

Modularly Programmable Syntax

Cyrus Omar

TODO: get TR number

December 24, 2015

School of Computer Science
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee:

Jonathan Aldrich, Chair
Robert Harper
Karl Crary
Eric Van Wyk, University of Minnesota

*Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy.*

Copyright © 2015 Cyrus Omar. TODO: CC0 license.

TODO: Support

DRAFT (December 24, 2015)

Keywords: TODO: keywords

TODO: dedication

Abstract

Full-scale functional programming languages often make *ad hoc* choices in the design of their concrete syntax. For example, nearly all major functional languages build in derived forms for lists, but introducing derived forms for other library constructs, e.g. for HTML elements or regular expressions, requires forming new syntactic dialects of these languages. Unfortunately, programmers cannot modularly combine syntactic dialects in general, limiting the choices ultimately available to them. In this work, we introduce and formally specify language primitives that mitigate the need for *ad hoc* derived forms and syntactic dialects by giving library providers the ability to programmatically control syntactic expansion while maintaining a type discipline, a hygienic binding discipline and modular reasoning principles.

Acknowledgments

TODO: Acknowledgments

Contents

1	Introduction	1
1.1	Motivation	1
1.1.1	Dialects Considered Harmful	2
1.1.2	Large Languages Considered Harmful	2
1.1.3	Toward More General Primitives	3
1.2	Overview of Contributions	3
1.3	Disclaimers	4
2	Background	7
2.1	Preliminaries	7
2.2	Motivating Examples	7
2.2.1	Regular Expressions	8
2.2.2	Lists, Sets, Maps, Vectors and Other Containers	10
2.2.3	HTML and Other Web Languages	10
2.2.4	Dates, URLs and Other Standardized Formats	10
2.2.5	Query Languages	10
2.2.6	Monadic Commands	10
2.2.7	Quasiquotation and Object Language Syntax	11
2.2.8	Grammars	11
2.2.9	Mathematical and Scientific Notations	11
2.2.10	Others	11
2.3	Existing Approaches	11
2.3.1	Dynamic String Parsing	11
2.3.2	Direct Syntax Extension	14
2.3.3	Term Rewriting	16
2.3.4	Active Libraries	17
3	Unparameterized Expression TSMs	19
3.1	Expression TSMs By Example	19
3.1.1	Usage	19
3.1.2	Definition	20
3.1.3	Splicing	22
3.1.4	Typing	22
3.1.5	Hygiene	23

3.1.6	Final Expansion	24
3.1.7	Scoping	24
3.1.8	Comparison to ML+Rx	25
3.2	miniVerse _{UE}	25
3.2.1	Syntax of the Inner Core	25
3.2.2	Statics of the Inner Core	25
3.2.3	Structural Dynamics	29
3.2.4	Syntax of the Outer Surface	30
3.2.5	Typed Expansion	32
3.2.6	ueTSM Definitions	36
3.2.7	ueTSM Application	38
3.2.8	Syntax of Candidate Expansions	39
3.2.9	Candidate Expansion Validation	41
3.2.10	Metatheory	46
4	Unparameterized Pattern TSMs	53
4.1	Pattern TSMs By Example	54
4.1.1	Usage	54
4.1.2	Definition	55
4.1.3	Splicing	56
4.1.4	Typing	56
4.1.5	Hygiene	57
4.1.6	Final Expansion	57
4.2	miniVerse _U	57
4.2.1	Syntax of the Inner Core	57
4.2.2	Statics of the Inner Core	59
4.2.3	Structural Dynamics	63
4.2.4	Syntax of the Outer Surface	64
4.2.5	Typed Expansion	65
4.2.6	upTSM Definition	69
4.2.7	upTSM Application	70
4.2.8	Syntax of Candidate Expansions	71
4.2.9	Candidate Expansion Validation	73
4.2.10	Metatheory	75
5	Parameterized TSMs	77
5.1	Parameterized TSMs By Example	77
5.1.1	Type Parameters By Example	77
5.1.2	Module Parameters By Example	77
5.2	miniVerse _∇	77
5.2.1	Signatures, Types and Expanded Expressions	77
5.2.2	Parameter Application and Deferred Substitution	77
5.2.3	Macro Expansion and Validation	77
5.2.4	Metatheory	77

6	Type-Specific Languages (TSLs)	79
6.1	TSLs By Example	79
6.2	Parameterized Modules	80
6.3	miniVerse _{TSL}	81
7	Discussion & Future Directions	83
7.1	Interesting Applications	83
7.1.1	TSMs For Defining TSMs	83
7.1.2	Monadic Commands	84
7.2	Summary	84
7.3	Future Directions	84
7.3.1	Static Language	84
7.3.2	TSM Packaging	84
7.3.3	TSMs and TSLs In Candidate Expansions	86
7.3.4	Pattern Matching Over Values of Abstract Type	86
7.3.5	Integration Into Other Languages	86
7.3.6	Mechanically Verifying TSM Definitions	86
7.3.7	Improved Error Reporting	87
7.3.8	Controlled Binding	87
7.3.9	Type-Aware Splicing	87
7.3.10	Integration With Code Editors	87
7.3.11	Resugaring	87
7.3.12	Non-Textual Display Forms	87
	LaTeX Source Code and Updates	88
	Bibliography	89

List of Figures

2.1	Definition of the recursive sum type Rx	8
2.2	Spliced subexpressions in $ML+Rx$	9
2.3	Derived pattern syntax in $ML+Rx$	9
2.4	Definition of the RX signature	10
3.1	Available Generalized Literal Forms	20
3.2	Definitions of $IndexRange$ and $ParseResult$ in $VerseML$	21
3.3	Abbreviated definitions of $CETyp$ and $CEExp$ in $VerseML$	21
3.4	Syntax of types and expanded expressions in $miniVerse_{UE}$	26
3.5	Syntax of unexpanded types and expressions in $miniVerse_{UE}$	30
3.6	Syntax of candidate expansion types and expressions in $miniVerse_{UE}$	40
4.1	Abbreviated definition of $CEPat$ in $VerseML$	56
4.2	Syntax of types and expanded expressions, rules and patterns in $miniVerse_U$	58
4.3	Syntax of unexpanded expressions, rules and patterns in $miniVerse_U$	64
4.4	Syntax of candidate expansion types and candidate expansion terms in $miniVerse_U$	72

Chapter 1

Introduction

The recent development of programming languages suggests that the simultaneous achievement of simplicity and generality in language design is a serious unsolved problem.

— John Reynolds (1970) [34]

1.1 Motivation

Programming languages come in many sizes. Small languages – i.e. “formal calculi” – allow language designers to study the mathematical properties of language primitives of interest in isolation. These studies then inform the design of “full-scale” languages, which combine several such primitives, or generalizations thereof.

Because small-scale languages are of interest mainly as objects of mathematical study, their designers often choose to specify only the abstract syntax of their primitives (or, when typesetting documents, stylized representations thereof). Full-scale languages, on the other hand, are both interesting objects of mathematical study and, ideally, useful for write large programs, so they typically also specify a more “programmer-friendly” textual concrete syntax that features various *derived syntactic forms*, i.e. forms defined by a context-independent “desugaring” to the set of base forms, that decrease the syntactic cost of certain common idioms. For example, Standard ML (SML) [17, 27], OCaml [25] and Haskell [23] build in derived forms that decrease the syntactic cost of working with lists. In these languages, the form `[1, 2, 3, 4, 5]` desugars to:

```
Cons(1, Cons(2, Cons(3, Cons(4, Cons(5, Nil)))))
```

The hope amongst many language designers is that a limited number of derived forms like these will suffice to produce a “general-purpose” programming language, i.e. one that satisfies programmers working in a wide variety of application domains. Unfortunately, a stable language design that fully achieves this ideal has yet to emerge, as evidenced by the diverse array of *syntactic dialects* – dialects that introduce only new derived forms – that continue to proliferate around all major contemporary languages. For example, Ur/Web is a syntactic dialect of Ur (an ML-like full-scale language [8]) that

builds in derived forms for SQL queries, HTML elements and other datatypes used in the domain of web programming [9]. We will consider a large number of other examples of syntactic dialects in Sec. 2.2. Tools like Camlp4 [25], Sugar* [11, 12] and Racket’s preprocessor [13], which we will discuss in Sec. 2.3, have decreased the engineering costs of constructing syntactic dialects, further contributing to their proliferation.

1.1.1 Dialects Considered Harmful

Some view this proliferation of dialects as harmless or even as desirable, arguing that programmers can simply choose the right dialect for the job at hand [41]. However, this “dialect-oriented” approach is, in an important sense, anti-modular: programmers cannot always “combine” different dialects when they want to use the primitives that they feature together within a single program. For example, a programmer might have access to a dialect featuring HTML syntax and to a dialect featuring regular expression syntax, but it is not always straightforward to, from these, construct a dialect featuring both. Both HTML and regular expression syntax might be useful when constructing, for example, a web-based bioinformatics tool.

In some cases, constructing the desired “combined dialect” is difficult simply because the constituent dialects are specified using different formalisms. In other cases, the constituent dialects may be specified using a formalism that does not operationalize the notion of dialect combination (e.g. Racket’s preprocessor [13]). But even if we restrict our interest to dialects specified using a formalism that does operationalize some notion of dialect combination (or, equivalently, one that allows programmers to combine “dialect fragments”), there may still be a problem: the formalism may not guarantee that the combined dialect will conserve important properties that can be established about the dialects in isolation. For example, consider two syntactic dialects specified using Camlp4, one specifying derived syntax for finite mappings, the other specifying overlapping syntax for *ordered* finite mappings. Though each dialect has a deterministic grammar, when these grammars are naively combined, syntactic ambiguities will arise. We are aware of only one formalism that guarantees that determinism is conserved when syntactic dialects are combined [35], but it has limited expressive power, as we will discuss in Sec. 2.3.2.

1.1.2 Large Languages Considered Harmful

Dialects do sometimes have a less direct influence on large-scale software development: they can help convince the designers in control of comparatively popular languages, like OCaml and Scala, to include some variant of the primitives that they feature into backwards-compatible language revisions. This *ad hoc* approach is unsustainable, for three main reasons. First, as we will demonstrate in Sec. 2.2, there are simply too many potentially useful such primitives, and many of these capture idioms common only in relatively narrow application domains. It is unreasonable to expect language designers to be able to evaluate all of these use cases in a timely and informed manner. Second,

primitives introduced earlier in a language’s lifespan can end up monopolizing finite “syntactic resources”, forcing subsequent primitives to use ever more esoteric forms. And third, primitives that prove after some time to be flawed in some way cannot be removed or modified without breaking backwards compatibility. For these reasons, language designers are justifiably reticent to add new primitives to major languages.

1.1.3 Toward More General Primitives

This leaves two possible paths forward. One is to simply eschew “niche” primitives and settle on the existing designs, which might be considered to sit at a “sweet spot” in the overall language design space (accepting that in some circumstances, this leads to high syntactic cost). The other path forward is to search for a small number of highly general primitives that allow us degrade many of the constructs that are built primitively into languages and their dialects today instead to modular library constructs. Encouragingly, primitives of this sort do occasionally arise. For example, a recent revision of OCaml added support for generalized algebraic data types (GADTs), based on research on guarded recursive datatype constructors [42]. Using GADTs, OCaml was able to move some of the *ad hoc* machinery for typechecking operations that use format strings, like `sprintf`, out of the language and into a library. Syntactic machinery related to `sprintf`, however, remains built in.

