Program Analysis System Zoo

Kwangkeun Yi
Research On Program Analysis System
National Creative Research Initiative Center
`ropas.kaist.ac.kr`
KAIST

2001

목 차

1 장

Syntax

1 Grammar

Notation:

$\mid$	alternative	$()$	grouping
$\langle\rangle$	optional	$\bullet^*$	zero or more
$\bullet^+$	one or more	$\dagger$	sugared alternative
αrow	one or more α's separated by **,**		

$$
\begin{array}{rcl}
\mathit{integer} & ::= & (\mathtt{0}-\mathtt{9})^{+} \\
 & | & (\mathtt{0X}|\mathtt{0x})(\mathtt{0}-\mathtt{9}|\mathtt{A}-\mathtt{F}|\mathtt{a}-\mathtt{f})^{+} \\
 & | & (\mathtt{0O}|\mathtt{0o})(\mathtt{0}-\mathtt{7})^{+} \\
 & | & (\mathtt{0B}|\mathtt{0b})(\mathtt{0}-\mathtt{1})^{+} \\
\mathit{comment} & ::= & \text{balanced } \mathtt{(*\ *)}\text{, between which any character can appear.} \\
 & | & \text{from } \mathtt{//} \text{ to the end of the line} \\
 & & \\
\mathit{alphanum} & ::= & \mathtt{a}-\mathtt{z} \mid \mathtt{A}-\mathtt{Z} \mid \mathit{hangul} \mid \mathtt{0}-\mathtt{9} \mid \mathtt{\_} \mid \mathtt{'} \\
\mathit{upper} & ::= & \mathtt{A}-\mathtt{Z} \mid \mathtt{\_} \\
\mathit{lower} & ::= & \mathtt{a}-\mathtt{z} \mid \mathit{hangul} \\
\mathit{hangul} & ::= & \text{syllables of KSX1001 (a.k.a. KSC5601 or eur-kr)} \\
 & | & \text{syllables of KSX1005-1 (a.k.a. KSC5700, unicode, or ISO/IEC10646-1)} \\
\mathit{sym} & ::= & \mathtt{!} \mid \mathtt{\%} \mid \mathtt{\&} \mid \mathtt{\$} \mid \mathtt{\#} \mid \mathtt{+} \mid \mathtt{-} \mid \mathtt{/} \mid \mathtt{:} \mid \mathtt{<} \mid \mathtt{=} \mid \mathtt{>} \mid \mathtt{?} \mid \mathtt{@} \mid \mathtt{\backslash} \mid \mathtt{\tilde{}} \mid \mathtt{`} \mid \mathtt{\hat{}} \mid \mathtt{|} \mid \mathtt{*} \\
\mathit{lid} & ::= & \mathit{lower}(\mathit{alphanum})^{*} \\
\mathit{uid} & ::= & \mathit{upper}(\mathit{alphanum})^{*} \\
\mathit{sid} & ::= & \mathit{sym}\,\mathit{sym}^{+} \\
\mathit{id} & ::= & \mathit{lid} \mid \mathit{uid} \mid \mathit{sid} \\
\mathit{varid} & ::= & \mathit{id} \\
\mathit{ctlid} & ::= & \mathit{id} \\
\mathit{elmtid} & ::= & \mathit{id} \\
\mathit{setid} & ::= & \mathit{uid} \\
\mathit{latid} & ::= & \mathit{uid} \\
\mathit{domid} & ::= & \mathit{setid} \mid \mathit{latid} \\
\mathit{anaid} & ::= & \mathit{id} \\
\mathit{sigid} & ::= & \mathit{id} \\
\mathit{temid} & ::= & \mathit{id} \\
\mathit{cvarid} & ::= & \mathit{id} \\
\mathit{conid} & ::= & \mathit{id} \\
\alpha\mathit{longid} & ::= & \alpha\mathit{id} \ \mid\ \mathit{anaid}.\alpha\mathit{id}
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{topdec} & ::= & \mathit{adec} \\
 & | & \mathit{anadec} \\
 & | & \mathit{sigdec} \\
 & | & \mathit{temdec} \\
 & | & \mathit{topdec}_1\ \mathit{topdec}_2 \\[2ex]
\mathit{adec} & ::= & \mathit{domdec} \\
 & | & \mathit{semdec} \\
 & | & \mathit{querydec} \\
 & | & \mathit{adec}_1\ \mathit{adec}_2 \\[2ex]
\mathit{anadec} & ::= & \texttt{analysis}\ \mathit{anaid}\ \texttt{=}\ \mathit{anaexp} \\
\mathit{anaexp} & ::= & \texttt{ana}\ \mathit{adec}\ \texttt{end} \\
 & | & \mathit{temid}\ \texttt{(}\mathit{anaexprow}\texttt{)} \\
 & | & \mathit{anaid} \\[2ex]
\mathit{sigdec} & ::= & \texttt{signature}\ \mathit{sigid}\ \texttt{=}\ \mathit{sigexp} \\
\mathit{sigexp} & ::= & \texttt{sig}\ \mathit{adesc}\ \texttt{end} \\
 & | & \mathit{sigid} \\[2ex]
\mathit{temdec} & ::= & \texttt{analysis}\ \mathit{temid}\texttt{(}(\mathit{anaid}\ \texttt{:}\ \mathit{sigexp})\mathit{row}\texttt{)}\ \texttt{=}\ \texttt{ana}\ \mathit{adec}\ \texttt{end} \\[2ex]
\mathit{adesc} & ::= & \texttt{set}\ \mathit{setdesc} \\
 & | & \texttt{lattice}\ \mathit{latdesc} \\
 & | & \texttt{val}\ \mathit{varid}\ \texttt{:}\ \mathit{ty} \\
 & | & \texttt{eqn}\ \mathit{varid}\ \texttt{:}\ \mathit{ty} \\
 & | & \texttt{query}\ \mathit{ctlid}\ \texttt{:}\ \mathit{ty} \\
 & | & \mathit{adesc}_1\ \mathit{adesc}_2 \\
 & \dagger & \texttt{set}\ \mathit{setdescrow} \\
 & \dagger & \texttt{lattice}\ \mathit{setdescrow} \\
\mathit{setdesc} & ::= & \mathit{setid}\ \mid\ \mathit{setid}\ \texttt{:}\ \mathit{kind}\ \mid\ \mathit{setbind} \\
\mathit{latdesc} & ::= & \mathit{latid}\ \mid\ \mathit{latid}\ \texttt{:}\ \mathit{kind}\ \mid\ \mathit{latbind}
\end{array}
$$

<table>
<tr><td>domdec</td><td>::=</td><td>setdec | latdec | widendec</td><td></td></tr>
<tr><td>setdec</td><td>::=</td><td><code>set</code> setbind</td><td></td></tr>
<tr><td>setbind</td><td>::=</td><td>setid <code>=</code> setexp</td><td></td></tr>
<tr><td>setexp</td><td>::=</td><td><code>/</code>tylongid<code>/</code> | <code>/</code>strlongid<code>/</code></td><td>nML type/structure id</td></tr>
<tr><td></td><td>|</td><td>setlongid</td><td>set id</td></tr>
<tr><td></td><td>|</td><td><code>{</code> e_1 <code>...</code> e_2 <code>}</code></td><td>integer interval set</td></tr>
<tr><td></td><td>|</td><td><code>{</code> elmtidrow <code>}</code></td><td>enumerated set</td></tr>
<tr><td></td><td>|</td><td><code>power</code> setexp</td><td>power set</td></tr>
<tr><td></td><td>|</td><td>$setexp_1$ <code>*</code> $setexp_2$</td><td>cartesian product</td></tr>
<tr><td></td><td>|</td><td>$setexp_1$ <code>+</code> $setexp_2$</td><td>separated sum</td></tr>
<tr><td></td><td>|</td><td>$setexp_1$ <code>-></code> $setexp_2$</td><td>finite function set</td></tr>
<tr><td></td><td>|</td><td>setexp <code>constraint</code> cnstdec</td><td>constraint set</td></tr>
<tr><td></td><td>|</td><td><code>(</code> setexp <code>)</code></td><td></td></tr>
<tr><td>cnstdec</td><td>::=</td><td><code>var = {</code> cvaridrow <code>}</code> ⟨<code>index</code> setexp⟩</td><td></td></tr>
<tr><td></td><td></td><td><code>rhs =</code> rhs</td><td></td></tr>
<tr><td>rhs</td><td>::=</td><td>cvar ⟨<code>|</code> rhs⟩</td><td></td></tr>
<tr><td></td><td>|</td><td>conid ⟨carg⟩ ⟨<code>: atomic</code>⟩ ⟨<code>|</code> rhs⟩</td><td></td></tr>
<tr><td>cvar</td><td>::=</td><td><code>var</code> | <code>var</code> setid</td><td></td></tr>
<tr><td>carg</td><td>::=</td><td>cvar</td><td></td></tr>
<tr><td></td><td>|</td><td>setexp</td><td></td></tr>
<tr><td></td><td>|</td><td><code>(</code> cargrow <code>)</code></td><td></td></tr>
<tr><td>latdec</td><td>::=</td><td><code>lattice</code> latbind</td><td></td></tr>
<tr><td>latbind</td><td>::=</td><td>latid <code>=</code> latexp</td><td></td></tr>
<tr><td>latexp</td><td>::=</td><td><code>/</code>strlongid<code>/</code></td><td>nML structure id</td></tr>
<tr><td></td><td>|</td><td>latlongid</td><td>lattice id</td></tr>
<tr><td></td><td>|</td><td><code>flat</code> setexp</td><td>flat lattice</td></tr>
<tr><td></td><td>|</td><td><code>power</code> setexp</td><td>powerset lattice</td></tr>
<tr><td></td><td>|</td><td>$latexp_1$ <code>*</code> $latexp_2$</td><td>cartesian product</td></tr>
<tr><td></td><td>|</td><td>$latexp_1$ <code>+</code> $latexp_2$</td><td>coalesced sum</td></tr>
<tr><td></td><td>|</td><td>$latexp_1$ <code>-></code> $latexp_2$</td><td>atomic function lattice</td></tr>
<tr><td></td><td>|</td><td>setexp <code>-></code> latexp</td><td>dependent product lattice</td></tr>
<tr><td></td><td>|</td><td>setexp <code>order</code> order</td><td>lattice with explicit orders</td></tr>
<tr><td></td><td>|</td><td><code>(</code> latexp <code>)</code></td><td></td></tr>
<tr><td>order</td><td>::=</td><td>po pat</td><td>chain</td></tr>
<tr><td></td><td>|</td><td>$order_1$ <code>|</code> $order_2$</td><td></td></tr>
<tr><td></td><td>†</td><td>pat (po pat)$^+$</td><td></td></tr>
<tr><td>po</td><td>::=</td><td><code><</code> | <code>></code></td><td>partial order</td></tr>
<tr><td>widendec</td><td>::=</td><td><code>widen</code> latid <code>with</code> match</td><td></td></tr>
<tr><td>kind</td><td>::=</td><td><code>syntree</code> | <code>index</code> | <code>integer</code> | <code>power</code></td><td></td></tr>
<tr><td></td><td>|</td><td><code>sum</code> | <code>product</code> | <code>arrow</code></td><td></td></tr>
</table>

