The Hume Report, Version 1.1

Kevin Hammond[1] Greg Michaelson[2]
Robert Pointon[2]

[1]School of Computer Science, University of St Andrews
kh@dcs.st-and.ac.uk, +44 1334 463241

[2]School of Mathematical and Computer Sciences
Heriot-Watt University
greg@macs.hw.ac.uk, +44 131 451 3422

Contents

David Hume, Scottish Sceptical Philosopher: 1711-1776

Chapter 1

Introduction

This document describes the Hume programming language. *Hume* (Higher-order Unified Meta-Environment) is a strongly typed, functionally-based language with an integrated tool set for developing, proving and assessing concurrent, resource-limited systems, such as embedded or safety-critical systems. It aims to extend the frontiers of language design for such systems, introducing new levels of abstraction and provability.

Hume is named for the Scottish Enlightenment sceptical philosopher David Hume (1711-1776), who counselled that:

> *To begin with clear and self-evident principles, to advance by timorous and sure steps, to review frequently our conclusions, and examine accurately all their consequences; though by these means we shall make both a slow and a short progress in our systems; are the only methods, by which we can ever hope to reach truth, and attain a proper stability and certainty in our determinations.*
> D. Hume, An Enquiry Concerning Human Understanding, 1748

These sentiments epitomise the philosophy of programming language design that has been followed in this document.

This report is structured as follows: the remainder of this chapter provides motivation and general background; Chapter 2 is an overview of the Hume language design, including detailed informal descriptions of the process and coordination sub-languages; future chapters will cover implementation and cost modelling. Appendix A describes the concrete syntax; Appendix B is the formal static semantics, including the type system and Appendix C gives the formal dynamic semantics. Finally Appendix D defines the Hume standard prelude.

1.1 Motivation and objectives

Since the focus of the Hume design is on dependable applications (such as safety critical or embedded systems), it is paramount that Hume programs have predictable and, preferably, provable properties. However, the strong properties of program equivalence, termination and time and space use are undecidable for Turing computable languages. Conversely, languages in which such properties are decidable (i.e. finite state machines) lack expressiveness. The goal of the Hume language design is to support a high level of expressive power, whilst providing strong guarantees of dynamic behavioural properties such as execution time and space usage.

Program proof and manipulation are greatly eased by abstractness as well as by succinctness. In particular, it is relatively hard to construct formal theories for imperative language constructs, where time ordering greatly complicates reasoning about programs. However, programs are ultimately intended to realise solutions to concrete problems on physical computers. Increased abstractness in languages, in particular away from modifiable state, tends to greater distance from the von Neumann paradigm, with corresponding complications and efficiency losses in implementations. The Hume design combines the desirable properties of abstraction and succinctness that are provided by a good functional programming language with a coordination language that explicitly captures time and space behaviour. Runtime efficiency is maintained through careful language design with a view to straightforward implementation on conventional computer architectures or embedded systems.

Where formal theories can be constructed, their static application to non-trivial programs is characterised by poor scalability through exponential growth in the space of properties to be explored. Alternatively, accuracy is lost through simplifying assumptions and heuristics. Dynamic evaluation of programs through instrumentation and profiling suffers from similar limitations. Typically, the volume of test data and the time required for exhaustive empirical exploration of program behaviour is prohibitive, both growing rapidly with the fineness of granularity at which exploration is conducted. Contrariwise, accuracy is lost at coarser granularity or with non-exhaustive testing.

Hume reflects these considerations in:

- the separation of the *expression* and *coordination* aspects of the language;
- the provision of an integrated *tool set*, spanning both static and dynamic program analysis and manipulation.

1.1.1 Key Design Characteristics

In general, dependable systems must meet both strong correctness criteria and strict performance criteria. The latter are most easily attained by working at a low level, whereas the former are most easily attained by working at a high level. A primary objective of the Hume design is to allow both types of criteria to be met while working at a high level of abstraction. Hume has also been designed to allow relatively simple formal cost models to be developed, capable of costing various metrics including space and time bounds. This is reflected in the design of both the coordination and expression aspects of the language.

Both system level and process level exceptions are supported, including the ability to set timeouts for expression computations. Exceptions may be raised from within the expression language but can only be handled by the process language. This reduces the cost of handling exceptions and maintains a pure expression language, as well as simplifying the expression cost calculus.

A radical design decision for high reliability systems is the use of automatic memory management techniques. Automatic memory management has the advantage of reducing errors due to poor manual management of memory. The disadvantage lies in terms of excessive time or space usage.

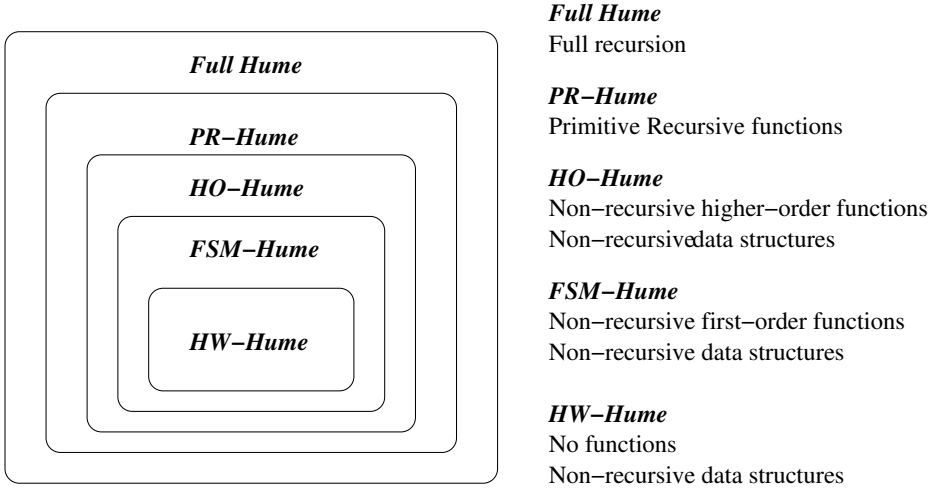

Figure 1.1: Expressibility versus Costability in the Hume Design

Hume implementations use static analysis tools to limit space usage, and exploit new bounded-time memory management techniques [26].

1.2 Language Structure

We define three distinct layers in Hume. The outermost, static, *declaration layer* provides definitions of types, streams, exceptions etc. to be used in the dynamic layers. The innermost *expression* layer is used to define values and (potentially higher-order) functions. Finally, the middle *coordination layer* links functions into possibly concurrent processes. Each of these layers is described below.

1.2.1 Hume Levels

Rather than attempting to apply cost modelling and correctness proving technology to an existing language framework either directly or by altering the language to a greater or lesser extent (as with e.g. RTSj [10]), our approach is to design Hume in such a way that we are certain that formal models and proofs can be constructed. We identify a series of overlapping Hume language levels shown in Figure 1.1, where each level adds expressibility to the expression semantics, but either loses some desirable behavioural property or increases the technical difficulty of providing formal correctness/cost models. These levels are:

HW-Hume: a hardware description language — capable of describing both synchronous and asynchronous hardware circuits, with pattern matching on tuples of bits, but with no other data types or operations [27];

FSM-Hume: a hardware/software language — HW-Hume plus first-order functions, conditionals expressions and local definitions [26];

Template-Hume: a language for template-based programmimng — FSM-Hume plus predefined higher-order functions, polymorphism and inductive data structures, but no user-defined higher-order functions or recursive function definitions;

PR-Hume: a language with decidable termination — Template-Hume plus user-defined primitive recursive and higher-order functions, and inductive data structure definitions;

Full-Hume: a Turing-complete language — PR-Hume plus unrestricted recursion in both functions and data structures.

A fuller description of these levels, including a description of how it is possible to transform programs from one level to another, can be found elsewhere [24].

1.2.2 The Hume Expression Layer

Hume *expressions* are defined using a purely functional, (possibly recursive) notation with a strict semantics. Expressions are built into single, one-shot, non-reentrant processes through coordination layer constructs, and have statically provable properties of:

1. *determinism*;
2. *termination*; and
3. *bounded time and space behaviour.*

This is achieved through appropriate type systems and formal semantics (see Appendices B and C).

Note that the expression notation has no concept of external, imperative state. Such state considerations are encapsulated entirely within the coordination layer.

1.2.3 The Hume Coordination Layer

The Hume *coordination layer* is a finite state notation for the description of multiple, interacting, re-entrant processes built from expressions defined in the purely functional expression layer. The coordination notation is designed to have statically provable properties that include both *process equivalence* and *safety* properties such as the absence of deadlock, livelock or resource starvation. Definitions in the coordination layer also inherit properties from exception expressions that are embedded within it.

The basic unit of coordination is the *box*, an abstract notion of a process that specifies the links between its input and output channels in terms of functional patterns and expressions, and which provides exception handling facilities including timeouts and system exceptions The coordination layer is responsible for interaction with external, imperative state through streams and ports that are ultimately connected to external devices. Boxes and external input/output devices are *wired* into a static process network.

1.3 The Hume Research Programme

In version 0.1 of the Hume report from November 2000, we laid out a long-term programme of basic research and tool development that would be needed to establish Hume as a viable research platform.

Support Tools We envisaged the construction of a number of tools to support Hume programmers. By *tools* we understand formal definitions and calculi, as well as software language processors such as compilers, interpreters, type checkers etc. The tools we intended to produce were:

- the Hume language definition: syntax, types and semantics;

- the Hume abstract machine(HAM)/abstract machine code(HAMC): syntax, types and semantics;
- a compiler from Hume source → HAMC supporting separate compilation;
- a compiler from HAMC → native assembler code.

The Hume language semantics tools were intended to comprise:

operational semantics — reference interpreter;
axiomatic semantics — correctness prover;
termination semantics — termination prover;
specification notation — refinement calculus;
rule checker — literate specification;
cost calculus — cost analyser;
transformation system.

The abstract machine tools comprised:

- the interpreter including a profiler and instrumentor;
- a transformation system.

The HAMC to native assembly code tools included: the run-time system; a profiler; and an instrumentor.

The Hume Research Programme Our intention was for the Hume design to proceed in a series of planned stages.

Our first priorities were:

- the core language definition - syntax, types & type system, and operational semantics;
- a reference interpreter;
- a set of reference Hume programs.

We then aimed to develop the HAM/HAMC formal definition a HAMC interpreter, and a Hume → HAMC compiler, using the reference programs to ensure behavioural consistency with the reference interpreter.

Finally, we intended to consider the cost/termination calculi systems; the profiler/instrumentor; and the program transformer; and to use them to analyse the reference program set.

We envisaged native code compilation, proof, specification, and refinement as longer term objectives.

We saw proof of formal properties of language processing tools as central to the success of this this programme, notably,

1. consistency with the Hume definition;
2. preservation of the meaning and behaviour of Hume programs.

1.3.1 Status of the Research

As of November 2006, we have constructed the core Hume language definition, a reference interpreter, an abstract machine interpreter, a native code compiler and a set of reference programs.

We have provided a static semantics for types and an axiomatic dynamic semantics (both included in this definition), plus an operational semantics reflecting stack and heap costs. We have developed new theoretical cost models for recursive function definitions, and used these to derive an analysis capable of determining stack and heap costs for recursive Hume programs.

1.3.2 Current Tools Supporting Hume Program Development

A wide range of tools now exist to support Hume development. While several of these are research quality, and primarily designed to demonstrate specific research results, we are steadily constructing a set of tools that can be used to develop real Hume programs.

Compilers and Interpreters: There are now four main implementations of Hume: the Hume reference interpreter produced at Heriot-Watt University; the prototype Hume abstract machine interpreter, produced at St Andrews; the Hume to C template-compiler, produced at Heriot-Watt, and the **hic** Hume interpreter, produced at LASMEA for use with their real-time exemplars.

The Hume reference interpreter is written in Haskell, and provides a simple, high-level interpretive framework, for rapid program development. The prototype Hume abstract machine (**HAM**) is primarily designed as a vehicle for research into cost modelling and compiler techniques, providing a portable bytecode implementation that is considerably faster and more memory efficient than the reference interpreter [25], and which provides useful instrumentation capabilities. The front-end **phamc** Hume to HAM compiler shares common modules with the reference interpreter. The HAM abstract machine back-end, **hami** is written in portable C and runs on a number of systems including Linux, MacOSX, the SymbianOS for smartphones, and the Real-Time operating system RT-Linux. It provides guaranteed hard-space bounds for the FSM-Hume subset of Hume [25], and has vastly superior time performance to embedded Java implementations, which implement a similar bytecode technology. The Hume to C compiler (**humec**) translates HAM instructions produced by the **phamc** compiler into portable C code using a template-instantiation approach. This provides a higher-performance route for deploying Hume code, that has been tested on a number of platforms, including Linux, MacOSX, the a Renesas M32C development board and the Tmote Sky. The Renesas board uses a 32-bit embedded microcontroller with 16KB DRAM, the Tmote Sky is a 16-bit standalone computing device with 8KB of DRAM Finally, the **hic** HUME interpreter provides a high-level interpretive framework. It basically supports the same features as the Hume reference interpreter but, being written in Caml, is significantly faster and offers an easier to use interface to low-level devices. It has been used mainly for developing real-time examplars.

All four implementations cover the key points of the Hume language design, including all expression forms, coordination, exceptions, and timeouts. At present, however, not all types are supported (notable exclusions are unicode characters, fixed-precision and exact arithmetic), and we are still clarifying issues related to interrupt handling and low-level I/O.

Development Tools: We have developed a graphical diagrammer for Hume programs. We have also developed an abstract machine code debugger. These are now being extended to form a full integrated development environment (IDE) for Hume. Both systems should be portable to a variety of development platforms.

KH: Some more here from Robert

Cost Models and Analyses: We have developed space cost models for HW=Hume and FSM-Hume that are integrated into the pham/humec compilers. We have developed space and time cost models for levels up to PR-Hume, and obtained concrete time metrics for the PowerPC G4 and for the Renesas M32C.

We have also developed a prototype implementation of a model checking for HW-Hume programs using the SPIN/Promela model-checking tools. We are currently adapting this to the TLA$^+$ temporal logic of actions, which will allow us to reason about real-time properties as well as safety and liveness.

Priorities for Tool Development: We are in the process of extending our cost analyses to cover time and space for PR-Hume. Having done this, our priorities are i) to integrate results from AbsInt's **aiT** low-level analyser with our high-level Hume sources; ii) to investigate the quality of analysis we can obtain on various programs; iii) to provide formal certification of resource usage; iv) to investigate other behavioural properties for Hume programs, and v) to consider how improved compiler optimisations may be incorporated into Hume without distorting the cost models.

1.3.3 Foundations for Bounded Space/Time Behaviour

The Hume design builds on foundational research in cost modelling which has been developed at St Andrews University, Scotland, UK and Ludwig-Maximilians Universität, München, Germany. We have developed new theoretical models of space and time usage for levels of Hume up to and including PR-Hume. These models [80, 11] form the basis for sound analyses that can derive guaranteed upper bounds on space and time usage. Our approach is based on a type-and-effect system analytical approach where we expose resource constraints from program source in the form of annotated types. These constraints can then be solved to give a closed-form solution to costs using either a linear solver [30] or one based on e.g. convex hulls [79].

Benchmarks and Applications: Within the EU Framework VI EmBounded project and a UK-funded project, we are developing a number of number of new realistic applications to demonstrate the use of Hume. These range from simple embedded systems to sophisticated computer vision algorithms. Work on some of these algorithms was presented at the International Symposium on Implementations and Applications of Functional Languages, IFL 2006, in Budapest, Hungary in September 2006 and further work will be presented at the ACM Symposium on Applied Computing in Seoul, Korea in March 2007.

1.4 Related Work

This section summarises work that is closely related to Hume. Fuller accounts may be found in research papers we have published elsewhere (e.g. [23, 24, 27]).

1.4.1 Languages for Programming Embedded Systems

Historically, real-time embedded systems have been programmed using low-level languages and techniques, most commonly C/C++ or assembler. Some high level languages have, however, been specifically designed or adapted for such use, and there is current interest in using formal model-driven development architecture approaches. Although we have not yet explored the details of how to do this, these model-driven approaches would seem to fit well with the strongly formal approach taken by Hume.

General-Purpose Languages: Ada is widely used for embedded systems, and many tools have been constructed to assist the understanding of space and time behaviour [4]. Compared with ANSI standard Ada, Hume provides much higher level of abstraction with a far more rigorously defined semantics, which is specifically designed to support cost semantics.

There has been recent interest in using variants of Java as the basis for embedded systems, though to our knowledge there is as yet no specifically safety-critical design. Two interesting variants are Embedded Java [74] and RTJava [39], for soft real-time applications. Like Hume, both languages support dynamic memory allocation with automatic garbage collection and provide strong exception handling mechanism. The primary differences from Hume are the omission of arbitrary recursion, an absence of formal design principles, the use of a single-layered approach in which coordination is merged with computation, and of course the use of an object-oriented expression language rather than one that is purely functional. We believe that the design choices made here are more suitable for applications where safety or correctness are important. For example, the use of purely functional rather than dynamically-linked object-oriented design allows straightforward static reasoning about the meaning of programs, at the cost of convenience in modifying a running system.

Synchronous Dataflow Languages: *Synchronous* languages such as Signal [6], Lustre [15], Esterel [12, 8] or the visual formalism Statecharts [28] obey the *synchrony hypothesis*: they assume that all events occur instantaneously, with no passage of time between the occurrence of consecutive events [5]. In contrast, *asynchronous* languages, such as the extended finite state machine languages Estelle [36, 13] and SDL [37], make no such assumption. Hume uses an asynchronous approach, for reasons of both expressiveness and realism. Like Estelle and SDL, it also employs an asynchronous model of communication and supports asynchronous execution of concurrent processes.

1.4.2 Real-Time Safety-Critical Systems

Typically, a formal approach to designing safety-critical systems progresses rigorously from requirements specification to systems prototyping. Languages and notations for specification/prototyping provide good formalisms and proof support, but are often weak on essential support for programming abstractions, such as data structures and recursion. Implementation therefore usually proceeds less formally, or more tediously, using conventional languages and techniques. Hume is intended to simplify this process by allowing more direct implementation of the abstractions provided by formal specification languages. Alternatively, in a less formal development process, it can be used to give a higher-level, more intuitive implementation of a real-time problem.

Specification Languages: Safety-critical systems have strong time-based correctness requirements, which can be expressed formally as properties of *safety*, *liveness* and *timeliness* [9]. Formal requirements specifications are expressed using notations such as temporal logics (e.g. XCTL [29] or MTL [43]), non-temporal logics (e.g. RTL [38]), or timed process algebras (e.g. LOTOS-T [56], Timed CCS [81] or Timed CSP [68]). Such notations are deliberately non-deterministic in order to allow alternative implementations, and may similarly leave some or all timing issues unspecified. It is essential to crystallise these factors amongst others when producing a working implementation.

Non-Determinism: Although non-determinism may be required in specification languages such as LOTOS [35], it is usually undesirable in implementation languages such as Hume, where predictable and repeatable behaviour is required [9]. Hume thus incorporates deterministic processes, but with the option of fair choice to allow the definition of alternative acceptable outcomes. Because of the emphasis on hard real-time, it is not possible to use the event synchronising approach based on *delayed timestamps* which has been adopted by e.g. the concurrent functional language BRISK [31]. The advantage of the BRISK approach is in ensuring strong determinism without requiring explicit specifications of time constraints as in Hume.

Persistency: In order to ensure essential progress even in the absence of some inputs, Hume is deliberately *non-persistent* [9]: the passage of time can force a timeout on an input channel, which can thus influence the choice made by a process. It is also possible for a timeout on an internal computation to have the same effect, although in this case no input will have been consumed. Determinacy is maintained through a strong formal cost model integrated with a formal dynamic semantics which collectively fully prescribe the outcome of a process instance given the inputs that have been provided.