1.2 Overview of Contributions

Our aim in this work is to introduce primitive language constructs that reduce the need for syntactic dialects and *ad hoc* derived syntactic forms. In particular, we introduce the following primitives:

1. **Typed syntax macros, or TSMs.** TSMs are applied like functions to *generalized literal forms* to programmatically control their parsing and expansion. This occurs statically (i.e. simultaneously with typing). We introduce TSMs first for a simple language of expressions and types in Chapter 3, then add support for pattern matching in Chapter 4 and type and module parameters in Chapter 5.
2. **Type-specific languages, or TSLs.** TSLs, described in Chapter 6, further reduce syntactic cost by allowing library providers to designate a privileged TSM for each type that they introduce. Library clients can then rely on local type inference to invoke that TSM and apply its parameters implicitly. TSLs can reduce the syntactic cost of an idiom to very nearly the same extent that a special-purpose dialect can, while avoiding the problems described above.

As vehicles for this work, we will specify a small-scale typed lambda calculus in each of the chapters just mentioned, each building upon the previous one. For the sake of examples, we will also describe (but not formally specify) a full-scale functional lan-

guage called VerseML.¹ VerseML is, as its name suggests, a dialect of ML. It diverges from other dialects of ML that have a similar underlying type structure, like Standard ML and OCaml, in that it uses a local type inference scheme [33] (like, for example, Scala [28]) for reasons that have to do with the mechanisms described in Chapter 6. The reason we will not follow Standard ML [27] in giving a complete formal specification of VerseML in this work is both to emphasize that the primitives we introduce are fairly insensitive to the details of the underlying type structure of the language (so TSMs can be considered for inclusion in a variety of languages, not only dialects of ML), and to avoid distracting the reader (and the author) with specifications of primitives that are already well-understood in the literature and that are orthogonal to those that are the focus of this work.

The main challenge will come in maintaining the following:

- a *type discipline*, meaning that the language must be type safe, and that programmers examining a well-typed expression must be able to determine its type without examining its expansion;
- a *hygienic binding discipline*, meaning that the expansion logic must not be permitted to make “hidden assumptions” about the names of variables at macro application sites, nor introduce “hidden bindings” into other terms; and
- *modular reasoning principles*, meaning that library providers must have the ability to reason about the syntax that they have defined in isolation, and clients must be able to use macros safely in any combination, without the possibility of conflict.²

We will, of course, make these notions more technically precise as we continue.

Thesis Statement

In summary, this work defends the following statement:

A functional programming language can give library providers the ability to express new syntactic expansions while maintaining a type discipline, a hygienic binding discipline and modular reasoning principles.

1.3 Disclaimers

Before we continue, it may be prudent to explicitly acknowledge that completely eliminating the need for dialects would indeed be asking for too much: certain language design decisions are fundamentally incompatible with others or require coordination across a language design. We aim only to decrease the need for syntactic dialects in this work. We will not consider situations that require modifications to the underlying type structure of a language (though this is a rich avenue for future work).

¹We distinguish VerseML from Wyvern, which is the language described in our prior publications about some of the work that we will describe, because Wyvern is a group effort evolving independently.

²This is not quite true – name clashes of the usual sort can arise. We will tacitly assume that in practice, they can be avoided extrinsically, e.g. by using a URI-based naming scheme as in the Java ecosystem.

It may also be useful to explicitly acknowledge that library providers could leverage the primitives we introduce to define constructs that are in “poor taste”. We expect that in practice, VerseML will come with a standard library defining an expertly curated collection of standard constructs, as well as guidelines for advanced users regarding when it would be sensible to use the mechanisms we introduce (following the example of languages that support operator overloading or type classes [16], which also have some potential for “abuse” or “overuse”).

Chapter 2

Background

2.1 Preliminaries

This work is rooted in the tradition of full-scale functional languages with non-trivial type structure like ML and Haskell (as might have been obvious from the exposition in Chapter 1). Familiarity with basic concepts in these languages, e.g. variables, types, functions, tuples, records, recursive datatypes and nested pattern matching, is assumed throughout this work. Readers who are not familiar with these concepts are encouraged to consult the early chapters of an introductory text like Harper’s *Programming in Standard ML* [17] (a working draft can be found online). We briefly discuss integration of TSMs and TSLs into languages from other language design traditions in Sec. 7.3.5.

Chapter 5 and Chapter 6, and some of the motivating examples given below, consider questions of integration with an ML-style module system, so readers with experience in a language without such a module system (e.g. Haskell) are also advised to review the relevant chapters in *Programming in Standard ML* [17] before delving into these portions of these chapters.

The formal systems that we will construct in later chapters are specified within the metatheoretic framework of type theory. More specifically, we assume familiarity with fundamental background concepts (e.g. abstract binding trees, substitution, implicit identification of terms up to α -equivalence, structural induction and rule induction) covered in detail in Harper’s *Practical Foundations for Programming Languages, Second Edition (PFPL)* [19] (a working draft can be found online). Familiarity with other formal accounts of type systems, e.g. Pierce’s *Types and Programming Languages (TAPL)* [32], should also suffice. This document is organized so as to be readable even if the sections describing formal systems are skipped (although some precision will, of course, be lost).

2.2 Motivating Examples

In Chapter 1, we gave the example of derived list syntax in languages like SML, OCaml and Haskell. To further motivate our contributions, we now provide more examples where defining new derived syntactic forms could decrease the syntactic cost of work-

ing with certain data structures. We cover the first example – regular expressions, expressed both using recursive sum types and abstract types – in substantial detail. We will refer back to this example in subsequent chapters. We then more concisely survey a number of other examples, grouped into categories, to establish the broad applicability of our contributions.

2.2.1 Regular Expressions

Regular expressions, or *regexes*, specify string patterns (of a certain class) [39]. They are particularly common in domains like natural language processing and bioinformatics. The abstract syntax of regexes, r , over strings, s , is specified below:

$$r ::= \text{empty} \mid \text{str}(s) \mid \text{seq}(r;r) \mid \text{or}(r;r) \mid \text{star}(r)$$

Recursive Sums One way to express this abstract syntax is by defining a recursive sum type [19]. In VerseML, a recursive labeled sum type can be defined like this:

```
type Rx = Empty | Str of string | Seq of Rx * Rx |
      Or of Rx * Rx | Star of Rx
```

Figure 2.1: Definition of the recursive sum type Rx

Values of type Rx are constructed by applying a label to a value of the type specified in the corresponding clause above (or simply using the label by itself if no corresponding type is specified). For example, we can define a regular expression that matches only the strings "A", "T", "G" and "C" as follows:

```
Or(Str "A", Or(Str "T", Or(Str "G", Str "C")))
```

This is too verbose to be practical in all but the simplest examples, so the POSIX standard specifies a more concise concrete syntax for regexes [3]. Several programming languages support derived syntax for regexes based on this standard, e.g. Perl [10]. Let us consider a hypothetical dialect of ML called ML+Rx (perhaps constructed using a tool like Camlp4, discussed in Sec. 2.3.2) that similarly builds in derived forms for regexes. We will compare VerseML to ML+Rx in later chapters. ML+Rx extends the concrete syntax of ML with support for *regex expression literals* delimited by forward slashes. For example, the following regex literal desugars to the expression above:

```
/A|T|G|C/
```

ML+Rx also supports *spliced subexpressions* in regex literals, so that regexes can be constructed from other values. For example, the function `example_rx` shown in Figure 2.2 constructs a regex by splicing in a string, `name`, and another regex, `ssn`. The prefix `@` followed by the variable name indicates that the expression `name` should be spliced in as a string, and the prefix `%` followed by the variable `ssn` indicates that `ssn` should be spliced in as a regex. The body of `example_rx` desugars to the following:

```
Seq(Str(name), Seq(Str ":", ssn))
```

```
let ssn = /\d\d\d-\d\d-\d\d\d\d/
fun example_rx(name : string) => /@name: %ssn/
```

Figure 2.2: Spliced subexpressions in ML+Rx

Notice that `name` appears wrapped in the constructor `Str` because it was prefixed by `@`, whereas `ssn` appears unadorned because it was prefixed by `%`.

To splice in an expression that does not take the form of a variable, e.g. a function call, we can delimit it with parentheses:

```
/@(capitalize name): %ssn/
```

Finally, ML+Rx allows us to pattern match over a value of type `Rx` using analogous derived pattern syntax. For example, the body of the following function reads the name and social security number back out of a regex generated by the function `example_rx`:

```
fun read_example_rx(r : Rx) : (string * Rx) option =>
  match r with
  | /@name: %ssn/ => Some (name, ssn)
  | _ => None
```

Figure 2.3: Derived pattern syntax in ML+Rx

This expression desugars to:

```
fun read_example_rx(r : Rx) : (string * Rx) option =>
  match r with
  | Seq(Str(name), Seq(Str ":", ssn)) => Some (name, ssn)
  | _ => None
```

Abstract Types Encoding regexes as values of type `Rx` is straightforward, but there are reasons why one might not wish to expose this encoding to clients directly. First, regexes are usually identified up to their reduction to a normal form. For example, `seq(empty, r)` has normal form `r`. It can be useful for regexes with the same normal form to be indistinguishable from the perspective of client code. Second, it can be useful for performance reasons to maintain additional data alongside regexes (e.g. a corresponding finite automaton), but one would not want to expose this “implementation detail” to clients. In fact, there may be many ways to represent regular expression patterns, each with different performance trade-offs, so we would like to provide clients with a choice of implementations. For these reasons, another approach in VerseML, as in ML, is to abstract over the choice of representation using the module system’s support for abstract types. In particular, we can define the *module signature* `RX`, shown in Figure 2.4, where the type of patterns, `t`, is held abstract.

Clients of any module `R` that has been sealed against `RX`, written `R :> RX`, manipulate patterns as values of the type `R.t` using the interface described by this signature. The identity of the type `R.t` is held abstract outside the module during typechecking (i.e.

```

signature RX = sig {
  type t
  val Empty : t
  val Str : string -> t
  val Seq : t * t -> t
  val Or : t * t -> t
  val Star : t -> t
  val Group : t -> t
  val case : (
    t -> {
      Empty : 'a,
      Str : string -> 'a,
      Seq : t * t -> 'a,
      Or : t * t -> 'a,
      Star : t -> 'a,
      Group : t -> 'a
    } -> 'a
  )
}

```

Figure 2.4: Definition of the RX signature

it acts as a newly generated type). As a result, the burden of proving that there is no way to use the case analysis function to distinguish patterns with the same normal form is local to the module, and implementation details do not escape (and can thus evolve freely).