semdec	::=	*valdec*	
	$\mid$	*eqndec*	
	$\mid$	*ccrdec*	
	$\mid$	*cimdec*	
valdec	::=	`val` *vbind*	auxiliary semantic value
	$\mid$	`val rec` *vbind*	auxiliary semantic value
	†	`fun` *fbind*	
	†	`map` *fbind*	
vbind	::=	*pat* `=` *e* ⟨`and` *vbind*⟩	
fbind	::=	*varid pat* `=` *e* $\mid \cdots \mid$ *varid pat* `=` *e* ⟨`and` *fbind*⟩	
eqndec	::=	`eqn` *ebind*	semantic equation
	$\mid$	`eqn rec` *ebind*	semantic equation
	†	`eqn` *efbind*	
ebind	::=	*varid* `=` *e* ⟨`and` *ebind*⟩	
efbind	::=	*varid pat* `=` *e* $\mid \cdots \mid$ *varid pat* `=` *e* ⟨`and` *efbind*⟩	
ccrdec	::=	`ccr` *cnstguard* `--`$^+$ *constraintrow*	constraint closure rule
cnstguard	::=	*constraint*	
	$\mid$	*guard*	
	$\mid$	$\mathit{cnstguard}_1$ `,` $\mathit{cnstguard}_2$	
constraint	::=	*cvarexp* `<-` *rhsexp*	
rhsexp	::=	*cvarexp*	
	$\mid$	*conid* ⟨*cargexp*⟩	
cargexp	::=	*cvarexp*	
	$\mid$	*pat*	
	$\mid$	`(` *cargexprow* `)`	
cvarexp	::=	*cvarid* $\mid$ *cvarid* `@` *pat*	
cimdec	::=	`cim` *conid* ⟨*pat*⟩ `=` *e*	constraint conid's image declaration

e	::=	/*nmlexp*/	embedded nML expr
	$\mid$	*setlongid*	set itself
	$\mid$	*const*	constant
	$\mid$	*varlongid*	bound id
	$\mid$	*constraint*	constraint
	$\mid$	e_1 *bop* e_2	binary op
	$\mid$	{ e_1 ... e_2 }	integer set
	$\mid$	{ *erow* }	set
	$\mid$	{ *erow* $\mid$ *qual* }	set comprehension
	$\mid$	{ *mrulerow* }	map
	$\mid$	{ *mrulerow* $\mid$ *qual* }	map comprehension
	$\mid$	{}	empty set/map
	$\mid$	+ *e*	fold join
	$\mid$	* *e*	fold meet
	$\mid$	(e_1 , e_2)	tuple
	$\mid$	*e* . 1 $\mid$ *e* . 2	projection
	$\mid$	in (1) *ty* *e* $\mid$ in (2) *ty* *e*	injection
	$\mid$	let *valdec* in *e* end	local expr
	$\mid$	fn *match*	abstraction
	$\mid$	e_1 e_2	application or map image
	$\mid$	(*e*)	
	$\mid$	*e* : *ty*	coercion
	$\mid$	$\langle$pre $\mid$ post$\rangle$ *varlongid* @ *e*	solution look-up
	†	(*e* , *erow*)	tuple
	†	*e* . *domlongid*	projection
	†	*e* [*mrule*]	modifying map
	†	mp *match*	map
	†	case *e* of *match*	branch
	†	if e_1 then e_2 else e_3	branch
bop	::=	+ $\mid$ * $\mid$ -	join, meet, set-minus
const	::=	*integer*	
	$\mid$	*elmtid*	set element id
	$\mid$	top	lattice top
	$\mid$	^	lattice top
	$\mid$	bottom	lattice bottom
	$\mid$	--	lattice bottom
	$\mid$	true	
	$\mid$	false	
ty	::=	int $\mid$ *domlongid* $\mid$ /*tylongid*/	
	$\mid$	ty_1 * ty_2 $\mid$ ty_1 + ty_2	
	$\mid$	ty_1 -> ty_2 $\mid$ power *ty*	
	$\mid$	(*ty*)	
	$\mid$	*ty* : *kind*	

qual	::=	*gen* ⟨`,` *guard*⟩	
gen	::=	*pat* `from` *e*	for each element of a set
	|	*mpat* `from` *e*	for each entry of a map
	|	gen_1 `,` gen_2	
guard	::=	e_1 *rop* e_2	relation
	|	e_1 `in` e_2	membership
	|	`not` *guard*	
	|	$guard_1$ `and` $guard_2$	
	|	$guard_1$ `or` $guard_2$	
	|	`!` *gen* `.` *guard*	for all
	|	`?` *gen* `.` *guard*	for some
	|	`(` *guard* `)`	
	†	*guardrow*	conjunction
rop	::=	`<` | `>` | `=` | `<=` | `>=`	
match	::=	*mrule* ⟨`|` $match_2$⟩	
mrule	::=	*pat* `=>` *e*	
pat	::=	`/`*npat*`/`	nML pattern
	|	`_`	wild pattern
	|	*varid*	pattern var
	|	`{` *patrow* ⟨`...`⟩ `}`	set pattern
	|	`{` pat_1 `...` pat_2 `}`	interval set pattern
	|	`{` *mpatrow* ⟨`...`⟩ `}`	map pattern
	|	`in` `(1`|`2)` *pat*	injection pattern
	|	`(` pat_1 `,` pat_2 `)`	tuple pattern
	|	*pat* `with` *guard*	guarded pattern
	|	pat_1 `or` pat_2	or pattern
	|	*varid* `as` *pat*	as pattern
	|	*pat* `:` *ty*	
	|	`(` *pat* `)`	
	†	*const*	const pattern
	†	`(` *pat* `,` *patrow* `)`	tuple pattern
	†	*pat* *rop* *e*	relation pattern
	†	*pat* `in` *e*	member pattern
mpat	::=	*pat* `=>` *pat*	

querydec	::=	`query` *ctlbind*	
ctlbind	::=	*ctlid* `=` *ctl* ⟨`and` *ctlbind*⟩	
ctl	::=	*varid* `:` ⟨`pre`$\mid$`post`⟩ *varid* `.` *form*	CTL formula with a binder
	$\mid$	*varid* `:` ⟨`pre`$\mid$`post`⟩ *varid* `.` *guard*	CTL formula with a binder
	$\mid$	`(` *ctl* `)`	
form	::=	*ctlid* *varid*	ctl application
	$\mid$	`not` *form*	
	$\mid$	form_1 `and` form_2	
	$\mid$	form_1 `or` form_2	
	$\mid$	form_1 `->` form_2	implication
	$\mid$	*upath* *ctl*	unary path formula
	$\mid$	*bpath* `(` ctl_1 `,` ctl_2 `)`	binary path formula
	$\mid$	`(` *form* `)`	
	†	form_1 `<->` form_2	equivalence
upath	::=	`AX` $\mid$ `AF` $\mid$ `AG`	
	$\mid$	`EX` $\mid$ `EF` $\mid$ `EG`	
bpath	::=	`AU` $\mid$ `EU`	until

2 Syntactic Sugars

Free identifiers must not be bound in the de-sugar'ed definitions.

