

# Implicitly Heterogeneous Multi-Stage Programming

## (Extended Version)

Jason Eckhardt, Roumen Kaiabachev, Emir Pašalić, Kedar Swadi,  
Walid Taha

*Rice University*  
*Department of Computer Science*  
*P.O. Box 1892, MS 132*  
*Houston, TX 77005, USA*

`{jle,roumen,pasalic,kswadi,taha}@cs.rice.edu`

Received 30 August 2005

**Abstract** Previous work on semantics-based multi-stage programming (MSP) language design focused on *homogeneous* designs, where the generating and the generated languages are the same. Homogeneous designs simply add a hygienic quasi-quotation and evaluation mechanism to a base language. An apparent disadvantage of this approach is that the programmer is bound to both the expressivity and performance characteristics of the base language. This paper proposes a practical means to avoid this by providing specialized translations from subsets of the base language to different target languages. This approach preserves the homogeneous “look” of multi-stage programs, and, more importantly, the static guarantees about the generated code. In addition, compared to an explicitly heterogeneous approach, it promotes reuse of generator source code and systematic exploration of the performance characteristics of the target languages.

---

Supported by NSF ITR-0113569 “Putting Multi-Stage Annotations to Work”, Texas ATP 003604-0032-2003 “Advanced Languages Techniques for Device Drivers” and NSF ITR-0205303 “Building Practical Compilers Based on Adaptive Search.”

To illustrate the proposed approach, we design and implement a translation to a subset of C suitable for numerical computation, and show that it preserves static typing. The translation is implemented, and evaluated with several benchmarks. The implementation is available in the online distribution of MetaOCaml.

**Keywords** Functional Programming, Multi-Stage Programming.

## §1 Introduction

Multi-stage programming (MSP) languages allow the programmer to use abstraction mechanisms such as functions, objects, and modules, without having to pay a runtime overhead for them. Operationally, these languages provide quasi-quotation and `eval` mechanisms similar to those of LISP and Scheme. In addition, to avoid accidental capture, bound variables are always renamed, and values produced by quasi-quotes can only be de-constructed by `eval`. This makes reasoning about quoted terms as programs sound<sup>18)</sup>, even in the untyped setting. Several type systems have been developed that statically ensure that all programs generated using these constructs are well-typed (c.f.<sup>19, 1)</sup>).

Currently, the main examples of MSP languages include MetaScheme<sup>7)</sup>, MetaML<sup>20)</sup>, MetaOCaml<sup>10)</sup>, and Metaphor<sup>11)</sup>. They are based, respectively, on Scheme, Standard ML, OCaml, and Java/C#. In all these cases, the language design is *homogeneous*, in that quoted values are fragments of the base language. Homogeneity has three distinct advantages. First, it is convenient for the language designer, as it often reduces the size of the definitions needed to model a language, and makes extensions to arbitrary stages feasible at little cost. Second, it is convenient for the language implementor, as it allows the implementation of the base language to be reused: In all three examples above, as in LISP and Scheme implementations, the `eval`-like construct calls the underlying implementation. In the case of MetaOCaml, the MetaOCaml compiler and the bytecode runtime system can be used to execute generated programs at runtime. Third, it is convenient for the programmer, as it requires learning only a small number of new language constructs.

While the homogeneous approach described above has its advantages, there are situations in which the programmer may wish to take advantage of the capability of other compilers that are only available for other languages. For example, very well-developed, specialized compilers exist for application domains

such as numerical computing, embedded systems, and parallel computation.

At first glance, this situation might suggest a need for *heterogeneous* quotation mechanisms, where quoted terms can contain expressions in a different language. Indeed, this approach has been used successfully for applications such as light-weight components <sup>8, 9)</sup>, FFT <sup>6)</sup>, and computer graphics <sup>5)</sup>. But heterogeneous quotation mechanisms also introduce two new complications:

1. How do we ensure that the generated program is statically typed?
2. How do we avoid restricting a generator to a particular target language?

One approach to addressing the first issue is to develop specialized two-level type systems. This means the language designer must work with type systems and semantics that are as big as both languages combined. Another possibility is to extend meta-programming languages with dependent type systems <sup>13)</sup> and thus give the programmers the ability to write data-types that encode the abstract syntax of only *well-typed* object-language terms. Currently, such type systems can introduce significant notational overhead for the programmer, as well as requiring familiarity with unfamiliar type systems.

In principle, the second problem can be avoided by parameterizing the generators themselves by constructs for the target language of choice. However, this is likely to reduce the readability of the generators, and it is not clear how a quotation mechanism can be used in this setting. Furthermore, to ensure that the generated program is statically typed, we would, in essence, need to parameterize the static type of the generator by a description of the static type system of the target language. The typing infrastructure needed is likely to be far beyond what has gained acceptance in mainstream programming.

## 1.1 Contributions

This paper proposes a practical approach to avoiding the two problems, which can be described as *implicitly heterogeneous* MSP. In this approach, the programmer does not need to know about the details of the target-language representation. Those details are supplied by the meta-language designer once and for all and invoked by the programmer through the familiar interface used to execute generated code. This is achieved by the language implementers providing specialized translations from subsets of the base language to different target languages. Thus, the homogeneous “look” of homogeneous MSP is preserved. An immediate benefit is that the programmer may not have to make any changes

to existing generators to target different languages. Additionally, if the translation itself is type preserving, the static guarantee about the type correctness of generated code is maintained.

The proposed approach is studied in the case when the target language is C. After a brief introduction to MSP (Section 2), we outline the details of what can be described as an *offshoring* translation that we have designed and implemented. The design begins by identifying the precise subset of the target language that we wish to make available to the programmer (Section 3). Once that is done, the next challenge is to identify an appropriate subset in the base language that can be used to represent the target subset.

Like a compiler, offshoring translations are provided by the language implementor and not by the programmer. But the requirements on offshoring translators are essentially the opposite of those on compilers (or compiling translators, such as Tarditi's <sup>21</sup>): First, offshoring is primarily concerned with the target, not the source language. The most expressive translation would cover the full target language, but not necessarily the source language. In contrast, a compiler must cover the source but not necessarily the target language. Second, the translation must be a direct mapping from source to target, and not a complex, optimizing translation. The direct connection between the base and target representations is essential for giving the programmer access to the target language.

To ensure that all generated programs are well typed, we show that the offshoring translation is type preserving (Section 4). This requires being explicit about the details of the type system for the target language as well as the source language, but is manageable because both subsets are syntactically limited. Again, this is something the language designer does once and benefits any programmer who uses the offshoring translation.

Having an offshoring translation makes it easier for the programmer to experiment with executing programs either in OCaml or C (using different C compilers). We present a detailed analysis of changes in performance behavior for a benchmark of dynamic programming algorithms (Section 5). Not surprisingly, C consistently outperforms the OCaml bytecode compiler. We also find that in several cases, the overhead of marshalling the results from the OCaml world to the C world can be a significant bottleneck, especially in cases where C is much faster than the OCaml bytecode compiler. And while C outperforms the OCaml native code compiler in many cases, there are exceptions.

## §2 Multi-Stage Programming

MSP languages <sup>20, 16)</sup> provide three high-level constructs that allow the programmer to break down computations into distinct stages. These constructs can be used for the construction, combination, and execution of code fragments. Standard problems associated with the manipulation of code fragments, such as accidental variable capture and the representation of programs, are hidden from the programmer (cf. <sup>16)</sup>). The following minimal example illustrates MSP programming in MetaOCaml:

```
let rec power n x = if n=0 then .<1>. else .< .~x * .~(power (n-1) x)>.
let power3 = .! .<fun x -> .~(power 3 .<x>.)>.
```

Ignoring the staging constructs (brackets `.<e>.`, escapes `.~e`, as well as run `.! e`) the above code is a standard definition of a function that computes  $x^n$ , which is then used to define the specialized function  $x^3$ . Without staging, the last step simply returns a function that would invoke the `power` function every time it gets invoked with a value for  $x$ . In contrast, the staged version builds a function that computes the third power directly (that is, using only multiplication). To see how the staging constructs work, we can start from the last statement in the code above. Whereas a term `fun x -> e x` is a value, an annotated term `.<fun x -> .~(e .<x>.)>.` is not, because the outer brackets contain an escaped expression that still needs to be evaluated. Brackets mean that we want to construct a future stage computation, and escapes mean that we want to perform an immediate computation *while* building the bracketed computation. In a multi-stage language, these constructs are not hints, they are imperatives. Thus, the application `e .<x>.` must be performed even though `x` is still an uninstantiated symbol. The expression `power 3 .<x>.` is performed immediately, once and for all, and not repeated every time we have a new value for `x`. In the body of the definition of the function `power`, the recursive application of `power` is escaped to ensure its immediate execution in the first stage. Evaluating the definition of `power3` first results in the equivalent of

```
.! .<fun x -> x*x*x*1>.
```

Once the argument to run `(.!)` is a code fragment that has no escapes, it is compiled and evaluated, and returns a function that has the same performance as if we had explicitly coded the last declaration as:

```
let power3 = fun x -> x*x*x*1
```

Applying this function does not incur the unnecessary overhead that the un-staged version would have had to pay every time `power3` is used.

## §3 Offshoring for Numerical Computation in C

This section presents an example of an offshoring translation aimed at supporting implicitly heterogeneous MSP for basic numerical computation. The method for defining the types and the syntax is presented, along with the resulting formal definitions. The mapping from base to target is only described informally. It bears repeating that the programmer will not need to write her program generators to explicitly produce the target language presented in this section. Rather, the interface to generating target programs is written using the source-language syntax (Section 3.3); however, the programmer does need to be aware of the target subset definitions to be able to express her algorithms in a way that makes the code they produce amenable to translation. (Please see Appendix 3 for full definition.) The section concludes by presenting the details of the programmer’s interface to offshoring, and discussing the practical issue of marshalling values between the runtime systems of the base and target languages.

### 3.1 Types for Target Subset

The types in the target C subset include:

1. Base numerical types `int`, `char` and `double`.
2. One- and two- dimensional arrays of these numerical types. One-dimensional arrays are represented as C arrays. Two-dimensional arrays are implemented as an array of pointers (C type `*[]`). While this representation is less efficient than two-dimensional arrays in C, it was chosen because it allows for a simpler translation, since it is a better semantic match with MetaOCaml arrays. OCaml array *types* do not explicitly declare their size, so it is not always possible to obtain a valid two-dimensional array type in C from a type of two-dimensional arrays in OCaml.
3. Functions that take base types or arrays of base types as arguments and return base type values. This subset does not include function pointers, functions with variable number of arguments, or functions that return `void`.

<i>Type keyword</i>	$t$	$\in$	$\{\text{int, double, char}\}$
<i>Constant</i>	$c$	$\in$	$\text{Int} \cup \text{Float} \cup \text{Char}$
<i>Variable</i>	$x$	$\in$	$X$
<i>Declaration</i>	$d$	$::=$	$t\ x = c \mid t\ x[n] = \{c^*\} \mid t^*x[n] = \{x^*\}$
<i>Arguments</i>	$a$	$::=$	$t\ x \mid t\ x[\ ] \mid t^*x[\ ]$
<i>Unary operator</i>	$f^{(1)}$	$\in$	$\{\text{(float)}, \text{(int)}, \text{cos}, \text{sin}, \text{sqrt}\}$
<i>Binary operator</i>	$f^{(2)}$	$\in$	$\{+, -, *, /, \%, \&\&,   , \&,  , \wedge, \ll, \gg, ==, !=, <, >, <=, >=\}$
<i>For loop op.</i>	$opr$	$::=$	$<= \mid >=$
<i>Expression</i>	$e$	$::=$	$c \mid x \mid f^{(1)}\ e \mid e\ f^{(2)}\ e \mid x\ (e^*) \mid x[e] \mid x[e][e] \mid e\ ?\ e : e$
<i>Incr. expression</i>	$i$	$::=$	$x++ \mid x--$
<i>Statement</i>	$s$	$::=$	$e \mid \text{return } e \mid \{d^*; s^*\} \mid x=e \mid x[e]=e \mid x[e][e]=e$ $\mid \text{if } (e)\ s\ \text{else } s \mid \text{while } (e)\ s \mid \text{for}(x = e; x\ opr\ e; i)\ s$ $\mid \text{switch } (e)\ \{w^*\text{default: } s\}$
<i>Switch branch</i>	$w$	$::=$	$\text{case } c: s\ \text{break};$
<i>Fun. decl.</i>	$g$	$::=$	$t\ x\ (a^*)\ \{d^*; s^*\}$
<i>Program</i>	$p$	$::=$	$d^*; g^*$

Fig. 1 Grammar for the C target

The C subset types are described by the following BNF:

<i>Base types</i>	$b$	$\in$	$\{\text{int, double, char}\}$
<i>Array types</i>	$a$	$::=$	$b[\ ] \mid *b[\ ]$
<i>Types</i>	$t$	$::=$	$b \mid a$
<i>Funtypes</i>	$f$	$::=$	$b\ (t_0, \dots, t_n)$

### 3.2 Syntax for Target Subset

Figure 1 presents the BNF of the target C subset. The set is essentially a subset of C that has all the basic numerical and array operations, first order functions, and structured control flow operators. The target subset is not determined in a vacuum but also involves considering what can be expressed naturally in the source language. The main restrictions we impose on this subset are:

1. All declarations are initialized. This restriction is caused by the fact that OCaml does not permit uninitialized bindings for variables, and representing uninstantiated declarations in OCaml can add complexity.
2. No unstructured control flow statements (i.e., `goto`, `break`, `continue` and fall-through non-defaulted `switch` statements). This restriction is motivated by the lack of equivalent unstructured control flow operators in OCaml. For the same reason, the increment operations are also limited.
3. Two-dimensional arrays are represented by an array of pointers (e.g., `int **x[]`) instead of standard two-dimensional arrays.