TODO: talk about module-parameterized derived syntactic forms for this

TODO: talk about pattern matching over values of abstract type

2.2.2 Lists, Sets, Maps, Vectors and Other Containers

TODO: write this (Spring 2016)

2.2.3 HTML and Other Web Languages

2.2.4 Dates, URLs and Other Standardized Formats

2.2.5 Query Languages

The language of regular expressions can be considered a query language over strings. There are many other query languages that focus on different types of data, e.g. XQuery for XML trees, or that are associated with various database technologies, e.g. SQL for relational databases. TODO: finish this (Spring 2016)

2.2.6 Monadic Commands

TODO: write this; cite Bob's blog (Spring 2016)

TODO: <http://www.cs.umd.edu/~mwh/papers/monadic.pdf>

2.2.7 Quasiquote and Object Language Syntax

TODO: write this (Spring 2016)

2.2.8 Grammars

TODO: write this (Spring 2016)

2.2.9 Mathematical and Scientific Notations

SMILES: Chemical Notation

TODO: write this; cite SMILES https://en.wikipedia.org/wiki/Simplified_molecular-input_line-entry_system (Spring 2016)

T_EX Mathematical Formula Notation

TODO: write this (Spring 2016)

2.2.10 Others

Get examples from: <http://voelter.de/data/pub/mbeddr-cs-oopsla2015-preprint.pdf>

2.3 Existing Approaches

TODO: revise, reformat and extend (Spring 2016 / as needed)

2.3.1 Dynamic String Parsing

To expose this more concise concrete syntax for regular expression patterns to clients, the most common approach is to provide a function that parses strings to produce patterns. Because, as just mentioned, there may be many implementations of the RX signature, the usual approach is to define a parameterized module (a.k.a. a *functor* in SML) defining utility functions like this abstractly:

```
module RXUtil(R : RX) => mod {  
  fun parse(s : string) : R.t => (* ... regex parser here ... *)  
}
```

This allows a client of any module $R : RX$ to use the following definitions:


```
let module RUtil = RXUtil(R)
let val rxparse = RUtil.parse
```

to construct patterns like this:

```
rxparse "A|T|G|C"
```

Unfortunately, this approach is imperfect for several reasons:

1. First, there are syntactic conflicts between string escape sequences and pattern escape sequences. For example, the following is not a well-formed term:

```
let val ssn = rxparse "\d\d\d-\d\d-\d\d\d\d"
```

When compiling an expression like this, the client would see an error message like `error: illegal escape character1`, because `\d` is not a valid string escape sequence. In a small lab study, we observed that this class of error often confused even experienced programmers if they had not used regular expressions recently [29]. One workaround has higher syntactic cost – we must double all backslashes:

```
let val ssn = rxparse "\\d\\d\\d-\\d\\d-\\d\\d\\d\\d"
```

Some languages, anticipating such modes of use, build in alternative string forms that leave escape sequences uninterpreted. For example, OCaml supports the following, which has only a constant syntactic cost:

```
let val ssn = rxparse {rx|\d\d\d-\d\d-\d\d\d\d|rx}
```

2. The next problem is that dynamic string parsing mainly decreases the syntactic cost of complete patterns. Patterns constructed compositionally cannot easily benefit from this technique. For example, consider the following function from strings to patterns:

```
fun example(name : string) =>
  R.Seq(R.Str(name), R.Seq(rxparse ":", ssn)) (* ssn as above *)
```

Had we built derived syntax for regular expression patterns into the language primitively (following Unix conventions of using forward slashes as delimiters), we could have used *splicing syntax*:

```
fun example_shorter(name : string) => /@name: %ssn/
```

An identifier (or parenthesized expression, not shown) prefixed with an `@` is a spliced string, and one prefixed with a `%` is a spliced pattern.

It is difficult to capture idioms like this using dynamic string parsing, because strings cannot contain sub-expressions directly.

3. For functions like `example` where we are constructing patterns on the basis of data of type `string`, using strings coincidentally to introduce patterns tempts programmers to use string concatenation in subtly incorrect ways. For example, consider the following seemingly more readable definition of `example`:

¹This is the error message that `javac` produces. When compiling an analogous expression using SML of New Jersey (SML/NJ), we encounter a more confusing error message: `Error: unclosed string`.

```
fun example_bad(name : string) =>
  rxparse (name ^ {rx|: \d\d\d-\d\d-\d\d\d\d|rx})
```

Both `example` and `example_bad` have the same type and behave identically at many inputs, particularly “typical” inputs (i.e. alphabetic names). It is only when the input name contains special characters that have meaning in the concrete syntax of patterns that a problem arises.

In applications that query sensitive data, mistakes like this lead to *injection attacks*, which are among the most common and catastrophic security threats on the web today [4]. These are, of course, a consequence of the programmer making a mistake in an effort to decrease syntactic cost, but proving that mistakes like this have not been made involves reasoning about complex run-time data flows, so it is once again notoriously difficult to automate. If our language supported derived syntax for patterns, this kind of mistake would be substantially less common (because `example_shorter` has lower syntactic cost than `example_bad`).

4. The next problem is that pattern parsing does not occur until the pattern is evaluated. For example, the following malformed pattern will only trigger an exception when this expression is evaluated during the full moon:

```
case (moon_phase) {
  Full => rxparse "(GC" (* malformedness not statically detected *)
  | _ => (* ... *)
}
```

Though malformed patterns can sometimes be discovered dynamically via testing, empirical data gathered from large open source projects suggests that there remain many malformed regular expression patterns that are not detected by a project’s test suite “in the wild” [37].

Statically verifying that pattern formation errors will not dynamically arise requires reasoning about arbitrary dynamic behavior. This is an undecidable verification problem in general and can be difficult to even partially automate. In this example, the verification procedure would first need to be able to establish that the variable `rxparse` is equal to the parse function `RUtil.parse`. If the string argument had not been written literally but rather computed, e.g. as `"(G" ^ "C"` where `^` is the string concatenation function applied in infix style, it would also need to be able to establish that this expression is equivalent to the string `"(GC"`. For patterns that are dynamically constructed based on input to a function, evaluating the expression statically (or, more generally, in some earlier “stage” of evaluation [22]) also does not suffice.

Of course, asking the client to provide a proof of well-formedness would defeat the purpose of lowering syntactic cost.

In contrast, were our language to primitively support derived pattern syntax, pattern parsing would occur at compile-time and so malformed patterns would produce a compile-time error.

5. Dynamic string parsing also necessarily incurs dynamic cost. Regular expression

patterns are common when processing large datasets, so it is easy to inadvertently incur this cost repeatedly. For example, consider mapping over a list of strings:

```
map exmpl_list (fn s => rxmatch (rxparse "A|T|G|C") s)
```

To avoid incurring the parsing cost for each element of `exmpl_list`, the programmer or compiler must move the parsing step out of the closure (for example, by eta-reduction in this simple example).² If the programmer must do this, it can (in more complex examples) increase syntactic cost and cognitive cost by moving the pattern itself far away from its use site. Alternatively, an appropriately tuned memoization (i.e. caching) strategy could be used to amortize some of this cost, but it is difficult to reason compositionally about performance using such a strategy.

In contrast, were our language to primitively support derived pattern syntax, the expansion would be computed at compile-time and incur no dynamic cost.

The problems above are not unique to regular expression patterns. Whenever a library encourages the use of dynamic string parsing to address the issue of syntactic cost (which is, fundamentally, not a dynamic issue), these problems arise. This fact has motivated much research on reducing the need for dynamic string parsing [6]. Existing alternatives can be broadly classified as being based on either *direct syntax extension* or *static term rewriting*. We describe these next, in Secs. 2.3.2 and 2.3.3 respectively.

2.3.2 Direct Syntax Extension

One tempting alternative to dynamic string parsing is to use a system that gives the users of a language the power to directly extend its concrete syntax with new derived forms.

The simplest such systems are those where the elaboration of each new syntactic form is defined by a single rewrite rule. For example, Gallina, the “external language” of the Coq proof assistant, supports such extensions [26]. A formal account of such a system has been developed by Griffin [15]. Unfortunately, a single equation is not enough to allow us to express pattern syntax following the usual conventions. For example, a system like Coq’s cannot handle escape characters, because there is no way to programmatically examine a form when generating its expansion.

Other syntax extension systems are more flexible. For example, many are based on context-free grammars, e.g. Sugar* [11] and Camlp4 [25] (amongst many others). Other systems give library providers direct programmatic access to the parse stream, like Common Lisp’s *reader macros* [38] (which are distinct from its term-rewriting macros, described in Sec. 2.3.3 below) and Racket’s preprocessor [13]. All of these would allow us to add pattern syntax into our language’s grammar, perhaps following Unix conventions and supporting splicing syntax as described above:

```
let val ssr = /\d\d\d-\d\d-\d\d\d\d/
fun example_shorter(name : string) => /@name: %ssr/
```

²Anecdotally, in major contemporary compilers, this optimization is not automatic.

We sidestep the problems of dynamic string parsing described above when we directly extend the syntax of our language using any of these systems. Unfortunately, direct syntax extension introduces serious new problems. First, the systems mentioned thus far cannot guarantee that syntactic conflicts between such extensions will not arise. As stated directly in the Coq manual: “mixing different symbolic notations in [the] same text may cause serious parsing ambiguity”. If another library provider used similar syntax for a different implementation or variant of regular expressions, or for some other unrelated construct, then a client could not simultaneously use both libraries at the same time. So properly considered, every combination of extensions introduced using these mechanisms creates a *de facto* syntactic dialect of our language. The benefit of these systems is only that they lower the implementation cost of constructing syntactic dialects.

In response to this problem, Schwerdfeger and Van Wyk developed a modular analysis that accepts only context-free grammar extensions that begin with an identifying starting token and obey certain constraints on the follow sets of base language’s non-terminals [35]. Extensions that specify distinct starting tokens and that satisfy these constraints can be used together in any combination without the possibility of syntactic conflict. However, the most natural starting tokens like `rx` cannot be guaranteed to be unique. To address this problem, programmers must agree on a convention for defining “globally unique identifiers”, e.g. the common URI convention used on the web and by the Java packaging system. However, this forces us to use a more verbose token like `edu_cmu_VerseML_rx`. There is no simple way for clients of our extension to define scoped abbreviations for starting tokens because this mechanism operates purely at the level of the context-free grammar.

Putting this aside, we must also consider another modularity-related question: which particular module should the expansion use? Clearly, simply assuming that some module identified as `R` matching `RX` is in scope is a brittle solution. In fact, we should expect that the system actively prevents such capture of specific variable names to ensure that variables (here, module variables) can be freely renamed. Such a *hygiene discipline* is well-understood only when performing term-to-term rewriting (discussed below) or in simple language-integrated rewrite systems like those found in Coq. For mechanisms that operate strictly at the level of context-free grammars or the parse stream, it is not clear how one could address this issue. The onus is then on the library provider to make no assumptions about variable names and instead require that the client explicitly identify the module they intend to use as an “argument” within the newly introduced form:

```
let val ssn = edu_cmu_VerseML_rx R /\d\d\d-\d\d-\d\d\d\d/
```

Another problem with the approach of direct syntax extension is that, given an unfamiliar piece of syntax, there is no straightforward method for determining what type it will have, causing difficulties for both humans (related to code comprehension) and tools.

TODO: Related work I haven’t mentioned yet:

- Fan: <http://zhanghongbo.me/fan/start.html>
- Well-Typed Islands Parse Faster:
<http://www.ccs.neu.edu/home/ejs/papers/TFP12-island.pdf>

- User-defined infix operators
- SML quote/unquote
- That Modularity paper
- Template Haskell and similar

2.3.3 Term Rewriting

An alternative approach is to leave the concrete syntax of the language fixed, but repurpose it for novel ends using a *local term-rewriting system*. The LISP macro system [20] is perhaps the most prominent example of such a system. Early variants of this system suffered from the problem of unhygienic variable capture just described, but later variants, notably in the Scheme dialect of LISP, brought support for enforcing hygiene [24]. In languages with a richer static type discipline, variants of macros that restrict rewriting to a particular type and perform the rewriting statically have also been studied [14, 21] and integrated into languages, e.g. MacroML [14] and Scala [7].

