The HOL4P4 P4 Formalization

Anoud Alshnakat
Didrik Lundberg

October 26, 2022

This is a description of the HOL4P4 formalization of P4, which includes a syntax and a strictly small-step style semantics. It is based on the official P4 specification and inspired by Core P4 [1].

HOL4P4 is constructed using the ott tool. ott files can then be exported to LaTeX commands (used in this document) as well as to the HOL4, Isabelle/HOL and Coq interactive theorem provers (of which only the first is currently supported).

1 Syntax

1.1 Types

x, f, tbl	string
b	boolean
bl	bit-string
i, w	natural number
m, n, o	indices

Figure 1: Variables

The variables shown in Figure 1 are standard designations for variables of P4 base types included in HOL4P4, plus the numerals i (sometimes w when referring to width) and the indices m, n, o which are not part of the P4 syntax, but used on a meta-level throughout this formalization. Depending on the context, strings are denoted with x (variable or parser state name), tbl (match-action table name) or f (function or field name). bl is a list of Boolean values, used to represent bit-strings of fixed width.

P4 types are sometimes explicitly referenced in the syntax, e.g. in declaration statements. The notation for this is shown in Figure 2.

1.2 Expressions

HOL4P4 includes a subset of the full set of P4 expressions found in Section 8 of the P4 specification, shown in Figure 4.

First, an expression can be a value v, the types of which are shown in Figure 3. It can also be a variable, in which case it has an abstract variable name $varn$ which is either the special "star"

τ	::=		type
	|	**bool**	boolean
	|	bs^{num_exp}	bit-string
	|	$\bot$	no value
	|	$struct\_ty[x_1\ \tau_1, .., x_n\ \tau_n]$	struct
	|	$\overline{x}\_list$ string literal	
	|	**err**	
	|	**ext**	

Figure 2: Types

v	::=	value
| $boolv$		boolean value
| $bitv$		bit-string
| x		string literal
| **struct** $\{x_1 = v_1; ...; x_n = v_n\}$		struct
| **header** $boolv\{x_1 = v_1; ...; x_n = v_n\}$		header
| **errmsg** x		error message
| **ext_ref** i		extern object reference
| **bot**		no value

Figure 3: P4 Values

e	::=	expression
| v		value
| **var** $varn$		variable
| $\{e_1, .., e_n\}$		expression list
| $e.x$		field access
| $\ominus e$		unary operation
| $e_1 \oplus e_2$		binary operation
| **concat** $e_1\ e_2$		concatenation of bit-strings
| $e_1[e_2 : e_3]$		bit-slice
| **call** $funn(e_1, .., e_n)$		function or extern call
| **select** $e\{v_1 : x_1; ...; v_n : x_n\}x$		select
| **eStruct** $\{x_1 = e_1; ...; x_n = e_n\}$		struct
| **eHeader** $boolv\{x_1 = e_1; ...; x_n = e_n\}$		header
| (e)	S	

Figure 4: P4 Expressions

function return placeholder variable, in which case it holds the corresponding *funn*, or a regular variable, which holds the variable name x. Lists of expressions can be used in initialisation of variables of struct types. The fields of these structs may be accessed, which is denoted in the usual manner. There exist unary and binary arithmetic operations, where the semantics of the individual operations are defined on some subset of the constants[1]. Bitstrings can be concatenated

[1]The concrete syntax of the many unary and binary operations is found in Appendix A

and sliced. The function call is built from the abstract function name *funn*, and a list of arguments (expressions).

The **select** expression is similar to a switch statement in C or Java. The expression e is evaluated, and then matched against $v_1, \ldots, v_n$. If some match is successful, the **select** expression evaluates to the string at the corresponding index. If no match occurs, then it instead evaluates to the default string x.

Furthermore, structs and headers can also have expression values assigned to their keys, and so be expressions (separate from the struct and header values).

1.3 Statements

stmt	::=		statement
	|	$\emptyset_{\text{stmt}}$	empty statement
	|	$lval := e$	assignment
	|	**if** e **then** $stmt_1$ **else** $stmt_2$	conditional
	|	$\{\overline{decl}\ stmt\}$	block
	|	**return** e	return
	|	$stmt_1; stmt_2$	sequence
	|	**verify** $e\ e'$	verify
	|	**transition** e	transition
	|	**apply** $tbl(e_1, .., e_n)$	apply
	|	■	extern function

Figure 5: P4 Statements

`HOL4P4` includes a subset of the full set of P4 statements found in Section 11 of the P4 specification, shown in Figure 5. The statements in Figure 5 can be found in the specification, with the following exceptions: the block, verify, apply and extern statements. The block statement features an additional list of declarations (note the absence of declarations from this syntax, in contrast to the P4 specification), the apply statement (replacing the apply method in Section 11 of the P4 specification) features the list of arguments that are to be matched to the table *tbl* (which is possible to resolve at compile time), and the extern captures the semantics of an extern function or method. The **verify** statement (modeled as a statement and not as an extern function as in Section 12.7 of the P4 specification) can be found uniquely in a parser block. It asserts the expression e and if it holds, does nothing. If e does not hold, it jumps to the 'reject" parser state with the error message being the result of evaluating e'.

lval	::=		
	|	*varn*	variable name
	|	**null**	null variable
	|	$lval.f$	field access
	|	$(lval)$	

Figure 6: P4 l-values

*lval*s are shown in Figure 6 and include variables identified by their names, a null variable (used

to model method calls) and struct fields, which are identified by the struct and field names, similar to the field access expression.

1.4 Execution State

t	::=		execution status
	|	**run**	
	|	**ret** v	
	|	**tra** x	transition to parser state
s	::=		execution state
	|	$(\gamma_A, \overline{\gamma_G}, \overline{\Phi}, t)$ M	

Figure 7: P4 Execution State

The P4 execution state is shown in Figure 7. Note that a "P4 execution state" is not defined in the P4 specification, so it is entirely an artifice of the `HOL4P4` implementation. In short, the execution state s is a tuple of the architectural state γ_A, the global scope list $\overline{\gamma}_G$, a frame list $\overline{\Phi}$, and the state status t.

Scope

More formally, a scope $\gamma : X \hookrightarrow V * (X \cup \{\bot\})$ is a partial function from variable names $x \in X$ to constant values $v \in V$. The following operations can be performed on γ:

- $\text{dom}(\gamma)$: Gets the domain of γ: obtains the set of variable names $x \in X$ which are mapped to values in γ.
- $(x \mapsto v)\ \gamma$: Updates a variable mapping in γ: yields the scope γ', which is just γ where x instead maps to v. By writing $\forall i \leq n.\ (x_i \mapsto v_i)\ \gamma$ we extend this to lists of mappings from variable names to values.