4. **For-loops** are restricted to the most common case where the initializer is a single assignment to a variable, and the mutator expression is simply increment or decrement by one. This covers the most commonly used C idiom, and matches the OCaml `for` loops.
5. No **do-while** loop commands. OCaml does not have control flow statements that correspond naturally to a **do-while** loop.
6. **Return** statements are not permitted inside `switch` and `for` statements. A return can only appear at the end of a block in a function declaration or in a terminal positions at both branches of the `if` statement. This restriction is enforced by the type system (See Appendix 1).

While this subset is syntactically restricted compared to full C, it still provides a semantically expressive first-order language. Many missing C constructs can be effectively simulated by the ones included: for example, arithmetical mutation operators (e.g., `+=`) can be simulated by assignments. Similarly **do-while** loops can be simulated with existing looping constructs. Since staging in MetaOCaml gives the programmer complete control over what code is generated, this imposes little burden on the programmer. This subset is particularly well-supported by many industrial-strength compilers. Giving the programmer safe access to such compilers is the main purpose of implicitly heterogeneous MSP.

### 3.3 Types in Base Language

We now turn to the base language representation of the target language subset: the types in the OCaml subset must match those of the C subset. OCaml base types `bool`, `int`, `char`, and `float` map to C `int`, `char` and `double`, (OCaml booleans are simply mapped to C integers). The OCaml reference type (`ref`) is used to model C variables of simple type. One- and two-dimensional arrays are represented by OCaml  `$\hat{b}$  array` and  `$\hat{b}$  array array` types. To reflect the different restrictions on them, we will also distinguish types for function arguments, variable types and function declarations. The resulting types are as follows:

<i>Constant</i>	$\hat{c} \in$	$Int \cup Bool \cup Float \cup Char$
<i>Variable</i>	$\hat{x} \in$	$\hat{X}$
<i>Unary op.</i>	$\hat{f}^{(1)} \in$	$\{\text{cos, sin, sqrt, float\_of\_int, int\_of\_float}\}$
<i>Limit op.</i>	$\hat{f}^{(2)} \in$	$\{\text{min, max}\}$
<i>Binary op.</i>	$\hat{f}^{[2]} \in$	$\{+, -, *, /, +., -., *, /., **, \text{mod, land, lor, lxor, lsl, lsr, asr, =, <>, <, >, \leq, \geq, \&\&,   \}$
<i>Expression</i>	$\hat{e} ::=$	$\hat{x} \mid \hat{x}(\hat{e}^*) \mid \hat{f}^{(1)} \hat{e} \mid \hat{f}^{(2)} \hat{e} \hat{e} \mid \hat{e} \hat{f}^{[2]} \hat{e} \mid \text{if } \hat{e} \text{ then } \hat{e} \text{ else } \hat{e}$ $\mid !\hat{x} \mid \hat{x}.\hat{e} \mid \hat{x}.\hat{e}.\hat{e}$
<i>Statement</i>	$\hat{d} ::=$	$\hat{e} \mid \hat{d}; \hat{d} \mid \text{let } \hat{x} = \hat{e} \text{ in } \hat{d} \mid \text{let } \hat{x} = \text{ref } \hat{c} \text{ in } \hat{d}$ $\mid \text{let } \hat{x} = \text{Array.make } \hat{c} \hat{c} \text{ in } \hat{d} \mid \hat{x}.\hat{e} \leftarrow \hat{e}$ $\mid \text{let } \hat{x} = \text{Array.make\_matrix } \hat{c} \hat{c} \hat{c} \text{ in } \hat{d} \mid \hat{x}.\hat{e}.\hat{e} \leftarrow \hat{e}$ $\mid \hat{x} := \hat{e} \mid \text{if } \hat{e} \text{ then } \hat{d} \text{ else } \hat{d} \mid \text{while } \hat{e} \text{ do } \hat{d} \text{ done}$ $\mid \text{for } \hat{x} = \hat{e} \text{ to } \hat{e} \text{ do } \hat{d} \text{ done} \mid \text{for } \hat{x} = \hat{e} \text{ downto } \hat{e} \text{ do } \hat{d} \text{ done}$ $\mid \text{match } \hat{e} \text{ with } ((\hat{c} \rightarrow \hat{d})^* \mid \_ \rightarrow \hat{d})$
<i>Program</i>	$\hat{s} ::=$	$\lambda(x^*).( \hat{d} : \hat{b} ) \mid \text{let } \hat{x} = \hat{c} \text{ in } \hat{s} \mid \text{let } f(\hat{x}^*) = \hat{d} \text{ in } \hat{s}$ $\mid \text{let } \hat{x} = \text{ref } \hat{c} \text{ in } \hat{s} \mid \text{let } \hat{x} = \text{Array.make } \hat{c} \hat{c} \text{ in } \hat{s}$ $\mid \text{let } \hat{x} = \text{Array.make\_matrix } \hat{c} \hat{c} \hat{c} \text{ in } \hat{s}$

Fig. 2 OCaml Subset Grammar

<i>Base</i>	$\hat{b} \in$	$\{\text{int, bool, float, char}\}$
<i>Reference</i>	$\hat{r} ::=$	$\hat{b} \text{ ref}$
<i>Array</i>	$\hat{a} ::=$	$\hat{b} \text{ array} \mid \hat{b} \text{ array array}$
<i>Argument</i>	$\hat{p} ::=$	$\hat{b} \mid \hat{a}$
<i>Variables</i>	$\hat{t} ::=$	$\hat{b} \mid \hat{r} \mid \hat{a}$
<i>Function</i>	$\hat{u} ::=$	$(\hat{p}_0, \dots, \hat{p}_n) \rightarrow \hat{b}$

### 3.4 Syntax for Base Language

The syntax of the source subset is presented in Figure 2. Semantically, this subset represents the first-order subset of OCaml with arrays and reference cells. We point out the most interesting syntactic features of the OCaml subset:

1. Syntactically, **let** bindings are used to represent C declarations. Bindings representing C function declarations are further restricted to exclude function declarations nested in the bodies of functions.
2. Assignments in C are represented by updating OCaml references or arrays.
3. We use a special syntactic form to indicate a top level entry function (analogous to C **main**).

### 3.5 What the Programmer Sees

The programmer is given access to offshoring simply by making MetaOCaml run construct `(.!e)` customizable. In addition to this standard form, the programmer can now write `!.{Trx.run_gcc}e` or `!.{Trx.run_icc}e` to indicate when offshoring should be used and whether the `gcc` or `icc` compilers, respectively, should be used to compile the resulting code. Additional arguments can also be passed to these constructs. For example, the programmer can write `{Trx.run_gcc}e` (resp. `{Trx.run_icc}e`) as follows:

```
!.{Trx.run_gcc with compiler = "cc"; compiler_flags="-g -O2"} ...
```

to use an alternative compiler `cc` with the flags `-g -O2`.

### 3.6 Marshalling and Dynamic Linking

The C and OCaml systems use different runtime representations for values. So, to use the offshored program, inputs and outputs must be marshalled from one representation to the other.

In our implementation of the translation described above, we generate a marshalling function for the top-level entry point of the offshored function. The marshalling function depends only on the type of the top-level function. First, OCaml values are converted to their C representations. The standard OCaml library provides conversions for base types. We convert arrays by allocating a new C array, converting each element of the OCaml array, and storing it in the C array. The C function is invoked with the marshalled C values. Its results are collected, and marshalled back into OCaml. To account for updates in arrays, the elements of the C are converted and copied back into the OCaml array.

Once a C program has been produced, the marshalling code is added, and the result is then compiled into a shared library (a `.so`) file. To load this shared library into MetaOCaml's runtime system, we extend Stolpmann's dynamic loading library for OCaml<sup>14)</sup> to support dynamic loading of function values.

## §4 Type Preservation

Showing that an offshoring translation can preserve typing requires formalizing the type system for the target language, the source language, as well as the translation itself.

The type system for top-level statements in OCaml programs is defined

by the derivability of the judgment  $\hat{\Gamma} \vdash \hat{p} : \hat{t}$  (Appendix 2). Similarly, the type system for C programs is defined by a judgment  $\Gamma \vdash g$  (Appendix 1). We also provide the definition of translation functions (Appendix 3). For example,  $\langle\hat{s}\rangle = (g_1, \dots, g_n, l_1, \dots, l_m)$  translates a top-level OCaml program into a set of C variable declarations and function definitions, and  $\llbracket\hat{\Gamma}\rrbracket$  translates the OCaml variable and function environment,  $\hat{\Gamma}$ , into the corresponding C environment. We define an operation  $|\cdot|$  on variable declarations and function definitions that translates them into a C type environment (Appendix 4).

Finally, we show that any valid term in the base language translates to a valid one in the target language.

#### Theorem 4.1 (Type Preservation)

If  $\hat{\Gamma} \vdash \hat{s} : \hat{a}_n \rightarrow \hat{b}$  and  $\langle\hat{s}\rangle = (g, l)$ , then  $\llbracket\hat{\Gamma}\rrbracket \cup |l| \cup |g| \vdash g$ .

**Proof** By induction over the height of first derivation. The details of the proof are presented in Appendix 4. ■

## §5 Effect on Performance Characteristics

This section summarizes some empirical measurements that we have gathered to evaluate the performance impact of offshoring. The questions we wanted these experiments to answer are: How does the performance of offshored code compare to that of the same code executed with *run*? Does marshalling impose a significant overhead on offshoring? As MetaOCaml currently only supports bytecode OCaml execution, would extending MetaOCaml to support native OCaml-style compilation be an acceptable alternative to offshoring?

### 5.1 Benchmarks

As a benchmark, we use a suite of staged dynamic programming algorithms. These algorithms were initially implemented to study how dynamic programming algorithms can be staged <sup>15)</sup>. The benchmark consists of (both un-staged and staged) MetaOCaml implementations of the following algorithms <sup>2)</sup>:

- **forward**, the forward algorithm for Hidden Markov Models. Specialization size (size of the observation sequence) is 7.
- **gib**, the Gibonacci function, a minor generalization of the Fibonacci function. This is not an example of dynamic programming, but gives rise to the same technical problems while staging. Specialization is for  $n = 25$ .

**Table 1** Speedups and Break-Even Points from Offshoring to C

Name	Unstaged (ms)	Generate (ms)	Compile (ms)	Staged Run ( $\mu$ s)	Speedup	<b>Speedup'</b>	<b>BEP</b>
forward	0.20	1.1	34.	0.37	530x	<b>20.x</b>	<b>180</b>
gib	0.13	0.26	19.	0.12	990x	<b>5.3x</b>	<b>170</b>
ks	5.2	36.	8300.	1.4	3700x	<b>69.x</b>	<b>1600</b>
lcs	5.5	46.	6400.	5.1	1100x	<b>24.x</b>	<b>1100</b>
obst	4.2	26.	5300.	4.6	910x	<b>22.x</b>	<b>1300</b>
opt	3.6	66.	8700.	3.4	1100x	<b>44.x</b>	<b>2500</b>

Using GNU's `gcc`

Name	Unstaged (ms)	Generate (ms)	Compile (ms)	Staged Run ( $\mu$ s)	Speedup	<b>Speedup'</b>	<b>BEP</b>
forward	0.20	1.1	33.0	0.35	580x	<b>21.x</b>	<b>170</b>
gib	0.13	0.26	20.0	0.098	1200x	<b>6.4x</b>	<b>180</b>
ks	5.2	36.	8100.	1.5	3500x	<b>66.x</b>	<b>1600</b>
lcs	5.5	46.	6500.	5.3	1000x	<b>25.x</b>	<b>1200</b>
obst	4.2	26.	5400.	4.5	940x	<b>23.x</b>	<b>1300</b>
opt	3.6	66.	9300.	3.3	1100x	<b>46.x</b>	<b>2600</b>

Using Intel's `icc`

- `ks`, the 0/1 knapsack problem. Specialization is for size 32 (number of items).
- `lcs`, the least common subsequence problems. Specialization is for string sizes 25 and 34 for the first and second arguments, respectively.
- `obst`, the optimal binary search tree algorithm. Specialization is a leaf-node-tree of size 15.
- `opt`, the optimal matrix multiplication problem. Specialization is for 18 matrices.

To evaluate offshoring, we compare executing the result of these algorithms in MetaOCaml to executing the result in C using offshoring. <sup>\*1</sup>

## 5.2 Comparing Offshoring with the OCaml Byte Code

Because of engineering issues with OCaml's support for dynamic loading, MetaOCaml currently extends only the bytecode compiler with staging constructs, but not the native code compiler. We therefore begin by considering the impact of offshoring in the bytecode setting.

<sup>\*1</sup> **Platform specs.** Timings were collected on a Pentium 4 machine (3055MHz, 8K L1 and 512K L2 cache, 1GB main memory) running Linux 2.4.20-31.9. All experiments are fully automated and available online <sup>3)</sup>. We report results based on version DP\_002/1.25 of the benchmark. It was executed using MetaOCaml version 308.alpha.020 bytecode compiler, Objective Caml version 3.08.0 native code compiler, and GNU's `gcc` version 2.95.3 20010315, and Intel's `icc` version 8.0 Build 20031016Z C compilers.

Table 1 displays measurements for offshoring with both `gcc` and Intel’s `icc`. The columns are computed as follows: **Unstaged** is the execution time of the unstaged version of a program. All times are averages, and are reported are in milliseconds (ms) unless otherwise stated. We measure execution times using MetaOCaml’s standard library function `Trxtime.timenew`. This function repeatedly executes a program until the cumulative execution time exceeds 1 second and reports the number of iterations and the average execution time per iteration. **Generate** reports code generation times. Generation is considered the first stage in a two-stage computation. The second stage is called Staged Run and will be described shortly. **Compile** is the time needed to translate the generated program and compile it with `gcc` (or `icc` in the second table), and dynamically load the resulting binary. **Staged Run** reports the C program execution time, including marshalling. The binary is generated by calling the C compiler with the flags `-g -O2`. **Speedup** is computed as Unstaged divided by Staged Run. **Speedup’** is the ratio between Speedup with staging (without offshoring) and staging with offshoring. **BEP** is the break-even point, i.e., the number of executions for a piece of code after which the initial overhead of offshoring (generation and compilation) pays off. For example, we need at least 180 uses of `forward` compiled using `gcc` before it is cheaper to use the staged version than to just use the unstaged one.