$\texttt{set}\ \mathit{setdesc}_1\texttt{,}\cdots\texttt{,}\mathit{setdesc}_n$	$\equiv$	$\texttt{set}\ \mathit{setdesc}_1\ \cdots\ \texttt{set}\ \mathit{setdesc}_n$	
$\texttt{lattice}\ \mathit{latdesc}_1\texttt{,}\cdots\texttt{,}\mathit{latdesc}_n$	$\equiv$	$\texttt{lattice}\ \mathit{latdesc}_1\ \cdots\ \texttt{lattice}\ \mathit{latdesc}_n$	
$\mathit{pat}\ \mathit{po}_1\ \mathit{pat}_1\cdots\mathit{po}_n\ \mathit{po}_n$	$\equiv$	$\mathit{po}_1\ \texttt{(}\ \mathit{pat}\texttt{,}\mathit{pat}_1\ \texttt{)}\ \texttt{\|}\cdots\texttt{\|}\ \mathit{po}_n\ \texttt{(}\ \mathit{pat}_{n-1}\texttt{,}\mathit{pat}_n\ \texttt{)}$	
$\texttt{(}\ e_1\texttt{,}e_2\texttt{,}e_3\ \texttt{)}$	$\equiv$	$\texttt{(}\ e_1\texttt{,(}\ e_2\texttt{,}e_3\ \texttt{)}\ \texttt{)}$	
$e\ \texttt{.}\ \mathit{domid}$	$\equiv$	$e\ \texttt{.}\ \texttt{k}$	$e : D = A_1 \times \cdots \times A_n$ and $\mathit{domid} =$
$e\ \texttt{[}\ \mathit{pat}\ \texttt{=>}\ e'\ \texttt{]}$	$\equiv$	$\texttt{\{}\ \mathit{pat}\ \texttt{=>}\ e'\ \texttt{,}\ \texttt{x}\ \texttt{=>}\ e\ \texttt{x}\ \texttt{\}}$	new $\texttt{x}$
$\texttt{mp}\ \mathit{mrule}_1\ \texttt{\|}\cdots\texttt{\|}\ \mathit{mrule}_n$	$\equiv$	$\texttt{\{}\ \mathit{mrule}_1\ \texttt{,}\cdots\texttt{,}\ \mathit{mrule}_n\ \texttt{\}}$	
$\texttt{case}\ e\ \texttt{of}\ \mathit{match}$	$\equiv$	$\texttt{(}\ \texttt{fn}\ \mathit{match}\ \texttt{)}\ e$	
$\texttt{if}\ e_1\ \texttt{then}\ e_2\ \texttt{else}\ e_3$	$\equiv$	$\texttt{case}\ e_1\ \texttt{of}\ \texttt{true}\ \texttt{=>}\ e_2\ \texttt{\|}\ \texttt{false}\ \texttt{=>}\ e_3$	
$\mathit{guard}_1\ \texttt{,}\ \mathit{guard}_2$	$\equiv$	$\mathit{guard}_1\ \texttt{and}\ \mathit{guard}_2$	
$\texttt{(}\ \mathit{pat}_1\ \texttt{,}\ \mathit{pat}_2\ \texttt{,}\ \mathit{pat}_3\ \texttt{)}$	$\equiv$	$\texttt{(}\ \mathit{pat}_1\ \texttt{,}\ \texttt{(}\ \mathit{pat}_2\ \texttt{,}\ \mathit{pat}_3\ \texttt{)}\ \texttt{)}$	
const	$\equiv$	$\texttt{x}\ \texttt{with}\ \texttt{x}\ \texttt{=}\ \mathit{const}$	new $\texttt{x}$
$\mathit{pat}\ \mathit{rop}\ e$	$\equiv$	$\texttt{x}\ \texttt{as}\ \mathit{pat}\ \texttt{with}\ \texttt{x}\ \mathit{rop}\ e$	new $\texttt{x}$
$\mathit{pat}\ \texttt{in}\ e$	$\equiv$	$\texttt{x}\ \texttt{as}\ \mathit{pat}\ \texttt{with}\ \texttt{x}\ \texttt{in}\ e$	new $\texttt{x}$
$\texttt{fun}\ \mathit{varid}\ \mathit{pat}_1\ \texttt{=}\ e_1\ \texttt{\|}\ \mathit{varid}\ \mathit{pat}_2\ \texttt{=}\ e_2$	$\equiv$	$\texttt{val}\ \texttt{rec}\ \mathit{varid}\ \texttt{=}\ \texttt{fn}\ \mathit{pat}_1\ \texttt{=>}\ e_1\ \texttt{\|}\ \mathit{pat}_2\ \texttt{=>}\ e_2$	
$\texttt{map}\ \mathit{varid}\ \mathit{pat}_1\ \texttt{=}\ e_1\ \texttt{\|}\ \mathit{varid}\ \mathit{pat}_2\ \texttt{=}\ e_2$	$\equiv$	$\texttt{val}\ \mathit{varid}\ \texttt{=}\ \texttt{\{}\ \mathit{pat}_1\ \texttt{=>}\ e_1\ \texttt{,}\ \mathit{pat}_2\ \texttt{=>}\ e_2\ \texttt{\}}$	
$\texttt{eqn}\ \mathit{varid}\ \mathit{pat}_1\ \texttt{=}\ e_1\ \texttt{\|}\ \mathit{varid}\ \mathit{pat}_2\ \texttt{=}\ e_2$	$\equiv$	$\texttt{eqn}\ \texttt{rec}\ \mathit{varid}\ \texttt{=}\ \texttt{fn}\ \mathit{pat}_1\ \texttt{=>}\ e_1\ \texttt{\|}\ \mathit{pat}_2\ \texttt{=>}\ e_2$	
$\mathit{form}_1\ \texttt{<->}\ \mathit{form}_2$	$\equiv$	$\mathit{form}_1\ \texttt{->}\ \mathit{form}_2\ \texttt{and}\ \mathit{form}_2\ \texttt{->}\ \mathit{form}_1$	

3 Precedences and Associativity

- Constructs' precedence (in decreasing order) and associativity

constructs	associativity
`order`	–
`power`, `flat`	right
`*`	left
`+`	left
`->`	right

- Constructs' precedence (in decreasing order) and associativity

constructs	associativity
`@`	left
`.`	left
`[`*mrule*`]`	left
application	left
`+` (prefix), `*` (prefix)	right
`*` (infix)	left
`+` (infix), `-` (infix)	left
`<,>,=,<=,>=`	left
`not`	right
`and`	right
`or`	right
`in`	right
`,`	left
`:`	left
`case`, `fn`, `mp`	right

- Pattern constructs' precedence (from higher to lower) and associativity

constructs	associativity
`:`	left
`as`	left
`with`	left

- CTL formula constructs' precedence (from higher to lower) and associativity

constructs	associativity
`not`	right
`and`	left
`or`	left
`->`	left
$(\mathtt{A} \mid \mathtt{E} \mid \mathtt{U})(\mathtt{X} \mid \mathtt{F} \mid \mathtt{G})$	right

4 Syntactic Constraints

- No wildcard pattern is allowed in both the `as`-pattern and `with`-pattern. Because the patterns must be legal as expressions.
- In a constraint set declaration, every constraint function symbol *conid* and constraint variable *cvarid* must be distinct.
- For a constraint closure rule (*ccrdec*), every pattern variable in each constraint or guard must be distinct.

5 Reserved words

```
analysis  ana  end  signature  sig   set  lattice  atomic  val  eqn  query
power  constraint  index  var  rhs  flat  order  widen  with  syntree  index
integer sum  product  arrow  val  rec  fun  map  ccr  cim  and  pre  post
top  bottom  true false int  not  or  let  fn  mp  case  of  as  from  widen
AX  AF  AG  AU  EX  EF  EG  EU  (  )  :  |  {  }  ...  *  +  ->  <- <  >  [  ]
=>  _  !  ?  .  ,  =  <=  >=  <->  @  ^  __
```

2 장

Well-formed Specification for Program Analysis

$$
\begin{array}{rcll}
\textit{Type} & \tau & ::= & \textit{int} \mid \textit{bool} \mid s \mid \ell \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \tau_1 \rightarrow \tau_2 \mid \textit{power}\ \tau \mid \textit{ty}_{nML} \mid \tau : \kappa \\
\textit{Set} & s & ::= & \textit{int} \mid \{\textit{elmtidrow}\} \mid \textit{power}\ s \\
 & & \mid & s_1 \times s_2 \mid s_1 + s_2 \mid s_1 \mapsto s_2 \\
 & & \mid & \textit{tylongid}_{nML} \\
\textit{Lattice} & \ell & ::= & \textit{flat}\ s \mid \textit{ordered}\ s \mid \textit{power}\ s \\
 & & \mid & \ell_1 \times \ell_2 \mid \ell_1 + \ell_2 \mid \ell_1 \mapsto \ell_2 \mid s \mapsto \ell \\
 & & \mid & \textit{strlongid}_{nML} \\
\textit{Kind} & \kappa & ::= & \textit{index} \mid \textit{syntree} \mid \textit{integer} \mid \textit{power} \mid \textit{sum} \mid \textit{product} \mid \textit{arrow} \mid \cdot
\end{array}
$$

$$
\begin{array}{rcrcl}
 & & Pre & = & Type \cup \{\cdot\} \\
 & & Post & = & Type \\
 & & Syntree & = & Set \cup \{\cdot\} \\
 & & Index & = & Set \cup \{\cdot\} \\
p \text{ or } (s_1, s_2) & \in & Pivot & = & Syntree \times Index \\
(\tau_1, \tau_2, p) & \in & EqnType & = & Pre \times Post \times Pivot \\
VE & \in & VarEnv & = & VarId \stackrel{\text{fin}}{\to} Type \cup EqnType \\
CE & \in & CnstEnv & = & CvarEnv \times ConEnv \\
CV & \in & CvarEnv & = & CvarId \stackrel{\text{fin}}{\to} Set \cup Set \times Index \\
CN & \in & ConEnv & = & ConId \stackrel{\text{fin}}{\to} Type \\
SE & \in & SetEnv & = & SetId \stackrel{\text{fin}}{\to} Set \cup Kind \\
LE & \in & LatEnv & = & LatId \stackrel{\text{fin}}{\to} Lattice \cup Kind \\
E \text{ or } (VE, SE, LE, CE) & \in & Env & = & VarEnv \times SetEnv \times LatEnv \times CnstEnv \\
 & & & & \\
AE & \in & AnaEnv & = & AnaId \stackrel{\text{fin}}{\to} Env \\
GE & \in & SigEnv & = & SigId \stackrel{\text{fin}}{\to} Env \\
TE & \in & TemEnv & = & TemId \stackrel{\text{fin}}{\to} ParamEnv \times Env \\
 & & ParamEnv & = & \cup_{k \geq 1}(AnaId \times Env)^k \\
C & \in & Context & = & AnaEnv \times SigEnv \times TemEnv \times Env
\end{array}
$$

$A \stackrel{\text{fin}}{\to} B$: The set of functions from finite subsets of A into B.

$\langle\rangle$: Optional case.

a/b: Alternative case. The correspondence is implied.

$f + g$: Overshadow f by g. If f is a tuple and g is of its one component type, other components of f is intact.

g in A: It denotes an element of a product set A that is made from g. For exampel, if $A = G \times H$ and $H = X \stackrel{\text{fin}}{\to} Y$, "$g$ in A" denotes "$\langle g, \{\}\rangle$."

A of B: When $B = (\cdots, A, \cdots)$, "A of B" denotes A.

$\tau \setminus \tau'$: It denotes the type that results from removing τ' component from a product type τ. When nothing is left, it denotes "empty type" $\cdot$.