Scope list

$\overline{\gamma}$ is a list of scopes $\gamma_1, \ldots, \gamma_n$ where the index 1 is the most recently entered scope, and n is the oldest.

Global scope list

The global scope list $\overline{\gamma_G}$ contains two elements; index 0 represents the programmable block local scope, while index 1 represents the global scope of the architecture. Initially when a programmable block is entered, for each function declared globally in the architecture or locally in a programmable block a return variable is declared in the local programmable block scope.

List of statements

The list of statements $\overline{stmt}$ is simply a list of $stmt_1, \ldots, stmt_n$ where $stmt_1$ belongs to the most recent block we have entered, and $stmt_n$ is the oldest one.

Whenever a block $\{\overline{decl}\ stmt_b\}; stmt$ is encountered, the block's statement $stmt_b$ will be appended to the old statement $stmt$ leaving an empty statement in it's original place. So the next transition will become $stmt_b :: (\emptyset_{stmt}; stmt$

Function name

The abstract function name $funn$ identifies the function name, extern method or extern constructor. In P4, functions can be declared globally, or locally in the programmable block (actions). We model the actions exactly as the functions, and to distinguish between them we store their signatures and bodies in two different locations: the programmable block-local functions' signature and body in the mapping F_b, and the globally declared functions' and actions' signatures and bodies are stored in the mapping F_g. Both F_b and F_g are stored in the context ctx which will be discussed later.

Frame

The frame Φ is a tuple of three members: a function name $funn$, a statement list $\overline{stmt}$ and a scope list $\overline{\gamma}$; represented as $\overline{stmt}_{\overline{\gamma}}^{funn}$. Whenever a function call occurs, in the state the frame of the callee will be appended to the frame of the caller as $\Phi_{callee} :: \overline{\Phi}$.

Control plane configuration

It is a function that takes a table name tbl, the key list expressions $e_1, \ldots, e_n$, and a list of matching kinds $mk_1, \ldots, mk_n$ then returns the actions and their arguments. This ill be explained further in the statements semantics.

Status

Represented in the state with t. The status **run** represents that the program is executing under regular circumstances. **ret** v is used when the **return** statement returns a value v ($\perp$ if it has a void return value) at the end of a function call. The status **tra** x signifies transition to a new parser state. The new parser state can be a final state in the case of **tra** $xaccept$ or **tra** $xreject$, or otherwise a state defined in the P4 program.

Context

The ctx is a tuple of the following:

1. $table\_apply$: the apply table function which takes a table name, parameters, match kinds and the architectural scope and returns an action with parameters.
2. X: the extern object map, which maps extern object names to tuples of constructors and their respective function maps.
3. F_g: the globally-declared function map. It maps global function and action names to tuples of their bodies, argument names and directions.
4. F_b: the programmable block-local function map. It maps local function names to tuples of their bodies, argument names and directions.
5. P parser states map. It maps the name of parser states to their bodies.
6. Tb the table map. It maps the table name to its list of match kinds and default action with parameters.

The context ctx is static in the statement semantics, and is therefore separated out from the execution state.

1.5 Calling convention

The calling conventions can be directioned or directionless. The direction can be either IN, OUT or INOUT. IN direction summary:

1. Should not be used on the left hand of assignment
2. Shouldn't be passed to a function without using the proper calling convention IN
3. Initialized by copying the value of the corresponding argument when the invocation is executed.

OUT summary:

1. usually uninitialized, and treated as l-values. after the execution of the call, the value of the OUT parameters copied to the corresponding location of the l-value. OUT parameters are initialized in the following cases
   (a) if the types are header or header_union, OUT parameter is set to "invalid"
   (b) if the type is a header stack, then all elements of the header stack set to "invalid" and the next index is initialized to 0.
   (c) if the type is compound (e.g. struct or tuple) apply the rules recursively to its members.
   (d) if any any other type than listed above (e.g. bit <W>), then it doesn't need any predictable value.

INOUT summary:

1. this type of parameters are both IN and OUT.
2. it must be an l-value, which means it can be assigned to a value.

NO direction summary:

1. those parameters are known at compile time.
2. it also can be an action parameter, can be set by the control plane.
3. it also can be an action parameter that set directly by an other action, then the behaviour will be like IN parameter.

The direction d can be $\downarrow$ denotes IN, $\uparrow$ denotes OUT, $\updownarrow$ denotes INOUT, $\circ$ denotes directionless. Thus, d ::= $\downarrow \mid \uparrow \mid \updownarrow \mid \circ$
Due to the calling conventions, the scope has the type; $\gamma : X \hookrightarrow V * (X \cup \{\perp\})$.
The list of scopes is identified with an arrow following $\overline{\gamma}$. The local $\overline{\gamma}$ is meant to be a local list of scopes to the frame. The global $\overline{\gamma}_G$ is a list with a length of 2. The first index determines the external architecture scope (can not be defined by a P4 program), while the second index determines the architecture local variables (defined in the architecture level). Opeations on list of scopes:

1. Operation $\gamma[x \longmapsto v]$ to update a variable name x with value v in the scope γ.
2. Operation $\overline{\gamma}[x \longmapsto v]$ to update a variable name x with value v in the most recent scope that contains the variable name x.
3. Operation $lookup_v(\overline{\gamma}, \overline{\gamma}_G, x)$ to return the value v of the tuple $(y, x \cup \perp)$, which is whatever variable x is mapped to in the most recent scope it is defined in after concatenating $\overline{\gamma}_G +\!\!+ \overline{\gamma}$.

2 Semantics

2.1 Expressions

Expression semantics and reductions are laid out in this section. Overall, the reductions can never alter or have any side effects on the state. The only thing it can perform is a reduction on the expressions - standard small step structural semantics - and also produce a new frame (which then indirectly can have side-effects on the state), which occurs only in the function call reduction.

Variable lookup

In the E_LOOKUP rule, the lookup function ensures that the variable name x is evaluated in the uppermost scope (i.e. most recent scope γ that x exists in). The evaluation will occur using the function lookup_v. It will sweep the list of scopes $\overline{\gamma} +\!\!+ \overline{\gamma}_G$ and find the most recent (leftmost in the list) scope that contains variable x and this is because the scopes grow from right to left. This agrees with the description in Sections 6.8 and 10.2 of the P4 specification. The constant value of this variable is then returned to the expression reduction.

$$\frac{v = \text{lookup}_\text{v}(\overline{\gamma}, \overline{\gamma_G}, varn)}{ctx\ \overline{\gamma_G}\ \overline{\gamma} \vdash (\textbf{var}\ varn) \rightsquigarrow (v, [\,])} \quad \text{E\_LOOKUP}$$

Function call

Note that function calls also include actions as well as extern function calls.