In general, the results obtained for offshoring to C are encouraging. The ratio between speedups (**Speedup’**) is always greater than 1. But it should be noted that the BEP’s are higher than for non-offshored staged execution within MetaOCaml. This is primarily a result of the C compilation times being higher than OCaml bytecode compilation times.

### 5.3 Marshalling overhead

To assess the impact of marshalling on the runtime performance, we compare the time to execute the benchmarks from within MetaOCaml against

**Table 2** Marshalling Overhead for `gcc` and Intel’s `icc` Compiled Offshored Code

Name	Marshalling (G) Overhead ( $\mu$ s)	Percentage (G)	Marshalling (I) Overhead ( $\mu$ s)	Percentage (I)
forward	0.19	<b>50. %</b>	0.22	<b>63. %</b>
gib	0.11	<b>91. %</b>	0.089	<b>91. %</b>
ks	0.37	<b>26. %</b>	1.4	<b>96. %</b>
lcs	3.8	<b>74. %</b>	4.2	<b>79. %</b>
obst	0.61	<b>13. %</b>	1.5	<b>34. %</b>
opt	0.61	<b>17. %</b>	0.24	<b>7.4 %</b>

the time it took to execute the same functions in a C program with no marshalling.

Table 2 displays the numbers for the `gcc` and `icc` compilers. Each program is run multiple times externally using the same number of iterations obtained from the measurements for the **Unstaged Run** in Figure 1. The Unix `time` command is used to measure the time for each program. This time is then divided by the number of iterations to obtain an average execution time per program. The columns are computed as follows: **Marshalling Overhead(G)** and **Marshalling Overhead(I)** show the difference in microseconds between running each function from within MetaOCaml and running it externally using `gcc` and `icc` respectively. **Percentage(G)** and **Percentage(I)** show the marshalling overhead as a percentage of the total time spent on the marshalled computation.

In the `forward` example, we marshal a 7-element integer array. In `gib`, we marshal only two integers, and thus have a low marshalling overhead. But because the total computation time in this benchmark small, the marshalling overhead is high. In `ks`, we marshal a 32-element integer array, and in `lcs` benchmark, we marshal two 25- and 34-element character arrays, which accounts for the high marshalling overhead in these benchmarks. Since both these benchmarks perform a significant amount of computation, the proportion of time spent marshalling is, however, lower than `gib` or `forward`. Similarly, `obst` and `opt` have significant marshalling overheads since they must marshal 15-element floating-point and 18-element integer arrays.

While the percentages given by both `gcc` and `icc` are comparable, there is one benchmark `ks` which shows a large difference. This can be explained by the fact that `icc` was able to optimize much better than `gcc`, reducing computation time to the point that most of the time was spent in marshalling.

The data indicates that marshalling overhead is significant in this benchmark. We chose the current marshalling strategy for implementation simplicity, and not for efficiency. These results suggest that it would be useful to explore an alternative marshalling strategy that allows sharing of the same data-structures across the OCaml/C boundary.

## 5.4 Comparing Offshoring with the OCaml Native Compiler

One motivation for offshoring is that standard implementations of high-

**Table 3** Speed of Offshored vs. OCaml Native Compiled Code

Name	OCamlOpt ( $\mu s$ )	Tweaked ( $\mu s$ )	Best GCC ( $\mu s$ )	Speedup	Speedup <sup>2</sup>
forward	0.29	0.25	0.13	<b>2.2x</b>	<b>2.1x</b>
gib	0.017	0.0095	0.0096	<b>1.7x</b>	<b>0.95x</b>
ks	23.	0.61	1.0	<b>23.x</b>	<b>0.59x</b>
lcs	24.	3.1	1.2	<b>20.x</b>	<b>3.0x</b>
obst	33.	10.	2.7	<b>12.x</b>	<b>3.9x</b>
opt	24.	4.9	2.8	<b>8.3x</b>	<b>1.7x</b>

Using GNU's gcc

Name	OCamlOpt ( $\mu s$ )	Tweaked ( $\mu s$ )	Best ICC ( $\mu s$ )	Speedup	Speedup <sup>2</sup>
forward	0.29	0.25	0.13	<b>2.2x</b>	<b>1.8x</b>
gib	0.017	0.0095	0.0091	<b>1.8x</b>	<b>1.1x</b>
ks	23.	0.61	0.061	<b>380.x</b>	<b>10.x</b>
lcs	24.	3.1	1.1	<b>22.x</b>	<b>2.2x</b>
obst	33.	10.	2.9	<b>11.x</b>	<b>3.6x</b>
opt	24.	4.9	3.1	<b>7.8x</b>	<b>1.6x</b>

Using Intel's icc

level languages are unlikely to compile automatically generated programs as effectively as implementations for lower-level languages such as C. The figures reported so far relate to the MetaOCaml bytecode compiler. How does offshoring perform against the native code compiler?

Table 3 displays measurements for execution times of the generated programs when executed using the native-code compiler for OCaml and the best runtime when running the result of their translation in C. The columns are computed as follows: **OCamlOpt** is the time for executing programs compiled with the `ocamlopt` compiler with the options `-unsafe -inline 50`. **Tweaked** are execution times for programs hand-optimized post-generation by the following transformations<sup>\*2</sup>: currying the arguments to functions, replacing the uses of the polymorphic OCaml operators `min` and `max` by their monomorphic versions, and moving array initializations outside the generated functions. The same compiler options as in **OCamlOpt** were used. **Best GCC (Best ICC)** is the execution time for generated and offshored code with the best performing optimization level (`-O[0-4]`). **Speedup** is the ratio of the **OCamlOpt** times to the **Best GCC (Best ICC)** times, and **Speedup<sup>2</sup>** is the ratio of the **Tweaked** execution times **Best GCC (Best ICC)**.

Without hand-optimizing the generated code, offshoring always outperforms the native code compiler. After hand-optimizing the generated code, the

<sup>\*2</sup> Thanks to Xavier Leroy for pointing out that these changes would improve the relative performance of the OCaml native code compiler.

**Table 4** Binary Image Sizes of OCaml Native Code Compiled vs. Offshored

Name	Generated	OCamlOpt	Ratio'	Tweaked	Ratio''
forward	13103	344817	<b>26.3x</b>	256204	<b>19.6x</b>
gib	11811	279205	<b>23.6x</b>	262243	<b>22.2x</b>
knapsack	41910	270031	<b>6.44x</b>	264012	<b>6.30x</b>
lcs	59037	341085	<b>5.78x</b>	251541	<b>4.26x</b>
obst	40711	213933	<b>5.26x</b>	213999	<b>5.26x</b>
opt	45389	234512	<b>5.17x</b>	234492	<b>5.17x</b>

Using GNU's `gcc`

Name	Generated	OCamlOpt	Ratio	Tweaked	Ratio''
forward	43957	344817	<b>7.84x</b>	256204	<b>5.83x</b>
gib	43270	279205	<b>6.45x</b>	262243	<b>6.06x</b>
knapsack	43425	270031	<b>6.22x</b>	264012	<b>6.08x</b>
lcs	84296	341085	<b>4.05x</b>	251541	<b>2.98x</b>
obst	68029	213933	<b>3.15x</b>	213999	<b>3.15x</b>
opt	69176	234512	<b>3.39x</b>	234492	<b>3.39x</b>

Using Intel's `icc`

situation is slightly different. In two cases, the OCaml native code compiler outperforms `gcc`. In fact, for the `ks` benchmark, the OCaml compiler does much better than `gcc`.

The tweaks that improved the relative performance of OCaml's native code compiler draw attention to an important issue in designing an offshoring transformation and in interpreting speedups such as the ones presented here: Speedups are sensitive to the particular representation that we chose in the base language, and the real goal is to give the programmer the ability to generate specific programs in the target language. Speedups reported here give one set of data-points exhibiting the potential of offshoring.

A comparison of the sizes of binaries (Table 4) generated by the OCaml native code compiler with the offshored code compiled with `gcc` shows that compiling using `gcc` resulted in binaries of much smaller sizes. Even for the **Tweaked** sources, the binary sizes ranged from 4 to 20 times the sizes of the `gcc` generated binaries. For `icc`, there was also a saving in binary sizes. OCaml-generated binaries were between 3 to 6 times larger than those generated by `icc`. The primary reason for the larger OCaml image is that it has a bigger runtime system than C.

## §6 Further Opportunities for Offshoring

The particular offshoring translation presented here is useful for building multi-stage implementations of several standard algorithms. But there are other fea-

tures of C that have distinct performance characteristics, and which the programmer might wish to gain access to. We expect that the translation presented here can be expanded fairly systematically. In particular, an offshoring translation can be viewed as an inverse of a total map from the target to the source language. The backwards map would be a kind of OCaml semantics for the constructs in the target language. With this insight, several features of C can be represented in OCaml as follows: Function pointers can be handled naturally in a higher order language, although the representative base language subset would have to be restricted to disallow occurrences of free variables in nested functions. Such free variables give rise to the need for closures when compiling functional languages, and our goal is not to compile, but rather to give the programmer access to the notion of function pointers in C. If the programmer wishes to implement closures in C, it can be done explicitly at the OCaml level. For control operators, we can use continuations, and more generally, a monadic style in the source language, but the source would have similar restrictions on free variables to ensure that no continuation requires closures to be (automatically) constructed in the target code. Targeting struct and union types should be relatively straightforward using OCaml's notion of datatypes. Dynamic memory management, bit manipulation, and pointer arithmetic can be supported by specially marked OCaml libraries that simulate operations on an explicit memory model in OCaml. Arbitrary dimension arrays are a natural extension of the two-dimensional representation that we have already addressed.

## §7 Conclusion

We have proposed the idea of implicitly heterogeneous MSP as a way of combining the benefits of the homogeneous and heterogeneous approaches. In particular, generators need not become coupled with the syntax of the target language, and the programmer need not be bound to the performance characteristics of the base language. To illustrate this approach, we target a subset of C suitable for numerical computation, and take MetaOCaml as the base language. We have proved that the offshoring translation proposed for this subset preserves typing. This is done once in the language design stage, and the programmer has the same static typing guarantees that he can rely on in homogeneous MSP.

Experimental results indicate that this approach yields significantly better performance as compared to the OCaml bytecode compiler, and often better

performance than the OCaml native code compiler. We have implemented this extension in MetaOCaml. A fully automated version of our performance measurement suite has been implemented and made available online <sup>3)</sup>. An offshoring translation targeting FORTRAN is under development.

***Acknowledgment*** We would like to thank John Mellor-Crummey, Gregory Malecha, and Jeremy Siek who read drafts of this paper and gave us several helpful suggestions. A shorter version of this paper was submitted to the Generative Programming and Component Engineering (GPCE) conference. We would like to thank the GPCE reviewers and editors for their detailed and constructive comments. One of the reviewers asked whether offshoring can be used to produce highly-optimized libraries such as those used in the SPIN model checker or in Andrew Goldberg’s network optimization library. We thank the reviewer for the intriguing suggestion, and we hope that further experience with offshoring will allow us to answer this question.

## ***References***

- 1) Cristiano Calcagno, Eugenio Moggi, and Walid Taha. ML-like inference for classifiers. In *European Symposium on Programming (ESOP)*, Lecture Notes in Computer Science. Springer-Verlag, 2004.
- 2) Thomas Cormen, Charles Leiserson, and Ronald Rivest. *Introduction to Algorithms*. MIT Press and McGraw-Hill Book Company, 14 edition, 1994.
- 3) Dynamic Programming Benchmarks. Available online from <http://www.metaocaml.org/examples/dp>, 2005.
- 4) Jason Eckhardt, Roumen Kaiabachev, Emir Pasalic, Kedar Swadi, and Walid Taha. Implicitly heterogeneous multi-stage programming (extended version). Available online from: <http://www.cs.rice.edu/~taha/publications/preprints/2005-06-28-TR.pdf>, June 2005.
- 5) Conal Elliott, Sigbjørn Finne, and Oege de Moore. Compiling embedded languages. In <sup>17)</sup>, pages 9–27, 2000.
- 6) Matteo Frigo and Steven G. Johnson. FFTW: An adaptive software architecture for the FFT. In *Proc. 1998 IEEE Intl. Conf. Acoustics Speech and Signal Processing*, volume 3, pages 1381–1384. IEEE, 1998.
- 7) Robert Glück and Jesper Jørgensen. Multi-level specialization (extended abstract). In John Hatcliff, Torben Mogensen, and Peter Thiemann, editors, *Partial Evaluation: Practice and Theory*, volume 1706 of *LNCS*, pages 326–337. Springer-Verlag, 1999.
- 8) Sam Kamin. Standard ML as a meta-programming language. Technical report, Univ. of Illinois Computer Science Dept, 1996. Available at

[www-faculty.cs.uiuc.edu/~kamin/pubs/](http://www-faculty.cs.uiuc.edu/~kamin/pubs/).