Dynamic Process Networks. The initial Hume design uses a static process network, as with Petri net approaches [64], but unlike recent innovations such as π-calculus [57]. This simplifies the formal language semantics, and very importantly, allows the total cost to be specified for the active process network, but does prevent the direct definition of e.g. mobile processes. We do anticipate that some forms of dynamic process could be supported without destroying our overall cost semantics, but have not yet explored this issue.

Summary Comparison: As a vehicle for implementing safety-critical or hard real-time problems, Hume thus has advantages over widely-used existing language designs. Compared with Estelle or SDL, for example, it is formally defined, deterministic, and provably bounded in both space and time. These factors lead to a better match with formal requirements specifications and enhance confidence in the correctness of Hume programs. Hume has the advantage over Lustre and Esterel of providing asynchronicity, which is required for distributed systems. Finally, it has the advantage over LOTOS or other process algbras of being designed as an implementation rather than specification language: *inter alia* it supports normal program and data structuring constructs, allowing a rich programming environment.

1.4.3 Other Models Enforcing Bounded Time/Space Properties

Other than our own work, we are aware of three main studies of formally bounded time and space behaviour in a functional setting [14, 34, 78].

Embedded ML: In their recent proposal for Embedded ML, Hughes and Pareto [34] have combined the earlier *sized type system* [33] with the notion of *region types* [75] to give bounded space and termination for a first-order strict functional language [34]. Their language is more restricted than Hume in a number of ways: most notably in not supporting higher-order functions, and in requiring programmer-specified memory usage.

Inductive Cases: Burstall[14] proposed the use of an extended *ind case* notation in a functional context, to define inductive cases from inductively defined data types. Here, notation is introduced to constrain recursion to always act on a component of the "argument" to the *ind case* i.e. a component of the data type pattern on which a match is made. While *ind case* enables static confirmation of termination, Burstall's examples suggest that considerable ingenuity is required to recast terminating functions based on a laxer syntax.

Elementary Strong Functional Programming. Turner's *elementary strong functional programming* [78] has similarly explored issues of guaranteed termination in a purely functional programming language. Turner's approach separates finite data structures such as tuples from potentially infinite structures such as streams. This allows the definition of functions that are guaranteed to be primitive recursive. In contrast with the Hume expression layer, it is necessary to identify functions that may be more generally recursive. We will draw on Turner's experiences in developing our termination analysis.

Other Related Work. Recent research by Kamareddine and Monin has formlised automatic proofs of termination of recursive functions, by augmenting proof trees with measures that establish an appropriate decreasing property [40]. They have also investigated widening the scope of automatic termination proof from inductive to non-inductive cases [41]. Also relevant to the problem of bounding time costs is recent work on *cost calculi* [69, 71] and *cost modelling* [67, 48, 72], which has so far been primarily applied to parallel computing.

1.5 Publications and On-Line References

Research papers on Hume, Hume implementations and programmer documentation can all be found at the Hume web page `http://www.hume-lang.org`. Information about the EU Framework VI EmBounded project can be found at `http://www.embounded.org`. Information on the DTC project on Systems Engineering for Autonomous Systems may be found at `http://www.macs.hw.ac.uk/~greg/SEAS/`.

1.6 Changes from Version 0.3/1.0

The main changes introduced in version 1.1 of the report are:

- vectors are now specified with a size rather than a bound;
- strings are properly defined as fixed-size immutable objects;
- new operations have been defined for vector maps, folds and initialisation;
- `fixed`, `exact` and `unicode` types have been removed;
- corrections to the basic operations;
- corrections to the syntax.

1.7 Changes from Version 0.2

The main changes introduced in version 1.0 of the report are:

- added `interrupt`, `fifo`, `memory` and `operation`;
- added foreign function interfacing and `operation`;
- added `profile` and `verify` expressions;
- added descriptions of declarations;
- extended `within` expressions to space as well as time;
- included timeouts on I/O descriptors;
- removed `port`, `stream` and `bandwidth` types.

Chapter 2

Hume Overview

This chapter introduces the Hume language informally. Section 2.1 describes the set of fundamental types that are supported by Hume, together with the operations that are provided on those types. Section 2.2 describes the coordination layer; Section 2.3 describes the declaration layer; and Section 2.4 describes the expression layer. These sections refer to syntax, which is expanded and formally defined in Chapter A.

One important concern for any such language is the matter of type coercion and conversion, especially between scalar values. Hume therefore provides a wide range of scalar types, and defines precisely the conversions between values of those types. (Section **??**. Hume scalar types include booleans, characters, variable sized word values, fixed-precision integers (including natural numbers), and floating-point values.

A second, related concern is the need to specify the sizes of such values. Hume meets this concern by requiring the size of all scalar values to be specified precisely.

In addition to scalar types, Hume supports four kinds of structured type: vectors, lists, tuples and user-defined discriminated unions. Vector and tuple types are fixed size, whereas lists may be arbitrary sized. All the elements of a single vector or list must have the same type.

2.1 Types

2.1.1 Base Types

All Hume type domains are unpointed [44]. That is, there is no explicit notion of an *undefined* value ($\perp$) in each type domain. The Hume *base types* are shown in Table 2.1. The type `bit` is a synonym for `word 1`, and the type `byte` is a synonym for `word 8`.

The basic operations provided for each type are shown in Table2.2. The integer division and remainder operators (mod) have the property that `a == (a div b)*b + (a mod b)`. The result of `x div y` has the same sign as `x * y` and is truncated towards zero. The value of `x ** 0` is 1 for any `x`, including zero. For `word`, `& | ^ ~` are bitwise and, inclusive or, exclusive or and negation respectively. The `lshl` and `lshr` operations pad to left/right with `0`s respectively, as required.

2.1.2 Structured types

The Hume structured types are shown in Table 2.3, with the corresponding operations shown in Table 2.4.

`bool`	boolean value denoted by `true`, `false`
`char`	8 bit - ISO Latin-1 character denoted by: `'<printable>'`, e.g. `'H',' ', '\\'`
`word <size>`	bits of specified size, in the range $0 \ldots 2^n - 1$ denoted by 0, 1, ...
`int <size>`	2's complement integer of specified bit size, in the range $-2^{n-1} \ldots 2^{n-1} - 1$ denoted by 0, 1, -1, ...
`nat <size>`	natural number i.e. $\geq$ `0` of specified bit size, in the range $0 \ldots 2^n - 1$ denoted by 0, 1, ...
`float <size>`	floating point number of specified bit size (IEEE representation) denoted by e.g. 0.0, -1.23456, 1e99, ...
`string [<size>]`	string of the specified length denoted by: `"<printable1> ... <printableN>"` where `N` ≥ 0, e.g. `""`, `"Hume"`, ...

Table 2.1: Hume base types

`bool`	`&& || not` `< <= == >= > !=`
`char`	`< <= == >= > !=`

`word`	`+ - * div mod`
	unary `-` — not provided for `nat`
	`**` — power
	`lshl lshr` — logical shift left/right
	`ashl ashr` — arithmetic shift left/right
	`rotl rotr` — rotate left/right
	`bittest bitset bitclr` — bit testing/setting
	`^& ^| ^ ~` — bitwise operations
	`< <= == >= > !=`

`int`
`nat`
	`+ - * div mod`
	unary `-` — not provided for `nat`
	`**` — power
	`< <= == >= > !=`

`float`	`+ - * /`
	unary `-`
	`sin cos tan asin acos atan`
	`sinh cosh tanh atan2`
	`log log10 ln exp`
	`sqrt`
	`**` — power
	`< <= == >= > !=`

`string`	`< <= == >= > !=` `@ ++ length`

Table 2.2: Basic operations on base types

Vectors	fixed length sequence of uniform type with the given bounds type: `vector <size> of <type>` where `<size>` ≥ 0 denoted by: `<< <expr1>, ... , <exprN> >>` where `N` ≥ 0
Tuples	fixed length sequence of mixed type type: `( <type1>, ... , <typeN> )` where `N` $= 0$ or `N` > 1 denoted by: `( <expr1>, ... , <exprN> )` where `N` $= 0$ or `N` > 1
Lists	variable length sequence of uniform type type: `[ <type> ]` denoted by: `[ <expr1>, ... , <exprN> ]` where `N` ≥ 0

Discriminated unions	declared by:
	`data <id> <var1> ... <varN> =`
	`<id1> <type11> ... <type1K> | ...`
	`<idM> <typeM1> ... <typeML>`
	where `K, L, N` ≥ 0; `N` ≥ 1
	type: `<id> <type1> ... <typeN>` where `N` ≥ 0
	denoted by: `<id> <expr1> ... <exprN>` where `N` ≥ 0

Table 2.3: Structured types

Vectors	construction by denotation
	selection by pattern matching
	`@ <expr>` — select `<expr>`th element
	`length`
	`vecdef, vecmake, vecmap, vecfoldr`
	`update` — copying update
	`++` — vector concatenation
	`< <= == > >= !=`

Tuples	construction by denotation `@ <expr>` — select `<expr>`th element selection by pattern matching `< <= == > >= !=`

Lists	`:` — list constructor
	construction by denotation
	`length`
	`hd tl`
	`@ <expr>` — select `<expr>`th element
	selection by pattern matching
	`++` — list concatenation
	`< <= == > >= !=`

Discriminated unions	construction by denotation selection by pattern matching `< <= == > >= !=`

Table 2.4: Basic Operations on Structured types

	bool	int	nat	float	char	word	string
bool	–	Y	Y	N	N	Y	Y
int	Y(1)	–	Y(2)	Y	Y(3)	Y(4)	Y
nat	Y(1)	Y(5)	–	Y	Y(3)	Y(4)	Y
float	N	Y(6)	Y(7)	–	N	Y(4)	Y
char	N	Y	Y	N	–	Y(4)	Y
word	Y	Y(4)	Y(4)	Y(4)	Y(4)	–	Y
string	N	N	N	N	N	N	–

Table 2.5: Valid Coercions between Hume base types.

Notes

1. `int = 0` or `int = 1`
2. `int` $\geq$ `0`
3. `0 <= int <= 255`
4. `0 <= int <= 2**word` size-1
5. `nat` size `<= int` size-1
6. `trunc, round, ceiling`
7. `float > 0` and as `int`

2.1.3 Type Conversions

There are two kinds of type conversion. Casting (or viewing) involves treating a value as if it belonged to another equivalent type. One type may be cast to another using `<expr> :: <type>` if there is no loss of information when converting from a value of the type of `<expr>` to `<type>`, and if the conversion can be done with no runtime cost.

The second form of type conversion is coercion. In this case, there may be loss of information and there may also be a runtime cost. The corresponding form is `<expr> as <type>`.

The conformancy between base types is as shown in Table 2.1.2. The most significant bit in a `word` is to the left. Base values are right aligned and left padded.

Coerced structured types:

- must have the same number of elements at all levels
- are aligned top down, recursively, element by element left to right

2.1.4 Exceptions

Exceptions are:

- declared by: `exception <id> <type>`, within declarations (Section 2.3);
- raised by: `raise <id> <expr>` within expressions (Section 2.4.10);
- handled by: `handle <handlers>` within boxes (Section 2.2.3).

System exceptions may be handled either within a box or by a general system handler. If a box defines a handler for a system exception, and the exception is raised as a consequence of executing that box, then the specified handler is called. If a box fails to define a handler for a system exception and that system exception occurs during the process of executing the box, then the general system handler is called. There must be precisely one general handler for each system

exception, and, at present, there is no mechanism to allow this to be user-defined. The system exceptions are:

`Div0`	division by 0
`Overflow/Underflow`	numeric overflow/underflow
`OutOfBounds`	out of bounds vector index
`HeapOverflow`	heap overflow
`StackOverflow`	stack overflow
`Timeout`	timeouts
`EndOfFile`	end of input file

Note that `HeapOverflow` and `StackOverflow` are only raised by code whose heap/stack costs have not been certified, and then in the context of a within-constraint on boxes or expressions. `Timeouts` occur through within/timeout constraints on ports, streams, wires, boxes or expressions.

2.2 The Coordination Layer

This section describes the Hume coordination layer and the wiring metalanguage. The formal dynamic semantics of Hume boxes is given in Appendix C.

2.2.1 Boxes

```
<boxdecl> ::= <prelude> <body>

<prelude> ::=
        "box" <boxid>
        "in"  <inoutlist>
        "out" <inoutlist>
        [ "within"  <constraint> ]
        [ "handles" <exnidlist>  ]

<inoutlist> ::=
        "(" <inout1> "," ... "," <inoutn> ")"    n >= 0

<inout> ::=
        <varids> "::" <type> [ "timeout" <cexpr> ]

<varids> ::=
        <varid1> "," ... "," <varidn>            n >= 1
```

The Hume unit of coordination is the *box*. A box has a unique name, specified in its *prelude*. A box has *inputs* and *outputs* termed *ins* and *outs*. Ins and outs are fixed width sequences of *inout* type. An *inout* type is any Hume type excluding a function or exception. A box's *ins* and *outs* are specified in its prelude. Each *in* and *out* has a unique name, and is typed. The exceptions a box handles are specified in the box's prelude. It is possible to provide a within-clause to limit costs within a box execution in the same way as they are limited in an expression.

2.2.2 Box Bodies

```
<body> ::=
        ( "match" | "fair" )
```

```
        <matches>
        [ "timeout" <cexpr> ]
        [ "handle" <handlers> ]
```

The body of a box consists of a set of matches against input values, an optional timeout covering all the matches, plus the exception handlers that apply during each iteration of the body.

Each `<match>` in a box must have:

1. a pattern component `<patt>` which is type consistent with the `in` declaration; and
2. an expression component `<expr>` which is type consistent with the `out` declaration.

Top-level patterns may include `*`s. The purpose of a `*` is to indicate that the corresponding input is neither matched nor consumed.

Matching may be either sequential (unfair) or "fair". Rules introduced by the `match` keyword are matched in order from top to bottom. The first rule (if any) that fully matches the inputs is selected. Thus a single rule may be matched repeatedly if the same inputs are encountered. In some cases, this can result in certain rules never being used. Fair matching, in contrast, guarantees that all rules are given an equal probability of being matched [3].

2.2.3 Exception Handlers

```
<handlers> ::=
        <handler1> "|" ... "|" <handlern>       n >= 1

<handler> ::=
        <hpatt> "->" <cexpr>

<hpatt> ::=
        <exnid> <patt1> ... <pattn>             n >= 1
```

There must be a `<handler>` for each exception specified in the box's `handles` clause. All non-system exceptions that can be raised by any expression within the body of the box, or which occur through input timeouts, must be handled by an explicit handler. No handler can perform any computation.

Every `<handler>` in a box must have:

1. a `<handlepatt>` corresponding to an entry in the `handles` declaration; and
2. a `<handleout>` which is type consistent with the `out`

2.2.4 Wiring

```
<wiringdecl> ::=
          "wire" <boxid> <sources> <dests>
        | "wire" <link> "to" <link>

<sources>/<dests> ::=
          "(" <link1> "," ... "," <linkn> ")"     n >= 0

<link> ::=
          <connection>
```

```
        | <strid>
        | <portid>

<connection> ::= <boxid> "." <varid>
```

Boxes are wired together by specifying for each *in* or *out*, the corresponding source or destination box's *in* or *out*, or the device (stream etc.) to which it is connected. Wires may either be specified for a complete set of box sources and destinations or individually for each input/output pair.

Connection to another box is specified by that box's name extended with the *in* or *out* name. Boxes may be wired to themselves. Each device (stream, port etc.) may only be wired to one box.

2.2.5 Box Templates and Instantiation

```
<wiredecl> ::=
          "template" <templateid> <prelude> <body>

<wiringdecl> ::= ...
        | "replicate"   <boxid> "as" <boxid> [ "*" <natconst> ]
        | "instantiate" <templateid> "as" <boxid> [ "*" <natconst> ]
```

A template can be defined to give the structure of a box, which is then instantiated to produced a number of boxes.

To simplify the construction of complex systems, both boxes and templates may be replicated to give new boxes. The box/template may be replicated either once or a number of times (indicated by `* <natconst>`). For example, `instantiate t as b * 4` will introduce boxes `b1`, `b2`, `b3` and `b4` are introduced.

2.2.6 Wiring Macros

```
<wiringdecl> ::= ...
        |  "wire" <wmacid> "(" <id1> ... <idn> ")"
                           "=" <wireid> <sources> <dests>
        |  "wire" <wmacid> <args>
```

Wiring macros can be introduced by associating a wiring definition with a name and set of parameter names. The parameter names declared on the LHS may be used on the RHS of the wiring macro and substitute the corresponding concrete name. Wiring macros are used in place of normal wiring declarations Depending on usage, wiring macro arguments may be either box names or names of inputs/outputs. It is not, however, possible to use unrestricted values such as integers as arguments to wiring macros.

We will use a running example adapted from Roscoe's book on CSP [**?**]. The example is a railway layout, formed from a set of track segments, where each segment is instantiated from a `Track` template, whose definition is given below.

```
data Channel   = RDY | SND TrainID | NAK;
data Ctl =       RCV | ACK;
data State =     Just TrainID | Nothing | Nothing2
                              | WaitI | WaitI2 | WaitO ;
type TrainID =   string;

template Track
```

```
in  ( value  :: State, inp    :: Channel,  outctl :: Ctl      )
out ( value' :: State, inctl  :: Ctl,      outp    :: Channel )
match
   ...
```

We can instantiate the basic track segment to give a ring of `RingSize` track segments as follows:

```
constant RingSize = 8;

for i =  0 to RingSize-1 except (ForkPos, JoinPos)
   instantiate Track as Ring{i};
```

This defines `Ring0`..`Ring7`. We can now define a wiring macro `TrackM` to link the current track segment to the previous and next segments by connecting the `value/value'`, `inctl/outctl` etc. pairs as required.

```
wire TrackM ( this, prev, next ) =
  wire {this} ( {this}.value', {prev}.outval, {next}.inctl )
              ( {this}.value,  {next}.outctl, {prev}.inval )
;
```

Now we can use the `TrackM` macro to wire the complete ring of track. To assist with this, we define two simple macros, `predR` and `succR` that are used to calculate the names of the previous and next elements of the ring. So if `i` is 0, then `Ring{i}` is `Ring0`, `Ring{succR(i)}` is `Ring1` and `Ring{predR(i)}` is `Ring7`.

```
macro predR i = (i-1) mod RingSize;
macro succR i = (i+1) mod RingSize;

for i = 0 to RingSize
        wire TrackM ( Ring{i}, Ring{predR(i)}, Ring{succR(i)})
;
```

2.2.7 Repeated Wiring

```
<wiringdecl> ::=
          "for" <id> "=" <expr> "to" <expr> [ "except" <excepts> ]
            <wiringdecl>
```

Wiring declarations can be repeated under the control of a variable (optionally omitting certain values). The repetition variable may be used within the wiring declaration (enclosed within braces), where it takes on each value in the iterator clause in turn. For example,

```
for i =  0 to 4 except (2, 1)
   instantiate Track as Ring{i};
```

will generate `Ring0`, `Ring3`, `Ring3` as instances of the Track template. It is possible to nest for-loops if required, and it is possible to use both loop variables, static constants and expression macros in the expressions. Note that such loops are part of the static coordination layer designed to create a static process network rather than part of the dynamic expression language.

2.2.8 Initial Values

```
<wiringdecl> ::= ...
        | "initial" <wireid> <inits>

<inits> ::=
          "(" <init1> "," ... "," <initn> ")"           n >= 1

<init> ::=  <wireid> "=" <expr>

<linkprop> ::= ...
        | "initially" <expr>
```

It is possible to specify initial values for wires. These may be provided either as part of the link specification for a wire or using an explicit `initial` declaration.