The E_CALL_ARGS is used whenever there is a function call expression with unreduced (in- and none-directioned) arguments. We fetch the function name's argument names and directions using **lookup_funn_sig**, then each function's argument will be checked against the function's direction in the same position. If the direction is in or none, then it will be reduced until it becomes a constant, otherwise if the argument has the direction out or inout it should not be reduced.

The E_CALL_NEWFRAME rule is used when all of the function arguments have been reduced to constants (for non-out directions) or variables (directions with out). The function call reduction will produce a placeholder we call **var**(**star**, $funn$) and a new frame. The new frame will be added by the enclosing statement semantic layer on top of the state's existing frames, as explained later. The way that this new frame is constructed is as follows: The function name *funn* will be the same as the call in the expression. The function name *funn* will be looked up in both the function maps and extern maps to retrieve the function body *stmt* and the signature of the parameters represented as a list of tuples of variable names and their directions $[(x_1, d_1), \ldots, (x_n, d_n)]$. Each argument will be checked to ensure that the arguments were reduced properly: (if d_i is in or none then the expression in the same position should be a constant, otherwise a variable name). The new frame's scope γ' is a new fresh empty scope that contains the copied-in arguments using the function **copyin**.

Headers and structs

The struct can be an expression, thus we need reductions for it. The E_ESTRUCT rule will reduce the expression fields one at a time from left to right. Once all the expressions have become constants we

$$\frac{\begin{array}{l}[(x_1,d_1),\,..\,,(x_n,d_n)] = \mathbf{lookup\_funn\_sig}\,(\mathit{funn},F_g,F_b,X)\\ i = \min\{j.\ [d_1,\,..\,,d_n][j] \in \{\circ,\downarrow\} \wedge \neg(\mathrm{is\_const}\,[e_1,\,..\,,e_n][j])\}\\ e = [e_1,\,..\,,e_n][i]\\ (\mathit{apply\_table},X,F_g,F_b,P,\mathit{Tb})\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e',\overline{\Phi})\\ [e'_1,\,..\,,e'_n] = (i \mapsto e')[e_1,\,..\,,e_n]\end{array}}{(\mathit{apply\_table},X,F_g,F_b,P,\mathit{Tb})\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{call}\,\mathit{funn}(e_1,\,..\,,e_n)) \rightsquigarrow (\mathbf{call}\,\mathit{funn}(e'_1,\,..\,,e'_n),\overline{\Phi})}\ \textsc{e\_call\_args}$$

$$\frac{\begin{array}{l}(\mathit{stmt},[(x_1,d_1),\,..\,,(x_n,d_n)]) = \mathbf{lookup\_funn\_sig\_body}\,(\mathit{funn},F_g,F_b,X)\\ \forall i \leqslant n.\,((d_i \in \{\circ,\downarrow\} \implies \mathrm{is\_const}\,e_i) \wedge (d_i \in \{\updownarrow,\uparrow\} \implies \mathrm{is\_var}\,e_i))\\ \gamma' = \mathrm{copyin}([x_1,\,..\,,x_n],[e_1,\,..\,,e_n],[d_1,\,..\,,d_n],,,\overrightarrow{\gamma})\end{array}}{(\mathit{apply\_table},X,F_g,F_b,P,\mathit{Tb})\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{call}\,\mathit{funn}(e_1,\,..\,,e_n)) \rightsquigarrow (\mathbf{var}\,(\mathbf{star}\,,\mathit{funn}),[([\mathit{stmt}])^{\mathit{funn}}_{[\gamma']}])}\ \textsc{e\_call\_newframe}$$

can transform the expression struct to a value struct via E_EStruct_to_V. The same operations are applied on the headers.

$$\frac{\begin{array}{l}i = \min\{j.\ \neg(\mathrm{is\_const}\,[e_1,\,...\,,e_n][j])\}\\ e = [e_1,\,...\,,e_n][i]\\ \mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e',\overline{\Phi})\\ [e'_1,\,...\,,e'_n] = (i \mapsto e')[e_1,\,...\,,e_n]\end{array}}{\mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{eStruct}\,\{f_1 = e_1;\,...\,;f_n = e_n\}) \rightsquigarrow (\mathbf{eStruct}\,\{f_1 = e'_1;\,...\,;f_n = e'_n\},\overline{\Phi})}\ \textsc{e\_eStruct}$$

$$\frac{\begin{array}{l}\mathrm{is\_consts}\ e_1,\,...\,,e_n\\ v_1,\,...\,,v_n = \mathrm{vl\_of\_el}\,(e_1,\,...\,,e_n)\end{array}}{\mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{eStruct}\,\{f_1 = e_1;\,...\,;f_n = e_n\}) \rightsquigarrow (\mathbf{struct}\,\{f_1 = v_1;\,...\,;f_n = v_n\},[\,])}\ \textsc{e\_eStruct\_to\_v}$$

$$\frac{\begin{array}{l}i = \min\{j.\ \neg(\mathrm{is\_const}\,[e_1,\,...\,,e_n][j])\}\\ e = [e_1,\,...\,,e_n][i]\\ \mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e',\overline{\Phi})\\ [e'_1,\,...\,,e'_n] = (i \mapsto e')[e_1,\,...\,,e_n]\end{array}}{\mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{eHeader}\,\mathit{boolv}\{f_1 = e_1;\,...\,;f_n = e_n\}) \rightsquigarrow (\mathbf{eHeader}\,\mathit{boolv}\{f_1 = e'_1;\,...\,;f_n = e'_n\},\overline{\Phi})}\ \textsc{e\_eHeader}$$

$$\frac{\begin{array}{l}\mathrm{is\_consts}\ e_1,\,...\,,e_n\\ v_1,\,...\,,v_n = \mathrm{vl\_of\_el}\,(e_1,\,...\,,e_n)\end{array}}{\mathit{ctx}\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\mathbf{eHeader}\,\mathit{boolv}\{f_1 = e_1;\,...\,;f_n = e_n\}) \rightsquigarrow (\mathbf{header}\,\mathit{boolv}\{f_1 = v_1;\,...\,;f_n = v_n\},[\,])}\ \textsc{e\_eHeader\_to\_v}$$

Access headers and structs

The E_S_ACC rule is used to access the values of fields in structs, and the E_H_ACC rule is similarly used for headers.

$$\frac{v = \textbf{struct}\,\{f_1 = v_1;\,...\,;f_n = v_n\}(f)}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\textbf{struct}\,\{f_1 = v_1;\,...\,;f_n = v_n\}.f) \rightsquigarrow (v, [\,])} \quad \text{E\_S\_ACC}$$

$$\frac{v = \textbf{header}\,boolv\{f_1 = v_1;\,...\,;f_n = v_n\}(f)}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\textbf{header}\,boolv\{f_1 = v_1;\,...\,;f_n = v_n\}.f) \rightsquigarrow (v, [\,])} \quad \text{E\_H\_ACC}$$