$C_\beta(\alpha longid)$:

$$
\begin{array}{rcl}
C_\beta(\alpha id) & = & (\beta \text{ of } (E \text{ of } C))(\alpha id) \\
C_\beta(anaid.\alpha id) & = & (\beta \text{ of } (AE \text{ of } C)(anaid))(\alpha id)
\end{array}
$$

$Kind(\tau)$:

$$
\begin{array}{rclcrcl}
Kind(power\,\tau) & = & power & \quad & Kind(\tau_1 \times \tau_2) & = & product \\
Kind(\tau_1 + \tau_2) & = & sum & & Kind(\tau_1 \mapsto \tau_2) & = & arrow \\
Kind(int) & = & integer & & Kind(\tau : \kappa) & = & \kappa
\end{array}
$$

Analysis Definition

$\boxed{C \vdash topdec \Rightarrow C'}$

$$\frac{C \vdash adec \Rightarrow E}{C \vdash adec \Rightarrow E \text{ in } Context} \tag{2.1}$$

$$\frac{C \vdash anadec \Rightarrow NE}{C \vdash anadec \Rightarrow NE \text{ in } Context} \tag{2.2}$$

$$\frac{C \vdash sigdec \Rightarrow SE}{C \vdash sigdec \Rightarrow SE \text{ in } Context} \tag{2.3}$$

$$\frac{C \vdash temdec \Rightarrow TE}{C \vdash temdec \Rightarrow TE \text{ in } Context} \tag{2.4}$$

$$\frac{C \vdash topdec_1 \Rightarrow C_1 \quad C + C_1 \vdash topdec_2 \Rightarrow C_2}{C \vdash topdec_1\ topdec_2 \Rightarrow C_1 + C_2} \tag{2.5}$$

Analysis Declaration

$\boxed{C \vdash anadec \Rightarrow NE}$

$$\frac{C \vdash anaexp \Rightarrow E}{C \vdash \texttt{analysis}\ anaid\ \texttt{=}\ anaexp \Rightarrow \{anaid \mapsto E\}} \tag{2.6}$$

Aanalysis Expression

$\boxed{C \vdash anaexp \Rightarrow E}$

$$\frac{C \vdash adec \Rightarrow E}{C \vdash \texttt{ana}\ adec\ \texttt{end} \Rightarrow E} \tag{2.7}$$

$$\frac{\begin{array}{c} TE(temid) = (((anaid_1, E'_1), \cdots, (anaid_n, E'_n)), E) \\ \forall i.C \vdash anaexp_i \Rightarrow E_i \quad \forall i.E_i : E'_i \end{array}}{C \vdash temid\ \texttt{(}\ anaexp_1, \cdots, anaexp_n\ \texttt{)} \Rightarrow E} \tag{2.8}$$

Analysis Signature Declaration

$\boxed{C \vdash sigdec \Rightarrow GE}$

$$\frac{C \vdash sigexp \Rightarrow E}{C \vdash \texttt{signature}\ sigid\ \texttt{=}\ sigexp \Rightarrow \{sigid \mapsto E\}} \tag{2.9}$$

Signatre Expression

$\boxed{C \vdash sigexp \Rightarrow E}$

$$\frac{C \vdash adesc \Rightarrow E}{C \vdash \texttt{sig}\ adesc\ \texttt{end} \Rightarrow E} \tag{2.10}$$

$$\frac{GE(\mathit{sigid}) = E}{C \vdash \mathit{sigid} \Rightarrow E} \tag{2.11}$$

Signature Expression Content $\boxed{C \vdash \mathit{adesc} \Rightarrow E}$

$$\frac{C \vdash \mathit{setdesc} \Rightarrow E}{C \vdash \texttt{set}\ \mathit{setdesc} \Rightarrow E} \tag{2.12}$$

$$\frac{C \vdash \mathit{latdesc} \Rightarrow E}{C \vdash \texttt{lattice}\ \mathit{latdesc} \Rightarrow E} \tag{2.13}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau}{C \vdash \texttt{val}\ \mathit{varid} : \mathit{ty} \Rightarrow \{\mathit{varid} \mapsto \tau\} \text{ in } \mathit{Env}} \tag{2.14}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau_1 \to \tau_2 \quad C \vdash \text{air'ed kinds}(\mathit{ty}) \Rightarrow (s_1, s_2) \quad \tau_1' = \tau_1 \setminus s_1 \setminus s_1}{C \vdash \texttt{eqn}\ \mathit{varid} : \mathit{ty} \Rightarrow \{\mathit{varid} \mapsto (\tau_1', \tau_2, (s_1, s_2))\} \text{ in } \mathit{Env}} \tag{2.15}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau \to \mathit{bool}}{C \vdash \texttt{query}\ \mathit{ctlid} : \mathit{ty} \Rightarrow \{\mathit{ctlid} \mapsto \mathit{ty}\} \text{ in } \mathit{Env}} \tag{2.16}$$

$$\frac{C \vdash \mathit{adesc}_1 \Rightarrow E_1 \quad C + E_1 \vdash \mathit{adesc}_2 \Rightarrow E_2}{C \vdash \mathit{adesc}_1\ \mathit{adesc}_2 \Rightarrow E_1 + E_2} \tag{2.17}$$

Set Kind Description $\boxed{C \vdash \mathit{setdesc} \Rightarrow E}$

$$\frac{}{C \vdash \mathit{setid} \Rightarrow \{\mathit{setid} \mapsto \cdot\} \text{ in } \mathit{Env}} \tag{2.18}$$

$$\frac{}{C \vdash \mathit{setid} : \mathit{kind} \Rightarrow \{\mathit{setid} \mapsto \mathit{kind}\} \text{ in } \mathit{Env}} \tag{2.19}$$

$$\frac{C \vdash \mathit{setbind} \Rightarrow E}{C \vdash \mathit{setbind} \text{ as } \mathit{setdesc} \Rightarrow E} \tag{2.20}$$

Lattice Kind Description $\boxed{C \vdash \mathit{latdesc} \Rightarrow E}$

$$\frac{}{C \vdash \mathit{latid} \Rightarrow \{\mathit{latid} \mapsto \cdot\} \text{ in } \mathit{Env}} \tag{2.21}$$

$$\frac{}{C \vdash \mathit{latid} : \mathit{kind} \Rightarrow \{\mathit{latid} \mapsto \mathit{kind}\} \text{ in } \mathit{Env}} \tag{2.22}$$

$$\frac{C \vdash \mathit{latbind} \Rightarrow E}{C \vdash \mathit{latbind} \text{ as } \mathit{latdesc} \Rightarrow E} \tag{2.23}$$

Analysis Type Match $\boxed{E : E'}$

$$\frac{VE : VE' \quad SE : SE' \quad LE : LE' \quad CV : CV' \quad CN : CN'}{E : E'} \tag{2.24}$$

$$\frac{\forall \mathit{varid} \in \mathrm{Dom}\ VE'.\, VE(\mathit{varid}) = VE'(\mathit{varid})}{VE : VE'} \tag{2.25}$$

$$\frac{\forall \mathit{setid} \in \mathrm{Dom}\ SE'.SE(\mathit{setid}) : SE'(\mathit{setid})}{SE : SE'} \tag{2.26}$$

$$\frac{\forall \mathit{latid} \in \mathrm{Dom}\ LE'.LE(\mathit{latid}) : LE'(\mathit{latid})}{LE : LE'} \tag{2.27}$$

$$\frac{\forall \mathit{cvarid} \in \mathrm{Dom}\ CV'.CV(\mathit{cvarid}) = CV'(\mathit{cvarid})}{CV : CV'} \tag{2.28}$$

$$\frac{\forall \mathit{conid} \in \mathrm{Dom}\ CN'.CN(\mathit{conid}) = CN'(\mathit{conid})}{CN : CN'} \tag{2.29}$$

$$\frac{}{\tau : \tau} \tag{2.30}$$

$$\frac{}{\tau : \cdot} \tag{2.31}$$

$$\frac{}{\tau : \mathit{Kind}(\tau)} \tag{2.32}$$

Analysis Template Declaration $\boxed{C \vdash \mathit{temdec} \Rightarrow TE}$

$$\frac{C \vdash \mathit{tembind} \Rightarrow TE}{C \vdash \texttt{analysis}\ \mathit{tembind} \Rightarrow TE} \tag{2.33}$$

$$\frac{\begin{array}{c} C \vdash \mathit{sigexp}_1 \Rightarrow E_1 \quad C \vdash \mathit{sigexp}_2 \Rightarrow E_2 \\ C + \{\mathit{anaid}_1 \mapsto E_1, \mathit{anaid}_2 \mapsto E_2\} \vdash \mathit{adec} \Rightarrow E \end{array}}{\begin{array}{c} C \vdash \mathit{temid}\ \texttt{(}\ \mathit{anaid}_1\ \texttt{:}\ \mathit{sigexp}_1\ \texttt{,}\ \mathit{anaid}_2\ \texttt{:}\ \mathit{sigexp}_2\ \texttt{)}\ \texttt{=}\ \texttt{ana}\ \mathit{adec}\ \texttt{end} \Rightarrow \\ \{\mathit{temid} \mapsto (((\mathit{anaid}_1, E_1), (\mathit{anaid}_2, E_2)), E)\} \end{array}} \tag{2.34}$$

Analysis Content Declaration

$\boxed{C \vdash adec \Rightarrow E}$

$$\frac{C \vdash adec_1 \Rightarrow E_1 \quad C + E_1 \vdash adec_2 \Rightarrow E_2}{C \vdash adec_1\ adec_2 \Rightarrow E_1 + E_2} \tag{2.35}$$

$$\frac{C \vdash domdec \Rightarrow E}{C \vdash domdec \text{ as } adec \Rightarrow E} \tag{2.36}$$

$$\frac{C \vdash semdec \Rightarrow E}{C \vdash semdec \text{ as } adec \Rightarrow E} \tag{2.37}$$

$$\frac{E \vdash querydec \Rightarrow VE}{C \vdash querydec \text{ as } adec \Rightarrow VE \text{ in } Env} \tag{2.38}$$

Domain Declarations

$\boxed{C \vdash domdec \Rightarrow E}$

$$\frac{C \vdash setbind \Rightarrow E}{C \vdash \texttt{set}\ setbind \Rightarrow E} \tag{2.39}$$

$$\frac{C \vdash latbind \Rightarrow E}{C \vdash \texttt{lattice}\ latbind \Rightarrow E} \tag{2.40}$$

$$\frac{\tau = LE(latid) \quad E \vdash match \Rightarrow \tau \to \tau}{C \vdash \texttt{widen}\ latid\ \texttt{with}\ match \Rightarrow \{\}} \tag{2.41}$$

Set Binding

$\boxed{C \vdash setbind \Rightarrow E}$

$$\frac{C \vdash setexp \Rightarrow s, VE \quad setid \notin \text{Dom } SE \cup \text{Dom } LE}{C \vdash setid \texttt{ = } setexp \Rightarrow (VE, \{setid \mapsto s\}, LE, CE)} \tag{2.42}$$

$$\frac{\begin{array}{c} C \vdash setexp \Rightarrow s, VE \quad Kind(s) = power \\ C + VE, s \vdash cnstdec \Rightarrow CE \quad setid \notin \text{Dom } SE \cup \text{Dom } LE \end{array}}{C \vdash setid \texttt{ = } setexp\ \texttt{constraint}\ cnstdec \Rightarrow (VE, \{setid \mapsto s\}, LE, CE)} \tag{2.43}$$

Lattice Binding

$\boxed{C \vdash latbind \Rightarrow E}$

$$\frac{C \vdash latexp \Rightarrow \ell, VE \quad latid \notin \text{Dom } SE \cup \text{Dom } LE}{C \vdash latid \texttt{ = } latexp \Rightarrow (VE, SE, \{latid \mapsto \ell\}, CE)} \tag{2.44}$$