The most immediate problem with using these for our example is that we are not aware of any such statically-typed macro system that integrates cleanly with an ML-style module system. In other words, macros cannot be parameterized by modules. However, let us imagine such a macro system. We could use it to repurpose string syntax as follows:

```
let val ssn = rx R {rx|\d\d\d-\d\d-\d\d\d\d|rx}
```

The definition of the macro `rx` might look like this:

```
1 macro rx[Q : RX](e) at Q.t {
2   static fun f(e : Exp) : Exp => case(e) {
3     StrLit(s) => (* regex parser here *)
4     | BinOp(Caret, e1, e2) => 'Q.Seq(Q.Str(%e1), %(f e2))'
5     | BinOp(Plus, e1, e2) => 'Q.Seq(%(f e1), %(f e2))'
6     | _ => raise Error
7   }
8 }
```

Here, `rx` is a macro parameterized by a module matching `rx` (we identify it as `Q` to emphasize that there is nothing special about the identifier `R`) and taking a single argument, identified as `e`. The macro specifies a type annotation, `at Q.t`, which imposes the constraint that the expansion the macro statically generates must be of type `Q.t` for the provided parameter `Q`. This expansion is generated by a *static function* that examines the syntax tree of the provided argument (syntax trees are of a type `Exp` defined in the standard library; cf. SML/NJ's visible compiler [2]). If it is a string literal, as in the example above, it statically parses the literal body to generate an expansion (the details of the parser, elided on line 3, would be entirely standard). By parsing the string statically, we avoid the problems of dynamic string parsing for statically-known patterns.

For patterns that are constructed compositionally, we need to get more creative. For example, we might repurpose the infix operators that are normally used for other purposes to support string and pattern splicing, e.g. as follows:

```
fun example_using_macro(name : string) =>
  rx R (name ^ ":" + ssn)
```

The binary operator `^` is repurposed to indicate a spliced string and `+` is repurposed to indicate a spliced pattern. The logic for handling these forms can be seen above on lines 4 and 5, respectively. We assume that there is derived syntax available at the type `Exp`, i.e. *quasiquote* syntax as in Lisp [5] and Scala [36], here delimited by backticks and using the prefix `%` to indicate a spliced value (i.e. `unquote`).

Having to creatively repurpose existing forms in this way limits the effect a library provider can have on syntactic cost (particularly when it would be desirable to express conventions that are quite different from the conventions adopted by the language). It also can create confusion for readers expecting parenthesized expressions to behave in a consistent manner. However, this approach is preferable to direct syntax extension because it avoids many of the problems discussed above: there cannot be syntactic conflicts (because the syntax is not extended at all), we can define macro abbreviations because macros are integrated into the language, there is a hygiene discipline that guarantees that the expansion will not capture variables inadvertently, and by using a typed macro system, programmers need not examine the expansion to know what type the expansion produced by a macro must have.

2.3.4 Active Libraries

The design we are proposing also has conceptual roots in earlier work on *active libraries*, which similarly envisioned using compile-time computation to give library providers more control over various aspects of a programming system, including its concrete (but did not take an approach rooted in the study of type systems) [40]. **TODO: flesh this out and connect it to previous stuff**

Chapter 3

Unparameterized Expression TSMs

We now introduce a new primitive – the **typed syntax macro** (TSM). TSMs, like term-rewriting macros (Sec. 2.3.3), generate expansions. Unlike term-rewriting macros, TSMs are applied to unparsed *generalized literal forms*, which gives them substantially more syntactic flexibility. This chapter considers perhaps the simplest manifestation of TSMs: **unparameterized expression TSMs** (ueTSMs), which generate expressions of a single specified type. We will consider unparameterized pattern TSMs (upTSMs) in Chapter 4 and parameterized TSMs (pTSMs) in Chapter 5.

3.1 Expression TSMs By Example

We begin in this section with a “tutorial-style” introduction to ueTSMs in VerseML. In particular, we discuss a ueTSM for constructing values of the recursive labeled sum type Rx that was defined in Figure 2.1. We then formally specify ueTSMs with a reduced calculus, $miniVerse_{UE}$, in Sec. 3.2.

3.1.1 Usage

In the following concrete VerseML expression, we apply a TSM named $\$rx$ to the *generalized literal form* $/A|T|G|C/$:

```
 $\$rx$   $/A|T|G|C/$ 
```

Generalized literal forms are left unparsed when concrete expressions are first parsed. It is only during the subsequent *typed expansion* process that the TSM parses the *body* of the provided literal form, i.e. the characters between forward slashes in blue here, to generate a *candidate expansion*. The language then *validates* the candidate expansion according to criteria that we will establish in Sec. 3.1.4. If candidate expansion validation succeeds, the language generates the *final expansion* (or more concisely, simply the *expansion*) of the expression. The program will behave as if the expression above has been replaced by its expansion. The expansion of the expression above, written concretely, is:

```
Or(Str "A", Or(Str "T", Or(Str "G", Str "C")))
```



```

1 'body cannot contain an apostrophe'
2 'body cannot contain a backtick'
3 [body cannot contain unmatched square brackets]
4 {body cannot contain an unmatched curly brace}
5 /body cannot contain a forward slash/
6 \body cannot contain a backslash\

```

Figure 3.1: Generalized literal forms available for use in VerseML’s concrete syntax. The characters in blue indicate where the literal bodies are located within each form. In this figure, each line describes how the literal body is constrained by the form shown on that line. The Wyvern language specifies additional forms, including whitespace-delimited forms [30] and multipart forms [31], but for simplicity we leave these out of VerseML.

A number of literal forms, shown in Figure 3.1, are available in VerseML’s concrete syntax. Any literal form can be used with any TSM, e.g. we could have equivalently written the example above as `$rx 'A|T|G|C'` (in fact, this would be convenient if we had wanted to express a regex containing forward slashes but not backticks). TSMs have access only to the literal bodies. Because TSMs do not extend the concrete syntax of the language directly, there cannot be syntactic conflicts between TSMs.

3.1.2 Definition

Let us now take the perspective of the library provider. The definition of the TSM `$rx` shown being applied above has the following form:

```

syntax $rx at Rx {
  static fn(body : Body) : CEEp ParseResult =>
    (* regex literal parser here *)
}

```

This TSM definition first names the TSM. TSM names must begin with the dollar symbol (\$) to clearly distinguish them from variables (and thereby clearly distinguish TSM application from function application). This is inspired by a similar convention enforced by the Rust macro system [1].

The TSM definition then specifies a *type annotation*, `at Rx`, and a *parse function* within curly braces. The parse function is a *static function* responsible for parsing the literal body when the TSM is applied to generate an encoding of the candidate expansion, or an indication of an error if one cannot be generated (e.g. when the body is ill-formed according to the syntactic specification that the TSM implements). Static functions are functions that are applied during the typed expansion process. For this reason, they do not have access to surrounding variable bindings (because those variables stand in for dynamic values). For now, let us simply assume that static functions are closed (we discuss introducing a distinct class of static bindings so that static values can be shared between TSM definitions in Sec. 7.3.1).

The parse function must have type `Body -> CEEp ParseResult`. These types are defined in the VerseML *prelude*, which is a collection of definitions available ambiently.

```

type IndexRange = {startIndex : nat, endIndex : nat}

type 'a ParseResult = Success of 'a
                    | ParseError of {
                        msg : string, loc : IndexRange
                    }

```

Figure 3.2: Definitions of IndexRange and ParseResult in the VerseML prelude.

```

type CETyp = TyVar of var_t
            | Arrow of CETyp * CETyp
            | (* ... *)
            | Spliced of IndexRange

type CEEExp = Var of var_t
            | Fn of var_t * CETyp * CEEExp
            | App of CEEExp * CEEExp
            | (* ... *)
            | Spliced of IndexRange

```

Figure 3.3: Abbreviated definitions CETyp and CEEExp in the VerseML prelude. We assume some suitable type var_t exists, not shown.

The input type, *Body*, gives the parse function access to the body of the provided literal form. For our purposes, it suffices to define *Body* as an abbreviation for the string type:

```

type Body = string

```

The output type, *CEExp ParseResult*, is a labeled sum type that distinguishes between successful parses and parse errors. The parameterized type 'a ParseResult is defined in Figure 3.2.

If parsing succeeds, the parse function returns a value of the form $\text{Success}(e_{\text{cand}})$, where e_{cand} is the *encoding of the candidate expansion*. Encodings of candidate expansions are, for expression TSMs, values of the type CEEExp defined in Figure 3.3 (in Chapter 4, we will introduce pattern TSMs, which generate patterns rather than expressions; this is why ParseResult is defined as a parameterized type). Expressions can mention types, so we also need to define a type CETyp in Figure 3.3. We discuss the constructors labeled Spliced in Sec. 3.1.3; the remaining constructors (some of which are elided for concision) encode the abstract syntax of VerseML expressions and types. To decrease the syntactic cost of working with the types defined in Figure 3.3, the prelude provides *quasiquotation syntax* at these types, which is itself implemented using TSMs. We will discuss these TSMs in more detail in Sec. 7.1.1. The definitions in Figure 3.3 are recursive labeled sum types to simplify our exposition, but we could have chosen alternative encodings of terms, e.g. based on abstract binding trees [19], with only minor modification to the semantics.

If the parse function determines that a candidate expansion cannot be generated, i.e. there is a parse error in the literal body, it returns a value labeled by ParseError. It must

provide an error message and indicate the location of the error within the body of the literal form as a value of type `IndexRange`, also defined in Figure 3.2. This information can be used by VerseML compilers when reporting errors to the programmer.

3.1.3 Splicing

To support splicing syntax, like that described in Sec. 2.2.1, the parse function must be able to parse subexpressions out of the supplied literal body. For example, consider the code snippet in Figure 2.2, expressed instead using the `$rx` TSM:

```
val ssn = $rx /\d\d\d-\d\d-\d\d\d\d/
fun example_rx_tsm(name: string) => $rx /@name: %ssn/
```

The subexpressions `name` and `ssn` on the second line appear directly in the body of the literal form, so we call them *spliced subexpressions* (and color them black when typesetting them in this document). When the parse function determines that a subsequence of the literal body should be treated as a spliced subexpression (here, by recognizing the characters `@` or `%` followed by a variable or parenthesized expression), it can refer to it within the candidate expansion it generates using the `Spliced` constructor of the `CEExp` type shown in Figure 3.3. The `Spliced` constructor requires a value of type `IndexRange` because spliced subexpressions are referred to indirectly by their position within the literal body. This prevents TSMs from “forging” a spliced subexpression (i.e. claiming that an expression is a spliced subexpression, even though it does not appear in the body of the literal form). Expressions can also contain types, so one can also mark spliced types in an analogous manner using the `Spliced` constructor of the `CETyp` type.

The candidate expansion generated by `$rx` for the body of `example_rx_tsm`, if written in a hypothetical concrete syntax for candidate expansions where references to spliced subexpressions are written `spliced<startIdx, endIndex>`, is:

```
Seq(Str(spliced<1, 4>), Seq(Str ":", spliced<8, 10>))
```

Here, `spliced<1, 4>` refers to the subexpression `name` by position and `spliced<8, 10>` refers to the subexpression `ssn` by position.