Select label

The E_SEL_ACC rule is used to match the given value v against the label-value list, in the case a match exists. If the match doesn't exist, then return the default label x.

$$\frac{x' = \{v_1 : x_1; ...; v_n : x_n; \_ : x\}(v)}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\textbf{select}\,v\{v_1 : x_1;\,...\,;v_n : x_n\}x) \rightsquigarrow (x', [\,])} \quad \text{E\_SEL\_ACC}$$

Bit slicing

This reduction gives a bitvector $bitv'''$ that is reduced from the slicing operation. It extracts a contiguous list from the original $bitv$ from the LSB $bitv$" to the MSB $bitv$'.

$$\frac{bitv''' = bitv[bitv' : bitv'']}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (bitv[bitv' : bitv'']) \rightsquigarrow (bitv''', [\,])} \quad \text{E\_SLICE\_V}$$

Concatenation

The reduction produces one bit string $bitv''$ that is the result of concatenating two bit strings $bitv$ and $bitv'$.

$$\frac{bitv'' = bitv +\!\!+ bitv'}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\textbf{concat}\,bitv\,bitv') \rightsquigarrow (bitv'', [\,])} \quad \text{E\_CONCAT\_V}$$

Unary and binary arithmetic operations

Unary and binary operations are basically standard operations on bit vectors, and are for this reason elided in this section.

2.2 Statement Semantics

The semantics of the statements are presented in this section[2]. Note that the statement semantics operates on single frames.

Assignment

The assignment can assign to *lval*s (shown in Figure 6), which can be either variables identified by their names, a null variable (used to model method calls) or struct fields, which are identified by the struct and field names, similar to the field access expression. Whenever an expression is assigned to an *lval*, that expression shall be reduced until it becomes a constant value. Then the appropriate scope in the current frame of execution will be updated with the mapping $x \mapsto v$. With appropriate we mean that the topmost (most recent) scope that the *lval* is declared in. The reduction results in the empty statement and an updated local or global scope lists. Note that this doesn't apply on **null** since it is used for method and action calls with no return values in mind.

$$\frac{\begin{array}{c}\overline{\gamma}' = (\overline{\gamma} + +\overline{\gamma_G})[lval \longmapsto v] \\ ((\overline{\gamma_G}', \overline{\gamma}'') = \text{separate}\overline{\gamma}')\end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([lval := v])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}', [([\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}''}], \mathbf{run})} \quad \text{STMT\_ASS\_V}$$

If-then-else

The STMT_COND2 and STMT_COND3 rules are the standard ones for conditional statements.

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\mathbf{if}\ \top\ \mathbf{then}\ stmt_1\ \mathbf{else}\ stmt_2])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([stmt_1])^{funn}_{\overline{\gamma}}], \mathbf{run})} \quad \text{STMT\_COND2}$$

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\mathbf{if}\ \bot\ \mathbf{then}\ stmt_1\ \mathbf{else}\ stmt_2])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([stmt_2])^{funn}_{\overline{\gamma}}], \mathbf{run})} \quad \text{STMT\_COND3}$$

Block

Once a block statement is encountered $\{\overline{decl}\ stmt\}$ the STMT_BLOCK_ENTER reduction will be used, which entails the $\overline{decl}$ being transformed and replicated into a scope that will be appended to the local $\overline{\gamma}$ of the frame, and then the body *stmt* of the block will be appended to the empty statement.

The STMT_BLOCK_EXIT rule is used in the case where the end of a block is reached, i.e. whenever a block contains only an empty statement: it pops the scope corresponding to the block (the most recent one) from the scope list $\overline{\gamma}$. The block will be exited and reduced to an empty statement $\emptyset_{\text{stmt}}$.

[2]Rules for reducing expressions in all contexts are found in Appendix B

The STMT_BLOCK_EXEC rule simply describes small-step reduction of the block contents. We also check if the previous list $\overline{stmt}$ is empty or not, if it is empty, then directly apply the other single block statement rules. It is also important to check that the head of the list $stmt :: \overline{stmt}$ is not empty statement $\emptyset_{\text{stmt}}$ otherwise it is non-deterministic with the block exit rule.

$$\frac{\begin{array}{l}\gamma = \text{replicate}(\overline{decl}) \\ \overline{\gamma}' = [\gamma] + +\overline{\gamma}\end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\{\overline{decl}\ stmt\}])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [(stmt :: [\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}'}], \textbf{run})} \text{ STMT\_BLOCK\_ENTER}$$

$$\frac{\begin{array}{l}\textbf{not\_empty}\ stmt \\ \textbf{not\_empty}\ \overrightarrow{stmt} \\ (apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [([stmt])^{funn}_{\overline{\gamma}}], t) \rightarrow (\gamma_A', \overline{\gamma_G}', \overline{\Phi}' +\!\!+ [(\overrightarrow{stmt'})^{funn}_{\overline{\gamma}'}], t')\end{array}}{(apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [(stmt :: \overrightarrow{stmt})^{funn}_{\overline{\gamma}}], t) \rightarrow (\gamma_A', \overline{\gamma_G}', \overline{\Phi}' +\!\!+ [(\overrightarrow{stmt'} + +\overrightarrow{stmt})^{funn}_{\overline{\gamma}'}], t')} \text{ STMT\_BLO}$$

$$\frac{\begin{array}{l}\textbf{not\_empty}\ \overrightarrow{stmt} \\ \overline{\gamma}' = \text{tl}\overline{\gamma}\end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [(\emptyset_{\text{stmt}} :: \overrightarrow{stmt})^{funn}_{\overline{\gamma}}], t) \rightarrow (\gamma_A, \overline{\gamma_G}, [(\overrightarrow{stmt})^{funn}_{\overline{\gamma}'}], t)} \text{ STMT\_BLOCK\_EXIT}$$

Apply

The STMT_APPLY_V describes the apply table statement. Note that this is particular to our formalization: it is not a statement in the P4 specification, but a method. Each apply statement has a table name *tbl* with the a list of key expressions $e_1, \ldots, e_n$ to match on. This list has been previously reduced to constants one at a time in the rule STMT_APPLY_E. The Tb will return a list of match kinds $mk_1, \ldots, mk_n$, which is then used with *apply_table* to perform the actual table matching.

Return

Once return's expression is reduced to a constant value, the status is changed to a **ret** v, and the statement becomes $\emptyset_{\text{stmt}}$. The rest of the return operation will be handled in the sequence rule and frame-level semantics.

Sequence

The sequential statements rules STMT_SEQ1 and STMT_SEQ2 are standard. The status t must be **run** to start with. The part that is different is that if any new frame being created by any function call or a statement added to the statement list, it will be added on top of the frame list.