For example, we can provide an initialiser for the `value` input of the `Ring{Train1Pos}` box as shown below. Initialisers may be provided either on input or output wires, as convenient. It is, however, an error for more than one initialiser to be provided for any wire.

```
constant Train1Pos = 3;

initial Ring{Train1Pos} ( value = Just "Train1" );
```

2.2.9 Expression Macros

```
<wiringdecl> ::= ...
           | "macro" <mid> <id1> ... <idn> "=" <expr>   n >= 0
```

Expression macros are used to construct simple compile-time macros that are resolved during construction of the static process network. Only compile-time constants may be used in macros.

2.2.10 I/O Declarations

```
<decl> ::= ...
           | "stream"    <iodes>
           | "port"      <iodes>
           | "interrupt" <iodes>
           | "memory"    <iodes>
           | "fifo"      <iodes>

<iodes> ::=
   <ioid> ( "from" | "to" ) <string>
          [ "timeout"/"within" <timeconst> [ "raise" <exnid> ] ]
```

Interactions with the operating system and devices are specified in the declaration language. The string in the `iodes` is a system-specific designator identifying the operating system entity (file, physical device etc.) that the device is attached to. Each device must be wired to precisely one box input or output. Input devices (specified with `from`) must be wired to box inputs; output devices (specified with `to`) must be wired to box outputs. Devices cannot be wired directly to other devices. The type of a device is not specified explicitly, but is inherited from the input/output to which it is connected.

2.3 The Declaration Layer

The declaration layer introduces types and values that scope over either or both the coordination and expression layers. The coordination layer is embedded in terms of box and wiring declarations while the expression layer is embedded in terms of function declarations.

While it is possible to define recursive and mutually recursive functions, simple values cannot be recursive.

2.3.1 Function, Value and Constant Declarations

```
<decl> ::= ...
        | <fundecl>
        | "constant" <varid> "=" <cexpr>

<fundecl> ::=
          <varid> "::" <type>
        | <varid> <args> "=" <expr>
        | <patt1> <op> <patt2> "=" <expr>

<args> ::=
        <patt1> ... <pattn>                    n >= 0
```

Functions and named values are introduced as shown above.Values may be declared to be *constant*, in which case their value is calculated at compile-time. Such constant values must be simple calculations and may not be defined using function calls, within constraints etc. Named constants may be used in the wiring metalanguage, in expression macros, or in any other place where a constant expression is mandated. The form `varid :: <type>` indicates only that the variable has the specified type, and must be accompanied by a value or function declaration in the same module. It is not an error to omit a type declaration, however: in this case, the variable or function is assigned the most general type possible by the compiler using a standard Damas-Milner type inference algorithm [17].

For example, we can define the ubiquitous `nfib` function as follows:

```
nfib :: int 32 -> int 32;
nfib 0 = 1;
nfib 1 = 1;
nfib n = 1 + nfib(n-1) + nfib (n-2);
```

and we could define a constant `arraylen`, by, e.g. `constant arraylen = 100`.

2.3.2 Type Declarations

```
<decl> ::= ...
        | "data" <typeid> <varids> "=" <constrs>
        | "type" <typeid> <varids> "=" <type>

<constrs> ::=                                  m > 0, k >= 0, n >= 0
            <conid1> <type11> ... <type1k>
        "|" ...
        "|" <conidm> <typem1> ... <typemn>
```

Hume includes two kinds of type declaration. The first form introduces a new constructed data type whose alternatives are distinguished by different data constructors (a discriminated union type). The second form introduce a *type synonym*; a named type equivalent to some pre-existing type. Either form of declaration may be *polymorphic*, in which case it must be provided with a number of type variable arguments (these may then appear within the type declaration part). Constructed types may also be defined recursively.

So, for example, we can define a new type of polymorphic binary trees, and a version that is specialised to 32-bit integers, by:

```
data Tree a  = Leaf a | Node (Tree a) (Tree a);

type IntTree = Tree (int 32);
```

User-defined types (whether data types or type synonyms) may be used wherever pre-defined types may be used, and data constructors may be used both in pattern-matching and in expressions.

2.3.3 Exception Declarations

```
<decl> ::= ...
        | "exception" <exnid> "::" <type>
```

Hume exceptions are typed. A Hume exception is a constructed value like a data type, which is raised by a `raise` expression or as the result of a system exception, and which is handled by exception handlers introduced at the box level.

For example, we can define a new exception over a string, with the corresponding `raise` and `handle` clauses as follows:

```
exception X :: string;

box B in ( ... ) out ( res :: string )
handles X
match
   ... -> ...  raise (X "overflow") ...
handle
   X s -> s;
```

2.3.4 Import/Export Declarations

```
<decl> ::= ...
        | "import" <id> [ <idlist> ]
        | "export" <idlist>
```

KH: check that idlist is properly bracketed

Hume import and export declarations respectively introduce identifiers that have been defined in some other module, or expose identifiers from the currently defined module for use elsewhere. In the import form, `<id>` is the name of the module to be imported. In both forms, `<idlist>` is the list of entities to be imported or exported.

So, for instance,

```
import M (a,b);
export f;
```

imports `a` and `b` defined in module `M` for use in the current module, and exports `f`.

2.3.5 Foreign Function Interfacing

```
<foreigndecl> ::=
          "foreign" "import" <callconv> [ <safety> ] [ <string> ]
                             <id> "::" <type>

<safety> ::=
           "safe" | "unsafe"

<callconv> ::=
          "ccall" | "stdcall" | "cplusplus" | "jvm" | "dotnet"
```

Hume uses the same notation for foreign function interfacing as Haskell [16]. This allows reuse of standard interface generator tools such as **GreenCard**. External calls are specified using foreign function declarations which provide information about the calling convention to be used, whether the function is safe or unsafe, and the Hume type of the function. The optional string is used to provide additional information to the compiler related to the calling language: for C calls (the normal convention), this includes the name of the function if different from the Hume name plus information about files that must be included in the compiled code. Note that it may be necessary to link compiled Hume code with additional libraries or undertake other special actions as specified by the implementation in order to exploit external calls.

Note that it is not permitted to use unsafe foreign calls in Hume expressions; they may only be used in Hume *operations* (see below). In this way referential transparency is preserved for Hume expressions even in the presence of foreign function calls. The safety clause is retained purely for backwards compatibility with the Haskell FFI and generator tools.

Note also that in `<foreigndecl>`, `<string>` typically consists of the library name followed by the name of the library entity, and `<id>` is the Hume name for the entity. For example, `foreign import ccall "math.h sinh" hsin :: float 32 -> float 32` specifies a Hume function `hsin` which is defined as the C function `sinh` in the `math.h` header file.

Operations

```
<decl> ::= ...
   | "operation" <boxid> "as" <string> "::" <type>
```

There is some question about whether operations could encapsulate pure functions. For now, I'm leaving this, since I don't really want to reimplement it – the code is a bit sensitive! KH

Operations extend the foreign function interface, providing a wrapper for (possibly) unsafe foreign function calls. An operation introduces a new box with one input, named `inp`, and one output, named `outp`. The string describes the foreign function as for the optional string in a foreign function import declaration. Only the `ccall` calling convention is supported.

For example, `operation System as "system" :: String -> ()` introduces a new box called `System` whose purpose is to execute the `system` function call (on a Unix system, this will cause its argument to be executed as an operating system command, for instance). The call is performed synchronously, returning the unit tuple value (`()`) on completion. The `System` box is wired in the same way as any other box. For example,

```
wire b.syscall to System.inp;
wire System.outp to b.done;
```

wires its input to `b.syscall` and its output to `b.done`, where `b` is a box defined elsewhere.

2.3.6 Expression Declarations

```
<decl> ::= ...
        | "expression" <expr>
```

Where the result of a Hume program is a single expression rather than a set of boxes, then a special shorthand form is available. An expression declaration introduces a box with no input, and whose output is directed to the standard output stream. The box runs precisely once, and may use any defined function or expression form. For example, `expression nfib 100` produces the program whose purpose is to calculate

2.4 The Expression Layer

The Hume expression layer follows the design of widely used functional languages such as Standard ML [58] and Haskell [32]. Like Standard ML, Hume expressions follow a strict evaluation order. This allows tight cost functions to be derived for Hume expressions and allows a relatively simple semantics of exceptions to be specified (see Appendix C). Like Haskell, the Hume expression layer is purely functional. In order to simplify code reuse, the syntax of the Hume expression layer is broadly based on that of Haskell, and is fully described in Appendix A. The formal dynamic semantics of the Hume expression layer is given in Appendix C.

2.4.1 Constants

```
<expr> ::= ...
          <constant>

<constant> ::=
          <intconst>
        | <floatconst>
        | <boolconst>
        | <charconst>
        | <stringconst>
        | <wordconst>
```

Constants are simple constant values covering the basic Hume types, including integers, floating point numbers, booleans, characters and strings. Characters are 1-byte ASCII characters conforming to the ISO-Latin-1 alphabet and have type `char`. Examples of valid constants are shown below. A full description of the lexical syntax for constants may be found in Appendix

```
0, 1, -1                            integer constants
0xff, 0x100, (-0x1)                 word constants
0.0, -1.23, 123.456e7               floating point constants
'a', ' ', '\\', '\n', '\012'        character constants
"", "David Hume", "\n"              string constants
true, false                         boolean constants
```

2.4.2 Variables

```
<expr> ::= ...
        | <varid>                                variable/constant
```

Variables are defined either in function declarations, constant declarations, or in pattern matches. In the first two cases, their value is as specified in the corresponding declaration. The value of a constant can be obtained without runtime computation, that of a variable declared in a function declaration may require computation. In the final case, the value of the variable is obtained by deconstructing the matched expression as a consequence of the pattern matching operation. No further computation is required.

2.4.3 Constructors

```
<expr> ::= ...
        | <conid> <expr1> ... <exprn>            constr. n >= 0
```

Constructors are used build new data structures. They are defined by `union` declarations to be components of some discrimated union type.

2.4.4 Tuples, Lists and Vectors

```
<expr> ::= ...
        | "[" <exprs> "]"                        list
        | "()"                                   empty tuple
        | "(" <expr1> "," ... "," <exprn> ")"    n-tuple, n >= 2
        | "<<" <exprs> ">>"                      vector

<exprs> ::=
        <expr1> "," ... "," <exprn>              n >= 0
```

Tuples, lists and vectors are created in a similar way to user-defined constructors, but for convenience, special syntax is provided. It is not possible to create a tuple of one element. An "empty" tuple can be created using the syntax `()`.

2.4.5 Function Applications

```
<expr> ::= ...
        | <expr1> <op> <expr2>                   binary operator
        | <varid> <expr1> ... <exprn>            function, n >= 1
```

Hume function applications have a strict semantics. All arguments to a function are evaluated from right-to-left before the function is called. Note that while higher-order functions *are* supported, they may have cost implications.

2.4.6 Case Expressions

```
<expr> ::= ...
        | "case" <expr> "of" <matches>           case expression

<matches> ::=
        <match1> "|"..."|" <matchn>              n >= 1

<match> ::=
       <patt> "->" <expr>
```

Case expressions must be *complete* in the sense that all possible values of the type of the expression which is discrimated on must be matched by one or more of the specified patterns. In determining whether an expression matches a pattern, the patterns are matched in order top-to-bottom, left-to-right. In matching a pattern, a variable or wildcard matches any value (in the former case also creating a new binding for the variable to the matched sub-expression), any other pattern matches if the pattern constructor matches the expression's constructor and all sub-expressions match all corresponding sub-patterns. Patterns are left-linear (there are no repeated variables within a single pattern).

2.4.7 Conditional Expressions

```
<expr> ::= ...
        | "if" <expr1> "then" <expr2>            conditional
                       "else" <expr3>
```

Conditionals can be seen as a special case of case-expressions where the expression being discriminated on has type `bool` and there are precisely two alternatives depending on whether the value of the expression is `true` or `false`.

2.4.8 Local Declarations

```
<expr> ::= ...
        | "let" <vardecls> "in" <expr>           local definition

<vardecls> ::=
          <vardecl1> ";" ... ";" <vardecln>      n >= 1

<vardecl> ::=
          <varid> "::" <type>
        | <varid> "=" <expr>
```

Local declarations are used to introduce one or more bindings of variables to expressions with a limited scope. The name introduced by a binding is visible within other bindings in the same set of declarations as well as within the target expression. All value bindings are evaluated before the body of the expression is evaluated. If a local declaration contains a type declaration for a variable, the same local declaration must also contain a definition for that variable.

2.4.9 Type Expressions and Type Coercions

```
<expr> ::= ...
        | <expr> "::" <type>                     type cast/view
        | <expr> "as" <type>                     type coercion
```

Types can be given to an expression using the "::" operator. In this case, the compiler will verify statically that the expression has the specified type, or can be "viewed" as the specified type. These operations are purely static and have no dynamic effect.

More powerful dynamic *type coercions* can be specified using "as"-expressions. A table of types that are compatible for coercion purposes is given in Section 2.1.3. In this case, some computation may be required to coerce a value from one type to another. Unlike the use of the "::" operator, a type coercion may not be reversible: information may be lost during the coercion process, for example. Coercions must therefore be treated with care.

2.4.10 Exceptions

```
<expr> ::= ...
        | "raise" <exnid> <expr>                raise exception
```

Exceptions can be raised in any expression. The exception is propagated immediately it is raised to the enclosing *box*, which must provide a handler to handle the exception.

2.4.11 Time and Space Constraints

```
<expr> ::= ...
        | <expr> "within" <constraint> [ "raise" <exnid> ]

<constraint> ::=
          <timeconst> [ "," <spaceconst> [ "(" <spaceconst> ")" ] ]
        | <spaceconst>  [ "(" <spaceconst> ")" ] ]
```

Within-expressions are used to specify that evaluation of the associated expression must complete within the specified constraint (which must be a constant). If the constraint is violated at run time, then an exception will be raised. If not given explicitly in the within-clause, this exception is one of `Timeout`, `StackOverflow` or `HeapOverflow` as appropriate to the constraint. The exception must be handled by the box, and will be raised with a `()` argument. If only one space constant is specified in a within-clause, it represents a heap constraint, otherwise the first constraint represents a heap constraint, and the second a stack constraint.

2.4.12 Constant Expressions

```
<cexpr> ::= <expr>
```

In some places, expressions have a statically fixed value. This is indicated by `<cexpr>`. Such expressions may include variables, constructors, constants, and predefined operators on such values, but may not include user-defined function calls, raise expressions, timeouts or case/if/let expressions where any of the above rules are violated, or which use any non-constant variable identifiers other than as the sole result of the expression. The compiler will evaluate such expressions at compile-time and generate code to ensure that the appropriate value or variable is loaded in constant time at runtime.

2.4.13 Profiling and Verification (Optional)

```
<expr> ::= ...
        | "profile"  <expr>
        | "verify"   <expr>
```

Two expression forms are used for profiling and cost verification purposes. `profile e` prints the costs of executing `e`, and returns the value of `e`. `verify e` applies the cost modeller to the expression `e` and checks that the actual costs are within those that are determined. A `StackOverflow` or `HeapOverflow` is raised as appropriate if the inferred costs are not achieved in practice. This is mainly useful to eliminate errors during the development of the cost modelling software.

Note that these forms may not be supported in all implementations.

2.4.14 Tracing (Optional)

```
<expr> ::= ...
        | "trace"  <expr1> <expr2>
```

For debugging purposes, Hume provides limited support for tracing execution values. `trace e1 e2` prints a string corresponding to the value of `e1` and returns the value of `e2`. The string that is printed is implementation-dependent. Some types (such as functions) may not return useful information.

Note that this form may not be supported in all implementations of Hume.

Appendix A

Syntax

This appendix gives a BNF definition of the concrete syntax for Hume programs. The meta-syntax is conventional. Terminals are enclosed in double quotes " ... ". Non-terminals are enclosed in angle brackets < ... >. Vertical bars | are used to indicate alternatives. Constructs enclosed in brackets [...] are optional. Parentheses (...) are used to indicate grouping. Ellipses (...) indicate obvious repetitions. An asterisk (*) indicates zero or more repetitions of the previous element, and a plus (+) indicates one or more repetitions.

Programs and modules

```
<program> ::=
        <decls>

<module> ::=
        "module" <modid> "where" <decls>
```

Declaration Language

```
<decls> ::=
          <decl1> ";" ... ";" <decln>            n >= 1

<decl> :: =
          "import" <modid> [ <idlist> ]
        | "export" <idlist>
        | "exception" <exnid> "::" <type>
        | "data" <typeid> <varids> "=" <constrs>
        | "type" <typeid> <varids> "=" <type>
        | "constant" <varid> "=" <cexpr>
        | "stream" <iodes>
        | "port" <iodes>
        | "memory" <iodes>
        | "interrupt" <iodes>
        | "fifo" <iodes>
        | <foreigndecl>
        | "operation" <boxid> "as" <string> "::" <type>
        | "expression" <expr>
```

```
        | <boxdecl>
        | <wiringdecl>
        | <fundecl>

<constrs> ::=
            <conid1> <type11> ... <type1n>       m > 0, n >= 0
        "|" ...
        "|" <conidm> <typem1> ... <typemn>

<iodes> ::=
           <ioid> ( "from" | "to" ) <string>
              ["timeout"/"within" <timeconst> ["raise" <exnid> ]]

<fundecl> ::=
          <varid> "::" <type>
        | <varid> <args> "=" <expr>
        | <patt1> <op> <patt2> "=" <expr>

<args> ::=
        <patt1> ... <pattn>                      n >= 0

<vardecl> ::=
          <varid> "::" <type>
        | <varid> "=" <expr>

<vardecls> ::=
          <vardecl1> ";" ... ";" <vardecln>      n >= 1

<foreigndecl> ::=
          "foreign" "import" <callconv> [ <safety> ] [ <string> ]
                             <id> "::" <type>

<safety> ::=
           "safe" | "unsafe"

<callconv> ::=
          "ccall" | "stdcall" | "cplusplus" | "jvm" | "dotnet"
```

Types

```
<type> ::=
          <basetype>                             base type
        | "vector" <natconst> "of" <type>        vector
        | "()"                                   empty tuple
        | "(" <type1> "," ... "," <typen> ")"    tuple, n >= 2
        | "[" <types> "]"                        list
        | <typeid> <type1> ... <typen>           datatype, n >= 0
        | <type> "->" <type>                     function type
        | "(" <type> ")"                         grouping

<types> ::=
          <type1> "," ... "," <typen>            n >= 0
```

```
<basetype> ::=
          "int" <size>
        | "nat" <size>
        | "bool"
        | "char"
        | "string" [ <natconst> ]
        | "word" <size>
        | "float" <size>

<size> ::=
          "1" | ... | "128"
```

Expression Language

```
<expr> ::=
          <constant>                              constant
        | <varid>                                 var./named const.
        | <expr1> <op> <expr2>                    binary operator
        | <varid> <expr1> ... <exprn>             function, n >= 1
        | <conid> <expr1> ... <exprn>             constr., n >= 0
        | "[" <exprs> "]"                         list
        | "()"                                    empty tuple
        | "(" <expr1> "," ... "," <exprn> ")"     n-tuple, n >= 2
        | "<<" <exprs> ">>"                       vector
        | "case" <expr> "of" <matches>            case expression
        | "if" <expr1> "then" <expr2>             conditional
                       "else" <expr3>
        | "let" <vardecls> "in" <expr>            local definition
        | <expr> "::" <type>                      type cast/view
        | <expr> "as" <type>                      type coercion
        | "raise" <exnid> <expr>                  raise exception
        | <expr> "within" <constraint>            constraint
                 [ "raise" <exnid> ]
        | "profile" <expr>                        profiling
        | "verify" <expr>                         cost verific.
        | "trace" <expr1> <expr2>                 expr. tracing
        | "(" <expr> ")"                          grouping
        | "{" <expr> "}"                          macro expansion
        | "*"                                     ignored output


<constraint> ::=                                  time,heap(stack)
          <cexpr> [ "," <cexpr> [ "(" <cexpr> ")" ] ]

<cexpr> ::= <expr>                                constant expr.

<exprs> ::=
          <expr1> "," ... "," <exprn>             n >= 0

<matches> ::=
          <match1> "|" ... "|" <matchn>           n >= 1
```

```
<match> ::=
          <patt> "->" <expr>
```