Set Expression

$\boxed{C \vdash \mathit{setexp} \Rightarrow s,\, \mathit{VE}}$

Note that s is a set structure, not a set name.

$$\frac{}{C \vdash \texttt{/}\mathit{tylongid}\texttt{/} \Rightarrow \mathit{tylongid}_{nML}, \{\}} \tag{2.45}$$

$$\frac{s = C_{SE}(\mathit{setlongid})}{C \vdash \mathit{setlongid} \Rightarrow s, \{\}} \tag{2.46}$$

$$\frac{C \vdash e_i \Rightarrow \mathit{int} \quad i = 1,2}{C \vdash \texttt{\{}\ e_1\ \texttt{...}\ e_2\ \texttt{\}} \Rightarrow \mathit{int}, \{\}} \tag{2.47}$$

$$\frac{\begin{array}{c}\{\mathit{elmtidrow}\} \cap \mathrm{Dom}\ \mathit{VE} = \emptyset \\ \mathit{VE}' = \{\mathit{elmtid} \mapsto \{\mathit{elmtidrow}\} \mid \mathit{elmtid} \in \{\mathit{elmtidrow}\}\}\end{array}}{C \vdash \texttt{\{}\ \mathit{elmtidrow}\ \texttt{\}} \Rightarrow \{\mathit{elmtidrow}\},\, \mathit{VE}'} \tag{2.48}$$

$$\frac{C \vdash \mathit{setexp} \Rightarrow s,\, \mathit{VE}}{C \vdash \texttt{power}\ \mathit{setexp} \Rightarrow \mathit{power}\ s,\, \mathit{VE}} \tag{2.49}$$

$$\frac{C \vdash \mathit{setexp}_1 \Rightarrow s_1,\, \mathit{VE}_1 \quad C + \mathit{VE}_1 \vdash \mathit{setexp}_2 \Rightarrow s_2,\, \mathit{VE}_2}{C \vdash \mathit{setexp}_1\ \texttt{*}\ \mathit{setexp}_2 \Rightarrow s_1 \times s_2,\, \mathit{VE}_1 + \mathit{VE}_2} \tag{2.50}$$

$$\frac{C \vdash \mathit{setexp}_1 \Rightarrow s_1,\, \mathit{VE}_1 \quad C + \mathit{VE}_1 \vdash \mathit{setexp}_2 \Rightarrow s_2,\, \mathit{VE}_2}{C \vdash \mathit{setexp}_1\ \texttt{+}\ \mathit{setexp}_2 \Rightarrow s_1 + s_2,\, \mathit{VE}_1 + \mathit{VE}_2} \tag{2.51}$$

$$\frac{C \vdash \mathit{setexp}_1 \Rightarrow s_1,\, \mathit{VE}_1 \quad C + \mathit{VE}_1 \vdash \mathit{setexp}_2 \Rightarrow s_2,\, \mathit{VE}_2}{C \vdash \mathit{setexp}_1\ \texttt{->}\ \mathit{setexp}_2 \Rightarrow s_1 \mapsto s_2,\, \mathit{VE}_1 + \mathit{VE}_2} \tag{2.52}$$

$$\frac{C \vdash \mathit{setexp} \Rightarrow s,\, \mathit{VE}}{C \vdash \texttt{(}\ \mathit{setexp}\ \texttt{)} \Rightarrow s,\, \mathit{VE}} \tag{2.53}$$

Constraint Declaration

$\boxed{C, s \vdash \mathit{cnstdec} \Rightarrow \mathit{CE}}$

$$\frac{\begin{array}{c}C \vdash \mathit{setexp} \Rightarrow s', \{\} \quad \mathit{CV}' \stackrel{\text{let}}{=} \{\forall i.\mathit{cvarid}_i \mapsto (s, s')\} \\ \mathrm{Dom}\ \mathit{CV} \cap \{\mathit{cvaridrow}\} = \{\} \quad C + \mathit{CV}', s \vdash \mathit{rhs} \Rightarrow \mathit{CN}\end{array}}{C, s \vdash \texttt{var = \{}\ \mathit{cvaridrow}\ \texttt{\} index}\ \mathit{setexp}\ \texttt{rhs =}\ \mathit{rhs} \Rightarrow (\mathit{CV}', \mathit{CN})} \tag{2.54}$$

$$\frac{\mathit{CV}' \stackrel{\text{let}}{=} \{\forall i.\mathit{cvarid}_i \mapsto s\} \quad \mathrm{Dom}\ \mathit{CV} \cap \{\mathit{cvaridrow}\} = \{\} \quad C + \mathit{CV}', s \vdash \mathit{rhs} \Rightarrow \mathit{CN}}{C, s \vdash \texttt{var = \{}\ \mathit{cvaridrow}\ \texttt{\} rhs =}\ \mathit{rhs} \Rightarrow (\mathit{CV}', \mathit{CN})} \tag{2.55}$$

Constraint's RHS Declaration

$\boxed{C, s \vdash rhs \Rightarrow CN}$

$$\frac{\langle SE(setid) = s\rangle}{C, s \vdash \texttt{var}\ \langle setid\rangle\ \langle \texttt{|}\ rhs\rangle \Rightarrow \{\}} \tag{2.56}$$

$$\frac{conid \notin \mathrm{Dom}\ CN \quad \langle C, s \vdash rhs \Rightarrow CN\rangle}{C, s \vdash conid\ \langle \texttt{: atomic}\rangle\ \langle \texttt{|}\ rhs\rangle \Rightarrow \{conid \mapsto s\}\ \langle +CN\rangle} \tag{2.57}$$

$$\frac{conid \notin \mathrm{Dom}\ CN \quad C, s \vdash carg \Rightarrow \tau_1 \quad \langle C, s \vdash rhs \Rightarrow CN\rangle}{C, s \vdash conid\ carg\ \langle \texttt{: atomic}\rangle\ \langle \texttt{|}\ rhs\rangle \Rightarrow \{conid \mapsto \tau_1 \to s\}\ \langle +CN\rangle} \tag{2.58}$$

$\boxed{C, s \vdash carg \Rightarrow \tau}$

$$\frac{}{C, s \vdash \texttt{var} \Rightarrow s} \tag{2.59}$$

$$\frac{SE(setid) = s'}{C, s \vdash \texttt{var}\ setid \Rightarrow s'} \tag{2.60}$$

$$\frac{C \vdash setexp \Rightarrow s', \{\}}{C, s \vdash setexp \Rightarrow s'} \tag{2.61}$$

$$\frac{C, s \vdash carg_1 \Rightarrow s_1 \quad C \vdash carg_2 \Rightarrow s_2}{C, s \vdash \texttt{(}\ carg_1\ \texttt{,}\ carg_2\ \texttt{)} \Rightarrow s_1 \times s_2} \tag{2.62}$$

Lattice Expression

$\boxed{C \vdash latexp \Rightarrow \ell, VE}$

Note that ℓ is a lattice structure, not a lattice name.

$$\frac{}{C \vdash \texttt{/}strlongid\texttt{/} \Rightarrow strlongid_{nML}, \{\}} \tag{2.63}$$

$$\frac{\ell = C_{LE}(latlongid)}{C \vdash latid \Rightarrow \ell, \{\}} \tag{2.64}$$

$$\frac{C \vdash setexp \Rightarrow s, VE}{C \vdash \texttt{flat}\ setexp \Rightarrow flat\ s, VE} \tag{2.65}$$

$$\frac{C \vdash setexp \Rightarrow s, VE}{C \vdash \texttt{power}\ setexp \Rightarrow power\ s, VE} \tag{2.66}$$

$$\frac{C \vdash \mathit{setexp} \Rightarrow s,\, VE \quad C \vdash \mathit{order} \Rightarrow s \quad \mathit{Lattice}(\mathit{order})}{C \vdash \mathit{setexp}\ \texttt{order}\ \mathit{order} \Rightarrow \mathit{ordered}\ s,\, VE} \tag{2.67}$$

$$\frac{C \vdash \mathit{latexp}_1 \Rightarrow \ell_1,\, VE_1 \quad C + VE_1 \vdash \mathit{latexp}_2 \Rightarrow \ell_2,\, VE_2}{C \vdash \mathit{latexp}_1\ \texttt{*}\ \mathit{latexp}_2 \Rightarrow \ell_1 \times \ell_2,\, VE_1 + VE_2} \tag{2.68}$$

$$\frac{C \vdash \mathit{latexp}_1 \Rightarrow \ell_1,\, VE_1 \quad C + VE_1 \vdash \mathit{latexp}_2 \Rightarrow \ell_2,\, VE_2}{C \vdash \mathit{latexp}_1\ \texttt{+}\ \mathit{latexp}_2 \Rightarrow \ell_1 + \ell_2,\, VE_2} \tag{2.69}$$

$$\frac{C \vdash \mathit{latexp}_1 \Rightarrow \ell_1,\, VE_1 \quad C + VE_1 \vdash \mathit{latexp}_2 \Rightarrow \ell_2,\, VE_2}{C \vdash \mathit{latexp}_1\ \texttt{->}\ \mathit{latexp}_2 \Rightarrow \ell_1 \mapsto \ell_2,\, VE_2} \tag{2.70}$$

$$\frac{C \vdash \mathit{setexp} \Rightarrow s,\, VE_1 \quad C + VE_1 \vdash \mathit{latexp} \Rightarrow \ell,\, VE_2}{C \vdash \mathit{setexp}\ \texttt{->}\ \mathit{latexp} \Rightarrow s \mapsto \ell,\, VE_2} \tag{2.71}$$

$$\frac{C \vdash \mathit{latexp} \Rightarrow \ell,\, VE}{C \vdash \texttt{(}\ \mathit{latexp}\ \texttt{)} \Rightarrow \ell,\, VE} \tag{2.72}$$

Partial Order

$\boxed{C \vdash \mathit{order} \Rightarrow s}$

$$\frac{C \vdash \mathit{pat} \Rightarrow\ VE, s \times \cdots \times s}{C \vdash \mathit{po}\ \mathit{pat} \Rightarrow s} \tag{2.73}$$

$$\frac{C \vdash \mathit{order}_i \Rightarrow s,\, VE \quad i = 1,2}{C \vdash \mathit{order}_1\ \texttt{|}\ \mathit{order}_2 \Rightarrow s} \tag{2.74}$$