Otherwise, the STMT_SEQ3 rule is used whenever the status is **ret** , or **tra** to indicate either a a transition to a parser state or a return from a function call. The rest of the sequential composition statements are not considered, this will give flexibility to the return or transition statements in the

$$\frac{\begin{array}{l} i = \min\{j.\neg(\text{is\_const}\,[e_1,\,..\,,e_n][j])\} \\ e = [e_1,\,..\,,e_n][i] \\ ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi}) \\ [e_1',\,..\,,e_n'] = (i \mapsto e')[e_1,\,..\,,e_n] \end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{apply}\,tbl(e_1,\,..\,,e_n)])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([\textbf{apply}\,tbl(e_1',\,..\,,e_n')])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_APPLY\_TAI}$$

$$\frac{\begin{array}{l} \text{is\_consts}\ e_1,\,..\,,e_n \\ \text{Tb}\,tbl\ =\ ([mk_1,\,..\,,mk_n], (f', [e_1',\,..\,,e_o'])) \\ apply\_table\,(tbl,\,(e_1,\,..\,,e_n),\,([mk_1,\,..\,,mk_n]), (f', [e_1',\,..\,,e_o']),\,\gamma_A\,) =\,(f, (v_1,\,..\,,v_m)) \end{array}}{(apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{apply}\,tbl(e_1,\,..\,,e_n)])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([\textbf{null} := (\textbf{call}\,f(v_1,\,..\,,v_m))])^{fun}_{\overline{\gamma}}}$$

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{return}\,v])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}}], \textbf{ret}\ v)}\ \text{STMT\_RET\_V}$$

body rather than only at the end. STMT_SEQ1 and STMT_SEQ3 are able to change the tables that are populated by the control plane.

$$\frac{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([stmt_1])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A', \overline{\gamma_G}', \overline{\Phi} +\!\!+ [(\overrightarrow{stmt'} + +[stmt_1'])^{funn}_{\overline{\gamma}'}], \textbf{run})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([stmt_1; stmt_2])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A', \overline{\gamma_G}', \overline{\Phi} +\!\!+ [(\overrightarrow{stmt'} + +[stmt_1'; stmt_2])^{funn}_{\overline{\gamma}'}], \textbf{run})}\ \text{STMT\_SEQ1}$$

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\emptyset_{\text{stmt}}; stmt])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([stmt])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_SEQ2}$$

$$\frac{\begin{array}{l} ctx \vdash (\gamma_A, \overline{\gamma_G}, [([stmt_1])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A', \overline{\gamma_G}', [([stmt_1'])^{funn}_{\overline{\gamma}'}], t) \\ t \neq \textbf{run} \end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([stmt_1; stmt_2])^{funn}_{\overline{\gamma}}], \textbf{run}) \rightarrow (\gamma_A', \overline{\gamma_G}', [([stmt_1'])^{funn}_{\overline{\gamma}'}], t)}\ \text{STMT\_SEQ3}$$

Extern

The symbol ■ represents a statement capturing the semantics of an extern function other than copy-in, copy-out and return behaviour. ■ is able to modify the architectural state, the local scope list $\overline{\gamma}$ and the execution status (which is always set to **ret** v). The exact behaviour is determined by looking up the entry of the name *funn* associated with the current frame in the extern function map X: since ■ is used in extern function call bodies, *funn* is the name of the extern function.

Note that calling an extern function works the same as calling any other function, as described in the function call subsection of Section 2.1. However, by convention the body of the extern function

consists only of ■.

$$\frac{\begin{array}{c} ext\_fun = \text{lookup\_ext\_fun}(funn, X) \\ (\gamma_A{}', \overline{\gamma}', v) = ext\_fun\ (\gamma_A, \overline{\gamma_G}, \overline{\gamma}) \end{array}}{(apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [([\blacksquare])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A{}', \overline{\gamma_G}, [([\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}'}], \mathbf{ret}\ v)}\ \text{STMT\_EXT}$$

Transition

The transition statement **transition** x, whose semantics is captured by the STMT_TRANS rule, makes a change to the state's status t based on the state name x.

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\mathbf{transition}\, x])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}}], \mathbf{tra}\ x)}\ \text{STMT\_TRANS}$$

Verify

The **verify** $e\, e'$ statement is used to check the whether the boolean expression e holds; if it does, then nothing happens, as in the STMT_VERIFY_3 rule. Otherwise, it assigns the error in e' to "*parseError*" and reduces the statement to a **transition** statement to the state 'reject".

$$\frac{}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\mathbf{verify}\ \top\ (\mathbf{errmsg}\, x)])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([\emptyset_{\text{stmt}}])^{funn}_{\overline{\gamma}}], \mathbf{run})}\ \text{STMT\_VERIFY\_3}$$

$$\frac{\begin{array}{c} x' = \text{“}parseError\text{”} \\ x'' = \text{“}reject\text{”} \end{array}}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\mathbf{verify}\ \bot\ (\mathbf{errmsg}\, x)])^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A, \overline{\gamma_G}, [([x' := (\mathbf{errmsg}\, x); \mathbf{transition}\, x''])^{funn}_{\overline{\gamma}}], \mathbf{run})}\ \text{STMT\_VE}$$

2.3 Frame-Level Semantics

The previous semantics operate on a single frame for a list of statements, however when a function being called, then it means that the state will contain two frames. The top frame that will be executed as can be seen in FRAMES_COMP1 reduction, where the previous frame Φ is not empty (otherwise, we can use the previous rules above).

The rule FRAMES_COMP2 is used specifically whenever there is a return occuring in a frame in that is being reduced. Here the the global scope list $\overline{\gamma}_G$ must contain a **var**(**star**, $funn$) declared for every function $funn$. This variable should be updated with the value v that is found in the state's status **ret** v. The copy out function takes the callee function signature, the "possibly updated"

global scope list (index 0 or 1 from depends on the location of $\mathbf{var}(\mathbf{star}, funn)$), the top most scope in the $\overline{\gamma}''$ and the callee's current scope list $\overline{\gamma}$. It returns a new updated scopes list for both the global and caller's frame.