Constants

```
<constant> ::=
          <intconst>
        | <floatconst>
        | <boolconst>
        | <charconst>
        | <stringconst>
        | <wordconst>
```

Patterns

```
<patt> :: =
          <constant>
        | <varid>                                  variable
        | "_"                                      wildcard
        | "[" <patts> "]"                          list pattern
        | "<<" <patts> ">>"                        vector pattern
        | "()"                                     empty tuple patt.
        | "(" <patt1> "," ... "," <pattn> ")"      n-tuple, n >= 2
        | <conid>                                  nullary constr.
        | <conid> <patt1> ... <pattn>              constr., n >= 1
        | "(" <patt> ")"                           grouping
        | "*"                                      ignored input
        | "_*"                                     ignored or
                                                   consumed input
        | <varid> "@" <patt>                       variable alias

<patts> ::=
          <patt0> "," ... "," <pattn>              n >= 0
```

Coordination language

```
<boxdecl> ::= "box" <boxid> <boxprelude> <body>

<boxprelude> ::=
          "in"  <inoutlist>
          "out" <inoutlist>
          [ "handles" <exnidlist> ]
          [ "within" <timeconst> ]

<inoutlist> ::=
        "(" <inout1> "," ... "," <inoutn> ")"      n >= 0

<inout> ::=                                        n >= 1
          <varid1> "," ... "," <varidn> "::" <type>
```

Boxes

```
<body> ::=
          ("match" | "fair" )
          <boxmatches>
          [ "handle" <handlers> ]

<handlers> ::=
          <handler1> "|" ... "|" <handlern>      n >= 1

<boxmatches> ::=
        <matches>

<handler> ::=
          <hpatt> "->" <cexpr>

<hpatt> ::=
          <exnid> <patt1> ... <pattn>            n >= 1
```

Wiring MetaLanguage

```
<wiringdecl> ::=
          "replicate" <wireid> "as" <wireid>
                      [ "*" <natconst> ]
        | "instantiate" <wireid> "as" <boxid>
                        [ "*" <natconst> ]
        | "macro" <mid> <id1> ... <idn> "=" <expr>        n >= 0
        | "initial" <wireid> <inits>
        | <templatedecl>
        | <wiredecl>
        | "for" <id> "=" <expr> "to" <expr> [ "except" <excepts> ]
            <wiringdecl>

<inits> ::=
          "(" <init1> "," ... "," <initn> ")"    n >= 0

<init> ::=  <wireid> "=" <expr>

<templateecl> ::= "template" <templateid> <prelude> <body>

<excepts> ::=
          "(" <expr1> "," ... "," <exprn> ")''   n >= 1
        | <id>
```

Wiring

```
<wiredecl> ::=
          "wire" <wireid> <sources> <dests>
        | "wire" <wireid> <idlist> "=" <wireid> <sources> <dests>
        | "wire" <link1> "to" <link2>

<sources>/<dests> ::=
        "(" <link1> "," ... "," <linkn> ")"     n >= 0
```

```
<link> ::=
          <linkspec> <linkprops>

<linkspec> ::=
          <connection>
        | <ioid>

<connection> ::= <boxid> "." <varid>

<linkprops> ::=
          <linkprop1> ... <linkpropn>

<linkprop> ::=
          "initially" <expr>
        | "trace"
        | "within" <timeconst>
        | "timeout" <timeconst>
```

Identifiers

```
<id>     ::= [ <modid> "." ] <localid>

<idlist> ::= "(" <id1> "," ... "," <idn> ")"     n >= 1

<varids> ::= <varid1> ... <varidn>               n >= 0

<exnidlist> ::= <exnid1> "," ... "," <exnidn>    n >= 1

<boxid>/<exnid>/<varid>/<conid>/<typeid>  ::= <id>
<modid> ::= <localid>
<streamid>/<portid>/<intid>/<fifoid>/<memid>      ::= <id>

<ioid>     ::= <streamid> | <portid> | <intid>
           |   <fifoid> | <memid>

<wireid>   ::= <id> | <id> "{" <expr> "}" | "{" <id> "}"
```

Lexical Syntax

```
<localid> ::= ("_" | <letter>) ( <letter> | <digit> ) *

<op> ::= ( "+" | "-" | "*" | "/" ... ) *

<intconst>      ::= <natconst> | "(-" <natconst> ")"
<natconst>      ::= <digit> +
<floatconst>    ::= <posfloatconst> | "(-" <posfloatconst> ")"
<posfloatconst> ::= <natconst> "." <natconst>
                      [ "e" ["+"|"-"] <natconst> ]
<boolconst>     ::= "true" | "false"
```

```
<charconst>     ::= "'" <char> "'"
<stringconst>   ::= """ <char> * """
<wordconst>     ::= "0x" <hexdigit> + | "(-0x" <hexdigit> + ")"
<timeconst>     ::= <natconst> <timedes>
<spaceconst>    ::= <natconst> <spacedes>
<timedes>       ::= "ps" | "ns" | "us" | "ms" | "s" | "min"
<spacedes>      ::= "B" | "KB" | "MB"
<char>          ::= "A" | ... | "Z" | " " | "\t" | "\n" | "\\" |
                    "\" <digit> + | "\0x" <hexdigit> +
```

Appendix B

Static Semantics

This appendix defines the static semantics of Hume, giving formal type rules etc.

B.1 Static Semantics: Notation

Except where noted, we use the same notation as the definition of Standard ML [58].

Our static semantics is given in terms of the semantic domain *SemVal* defined below. The notation $D^{(k)}$ is used to denote a sequence of k instances of D, DD, ..., DD^{k-1}.

BasVal and *BasCon* are fully defined in Section B.8. The function *coerceable* is defined with reference to the table in Section 2.1.3.

	BasVal =	$\{ (+), (==), \ldots \}$	Basic Values
	BasCon =	$\{ (:), \text{Nil}, \text{True}, \text{False}, \ldots \}$	Basic Constructors
	Con =	BasCon + con	Constructors
	Var =	BasCon + var	Variables
id $\in$	Id =	BasVal + Con + Var	Identifiers
E, E' $\in$	Env =	$\langle$ VarEnv, TyVarEnv $\rangle$	Environments
IE, VE, VE', SE $\in$	VarEnv =	$\{$ var $\mapsto$ PolyType $\}$	Variable Environments
TE $\in$	TypeEnv =	$\{ \chi \}$	Type Environments
AE $\in$	TyVarEnv =	$\{ \alpha \}$	Type Variable Environments
$\alpha, \beta \in$	TyVar		Type Variables
$\chi \in$	TyCon		Type Constructors
$\tau, \tau' \in$	Type =	TyVar + TyConType$^{(k)}$ +Type $\rightarrow$ Type	Monomorphic Types
$\sigma, \sigma' \in$	PolyType =	$\forall$ TyVar$^{(k)}$. Type	Polymorphic Types

Environments are unique maps. They are used by applying the environment to an identifier to give the corresponding entry in the map, for example if E is the environment $\{$ var $\mapsto$ v $\}$, then E (var) = v. The $m_1 \oplus m_2$ operation updates an environment mapping m_1 by the new mapping m_2. The domains of m_1 and m_2 must be disjoint (this introduces an implicit side-condition on each semantic rule that uses the $\oplus$ operation). The $m_1 \stackrel{\rightarrow}{\oplus} m_2$ operation is similar, but allows values in m_1 to be "shadowed" by those in m_2. It is therefore unnecessary for the domains of m_1 and m_2 to be disjoint. There are two degenerate environments, type environments (which are sets of type constructors) and type variable environments (which are sets of type variables). These environments simply record the presence or absence of their components in the environment, and are used as TE (χ), for example. Where an environment contains sub-environment, the notation E' E is used to select the sub-environment E' from E. The notation E $\oplus_{\text{E'}}$ E" updates subenvironment E' of E with the value E".

B.2 Static Semantics: Declarations

Declarations are processed to generate a *variable environment* (VE) mapping identifiers to types, and a *type environment* (TE) recording the arity of type constructors. Declarations may be self-recursive or mutually recursive.

$$\boxed{\mathrm{E} \vdash \mathrm{decls} \Rightarrow \mathrm{E}}$$

$$\frac{\forall i.\ 1 \leq i \leq n,\ \mathrm{E} \oplus \bigoplus_{j=1}^{n} \mathrm{E'}_j \vdash \mathrm{decl}_i \Rightarrow \mathrm{VE}_i, \mathrm{TE}_i}{\mathrm{E} \vdash \mathrm{decl}_1\ \ldots\ \mathrm{decl}_n \Rightarrow \mathrm{E} \oplus_{VE} (\bigoplus_{i=1}^{n} \mathrm{VE}_i) \oplus_{TE} (\bigoplus_{i=1}^{n} \mathrm{TE}_i)} \quad (1)$$

$$\boxed{\mathrm{E} \vdash \mathrm{decl} \Rightarrow \mathrm{VE}, \mathrm{TE}}$$

$$\frac{\mathrm{E} \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \tau \Rightarrow \sigma}{\mathrm{E} \vdash \texttt{foreign import}\ [\ \mathrm{s}\ ]\ [\ \mathrm{c}\ ]\ [\ \mathrm{str}\ ]\ \mathrm{var} :: \mathrm{type} \Rightarrow \{\ \mathrm{var} \mapsto \sigma\ \},\ \{\ \}} \quad (2)$$

$$\frac{\mathrm{E} \vdash \mathrm{var} \Rightarrow \sigma \qquad \mathrm{E} \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \tau \Rightarrow \sigma}{\mathrm{E} \vdash \texttt{foreign export}\ [\ \mathrm{c}\ ]\ [\ \mathrm{str}\ ]\ \mathrm{var} :: \mathrm{type} \Rightarrow \{\ \},\ \{\ \}} \quad (3)$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \sigma}{\mathrm{E} \vdash \texttt{constant}\ \mathrm{var}\ =\ \mathrm{exp} \Rightarrow \{\ \mathrm{var} \mapsto \sigma\ \},\ \{\ \}} \quad (4)$$

$$\frac{\begin{array}{c}(\mathrm{SE}\ \mathit{of}\ \mathrm{E})\ \mathrm{var'}\ =\ \forall\ \alpha_1\ \ldots\ \alpha_n.\ \tau \qquad [\mathrm{E} \vdash \mathrm{cexpr} \Rightarrow \tau] \\ \mathrm{E} \vdash \textbf{Port}\ \tau/\textbf{Stream}\ \tau/\textbf{Memory}\ \tau/\textbf{Fifo}\ \tau/\textbf{Interrupt}\ \tau \Rightarrow \sigma\end{array}}{\begin{array}{c}\mathrm{E} \vdash \texttt{port/stream/memory/fifo/interrupt}\ \mathrm{var}\ \texttt{from}\ \mathrm{var'}\ [\texttt{initial}\ \mathrm{cexpr}] \\ \Rightarrow \{\ \mathrm{var} \mapsto \sigma\ \},\ \{\ \}\end{array}} \quad (5)$$

$$\frac{\mathrm{E} \vdash \mathrm{matches} \Rightarrow \sigma \qquad \mathit{primrec}\ (\ \mathrm{var\ matches}\ )}{\mathrm{E} \vdash \mathrm{var\ matches} \Rightarrow \{\ \mathrm{var} \mapsto \sigma\ \},\ \{\ \}} \quad (6)$$

$$\frac{\mathrm{E} \vdash \mathrm{op}\ \mathrm{pat}_1\ \mathrm{pat}_2\ =\ \mathrm{exp} \Rightarrow \mathrm{VE}, \mathrm{TE}}{\mathrm{E} \vdash \mathrm{pat}_1\ \mathrm{op}\ \mathrm{pat}_2\ =\ \mathrm{exp} \Rightarrow \mathrm{VE}, \mathrm{TE}} \quad (7)$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \sigma}{\mathrm{E} \vdash \mathrm{var} \ = \ \mathrm{exp} \Rightarrow \{ \ \mathrm{var} \ \mapsto \ \sigma \ \}, \ \{ \ \}} \tag{8}$$

$$\frac{\mathrm{E} \vdash \mathrm{var} \Rightarrow \sigma \qquad \mathrm{E} \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \tau \Rightarrow \sigma}{\mathrm{E} \vdash \mathrm{var} :: \mathrm{type} \Rightarrow \{ \ \}, \ \{ \ \}} \tag{9}$$

$$\frac{\mathrm{E} \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathbf{Exn} \ \tau \Rightarrow \sigma}{\mathrm{E} \vdash \texttt{exception} \ \mathrm{exnid} \ \mathrm{type} \Rightarrow \{ \ \mathrm{exnid} \ \mapsto \ \sigma \ \}, \ \{ \ \}} \tag{10}$$

$$\frac{(\ \mathrm{E} \ \overrightarrow{\oplus}_{VE} \ (\bigoplus_{i=1}^{n} \{ \ \mathrm{var}_i \ \mapsto \ \alpha_i \ \} \ )) \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \tau \Rightarrow \sigma}{\mathrm{E} \vdash \texttt{type} \ \mathrm{typeid} \ \mathrm{var}_1 \ \ldots \ \mathrm{var}_n = \mathrm{type} \Rightarrow \{ \ \mathrm{typeid} \ \mapsto \ \sigma \ \}, \{ \ \}} \tag{11}$$

$$\frac{\begin{array}{c} \sigma \ = \ \forall \ \alpha_1 \ \ldots \ \alpha_n . \ \chi \ \alpha_1 \ \ldots \ \alpha_n \\ \mathrm{VE} \ = \ \{ \ \mathrm{typeid} \ \mapsto \ \sigma \ \} \qquad \mathrm{TE} \ = \ \{ \ \chi \ \} \\ ((\ \mathrm{E} \ \overrightarrow{\oplus}_{VE} \ (\bigoplus_{i=1}^{n} \{ \ \mathrm{var}_i \ \mapsto \ \alpha_i \ \} \ )) \ \oplus \ \mathrm{VE} \ ), \tau \vdash \mathrm{constrs} \Rightarrow \mathrm{VE'} \end{array}}{\mathrm{E} \vdash \texttt{data} \ \mathrm{typeid} \ \mathrm{var}_1 \ \ldots \ \mathrm{var}_n = \mathrm{constrs} \Rightarrow (\mathrm{VE} \ \oplus \ \mathrm{VE'}), \mathrm{TE}} \tag{12}$$

$$\frac{\forall i. \ 1 \leq i \leq n, \ (\mathrm{IE} \ of \ \mathrm{E}) \ (\mathrm{var}_i) \ = \ \sigma_i}{\mathrm{E} \vdash \texttt{import} \ \mathrm{modid} \ \mathrm{var}_1 \ \ldots \ \mathrm{var}_n \Rightarrow \bigoplus_{i=1}^{n} \{ \ \mathrm{var}_i \ \mapsto \ \sigma_i \ \}, \{ \ \}} \tag{13}$$

$$\frac{}{\mathrm{E} \vdash \texttt{export} \ \mathrm{var}_1 \ \ldots \ \mathrm{var}_n \Rightarrow \{ \ \}, \{ \ \}} \tag{14}$$

$\boxed{\mathrm{E} \vdash \mathrm{constrs} \Rightarrow \mathrm{VE}}$

$$\frac{\forall i. \ 1 \leq i \leq n, \ \mathrm{E}, \tau \vdash \mathrm{constr}_i \Rightarrow \mathrm{VE}_i}{\mathrm{E}, \tau \vdash \mathrm{constr}_1 \mid \ldots \mid \mathrm{constr}_n \Rightarrow \bigoplus_{i=1}^{n} \mathrm{VE}_i} \tag{15}$$

$\boxed{\mathrm{E} \vdash \mathrm{constr} \Rightarrow \mathrm{VE}}$

$$\frac{\forall i. \ 1 \leq i \leq n, \ \mathrm{E} \vdash \mathrm{type}_i \Rightarrow \tau_i' \qquad \mathrm{E} \vdash \tau_1' \rightarrow \ldots \rightarrow \tau_n' \rightarrow \tau \Rightarrow \sigma}{\mathrm{E}, \tau \vdash \mathrm{conid} \ \mathrm{type}_1 \ \ldots \ \mathrm{type}_n \Rightarrow \{ \ \mathrm{conid} \ \mapsto \ \sigma \ \}} \ n \ \geq \ 0 \tag{16}$$

B.3 Static Semantics: Programs and Wiring

$$\boxed{\text{IE} \vdash \text{program}}$$

$$\frac{\begin{array}{c}\text{E}_0 \ \oplus_{VE} \ \text{IE} \vdash \text{decls} \Rightarrow \text{E} \\ (((\text{E}_0 \overrightarrow{\oplus} \text{E}) \oplus_{VE} \text{IE}) \oplus_{VE} \text{SE}) \vdash \text{boxes} \Rightarrow \text{VE} \\ \text{VE} \vdash \text{wires}\end{array}}{\text{IE} \vdash \texttt{program}\ \text{decls boxes wires}} \tag{17}$$

$$\boxed{\text{E} \vdash \text{boxes} \Rightarrow \text{VE}}$$

$$\frac{\forall i.\ 1 < i \leq n, \quad \vdash \text{box}_i \Rightarrow \text{VE}_i}{\vdash \text{box}_1 \ \ldots \ \text{box}_n \Rightarrow \bigoplus_{i=1}^{n} \text{VE}_i} \tag{18}$$

$$\boxed{\vdash \text{box} \Rightarrow \text{VE}}$$

$$\frac{\begin{array}{ccc}\text{E} \vdash \text{body} \Rightarrow \tau \to \tau' & \text{E} \vdash \text{ins} \Rightarrow \tau & \text{E} \vdash \text{outs} \Rightarrow \tau' \\ \multicolumn{3}{c}{\text{E} \vdash \tau \to \tau' \Rightarrow \sigma}\end{array}}{\vdash \texttt{box}\ \text{boxid ins outs body} \Rightarrow \{\ \text{boxid} \ \mapsto \ \sigma\ \}} \tag{19}$$

$$\boxed{\text{E} \vdash \text{wires}}$$

$$\frac{\forall i.\ 1 < i \leq n, \quad \vdash \text{wire}_i}{\vdash \text{wire}_1 \ \ldots \ \text{wire}_n} \tag{20}$$

$$\boxed{\vdash \text{wire}}$$

$$\frac{\mathrm{E} \vdash \text{sources} \Rightarrow \tau \qquad \mathrm{E} \vdash \text{dests} \Rightarrow \tau' \qquad \mathrm{E} \vdash \text{boxid} \Rightarrow \tau \to \tau'}{\vdash \texttt{wire}\ \text{boxid sources dests}} \tag{21}$$

$$\boxed{\mathrm{E} \vdash \text{body} \Rightarrow \tau}$$

$$\frac{\mathrm{E} \vdash \text{time} \Rightarrow \textbf{Time} \qquad \mathrm{E} \vdash \text{matches} \Rightarrow \tau \to \tau' \qquad \mathrm{E} \vdash \text{handlers} \Rightarrow \tau'}{\mathrm{E}, \text{vs} \vdash \texttt{timeout}\ \text{time matches}\ \texttt{handle}\ \text{handles} \Rightarrow \tau \to \tau'} \tag{22}$$

B.4 Static Semantics: Expressions

The first rule generalises the types of expressions from monotypes to polytypes. The second determines the type of a variable using the variable environment.