3.1.4 Typing

The language *validates* candidate expansions before a final expansion is generated. One aspect of candidate expansion validation is checking the candidate expansion against the type annotation specified by the TSM, e.g. the type `Rx` in the example above. This maintains a *type discipline*: if a programmer sees a TSM being applied when examining a well-typed program, they need only look up the TSM’s type annotation to determine the type of the generated expansion. Determining the type does not require examine the expansion directly.

3.1.5 Hygiene

The spliced subexpressions that the candidate expansion refers to (by their position within the literal body, cf. above) must be parsed, typed and expanded during the candidate expansion validation process (otherwise, the language would not be able to check the type of the candidate expansion). To maintain a useful *binding discipline*, i.e. to allow programmers to reason also about variable binding without examining expansions directly, the validation process maintains two additional properties related to spliced subexpressions: **context independent expansion** and **expansion independent splicing**. These are collectively referred to as the *hygiene properties* (because they are conceptually related to the concept of hygiene in term rewriting macro systems, cf. Sec. 2.3.3.)

Context Independent Expansion Programmers expect to be able to choose variable and symbol names freely, i.e. without needing to satisfy “hidden assumptions” made by the TSMs that are applied in scope of a binding. For this reason, context-dependent candidate expansions, i.e. those with free variables or symbols, are deemed invalid (even at application sites where those variables happen to be bound). An example of a TSM that generates context-dependent candidate expansions is shown below:

```
syntax $bad1 at Rx {  
  static fn(body : Body) : ParseResultExp => Success (Var 'x')  
}
```

The candidate expansion this TSM generates would be well-typed only when there is an assumption $x : Rx$ in the application site typing context. This “hidden assumption” makes reasoning about binding and renaming especially difficult, so this candidate expansion is deemed invalid (even when \$bad1 is applied in a context where x happens to be bound).

Of course, this prohibition does not extend into the spliced subexpressions referred to in a candidate expansion because spliced subexpressions are authored by the TSM client and appear at the application site, and so can justifiably refer to application site bindings. We saw examples of spliced subexpressions that referred to variables bound at the application site in Sec. 3.1.3. Because candidate expansions refer to spliced subexpressions indirectly, checking this property is straightforward – we only allow access to the application site typing context when typing spliced subexpressions. In the next section, we will formalize this intuition.

In the examples in Sec. 3.1.1 and Sec. 3.1.3, the expansion used constructors associated with the Rx type, e.g. Seq and Str. This might appear to violate our prohibition on context-dependent expansions. This is not the case only because in VerseML, constructor labels are not variables or scoped symbols. Syntactically, they must begin with a capital letter (like Haskell’s datatype constructors). Different labeled sum types can use common constructor labels without conflict because the type the term is being checked against – e.g. Rx , due to the type ascription on $\$rx$ – determines which type of value will be constructed. For dialects of ML where datatype definitions do introduce new

variables or scoped symbols, we need parameterized TSMs. We will return to this topic in Chapter 5.

Expansion Independent Splicing Spliced subexpressions, as just described, must be given access to application site bindings. The *expansion independent splicing* property ensures that spliced subexpressions have access to *only* those bindings, i.e. a TSM cannot introduce new bindings into spliced subexpressions. For example, consider the following hypothetical candidate expansion (written concretely as above):

```
fn(x : Rx) => spliced<0, 4>
```

The variable `x` is not available when typing the indicated spliced subexpression, nor can it shadow any bindings of `x` that might appear at the application site.

For TSM providers, the benefit of this property is that they can choose the names of variables used internally within expansions freely, without worrying about whether they might shadow those that a client might have defined at the application site.

TSM clients can, in turn, determine exactly which bindings are available in a spliced subexpression without examining the expansion it appears within. In other words, there can be no “hidden variables”.

The trade-off is that this prevents library providers from defining alternative binding forms. For example, Haskell’s derived form for monadic commands (i.e. **do**-notation) supports binding the result of executing a command to a variable that is then available in the subsequent commands in a command sequence. In VerseML, this cannot be expressed in the same way. We will show an alternative formulation of Haskell’s syntax for monadic commands that uses VerseML’s anonymous function syntax to bind variables in Sec. 7.1.2. We will discuss mechanisms that would allow us to relax this restriction while retaining client control over variable names as future work in Sec. 7.3.8.

3.1.6 Final Expansion

If validation succeeds, the language generates the *final expansion* from the candidate expansion by replacing references to spliced subexpressions with their final expansions. The final expansion of the body of `example_rx_tsm` is:

```
Seq(Str(name), Seq(Str ":", ssn))
```

3.1.7 Scoping

A benefit of specifying TSMs as a language primitive, rather than relying on extralinguistic mechanisms to manipulate the concrete syntax of our language directly, is that TSMs follow standard scoping rules.

For example, we can define a TSM that is visible only to a single expression like this:

```
let x = let
  syntax $rx at Rx { (* ... *) }
  in (* $rx is in scope here *) end
in (* $rx is no longer in scope *) end
```

We will consider the question of how TSM definitions can be exported from compilation units in Sec. 7.3.2.

3.1.8 Comparison to ML+Rx

Let us compare the VerseML TSM $\$rx$ to ML+Rx, the hypothetical syntactic dialect of ML with support for derived forms for regular expressions described in Sec. 2.2.1.

Both ML+Rx and $\$rx$ give programmers the ability to use the same standard syntax for constructing regexes, including syntax for splicing in other strings and regexes. In VerseML, however, we incur the additional syntactic cost of explicitly applying the $\$rx$ TSM each time we wish to use regex syntax. This cost does not grow with the size of the regex, so it would only be significant in programs that involve a large number of small regexes (which do, of course, exist). In Chapter 6 we will consider a design where even this syntactic cost can be eliminated in certain situations.

The benefit of this approach is that we can easily define other TSMs to use alongside the $\$rx$ TSM without needing to consider the possibility of syntactic conflict. Furthermore, programmers can rely on the typing discipline and the hygienic binding discipline described above to reason about programs, including those that contain unfamiliar forms. Put pithily, VerseML helps programmers avoid “conflict and confusion”.

3.2 miniVerse_{UE}

To make the intuitions developed in the previous section mathematically precise, we will now introduce a reduced formal system called miniVerse_{UE} with support for ueTSMs. miniVerse_{UE} consists of an *inner core* and an *outer surface*.

3.2.1 Syntax of the Inner Core

The *inner core* of miniVerse_{UE} consists of *types*, τ , and *expanded expressions*, e . The syntax of the inner core is specified by the syntax chart in Figure 3.4. The inner core forms a pure language with support for partial functions, quantification over types, recursive types, labeled product types and labeled sum types. The reader is directed to *PFPL* [19] (or another text on type systems, e.g. *TAPL* [32]) for a detailed introductory account of these (or very similar) constructs. We will tersely define the statics of the inner core, and outline the structural dynamics, in the next two subsections, respectively.

3.2.2 Statics of the Inner Core

The *statics of the inner core* is defined by hypothetical judgements of the following form:

Judgement Form	Description
$\Delta \vdash \tau \text{ type}$	τ is a well-formed type assuming Δ
$\Delta \Gamma \vdash e : \tau$	e is assigned type τ assuming Δ and Γ

Sort	Operational Form	Stylized Form	Description
Typ $\tau ::=$	t	t	variable
	$\text{parr}(\tau; \tau)$	$\tau \multimap \tau$	partial function
	$\text{all}(t.\tau)$	$\forall t.\tau$	polymorphic
	$\text{rec}(t.\tau)$	$\mu t.\tau$	recursive
	$\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tau_i\}_{i \in L} \rangle$	labeled product
	$\text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$	$[\{i \hookrightarrow \tau_i\}_{i \in L}]$	labeled sum
Exp $e ::=$	x	x	variable
	$\text{lam}\{\tau\}(x.e)$	$\lambda x:\tau.e$	abstraction
	$\text{ap}(e; e)$	$e(e)$	application
	$\text{tlam}(t.e)$	$\Lambda t.e$	type abstraction
	$\text{tap}\{\tau\}(e)$	$e[\tau]$	type application
	$\text{fold}\{t.\tau\}(e)$	$\text{fold}(e)$	fold
	$\text{unfold}(e)$	$\text{unfold}(e)$	unfold
	$\text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})$	$\langle \{i \hookrightarrow e_i\}_{i \in L} \rangle$	labeled tuple
	$\text{pr}[\ell](e)$	$e \cdot \ell$	projection
	$\text{in}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(e)$	$\ell \cdot e$	injection
	$\text{case}[L]\{\tau\}(e; \{i \hookrightarrow x_i.e_i\}_{i \in L})$	$\text{case } e \{i \hookrightarrow x_i.e_i\}_{i \in L}$	case analysis

Figure 3.4: Abstract syntax of types and expanded expressions, which form the *inner core* of $\text{miniVerse}_{\text{UE}}$. Metavariables x range over variables, t over type variables, ℓ over labels and L over finite sets of labels. We adopt *PFPL*’s conventions for operational forms, i.e. the names of operators and indexed families of operators are written in *typewriter* font, indexed families of operators specify non-symbolic indices within [mathematical braces] and symbolic indices within [textual braces], and term arguments are grouped arbitrarily (roughly, by “phase”) using {textual curly braces} and (textual rounded braces) [19]. We write $\{i \hookrightarrow \tau_i\}_{i \in L}$ for a sequence of arguments τ_i , one for each $i \in L$, and similarly for arguments of other valences. Operations parameterized by label sets, e.g. $\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$, are identified up to mutual reordering of the label set and the corresponding argument sequence. When we use the stylized forms, we assume that the reader can infer suppressed indices and arguments from the surrounding context. Types and expanded expressions are identified up to α -equivalence.

Type formation contexts, Δ , are finite sets of hypotheses of the form $t \text{ type}$. Empty finite sets are written \emptyset , or omitted entirely within judgements, and non-empty finite sets are written as comma-separated finite sequences identified up to exchange and contraction. We write $\Delta, t \text{ type}$, when $t \text{ type} \notin \Delta$, for Δ extended with the hypothesis $t \text{ type}$.

The type formation judgement, $\Delta \vdash \tau \text{ type}$, is inductively defined by the following rules:

$$\frac{}{\Delta, t \text{ type} \vdash t \text{ type}} \quad (3.1a)$$

$$\frac{\Delta \vdash \tau_1 \text{ type} \quad \Delta \vdash \tau_2 \text{ type}}{\Delta \vdash \text{parr}(\tau_1; \tau_2) \text{ type}} \quad (3.1b)$$

$$\frac{\Delta, t \text{ type} \vdash \tau \text{ type}}{\Delta \vdash \text{all}(t.\tau) \text{ type}} \quad (3.1c)$$

$$\frac{\Delta, t \text{ type} \vdash \tau \text{ type}}{\Delta \vdash \text{rec}(t.\tau) \text{ type}} \quad (3.1d)$$

$$\frac{\{\Delta \vdash \tau_i \text{ type}\}_{i \in L}}{\Delta \vdash \text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L}) \text{ type}} \quad (3.1e)$$

$$\frac{\{\Delta \vdash \tau_i \text{ type}\}_{i \in L}}{\Delta \vdash \text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L}) \text{ type}} \quad (3.1f)$$

Premises of the form $\{J_i\}_{i \in L}$ mean that for each $i \in L$, the judgement J_i must hold.