In the copyout function, each parameter with (out or inout directions) should be copied out to the variable name it is mapping to. i.e. the mapping of a single scope looks as $x \mapsto (v, y)$ so for each variable name x that is part of the current argument list in the signature we will check the direction of it, if the direction is (none or in) then we do not copy them out. However, if the direction is (out or inout) we will look into the mapping of it, and retrive a tuple (v, y) which is the value and the original argument of the function to be copied out in the poroper scope (top most one it is defined in).

$$\frac{\begin{array}{l}\overline{\gamma_G}' = \text{scopes\_to\_pass}(funn, F_g, F_b, \overline{\gamma_G}) \\ (apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}', [(\overrightarrow{stmt})^{funn}_{\overline{\gamma}}], t) \rightarrow (\gamma_A', \overline{\gamma_G}'', \overline{\Phi}', t') \\ \overline{\Phi}'' \neq [] \Rightarrow t' \neq \mathbf{ret\ v} \\ \overline{\gamma_G}''' = \text{scopes\_to\_retrieve}(funn, F_g, F_b, \overline{\gamma_G}, \overline{\gamma_G}'')\end{array}}{(apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [(\overrightarrow{stmt})^{funn}_{\overline{\gamma}}] +\!\!+ \overline{\Phi}'', t) \longrightarrow_{\Phi} (\gamma_A', \overline{\gamma_G}''', \overline{\Phi}' +\!\!+ \overline{\Phi}'', t')} \text{ FRAMES\_COMP1}$$

$$\frac{\begin{array}{l}\overline{\gamma_G}' = \text{scopes\_to\_pass}(funn, F_g, F_b, \overline{\gamma_G}) \\ (apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}', [(\overrightarrow{stmt})^{funn}_{\overline{\gamma}}], \mathbf{run}) \rightarrow (\gamma_A', \overline{\gamma_G}'', [(\overrightarrow{stmt''})^{funn}_{\overline{\gamma}''}], \mathbf{ret}\ v) \\ \overline{\gamma_G}''' = (\overline{\gamma_G}'')[(\mathbf{star}, funn) \longmapsto v] \\ (stmt''', [(x_1, d_1), .., (x_n, d_n)]) = \mathbf{lookup\_funn\_sig\_body}\ (funn, F_g, F_b, X) \\ \overline{\gamma_G}'''' = \text{scopes\_to\_retrieve}(funn, F_g, F_b, \overline{\gamma_G}, \overline{\gamma_G}''') \\ (\overline{\gamma_G}''''', \overline{\gamma}''') = \text{copyout}\ ([x1, .., xn], [d1, .., dn], \overrightarrow{\gamma_G}'', \overrightarrow{\gamma}', \overrightarrow{\gamma})\end{array}}{(apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, [(\overrightarrow{stmt})^{funn}_{\overline{\gamma}}] +\!\!+ [(\overrightarrow{stmt'})^{funn'}_{\overline{\gamma}'}] +\!\!+ \overline{\Phi}, \mathbf{run}) \longrightarrow_{\Phi} (\gamma_A', \overline{\gamma_G}''''', [(\overrightarrow{stmt'})^{funn'}_{\overline{\gamma}'''}] +\!\!+ \overline{\Phi}, \mathbf{run})}$$

We define scopes_to_pass $(funn, F_g, F_b, \overrightarrow{\gamma_G})$ as :

$$\overrightarrow{\gamma_G}' = \begin{cases} \text{if } funn \in dom(F_g) & \text{, then } [\emptyset_\gamma; \overrightarrow{\gamma_G}[1]] \\ \text{otherwise} & \text{, then } \overrightarrow{\gamma_G} \end{cases}$$

Where $\overrightarrow{\gamma_G}$ is a list of two elements, index 1 is the global scope, and index 0 is the programmable block global scope, it is fetched from the frame reduction rule and considered to be the initial global scope list. $\overrightarrow{\gamma_G}'$ is the scope that will be used to implement one frame at a time (statement reduction) in FRAMES_COMP1.

We define scopes_to_retrieve $(funn, F_g, F_b, \overrightarrow{\gamma_G}, \overrightarrow{\gamma_G}')$ as :

$$\overrightarrow{\gamma_G}'' = \begin{cases} \text{if } funn \in dom(F_g) & \text{, then } [\overrightarrow{\gamma_G}[0]; \overrightarrow{\gamma_G}'[1]] \\ \text{otherwise} & \text{, then } \overrightarrow{\gamma_G}' \end{cases}$$

Where $\overrightarrow{\gamma_G}''$ is a list of two elements, index 1 is the global scope, and index 0 is the programmable block global scope, and we will retrieve it to be added as the resulted scope of the frame reduction.

$\overrightarrow{\gamma_G}'$ is the scope that is resulted from the statement reduction. $\overrightarrow{\gamma_G}$ is the original (initial) starting state's global list of the frame reduction.

2.4 Architecture-Level Semantics

The architecture-level semantics is the topmost-level semantics, describing the entirety of the P4 pipeline from input packets to output packets, and it uses the frame semantics for reduction steps inside programmable blocks. The judgment form, shown at the top of Figure 8, consists of multiple components: starting from the left, an *architectural context* ctx_A (which contains the static componenents not changed by reduction steps) on the left-hand side of the turnstile, which contains the following:

1. The *architectural block list* $\overline{ab}$: an architectural block represents a stage of packet processing. There are four fundamental stages of packet processing in a P4-compatible architecture. First, there are the input (**inp**) and output (**out**) stages: these stages just perform translation between the architectural packet format and the generic I/O format (consisting of a list of ports, each with pending packets to be arbitrated/sent off)[3]. Second, there are the programmable blocks (parser blocks and control blocks) and the fixed-function block stages. Fixed-function blocks, like their name implies, perform the parts of packet processing in the P4-programmable network element that are actually not P4-programmable.

2. The *programmable block map* B_p, which is a partial map between names of programmable block names (strings) and the all necessary items that model the block in question. This is the block type (parser or control), the list of directed parameters, the block-local function map containing function declared inside the block, a list of declarations of variables done at a block-global level, a statement representing initialisations and instantiations of these block-global variables followed by the body (for parsers, a transition statement pointing to "start", for control blocks the content of the apply statement encased in a block), and the parser state map P between parser state names and their bodies (statements)[4] and a table map Tb between names of tables and tuples of expressions and matching kinds. Note that the parser state map is empty for control blocks, as is the table map for parser blocks.

3. The *fixed-function block map* B_{ff}, which is a partial map between names of fixed-function blocks to the implementation of the fixed function itself, which is a partial function that maps the architectural scope to an updated architectural scope.

4. The *input function* f_{in} and the *output function* f_{out}, which are both partial functions from an IO list and the architectural scope to an updated IO list and architectural scope. They are used in the input and output stages.

5. The *programmable block copy-in function* $copyin_{pbl}$ and the *programmable block copy-out function* $copyout_{pbl}$: $copyin_{pbl}$ is a partial function from a list of directed parameters, a list of expression arguments, the architectural scope and the block type to a scope (the block-global scope of the programmable block). $copyout_{pbl}$ is a partial function from the global scopes

[3] The demux block functionality may be modeled as part of the output stage, or it may be its own fixed-function block preceding the output stage

[4] Note that `HOL4P4` represents all parser state bodies as encased in a block by convention

list, a list of directed parameters, the architectural scope, the block type and status to an updated architectural scope. Note that these functions are responsible for the copy-in copy-out behaviour of the *parseError* variable in parser blocks.