$$\boxed{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \sigma}$$

$$\frac{(\mathrm{VE}\ \mathit{of}\ \mathrm{E})\ (\mathrm{id}) \ = \ \sigma}{\mathrm{E} \vdash \mathrm{id} \Rightarrow \sigma} \tag{23}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau \qquad \mathrm{E} \vdash \tau \Rightarrow \sigma}{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \sigma}\ \mathrm{exp} \notin \mathrm{Id} \tag{24}$$

$$\boxed{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau}$$

$$\frac{\mathrm{E} \vdash \mathrm{id} \Rightarrow \forall\ \alpha_1\ \ldots\ \alpha_n.\ \tau \qquad \forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \tau_i}{\mathrm{E} \vdash \mathrm{id} \Rightarrow \tau[\tau_1/\alpha_1, \ldots, \tau_n/\alpha_n]} \tag{25}$$

$$\frac{}{\mathrm{E} \vdash \mathrm{char} \Rightarrow \mathbf{Char}} \tag{26}$$

$$\frac{}{\mathrm{E} \vdash \mathrm{string} \Rightarrow \mathbf{String}} \tag{27}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{con/var} \Rightarrow \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau' \\ \forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \tau_i\end{array}}{\mathrm{E} \vdash \mathrm{con/var}\ \mathrm{exp}_1\ \ldots\ \mathrm{exp}_n \Rightarrow \tau'}\ n \ > \ 0 \tag{28}$$

$$\frac{\mathrm{E} \vdash \forall i.\ 1 \leq i \leq n,\ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \tau \Rightarrow \mathbf{List}\ \tau}{\mathrm{E} \vdash [\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ] \Rightarrow \mathbf{List}\ \tau}\ \mathrm{n} \geq 1 \tag{29}$$

$$\frac{}{\mathrm{E} \vdash [\ ] \Rightarrow \mathbf{List}\ \tau} \tag{30}$$

$$\frac{}{\mathrm{E} \vdash () \Rightarrow \mathbf{Tuple}_0} \tag{31}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \tau_i}{\mathrm{E} \vdash (\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ) \Rightarrow \mathbf{Tuple}_n\ \tau_1\ \ldots\ \tau_n} \tag{32}$$

$$\frac{}{\mathrm{E} \vdash << \ >> \Rightarrow \mathbf{Vector}\ \tau} \tag{33}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \tau}{\mathrm{E} \vdash << \ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ >> \Rightarrow \mathbf{Vector}\ \tau} \tag{34}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{match} \Rightarrow \tau \rightarrow \tau'}{\mathrm{E} \vdash \texttt{case}\ \mathrm{exp}\ \texttt{of}\ \mathrm{match} \Rightarrow \tau'} \tag{35}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp}_1 \Rightarrow \mathbf{Bool} \qquad \mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{exp}_3 \Rightarrow \tau}{\mathrm{E} \vdash \texttt{if}\ \mathrm{exp}_1\ \texttt{then}\ \mathrm{exp}_2\ \texttt{else}\ \mathrm{exp}_3 \Rightarrow \tau} \tag{36}$$

$$\frac{\mathrm{E} \vdash \mathrm{decls} \Rightarrow \mathrm{E'} \qquad \mathrm{E} \stackrel{\rightarrow}{\oplus} \mathrm{E'} \vdash \mathrm{exp} \Rightarrow \tau}{\mathrm{E} \vdash \texttt{let}\ \mathrm{decls}\ \texttt{in}\ \mathrm{exp} \Rightarrow \tau} \tag{37}$$

$$\frac{\mathrm{E} \vdash \mathrm{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau}{\mathrm{E} \vdash \mathrm{exp} :: \mathrm{type} \Rightarrow \tau} \tag{38}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{type} \Rightarrow \tau' \qquad \textit{coerceable}\ (\ \tau,\ \tau'\ )}{\mathrm{E} \vdash \mathrm{exp}\ \mathrm{as}\ \mathrm{type} \Rightarrow \tau'} \tag{39}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{exnid} \Rightarrow \mathbf{Exn}\ \tau}{\mathrm{E} \vdash \texttt{raise}\ \mathrm{exnid}\ \mathrm{exp} \Rightarrow \tau'} \tag{40}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \mathbf{Time} \qquad \mathrm{E} \vdash \mathrm{exp}_1 \Rightarrow \tau}{\mathrm{E} \vdash \mathrm{exp}_1\ \texttt{within}\ \mathrm{exp}_2[\texttt{raise}\mathrm{exnid}] \Rightarrow \tau} \tag{41}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau}{\mathrm{E} \vdash \texttt{profile}\ \mathrm{exp} \Rightarrow \tau} \tag{42}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau}{\mathrm{E} \vdash \texttt{verify}\ \mathrm{exp} \Rightarrow \tau} \tag{43}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \tau}{\mathrm{E} \vdash (\ \mathrm{exp}\ ) \Rightarrow \tau} \tag{44}$$

B.5 Static Semantics: Matches

$$\boxed{\mathrm{E} \vdash \mathrm{match} \Rightarrow \tau}$$

$$\frac{\mathrm{E} \vdash \{\ \mathrm{match}\ \} \Rightarrow \tau \qquad \mathrm{E} \vdash \{\ \mathrm{matches}\ \} \Rightarrow \tau}{\mathrm{E}, \mathrm{v} \vdash \{\ \mathrm{match} \mid \mathrm{matches}\ \} \Rightarrow \tau} \tag{45}$$

$$\frac{\begin{array}{c}\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{match}_i \Rightarrow \tau_i, \mathrm{VE}_i \\ \mathrm{E} \stackrel{\rightarrow}{\oplus}_{VE} (\bigoplus_{i=1}^{n} \mathrm{VE}_i) \vdash \mathrm{exp} \Rightarrow \tau'\end{array}}{\mathrm{E} \vdash \{\ \mathrm{pat}_1\ \ldots\ \mathrm{pat}_n\ \rightarrow\ \mathrm{exp}\} \Rightarrow \tau_1 \rightarrow\ \ \ldots \rightarrow \tau_n \rightarrow \tau'} \tag{46}$$

$$\boxed{\mathrm{E} \vdash \mathrm{pat} \Rightarrow \tau, \mathrm{VE}}$$

$$\frac{}{\mathrm{E} \vdash \_ \Rightarrow \tau, \{\ \}} \tag{47}$$

$$\frac{}{\mathrm{E} \vdash \mathrm{var} \Rightarrow \tau, \{\ \mathrm{var}\ \mapsto\ \tau\ \}} \tag{48}$$

$$\frac{\mathrm{E} \vdash \mathrm{con} \Rightarrow \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau' \qquad \forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{pat}_i \Rightarrow \tau_i, \mathrm{VE}_i}{\mathrm{E} \vdash \mathrm{con}\ \mathrm{pat}_1\ \ldots\ \mathrm{pat}_n \Rightarrow \tau', \bigoplus_{i=1}^{n} \mathrm{VE}_i} \tag{49}$$

$$\frac{}{\mathrm{E} \vdash () \Rightarrow \mathbf{Tuple}_0\ , \{\ \}} \tag{50}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{pat}_i \Rightarrow \tau_i, \mathrm{VE}_i}{\mathrm{E} \vdash (\ \mathrm{pat}_1,\ \ldots,\ \mathrm{pat}_n\ ) \Rightarrow \mathbf{Tuple}_n\ \tau_1\ \ldots\ \tau_n, \bigoplus_{i=1}^{n} \mathrm{VE}_i} \tag{51}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{pat}_i \Rightarrow \tau, \mathrm{VE}_i}{\mathrm{E} \vdash <\ \mathrm{pat}_1,\ \ldots,\ \mathrm{pat}_n\ > \Rightarrow \mathbf{Vector}\ \tau, \bigoplus_{i=1}^{n} \mathrm{VE}_i} \tag{52}$$

B.5.1 Static Semantics: Exception Handler Matches

$$\frac{\mathrm{E} \vdash \mathrm{exnid} \Rightarrow \mathbf{Exn}\ \tau \qquad \mathrm{E} \vdash \mathrm{pat} \Rightarrow \tau, \mathrm{VE} \qquad \mathrm{E} \overrightarrow{\oplus}_{VE}\ \mathrm{VE} \vdash \mathrm{exp} \Rightarrow \tau'}{\mathrm{E} \vdash \mathrm{exnid\ pat}\ \rightarrow\ \mathrm{exp} \Rightarrow \tau'} \tag{53}$$

$$\frac{\mathrm{E} \vdash \mathrm{handler} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathrm{handlers} \Rightarrow \tau}{\mathrm{E} \vdash \mathrm{handler} \mid \mathrm{handlers} \Rightarrow \tau} \tag{54}$$

B.6 Static Semantics: Type Expressions

$$\boxed{\mathrm{E} \vdash \mathrm{type} \Rightarrow \tau}$$

$$\frac{(\mathrm{VE}\ \mathit{of}\ \mathrm{E})\ (\mathit{tyvar})\ =\ \alpha}{\mathrm{E} \vdash \mathrm{tyvar} \Rightarrow \alpha} \tag{55}$$

$$\frac{\begin{array}{c}(\mathrm{VE}\ \mathit{of}\ \mathrm{E})\ (\mathit{tycon})\ =\ \forall\ \alpha_1\ \ldots\ \alpha_n.\chi\ \alpha_1\ \ldots\ \alpha_n \\ \forall i.\ 1 \leq i \leq n,\ \mathrm{E} \vdash \mathrm{type}_i \Rightarrow \tau_i\end{array}}{\mathrm{E} \vdash \mathrm{tycon\ type}_1\ \ldots\ \mathrm{type}_n \Rightarrow \chi\ \tau_1\ \ldots\ \tau_n} \tag{56}$$

$$\frac{\mathrm{E} \vdash \mathit{type} \Rightarrow \tau \qquad \mathrm{E} \vdash \mathit{type} \Rightarrow \tau'}{\mathrm{E} \vdash \mathrm{type}\ \rightarrow\ \mathrm{type'} \Rightarrow \tau \rightarrow \tau'} \tag{57}$$

$$\frac{\mathrm{E} \vdash \mathit{type} \Rightarrow \tau}{\mathrm{E} \vdash (\mathrm{type}) \Rightarrow \tau} \tag{58}$$

B.7 Static Semantics: Types

$$\boxed{\mathrm{E} \vdash \tau}$$

$$\frac{(\mathrm{AE}\ \mathit{of}\ \mathrm{E})\ \alpha\ =\ n}{\mathrm{E} \vdash \alpha} \tag{59}$$

$$\frac{(\mathrm{TE}\ \mathit{of}\ \mathrm{E})\ \chi\ =\ n \qquad \forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \tau_i}{\mathrm{E} \vdash \chi\ \tau_1\ \ldots\ \tau_n} \tag{60}$$

$$\frac{\mathrm{E} \vdash \tau \Rightarrow \qquad \mathrm{E} \vdash \tau' \Rightarrow}{\mathrm{E} \vdash \tau \to \tau' \Rightarrow} \tag{61}$$

$$\boxed{\mathrm{E} \vdash \sigma}$$

$$\frac{\mathrm{E}\ \oplus_{AE}\ \{\ \alpha_1,\ \ldots,\ \alpha_n\ \} \vdash \tau}{\mathrm{E} \vdash \forall\ \alpha_1\ \ldots\ \alpha_n.\ \tau} \tag{62}$$

$$\boxed{\mathrm{E} \vdash \tau \Rightarrow \sigma}$$

$$\frac{\mathrm{E} \vdash \forall\ \alpha_1\ \ldots\ \alpha_n.\ \tau}{\mathrm{E} \vdash \tau \Rightarrow \forall\ \alpha_1\ \ldots\ \alpha_n.\ \tau} \tag{63}$$

B.8 Static Semantics: The Initial Environment

The initial environment used in the static semantics comprises type bindings for all values defined in the module *Prelude*, including functions, data constructors, type constructors and exceptions, plus bindings for basic values as given below.

The initial variable environment contains types for the following functions (*BasVal*):

PrimPlusInt $\mapsto$ **Int** $\to$ **Int**
PrimMulInt $\mapsto$ **Int** $\to$ **Int**
...

plus types for the standard constructors (*BasCon*):

$0 \mapsto$ **Int** , $1 \mapsto$ **Int** , ..., $0.0 \mapsto$ **Float** , $0.1 \mapsto$ **Float** , ...,
True $\mapsto$ **Bool** , False $\mapsto$ **Bool** , 'a' $\mapsto$ **Char** , ...,
$(:) \mapsto \forall\ \alpha.\ \alpha \to$ **List** $\alpha \to$ **List** α, Nil $\mapsto$ **List** α

Appendix C

Dynamic Semantics

This appendix defines the Hume dynamic semantics using an axiomatic style. It is divided into five parts: i) overview and definitions; ii) the semantics of declarations; iii) the semantics of processes; iv) the semantics of expressions; and v) the semantics of pattern matches. The semantics assumes that all static checks and translations defined by the static semantics are valid and have been properly carried out.

C.1 Limitations

There are a number of limitations on the semantics given here. Firstly, we do not consider the semantics of imported values. This can be added straightforwardly by extending the initial value environment with bindings for the imported values. Secondly, the semantics of processes assumes that all active processes are scheduled for precisely one step. The status of all processes is then reassessed to determine whether each process is active or inactive. A more flexible semantics would schedule precisely one active process. This modification should not be too hard to incorporate into the semantics. Thirdly, we need to define the semantics of the *timecost*, *stackcost*, *heapcost* and *coerce* functions which are used to calculate timeouts and type coercions respectively. We anticipate that the semantics of type coercions can be defined without great difficulty. We are in the process of developing formal analyses for providing upper bound on stack and heap usage for Hume programs, including primitive recursion. We anticipate that it will be possible to extend these analyses to cover time using analytical techniques developed for other real-time languages [7, 18]. Fourthly, we have not defined the semantics for interrupts. Clearly a polling semantics is not ideal for such objects, though they may possess a similar semantics to other kinds of I/O operation? Finally, the dynamic semantics is currently defined only for the synchronous language (i.e. omitting fair matches and $*$), and does not consider higher-order functions. We anticipate extending the semantics to cover these constructs in due course.

C.2 Dynamic Semantics: Notation

The dynamic semantics uses a similar style to that used for the static semantics in Appendix B. Our semantics is given in terms of the semantic domain *SemVal* defined below. We use $\langle \ldots \rangle$ to enclose semantic tuples in the *SemVal* domain. This avoids confusion with the syntactic tuple domains, and allows the direct representation of 1-tuples where necessary. The notation D^* is used to define the domain of all tuples of D: $\langle\rangle$, $\langle D \rangle$, $\langle D, D \rangle$, $\ldots$

BasVal and *BasCon* are fully defined in Section C.7.

	BasVal =	$\{$ PrimPlusInt, PrimEqInt, $\ldots$ $\}$	Basic Values
	BasCon =	$\{$ (:), Nil, True, False, $\ldots$ $\}$	Basic Constructors
$c \in$	Con =	BasCon + con	
$t, v, vs \in$	SemVal =	BasVal + Con SemVal*+ SemVal* + Exn + matches	Semantic Values
E $\in$	Env =	$\langle$ VarEnv, SysEnv $\rangle$	Environments
IE, VE $\in$	VarEnv =	$\{$ var $\mapsto$ SemVal $\}$	Value Environments
SE $\in$	SysEnv =	$\{$ var $\mapsto$ SemVal* $\}$	System Environment
$b \in$	*bool* =	$\{$ *true*, *false* $\}$	Booleans
W $\in$	Wire =	$\{$ var $\mapsto \langle$var*, var* $\rangle$ $\}$	Wires
I, A, P $\in$	Process =	$\{$ Proc $\}$	Processes
	Proc =	$\langle$ var, SemVal*, SemVal*, exp $\rangle$	Process
x $\in$	Exn =	$\langle$ var, SemVal $\rangle$	Exceptions

Environments are unique maps from identifiers to values. They are used by applying the environment to an identifier to give the corresponding entry in the map, for example if E is the environment $\{$ var $\mapsto$ v $\}$, then E (var) = v. The $m_1 \oplus m_2$ operation updates an environment mapping m_1 by the new mapping m_2. The $m_1 \stackrel{\rightarrow}{\oplus} m_2$ operation is similar, but allows values in m_1 to be "shadowed" by those in m_2. Conversely, $e \ominus m$ removes the mapping m from an environment e.

C.3 Dynamic Semantics: Declarations

Declarations are processed to generate an initial environment mapping identifiers to initial values. This environment is used in the dynamic semantics for expressions to determine the value of identifers in function applications and variable expressions (rules 99, 94) and in the semantics of boxes to determine the value attached to an I/O object (rule 90). Declarations may be self-recursive or mutually recursive.

$$\boxed{\mathrm{E} \vdash \mathrm{decls} \Rightarrow \mathrm{E}}$$

$$\frac{\forall i.\ 1 \leq i \leq n,\ \mathrm{E} \oplus \bigoplus_{j=1}^{n} \mathrm{E'}_j \vdash \mathrm{decl}_i \Rightarrow \mathrm{E'}_i}{\mathrm{E} \vdash \mathrm{decl}_1\ \ldots\ \mathrm{decl}_n \Rightarrow \mathrm{E} \oplus \bigoplus_{i=1}^{n} \mathrm{E'}_i} \tag{64}$$

Each declaration is processed to produce a corresponding value environment.

$$\boxed{\mathrm{E} \vdash \mathrm{decl} \Rightarrow \mathrm{VE}}$$

$$\frac{}{\mathrm{E} \vdash \texttt{import}\mathrm{modid}\ \mathrm{var}_1\ \ldots\ \mathrm{var}_n \Rightarrow \{\ \}} \tag{65}$$

$$\frac{}{\mathrm{E} \vdash \texttt{export}\ \mathrm{var}_1\ \ldots\ \mathrm{var}_n \Rightarrow \{\ \}} \tag{66}$$

$$\frac{}{\mathrm{E} \vdash \texttt{foreign import}\ [\ \mathrm{s}\ ]\ [\ \mathrm{c}\ ]\ [\ \mathrm{str}\ ]\ \mathrm{var} :: \mathrm{type} \Rightarrow \{\ \}} \tag{67}$$

$$\frac{}{\mathrm{E} \vdash \texttt{foreign export}\ [\ \mathrm{c}\ ]\ [\ \mathrm{str}\ ]\ \mathrm{var} :: \mathrm{type} \Rightarrow \{\ \}} \tag{68}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{constant}\ \mathrm{id}\ =\ \mathrm{exp} \Rightarrow \{\ \mathrm{id}\ \mapsto\ \mathrm{v}\ \}} \tag{69}$$

$$\frac{(\mathrm{SE}\ \textit{of}\ \mathrm{E})\ \mathrm{id'}\ =\ \mathrm{vs}}{\mathrm{E} \vdash \texttt{port/stream/memory/fifo}\ \mathrm{id}\ \texttt{from}\ \mathrm{id'} \Rightarrow \{\ \mathrm{id}\ \mapsto\ \langle\ \texttt{true}, \mathrm{vs}\ \rangle\ \}} \tag{70}$$

$$\frac{\mathrm{E} \vdash \mathrm{cexpr} \Rightarrow \mathrm{v} \qquad (\mathrm{SE}\ \textit{of}\ \mathrm{E})\ \mathrm{id'}\ =\ \mathrm{vs} \qquad \mathrm{vs'}\ =\ \langle\ \mathrm{v},\ \mathrm{vs}\ \rangle}{\begin{array}{c}\mathrm{E} \vdash \texttt{port/stream/memory/fifo}\ \mathrm{id}\ \texttt{from}\ \mathrm{id'}\ \texttt{initial}\ \mathrm{cexpr} \\ \Rightarrow \{\ \mathrm{id}\ \mapsto\ \langle\ \texttt{true}, \mathrm{vs'}\ \rangle\ \}\end{array}} \tag{71}$$

$$\frac{}{\text{E} \vdash \text{var matches} \Rightarrow \{\ \text{var} \mapsto \text{matches}\ \}} \tag{72}$$

$$\frac{\text{E} \vdash \text{op pat}_1\ \text{pat}_2\ =\ \text{exp} \Rightarrow \text{E'}}{\text{E} \vdash \text{pat}_1\ \text{op pat}_2\ =\ \text{exp} \Rightarrow \text{E'}} \tag{73}$$

$$\frac{\text{E} \vdash \text{exp} \Rightarrow \text{v}}{\text{E} \vdash \text{var}\ =\ \text{exp} \Rightarrow \{\ \text{var} \mapsto \text{v}\ \}} \tag{74}$$

$$\frac{}{\text{E} \vdash \text{var} :: \text{type} \Rightarrow \{\ \}} \tag{75}$$

...