Analysis Expression

$\boxed{C \vdash e \Rightarrow \tau}$

$$\frac{}{C \vdash \texttt{/}\mathit{ne}\texttt{/} \Rightarrow \mathit{ty}_{nML}} \tag{2.75}$$

$$\frac{s = C_{SE}(\mathit{setlongid})}{C \vdash \mathit{setlongid} \Rightarrow s} \tag{2.76}$$

$$\frac{s = C_{VE}(\mathit{varlongid})}{C \vdash \mathit{varlongid} \Rightarrow s} \tag{2.77}$$

$$\frac{CV(\mathit{cvarid}) = (s, s') \quad C, s \vdash \mathit{rhsexp} \Rightarrow \_ \quad C \vdash \mathit{pat} \Rightarrow \_, s'}{C \vdash \mathit{cvarid}\ \texttt{@}\ \mathit{pat}\ \texttt{<-}\ \mathit{rhsexp} \Rightarrow s} \tag{2.78}$$

$$\frac{CV(cvarid) = s \quad C, s \vdash rhsexp \Rightarrow \_}{C \vdash cvarid \texttt{ <- } rhsexp \Rightarrow s} \tag{2.79}$$

$$\frac{}{C \vdash integer \Rightarrow int} \tag{2.80}$$

$$\frac{}{C \vdash (\texttt{top}|\texttt{bottom}|\texttt{\^{}}|\texttt{\_\_}) \Rightarrow \ell} \tag{2.81}$$

$$\frac{C \vdash e_i \Rightarrow int \quad i = 1, 2}{C \vdash e_1 \ (\texttt{+}|\texttt{*}|\texttt{-}) \ e_2 \Rightarrow int} \tag{2.82}$$

$$\frac{C \vdash e_i \Rightarrow \ell \quad i = 1, 2}{C \vdash e_1 \ (\texttt{+}|\texttt{*}) \ e_2 \Rightarrow \ell} \tag{2.83}$$

$$\frac{C \vdash e_i \Rightarrow power\ \tau \quad i = 1, 2}{C \vdash e_1 \ (\texttt{+}|\texttt{*}|\texttt{-}) \ e_2 \Rightarrow power\ \tau} \tag{2.84}$$

$$\frac{C \vdash e_i \Rightarrow int \quad i = 1, 2}{C \vdash \texttt{\{} \ e_1 \ \ldots \ e_2 \ \texttt{\}} \Rightarrow power\ int} \tag{2.85}$$

$$\frac{\forall e \in \{erow\}. C \vdash e \Rightarrow \tau}{C \vdash \texttt{\{} \ erow \ \texttt{\}} \Rightarrow power\ \tau} \tag{2.86}$$

$$\frac{C \vdash qual \Rightarrow VE \quad \forall e \in \{erow\}. C + VE \vdash e \Rightarrow \tau}{C \vdash \texttt{\{} \ erow \ \texttt{|} \ qual \ \texttt{\}} \Rightarrow power\ \tau} \tag{2.87}$$

$$\frac{\forall mrule \in \{mrulerow\}. C \vdash mrule \Rightarrow \tau_1 \rightarrow \tau_2 \quad \tau_1 \mapsto \tau_2 \in Set \cup Lattice}{C \vdash \texttt{\{} \ mrulerow \ \texttt{\}} \Rightarrow \tau_1 \mapsto \tau_2} \tag{2.88}$$

$$\frac{\begin{array}{c} C \vdash qual \Rightarrow VE \quad \tau_1 \mapsto \tau_2 \in Set \cup Lattice \\ \forall mrule \in \{mrulerow\}. C + VE \vdash mrule \Rightarrow \tau_1 \rightarrow \tau_2 \end{array}}{C \vdash \texttt{\{} \ mrulerow \ \texttt{|} \ qual \ \texttt{\}} \Rightarrow \tau_1 \mapsto \tau_2} \tag{2.89}$$

$$\frac{C \vdash e \Rightarrow power\ \ell / power\ power\ \tau}{C \vdash (\texttt{+}|\texttt{*}) \ e \Rightarrow \ell / power\ \tau} \tag{2.90}$$

$$\frac{C \vdash e_i \Rightarrow \tau_i \quad i = 1, 2}{C \vdash \texttt{(} \ e_1 \ \texttt{,} \ e_2 \ \texttt{)} \Rightarrow \tau_1 \times \tau_2} \tag{2.91}$$

$$\frac{C \vdash e \Rightarrow \tau_1 \times \tau_2}{C \vdash e\ \texttt{.}\ \texttt{1} \Rightarrow \tau_1} \tag{2.92}$$

$$\frac{C \vdash e \Rightarrow \tau_1 \times \tau_2}{C \vdash e\ \texttt{.}\ \texttt{2} \Rightarrow \tau_2} \tag{2.93}$$

$$\frac{C \vdash e \Rightarrow \tau_1 \quad C \vdash \mathit{ty} \Rightarrow \tau_1 + \tau_2}{C \vdash \texttt{in (1)}\ \mathit{ty}\ e \Rightarrow \tau_1 + \tau_2} \tag{2.94}$$

$$\frac{C \vdash e \Rightarrow \tau_2 \quad C \vdash \mathit{ty} \Rightarrow \tau_1 + \tau_2}{C \vdash \texttt{in (2)}\ \mathit{ty}\ e \Rightarrow \tau_1 + \tau_2} \tag{2.95}$$

$$\frac{C \vdash \mathit{valdec} \Rightarrow \mathit{VE} \quad C + \mathit{VE} \vdash e \Rightarrow \tau}{C \vdash \texttt{let}\ \mathit{valdec}\ \texttt{in}\ e\ \texttt{end} \Rightarrow \tau} \tag{2.96}$$

$$\frac{C \vdash \mathit{match} \Rightarrow \tau_1 \to \tau_2}{C \vdash \texttt{fn}\ \mathit{match} \Rightarrow \tau_1 \to \tau_2} \tag{2.97}$$

$$\frac{C \vdash e_1 \Rightarrow \tau_1 \to \tau_2 \text{ or } \tau_1 \mapsto \tau_2 \quad C \vdash e_2 \Rightarrow \tau_1}{C \vdash e_1\ e_2 \Rightarrow \tau_2} \tag{2.98}$$

$$\frac{C \vdash e \Rightarrow \tau}{C \vdash \texttt{(}\ e\ \texttt{)} \Rightarrow \tau} \tag{2.99}$$

$$\frac{C \vdash e \Rightarrow \tau \quad C \vdash \mathit{ty} \Rightarrow \tau}{C \vdash e\ \texttt{:}\ \mathit{ty} \Rightarrow \tau} \tag{2.100}$$

$$\frac{C_{VE}(\mathit{varlongid}) = (\tau_1, \tau_2, (s_1, s_2)) \quad C \vdash e \Rightarrow s_2}{C \vdash \langle\texttt{pre}\rangle\ \mathit{varlongid}\ \texttt{@}\ e \Rightarrow \tau_1} \tag{2.101}$$

$$\frac{C_{VE}(\mathit{varlongid}) = (\tau_1, \tau_2, (s_1, s_2)) \quad C \vdash e \Rightarrow s_2}{C \vdash \langle\texttt{post}\rangle\ \mathit{varlongid}\ \texttt{@}\ e \Rightarrow \tau_2} \tag{2.102}$$

Type Expression $\boxed{C \vdash \mathit{ty} \Rightarrow \tau}$

$$\frac{}{C \vdash \texttt{int} \Rightarrow \mathit{int}} \tag{2.103}$$

$$\frac{}{C \vdash \texttt{/}\mathit{tylongid}\texttt{/} \Rightarrow \mathit{tylongid}_{nML}} \tag{2.104}$$

$$\frac{\tau = (\mathit{SE} + \mathit{LE})(\mathit{domid})}{C \vdash \mathit{domid} \Rightarrow \tau} \tag{2.105}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau}{C \vdash \texttt{power}\ \mathit{ty} \Rightarrow \mathit{power}\ \tau} \tag{2.106}$$

$$\frac{C \vdash \mathit{ty}_i \Rightarrow \tau_i \quad i = 1, 2}{C \vdash \mathit{ty}_1\ \texttt{->}\ \mathit{ty}_2 \Rightarrow \tau_1 \rightarrow \tau_2} \tag{2.107}$$

$$\frac{C \vdash \mathit{ty}_i \Rightarrow \tau_i \quad i = 1, 2}{C \vdash \mathit{ty}_1\ \texttt{*}\ \mathit{ty}_2 \Rightarrow \tau_1 \times \tau_2} \tag{2.108}$$

$$\frac{C \vdash \mathit{ty}_i \Rightarrow \tau_i \quad i = 1, 2}{C \vdash \mathit{ty}_1\ \texttt{+}\ \mathit{ty}_2 \Rightarrow \tau_1 + \tau_2} \tag{2.109}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau}{C \vdash \texttt{(}\ \mathit{ty}\ \texttt{)} \Rightarrow \tau} \tag{2.110}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow \tau}{C \vdash \mathit{ty}\ \texttt{:}\ \mathit{kind} \Rightarrow \tau\ \texttt{:}\ \mathit{kind}} \tag{2.111}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow s \quad \text{air}\ \tau\ \texttt{:}\ \mathit{index}}{C \vdash \mathit{ty}\ \texttt{:}\ \texttt{index} \Rightarrow s\ \texttt{:}\ \mathit{index}} \tag{2.112}$$

$$\frac{C \vdash \mathit{ty} \Rightarrow s \quad \text{air}\ \tau\ \texttt{:}\ \mathit{syntree}}{C \vdash \mathit{ty}\ \texttt{:}\ \texttt{syntree} \Rightarrow s\ \texttt{:}\ \mathit{syntree}} \tag{2.113}$$

Aired Kind Hints

$\boxed{C \vdash \text{air'ed kinds}(\star) \Rightarrow (s_1, s_2)}$

$\star$ is either e or ty.

$$\frac{s_1\ \texttt{:}\ \mathit{syntree}\ \ s_2\ \texttt{:}\ \mathit{index}\ \text{are air'ed from}\ \star}{C \vdash \text{air'ed kinds}(\star) \Rightarrow (s_1, s_2)} \tag{2.114}$$

$$\frac{\text{only}\ s\ \texttt{:}\ \mathit{syntree}\ \text{is air'ed from}\ \star}{C \vdash \text{air'ed kinds}(\star) \Rightarrow (s, s)} \tag{2.115}$$

$$\frac{\text{only}\ s\ \texttt{:}\ \mathit{index}\ \text{is air'ed from}\ \star}{C \vdash \text{air'ed kinds}(\star) \Rightarrow (\cdot, s)} \tag{2.116}$$

$$\frac{\text{nothing is air'ed from } \star}{C \vdash \text{air'ed kinds}(\star) \Rightarrow (\cdot, \cdot)} \tag{2.117}$$