6. The *extern object map* X, which is a partial map from extern object names to tuples of extern function maps (a map holding the extern functions of the object: tuples of directed parameter lists, function bodies, and the extern semantics), and an optional constructor (holding a tuple same as that of the extern function map).

7. The *function map* F, which is a partial map from globally-declared function names to tuples of function bodies (statements) and their directed parameter lists.

The states on the left-hand and right-hand sides of the reduction both have the same elements.

1. The *architectural environment* env_A, which in turn has four components:

   (a) The *architectural block index*: This is an index which informs us of which architectural block in $\overline{ab}$ is currently being reduced.

   (b) The *input list*, which is a list of incoming packets (represented as tuples of lists of Booleans and numbers signifying input ports)

   (c) The *output list*, which is the same as the input list, but used for output.

   (d) The *architectural scope* γ_A, which is of polymorphic type, and is used for storing things in-between the programmable blocks, as well as things that are not accessible directly by P4 code.

2. The global scope list $\overline{\gamma_G}$, which contains the top-level global scope with constants common to all programmable blocks as well as the block-global scope containing variables declared at the start of progrmamable blocks.

3. The *architecture-level frame list*: this contains either a regular frame list (as described in the statement semantics), or it is a special empty architecture-level frame list ($[\,]_A$).

4. The control-plane configuration C, a partial function from strings, values and match kinds to tuples of strings and expression lists.

5. The status, which informs us of whether a parser state machine is finished, or the apply of a control block is finished.

The rules of the architecture-level semantics are the following:

1. ARCH_IN: The first antecedent requires that the pending architecture block is **inp**, and then f_{in} updates the input list and the architectural scope.

2. ARCH_PBL_INIT: when the pending architecture block is a programmable block, a new block-global scope γ' is created and initialised with the arguments of the programmable block (in the case of a parser block, *parseError* is also initially set to *NoError*). After this, the variables in the list of declarations are declared in γ'. The final result γ''' is appended to the top-level global scope $\overline{\gamma_G}[0]$, forming a new global scopes list $\overline{\gamma_G}'$. Also, the empty architecture frame list is changed to a single frame where the singleton statement list contains the initialisations

of the parser block *stmt* followed by the body of the programmable block[5], the scopes stack contains a single empty scope and the current function name is the name of the programmable block.

3. ARCH_FFBL handles the fixed-function block: when the pending architecture block is a fixed-function block with name x, the implementation ff of the fixed-function is looked-up in B_{ff} using x, after which it is used to update the architectural scope. Also, the architecture block index is incremented.

4. ARCH_OUT: Similar to the above, but the pending architecture block must be **out**, and then the output list and the architectural scope are updated by f_{out}.

5. ARCH_PARSER_TRANS: In case the block at the block index i is a parser block and the current status is **tra** x', this rule will obtain the parser state body $stmt'$ of $P(x')$ (where P is the parser state map of the current parser block), and set the next frame to the singleton list of $stmt'$ with $[\gamma_\emptyset]$ as the scope stack and x' as the current function name, as well as set the status to **run**.

6. ARCH_PBL_EXEC describes a reduction step inside a programmable block: the first two premises are there to obtain the content of the statement semantics context. Then, the global block list, the frame list, the control plane configuration and the status are updated by a statement reduction step $\longrightarrow$.

7. ARCH_PBL_RET rule describes the final step of programmable block reduction that reduces to an empty frame list. The first two premises obtain the directed parameters of the block. If *state_fin* (termination conditions of the two programmable blocks) holds of the status and frame list (if status was **run**, it is then set to **tra** "*reject*" if we are in a parser block). The block output function out_p proceeds to update the architectural scope (notably dependent on architecture, it copies out the value of *parseError*). Furthermore, the architecture block list index is incremented by 1 and the block-global scope is dropped from the global scopes list.

[5]Conventions for how these are represented are mentioned in the explanation of B_p

$\boxed{ctx_A \vdash s_A \longrightarrow_A s_A'}$ architecture-level semantics

$$\frac{\begin{array}{l}\mathbf{inp} = \overline{ab}[i] \\ (\overline{io}'', \gamma_A') = in_A(\overline{io}, \gamma_A)\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, [\,]_A, \mathbf{run}) \longrightarrow_A ((i+1, \overline{io}'', \overline{io}', \gamma_A'), \overline{\gamma_G}, [\,]_A, \mathbf{run})} \text{ ARCH\_IN}$$

$$\frac{\begin{array}{l}\mathbf{pbl}\, f(e_1, .., e_n) = \overline{ab}[i] \\ pbl\_type((x_1, d_1), .., (x_n, d_n)) F_b\, \overline{decl}\; stmt\; P\; Tb = B_p(f) \\ \gamma' = in_p((x_1, .., x_n), [d_1, .., d_n], [e_1, .., e_n], \gamma_A, pbl\_type) \\ \gamma'' = \mathrm{replicate}(\overline{decl}, \gamma') \\ \overline{\gamma_G}' = \mathrm{lastn}(1, \overline{\gamma_G}) \\ \overline{\gamma_G}'' = [\gamma''] + + \overline{\gamma_G}' \\ \overline{\gamma_G}''' = \mathrm{initialise\_var\_stars}(F_g, F_b, X, \overline{\gamma_G}'')\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, [\,]_A, \mathbf{run}) \longrightarrow_A ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}''', [([stmt])^f_{[\gamma\emptyset]}], \mathbf{run})} \text{ ARCH\_PBL\_INIT}$$

$$\frac{\begin{array}{l}\mathbf{ffbl}\, x = \overline{ab}[i] \\ \mathit{ff} = B_{\mathrm{ff}}(x) \\ \gamma_A' = \mathit{ff}(\gamma_A)\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, [\,]_A, \mathbf{run}) \longrightarrow_A ((i+1, \overline{io}, \overline{io}', \gamma_A'), \overline{\gamma_G}, [\,]_A, \mathbf{run})} \text{ ARCH\_FFBL}$$

$$\frac{\begin{array}{l}\mathbf{out} = \overline{ab}[i] \\ (\overline{io}'', \gamma_A') = out_A(\overline{io}', \gamma_A)\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, [\,]_A, \mathbf{run}) \longrightarrow_A ((0, \overline{io}, \overline{io}'', \gamma_A'), \overline{\gamma_G}, [\,]_A, \mathbf{run})} \text{ ARCH\_OUT}$$

$$\frac{\begin{array}{l}\mathbf{pbl}\, x(e_1, .., e_n) = \overline{ab}[i] \\ \mathbf{parser}((x_1, d_1), .., (x_n, d_n)) F_b\, \overline{decl}\; stmt\; P\; Tb = B_p(x) \\ \mathrm{not\_final\_state}(x') \\ stmt' = P(x')\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, \overline{\Phi}, \mathbf{tra}\; x') \longrightarrow_A ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}', [([stmt'])^{x'}_{[\gamma\emptyset]}], \mathbf{run})} \text{ ARCH\_PARSER\_TRAN}$$