C.4 Dynamic Semantics: Processes

The dynamic semantics of a Hume program is given by the dynamic semantics of the boxes that are defined in the program. This semantics is produced in the context of the declarations and wirings that are specified in that program plus the initial environment of prelude bindings and imported values. The result of a Hume program is a new environment reflecting the state of new bindings in the system or value environments.

$$\boxed{\mathrm{SE}, \mathrm{IE} \vdash \text{program} \Rightarrow \mathrm{E}}$$

$$\frac{\mathrm{E}_0 \oplus \mathrm{IE} \vdash \text{decls} \Rightarrow \mathrm{E} \qquad \vdash \text{boxes} \Rightarrow \mathrm{P} \qquad \vdash \text{wires} \Rightarrow \mathrm{W} \qquad ((\mathrm{E}_0 \overrightarrow{\oplus}\, \mathrm{E}) \oplus \mathrm{IE} \oplus \mathrm{SE}),\ \mathrm{W} \vdash \mathrm{P} \Rightarrow \mathrm{E'}}{\mathrm{SE}, \mathrm{IE} \vdash \texttt{program}\ \text{decls boxes wires} \Rightarrow \mathrm{E'}} \tag{76}$$

Box declarations are processed to give a set of initial processes, P.

$$\boxed{\vdash \text{boxes} \Rightarrow \mathrm{P}}$$

$$\frac{\forall i.\ 1 < i \leq n, \quad \vdash \text{box}_i \Rightarrow \mathrm{P}_i}{\vdash \text{box}_1\ \ldots\ \text{box}_n \Rightarrow \bigcup_{i=1}^{n} \mathrm{P}_i} \tag{77}$$

$$\boxed{\vdash \text{box} \Rightarrow \mathrm{P}}$$

$$\frac{}{\vdash \texttt{box}\ \text{boxid ins outs body} \Rightarrow \{\ \langle\ \text{boxid}, \text{ins}, \text{outs}, \text{body}\ \rangle\ \}} \tag{78}$$

`wiring` declarations are processed to give the wiring layout mapping the outputs of boxes or I/O operations to the inputs of other boxes.

$$\boxed{\vdash \text{wires} \Rightarrow \mathrm{W}}$$

$$\frac{\forall i.\ 1 < i \leq n, \quad \vdash \text{wire}_i \Rightarrow \mathrm{W}_i}{\vdash \text{wire}_1\ \ldots\ \text{wire}_n \Rightarrow \bigcup_{i=1}^{n} \mathrm{W}_i} \tag{79}$$

$$\boxed{\vdash \text{wire} \Rightarrow \mathrm{W}}$$

$$\frac{\mathrm{W} \;=\; \{\; \mathrm{boxid} \;\mapsto\; \langle\; \mathrm{sources}, \mathrm{dests} \;\rangle\; \}}{\vdash \texttt{wire}\ \mathrm{boxid}\ \mathrm{sources}\ \mathrm{dests} \;\Rightarrow\; \mathrm{W}} \tag{80}$$

The set of processes is split into active (A) and inactive processes (I). A process is active if input is available on all its input channels, *or* if a timeout has been raised on any input channel.

$$\boxed{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \;\Rightarrow\; \mathrm{P}, \mathrm{P}}$$

$$\frac{\forall i.\ 1 \leq i \leq n,\ \mathrm{E}, \mathrm{W} \vdash \mathrm{P}_i \;\Rightarrow\; \mathrm{I}_i, \mathrm{A}_i \qquad \mathrm{I} \;=\; \bigcup_{i=1}^{n} \mathrm{I}_i \qquad \mathrm{A} \;=\; \bigcup_{i=1}^{n} \mathrm{A}_i}{\mathrm{E}, \mathrm{W} \vdash \{\; \mathrm{P}_1, \ldots, \mathrm{P}_n \;\} \;\Rightarrow\; \mathrm{I}, \mathrm{A}} \tag{81}$$

Rules 82–85 determine whether individual inputs are available or have timed out.

$$\boxed{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \;\Rightarrow\; \mathrm{P}, \mathrm{P}}$$

$$\frac{\begin{array}{c}\mathrm{P} \;=\; \langle\; \mathrm{boxid}, \mathrm{ins}, \mathrm{outs}, \mathrm{body} \;\rangle \qquad \mathrm{W}\ (\mathrm{boxid}) \;=\; \langle\; \mathrm{wins}, \mathrm{wouts} \;\rangle \\ \mathrm{E} \vdash \mathrm{wins} \;\Rightarrow\; \mathrm{b}, \mathrm{b'} \qquad \mathrm{I}, \mathrm{A} \;=\; \mathit{if}\ b \;\vee\; b'\ \mathit{then}\ \{\;\}, \{\; \mathrm{P} \;\}\mathit{else}\ \{\; \mathrm{P} \;\}, \{\;\}\end{array}}{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \;\Rightarrow\; \mathrm{I}, \mathrm{A}} \tag{82}$$

$$\boxed{\mathrm{E} \vdash \mathrm{ids} \;\Rightarrow\; \mathit{bool}, \mathit{bool}}$$

$$\frac{\mathrm{E} \vdash \mathrm{id}_1 \;\Rightarrow\; \mathit{true}, \mathrm{b} \qquad \mathrm{E} \vdash \mathrm{id}_2 \;\ldots\; \mathrm{id}_n \;\Rightarrow\; \mathrm{b'}, \mathrm{b''}}{\mathrm{E} \vdash \mathrm{id}_1 \;\ldots\; \mathrm{id}_n \;\Rightarrow\; \mathrm{b'},\ (\mathrm{b} \;\vee\; \mathrm{b''})} \tag{83}$$

$$\frac{\mathrm{E} \vdash \mathrm{id}_1 \;\Rightarrow\; \mathit{false}, \mathrm{b} \qquad \mathrm{E} \vdash \mathrm{id}_2 \;\ldots\; \mathrm{id}_n \;\Rightarrow\; \mathrm{b'}, \mathrm{b''}}{\mathrm{E} \vdash \mathrm{id}_1 \;\ldots\; \mathrm{id}_n \;\Rightarrow\; \mathit{false},\ (\mathrm{b} \;\vee\; \mathrm{b''})} \tag{84}$$

$$\boxed{\mathrm{E} \vdash \mathrm{id} \;\Rightarrow\; \mathit{bool}, \mathit{bool}}$$

$$\frac{\begin{array}{c}\mathrm{E}\ (\mathrm{id}) \;=\; \langle\; \mathrm{b},\ \mathrm{vs} \;\rangle \\ \mathrm{b'} \;=\; \mathit{if}\ \mathrm{vs} \;=\; \langle\rangle \;\vee\; \mathit{hd}\ \mathrm{vs} \;\neq\; \langle\; \mathrm{Timeout}, \langle\;\rangle \;\rangle\ \mathit{then\ false\ else\ true}\end{array}}{\mathrm{E} \vdash \mathrm{id} \;\Rightarrow\; \mathrm{b}, \mathrm{b'}} \tag{85}$$

Processes are split into active/inactive sets, and all active processes are scheduled for one step, yielding a new environment.

$$\boxed{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \Rightarrow \mathrm{E}}$$

$$\frac{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \Rightarrow \mathrm{I}, \mathrm{A} \qquad \mathrm{E}, \mathrm{W} \vdash \mathrm{I}, \mathrm{A} \Rightarrow \mathrm{E'}}{\mathrm{E}, \mathrm{W} \vdash \mathrm{P} \Rightarrow \mathrm{E'}} \tag{86}$$

Processes are scheduled repeatedly until the set of active processes becomes empty.

$$\boxed{\mathrm{E}, \mathrm{W} \vdash \mathrm{P}, \mathrm{P} \Rightarrow \mathrm{E}}$$

$$\frac{\mathrm{E}, \mathrm{W} \vdash \mathrm{I}, \mathrm{A} \Rightarrow \mathrm{E'}, \mathrm{I'}, \mathrm{A'} \qquad \mathrm{E'}, \mathrm{W} \vdash \mathrm{I'}, \mathrm{A'} \Rightarrow \mathrm{E''}}{\mathrm{E}, \mathrm{W} \vdash \mathrm{I}, \mathrm{A} \Rightarrow \mathrm{E''}, \mathrm{I'}, \mathrm{A'}} \ \mathrm{A} \neq \{\,\} \tag{87}$$

When there are no further active processes, the program terminates.

$$\frac{}{\mathrm{E}, \mathrm{W} \vdash \mathrm{I}, \{\,\} \Rightarrow \mathrm{E}} \tag{88}$$

Each active process is executed for one step and the output redirected to the input specified in the wiring specification. All processes are then reassessed to determine their new activity status.

$$\boxed{\mathrm{E}, \mathrm{W} \vdash \mathrm{P}, \mathrm{P} \Rightarrow \mathrm{E}, \mathrm{P}, \mathrm{P}}$$

$$\forall i.\ 1 \leq i \leq |\mathrm{A}|,\ \mathrm{E}, \mathrm{W} \vdash \mathrm{A}_i \Rightarrow \mathrm{outs}_i,\ \mathrm{E}_i^I, \mathrm{E}_i^O$$

$$\mathrm{E'} = \bigcup_{i=1}^{|\mathrm{A}|} \mathrm{E}_i^I \ \vec{\oplus}\ \bigcup_{i=1}^{|\mathrm{A}|} \mathrm{E}_i^O$$

$$\frac{\mathrm{E} \ \vec{\oplus}\ \mathrm{E'}, \mathrm{W} \vdash \mathrm{I} \cup \mathrm{A} \Rightarrow \mathrm{I'}, \mathrm{A'}}{\mathrm{E}, \mathrm{W} \vdash \mathrm{I}, \mathrm{A} \Rightarrow (\mathrm{E} \ \vec{\oplus}\ \mathrm{E'}), \mathrm{I'}, \mathrm{A'}} \tag{89}$$

A process is executed by determining the value of each of its inputs, and then executing the body of the process in the context of those values. The new values of the inputs and outputs are returned.

$$\boxed{\mathrm{E} \vdash \mathrm{P} \Rightarrow \mathrm{v}, \mathrm{E}, \mathrm{E}}$$

$$\frac{\begin{array}{c}\mathrm{W}\ (\mathrm{boxid}) = \langle\ \mathrm{wins}, \mathrm{wouts}\ \rangle \\ n = |\mathrm{wins}| \\ \mathrm{SE} = SE\ of\ E \\ \mathrm{vs} = \langle\ snd(SE\ (\mathrm{wins}_1)),\ \ldots,\ snd(SE\ (\mathrm{wins}_n))\ \rangle \\ \mathrm{E}, \mathrm{vs} \vdash \mathrm{body} \Rightarrow \mathrm{vs'} \\ \mathrm{SE}^I = \{\ \forall i.\ 1 \leq i \leq n,\ \mathrm{wins}_i \mapsto \langle\ isport\ \mathrm{wins}_i, tl\ \mathrm{vs}_i\ \rangle\ \} \\ \mathrm{SE}^O = \{\ \forall i.\ 1 \leq i \leq |\mathrm{wouts}|,\ \mathrm{wouts}_i \mapsto \langle\ true, [\mathrm{vs'}_i]\ \rangle\ \}\end{array}}{\mathrm{E}, \mathrm{W} \vdash \langle\ \mathrm{boxid}, \mathrm{ins}, \mathrm{outs}, \mathrm{body}\ \rangle \Rightarrow \mathrm{vs'}, \mathrm{SE}^I, \mathrm{SE}^O} \tag{90}$$

The final set of process rules define the semantics of executing a single box body. There are three cases, corresponding to normal execution, an exception or a timeout respectively. In order to implement fair matching, the new rule ordering returned by the match rule should update the definition of the matches for the box in the environment. In this way, each successful fair match will change the rule ordering, thereby ensuring that each rule is matched equally, as required by the semantics.

$$\boxed{\mathrm{E}, \mathrm{v} \vdash \mathrm{body} \Rightarrow \mathrm{v}}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{time} \Rightarrow \mathrm{t} \qquad timecost\ (\ \mathrm{E}, \mathrm{matches}\ (\mathrm{vs})\ ) < \mathrm{t} \\ \mathrm{E}, \mathrm{vs} \models \mathrm{matches} \Rightarrow \mathrm{v}, \mathrm{matches'}\end{array}}{\vdash \mathrm{E}, \mathrm{vs} \Rightarrow \ \texttt{timeout}\ \mathrm{time}\ \mathrm{matches}\ \texttt{handle}\ \mathrm{handlesv}} \ v \notin \mathrm{Exn} \tag{91}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{time} \Rightarrow \mathrm{t} \qquad \mathit{timecost}\ (\ \mathrm{E}, \mathrm{matches}\ (\mathrm{vs})\ ) \ < \ \mathrm{t} \\ \mathrm{E}, \mathrm{vs} \vdash \mathrm{matches} \Rightarrow \mathrm{v} \\ \mathrm{E}, \mathrm{v} \models \mathrm{handle} \Rightarrow \mathrm{v'}, \mathrm{matches'}\end{array}}{\mathrm{E}, \mathrm{vs} \vdash \ \texttt{timeout}\ \mathrm{time}\ \mathrm{matches}\ \texttt{handle}\ \mathrm{handles} \Rightarrow \mathrm{v'}} \ v \in \mathrm{Exn} \tag{92}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{time} \Rightarrow \mathrm{t} \qquad \mathit{timecost}\ (\ \mathrm{E}, \mathrm{matches}\ \mathrm{vs}\ ) \ \geq \ \mathrm{t} \\ \mathrm{E}, \langle\ \mathrm{Timeout},\ \langle\ \rangle\ \rangle \models \mathrm{handle} \Rightarrow \mathrm{v}, \mathrm{matches'}\end{array}}{\mathrm{E}, \mathrm{vs} \vdash \ \texttt{timeout}\ \mathrm{time}\ \mathrm{matches}\ \texttt{handle}\ \mathrm{handles} \Rightarrow \mathrm{v}} \tag{93}$$

C.5 Dynamic Semantics: Expressions

$$\boxed{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}$$

The first few rules handle the semantics for simple expressions, including variables, basic values, nullary constructors, characters, and strings.

$$\frac{\mathrm{E}\ (\mathrm{var}) \ = \ \mathrm{v}}{\mathrm{E} \vdash \mathrm{var} \Rightarrow \mathrm{v}} \tag{94}$$

$$\frac{\mathrm{E}_0\ (\mathrm{b}) \ = \ \mathrm{exp} \qquad \mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \mathrm{b} \Rightarrow \mathrm{v}} \tag{95}$$

$$\frac{}{\mathrm{E} \vdash \mathrm{con} \Rightarrow \mathrm{con}\ \langle\rangle} \tag{96}$$

$$\frac{}{\mathrm{E} \vdash \mathrm{char} \Rightarrow \mathrm{char}} \tag{97}$$

$$\frac{\mathit{sval}\ (\mathrm{string}) \ = \ \mathrm{v}}{\mathrm{E} \vdash \mathrm{string} \Rightarrow \mathrm{v}} \tag{98}$$

The next rule defines the semantics of function applications as the application of the body of the function to a tuple of the arguments. There is no semantics of partial application.

$$\frac{\begin{array}{c}\mathrm{E}\ (\mathrm{var}) \ = \ \mathrm{matches} \qquad \forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \mathrm{v}_i \\ \mathrm{E}, \langle\ \mathrm{v}_1, \ldots, \mathrm{v}_n\ \rangle \vdash \mathrm{matches} \Rightarrow \mathrm{v'}\end{array}}{\mathrm{E} \vdash \mathrm{var}\ \mathrm{exp}_1\ \ldots\ \mathrm{exp}_n \Rightarrow \mathrm{v'}} \tag{99}$$

Rules 100–101 deal with constructors by interpreting their arguments as a tuple. If the value of the tuple is an exception, then this is the value of the expression; otherwise the value of the expression is constructed as the combination of the constructor and the semantic tuple of arguments.

$$\frac{\mathrm{E} \vdash (\mathrm{exp}_1 \ldots, \mathrm{exp}_n) \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \mathrm{con}\ \mathrm{exp}_1\ \ldots\ \mathrm{exp}_n \Rightarrow \mathrm{con}\ \mathrm{v}}\ \mathrm{v} \notin \mathrm{Exn} \tag{100}$$

$$\frac{\mathrm{E} \vdash (\mathrm{exp}_1 \ldots, \mathrm{exp}_n) \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \mathrm{con}\ \mathrm{exp}_1\ \ldots\ \mathrm{exp}_n \Rightarrow \mathrm{v}}\ \mathrm{v} \in \mathrm{Exn} \tag{101}$$

The next set of rules define the semantics for primitive constructors, including lists, tuples and vectors. The semantics of non-empty lists is given in terms of that for the constructors `(:)` and `Nil`, while that for non-empty vectors is given in terms of that for tuples.

$$\frac{\mathrm{E} \vdash (:)\ \mathrm{exp}_1\ (\ldots((:)\ \mathrm{exp}_n\ [\,])\ldots) \Rightarrow \mathrm{v}}{\mathrm{E} \vdash [\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ] \Rightarrow \mathrm{v}}\ \mathrm{n} \geq 1 \tag{102}$$

$$\frac{}{\mathrm{E} \vdash [\,] \Rightarrow \texttt{Nil}\ \langle\,\rangle} \tag{103}$$

$$\frac{}{\mathrm{E} \vdash () \Rightarrow \langle\,\rangle} \tag{104}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \mathrm{v}_i \qquad \vdash \langle\ \mathrm{v}_1,\ \ldots,\ \mathrm{v}_n\ \rangle \Rightarrow \mathrm{v'} \qquad \mathrm{v'} \notin \mathrm{Exn}}{\mathrm{E} \vdash (\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ) \Rightarrow \langle\ \mathrm{v}_1,\ \ldots,\ \mathrm{v}_n\ \rangle} \tag{105}$$

$$\frac{\forall i.\ 1 < i \leq n,\ \ \mathrm{E} \vdash \mathrm{exp}_i \Rightarrow \mathrm{v}_i \qquad \vdash \langle\ \mathrm{v}_1,\ \ldots,\ \mathrm{v}_n\ \rangle \Rightarrow \mathrm{v'} \qquad \mathrm{v'} \in \mathrm{Exn}}{\mathrm{E} \vdash (\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ) \Rightarrow \mathrm{v'}} \tag{106}$$

$$\frac{\mathrm{E} \vdash (\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ ) \Rightarrow \mathrm{v}}{\mathrm{E} \vdash {<<}\ \mathrm{exp}_1,\ \ldots,\ \mathrm{exp}_n\ {>>} \Rightarrow \langle\ v_1,\ \ldots,\ v_n\ \rangle} \tag{107}$$

The semantics of case-expressions is defined by matching the value of the expression against the match. Note that the semantics for conditional expressions (rule 109) is defined in terms of the semantics for case-expressions (rule 108).