- 9) Samuel N. Kamin, Miranda Callahan, and Lars Clausen. Lightweight and generative components i: Source-level components. In *GCSE '99: Proceedings of the First International Symposium on Generative and Component-Based Software Engineering*, pages 49–64, London, UK, 2000. Springer-Verlag.
- 10) MetaOCaml: A compiled, type-safe multi-stage programming language. Available online from <http://www.metaocaml.org/>, 2004.
- 11) Gregory Neverov and Paul Roe. *Towards a Fully-reflective Meta-programming Language*, volume 38 of *Conferences in Research and Practice in Information Technology*. ACS, Newcastle, Australia, 2005. Twenty-Eighth Australasian Computer Science Conference (ACSC2005).
- 12) Oregon Graduate Institute Technical Reports. P.O. Box 91000, Portland, OR 97291-1000, USA. Available online from <ftp://cse.ogi.edu/pub/tech-reports/README.html>.
- 13) Emir Pašalić, Walid Taha, and Tim Sheard. Tagless staged interpreters for typed languages. In *the International Conference on Functional Programming (ICFP '02)*, Pittsburgh, USA, October 2002. ACM.
- 14) Gerd Stolpmann. DL- ad-hoc dynamic loading for OCaml. Available from <http://www.ocaml-programming.de/packages/documentation/dl/>.
- 15) Kedar Swadi, Walid Taha, and Oleg Kiselyov. Staging dynamic programming algorithms, April 2005. Unpublished manuscript, available from <http://www.cs.rice.edu/~taha/publications.html>.
- 16) Walid Taha. *Multi-Stage Programming: Its Theory and Applications*. PhD thesis, Oregon Graduate Institute of Science and Technology, 1999. Available from <sup>12)</sup>.
- 17) Walid Taha, editor. *Semantics, Applications, and Implementation of Program Generation*, volume 1924 of *Lecture Notes in Computer Science*, Montréal, 2000. Springer-Verlag.
- 18) Walid Taha. A sound reduction semantics for untyped CBN multi-stage computation. Or, the theory of MetaML is non-trivial. In *Proceedings of the Workshop on Partial Evaluation and Semantics-Based Program Manipulation (PEPM)*, Boston, 2000. ACM Press.
- 19) Walid Taha and Michael Florentin Nielsen. Environment classifiers. In *The Symposium on Principles of Programming Languages (POPL '03)*, New Orleans, 2003.
- 20) Walid Taha and Tim Sheard. Mult-stage programming with explicit annotations. In *Proceedings of Symposium on Partial Evaluation and Semantics Based Program manipulation*, pages 203–217. ACM SIGPLAN, 1997.
- 21) David Tarditi, Peter Lee, and Anurag Acharya. No assembly required: Compiling standard ML to C. *ACM Letters on Programming Languages and Systems*, 1(2):161–177, June 1992.

## §1 Type System for the C Fragment

The type system for the target language is defined for a fixed type assignment  $\Sigma$  that assigns types to constants and operators. We assume the type assignment  $\Gamma$  must be well-formed in the sense that it assigns at most one type for each variable.

Expressions ( $\Gamma \vdash e : t$ )

$$\begin{array}{c}
\frac{c : b \in \Sigma}{\Gamma \vdash c : b} \text{Const} \quad \frac{\Gamma(x) = t}{\Gamma \vdash x : t} \text{Var} \quad \frac{f^{(1)} : b \ f(b_1) \in \Sigma \quad \Gamma \vdash e : b_1}{\Gamma \vdash f^{(1)}(e) : b} \text{Op1} \quad \frac{f^{[2]} : b \ f^{[2]}(b_1, b_2) \in \Sigma \quad \Gamma \vdash e_1 : b_1 \quad \Gamma \vdash e_2 : b_2}{\Gamma \vdash e_1 \ f^{[2]} \ e_2 : b} \text{Op2} \\
\\
\frac{\Gamma(x) = b \ (t_i)^{i \in \{ \dots n \}} \quad \{ \Gamma \vdash e_i : t_i \}^{i \in \{ \dots n \}}}{\Gamma \vdash x \ (e_i)^{i \in \{ \dots n \}} : b} \text{FCall} \quad \frac{\Gamma(x) = \text{int}}{\Gamma \vdash x++ : \text{int}} \text{Inc} \quad \frac{\Gamma(x) = \text{int}}{\Gamma \vdash x-- : \text{int}} \text{Dec} \\
\\
\frac{\Gamma(x) = b \ [ \ ] \quad \Gamma \vdash e : \text{int}}{\Gamma \vdash x[e] : b} \text{Arr1} \quad \frac{\Gamma(x) = * \ b \ [ \ ] \quad \Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : \text{int}}{\Gamma \vdash x[e_1][e_2] : b} \text{Arr2} \quad \frac{\Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : t \quad \Gamma \vdash e_3 : t}{\Gamma \vdash e_1 ? e_2 : e_3 : t} \text{If}
\end{array}$$

Statements ( $\Gamma \vdash s : t$ )

To indicate which terms must or can include a return statement, we define a more general judgment  $\Gamma \vdash s : r$ , where  $r$  is defined as follows:

$$r ::= t \mid \perp$$

The  $r$  types indicate return contexts: if a statement is well-formed with respect to the return context  $\perp$ , no return statements are permitted in it. If the return context is  $t$ , the judgment ensures that the rightmost leaf of the statement is a return statement of type  $t$ . For example, the definition body of a function with return type  $t$ , must be typed with  $t$  as its return context.

$$\begin{array}{c}
 \frac{\Gamma \vdash e : t_1}{\Gamma \vdash e : \perp} \text{EStat} \quad \frac{\Gamma(x) = b \quad \Gamma \vdash e : b}{\Gamma \vdash x = e : \perp} \text{Assign} \quad \frac{\Gamma(x) = b[] \quad \Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : b}{\Gamma \vdash x[e_1] = e_2 : \perp} \text{SetArr1} \\
 \\
 \frac{\Gamma(x) = *b[] \quad \Gamma \vdash e_1 : \text{int}}{\Gamma \vdash x[e_1][e_2] = e_3 : \perp} \text{SetArr2} \quad \frac{\Gamma \vdash e_2 : \text{int} \quad \Gamma \vdash e_3 : b}{\Gamma \vdash x[e_1][e_2] = e_3 : \perp} \text{SetArr2} \quad \frac{\Gamma \vdash e : \text{int} \quad \Gamma \vdash s_1 : r \quad \Gamma \vdash s_2 : r}{\Gamma \vdash \text{if } (e) \text{ } s_1 \text{ else } s_2 : r} \text{IfS} \\
 \\
 \frac{\Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash s : \perp}{\Gamma \vdash \text{while } (e_1) \text{ } s : \perp} \text{While} \quad \frac{\Gamma(x) = \text{int} \quad \Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : \text{int} \quad \Gamma \vdash s : \perp}{\Gamma \vdash \text{for } (x = e_1; e_2; x++) \text{ } s : \perp} \text{For} \quad \frac{\Gamma \vdash e : t}{\Gamma \vdash \text{return } (e) : t} \text{Ret} \\
 \\
 \frac{\{c_i : \text{int} \in \Sigma\}^{i \in \{\dots n\}} \quad \Gamma \vdash e : \text{int}}{\Gamma \vdash e : \text{int}} \quad \frac{\{ \Gamma \vdash s_i : \perp \}^{i \in \{\dots n\}} \quad \Gamma \vdash s : \perp}{\Gamma \vdash s : \perp} \quad \frac{\{ \Gamma \cup (d_j)^{j \in \{\dots m\}} \vdash s_i \}^{i \in \{\dots n-1\}} : \perp \quad \Gamma \cup (d_j)^{j \in \{\dots m\}} \vdash s_n : r}{\Gamma \vdash \{(d_j)^{j \in \{\dots m\}} ; (s_n)^{i \in \{\dots n\}}\} : r} \text{Blk} \\
 \Gamma \vdash \left\{ \begin{array}{l} \text{switch } (e) \{ \\ \text{case } c_i : s_i \text{ break;} \\ \text{default : } s \} \end{array} \right\} : \perp \quad \text{Sw}
 \end{array}$$

Function definition ( $\Gamma \vdash f$ )

$$\frac{\Gamma \cup (a_i)^{i \in \{\dots n\}} \vdash \{(d_j)^{j \in \{\dots m\}} ; (s_k)^{k \in \{\dots z\}}\} : b}{\Gamma \vdash (b \text{ f } (a_i)^{i \in \{\dots n\}} \{(d_j)^{j \in \{\dots m\}} ; (s_k)^{k \in \{\dots z\}}\})} \text{TFun}$$

Program ( $\Gamma \vdash g$ )

$$\frac{}{\Gamma \vdash \cdot} \text{Empty} \quad \frac{\Gamma \vdash b \text{ f } (a_i)^{i \in \{\dots n\}} \text{ } s \quad \Gamma, b \text{ f } (a_i)^{i \in \{\dots n\}} \vdash g}{\Gamma \vdash (b \text{ f } (a_i)^{i \in \{\dots n\}} \text{ } s); g} \text{ExtTop}$$

### Lemma 1.1 (Weakening)

1.  $\forall e, \Gamma, \Gamma', t$ . if  $\Gamma \vdash e : t$  and  $\text{dom } \Gamma' \cap FV(e) = \emptyset$ , then  $\Gamma \cup \Gamma' \vdash e : t$ .
2.  $\forall s, \Gamma, \Gamma', r$ . if  $\Gamma \vdash s : r$  and  $\text{dom } \Gamma' \cap FV(s) = \emptyset$ , then  $\Gamma \cup \Gamma' \vdash s : r$ .

**Proof** Proofs are by induction on the height of the typing derivations. ■

## §2 Type System for the OCaml Fragment

Expressions ( $\Gamma \vdash e : t$ )

$$\begin{array}{c}
\frac{\hat{c} : \hat{b} \in \Sigma}{\Gamma \vdash \hat{c} : \hat{b}} \text{Const} \quad \frac{\Gamma(\hat{x}) = \hat{t}}{\Gamma \vdash \hat{x} : \hat{t}} \text{Var} \\
\\
\frac{\Gamma \vdash \hat{x} : (\hat{p}_1, \dots, \hat{p}_n) \rightarrow \hat{b} \quad \{\Gamma \vdash \hat{e}_i : \hat{p}_i\}_{i \in \{1 \dots n\}}}{\Gamma \vdash \hat{x} (e_i)_{i \in \{1 \dots n\}} : \hat{b}} \text{FCall} \quad \frac{\hat{f}^{(1)} : \hat{b}_1 \rightarrow \hat{b} \in \Sigma \quad \Gamma \vdash \hat{e} : \hat{b}_1}{\Gamma \vdash \hat{f}^{(1)} \hat{e} : \hat{b}} \text{Fun[1]} \quad \frac{\hat{f}^{(2)} : \hat{b}_1 \rightarrow \hat{b}_2 \rightarrow \hat{b} \in \Sigma \quad \Gamma \vdash \hat{e}_1 : \hat{b}_1 \quad \Gamma \vdash \hat{e}_2 : \hat{b}_2}{\Gamma \vdash \hat{f}^{(2)} \hat{e}_1 \hat{e}_2 : \hat{b}} \text{Fun(2)} \\
\\
\frac{\hat{f}^{[2]} : \hat{b}_1 \rightarrow \hat{b}_2 \rightarrow \hat{b} \in \Sigma \quad \Gamma \vdash \hat{e}_1 : \hat{b}_1 \quad \Gamma \vdash \hat{e}_2 : \hat{b}_2}{\Gamma \vdash \hat{e}_1 \hat{f}^{[2]} \hat{e}_2 : \hat{b}} \text{Fun[2]} \quad \frac{\Gamma \vdash \hat{e}_1 : \text{bool} \quad \Gamma \vdash \hat{e}_2 : \hat{t} \quad \Gamma \vdash \hat{e}_3 : \hat{t}}{\Gamma \vdash \text{if } \hat{e}_1 \text{ then } \hat{e}_2 \text{ else } \hat{e}_3 : \hat{t}} \text{If} \\
\\
\frac{\Gamma(\hat{x}) = \hat{t} \text{ ref}}{\Gamma \vdash !\hat{x} : \hat{t}} \text{Ref} \quad \frac{\Gamma \vdash \hat{e} : \text{int} \quad \Gamma(\hat{x}) = \hat{b} \text{ array}}{\Gamma \vdash \hat{x}.(\hat{e}) : \hat{b}} \text{Arr1} \quad \frac{\Gamma \vdash \hat{e}_1 : \text{int} \quad \Gamma \vdash \hat{e}_2 : \text{int} \quad \Gamma(\hat{x}) = \hat{b} \text{ array array}}{\Gamma \vdash \hat{x}.(\hat{e}_1).(\hat{e}_2) : \hat{b}} \text{Arr2}
\end{array}$$