$$\frac{\begin{array}{l}\mathbf{pbl}\, x(e_1, .., e_n) = \overline{ab}[i] \\ pbl\_type((x_1, d_1), .., (x_n, d_n)) F_b\, \overline{decl}\; stmt\; P\; Tb = B_p(x) \\ (apply\_table, X, F_g, F_b, P, Tb) \vdash (\gamma_A, \overline{\gamma_G}, \overline{\Phi}, \mathbf{run}) \longrightarrow_\Phi (\gamma_A', \overline{\gamma_G}', \overline{\Phi}', t')\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, \overline{\Phi}, \mathbf{run}) \longrightarrow_A ((i, \overline{io}, \overline{io}', \gamma_A'), \overline{\gamma_G}', \overline{\Phi}', t')} \text{ ARCH\_PBL\_EXEC}$$

$$\frac{\begin{array}{l}\mathbf{pbl}\, f(e_1, .., e_n) = \overline{ab}[i] \\ pbl\_type((x_1, d_1), .., (x_n, d_n)) F_b\, \overline{decl}\; stmt\; P\; Tb = B_p(f) \\ \mathrm{state\_fin}(t, \overline{\Phi}) \\ t' = \mathrm{set\_fin\_status}(pbl\_type, t) \\ \gamma_A' = out_p(\overline{\gamma_G}, \gamma_A, [d_1, .., d_n], (x_1, .., x_n), pbl\_type, t')\end{array}}{(\overline{ab}, B_p, B_{\mathrm{ff}}, in_A, out_A, in_p, out_p, apply\_table, X, F_g) \vdash ((i, \overline{io}, \overline{io}', \gamma_A), \overline{\gamma_G}, \overline{\Phi}, t) \longrightarrow_A ((i+1, \overline{io}, \overline{io}', \gamma_A'), \mathrm{lastn}(1, \overline{\gamma_G}), [\,]_A, \mathbf{run})} \text{ ARCH\_PBL\_RET}$$

Figure 8: Architecture-Level Semantics

A Concrete Syntax of Operations

$\ominus$	::=		
	|	!	negation
	|	¬	bitwise complement
	|	−	signed negation
	|	+	unary plus

Figure 9: P4 Unary Operations

The unary expressions included are shown in Figure 9. These include all of the unary operations in P4. Boolean negation is only defined on Booleans, the other operations have their standard meanings (note that unary plus is a no-op).

$\oplus$	::=		
	|	$\times$	multiplication
	|	/	division
	|	mod	modulo
	|	$+$	addition
	|	$-$	subtraction
	|	$\ll$	logical left-shift
	|	$\gg$	logical right-shift
	|	$\leq$	less or equal
	|	$\geq$	greater or equal
	|	$<$	less
	|	$>$	greater
	|	$\neq$	not equal
	|	$=$	equal
	|	&	bitwise and
	|	$\underline{\vee}$	bitwise xor
	|	|	bitwise or
	|	$\wedge$	binary and
	|	$\vee$	binary or

Figure 10: P4 Binary Operations

The binary expressions included are shown in Figure 9. These include all of the binary operations in P4.

B Semantics of Expression Reduction

This appendix describes semantics for reducing expressions in certain contexts. The expression semantics are shown in Figure 11. The statement semantics are shown in Figure 12.

The E_FUNC_CALL_ARGS rule reduces the leftmost function argument which has yet to be reduced to a constant with one expression evaluation step. The first two antecedents divide the list of arguments into two sub-lists, where the prefix must contain all constants. The head of the suffix is then reduced with one step, after which the corresponding index in the original list of arguments is update with the resulting expression.

8.1 of the P4 specification states that expressions are evaluated left-to-right. Accordingly, the rules for binary operations - E_BINOP1 and E_BINOP2 - are split up so that reduction of the second operand requires that the first operand has been completely reduced to a constant. This is trivial for unary operations (E_UNOP).

References

[1] Ryan Doenges et al. "Petr4: formal foundations for p4 data planes". In: *Proceedings of the ACM on Programming Languages* 5.POPL (2021), pp. 1–32.

$\boxed{[e](\sigma) \rightsquigarrow [e'](\sigma')}$ expression semantics

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\textbf{select}\ e\{v_1 : x_1;\ \ldots;\ v_n : x_n\}x) \rightsquigarrow (\textbf{select}\ e'\{v_1 : x_1;\ \ldots;\ v_n : x_n\}x, \overline{\Phi})}\ \text{E\_SEL\_ARG}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (\ominus e) \rightsquigarrow (\ominus e', \overline{\Phi})}\ \text{E\_UNOP\_ARG}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e'', \overline{\Phi})}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e \oplus e') \rightsquigarrow (e'' \oplus e', \overline{\Phi})}\ \text{E\_BINOP\_ARG1}$$

$$\frac{\text{is\_short\_circuit}(\oplus) \quad ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (v \oplus e) \rightsquigarrow (v \oplus e', \overline{\Phi})}\ \text{E\_BINOP\_ARG2}$$

Figure 11: Expression Reduction-of-Argument Semantics

$\boxed{[stmt]s \to [stmt']s'}$ statement semantics

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{return}\ e])^{funn}_{\overline{\gamma}}], \textbf{run}) \to (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([\textbf{return}\ e'])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_RET\_E}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([lval := e])^{funn}_{\overline{\gamma}}], \textbf{run}) \to (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([lval := e'])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_ASS\_E}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{if}\ e\ \textbf{then}\ stmt_1\ \textbf{else}\ stmt_2])^{funn}_{\overline{\gamma}}], \textbf{run}) \to (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([\textbf{if}\ e'\ \textbf{then}\ stmt_1\ \textbf{else}\ stmt_2])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e'', \overline{\Phi})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{verify}\ e\ e'])^{funn}_{\overline{\gamma}}], \textbf{run}) \to (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([\textbf{verify}\ e''\ e'])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_VERIFY\_E1}$$

$$\frac{ctx\,\overline{\gamma_G}\,\overline{\gamma} \vdash (e) \rightsquigarrow (e', \overline{\Phi})}{ctx \vdash (\gamma_A, \overline{\gamma_G}, [([\textbf{verify}\ b\ e])^{funn}_{\overline{\gamma}}], \textbf{run}) \to (\gamma_A, \overline{\gamma_G}, \overline{\Phi} +\!\!+ [([\textbf{verify}\ b\ e'])^{funn}_{\overline{\gamma}}], \textbf{run})}\ \text{STMT\_VERIFY\_E2}$$

Figure 12: Statement Reduction-of-Argument Semantics