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v} \qquad \mathrm{E}, \mathrm{v} \vdash \mathrm{match} \Rightarrow \mathrm{v'}}{\mathrm{E} \vdash \texttt{case}\ \mathrm{exp}\ \texttt{of}\ \mathrm{match} \Rightarrow \mathrm{v'}} \tag{108}$$

$$\frac{\mathrm{E} \vdash \texttt{case}\ \mathrm{exp}_1\ \texttt{of}\ \{\ \mathrm{True}\ \rightarrow\ \mathrm{exp}_2 \mid \mathrm{False}\ \rightarrow\ \mathrm{exp}_3\ \} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{if}\ \mathrm{exp}_1\ \texttt{then}\ \mathrm{exp}_2\ \texttt{else}\ \mathrm{exp}_3 \Rightarrow \mathrm{v}} \tag{109}$$

Let-expressions have a simple semantics.

$$\frac{\mathrm{E} \vdash \mathrm{decls} \Rightarrow \mathrm{E'} \qquad \mathrm{E} \stackrel{\rightarrow}{\oplus} \mathrm{E'} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{let}\ \mathrm{decls}\ \texttt{in}\ \mathrm{exp} \Rightarrow \mathrm{v}} \tag{110}$$

Type signatures have no dynamic component.

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \mathrm{exp} :: \mathrm{type} \Rightarrow \mathrm{v}} \tag{111}$$

The semantics of type coercion is defined in terms of an auxiliary *coerce* function that implements the semantics of coercion as defined in Section 2.1.3. This function is not specified here.

$$\frac{\mathrm{E} \vdash \mathrm{exp'} \Rightarrow \mathrm{v} \qquad \mathit{coerce}(\mathrm{v}, \mathrm{type}) \;=\; \mathrm{v'}}{\mathrm{E} \vdash \mathrm{exp}\ \texttt{as}\ \mathrm{type} \Rightarrow \mathrm{v'}} \tag{112}$$

Raising an exception simply involves returning it as the value of the expression.

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{raise}\ \mathrm{exnid}\ \mathrm{exp} \Rightarrow \langle\ \mathrm{exnid},\ \mathrm{v}\ \rangle} \tag{113}$$

The next set of rules define the semantics of constrained expressions. If the cost of evaluating the expression (as given by the cost function) is greater than the specified constant value, then the corresponding exception is raised, otherwise the value of the within-expression is the same as the encapsulated expression.

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \mathrm{t} \qquad \mathrm{E} \vdash \mathrm{exp}_3 \Rightarrow \mathrm{h} \qquad \mathrm{E} \vdash \mathrm{exp}_4 \Rightarrow \mathrm{s} \\ \mathit{timecost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;<\; \mathrm{t} \\ \mathit{heapcost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;<\; \mathrm{h} \\ \mathit{stackcost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;<\; \mathrm{s} \\ \mathrm{E} \vdash \mathrm{exp}_1 \Rightarrow \mathrm{v}\end{array}}{\mathrm{E} \vdash \mathrm{exp}_1\ \texttt{within}\ \mathrm{exp}_2\ ,\ \mathrm{exp}_3\ (\mathrm{exp}_4\ )\ [\ \texttt{raise}\ \mathrm{exnid}\ ] \Rightarrow \mathrm{v}} \tag{114}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \mathrm{t} \\ \mathit{timecost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;\geq\; \mathrm{t}\end{array}}{\mathrm{E} \vdash \mathrm{exp}_1\ \texttt{within}\ \mathrm{exp}_2\ ,\ \mathrm{exp}_3\ (\mathrm{exp}_4\ )\ [\ \texttt{raise}\ \mathrm{exnid}\ ] \Rightarrow \langle\ \mathrm{exnid/Timeout},\ \langle\ \rangle\ \rangle} \tag{115}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \mathrm{t} \qquad \mathrm{E} \vdash \mathrm{exp}_3 \Rightarrow \mathrm{h} \\ \mathit{timecost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;<\; \mathrm{t} \qquad \mathit{heapcost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \;\geq\; \mathrm{h}\end{array}}{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_1\ \texttt{within}\ \mathrm{exp}_2\ ,\ \mathrm{exp}_3\ (\mathrm{exp}_4\ )\ [\ \texttt{raise}\ \mathrm{exnid}\ ] \\ \Rightarrow \langle\ \mathrm{exnid/HeapOverflow},\ \langle\ \rangle\ \rangle\end{array}} \tag{116}$$

$$\frac{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_2 \Rightarrow \mathrm{t} \qquad \mathrm{E} \vdash \mathrm{exp}_3 \Rightarrow \mathrm{h} \qquad \mathrm{E} \vdash \mathrm{exp}_4 \Rightarrow \mathrm{s} \\ \mathit{timecost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) < \mathrm{t} \\ \mathit{heapcost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) < \mathrm{h} \\ \mathit{stackcost}\ (\mathrm{E},\ \mathrm{exp}_1\ ) \geq \mathrm{s}\end{array}}{\begin{array}{c}\mathrm{E} \vdash \mathrm{exp}_1\ \texttt{within}\ \mathrm{exp}_2\ ,\ \mathrm{exp}_3\ (\mathrm{exp}_4\ )\ [\ \texttt{raise}\ \mathrm{exnid}\ ] \\ \Rightarrow \langle\ \mathrm{exnid/StackOverflow},\ \langle\ \rangle\ \rangle\end{array}} \tag{117}$$

The next expression rules define the semantics of bracketed expressions in terms of the enclosed expression. Profiling and verification expressions are evaluated purely for their effect, and brackets are ignored, as usual.

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{profile}\ \mathrm{exp}\ ) \Rightarrow \mathrm{v}} \tag{118}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash \texttt{verify}\ \mathrm{exp}\ ) \Rightarrow \mathrm{v}} \tag{119}$$

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v}}{\mathrm{E} \vdash (\ \mathrm{exp}\ ) \Rightarrow \mathrm{v}} \tag{120}$$

Rules 121–126 extract exceptions from constructed values such as lists or tuples. The rules are applied to a value that is being matched in order to ensure that any exception that is embedded within the matched value is raised as a result of a match. If there are multiple exceptions, then the rightmost-outermost is returned. – the first such exception working from right-to-left is used the value of the constructed item. If there is no exception, this is signalled by the value $\langle\rangle$.

$$\boxed{\vdash \mathrm{v} \Rightarrow \mathrm{v}}$$

$$\frac{}{\vdash \mathrm{v} \Rightarrow \mathrm{v}} \quad \mathrm{v} \in \mathrm{Exn} \tag{121}$$

$$\frac{}{\vdash \langle\, \mathrm{v}_1 \ldots, \mathrm{v}_n \,\rangle \Rightarrow \mathrm{v}_n} \quad \mathrm{v}_n \in \mathrm{Exn} \tag{122}$$

$$\frac{\vdash \langle\, \mathrm{v}_1, \ \ldots, \ \mathrm{v}_{n-1} \,\rangle \Rightarrow \mathrm{v'}}{\vdash \langle\, \mathrm{v}_1, \ \ldots, \ \mathrm{v}_n \,\rangle \Rightarrow \mathrm{v'}} \quad \mathrm{v}_n \notin \mathrm{Exn} \tag{123}$$

$$\frac{\vdash \langle\, \mathrm{v}_1, \ \ldots, \ \mathrm{v}_{n-1} \,\rangle \Rightarrow \mathrm{v'}}{\vdash \mathrm{con}\ \mathrm{v}_1 \ \ldots \mathrm{v}_n \Rightarrow \mathrm{v'}} \quad \mathrm{v}_n \notin \mathrm{Exn} \tag{124}$$

$$\frac{}{\vdash \langle\rangle \Rightarrow \langle\rangle} \tag{125}$$

$$\frac{}{\vdash \mathrm{v} \Rightarrow \langle\rangle} \quad \mathrm{v} \in \mathrm{BasVal} \tag{126}$$

The final expression rules are used in constructing matches for case-expressions and function applications. If the expression to be matched is an exception, then the result of the match is an exception; otherwise the matching rules defined below are used. Since fair matching is never used for case-expressions, the reordered match list is discarded.

$$\boxed{\mathrm{E}, \mathrm{v} \vdash \mathrm{match} \Rightarrow \mathrm{v}}$$

$$\frac{\vdash \mathrm{v} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \vdash \mathrm{match} \Rightarrow \mathrm{v'}} \quad \mathrm{v'} \in \mathrm{Exn} \tag{127}$$

$$\frac{\vdash \mathrm{v} \Rightarrow \langle\rangle \qquad \mathrm{E}, \mathrm{v} \models \mathrm{match} \Rightarrow \mathrm{v'}, \mathrm{match'}}{\mathrm{E}, \mathrm{v} \vdash \mathrm{match} \Rightarrow \mathrm{v'}} \tag{128}$$

C.6 Dynamic Semantics: Matches

For clarity, we use a different kind of turnstile ($\models$) for match inference rules. E,v $\models$ e $\Rightarrow$ v' defines the meaning of *match* with respect to a single matched value *e*. The semantics for definitions and applications ensures that matches are curried appropriately.

The semantics for pattern-matching is derived from that presented in the Haskell report for **case** expressions (where the semantics was defined as a translation into a Haskell kernel). This gives a less direct semantics than that of, e.g., Standard ML.

Rules (129–130) define sequences of matches. The first rule applies when the first match in a sequence succeeds, the second when it fails. Failure of the last match in a sequence is as defined by the specific case below, e.g. in the rule for non-matching constructors (Rule 138). Since Hume requires matches to be complete, this will never occur in practice, however. The rules return a new list of matches, with the matched rule at the end. This new list would be used to ensure fair matching on subsequent uses of the box. Rule (131) is used to ensure that the final rule in a sequence is returned if it matches, and to avoid tedious repetition in the individual cases.

$$\boxed{\mathrm{E, v} \models \text{ matches} \Rightarrow \mathrm{v}/FAIL, \text{match}}$$

$$\frac{\mathrm{E, v} \models \{\ \text{match}\ \} \Rightarrow \mathrm{v'}, \text{matches'}}{\mathrm{E, v} \models \{\ \text{match} \mid \text{matches}\ \} \Rightarrow \mathrm{v'}, \{\ \text{matches} \mid \text{match}\ \}} \quad (129)$$

$$\frac{\mathrm{E, v} \models \{\ \text{match}\ \} \Rightarrow FAIL \qquad \mathrm{E, v} \models \{\ \text{matches}\ \} \Rightarrow \mathrm{v}, \{\ \text{matches'}\ \}}{\mathrm{E, v} \models \{\ \text{match} \mid \text{matches}\ \} \Rightarrow \mathrm{v}, \{\ \text{match} \mid \text{matches'}\ \}} \quad (130)$$

$$\frac{\mathrm{E, v} \models \{\ \text{match}\ \} \Rightarrow \mathrm{v'}}{\mathrm{E, v} \models \{\ \text{match}\ \} \Rightarrow \mathrm{v'}, \{\ \text{match}\ \}} \quad (131)$$

Rule (132) simplifies multi-argument matches to single-argument matches.

$$\boxed{\mathrm{E}, \mathrm{v} \models \text{match} \Rightarrow \mathrm{v}/FAIL}$$

$$\frac{\forall i.\ 0 < i \leq m, \quad \mathrm{var}_i \notin (\bigcup_{j=1}^{n} \mathrm{fv}(\mathrm{pat}_{ij} \cup \mathrm{fv}(\mathrm{exp}_i))}{\mathrm{E}, \mathrm{v} \models \left\{ \begin{array}{l} (\mathrm{var}_1, \ldots, \mathrm{var}_n) \ \rightarrow \\ \quad \texttt{case}\ (\mathrm{var}_1, \ldots, \mathrm{var}_n)\ \texttt{of} \\ \qquad \{ \quad (\mathrm{pat}_{11}, \ldots, \mathrm{pat}_{1n}) \ \rightarrow \ \mathrm{exp}_1 \\ \qquad\quad \mid \ldots \\ \qquad\quad \mid (\mathrm{pat}_{m1}, \ldots, \mathrm{pat}_{mn}) \ \rightarrow \ \mathrm{exp}_m \ \} \end{array} \right\} \Rightarrow \mathrm{v'} \quad m \geq 1, n \geq 2}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{pat}_{11} \ldots \mathrm{pat}_{1n} \ \rightarrow \ \mathrm{exp}_1 \mid \ldots \mid \mathrm{pat}_{m1} \ldots \ \mathrm{pat}_{mn} \ \rightarrow \ \mathrm{exp}_m \ \} \Rightarrow \mathrm{v'}} \tag{132}$$

Rule (133) simplifies matches into matches of the form { pat → exp | var → exp' }.

$$\frac{\forall i.\ 1 \leq i \leq n, \quad \mathrm{var}_i \notin (\bigcup_{j=1}^{n} \mathrm{fv}(\mathrm{pat}_j) \cup \mathrm{fv}(\mathrm{exp}_i))}{\mathrm{E}, \mathrm{v} \models \left\{ \begin{array}{l} \mathrm{pat}_1 \ \rightarrow \ \mathrm{exp}_1 \\ \mid \mathrm{var}_1 \ \rightarrow \ \texttt{case}\ \mathrm{var}_1\ \texttt{of}\ \{ \\ \quad \mathrm{pat}_2 \ \rightarrow \ \mathrm{exp}_2 \\ \quad \mid \mathrm{var}_2 \ \rightarrow \ \texttt{case}\ \mathrm{var}_2\ \texttt{of}\ \{ \\ \qquad \ldots \\ \qquad \mid \mathrm{var}_{n-1} \ \rightarrow \ \texttt{case}\ \mathrm{var}_{n-1}\ \texttt{of}\ \{\ \mathrm{pat}_n \ \rightarrow \ \mathrm{exp}_n\ \} \ldots\ \}\ \} \end{array} \right\} \Rightarrow \mathrm{v'} \quad n \geq 1}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{pat}_1 \ \rightarrow \ \mathrm{exp}_1 \mid \ldots \mid \mathrm{pat}_n \ \rightarrow \ \mathrm{exp}_n\ \} \Rightarrow \mathrm{v'}} \tag{133}$$

Rules (134)–(135) define the semantics of wildcard and variable matches.

$$\frac{\mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ \_ \ \rightarrow \ \mathrm{exp}\ \} \Rightarrow \mathrm{v'}} \tag{134}$$

$$\frac{\mathrm{E} \stackrel{\rightarrow}{\oplus} \{\ \mathrm{var} \ \mapsto \ \mathrm{v}\ \} \vdash \mathrm{exp} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{var} \ \rightarrow \ \mathrm{exp}\ \} \Rightarrow \mathrm{v'}} \tag{135}$$

Rules (136)–(140) define the semantics of matches against constructor patterns. Rules (136) and (140) are simplification rules, simplifying general constructor matches and tuple matches, respectively; the remaining rules define the matching semantics. The simplification rules are used to simplify deep pattern matches (such as [1,2]) into single-level matches.

$$\forall i.\ 1 \leq i \leq n,\ \ \mathrm{var}_i\ \notin\ (\bigcup_{j=1}^{n} \mathrm{fv}(\mathrm{pat}_j) \cup \mathrm{fv}(\mathrm{exp}))$$

$$\frac{\mathrm{E}, \mathrm{v} \models \left\{ \begin{array}{l} \mathrm{con}\ \mathrm{var}_1 \ldots \mathrm{var}_n\ \rightarrow \\ \quad \texttt{case}\ \mathrm{var}_1\ \texttt{of}\ \{\ \mathrm{pat}_1\ \rightarrow\ \ldots \\ \quad \texttt{case}\ \mathrm{var}_n\ \texttt{of}\ \{\ \mathrm{pat}_n\ \rightarrow\ \mathrm{exp}\ \}\ldots\ \} \end{array} \right\} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{con}\ \mathrm{pat}_1 \ldots \mathrm{pat}_n\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathrm{v'} \qquad (136)$$

$$\frac{\mathrm{v}\ =\ \mathrm{con}\ <\mathrm{v}_1, \ldots, \mathrm{v}_n> \qquad \mathrm{E} \overrightarrow{\oplus} \{\ \forall i.\ 1 \leq i \leq n,\ \ \mathrm{var}_i\ \mapsto\ \mathrm{v}_i\ \} \vdash \mathrm{exp} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{con}\ \mathrm{var}_1 \ldots \mathrm{var}_n\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathrm{v'} \qquad (137)$$

$$\frac{\mathrm{v}\ \neq\ \mathrm{con}\ \langle\ \mathrm{v}_1,\ \ldots,\ \mathrm{v}_n\ \rangle}{\mathrm{E}, \mathrm{v} \models \{\ \mathrm{con}\ \mathrm{var}_1\ \ldots\ \mathrm{var}_n\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathit{FAIL} \qquad (138)$$

$$\frac{\mathrm{v}\ =<>\qquad \mathrm{E} \vdash \mathrm{exp} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ ()\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathrm{v'} \qquad (139)$$

$$\forall i.\ 0 < i \leq n,\ \mathrm{var}_i \notin\ (\bigcup_{j=1}^{n} \mathrm{fv}(\mathrm{pat}_j) \cup \mathrm{fv}(\mathrm{exp}))$$

$$\frac{\mathrm{E}, \mathrm{v} \models \left\{ \begin{array}{l} (\mathrm{var}_1, \ldots, \mathrm{var}_n)\ \rightarrow \\ \quad \texttt{case}\ \mathrm{var}_1\ \texttt{of}\ \{\ \mathrm{pat}_1\ \rightarrow\ \ldots \\ \quad \texttt{case}\ \mathrm{var}_n\ \texttt{of}\ \{\ \mathrm{pat}_n\ \rightarrow\ \mathrm{exp}\ \}\ldots\ \} \end{array} \right\} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ (\mathrm{pat}_1, \ldots, \mathrm{pat}_n)\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathrm{v'} \qquad (140)$$

$$\frac{\mathrm{v}\ =\ \langle\ \mathrm{v}_1,\ \ldots,\ \mathrm{v}_n\ \rangle \qquad \mathrm{E} \overrightarrow{\oplus} \bigcup_{i=1}^{n} \{\ \mathrm{var}_i\ \mapsto\ \mathrm{v}_i\ \} \vdash \mathrm{exp} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \{\ (\ \mathrm{var}_1,\ \ldots,\ \mathrm{var}_n\ )\ \rightarrow\ \mathrm{exp}\ \} \Rightarrow \mathrm{v'} \qquad (141)$$

C.6.1 Exception Handler Matches

Rules 142–143 match against sequences of exception handlers.

$$\frac{\mathrm{E}, \mathrm{v} \models \mathrm{handler} \Rightarrow \langle\ \rangle \qquad \mathrm{E}, \mathrm{v} \models \mathrm{handlers} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \mathrm{handler}\ |\ \mathrm{handlers} \Rightarrow \mathrm{v'} \qquad (142)$$

$$\frac{\mathrm{E}, \mathrm{v} \models \text{handler} \Rightarrow \mathrm{v'}}{\mathrm{E}, \mathrm{v} \models \text{handler} \mid \text{handlers} \Rightarrow \mathrm{v'}} \tag{143}$$

Finally, rules 144–145 handle matches against individual exceptions, either success or failure.

$$\frac{\mathrm{v} = \langle\ \text{exnid},\ \mathrm{v'}\ \rangle \qquad \mathrm{E}, \mathrm{v'} \models \text{pat} \Rightarrow \mathrm{v''}}{\mathrm{E}, \mathrm{v} \models \text{exnid pat} \rightarrow \text{exp} \Rightarrow \mathrm{v''}} \tag{144}$$

$$\frac{\mathrm{v} = \langle\ \text{exnid'},\ \mathrm{v'}\ \rangle}{\mathrm{E}, \mathrm{v} \models \text{exnid pat} \rightarrow \text{exp} \Rightarrow \langle\ \rangle} \tag{145}$$

C.7 Dynamic Semantics: The Initial Environment

The initial environment comprises definitions for all functions and constructors defined in the module *Prelude*. These values must be available in all Hume programs. The meanings of other *Prelude* functions is defined by reference to Appendix D, which provides a source language definition. We assume that the meaning of basic operations (such as addition on numbers) is obvious. To define this formally would be tedious in the extreme. We will also assume without formal specification that the initial environment for some Hume program will include definitions for those functions and values that are imported into a Hume program, whether or not these were originally defined in Hume (i.e. whether or not they are "foreign" functions).