Statements ( $\Gamma \vdash d : \hat{t}$ )

$$\begin{array}{c}
\frac{\Gamma \vdash e : t \quad \Gamma \vdash d_1 : \text{unit} \quad \Gamma \vdash d_2 : \hat{t}}{\Gamma \vdash e : t} \text{DExp} \quad \frac{\Gamma \vdash d_1 : \text{unit} \quad \Gamma \vdash d_2 : \hat{t}}{\Gamma \vdash d_1; d_2 : \hat{t}} \text{SeqD} \quad \frac{\Gamma \vdash \hat{e} : \hat{b} \quad \Gamma, \hat{x} : \hat{b} \vdash \hat{d} : \hat{t}}{\Gamma \vdash \left\{ \begin{array}{l} \text{let } \hat{x} : \hat{b} = \hat{e} \\ \text{in } \hat{d} \end{array} \right\} : \hat{t}} \text{Let} \\
\\
\frac{\Gamma \vdash \hat{e} : \hat{b} \quad \Gamma, \hat{x} : \hat{b} \text{ ref } \vdash \hat{d} : \hat{t}}{\Gamma \vdash \left\{ \begin{array}{l} \text{let } \hat{x} : \hat{b} \text{ ref} = \text{ref } \hat{e} \\ \text{in } \hat{d} \end{array} \right\} : \hat{t}} \text{LetRef} \quad \frac{\Gamma \vdash \hat{e}_2 : \hat{b} \quad \Gamma, \hat{x} : \hat{b} \text{ array } \vdash \hat{d} : \hat{t} \quad \Gamma \vdash \hat{c}_1 : \text{int}}{\Gamma \vdash \left\{ \begin{array}{l} \text{let } \hat{x} : \hat{b} \text{ array} = \\ \text{Array.make } \hat{c}_1 \hat{c}_2 \text{ in } \hat{d} \end{array} \right\} : \hat{t}} \text{LetArr1} \\
\\
\frac{\Gamma \vdash \hat{c}_1 : \text{int} \quad \Gamma \vdash \hat{c}_3 : \hat{b} \quad \Gamma \vdash \hat{c}_2 : \text{int} \quad \Gamma, \hat{x} : \hat{b} \text{ array array } \vdash \hat{d} : \hat{t}}{\Gamma \vdash \left\{ \begin{array}{l} \text{let } \hat{x} : \hat{b} \text{ array array} = \\ \text{Array.make\_matrix } \hat{c}_1 \hat{c}_2 \hat{c}_3 \text{ in } \hat{d} \end{array} \right\} : \hat{t}} \text{LetArr2} \quad \frac{\Gamma \vdash \hat{e} : \hat{b} \quad \Gamma(\hat{x}) = \hat{b} \text{ ref}}{\Gamma \vdash (\hat{x} := \hat{e}) : \text{unit}} \text{Ref} \\
\\
\frac{\Gamma(\hat{x}) = \hat{b} \text{ array} \quad \Gamma \vdash \hat{e}_1 : \text{int} \quad \Gamma \vdash \hat{e}_2 : \hat{b}}{\Gamma \vdash \hat{x}.(\hat{e}_1) \leftarrow (\hat{e}_2) : \text{unit}} \text{SetArr1} \quad \frac{\Gamma(\hat{x}) = \hat{b} \text{ array array} \quad \Gamma \vdash \hat{e}_2 : \text{int} \quad \Gamma \vdash \hat{e}_1 : \text{int} \quad \Gamma \vdash \hat{e}_3 : \hat{b}}{\Gamma \vdash \hat{x}.(\hat{e}_1).(\hat{e}_2) \leftarrow (\hat{e}_3) : \text{unit}} \text{SetArr2} \\
\\
\frac{\Gamma \vdash \hat{e} : \text{bool} \quad \Gamma \vdash \hat{d}_1 : \hat{t} \quad \Gamma \vdash \hat{d}_2 : \hat{t}}{\Gamma \vdash \text{if } \hat{e} \text{ then } \hat{d}_1 \text{ else } \hat{d}_2 : \hat{t}} \text{IfD} \quad \frac{\Gamma \vdash \hat{e} : \text{bool} \quad \Gamma \vdash \hat{d} : \text{unit}}{\Gamma \vdash \left\{ \begin{array}{l} \text{while } \hat{e} \\ \text{do } \hat{d} \text{ done} \end{array} \right\} : \text{unit}} \text{While} \\
\\
\frac{z \in \{\text{to, downto}\} \quad \Gamma \vdash \hat{e}_2 : \text{int} \quad \Gamma \vdash \hat{e}_1 : \text{int} \quad \Gamma, \hat{x} : \text{int} \vdash \hat{d} : \text{unit}}{\Gamma \vdash \left\{ \begin{array}{l} \text{for } \hat{x} : \text{int} = \hat{e}_1 \text{ z } \hat{e}_2 \\ \text{do } \hat{d} \text{ done} \end{array} \right\} : \text{unit}} \text{For} \quad \frac{\Gamma \vdash \hat{e} : \hat{b} \quad \hat{b} \neq \text{float} \quad \{\Gamma \vdash \hat{c}_i : \hat{b}\}_{i \in \{1 \dots n\}} \quad \Gamma \vdash \hat{d} : \text{unit} \quad \{\Gamma \vdash \hat{d}_i : \hat{t}\}_{i \in \{1 \dots n\}}}{\Gamma \vdash \left\{ \begin{array}{l} \text{match } \hat{e} \text{ with} \\ ((\hat{c}_i \rightarrow \hat{d}_i))_{i \in \{1 \dots n\}} \\ | \_ \leftarrow \hat{d} \end{array} \right\} : \text{unit}} \text{Match}
\end{array}$$

Programs  $(\Gamma \vdash \hat{s} : \hat{t})$

$$\begin{array}{c}
 \frac{\Gamma, (\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} \vdash \hat{d} : \hat{b}}{\Gamma \vdash \lambda (\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} . (\hat{d} : \hat{b}) : (p_i)^{i \in \{\dots n\}} \rightarrow \hat{b}} \text{Toplevel} \quad \frac{\Gamma \vdash \hat{c} : \hat{b}}{\Gamma, \hat{x} : \hat{b} \vdash \hat{s} : \hat{t}} \text{LetS} \\
 \\
 \frac{\Gamma \vdash \hat{c} : \hat{b}}{\Gamma, \hat{x} : \hat{b} \text{ ref} \vdash \hat{s} : \hat{t}} \text{LetRefS} \quad \frac{\Gamma \cup (\hat{x}_i : \hat{p}_i)^{i \in \{m \dots n\}} \vdash \hat{d} : \hat{b}}{\Gamma \cup (\hat{x}_i : \hat{p}_i)^{i \in \{m \dots n\}}, \hat{x} : (\overline{p_n} \rightarrow \hat{b}) \vdash \hat{s} : \hat{t}} \text{LetFun} \\
 \\
 \frac{\Gamma \vdash \hat{c}_1 : \text{int} \quad \Gamma \vdash \hat{c}_3 : \hat{b}}{\Gamma \vdash \hat{c}_2 : \text{int} \quad \Gamma, \hat{x} : \hat{b} \text{ array array} \vdash \hat{s} : \hat{t}} \text{LetArr2S} \quad \frac{\Gamma \vdash \hat{c}_1 : \text{int} \quad \Gamma \vdash \hat{c}_2 : \hat{b}}{\Gamma, \hat{x} : \hat{b} \text{ array} \vdash \hat{s} : \hat{t}} \text{LetArr1S} \\
 \\
 \Gamma \vdash \left\{ \text{let } \hat{x} : \hat{b} \text{ array array} = \text{Array.make\_matrix } \hat{c}_1 \ \hat{c}_2 \ \hat{c}_3 \text{ in } \hat{s} \right\} : \hat{t} \quad \Gamma \vdash \left\{ \text{let } \hat{x} : \hat{b} \text{ array} = \text{Array.make } \hat{c}_1 \ \hat{c}_2 \text{ in } \hat{s} \right\} : \hat{t}
 \end{array}$$

### §3 Offshoring Translation

This section formalizes the translation from the OCaml subset to C. OCaml types and expressions are translated directly into C types and expressions.

$$\begin{array}{l}
 \boxed{[[\hat{t}]]} \\
 \begin{array}{l}
 [[\text{int}]] = \text{int} \\
 [[\text{bool}]] = \text{int} \\
 [[\text{char}]] = \text{char} \\
 [[\text{float}]] = \text{double} \\
 [[b \text{ array}]] = [[b]] [] \\
 [[b \text{ array array}]] = *[[b]] []
 \end{array} \\
 \boxed{[[\hat{e}]]} \\
 \begin{array}{l}
 [[\hat{c}]] = c \\
 [[\hat{x}]] = x \\
 [[\hat{x}(\hat{e}_1, \dots, \hat{e}_n)]] = x([[ \hat{e}_1 ]], \dots, [[ \hat{e}_n ]]) \\
 [[\hat{f}^{(1)} \hat{e}]] = [[ \hat{f}^{(1)} ]][[\hat{e}]] \\
 [[\hat{f}^{(2)} \hat{e}_1 \hat{e}_2]] = [[ \hat{f}^{(2)} ]][[\hat{e}_1]][[\hat{e}_2]] \\
 [[\hat{e}_1 \hat{f}^{(2)} \hat{e}_2]] = [[ \hat{e}_1 ]][[\hat{f}^{(2)}]][[\hat{e}_2]] \\
 [[\text{if } \hat{e}_1 \text{ then } \hat{e}_2 \text{ else } \hat{e}_3]] = [[ \hat{e}_1 ]][[\hat{e}_2]] : [[ \hat{e}_3 ]]] \\
 [[!\hat{x}]] = x \\
 [[\hat{x}(\hat{e})]] = x([[ \hat{e} ]]) \\
 [[\hat{x}(\hat{e}_1)(\hat{e}_2)]] = x([[ \hat{e}_1 ]][[\hat{e}_2]])
 \end{array}
 \end{array}$$

The statement subset of OCaml is translated to a pair  $(\bar{l}, \bar{s})$ , where  $\bar{l}$  are declarations of variables that are bound in OCaml **let** expressions, and  $\bar{s}$ , the sequence of C statements that corresponds to OCaml statements. The translation for OCaml statements  $\{\hat{d}\}$  is written with a *return context* which can be  $\perp$  or  $\top$ .

$$\text{Return context } a ::= \perp \mid \top$$

If the return context is  $\perp$ , the translation does not generate **return** statements at the leaves; on the other hand, if the return context is  $\top$ , bottoming out at a leaf OCaml expression produces the appropriate C **return** statement.

$$\boxed{\{\hat{d}\}_a = (l, s)}$$

$$\begin{array}{c}
\frac{}{\{\hat{e}\}_\perp = (\cdot, \llbracket \hat{e} \rrbracket)} \quad \frac{}{\{\hat{e}\}_\top = (\cdot, \mathbf{return} \llbracket \hat{e} \rrbracket)} \quad \frac{}{\{\hat{x} := \hat{e}\}_\perp = (\cdot, x = \llbracket \hat{e} \rrbracket)} \quad \frac{}{\{\hat{x}.(\hat{e}_1) \leftarrow \hat{e}_2\}_\perp = (\cdot, x[\llbracket \hat{e}_1 \rrbracket] = \llbracket \hat{e}_2 \rrbracket)} \\
\frac{}{\{\hat{d}\}_a = (l, s)} \\
\frac{}{\{\hat{x}.(\hat{e}_1).(\hat{e}_2) \leftarrow \hat{e}_3\}_\perp = (\cdot, x[\llbracket \hat{e}_1 \rrbracket][\llbracket \hat{e}_2 \rrbracket] = \llbracket \hat{e}_3 \rrbracket)} \quad \frac{}{\left\{ \begin{array}{l} \mathbf{let} \hat{x} : \hat{t} = \hat{e} \\ \mathbf{in} \hat{d} \end{array} \right\}}_a = ((\llbracket \hat{t} \rrbracket x; l), (x = \llbracket \hat{e} \rrbracket; s)) \\
\frac{}{\{\hat{d}_1\}_\perp = (l_1, s_1)} \quad \frac{}{\{\hat{d}_2\}_a = (l_2, s_2)} \quad \frac{}{\{\hat{d}\}_a = (l, s)} \\
\frac{}{\{\hat{d}_1; \hat{d}_2\}_a = (l_1; l_2, s_1; s_2)} \quad \frac{}{\{\mathbf{let} \hat{x} : \mathbf{ref} \hat{t} = \mathbf{ref} \hat{c} \mathbf{in} \hat{d}\}_a = ((\llbracket \hat{t} \rrbracket (c)x; l), (x = \llbracket c \rrbracket; s))} \\
\frac{}{\left\{ \begin{array}{l} \mathbf{let} x : \hat{t} \mathbf{array} = \\ \mathbf{Array.make} \hat{c}_1 \hat{c}_2 \mathbf{in} \hat{d} \end{array} \right\}}_a = \frac{}{\left\{ \begin{array}{l} \mathbf{let} \hat{x} : \hat{t} \mathbf{array} \mathbf{array} = \\ \mathbf{Array.make\_matrix} \hat{e} \hat{c}_2 \hat{c}_3 \mathbf{in} \hat{d} \end{array} \right\}}_a = \\
\frac{}{\left( \llbracket \hat{t} \rrbracket x[] = \{\overline{c_2}^{c_1 \text{ times}}\}, l; s \right)} \quad \frac{}{\left( \llbracket \hat{t} \rrbracket y_m = \{\llbracket \hat{e} \rrbracket^{c_2 \text{ times}}\}^{c_1 \text{ times}}; \right.} \\
\left. \llbracket \hat{t} \rrbracket * x[] = \{y_1, \dots, y_{c_1}\}; l, s \right)} \\
\frac{}{\{\hat{d}_1\}_a = (l_1, s_1)} \quad \frac{}{\{\hat{d}_2\}_a = (l_2, s_2)} \quad \frac{}{\{\hat{d}\}_\perp = (l, s)} \\
\frac{}{\{\mathbf{if} (\hat{e}) \mathbf{then} \hat{d}_1 \mathbf{else} \hat{d}_2\}_a = (\cdot, \mathbf{if} (\llbracket \hat{e} \rrbracket) \{l_1; s_1\} \mathbf{else} \{l_2; s_2\})} \quad \frac{}{\{\mathbf{while} (\hat{e}) \mathbf{do} \hat{d} \mathbf{done}\}_\perp = (\cdot, \mathbf{while} (\llbracket \hat{e} \rrbracket) \{l; s\})} \\
\frac{}{\{\hat{d}\}_\perp = (l, s)} \quad \frac{}{\{\hat{d}\}_\perp = (l, s)} \\
\frac{}{\{\mathbf{for} \hat{x} = \hat{e}_1 \mathbf{to} \hat{e}_2 \mathbf{do} \hat{d} \mathbf{done}\}_\perp = (\mathbf{int} x, \mathbf{for} (x = \llbracket \hat{e}_1 \rrbracket; x <= \llbracket \hat{e}_2 \rrbracket; x++) \{l; s\})} \quad \frac{}{\{\mathbf{for} \hat{x} = \hat{e}_1 \mathbf{downto} \hat{e}_2 \mathbf{do} \hat{d} \mathbf{done}\}_\perp = (\mathbf{int} x, \mathbf{for} (x = \llbracket \hat{e}_1 \rrbracket; x >= \llbracket \hat{e}_2 \rrbracket; x--) \{l; s\})} \\
\frac{}{\{\hat{d}_n\}_\perp = (l_n, s_n)} \quad \frac{}{\{\hat{d}\}_\perp = (l, s)} \\
\frac{}{\{\mathbf{match} \hat{e} \mathbf{with} \hat{c}_n \rightarrow \hat{d}_{n,n} \mid \_ \rightarrow \hat{d}\}_\perp = \mathbf{case} c_n : \{l_n; s_n; \mathbf{break}\}; \mathbf{default} : \{l; s\}}
\end{array}$$