Typing contexts, Γ , are finite functions that map each variable $x \in \text{dom}(\Gamma)$, to the hypothesis $x : \tau$, for some τ . Empty typing contexts are written \emptyset , or omitted entirely within judgements, and non-empty typing contexts are written as finite sequences of hypotheses identified up to exchange (we do not separately write down the finite set $\text{dom}(\Gamma)$ because it can be determined from the listed hypotheses). We write $\Gamma, x : \tau$, when $x \notin \text{dom}(\Gamma)$, for the extension of Γ with a mapping from x to $x : \tau$, and $\Gamma \cup \Gamma'$ when $\text{dom}(\Gamma) \cap \text{dom}(\Gamma') = \emptyset$ for the typing context mapping each $x \in \text{dom}(\Gamma) \cup \text{dom}(\Gamma')$ to $x : \tau$ if $x : \tau \in \Gamma$ or $x : \tau \in \Gamma'$. We write $\Delta \vdash \Gamma \text{ ctx}$ if every type in Γ is well-formed relative to Δ .

Definition 3.1 (Typing Context Formation). $\Delta \vdash \Gamma \text{ ctx}$ iff for each hypothesis $x : \tau \in \Gamma$, we have $\Delta \vdash \tau \text{ type}$.

The typing judgement, $\Delta \Gamma \vdash e : \tau$, assigns types to expressions. It is inductively defined by the following rules:

$$\frac{}{\Delta \Gamma, x : \tau \vdash x : \tau} \quad (3.2a)$$

$$\frac{\Delta \vdash \tau \text{ type} \quad \Delta \Gamma, x : \tau \vdash e : \tau'}{\Delta \Gamma \vdash \text{lam}\{\tau\}(x.e) : \text{parr}(\tau; \tau')} \quad (3.2b)$$

$$\frac{\Delta \Gamma \vdash e_1 : \text{parr}(\tau; \tau') \quad \Delta \Gamma \vdash e_2 : \tau}{\Delta \Gamma \vdash \text{ap}(e_1; e_2) : \tau'} \quad (3.2c)$$

$$\frac{\Delta, t \text{ type } \Gamma \vdash e : \tau}{\Delta \Gamma \vdash \mathbf{tlam}(t.e) : \mathbf{all}(t.\tau)} \quad (3.2d)$$

$$\frac{\Delta \Gamma \vdash e : \mathbf{all}(t.\tau) \quad \Delta \vdash \tau' \text{ type}}{\Delta \Gamma \vdash \mathbf{tap}\{\tau'\}(e) : [\tau'/t]\tau} \quad (3.2e)$$

$$\frac{\Delta, t \text{ type } \vdash \tau \text{ type} \quad \Delta \Gamma \vdash e : [\mathbf{rec}(t.\tau)/t]\tau}{\Delta \Gamma \vdash \mathbf{fold}\{t.\tau\}(e) : \mathbf{rec}(t.\tau)} \quad (3.2f)$$

$$\frac{\Delta \Gamma \vdash e : \mathbf{rec}(t.\tau)}{\Delta \Gamma \vdash \mathbf{unfold}(e) : [\mathbf{rec}(t.\tau)/t]\tau} \quad (3.2g)$$

$$\frac{\{\Delta \Gamma \vdash e_i : \tau_i\}_{i \in L}}{\Delta \Gamma \vdash \mathbf{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L}) : \mathbf{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})} \quad (3.2h)$$

$$\frac{\Delta \Gamma \vdash e : \mathbf{prod}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)}{\Delta \Gamma \vdash \mathbf{pr}[\ell](e) : \tau} \quad (3.2i)$$

$$\frac{\{\Delta \vdash \tau_i \text{ type}\}_{i \in L} \quad \Delta \vdash \tau \text{ type} \quad \Delta \Gamma \vdash e : \tau}{\Delta \Gamma \vdash \mathbf{in}[L, \ell][\ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)(e) : \mathbf{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)} \quad (3.2j)$$

$$\frac{\Delta \Gamma \vdash e : \mathbf{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L}) \quad \Delta \vdash \tau \text{ type} \quad \{\Delta \Gamma, x_i : \tau_i \vdash e_i : \tau\}_{i \in L}}{\Delta \Gamma \vdash \mathbf{case}[L]\{\tau\}(e; \{i \hookrightarrow x_i.e_i\}_{i \in L}) : \tau} \quad (3.2k)$$

Rules (3.1) and (3.2) are syntax-directed, so we assume an inversion lemma for each rule as needed without stating it separately. The following standard lemmas also hold.

The Weakening Lemma establishes that extending a context with unnecessary hypotheses preserves well-formedness and typing.

Lemma 3.2 (Weakening). *All of the following hold:*

1. If $\Delta \vdash \tau \text{ type}$ then $\Delta, t \text{ type } \vdash \tau \text{ type}$.
2. If $\Delta \Gamma \vdash e : \tau$ then $\Delta, t \text{ type } \Gamma \vdash e : \tau$.
3. If $\Delta \Gamma \vdash e : \tau$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta \Gamma, x : \tau' \vdash e : \tau$.

Proof Sketch. For each part, by rule induction on the assumption. \square

We assume that renaming of bound variables, α -equivalence and substitution are defined as in PFPL [19]. The Substitution Lemma establishes that substitution of a well-formed type for a type variable, or an expanded expression of the appropriate type for an expanded expression variable, preserves well-formedness and typing.

Lemma 3.3 (Substitution). *All of the following hold:*

1. If $\Delta, t \text{ type } \vdash \tau \text{ type}$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta \vdash [\tau'/t]\tau \text{ type}$.
2. If $\Delta, t \text{ type } \Gamma \vdash e : \tau$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$.
3. If $\Delta \Gamma, x : \tau' \vdash e : \tau$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma \vdash [e'/x]e : \tau$.

Proof Sketch. For each part, by rule induction on the first assumption. \square

The Decomposition Lemma is the converse of the Substitution Lemma.

Lemma 3.4 (Decomposition). *All of the following hold:*

1. If $\Delta \vdash [\tau'/t]\tau \text{ type}$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta, t \text{ type } \vdash \tau \text{ type}$.

2. If $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$ and $\Delta \vdash \tau'$ type then $\Delta, t \text{ type } \Gamma \vdash e : \tau$.
3. If $\Delta \Gamma \vdash [e'/x]e : \tau$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma, x : \tau' \vdash e : \tau$.

Proof Sketch.

1. By rule induction over Rules (3.1) and case analysis on the definition of substitution. In all cases, the derivation of $\Delta \vdash [\tau'/t]\tau$ type does not depend on the form of τ' .
2. By rule induction over Rules (3.2) and case analysis on the definition of substitution. In all cases, the derivation of $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$ does not depend on the form of τ' .
3. By rule induction over Rules (3.2) and case analysis on the definition of substitution. In all cases, the derivation of $\Delta \Gamma \vdash [e'/x]e : \tau$ does not depend on the form of e' .

□

The Regularity Lemma establishes that the type assigned to an expanded expression under a well-formed typing context is always well-formed.

Lemma 3.5 (Regularity). *If $\Delta \Gamma \vdash e : \tau$ and $\Delta \vdash \Gamma$ ctx then $\Delta \vdash \tau$ type.*

Proof Sketch. By rule induction over Rules (3.2) and application of Definition 3.1 and Lemma 3.3. □

3.2.3 Structural Dynamics

The *structural dynamics* of $\text{miniVerse}_{\text{UE}}$ is specified as a transition system by judgements of the following form:

Judgement Form	Description
$e \mapsto e'$	e transitions to e'
$e \text{ val}$	e is a value

We also define auxiliary judgements for *iterated transition*, $e \mapsto^* e'$, and *evaluation*, $e \Downarrow e'$.

Definition 3.6 (Iterated Transition). $e \mapsto^* e'$ is the reflexive, transitive closure of $e \mapsto e'$.

Definition 3.7 (Evaluation). $e \Downarrow e'$ iff $e \mapsto^* e'$ and $e' \text{ val}$.

Our subsequent developments do not require making reference to particular rules in the structural dynamics (because TSMs operate statically), so we do not reproduce the rules here. Instead, it suffices to state the following conditions.

The Canonical Forms condition characterizes well-typed values. Satisfying this condition requires an *eager* (i.e. *by-value*) formulation of the dynamics.

Condition 3.8 (Canonical Forms). *If $\vdash e : \tau$ and $e \text{ val}$ then:*

1. If $\tau = \text{parr}(\tau_1; \tau_2)$ then $e = \text{lam}\{\tau_1\}(x.e')$ and $x : \tau_1 \vdash e' : \tau_2$.
2. If $\tau = \text{all}(t.\tau')$ then $e = \text{tlam}(t.e')$ and $t \text{ type } \vdash e' : \tau'$.
3. If $\tau = \text{rec}(t.\tau')$ then $e = \text{fold}\{t.\tau'\}(e')$ and $\vdash e' : [\text{rec}(t.\tau')/t]\tau'$ and $e' \text{ val}$.
4. If $\tau = \text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ then $e = \text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})$ and $\vdash e_i : \tau_i$ and $e_i \text{ val}$ for each $i \in L$.

Sort	Operational Form	Stylized Form	Description
UTyp $\hat{\tau} ::=$	\hat{t}	\hat{t}	sigil
	$\text{uparr}(\hat{\tau}; \hat{\tau})$	$\hat{\tau} \rightarrow \hat{\tau}$	partial function
	$\text{uall}(\hat{t}. \hat{\tau})$	$\forall \hat{t}. \hat{\tau}$	polymorphic
	$\text{urec}(\hat{t}. \hat{\tau})$	$\mu \hat{t}. \hat{\tau}$	recursive
	$\text{uprod}[L](\{i \hookrightarrow \hat{\tau}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \hat{\tau}_i\}_{i \in L} \rangle$	labeled product
	$\text{usum}[L](\{i \hookrightarrow \hat{\tau}_i\}_{i \in L})$	$[\{i \hookrightarrow \hat{\tau}_i\}_{i \in L}]$	labeled sum
UExp $\hat{e} ::=$	\hat{x}	\hat{x}	sigil
	$\text{ulam}\{\hat{\tau}\}(\hat{x}. \hat{e})$	$\lambda \hat{x} : \hat{\tau}. \hat{e}$	abstraction
	$\text{uap}(\hat{e}; \hat{e})$	$\hat{e}(\hat{e})$	application
	$\text{utlam}(\hat{t}. \hat{e})$	$\Lambda \hat{t}. \hat{e}$	type abstraction
	$\text{utap}\{\hat{\tau}\}(\hat{e})$	$\hat{e}[\hat{\tau}]$	type application
	$\text{ufold}\{\hat{t}. \hat{\tau}\}(\hat{e})$	$\text{fold}(\hat{e})$	fold
	$\text{uunfold}(\hat{e})$	$\text{unfold}(\hat{e})$	unfold
	$\text{utpl}[L](\{i \hookrightarrow \hat{e}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \hat{e}_i\}_{i \in L} \rangle$	labeled tuple
	$\text{upr}[\ell](\hat{e})$	$\hat{e} \cdot \ell$	projection
	$\text{uin}[L][\ell](\{i \hookrightarrow \hat{\tau}_i\}_{i \in L})(\hat{e})$	$\ell \cdot \hat{e}$	injection
	$\text{ucase}[L](\{\hat{\tau}\}(\hat{e}; \{i \hookrightarrow \hat{x}_i. \hat{e}_i\}_{i \in L}))$	$\text{case } \hat{e} \{i \hookrightarrow \hat{x}_i. \hat{e}_i\}_{i \in L}$	case analysis
	$\text{usyntaxue}\{e\}\{\hat{\tau}\}(\hat{a}. \hat{e})$	$\text{syntax } \hat{a} \text{ at } \hat{\tau} \{e\} \text{ in } \hat{e}$	ueTSM definition
	$\text{uapuetism}[b][\hat{a}]$	$\hat{a} / b /$	ueTSM application

Figure 3.5: Abstract syntax of unexpanded types and expressions in miniVerse_{UE}. Metavariable \hat{t} ranges over type sigils, \hat{x} ranges over expression sigils, \hat{a} over TSM names and b over sequences of characters, which, when they appear in an unexpanded expression, are called literal bodies. Literal bodies might contain spliced subterms that are only “surfaced” during typed expansion, so renaming of bound identifiers and substitution are not defined over unexpanded types and expressions.