The initial environment contains the following functions (*BasVal*)

PrimPlusInt $\mapsto$ (a, b) `->` $a + b$ $+$ is fixed-precision integer addition
PrimMulInt $\mapsto$ (a, b) `->` $a \times b$ $\times$ is fixed-precision integer multiplication
...

plus the standard constructors (*BasCon*):

0, 1, ..., 0.0, 0.1, ..., *True*, *False*, 'a', ..., (:), *Nil*

The characters correspond to those defined by the ASCII character set. The mapping from syntactic variables to semantic constructors is the obvious one, that is, E_0 (SetEnv) = SetEnv ....

Appendix D

Standard Prelude

Summary of Standard Hume Functions and Operators

Operations on *bool* types

```
==, !=, <=, <, >, >= :: bool -> bool -> bool
and, or :: bool -> bool -> bool
not :: bool -> bool
```

Operations on *char* types

```
==, !=, <=, <, >, >= :: char -> char -> bool
```

Operations on *int s* types

```
+, -, *, div, **, mod :: int s -> int s -> int s
==, !=, <=, <, >, >= :: int s -> int s -> bool
```

Operations on *nat s* types

```
+, -, *, div, **, mod :: nat s -> nat s -> nat s
==, !=, <=, <, >, >= :: nat s -> nat s -> bool
```

Operations on *word s* types

```
+, -, mod, ^&, ^|, ^ :: word s -> word s -> word s
~ :: word s -> word s
rotl, rotr, lshl, lshr, ashl, ashr :: word s -> int s -> word s
==, !=, <=, <, >, >= :: word s -> word s -> bool
```

Operations on *float s* types

```
+, -, *, /, ** :: float s -> float s -> float s
sin, cos, tan, asin, acos, atan, sqrt :: float s -> float s
log, log10, ln, exp  :: float s -> float s
sinh, cosh, tanh, atan2 :: float s -> float s
==, !=, <=, <, >, >= :: float s -> float s -> bool
```

Operations on *string s* types

```
length :: string s -> int s'
@ :: string s -> int s' -> char
++ :: string s1 -> string s2 -> string (s1+s2)
slice :: string s1 -> int s2 -> int s2 -> string s3
==, !=, <=, <, >, >= :: string s -> string s -> bool
```

Operations on *vector s of a* types

```
length :: <<a>> -> int s'
@ :: <<a> -> int s' -> a
vecdef :: int s1 -> (int s2->a) -> <<a>>
vecmake :: int s1 -> (int s2 -> a -> b)) -> a -> <<b>>
vecmap :: <<a>> -> (a->b) -> <<b>>
vecfoldr :: <<a>> -> b -> (a->b->b) -> b
update :: <<a>> -> int s -> a -> <<a>>
slice :: <<a>> -> int s -> int s -> <<a>>
==, !=, <=, <, >, >= :: <<a>> -> <<a>> -> bool
```

Operations on *tuple a1 ... an* types

```
==, !=, <=, <, >, >= :: (a1, .., an) -> (a1, ..., an) -> bool
```

Operations on *list a* types

```
length :: [a] -> int s
@ ::  [a] -> int s -> a
++ :: [a] -> [a] -> [a]
hd :: [a] -> a
tl :: [a] -> [a]
==, !=, <=, <, >, >= :: [a] -> [a] -> bool
```

Operations on discriminated union types

```
==, !=, <=, <, >, >= :: a -> a -> bool
```

Bibliography

[1] J.-R. Abrial, E. Börger, and H. Langmaack (Eds.), "Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control", Springer-Verlag, LNCS 1165, October 1996.

[2] W. Ackermann, *Solvable Cases of the Decision Problem*, North Holland, 1954.

[3] K.R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs*. Springer Verlag, 1997. 2nd Edition.

[4] J.G.P. Barnes, *High Integrity Ada: the Spark Approach*, Addison-Wesley, 1997.

[5] A. Benveniste and G. Berry, "The Synchronous Approach to Reactive and Real-Time Systems", *Proceedings of the IEEE*, **79**(9), Sept. 1991, pp. 1270-1282.

[6] A. Benveniste and P.L. Guernic, "Synchronous Programming with Events and Relations: the Signal Language and its Semantics", *Science of Computer Programming*, **16**, 1991, pp. 103–149.

[7] G. Bernat, A. Burns, and A. Wellings. Portable Worst-Case Execution Time Analysis Using Java Byte Code. In *Proc. 12th Euromicro International Conference on Real-Time Systems*, Stockholm, June 2000.

[8] G. Berry and G. Gonthier, "The Esterel Synchronous Programming Language: Design, Semantics, Implementation", *Science of Computer Programming*, **19**(2), 1992, pp. 87–152.

[9] G. Blair, L. Blair, H. Bowman and A. Chetwynd, *Formal Specification of Distributed Multimedia Systems*, UCL Press, 1998.

[10] G. Bollela and et al. *The Real-Time Specification for Java*. Addison-Wesley, 2000.

[11] A. Bonenfant, Z. Chen, K. Hammond, G.J. Michaelson, A. Wallace, and I. Wallace. Towards resource-certified software: A Formal Cost Model for Time and its Application to an Image-Processing Example. *Proc. 2007 ACM Symposium on Applied Computing*, to appear, 2007.

[12] F. Boussinot and R. de Simone, "The Esterel Language", *Proceedings of the IEEE*, **79**(9), Sept. 1991, pp. 1293–1304.

[13] S. Budkowski and P. Dembrinski, "An Introduction to Estelle: a Specification Language for Distributed Systems", *Computer Networks and ISDN Systems*, **4**, 1987, pp. 3–23.

[14] R. Burstall, "Inductively Defined Functions in Functional Programming Languages", LFCS, Department of Computer Science, University of Edinburgh, ECS-LFCS-87-25, April, 1987.

[15] P. Caspi, D. Pilaud, N. Halbwachs and J. Place, "Lustre: a Declarative Language for Programming Synchronous Systems", *Proc. 14th ACM Symposium on Principles of Programming Languages (POPL '87)*, München, Germany, 1987.

[16] M. Chakravarty, "The Haskell 98 Foreign Function Interface 1.0: An Addendum to the Haskell 98 Report", `http://www.cse.unsw.edu.au/ chak/haskell/ffi/`, 2006.

[17] , L. Damas and A.J.R.G. Milner, "Principal Type-Schemes for Functional Programs", *Proc. 1982 ACM Symp. on Principles of Prog. Langs. – POPL '82*, 1982, 207–212.

[18] C. Ferdinand, R. Heckmann, M. Langenbach, F. Martin, M. Schmidt, H. Theiling, S. Thesing, and R. Wilhelm. Reliable and precise WCET determination for a real-life processor. In *Proc. EMSOFT 2001, First Workshop on Embedded Software*, volume 2211 of *Lecture Notes in Computer Science*, pages 469–485. Springer-Verlag, 2001.

[19] C. Grelck and S.-B. Scholz, "HPF vs. SAC — a Case Study", *Proc. EuroPar 2000*, Munich, Germany, Springer Verlag, LNCS, September 2000.

[20] K. Hammond, H.-W. Loidl and A.S. Partridge, "Improving Granularity for Parallel Functional Programs: a Graphical Winnowing System for Haskell", *Proc. 1995 Conf. on High Performance Functional Computing (HPFC '95)*, Denver, Co., Apr. 1995, pp. 208–221.

[21] K. Hammond and G.J. Michaelson (Eds.), *Research Directions in Parallel Functional Programming*, Springer-Verlag, November 1999.

[22] K. Hammond, "Hume: a Bounded Time Concurrent Language", *Proc. IEEE International Conf. on Electronic Control Systems (ICECS '2K)*, Kaslik, Lebanon, December 2000.

[23] K. Hammond. Is it Time for Real-Time Functional Programming? In *Trends in Functional Programming, volume 4*. Intellect, 2004.

[24] K. Hammond and G. Michaelson. Bounded Space Programming using Finite State Machines and Recursive Functions: the Hume Approach. Submitted to *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2006.

[25] K. Hammond and G.J. Michaelson. Hume: a Domain-Specific Language for Real-Time Embedded Systems. In *Proc. GPCE '03: Conf. Generative Programming and Component Engineering*, pages 37–56. Springer-Verlag LNCS 2830, 2003.

[26] K. Hammond and G.J. Michaelson. Predictable Space Behaviour in FSM-Hume. In *Proc. Implementation of Functional Langs.(IFL '02), Madrid, Spain*, number 2670 in Lecture Notes in Computer Science. Springer-Verlag, 2003.

[27] K. Hammond, G. Grov, G.J. Michaelson and A. Ireland, "Low-Level Programming in Hume: an Exploration of the HW-Hume Level", Submitted to IFL 2006: Intl Symposium on Implementations and Applications of Functional Languages, Budapest, Hungary, Sept. 2006.

[28] D. Harel, "Statecharts: a Visual Approach to Complex Systems", *Science of Computer Programming*, **8**(3), 1987, pp. 231–274.

[29] D. Harel, O. Lichtenstein and A. Pnueli, "Explicit Clock Temporal Logic", *Proc. 5th IEEE Symposium on Logic in Computer Science*, 1990, pp. 402–413.

[30] M. Hofmann and S. Jost. Static Prediction of Heap Space Usage for First-Order Functional Programs. In *POPL'03 — Symposium on Principles of Programming Languages*, New Orleans, LA, USA, January 2003. ACM Press.

[31] I. Holyer and E. Spiliopoulou, "Concurrent Monadic Interfacing", *Proc. 10th. Intl. Workshop on Implementation of Functional Programming (IFL '98)*, Springer-Verlag, LNCS 1595, 1998, pp. 73–89.

[32] P. Hudak, S.L. Peyton Jones, and P.L. Wadler (editors). Report on the Programming Language Haskell, A Non-strict Purely Functional Language (Version 1.2). *ACM SIGPLAN Notices*, 27(5), May 1992.

[33] R.J.M. Hughes, L. Pareto, and A. Sabry, "Proving the Correctness of Reactive Systems using Sized Types", *Proc. 1996 ACM Symposium on Principles of Programming Languages (POPL '96)*, St Petersburg, Fl., Jan. 1996.

[34] R.J.M. Hughes and L. Pareto, "Recursion and Dynamic Data Structures in Bounded Space: Towards Embedded ML Programming", *Proc. 1999 ACM Intl. Conf. on Functional Programming (ICFP '99)*, 1999.

[35] International Organisation for Standardisation, "ISO: Information Processing Systems — Open Systems Interconnection — LOTOS, A Formal Description Technique based on the Temporal Ordering of Observational Behaviour", ISO 8807, Geneva, August 1988.

[36] International Organisation for Standardisation, "ISO: Information Processing Systems — Open Systems Interconnection — Estelle, A Formal Description Technique based on an Extended State Transition Model", ISO 9074, Geneva, May 1989.

[37] International Telecommunication Union, *[Z.100] Recommendation Z.100 (11/99) – Specification and description language (SDL)*, 1999.

[38] F. Jahanian and A. Mok, "Safety Analysis of Timing Properties in Real-Time Systems", *IEEE Trans. on Software Eng.*, **12**(9), 1986, pp. 890–904.

[39] D. Jensen, "'Real-time Java'. What could and what should it mean?",
URL: `http://www.sdct.itl.nist.gov/`
`~carnahan/real-time/vocab/`
`rt-java_glossary.htm`, May 1998.

[40] F. Kamareddine and F. Monin, "On Formalised Proofs of Termination of Recursive Functions", *PPDP'99*, LNCS 1702, pp 29-46, 1999.

[41] F. Kamareddine and F. Monin, "On Automating Inductive and Non-inductive Termination Methods", *ASIAN'99*, LNCS 1742, pp. 177-189, 1999.

[42] P.H.J. Kelly and F.A. Taylor, "Coordination Languages", In [21].

[43] R. Koymans, "Specifying Real-Time Properties with Metric Temporal Logic", *Real-Time Systems*, **2**, 1990, pp. 255-299.

[44] J Launchbury and R Paterson, "Parametricity and Unboxing with Unpointed Types", *Proc. European Symposium on Programming (ESOP'96)*, Linkoping, Sweden, Springer Verlag LNCS 1058, Jan 1996.

[45] N.G. Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995.

[46] H-W. Loidl, *Granularity in Large-Scale Parallel Functional Programming*, PhD Thesis, Department of Computer Science, University of Glasgow, 1998.

[47] H-W. Loidl, R. Morgan, S.L. Peyton Jones, R. Garagliano, P.W. Trinder and C. Cooper, "Parallelising a Large Functional Program. Or Keeping Lolita Busy", *Proc. 1997 International Workshop on Implementing Functional Languages (IFL '97)*, St Andrews, Scotland, Sept. 1997, Springer-Verlag LNCS 1467.

[48] D. Le Métayer, "ACE: An Automatic Complexity Evaluator", *ACM TOPLAS*, **10**(2), April 1988.

[49] H.-W. Loidl, A.J. Rebón Portillo and Kevin Hammond, "A Sized Time System for a Parallel Functional Language (Revised)", *Draft Proc. 2nd Scottish Functional Programming Workshop*, St Andrews, July 2000.

[50] M. Lücker and T. Noll, "The Implementation of the TRUTH Model Checker in Haskell", *Draft Proc. International Workshop on Implementation of Functional Programming (IFL 2000)*, Aachen, Germany, RWTH Fachgruppe Informatik Research Report 00-7, M. Mohnen and P. Koopman (Eds.), September 2000, pp. 363-380.

[51] G.J. Michaelson, "Interpreter prototypes from formal language definitions", PhD thesis, Dept of Computing and Electrical Engineering, Heriot-Watt University, 1993.

[52] G.J. Michaelson, "Constraints on Recursion in the Hume Expression Language", *Draft Proc. International Workshop on Implementation of Functional Programming (IFL 2000)*, Aachen, Germany, RWTH Fachgruppe Informatik Research Report 00-7, M. Mohnen and P. Koopman (Eds.), September 2000, pp. 231–246.

[53] G.J. Michaelson and K.Hammond, "The Hume Language Definition and Report, Version 0.1", Heriot-Watt University and University of St Andrews, July 2000.

[54] G.J. Michaelson and N. Scaife , "Prototyping a parallel vision system in Standard ML", *Journal of Functional Programming*, special issue on Applications of Functional Programming, **5**(3), pp. 345–382, July 1995

[55] G. Michaelson, N. Scaife, P. Bristow and P. King, "Nested algorithmic skeletons from higher order functions", *Parallel Algorithms and Applications*, special issue on High Level Models and Languages for Parallel Processing, to appear, September 2000

[56] C. Miguel, *Extended LOTOS Definition*, OSI 95 (Esprit Project 5341), Report OSI95/DIT/B5/8/TR/R/V0, Depto. Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid, Madrid, Spain.

[57] A.J.R.G. Milner, J. Parrow and D. Walker, "A Calculus of Mobile Processes, Parts I and II", *Information and Computation*, **100**(1), 1992, pp. 1–77.

[58] A.J.R.G. Milner, M. Tofte, R. Harper, and D. MacQueen, *The Definition of Standard ML (Revised)*, *MIT Press*, 1997.

[59] R. Mirani, and P. Hudak, "First-Class Schedules and Virtual Maps", *Proc. FPCA '95 — Functional Prog. Langs. and Computer Architecture*, La Jolla, CA, June, 1995, pp. 78–85.

[60] J.W. Peterson, K. Hammond (eds.), L. Augustsson, B. Boutel, F.W. Burton, J.H. Fasel, A.D. Gordon, R.J.M. Hughes, P. Hudak, T. Johnsson, M.P. Jones, E. Meijer, S.L. Peyton Jones, A. Reid and P.L. Wadler, "Report on the Programming Language Haskell: a Non-Strict Purely Functional Language, Version 1.4", April 1997.

[61] *Report on the Non-Strict Functional Language, Haskell* S.L. Peyton Jones (ed.), L. Augustsson, B. Boutel, F.W. Burton, J.H. Fasel, A.D. Gordon, K. Hammond, R.J.M. Hughes, P. Hudak, T. Johnsson, M.P. Jones, E. Meijer, J.C. Peterson, A. Reid, and P.L. Wadler, Yale University, 1999.

[62] S.L. Peyton Jones, C.V. Hall, K. Hammond, W.D. Partain and P.L. Wadler, "The Glasgow Haskell Compiler: a Technical Overview", *Proc. JFIT '93*, Keele, March 1993.

[63] R. Peter, *"Recursive Functions"*, Academic Press, 1967.

[64] J.L. Peterson, "Petri Nets" *ACM Computing Surveys* **9**(3):223–252, 1977.

[65] A. Pnueli, "The Temporal Logic of Programs", *Proc. 18th. IEEE Symposium on Foundations of Computer Science*, Los Alamitos, CA, 1977, pp. 46-57.

[66] B. Randall, "Facing up to faults", Computer Journal, **43**(2), 2000, pp. 95–106.

[67] R. Rangaswami, "Compile-Time Cost Analysis for Parallel Programming", *Proc. EUROPAR '96*, Lyon, France, 1996.

[68] G.M. Reed and A.W. Roscoe, "A Timed Model for Communicating Sequential Processes", *Theoretical Computer Science*, **58**, 1988, pp. 249–261.

[69] B. Reistad and D.K. Gifford., "Static Dependent Costs for Estimating Execution Time", *Proc. 1994 ACM Conf. on Lisp and Functional Programming*, pp. 6578, Orlando, Fl., June 2729, June 1994.

[70] A.W. Roscoe, *The Theory and Practice of Concurrency*, Prentice-Hall, 1998.

[71] D. Sands, "Complexity Analysis for a Lazy Higher-Order Language", *Proc. 1990 European Symposium on Programming (ESOP '90)*, Springer-Verlag LNCS 432, May 1990.

[72] D.B. Skillicorn, "Deriving Parallel Programs from Specifications using Cost Information", *Science of Computer Programming*, **20**(3), June 1993.

[73] S. Stepney, *High Integrity Compilation: a Case Study*, Prentice-Hall, 1993.

[74] Sun Microsystems, "EmbeddedJava Technical Overview", URL: `http://java.sun.com/products/embeddedjava/spec/1.0/eJavaTechnicalOverview.html`, 1998.

[75] M. Tofte and J.-P. Talpin, "Region-based Memory Management", *Information and Control*, **132**(2), 1997, pp. 109–176.

[76] P.W. Trinder, K. Hammond, H.-W. Loidl and S.L. Peyton Jones, "Algorithm + Strategy = Parallelism", *Journal of Functional Programming*, **8**(1), Jan. 1998, pp. 23–60.

[77] P.W. Trinder, K. Hammond, J.S. Mattson Jr., A.S. Partridge and S.L. Peyton Jones, "GUM: a Portable Parallel Implentatiion of Haskell", *Proc. 1996 ACM. Conf. on Programming Language Design and Implementation (PLDI '96)*, Philadelphia, May 1996, pp. 79–90.

[78] D.A. Turner, "Elementary Strong Functional Programming", *Proc. 1st. Symposium on Functional Programming Languages in Education — FPLE '95*, Springer-Verlag LNCS No. 1022, December 1995.

[79] P.B. Vasconcelos. *Cost Inference and Analysis for Recursive Functional Programs.* PhD thesis, University of St Andrews, 2006. in preparation.

[80] P.B. Vasconcelos and K. Hammond. Inferring Costs for Recursive, Polymorphic and Higher-Order Functional Programs. In *Proc. Implementation of Functional Languages (IFL 2003)*, 2004.

[81] W. Yi, "Real-Time Behaviour of Asynchronous Agents", *Proc. CONCUR '90*, Springer-Verlag, LNCS 458, 1990, pp. 502–520.