Pattern Match

$\boxed{C \vdash \mathit{match} \Rightarrow \tau_1 \to \tau_2}$

$$\frac{C \vdash \mathit{mrule} \Rightarrow \tau_1 \to \tau_2 \quad \langle C \vdash \mathit{match} \Rightarrow \tau_1 \to \tau_2 \rangle}{C \vdash \mathit{mrule}\ \langle \texttt{|}\ \mathit{match} \rangle \Rightarrow \tau_1 \to \tau_2} \tag{2.118}$$

Match Rule

$\boxed{C \vdash \mathit{mrule} \Rightarrow \tau_1 \to \tau_2}$

$$\frac{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau_1 \quad C + \mathit{VE} \vdash e \Rightarrow \tau_2}{C \vdash \mathit{pat}\ \texttt{=>}\ e \Rightarrow \tau_1 \to \tau_2} \tag{2.119}$$

Pattern

$\boxed{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau}$

$$\frac{}{C \vdash \texttt{/}\mathit{npat}\texttt{/} \Rightarrow \mathit{VE}, \mathit{tylongid}_{\mathit{nML}}} \tag{2.120}$$

$$\frac{}{C \vdash \texttt{\_} \Rightarrow \{\}, \tau} \tag{2.121}$$

$$\frac{}{C \vdash \mathit{varid} \Rightarrow \{\mathit{varid} \mapsto \tau\}, \tau} \tag{2.122}$$

$$\frac{C \vdash \mathit{patrow} \Rightarrow \mathit{VE}, \tau}{C \vdash \texttt{\{}\ \mathit{patrow}\ \langle \ldots \rangle\ \texttt{\}} \Rightarrow \mathit{VE}, \mathit{power}\ \tau} \tag{2.123}$$

$$\frac{C \vdash \mathit{pat}_1 \Rightarrow \mathit{VE}_1, \mathit{int} \quad C \vdash \mathit{pat}_2 \Rightarrow \mathit{VE}_2, \mathit{int} \quad \mathrm{Dom}\ \mathit{VE}_1 \cap \mathrm{Dom}\ \mathit{VE}_2 = \emptyset}{C \vdash \texttt{\{}\ \mathit{pat}_1\ \ldots\ \mathit{pat}_2\ \texttt{\}} \Rightarrow \mathit{VE}_1 + \mathit{VE}_2, \mathit{power}\ \mathit{int}} \tag{2.124}$$

$$\frac{C \vdash \mathit{mpatrow} \Rightarrow \mathit{VE}, \tau_1 \mapsto \tau_2}{C \vdash \texttt{\{}\ \mathit{mpatrow}\ \langle \ldots \rangle\ \texttt{\}} \Rightarrow \mathit{VE}, \tau_1 \mapsto \tau_2} \tag{2.125}$$

$$\frac{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau_1 \quad C \vdash \mathit{ty} \Rightarrow \tau_1 + \tau_2}{C \vdash \texttt{in (1)}\ \mathit{ty}\ \mathit{pat} \Rightarrow \mathit{VE}, \tau_1 + \tau_2} \tag{2.126}$$

$$\frac{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau_2 \quad C \vdash \mathit{ty} \Rightarrow \tau_1 + \tau_2}{C \vdash \texttt{in (2)}\ \mathit{ty}\ \mathit{pat} \Rightarrow \mathit{VE}, \tau_1 + \tau_2} \tag{2.127}$$

$$\frac{C \vdash pat \Rightarrow VE, \tau \quad C + VE \vdash guard}{C \vdash pat \; \texttt{with} \; guard \Rightarrow VE, \tau} \tag{2.128}$$

$$\frac{C \vdash pat_1 \Rightarrow VE, \tau \quad C \vdash pat_2 \Rightarrow VE, \tau}{C \vdash pat_1 \; \texttt{or} \; pat_2 \Rightarrow VE, \tau} \tag{2.129}$$

$$\frac{C \vdash pat \Rightarrow VE, \tau}{C \vdash varid \; \texttt{as} \; pat \Rightarrow VE + \{varid \mapsto \tau\}, \tau} \tag{2.130}$$

$$\frac{C \vdash pat \Rightarrow VE, \tau \quad C \vdash ty \Rightarrow \tau}{C \vdash pat \; \texttt{:} \; ty \Rightarrow VE, \tau} \tag{2.131}$$

$$\frac{C \vdash pat \Rightarrow VE, \tau}{C \vdash \texttt{(} \; pat \; \texttt{)} \Rightarrow VE, \tau} \tag{2.132}$$

Patttern Row

$\boxed{C \vdash patrow \Rightarrow VE, \tau}$

$$\frac{C \vdash pat \Rightarrow VE, \tau \quad C \vdash patrow \Rightarrow VE', \tau \quad \mathrm{Dom}\; VE \cap \mathrm{Dom}\; VE' = \emptyset}{C \vdash pat \; \texttt{,} \; patrow \Rightarrow VE + VE', \tau} \tag{2.133}$$

Match-Rule Pattern

$\boxed{C \vdash mpat \Rightarrow VE, \tau}$

$$\frac{C \vdash pat_1 \Rightarrow VE_1, \tau_1 \quad C \vdash pat_2 \Rightarrow VE_2, \tau_2 \quad \mathrm{Dom}\; VE_1 \cap \mathrm{Dom}\; VE_2 = \emptyset}{C \vdash pat_1 \; \texttt{=>} \; pat_2 \Rightarrow VE_1 + VE_2, \tau_1 \mapsto \tau_2} \tag{2.134}$$

Match-Rule Pattern Row

$\boxed{C \vdash mpatrow \Rightarrow VE, \tau}$

$$\frac{C \vdash mpat \Rightarrow VE, \tau \quad C \vdash mpatrow \Rightarrow VE', \tau \quad \mathrm{Dom}\; VE \cap \mathrm{Dom}\; VE' = \emptyset}{C \vdash mpat \; \texttt{,} \; mpatrow \Rightarrow VE + VE', \tau} \tag{2.135}$$

Qualification

$\boxed{C \vdash qual \Rightarrow VE}$

$$\frac{C \vdash gen \Rightarrow VE \quad C + VE \vdash guard}{C \vdash gen\langle \; \texttt{,} \; guard\rangle \Rightarrow VE} \tag{2.136}$$

Generation

$\boxed{C \vdash gen \Rightarrow VE}$

$$\frac{C \vdash pat \Rightarrow VE, \tau \quad C \vdash e \Rightarrow power\ \tau}{C \vdash pat\ \texttt{from}\ e \Rightarrow VE} \tag{2.137}$$

$$\frac{C \vdash mpat \Rightarrow VE, \tau_1 \mapsto \tau_2 \quad C \vdash e \Rightarrow \tau_1 \mapsto \tau_2}{C \vdash mpat\ \texttt{from}\ e \Rightarrow VE} \tag{2.138}$$

$$\frac{C \vdash gen_1 \Rightarrow VE_1 \quad C \vdash gen_2 \Rightarrow VE_2 \quad \mathrm{Dom}\ VE_1 \cap \mathrm{Dom}\ VE_2 = \emptyset}{C \vdash gen_1\ \texttt{,}\ gen_2 \Rightarrow VE_1 + VE_2} \tag{2.139}$$

Guard

$\boxed{C \vdash guard}$

$$\frac{C \vdash e_i \Rightarrow \tau \quad i = 1,2 \quad firstOrder(\tau)}{C \vdash e_1\ rop\ e_2} \tag{2.140}$$

$$\frac{C \vdash e_1 \Rightarrow \tau \quad C \vdash e_2 \Rightarrow power\ \tau}{C \vdash e_1\ \texttt{in}\ e_2} \tag{2.141}$$

$$\frac{C \vdash guard}{C \vdash \texttt{not}\ guard} \tag{2.142}$$

$$\frac{C \vdash guard_1 \quad C \vdash guard_2}{C \vdash guard_1\ (\texttt{and}|\texttt{or})\ guard_2} \tag{2.143}$$

$$\frac{C \vdash gen \Rightarrow VE \quad C + VE \vdash guard}{C \vdash\ \texttt{!}\ gen\ \texttt{.}\ guard} \tag{2.144}$$

$$\frac{C \vdash gen \Rightarrow VE \quad C + VE \vdash guard}{C \vdash \texttt{?}\ gen\ \texttt{.}\ guard} \tag{2.145}$$

$$\frac{C \vdash guard}{C \vdash \texttt{(}\ guard\ \texttt{)}} \tag{2.146}$$

Semantics Declarations

$\boxed{C \vdash semdec \Rightarrow E}$

$$\frac{C \vdash valdec \Rightarrow VE}{C \vdash valdec \Rightarrow VE \text{ in } Env} \tag{2.147}$$

$$\frac{C \vdash \mathit{eqndec} \Rightarrow \mathit{VE}}{C \vdash \mathit{eqndec} \Rightarrow \mathit{VE} \text{ in } \mathit{Env}} \tag{2.148}$$

$$\frac{C \vdash \mathit{ccrdec}}{C \vdash \mathit{ccrdec} \Rightarrow \{\}} \tag{2.149}$$

Auxiliary Value Declaration $\boxed{C \vdash \mathit{valdec} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash \mathit{vbind} \Rightarrow \mathit{VE}}{C \vdash \texttt{val}\ \mathit{vbind} \Rightarrow \mathit{VE}} \tag{2.150}$$

$$\frac{C + \mathit{VE} \vdash \mathit{vbind} \Rightarrow \mathit{VE}}{C \vdash \texttt{val rec}\ \mathit{vbind} \Rightarrow \mathit{VE}} \tag{2.151}$$

Auxiliary Value Binding $\boxed{C \vdash \mathit{vbind} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau \quad C \vdash e \Rightarrow \tau \quad \langle C \vdash \mathit{vbind} \Rightarrow \mathit{VE}' \quad \mathrm{Dom}\ \mathit{VE} \cap \mathrm{Dom}\ \mathit{VE}' = \emptyset \rangle}{C \vdash \mathit{pat}\ \texttt{=}\ e\ \langle \texttt{and}\ \mathit{vbind} \rangle \Rightarrow \mathit{VE}\ \langle + \mathit{VE}' \rangle} \tag{2.152}$$