5. If $\tau = \text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ then for some label set L' and label ℓ and type τ_ℓ , we have that $L = L', \ell$ and $\tau = \text{sum}[L', \ell](\{i \hookrightarrow \tau_i\}_{i \in L'}; \ell \hookrightarrow \tau_\ell)$ and $e = \text{in}[L', \ell][\ell](\{i \hookrightarrow \tau_i\}_{i \in L'}; \ell \hookrightarrow \tau_\ell)(e')$ and $\vdash e' : \tau_\ell$ and $e' \text{ val}$.

The Preservation condition ensures that evaluation preserves typing.

Condition 3.9 (Preservation). *If $\vdash e : \tau$ and $e \mapsto^* e'$ then $\vdash e' : \tau$.*

The Progress condition ensures that evaluation of a well-typed expanded expression cannot “get stuck”.

Condition 3.10 (Progress). *If $\vdash e : \tau$ then either $e \text{ val}$ or there exists an e' such that $e \mapsto e'$.*

Together, these two conditions constitute the Type Safety condition.

3.2.4 Syntax of the Outer Surface

A miniVerse_{UE} program ultimately evaluates as an expanded expression. However, the programmer does not write the expanded expression directly. Instead, the programmer writes a textual sequence, b , consisting of characters in some suitable alphabet (e.g. in

practice, ASCII or Unicode), which is parsed by some partial metafunction $\text{parseUExp}(b)$ to produce an *unexpanded expression*, \hat{e} . Unexpanded expressions can contain *unexpanded types*, \hat{t} , so we also need a partial metafunction $\text{parseUTyp}(b)$. The abstract syntax of unexpanded types and expressions, which form the *outer surface* of $\text{miniVerse}_{\text{UE}}$, is defined in Figure 3.5. The full definition of the textual syntax of $\text{miniVerse}_{\text{UE}}$, which $\text{parseUExp}(b)$ and $\text{parseUTyp}(b)$ implement, is not important for our purposes, so we simply give the following condition, which states that there is some way to textually represent every unexpanded type and expression.

Condition 3.11 (Textual Representability). *Both of the following hold:*

1. For each \hat{t} , there exists b such that $\text{parseUTyp}(b) = \hat{t}$.
2. For each \hat{e} , there exists b such that $\text{parseUExp}(b) = \hat{e}$.

Unexpanded types and expressions are given meaning by expansion to types and expanded expressions, respectively, according to the *typed expansion judgements*, which are defined in the next subsection.

Unexpanded types and expressions bind *type sigils*, \hat{t} , *expression sigils*, \hat{x} , and *TSM names*, \hat{a} . Sigils are given meaning by expansion to variables during typed expansion. We **cannot** adopt the usual definitions of α -renaming of identifiers, because unexpanded types and expressions are still in a “partially parsed” state – the literal bodies, b , within an unexpanded expression might contain spliced subterms that are “surfaced” by a TSM only during typed expansion, as we will detail below.

Each inner core form (defined in Figure 3.4) maps onto an outer surface form. We refer to these as the *shared forms*. In particular:

- Each type variable, t , maps onto a unique type sigil, written \hat{t} (pronounced “sigil of t ”). Notice the distinction between \hat{t} , which is a metavariable ranging over type sigils, and \hat{t} , which is a metafunction, written in stylized form, applied to a type variable to produce a type sigil.
- Each type form maps onto an unexpanded type form $\mathcal{U}(\tau)$ as follows:

$$\begin{aligned}
 \mathcal{U}(t) &= \hat{t} \\
 \mathcal{U}(\text{parr}(\tau_1; \tau_2)) &= \text{uparr}(\mathcal{U}(\tau_1); \mathcal{U}(\tau_2)) \\
 \mathcal{U}(\text{all}(t.\tau)) &= \text{uall}(\hat{t}.\mathcal{U}(\tau)) \\
 \mathcal{U}(\text{rec}(t.\tau)) &= \text{urec}(\hat{t}.\mathcal{U}(\tau)) \\
 \mathcal{U}(\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})) &= \text{uprod}[L](\{i \hookrightarrow \mathcal{U}(\tau_i)\}_{i \in L}) \\
 \mathcal{U}(\text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})) &= \text{usum}[L](\{i \hookrightarrow \mathcal{U}(\tau_i)\}_{i \in L})
 \end{aligned}$$

- Each expression variable, x , maps onto a unique expression sigil written \hat{x} . Again, notice the distinction between \hat{x} and \hat{x} .
- Each expanded expression form maps onto an unexpanded expression form $\mathcal{U}(e)$

as follows:

$$\begin{aligned}
\mathcal{U}(x) &= \hat{x} \\
\mathcal{U}(\text{lam}\{\tau\}(x.e)) &= \text{ulam}\{\mathcal{U}(\tau)\}(\hat{x}.\mathcal{U}(e)) \\
\mathcal{U}(\text{ap}(e_1;e_2)) &= \text{uap}(\mathcal{U}(e_1);\mathcal{U}(e_2)) \\
\mathcal{U}(\text{tlam}(t.e)) &= \text{utlam}(\hat{t}.\mathcal{U}(e)) \\
\mathcal{U}(\text{tap}\{\tau\}(e)) &= \text{utap}\{\mathcal{U}(\tau)\}(\mathcal{U}(e)) \\
\mathcal{U}(\text{fold}\{t.\tau\}(e)) &= \text{ufold}\{\hat{t}.\mathcal{U}(\tau)\}(\mathcal{U}(e)) \\
\mathcal{U}(\text{unfold}(e)) &= \text{uunfold}(\mathcal{U}(e)) \\
\mathcal{U}(\text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})) &= \text{utpl}[L](\{i \hookrightarrow \mathcal{U}(e_i)\}_{i \in L}) \\
\mathcal{U}(\text{in}[L][\ell]\{\{i \hookrightarrow \tau_i\}_{i \in L}\}(e)) &= \text{uin}[L][\ell]\{\{i \hookrightarrow \mathcal{U}(\tau_i)\}_{i \in L}\}(\mathcal{U}(e)) \\
\mathcal{U}(\text{case}[L]\{\tau\}(e; \{i \hookrightarrow x_i.e_i\}_{i \in L})) &= \text{ucase}[L]\{\mathcal{U}(\tau)\}(\mathcal{U}(e); \{i \hookrightarrow \hat{x}_i.\mathcal{U}(e_i)\}_{i \in L})
\end{aligned}$$

There are only two unexpanded expression forms, highlighted in gray in Figure 3.5, that do not correspond to expanded expression forms – the ueTSM definition form and the ueTSM application form.

3.2.5 Typed Expansion

Unexpanded expressions, and the unexpanded types therein, are checked and expanded simultaneously according to the *typed expansion judgements*:

Judgement Form	Description
$\hat{\Delta} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}$	$\hat{\tau}$ is well-formed and has expansion τ assuming $\hat{\Delta}$
$\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau$	\hat{e} has expansion e and type τ under ueTSM context $\hat{\Sigma}$ assuming $\hat{\Delta}$ and $\hat{\Gamma}$

Type Expansion

The *type expansion judgement*, $\hat{\Delta} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}$, is inductively defined by the following rules.

$$\frac{}{\hat{\Delta}, \hat{t} \rightsquigarrow t \text{ type} \vdash \hat{t} \rightsquigarrow t \text{ type}} \quad (3.3a)$$

$$\frac{\hat{\Delta} \vdash \hat{\tau}_1 \rightsquigarrow \tau_1 \text{ type} \quad \hat{\Delta} \vdash \hat{\tau}_2 \rightsquigarrow \tau_2 \text{ type}}{\hat{\Delta} \vdash \text{uparr}(\hat{\tau}_1; \hat{\tau}_2) \rightsquigarrow \text{parr}(\tau_1; \tau_2) \text{ type}} \quad (3.3b)$$

$$\frac{\hat{\Delta}, \hat{t} \rightsquigarrow t \text{ type} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}}{\hat{\Delta} \vdash \text{uall}(\hat{t}.\hat{\tau}) \rightsquigarrow \text{all}(t.\tau) \text{ type}} \quad (3.3c)$$

$$\frac{\hat{\Delta}, \hat{t} \rightsquigarrow t \text{ type} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}}{\hat{\Delta} \vdash \text{urec}(\hat{t}.\hat{\tau}) \rightsquigarrow \text{rec}(t.\tau) \text{ type}} \quad (3.3d)$$

$$\frac{\{\hat{\Delta} \vdash \hat{\tau}_i \rightsquigarrow \tau_i \text{ type}\}_{i \in L}}{\hat{\Delta} \vdash \text{uprod}[L](\{i \hookrightarrow \hat{\tau}_i\}_{i \in L}) \rightsquigarrow \text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L}) \text{ type}} \quad (3.3e)$$

$$\frac{\{\hat{\Delta} \vdash \hat{\tau}_i \rightsquigarrow \tau_i \text{ type}\}_{i \in L}}{\hat{\Delta} \vdash \text{usum}[L](\{i \hookrightarrow \hat{\tau}_i\}_{i \in L}) \rightsquigarrow \text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L}) \text{ type}} \quad (3.3f)$$

Unexpanded type formation contexts, $\hat{\Delta}$, are of the form $\langle \mathcal{D}; \Delta \rangle$, where \mathcal{D} is a *type sigil expansion context*, and Δ is a type formation context. A type sigil expansion context, \mathcal{D} , is a finite function that maps each type sigil $\hat{t} \in \text{dom}(\mathcal{D})$ to the hypothesis $\hat{t} \rightsquigarrow t$, for some type variable t . We write $\mathcal{D} \uplus \hat{t} \rightsquigarrow t$ for the type sigil expansion context that maps \hat{t} to $\hat{t} \rightsquigarrow t$ and defers to \mathcal{D} for all other type sigils (i.e. the previous mapping, if it exists, is updated). We define $\hat{\Delta}, \hat{t} \rightsquigarrow t \text{ type}$ when $\hat{\Delta} = \langle \mathcal{D}; \Delta \rangle$ as an abbreviation of

$$\langle \mathcal{D} \uplus \hat{t} \rightsquigarrow t; \Delta, t \text{ type} \rangle$$

