[\varepsilon_{CoreSet}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!] \\
\sqsubseteq \\
Asm_{mc}(Boot) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]
\end{array}$$



$$Asm_{thrd}(TSched[tid, \varepsilon'_{cpu}, \varepsilon_{thrd}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$Asm_{cpu}(CSched[cid, \varepsilon'_{cpu}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$Asm_{cpu}(Boot[cid, \varepsilon_{ccpu}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$Asm_{mc}(Boot) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$$

$$(\text{where } \boxed{\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS_{cpu}} \oplus \mathbf{CertiKOS_{td}}})$$

Link per-CPU machine compiler with per-thread machine **(5)**

Introduce per-thread machine **(1, 2, 3)**

Introduce multithreaded machine and prove linking theorem **(1, 2, 3, 4)**

$$Asm_{thrd}(PHThread[tid, \varepsilon'_{cpu}, \varepsilon_{thrd}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsupseteq$$

$$IAsm_{thrd}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_T^{zip}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsupseteq$$

$$IAsm_{mt}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_T]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsupseteq$$

$$IAsm_{mt}(\|_{ti \in TSet}\ PHBThread[cid, \varepsilon'_{cpu}\ ]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsupseteq$$

$$Asm_{mt}(\|_{ti \in TSet}\ PHBThread[cid, \varepsilon'_{cpu}\ ]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsupseteq$$

$$Asm_{cpu}(PBThread[cid, \varepsilon'_{cpu}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$