Semantic Equation Declaration $\boxed{C \vdash \mathit{eqndec} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash \mathit{ebind} \Rightarrow \mathit{VE}}{C \vdash \texttt{eqn}\ \mathit{ebind} \Rightarrow \mathit{VE}} \tag{2.153}$$

$$\frac{C \vdash \mathit{ebind} \Rightarrow \mathit{VE}}{C + \mathit{VE} \vdash \texttt{eqn rec}\ \mathit{ebind} \Rightarrow \mathit{VE}} \tag{2.154}$$

Semantic Equation Binding $\boxed{C \vdash \mathit{ebind} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash e \Rightarrow \tau \quad \langle C \vdash \mathit{ebind} \Rightarrow \mathit{VE} \quad \mathit{varid} \notin \mathrm{Dom}\ \mathit{VE} \rangle}{C \vdash \mathit{varid}\ \texttt{=}\ e\ \langle \texttt{and}\ \mathit{ebind} \rangle \Rightarrow \{\mathit{varid} \mapsto \tau\}\ \langle + \mathit{VE} \rangle} \tag{2.155}$$

$$\frac{\begin{array}{c} C \vdash e \Rightarrow \tau_1 \rightarrow \tau_2 \quad C \vdash \text{air'ed kinds}(e) \Rightarrow (s_1, s_2) \quad s_1 \in \tau_1 \quad s_2 \in \tau_1 \\ \tau_1' = \tau_1 \setminus s_1 \setminus s_1 \quad \langle C \vdash \mathit{ebind} \Rightarrow \mathit{VE} \quad \mathit{varid} \notin \mathrm{Dom}\ \mathit{VE} \rangle \end{array}}{C \vdash \mathit{varid}\ \texttt{=}\ e\ \langle \texttt{and}\ \mathit{ebind} \rangle \Rightarrow \{\mathit{varid} \mapsto (\tau_1', \tau_2, (s_1, s_2))\}\ \langle + \mathit{VE} \rangle} \tag{2.156}$$

Constraint Closure Rules $\boxed{C \vdash \mathit{ccrdec}}$

$$\frac{C \vdash \mathit{cnstguard} \Rightarrow \mathit{VE} \quad \forall i. C \vdash \mathit{constraint}_i \Rightarrow \_}{C \vdash \texttt{ccr}\ \mathit{cnstguard}\ \texttt{--}^{+}\ \mathit{constraintrow}} \tag{2.157}$$

Constraint or Guard Sequence

$\boxed{C \vdash cnstguard \Rightarrow VE}$

$$\frac{C \vdash constraint \Rightarrow VE}{C \vdash constraint \text{ as } cnstguard \Rightarrow VE} \tag{2.158}$$

$$\frac{C \vdash guard}{C \vdash guard \text{ as } cnstguard \Rightarrow \{\}} \tag{2.159}$$

$$\frac{C \vdash cnstguard_1 \Rightarrow VE_1 \quad C + VE_1 \vdash cnstguard_2 \Rightarrow VE_2}{C \vdash cnstguard_1 \texttt{ , } cnstguard_2 \Rightarrow VE_1 + VE_2} \tag{2.160}$$

Constraint

$\boxed{C \vdash constraint \Rightarrow VE}$

$$\frac{CV(cvarid) = (s, s') \quad C, s \vdash rhsexp \Rightarrow VE \quad C \vdash pat \Rightarrow \_, s'}{C \vdash cvarid \texttt{ @ } pat \texttt{ <- } rhsexp \Rightarrow VE} \tag{2.161}$$

$$\frac{CV(cvarid) = s \quad C, s \vdash rhsexp \Rightarrow VE}{C \vdash cvarid \texttt{ <- } rhsexp \Rightarrow VE} \tag{2.162}$$

Constraint's RHS Expression

$\boxed{C, s \vdash rhsexp \Rightarrow VE}$

$$\frac{CV(cvarid) = s}{C, s \vdash cvarid \Rightarrow \{\}} \tag{2.163}$$

$$\frac{CV(cvarid) = (s, s') \quad C \vdash pat \Rightarrow VE, s'}{C, s \vdash cvarid \texttt{ @ } pat \Rightarrow VE} \tag{2.164}$$

$$\frac{CN(conid) = s}{C, s \vdash conid \Rightarrow \{\}} \tag{2.165}$$

$$\frac{CN(conid) = \tau \to s \quad C, \tau \vdash cargexp \Rightarrow VE}{C, s \vdash conid\ cargexp \Rightarrow VE} \tag{2.166}$$

Constraint's RHS Arguments

$\boxed{C, \tau \vdash cargexp \Rightarrow VE}$

$$\frac{CV(cvarid) = (\tau, s) \quad \langle C \vdash pat \Rightarrow \_, s\rangle}{C, \tau \vdash cvarid\ \langle \texttt{@ } pat\rangle \Rightarrow \{\}} \tag{2.167}$$

$$\frac{C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau}{C, \tau \vdash \mathit{pat} \Rightarrow \mathit{VE}} \tag{2.168}$$

$$\frac{C, \tau \vdash \mathit{cargexp} \Rightarrow \mathit{VE}}{C, \tau \vdash \texttt{(}\ \mathit{cargexp}\ \texttt{)} \Rightarrow \mathit{VE}} \tag{2.169}$$

$$\frac{C, \tau_1 \vdash \mathit{cargexp}_1 \Rightarrow \mathit{VE} \quad C, \tau_2 \vdash \mathit{cargexp}_2 \Rightarrow \mathit{VE}'}{C, \tau_1 \times \tau_2 \vdash \texttt{(}\ \mathit{cargexp}_1\ \texttt{,}\ \mathit{cargexp}_2\ \texttt{)} \Rightarrow \mathit{VE} + \mathit{VE}'} \tag{2.170}$$

Constraint RHS's Image

$\boxed{C \vdash \mathit{cimdec}}$

$$\frac{\mathit{CN}(\mathit{conid}) = \tau \to s \quad C \vdash \mathit{pat} \Rightarrow \mathit{VE}, \tau \quad C + \mathit{VE} \vdash e \Rightarrow s}{C \vdash \texttt{cim}\ \mathit{conid}\ \mathit{pat}\ \texttt{=}\ e} \tag{2.171}$$

$$\frac{\mathit{CN}(\mathit{conid}) = s \quad C + \mathit{VE} \vdash e \Rightarrow s}{C \vdash \texttt{cim}\ \mathit{conid}\ \texttt{=}\ e} \tag{2.172}$$

Query

$\boxed{C \vdash \mathit{querydec} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash \mathit{ctlbind} \Rightarrow \mathit{VE}}{C \vdash \texttt{query}\ \mathit{ctlbind} \Rightarrow \mathit{VE}} \tag{2.173}$$

Query Formula Bind

$\boxed{C \vdash \mathit{ctlbind} \Rightarrow \mathit{VE}}$

$$\frac{C \vdash \mathit{ctl} \Rightarrow \tau \quad \langle C \vdash \mathit{ctlbind} \Rightarrow \mathit{VE}' \rangle}{C \vdash \mathit{varid}\ \texttt{=}\ \mathit{ctl}\ \langle \texttt{and}\ \mathit{ctlbind} \rangle \Rightarrow \{\mathit{varid} \mapsto \tau\}\ \langle + \mathit{VE}' \rangle} \tag{2.174}$$

Query Formula

$\boxed{C \vdash \mathit{ctl} \Rightarrow \ell \to \mathit{bool}}$

$$\frac{\mathit{VE}(\mathit{varid}_2) = \tau \quad E + \{\mathit{varid}_1 \mapsto \tau\} \vdash \mathit{form/guard}}{C \vdash \mathit{varid}_1\ \texttt{:}\ \mathit{varid}_2\ \texttt{.}\ \mathit{form/guard} \Rightarrow \tau \to \mathit{bool}} \tag{2.175}$$

$$\frac{\mathit{VE}(\mathit{varid}_2) = (\tau_1, \tau_2, p) \quad \tau' = \tau_1 \setminus p \quad E + \{\mathit{varid}_1 \mapsto \tau'\} \vdash \mathit{form/guard}}{C \vdash \mathit{varid}_1\ \texttt{:}\ \texttt{pre}\ \mathit{varid}_2\ \texttt{.}\ \mathit{form/guard} \Rightarrow \tau' \to \mathit{bool}} \tag{2.176}$$

$$\frac{\mathit{VE}(\mathit{varid}_2) = (\tau_1, \tau_2, p) \quad E + \{\mathit{varid}_1 \mapsto \tau_2\} \vdash \mathit{form/guard}}{C \vdash \mathit{varid}_1\ \texttt{:}\ \texttt{post}\ \mathit{varid}_2\ \texttt{.}\ \mathit{form/guard} \Rightarrow \tau_2 \to \mathit{bool}} \tag{2.177}$$

$$\frac{C \vdash ctl \Rightarrow \tau \rightarrow bool}{C \vdash \texttt{(}\ ctl\ \texttt{)} \Rightarrow \tau \rightarrow bool} \tag{2.178}$$

Query Expression

$\boxed{C \vdash form}$

$$\frac{C \vdash ctlid\ varid \Rightarrow bool}{C \vdash ctlid\ varid} \tag{2.179}$$

$$\frac{C \vdash form}{C \vdash \texttt{not}\ form} \tag{2.180}$$

$$\frac{C \vdash form_1 \quad C \vdash form_2}{C \vdash form_1\ (\texttt{and}|\texttt{or}|\texttt{->})\ form_2} \tag{2.181}$$

$$\frac{C \vdash ctl \Rightarrow \_}{C \vdash (\texttt{A}|\texttt{E})(\texttt{X}|\texttt{F}|\texttt{G})\ ctl} \tag{2.182}$$

$$\frac{C \vdash ctl_1 \Rightarrow \_ \quad C \vdash ctl_2 \Rightarrow \_}{C \vdash (\texttt{A}|\texttt{E})\texttt{U}\ \texttt{(}\ ctl_1\ \texttt{,}\ ctl_2\ \texttt{)}} \tag{2.183}$$

$$\frac{C \vdash form}{C \vdash \texttt{(}\ form\ \texttt{)}} \tag{2.184}$$

3 장

Compiling Into Executable Analyzers

Well-formed Rabbit specification gurantees to transform into typeful nML programs:

Theorem 1 (Type Safety) *If* $\vdash spec$ *then* $spec \hookrightarrow topdec_{nML}$ *and for an nML basis* B*,* $B \vdash_{nML} topdec \Rightarrow B'$*.*