OCaml programs  $\hat{s}$  are translated into a pair  $(g, l)$ , where  $g$  is a sequence of function definitions and  $l$  is a sequence of variable declarations. Note, we use the name *procedure* for our main function, which is different than any other function, so we can assume there are no name clashes with the procedure names.

$$\boxed{\langle \hat{s} \rangle = (g, l)}$$

$$\begin{array}{c}
\frac{}{\langle \hat{s} \rangle = (g, l)} \quad \frac{}{\langle \hat{s} \rangle = (g, l)} \quad \frac{}{\langle \hat{s} \rangle = (g, l)} \\
\frac{}{\langle \mathbf{let} \hat{x} : \hat{t} = \hat{c} \mathbf{in} \hat{s} \rangle = (g, (\llbracket \hat{t} \rrbracket x = c; l))} \quad \frac{}{\langle \mathbf{let} \hat{x} : \mathbf{ref} \hat{t} = \mathbf{ref} \hat{c} \mathbf{in} \hat{s} \rangle = (g, \llbracket \hat{t} \rrbracket x = c; l)} \quad \frac{}{\left\{ \begin{array}{l} \mathbf{let} \hat{x} : \hat{t} \mathbf{array} = \\ \mathbf{Array.make} \hat{c}_1 \hat{c}_2 \mathbf{in} \hat{s} \end{array} \right\}} = \\
(g, \llbracket \hat{t} \rrbracket x[] = \{\overline{c_2}^{c_1 \text{ times}}\}; l)} \\
\frac{}{\langle \hat{d} \rangle = (g, l)} \quad (y_i \text{ fresh})^{i \in \{1 \dots c_1\}} \\
\frac{}{\langle \mathbf{let} \hat{x} : \hat{t} \mathbf{array} \mathbf{array} = \mathbf{Array.make\_matrix} \hat{e} \hat{c}_2 \hat{c}_3 \mathbf{in} \hat{d} \rangle_a = (g, \left( \llbracket \hat{t} \rrbracket y_i = \{\llbracket \hat{e} \rrbracket^{c_2 \text{ times}}\}^{i \in \{1 \dots c_1\}}; \right.} \\
\left. \llbracket \hat{t} \rrbracket * x[] = \{y_1, \dots, y_{c_1}\}; l \right)} \\
\frac{}{\langle \hat{s} \rangle = (g, l)} \quad \frac{}{\langle \hat{d} \rangle_\top = (l, s)} \quad \frac{}{\langle \hat{d} \rangle_\top = (l, s)} \\
\frac{}{\langle \mathbf{let} \hat{f} (\hat{x}_i : \hat{p}_i)^{i \in \{1 \dots n\}} : \hat{b} = \hat{d} \mathbf{in} \hat{s} \rangle = (\llbracket \hat{b} \rrbracket f (\llbracket \hat{p} \rrbracket_i x_i)^{i \in \{1 \dots n\}} \{l_d; s_d; \}; g, l)} \quad \frac{}{\langle \lambda (\hat{x}_i : \hat{p}_i)^{i \in \{1 \dots n\}} . (\hat{d} : \hat{b}) \rangle = ((\llbracket \hat{b} \rrbracket \mathbf{procedure} (\llbracket \hat{p} \rrbracket_i x_i)^{i \in \{1 \dots n\}} \{l; s\}), \cdot)}
\end{array}$$

**Lemma 3.1 (Basic properties of translation.)**

1. Translation relations  $\{\cdot\} = (\cdot, \cdot)$ , and  $\langle\cdot\rangle = (\cdot, \cdot)$  are functions.
2. If  $\{\hat{d}\} = (l, s)$ , then  $\text{dom } l \subseteq BV(d)$ . If  $\langle\hat{s}\rangle = (g, l)$ , then  $\text{dom } l \subseteq BV(s)$ ,  $\text{dom } g \subseteq BV(s)$  and  $\text{dom } l \cap \text{dom } g = \emptyset$ .

**Proof** Both proofs are by induction on the type derivations and translation relation derivations, respectively.  $\blacksquare$

## §4 Type Preservation

The main technical result we present in this paper is that the offshoring translation preserves well-typedness of programs: a well-typed OCaml program from the designated subset of OCaml is translated into a well-typed C program in the designated subset of C.

First, we define an operation  $|\cdot|$  which translates variable declarations and function definitions to C type assignments.

$$\begin{aligned}
 |\cdot| &= \emptyset \\
 |t \ x = \_ ; l| &= \{x : t\} \cup |l| \\
 |t \ f \ (t_i)^{i \in \{ \dots n \}} \ s ; g| &= \{t \ f \ (t_i)^{i \in \{ \dots n \}}\} \cup |g|
 \end{aligned}$$

We also define an operation  $\llbracket \hat{\Gamma} \rrbracket$  which translates the OCaml variable and function environment,  $\hat{\Gamma}$ , into the corresponding C environment.

$$\begin{aligned}
 \llbracket \cdot \rrbracket &= \emptyset \\
 \llbracket \hat{\Gamma} ; \hat{x} : \hat{b} \rrbracket &= \llbracket \hat{\Gamma} \rrbracket \cup \{x : \llbracket \hat{b} \rrbracket\} \\
 \llbracket \hat{\Gamma} ; (\hat{x}_i : \hat{p}_i)^{i \in \{ m \dots n \}} , \hat{x} : (\overline{p_n} \rightarrow \hat{b}) \rrbracket &= \llbracket \hat{\Gamma} \rrbracket \cup \{ \llbracket \hat{b} \rrbracket \ x(\llbracket p_n \rrbracket) \}
 \end{aligned}$$

Throughout the proofs the following assumption about free and bound variables in OCaml and C programs will be considered to hold:

**Assumption 1**

For any finite set of terms, no two bound variables in these terms have the same name.

Assumption 1 allows us to treat the nested scoping of OCaml let statements, in which a variable can be rebound (e.g., `let x = 1 in let x = 2 in x`), as

morally equivalent to the flat scoping of C declarations and statements into which they are translated.

**Theorem 4.1 (Type preservation).** If  $\hat{\Gamma} \vdash \hat{s} : \hat{a}_n \rightarrow \hat{b}$  and  $\langle \hat{s} \rangle = (g, l)$ , then  $\llbracket \hat{\Gamma} \rrbracket \cup |l| \cup |g| \vdash g$ .

**Proof** Proof is by induction on the height of various derivations.

1. **Case**  $\Gamma \vdash \lambda(\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} . (\hat{d} : \hat{b}) : (p_i)^{i \in \{\dots n\}} \rightarrow \hat{b}$ . By inversion of typing for programs,  $\Gamma, (\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} \vdash \hat{d} : \hat{b}$ . By translation for programs,  $\langle \lambda(\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} . (\hat{d} : \hat{b}) : (p_i)^{i \in \{\dots n\}} \rightarrow \hat{b} \rangle = (\llbracket \hat{b} \rrbracket \text{ procedure } (\llbracket \hat{p}_i \rrbracket x_i)^{i \in \{\dots n\}} \{l; s\}, \cdot)$  where  $\{\hat{d}\}_\top = (l, s)$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{b} \rrbracket \text{ procedure } (\llbracket \hat{p}_i \rrbracket x_i)^{i \in \{\dots n\}} \{l; s\}$ . This is true if  $\llbracket \hat{\Gamma} \rrbracket \cup (\llbracket \hat{p}_i \rrbracket x_i)^{i \in \{\dots n\}} \vdash \{l; s\} : \llbracket \hat{b} \rrbracket$  following the C TFun typing rule. We know this immediately by Lemma 4.1.3 and by definition of  $\llbracket \hat{\Gamma} \rrbracket$ .
2. **Case**  $\hat{\Gamma} \vdash \text{let } \hat{x} : \hat{b} = \hat{c} \text{ in } \hat{s} : \hat{t}$ . We are also given  $\langle \text{let } \hat{x} : \hat{b} = \hat{c} \text{ in } \hat{s} \rangle = (g, l)$ . By inversion of typing for programs, we know that  $\hat{\Gamma} \vdash \hat{c} : \hat{b}$  and  $\hat{\Gamma}, \hat{x} : \hat{b} \vdash \hat{s} : \hat{t}$ . Let  $\langle \hat{s} \rangle = (g', l')$ . Then we know by the translation function  $\langle \text{let } x : \hat{b} = \hat{c} \text{ in } \hat{s} \rangle = (g', (\llbracket \hat{b} \rrbracket x = \hat{c}; l'))$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \cup |l| \cup |g| \vdash g$ . By the induction hypothesis,  $\llbracket \hat{\Gamma}, b x \rrbracket \cup |l'| \cup |g'| \vdash g'$ . But now by definition of  $\llbracket \hat{\Gamma} \rrbracket$ ,  $\llbracket \hat{\Gamma} \rrbracket \cup \{b x\} \cup |l'| \cup |g'| \vdash g'$ . However, what is given and what we know by the translation function imply  $|g'| = |g|$  and  $\{b x\} \cup |l'| = |l|$ . Therefore,  $\llbracket \hat{\Gamma} \rrbracket \cup |l| \cup |g| \vdash g$ .
3. **Case**  $\text{let } \hat{x} (x_i : \hat{p}_i)^{i \in \{\dots n\}} : \hat{b} = \hat{d} \text{ in } \hat{s} : \hat{t}$ . We are also given  $\langle \text{let } \hat{x} (x_i : \hat{p}_i)^{i \in \{\dots n\}} = \hat{d} \text{ in } \hat{s} \rangle = (g, l)$ . By inversion of OCaml function typing, we know  $\Gamma \cup (\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}} \vdash \hat{d} : \hat{b}$  and  $\Gamma \cup (\hat{x}_i : \hat{p}_i)^{i \in \{\dots n\}}, \hat{x} : (\overline{p_n} \rightarrow \hat{b}) \vdash \hat{s} : \hat{t}$ . By translation we know that  $\langle \text{let } \hat{x} (x_i : \hat{p}_i)^{i \in \{\dots n\}} : \hat{b} = \hat{d} \text{ in } \hat{s} \rangle = (\llbracket \hat{b} \rrbracket x (\llbracket p \rrbracket_i x_i)^{i \in \{\dots n\}} \{l_d; s_d\}; g', l')$  where  $\langle \hat{s} \rangle = (g', l')$  and  $\{\hat{d}\}_\top = (l_d, s_d)$ . We are trying to show  $\llbracket \hat{\Gamma} \rrbracket \cup |l'| \cup \llbracket \hat{b} \rrbracket x (\llbracket p_n \rrbracket) \cup |g'| \vdash (\llbracket \hat{b} \rrbracket x (\llbracket p \rrbracket_i x_i)^{i \in \{\dots n\}} \{l_d; s_d\}; g')$ . By induction we have  $\llbracket \hat{\Gamma} \rrbracket \cup \llbracket \hat{b} \rrbracket x (\llbracket p_n \rrbracket) \cup |l'| \cup |g'| \vdash g'$ . Also by Lemma 4.1.3 and weakening, the function definition is well-typed, i.e.:  $\llbracket \hat{\Gamma} \rrbracket \cup |l_d| \cup |s_d| \vdash (\llbracket \hat{b} \rrbracket x (\llbracket p \rrbracket_i x_i)^{i \in \{\dots n\}} \{l_d; s_d\} : \llbracket \hat{b} \rrbracket)$ . By C TFun,  $\llbracket \hat{\Gamma} \rrbracket \vdash (\llbracket \hat{b} \rrbracket x (\llbracket p \rrbracket_i x_i)^{i \in \{\dots n\}} \{l_d; s_d\})$ . Now by the C program typing  $\llbracket \hat{\Gamma} \rrbracket \cup \llbracket \hat{b} \rrbracket x (\llbracket p_n \rrbracket) \cup |l'| \cup |g'| \vdash (\llbracket \hat{b} \rrbracket x (\llbracket p \rrbracket_i x_i)^{i \in \{\dots n\}} \{l_d; s_d\}; g')$ .
4. **Case**  $\hat{\Gamma} \vdash \text{let } x : \hat{b} \text{ ref} = \text{ref } \hat{c} \text{ in } \hat{s} : \hat{t}$ . By inversion of OCaml typing, we know that  $\hat{\Gamma} \vdash \hat{c} : \hat{b}$  and that  $\hat{\Gamma}, \hat{x} : \hat{b} \text{ ref} \vdash \hat{s} : \hat{t}$ . Let  $\langle \hat{s} \rangle = (g, l)$ .

By translation,  $\langle \mathbf{ref} = \mathbf{ref} \hat{c} \text{ in } \hat{s} \rangle = (g, (\llbracket \hat{b} \rrbracket x = c, l))$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \cup |g| \cup |l| \cup \{b x\} \vdash g$ . By the induction hypothesis,  $\llbracket \hat{\Gamma}, b x \rrbracket \cup |g| \cup |l| \vdash g$ . But now by definition of  $\llbracket \hat{\Gamma} \rrbracket$ ,  $\llbracket \hat{\Gamma} \rrbracket \cup |g| \cup |l| \cup \{b x\} \vdash g$ .

5. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \text{ array} = \mathbf{Array.make} \hat{c}_1 \hat{c}_2 \text{ in } \hat{s} : \hat{t}$ . By inversion of OCaml typing, we know that  $\hat{\Gamma} \vdash \hat{c}_1 : \mathit{int}$ ,  $\hat{\Gamma} \vdash \hat{c}_2 : \hat{b}$  and that  $\hat{\Gamma}, \hat{x} : \hat{b} \text{ array} \vdash \hat{s} : \hat{t}$ . Let  $\langle \hat{s} \rangle = (g, l)$ . By translation,  $\langle \hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \text{ array} = \mathbf{Array.make} \hat{c}_1 \hat{c}_2 \text{ in } \hat{s} \rangle = (g, \{\llbracket \hat{b} \rrbracket x[] = \{\llbracket \hat{c}_2 \rrbracket, \dots, \llbracket \hat{c}_2 \rrbracket\}\}; l)$ . By type preservation of expressions, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash c_1 : \mathit{int}$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash c_2 : \llbracket \hat{b} \rrbracket$ . Thus we know that the definition of the array is legal. We must show that  $\llbracket \hat{\Gamma} \rrbracket \cup |l| \cup |g| \cup \{b x[]\} \vdash g$ . By the induction hypothesis,  $\llbracket \hat{\Gamma}, b x[] \rrbracket \cup |l| \cup |g| \vdash g$ . But now by definition of  $\llbracket \hat{\Gamma} \rrbracket$ , we have  $\llbracket \hat{\Gamma} \rrbracket \cup |l| \cup |g| \cup \{b x[]\} \vdash g$ .
6. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \text{ array array} = \mathbf{Array.make\_matrix} \hat{c}_1 \hat{c}_2 \hat{c}_3 \text{ in } \hat{s} : \hat{t}$ . Similar to previous case. ■

#### Lemma 4.1 (Type preservation for expressions and statements)

1.  $\forall \hat{\Gamma}, \hat{e}, \hat{t}$ . if  $\hat{\Gamma} \vdash \hat{e} : \hat{\tau}$ , then  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \llbracket \hat{t} \rrbracket$
2.  $\forall \hat{\Gamma}, \hat{d}$ . if  $\hat{\Gamma} \vdash \hat{d} : \hat{t}$ , and  $\{\hat{d}\}_\perp = (l, s)$ , then  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l, s\} : \perp$
3.  $\forall \hat{\Gamma}, \hat{d}$ . if  $\hat{\Gamma} \vdash \hat{d} : \hat{t}$ , and  $\{\hat{d}\}_\top = (l, s)$ , then  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l, s\} : \llbracket \hat{t} \rrbracket$

**Proof** [Lemma 4.1.1] Proof is by induction on the height of the typing derivation of expressions.

1. **Case**  $\hat{\Gamma} \vdash \hat{c} : \hat{t}$ . Base case. Constants are translated to constants, the rules are virtually identical.
2. **Case**  $\hat{\Gamma} \vdash \hat{x} : \hat{t}$ . Base case. By inversion, of the typing judgment, we have  $\hat{\Gamma}(\hat{x}) = \hat{t}$ . Then, by definition of  $\llbracket \cdot \rrbracket$ ,  $\llbracket \hat{\Gamma} \rrbracket(x) = \llbracket \hat{t} \rrbracket$ , and therefore by the C **Var** rule  $\llbracket \hat{\Gamma} \rrbracket \vdash x : \llbracket \hat{t} \rrbracket$ .
3. **Case**  $\hat{\Gamma} \vdash \hat{x} (\hat{e}_1, \dots, \hat{e}_n) : \hat{b}$ . By inversion we have  $\hat{\Gamma} \vdash \hat{x} : (\hat{p}_1, \dots, \hat{p}_n) \rightarrow \hat{b}$  thus  $\hat{\Gamma}(\hat{x}) = (\hat{p}_i)^{i \in \{1..n\}} \rightarrow \hat{b}$ , and we have  $\forall i. 0 \leq i \leq n$ ,  $\hat{\Gamma} \vdash \hat{e}_i : \hat{p}_i$ . We apply the induction hypothesis to  $\forall i. 0 \leq i \leq n$ ,  $\hat{\Gamma} \vdash \hat{e}_i : \hat{p}_i$  to obtain  $\forall i. 0 \leq i \leq n$ ,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_i \rrbracket : \llbracket \hat{p}_i \rrbracket$ . Then, by the C **Fcall** rule, we have  $\llbracket \hat{\Gamma} \rrbracket \vdash x(\llbracket \hat{e}_1 \rrbracket, \dots, \llbracket \hat{e}_n \rrbracket) : \llbracket \hat{b} \rrbracket$ .
4. **Case**  $\hat{\Gamma} \vdash f^{(1)} \hat{e} : \hat{b}$ . By inversion we have  $f^{(1)} : \hat{b}_1 \rightarrow \hat{b} \in \Sigma$  and  $\hat{\Gamma} \vdash \hat{e} : \hat{b}_1$ . We apply the induction hypothesis to  $\hat{\Gamma} \vdash \hat{e} : \hat{b}_1$  to obtain

- $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \llbracket \hat{b}_1 \rrbracket$ . Then, by the C **Op1** rule, we have  $\llbracket \hat{\Gamma} \rrbracket \vdash f^{(1)}(\llbracket \hat{e} \rrbracket) : \llbracket \hat{b} \rrbracket$ .
5. **Case**  $\hat{\Gamma} \vdash f^{(2)} \hat{e}_1 \hat{e}_2 : \hat{b}$ . Similar to previous case.
  6. **Case**  $\hat{\Gamma} \vdash \hat{e}_1 f^{[2]} \hat{e}_2 : \hat{b}$ . Similar to previous case.
  7. **Case**  $\hat{\Gamma} \vdash \text{if } \hat{e}_1 \text{ then } \hat{e}_2 \text{ else } \hat{e}_3 : \hat{t}$ . By inversion, followed by the induction hypothesis, we obtain  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_1 \rrbracket : \text{int}$ ,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_2 \rrbracket : \llbracket \hat{t} \rrbracket$ ,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_3 \rrbracket : \llbracket \hat{t} \rrbracket$ . Then, by definition of  $\vdash$ , we have  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_1 \rrbracket ? \llbracket \hat{e}_2 \rrbracket : \hat{e}_3 : \llbracket \hat{t} \rrbracket$ .
  8. **Case**  $\hat{\Gamma} \vdash !\hat{x} : \hat{t}$ . Base case. By inversion we have  $\hat{\Gamma}(\hat{x}) = \hat{t}$  **ref**. By definition of  $\llbracket \hat{\Gamma} \rrbracket$ ,  $\llbracket \hat{\Gamma} \rrbracket(x) = \llbracket \hat{t} \rrbracket$ . Then, by the C **if** rule, we have  $\llbracket \hat{\Gamma} \rrbracket \vdash x : \llbracket \hat{t} \text{ ref} \rrbracket$ .
  9. **Case**  $\hat{\Gamma} \vdash \hat{x}.\hat{e} : \hat{b}$ . By inversion of  $\vdash$ , we obtain  $\hat{\Gamma} \vdash \hat{e} : \text{int}$  and  $\hat{\Gamma}(\hat{x}) = \hat{b}$  **array**. We apply the induction hypothesis to  $\hat{\Gamma} \vdash \hat{e} : \text{int}$  to obtain  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \text{int}$ . Also, by definition of  $\llbracket \hat{\Gamma} \rrbracket$ , we have  $\llbracket \hat{\Gamma} \rrbracket(x) = b$ . Applying the **Arr1** rule of  $\vdash$ , we obtain  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{x}.\hat{e} \rrbracket : \llbracket \hat{b} \rrbracket$ .
  10. **Case**  $\hat{\Gamma} \vdash \hat{x}.\hat{e}_1.\hat{e}_2 : \hat{b}$ . Similar to (9).

■

**Proof** [Lemma 4.1.2] Proof is by induction on the height of the typing derivation of statements.

1. **Case**  $\hat{\Gamma} \vdash \hat{e} : \hat{t}$ . It is given that  $\{\hat{e}\}_\perp = (l, s)$ . Consider the case when by translation  $\{\hat{e}\}_\perp = (\cdot, \llbracket \hat{e} \rrbracket)$ . We know  $l = \cdot$  and  $s = \llbracket \hat{e} \rrbracket$ . By Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \llbracket \hat{t} \rrbracket$ , thus by the C **EStat** rule  $\llbracket \hat{\Gamma} \rrbracket \vdash (\cdot, \llbracket \hat{e} \rrbracket) : \perp$ .
2. **Case**  $\hat{\Gamma} \vdash \hat{d}_1; \hat{d}_2 : \hat{t}$ . It is given that  $\{\hat{d}_1; \hat{d}_2\}_\perp = (l, s)$ . Having  $\hat{\Gamma} \vdash \hat{d}_1; \hat{d}_2 : \hat{t}$ , by inversion we know that  $\hat{\Gamma} \vdash \hat{d}_1 : \text{unit}$  and  $\hat{\Gamma} \vdash \hat{d}_2 : \hat{t}$ . Let  $\{\hat{d}_1\}_\perp = (l_1, s_1)$  and  $\{\hat{d}_2\}_\perp = (l_2, s_2)$ . By translation,  $\{\hat{d}_1; \hat{d}_2\}_\perp = (l_1; l_2, s_1; s_2)$ . We know  $l = l_1; l_2$  and  $s = s_1; s_2$ . We are trying to show  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1; l_2, s_1; s_2\} : \perp$ . We apply the induction hypothesis to  $\hat{\Gamma} \vdash \hat{d}_1 : \text{unit}$  and  $\hat{\Gamma} \vdash \hat{d}_2 : \hat{t}$  to obtain  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1, s_1\} : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_2, s_2\} : \perp$ . By inversion of the C **Blk** rule for  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1, s_1\} : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_2, s_2\} : \perp$ , we have  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \vdash s_1 : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \cup |l_2| \vdash s_2 : \perp$ . By Lemma 3.1.2 we know  $\text{dom } l_1 \subseteq BV(d_1)$  and  $\text{dom } l_2 \subseteq BV(d_2)$ . Now by Assumption 1,  $\text{dom } l_1 \cap \text{dom } l_2 = \emptyset$ . We can conclude, by weakening that  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \cup |l_2| \vdash s_1 : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \cup |l_2| \vdash s_2 : \perp$ . The final result,  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1; l_2, s_1; s_2\} : \perp$ , follows by the C rule **Blk**.
3. **Case**  $\hat{\Gamma} \vdash \hat{x} := \hat{e} : \text{unit}$ . It is given that  $\{\hat{x} := \hat{e}\}_\perp = (l, s)$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{e} : \hat{b}$  and  $\hat{\Gamma}(\hat{x}) = \hat{b}$  **ref**. Let  $\{\hat{x} :=$

$\hat{e}\}_{\perp} = (\cdot, x = \llbracket \hat{e} \rrbracket)$ . By Lemma 4.1.1, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash e : \llbracket \hat{b} \rrbracket$ . By definition of  $\llbracket \hat{\Gamma} \rrbracket$ , we know  $\llbracket \hat{\Gamma} \rrbracket(x) = \llbracket \hat{b} \rrbracket$ . Therefore, by the C Assign rule,  $\llbracket \hat{\Gamma} \rrbracket \vdash x = \llbracket \hat{e} \rrbracket : \perp$ .

4. **Case**  $\hat{\Gamma} \vdash \text{let } x : \hat{b} = \hat{e} \text{ in } \hat{d} : \hat{t}$ . It is given that  $\{\text{let } x = \hat{e} \text{ in } \hat{d}\}_{\perp} = (l, s)$ . By inversion of OCaml typing, we know that  $\hat{\Gamma} \vdash \hat{e} : \hat{b}$  and  $\hat{\Gamma}, \hat{x} : \hat{b} \vdash \hat{d} : \hat{t}$ . Let  $\{\hat{d}\}_{\perp} = (l', s')$ . Then by translation we know  $\{\text{let } x : \hat{b} = \hat{e} \text{ in } \hat{d}\}_{\perp} = ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{e} \rrbracket; s'))$ . By Lemma 4.1.1, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash e : \llbracket \hat{b} \rrbracket$ . By the C Assign rule, we know  $\llbracket \hat{\Gamma} \rrbracket \vdash x = e : \perp$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \vdash ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{e} \rrbracket; s')) : \perp$ . By the induction hypothesis,  $\llbracket \hat{\Gamma} \rrbracket, \hat{x} : \hat{b} \vdash (l', s') : \perp$ . The final result follows by the C Blk rule.
5. **Case**  $\hat{\Gamma} \vdash \text{let } x : \hat{b} \text{ ref} = \text{ref } \hat{c} \text{ in } \hat{d} : \hat{t}$ . It is given that  $\{\text{let } x = \text{ref } \hat{c} \text{ in } \hat{d}\}_{\perp} = (l, s)$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{c} : \hat{b} \text{ ref}$  and  $\hat{\Gamma}, \hat{x} : \hat{b} \text{ ref} \vdash \hat{d} : \hat{t}$ . Let  $\{\hat{d}\}_{\perp} = (l', s')$ . Then by translation we know  $\{\text{let } x : \hat{b} \text{ ref} = \text{ref } \hat{c} \text{ in } \hat{d}\}_{\perp} = ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{c} \rrbracket; s'))$ . By Lemma 4.1.1, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash c : \llbracket \hat{b} \rrbracket$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \vdash ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{c} \rrbracket; s'))$ . By the induction hypothesis,  $\llbracket \hat{\Gamma} \rrbracket \vdash (l', s')$ . The final result follows by the C Blk rule.
6. **Case**  $\hat{\Gamma} \vdash \text{let } x : \hat{b} \text{ array} = \text{Array.make } \hat{c}_1 \hat{c}_2 \text{ in } \hat{d} : \hat{t}$ . It is given that  $\{\text{let } x = \text{Array.make } \hat{c}_1 \hat{c}_2 \text{ in } \hat{d}\}_{\perp} = (l, s)$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{c}_1 : \text{int}$ ,  $\hat{\Gamma} \vdash \hat{c}_2 : \hat{b}$  and that  $\hat{\Gamma}, \hat{x} : \hat{b} \text{ array} \vdash \hat{d} : \hat{t}$ . By translation,  $\{\hat{\Gamma} \vdash \text{let } x : \hat{b} \text{ array} = \text{Array.make } \hat{c}_1 \hat{c}_2 \text{ in } \hat{d}\}_{\perp} = (\llbracket \hat{t} \rrbracket x \square = \{\overline{\hat{c}_2}^{\text{times}}\}, l'; s')$  where  $\{\hat{d}\}_{\perp} = (l', s')$ . By Lemma 4.1.1, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash c_1 : \text{int}$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash c_2 : \llbracket \hat{b} \rrbracket$ . Thus we know the definition of the array is valid. Also, by definition of  $\llbracket \hat{\Gamma} \rrbracket$ , we have  $\llbracket \hat{\Gamma} \rrbracket(x) = \llbracket \hat{b} \rrbracket$ . We now apply the induction hypothesis to  $\hat{\Gamma}, \hat{x} : \hat{b} \text{ array} \vdash \hat{d} : \hat{t}$ , weakening, and the C Blk typing rule to obtain  $\llbracket \hat{\Gamma} \rrbracket, b x \square \vdash \llbracket \hat{t} \rrbracket x \square = \{\overline{\hat{c}_2}^{\text{times}}\}, l'; s'$ .
7. **Case**  $\hat{\Gamma} \vdash \text{let } x : \hat{b} \text{ array} = \text{Array.make\_matrix } \hat{c}_1 \hat{c}_2 \hat{c}_3 \text{ in } \hat{d} : \hat{t}$ . Similar to previous case.
8. **Case**  $\hat{\Gamma} \vdash \hat{x}.(\hat{e}_1) \leftarrow \hat{e}_2 : \text{unit}$ . It is given that  $\{\hat{x}.(\hat{e}_1) \leftarrow \hat{e}_2\}_{\perp} = (l, s)$ . By inversion we know  $\hat{\Gamma}(x) = \hat{b} \text{ array}$ ,  $\hat{\Gamma} \vdash \hat{e}_1 : \text{int}$  and  $\hat{\Gamma} \vdash \hat{e}_2 : \hat{b}$ . Let  $\{\hat{x}.(\hat{e}_1) \leftarrow \hat{e}_2\}_{\perp} = (\cdot, x[\llbracket \hat{e}_1 \rrbracket] = \llbracket \hat{e}_2 \rrbracket)$ . We apply the definition of  $\{\hat{\Gamma}\}$  to  $\hat{\Gamma} \vdash \hat{e}_1 : \text{int}$  and Lemma 4.1.1 to  $\hat{\Gamma} \vdash \hat{e}_1 : \text{int}$  and  $\hat{\Gamma} \vdash \hat{e}_2 : \hat{b}$  to obtain  $\llbracket \hat{\Gamma} \rrbracket(x) = b$ ,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_1 \rrbracket : \text{int}$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_2 \rrbracket : b$  respectively. By the C rule for array assignment `SetArr1`, we now have:  $\llbracket \hat{\Gamma} \rrbracket \vdash x[\llbracket \hat{e}_1 \rrbracket] =$

- $\llbracket (\hat{e}_2) \rrbracket : \perp$ .
9. **Case**  $\hat{\Gamma} \vdash \hat{x}.(\hat{e}_1).(\hat{e}_2) \leftarrow \hat{e}_3 : \text{unit}$ . Similar to previous case.
  10. **Case**  $\hat{\Gamma} \vdash \text{if } \hat{e}_1 \text{ then } \hat{d}_1 \text{ else } \hat{d}_2 : \hat{t}$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{e} : \text{bool}$ ,  $\hat{\Gamma} \vdash \hat{d}_1 : \hat{t}$  and  $\hat{\Gamma} \vdash \hat{d}_2 : \hat{t}$ . By translation,  $\{\text{if } \hat{e}_1 \text{ then } \hat{d}_1 \text{ else } \hat{d}_2\}_\perp = (\cdot, \text{if } (\llbracket \hat{e} \rrbracket)\{l_1; s_1\} \text{ else } \{l_2; s_2\})$  where  $\{\hat{d}_1\}_\perp = (l_1; s_1)$  and  $\{\hat{d}_2\}_\perp = (l_2; s_2)$  From Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \text{int}$ . By induction,  $\llbracket \hat{\Gamma} \rrbracket \vdash (l_1, s_1) : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash (l_2, s_2) : \perp$ . Then by the C Ifs rule,  $\llbracket \hat{\Gamma} \rrbracket \vdash (\cdot, \text{if } (\llbracket \hat{e} \rrbracket)\{l_1; s_1\} \text{ else } \{l_2; s_2\}) : \perp$ .
  11. **Case**  $\hat{\Gamma} \vdash \text{while } \hat{e} \text{ do } \hat{d} \text{ done} : \text{unit}$ . By inversion we know that  $\hat{\Gamma} \vdash \hat{e} : \text{bool}$  and  $\hat{\Gamma} \vdash \hat{d} : \hat{t}$ . By translation,  $\{\text{while } \hat{e} \text{ do } \hat{d} \text{ done}\}_\perp = (\cdot, \text{while } (\llbracket \hat{e} \rrbracket)\{l'; s'\})$  where  $\{\hat{d}\}_\perp = (l'; s')$ . From Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \text{int}$ . By induction,  $\llbracket \hat{\Gamma} \rrbracket \vdash (l'; s') : \perp$  Then by the C While rule,  $\llbracket \hat{\Gamma} \rrbracket \vdash (\cdot, \text{while } (\llbracket \hat{e} \rrbracket)\{l'; s'\}) : \perp$ .
  12. **Case**  $\hat{\Gamma} \vdash \text{for } \hat{x} = \hat{e}_1 \{ \text{to, downto} \} \hat{e}_2 \text{ do } \hat{d} \text{ done} : \text{unit}$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{e}_1 : \text{int}$ ,  $\hat{\Gamma} \vdash \hat{e}_2 : \text{int}$  and  $\hat{\Gamma}, \hat{x} : \text{int} \vdash \hat{d} : \hat{t}$ . By translation,  $\{\text{for } \hat{x} = \hat{e}_1 \text{ to } \hat{e}_2 \text{ do } \hat{d} \text{ done}\}_\perp = (\text{int } x, \text{for } (x = \llbracket \hat{e}_1 \rrbracket; x <= \llbracket \hat{e}_2 \rrbracket; x++)\{l'; s'\})$  where  $\{\hat{d}\}_\perp = (l'; s')$ . From Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_1 \rrbracket : \text{int}$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e}_2 \rrbracket : \text{int}$ . Also, by definition of  $\llbracket \hat{\Gamma} \rrbracket$ , we have  $\llbracket \hat{\Gamma} \rrbracket(x) = \text{int}$ . By induction,  $\llbracket \hat{\Gamma} \rrbracket \vdash (l, s) : \perp$ . Then by the C For rule,  $\llbracket \hat{\Gamma} \rrbracket \vdash (\text{int } x, \text{for } (x = \llbracket \hat{e}_1 \rrbracket; x <= \llbracket \hat{e}_2 \rrbracket; x++)\{l'; s'\}) : \perp$ .
  13. **Case**  $\text{match } \hat{e} \text{ with } (\hat{c}_i \rightarrow \hat{d}_i)^{i \in \{ \dots n \}} \mid \_ \leftarrow \hat{d} : \text{unit}$ . By inversion, we know that  $\hat{\Gamma} \vdash \hat{e} : \hat{b}$  where  $\hat{b}$  is not a float. Also,  $\hat{\Gamma} \vdash \overline{\hat{c}_n : \hat{b}}$  and  $\hat{\Gamma} \vdash \overline{\hat{d}_n : \hat{t}}$  and  $\hat{\Gamma} \vdash \hat{d} : \text{unit}$ . By translation,  $\{\text{match } \hat{e} \text{ with } (\hat{c}_i \rightarrow \hat{d}_i)^{i \in \{ \dots n \}} \mid \_ \leftarrow \hat{d}\}_\perp = \text{switch } (\llbracket \hat{e} \rrbracket)\{\overline{\text{case } c_n : \{l'_n; s'_n; \text{break}\}}; \text{default} : \{l'; s'\}\}$  where  $\{\hat{d}_n\}_\perp = (\overline{l'_n; s'_n})$  and  $\{\hat{d}\}_\perp = (l', s')$ . From Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \hat{e} : \llbracket \hat{b} \rrbracket$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \overline{c_n : \text{int}}$ . By induction,  $\llbracket \hat{\Gamma} \rrbracket \vdash \overline{(l'_n, s'_n)} : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash (l', s') : \perp$ . Then by the C Switch rule  $\llbracket \hat{\Gamma} \rrbracket \vdash \text{switch } (\llbracket \hat{e} \rrbracket)\{\overline{\text{case } c_n : \{l'_n; s'_n; \text{break}\}}; \text{default} : \{l'; s'\}\} : \perp$ .

■

**Proof** [Lemma 4.1.3] Proof is by induction on the height of the typing derivation of statements. The proof is similar to the one for Lemma 4.1.2. Cases where  $\{\dot{\cdot}\}$  is undefined follow trivially. We concentrate on the remaining cases.

1. **Case**  $\hat{\Gamma} \vdash \hat{e} : \hat{t}$ . It is given that  $\{\{\hat{e}\}\}_\top = (l, s)$ . Consider the case when by translation  $\{\{\hat{e}\}\}_\top = (\cdot, \mathbf{return} \llbracket \hat{e} \rrbracket)$ . We know  $l = \cdot$  and  $s = \mathbf{return} \llbracket \hat{e} \rrbracket$ . By Lemma 4.1.1,  $\llbracket \hat{\Gamma} \rrbracket \vdash \llbracket \hat{e} \rrbracket : \llbracket \hat{t} \rrbracket$ , thus by the C Ret rule  $\llbracket \hat{\Gamma} \rrbracket \vdash (\cdot, \mathbf{return} \llbracket \hat{e} \rrbracket) : \llbracket \hat{t} \rrbracket$ .
2. **Case**  $\hat{\Gamma} \vdash \hat{d}_1; \hat{d}_2 : \hat{t}$ . It is given that  $\{\{\hat{d}_1; \hat{d}_2\}\}_\top = (l, s)$ . Having  $\hat{\Gamma} \vdash \hat{d}_1; \hat{d}_2 : \hat{t}$ , by inversion we know that  $\hat{\Gamma} \vdash \hat{d}_1 : \mathbf{unit}$  and  $\hat{\Gamma} \vdash \hat{d}_2 : \hat{t}$ . Let  $\{\{\hat{d}_1\}\}_\perp = (l_1, s_1)$  and  $\{\{\hat{d}_2\}\}_\top = (l_2, s_2)$ . By translation,  $\{\{\hat{d}_1; \hat{d}_2\}\}_\top = (l_1; l_2, s_1; s_2)$ . We know  $l = l_1; l_2$  and  $s = s_1; s_2$ . We are trying to show  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1; l_2, s_1; s_2\} : \llbracket \hat{t} \rrbracket$ . We apply Lemma 4.1.2 to  $\hat{\Gamma} \vdash \hat{d}_1 : \mathbf{unit}$  and the induction hypothesis to  $\hat{\Gamma} \vdash \hat{d}_2 : \hat{t}$  to obtain  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1, s_1\} : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_2, s_2\} : \llbracket \hat{t} \rrbracket$ . By inversion of the C Blk rule for  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1, s_1\} : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_2, s_2\} : \llbracket \hat{t} \rrbracket$ , we have  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \vdash s_1 : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \cup |l_2| \vdash s_2 : \llbracket \hat{t} \rrbracket$ . By Lemma 3.1.2 we know  $\mathbf{dom} l_1 \subseteq BV(d_1)$  and  $\mathbf{dom} l_2 \subseteq BV(d_2)$ . Now by Assumption 1,  $\mathbf{dom} l_1 \cap \mathbf{dom} l_2 = \emptyset$ . We can conclude, by weakening that  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \cup |l_2| \vdash s_1 : \perp$  and  $\llbracket \hat{\Gamma} \rrbracket \cup |l_1| \cup |l_2| \vdash s_2 : \llbracket \hat{t} \rrbracket$ . The final result,  $\llbracket \hat{\Gamma} \rrbracket \vdash \{l_1; l_2, s_1; s_2\} : \llbracket \hat{t} \rrbracket$ , follows by the C rule Blk.
3. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} = \hat{e} \mathbf{in} \hat{d} : \hat{t}$ . It is given that  $\{\{\mathbf{let} x = \hat{e} \mathbf{in} \hat{d}\}\}_\top = (l, s)$ . By inversion of OCaml typing, we know that  $\hat{\Gamma} \vdash \hat{e} : \hat{b}$  and  $\hat{\Gamma}, \hat{x} : \hat{b} \vdash \hat{d} : \hat{t}$ . Let  $\{\{\hat{d}\}\}_\top = (l', s')$ . Then by translation we know  $\{\{\mathbf{let} x : \hat{b} = \hat{e} \mathbf{in} \hat{d}\}\}_\top = ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{e} \rrbracket; s'))$ . By Lemma 4.1.1, we know that  $\llbracket \hat{\Gamma} \rrbracket \vdash e : \llbracket \hat{b} \rrbracket$ . By the C Assign rule, we know  $\llbracket \hat{\Gamma} \rrbracket \vdash x = e : \perp$ . We must show that  $\llbracket \hat{\Gamma} \rrbracket \vdash ((\llbracket \hat{b} \rrbracket x; l'), (x = \llbracket \hat{e} \rrbracket; s')) : \llbracket \hat{t} \rrbracket$ . By the induction hypothesis,  $\llbracket \hat{\Gamma}, \hat{x} : \hat{b} \rrbracket \vdash (l', s') : \llbracket \hat{t} \rrbracket$ . The final result follows by the C Blk rule.
4. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \mathbf{ref} = \mathbf{ref} \hat{e} \mathbf{in} \hat{d} : \hat{t}$ . Similar to previous case.
5. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \mathbf{array} = \mathbf{Array.make} \hat{c}_1 \hat{c}_2 \mathbf{in} \hat{d} : \hat{t}$ . Similar to previous case.
6. **Case**  $\hat{\Gamma} \vdash \mathbf{let} x : \hat{b} \mathbf{array array} = \mathbf{Array.make\_matrix} \hat{c}_1 \hat{c}_2 \hat{c}_3 \mathbf{in} \hat{d} : \hat{t}$ . Similar to previous case.

■