To understand how type sigil expansion contexts operate, it is instructive to derive an expansion for the unexpanded type $\forall \hat{t}. \forall \hat{t}'. \hat{t}. \hat{t}'$, or in operational form, $\text{uall}(\hat{t}. \text{uall}(\hat{t}'. \hat{t}))$:

$$\begin{aligned} & \frac{}{\langle \hat{t} \rightsquigarrow t'; t \text{ type}, t' \text{ type} \rangle \vdash \hat{t} \rightsquigarrow t' \text{ type}} \quad (3.3a) \\ & \frac{}{\langle \hat{t} \rightsquigarrow t; t \text{ type} \rangle \vdash \text{uall}(\hat{t}. \hat{t}) \rightsquigarrow \text{all}(t'. t') \text{ type}} \quad (3.3c) \\ & \frac{}{\langle \emptyset; \emptyset \rangle \vdash \text{uall}(\hat{t}. \text{uall}(\hat{t}'. \hat{t})) \rightsquigarrow \text{all}(t. \text{all}(t'. t')) \text{ type}} \quad (3.3c) \end{aligned}$$

Notice that when a type sigil is bound, a fresh type variable is generated. The type sigil expansion context is extended (when the outermost binding is encountered) or updated (at all inner bindings) and the type formation context is simultaneously extended at each binding (so that typing contexts and ueTSM contexts, discussed below, that contain types that refer to the previous binding remain well-formed). Had we used type variables in the syntax and type formation contexts in the rules above, rather than type sigils and type sigil expansion contexts, derivations for unexpanded types where an inner binding shadows an outer binding would not exist, because by definition we cannot extend a type formation context with a variable it already mentions nor implicitly α -vary the unexpanded type to sidestep this problem.

These rules validate the following lemmas. The Type Expansion Lemma establishes that the expansion of an unexpanded type is a well-formed type.

Lemma 3.12 (Type Expansion). *If $\langle \mathcal{D}; \Delta \rangle \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}$ then $\Delta \vdash \tau \text{ type}$.*

Proof. By rule induction over Rules (3.3). In each case, we apply the IH to or over each premise, then apply the corresponding type formation rule in Rules (3.1). \square

The Type Expressibility Lemma establishes that every well-formed type, τ , can be expressed as a well-formed unexpanded type, $\mathcal{U}(\tau)$. This requires defining the meta-function $\mathcal{U}(\Delta)$ which maps Δ onto an unexpanded type formation context as follows:

$$\begin{aligned} \mathcal{U}(\emptyset) &= \langle \emptyset; \emptyset \rangle \\ \mathcal{U}(\Delta, t \text{ type}) &= \mathcal{U}(\Delta), \hat{t} \rightsquigarrow t \text{ type} \end{aligned}$$

Lemma 3.13 (Type Expressibility). *If $\Delta \vdash \tau$ type then $\mathcal{U}(\Delta) \vdash \mathcal{U}(\tau) \rightsquigarrow \tau$ type.*

Proof. By rule induction over Rules (3.1) using the definitions of $\mathcal{U}(\tau)$ and $\mathcal{U}(\Delta)$ above. In each case, we apply the IH to or over each premise, then apply the corresponding type expansion rule in Rules (3.3). \square

Typed Expression Expansion

Unexpanded typing contexts, $\hat{\Gamma}$, are of the form $\langle \mathcal{G}; \Gamma \rangle$, where \mathcal{G} is an *expression sigil expansion context*, and Γ is a typing context. An expression sigil expansion context, \mathcal{G} , is a finite function that maps each expression sigil $\hat{x} \in \text{dom}(\mathcal{G})$ to the hypothesis $\hat{x} \rightsquigarrow x$, for some expression variable, x . We write $\mathcal{G} \uplus \hat{x} \rightsquigarrow x$ for the expression sigil expansion context that maps \hat{x} to $\hat{x} \rightsquigarrow x$ and defers to \mathcal{G} for all other expression sigils (i.e. the previous mapping, if it exists, is updated). We define $\hat{\Gamma}, \hat{x} \rightsquigarrow x : \tau$ when $\hat{\Gamma} = \langle \mathcal{G}; \Gamma \rangle$ as an abbreviation of

$$\langle \mathcal{G}, \hat{x} \rightsquigarrow x; \Gamma, x : \tau \rangle$$

The *typed expression expansion judgement*, $\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau$, is inductively defined by Rules (3.4) as follows.

Shared Forms Rules (3.4a) through (3.4k) handle unexpanded expressions of shared form. The first five of these rules are defined below:

$$\frac{}{\hat{\Delta} \hat{\Gamma}, \hat{x} \rightsquigarrow x : \tau \vdash_{\hat{\Sigma}} \hat{x} \rightsquigarrow x : \tau} \quad (3.4a)$$

$$\frac{\hat{\Delta} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type} \quad \hat{\Delta} \hat{\Gamma}, \hat{x} \rightsquigarrow x : \tau \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau'}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \text{ulam}\{\hat{\tau}\}(\hat{x}.\hat{e}) \rightsquigarrow \text{lam}\{\tau\}(x.e) : \text{parr}(\tau; \tau')} \quad (3.4b)$$

$$\frac{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e}_1 \rightsquigarrow e_1 : \text{parr}(\tau; \tau') \quad \hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e}_2 \rightsquigarrow e_2 : \tau}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \text{uap}(\hat{e}_1; \hat{e}_2) \rightsquigarrow \text{ap}(e_1; e_2) : \tau'} \quad (3.4c)$$

$$\frac{\hat{\Delta}, \hat{t} \rightsquigarrow t \text{ type} \quad \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \text{utlam}(\hat{t}.\hat{e}) \rightsquigarrow \text{tlam}(t.e) : \text{all}(t.\tau)} \quad (3.4d)$$

$$\frac{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \text{all}(t.\tau) \quad \hat{\Delta} \vdash \hat{\tau}' \rightsquigarrow \tau' \text{ type}}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \text{utap}\{\hat{e}\}(\hat{\tau}') \rightsquigarrow \text{tap}\{e\}(\tau') : [\tau'/t]\tau} \quad (3.4e)$$

Observe that, in each of these rules, the unexpanded and expanded expression forms in the conclusion correspond, and the premises correspond to those of the typing rule for the expanded expression form, i.e. Rules (3.2a) through (3.2e), respectively. In particular, the type expansion premises and type formation premises correspond, and the typed expression expansion and typing premises correspond. The ueTSM context, $\hat{\Sigma}$, passes opaquely through these rules (we will define ueTSM contexts below). Rules (3.3) were similarly generated by mechanically transforming Rules (3.1).

We can express this scheme more precisely with the following rule transformation. For each rule in Rules (3.1) and Rules (3.2),

$$\frac{J_1 \quad \cdots \quad J_k}{J}$$

the corresponding typed expansion rule is

$$\frac{\mathcal{U}(J_1) \quad \cdots \quad \mathcal{U}(J_k)}{\mathcal{U}(J)}$$

where

$$\begin{aligned} \mathcal{U}(\Delta \vdash \tau \text{ type}) &= \mathcal{U}(\Delta) \vdash \mathcal{U}(\tau) \rightsquigarrow \tau \text{ type} \\ \mathcal{U}(\Gamma \Delta \vdash e : \tau) &= \mathcal{U}(\Gamma) \mathcal{U}(\Delta) \vdash_{\hat{\Sigma}} \mathcal{U}(e) \rightsquigarrow e : \tau \\ \mathcal{U}(\{J_i\}_{i \in L}) &= \{\mathcal{U}(J_i)\}_{i \in L} \end{aligned}$$

and where:

- $\mathcal{U}(\tau)$ is defined as follows:
 - When τ is of definite form, $\mathcal{U}(\tau)$ is defined as in Sec. 3.2.4.
 - When τ is of indefinite form, $\mathcal{U}(\tau)$ is a uniquely corresponding metavariable of sort UTyp also of indefinite form. For example, in Rule (3.1b), τ_1 and τ_2 are of indefinite form, i.e. they match arbitrary types. The rule transformation simply “hats” them, i.e. $\mathcal{U}(\tau_1) = \hat{\tau}_1$ and $\mathcal{U}(\tau_2) = \hat{\tau}_2$.
- $\mathcal{U}(e)$ is defined as follows
 - When e is of definite form, $\mathcal{U}(e)$ is defined as in Sec. 3.2.4.
 - When e is of indefinite form, $\mathcal{U}(e)$ is a uniquely corresponding metavariable of sort UExp also of indefinite form. For example, $\mathcal{U}(e_1) = \hat{e}_1$ and $\mathcal{U}(e_2) = \hat{e}_2$.
- $\mathcal{U}(\Delta)$ is defined as follows:
 - When Δ is of definite form, $\mathcal{U}(\Delta)$ is defined as above.
 - When Δ is of indefinite form, $\mathcal{U}(\Delta)$ is a uniquely corresponding metavariable ranging over unexpanded type formation contexts. For example, $\mathcal{U}(\Delta) = \hat{\Delta}$.
- $\mathcal{U}(\Gamma)$ is defined as follows:
 - When Γ is of definite form, $\mathcal{U}(\Gamma)$ produces the corresponding unexpanded typing context as follows:

$$\begin{aligned} \mathcal{U}(\emptyset) &= \langle \emptyset; \emptyset \rangle \\ \mathcal{U}(\Gamma, x : \tau) &= \mathcal{U}(\Gamma), \hat{x} \rightsquigarrow x : \tau \end{aligned}$$

- When Γ is of indefinite form, $\mathcal{U}(\Gamma)$ is a uniquely corresponding metavariable ranging over unexpanded typing contexts. For example, $\mathcal{U}(\Gamma) = \hat{\Gamma}$.

It is instructive to use this rule transformation to generate Rules (3.3) and Rules (3.4a) through (3.4e) above. We omit the remaining rules, i.e. Rules (3.4f) through (3.4k). By instead defining these rules solely by the rule transformation just described, we avoid having to write down a number of rules that are of limited marginal interest. Moreover, this demonstrates the general technique for generating typed expansion rules for unexpanded types and expressions of shared form, so our exposition is somewhat “robust” to changes to the inner core.

We can now establish the Expressibility Theorem – that each well-typed expanded expression, e , can be expressed as an unexpanded expression, \hat{e} , and assigned the same type under the corresponding contexts.

Theorem 3.14 (Expressibility). *If $\Delta \Gamma \vdash e : \tau$ then $\mathcal{U}(\Delta) \mathcal{U}(\Gamma) \vdash_{\hat{\Sigma}} \mathcal{U}(e) \rightsquigarrow e : \tau$.*

Proof. By rule induction over Rules (3.2). The above rule transformation guarantees that this theorem holds by its construction. In particular, in each case, we can apply Lemma 3.13 to or over each type formation premise, the IH to or over each typing premise, then apply the corresponding rule in Rules (3.4). \square

ueTSM Definition and Application The two remaining typed expansion rules, Rules (3.4l) and (3.4m), govern the ueTSM definition and application forms, and are defined in the next two subsections, respectively.

3.2.6 ueTSM Definitions

The stylized ueTSM definition form is

$$\text{syntax } \hat{a} \text{ at } \hat{\tau} \{e_{\text{parse}}\} \text{ in } \hat{e}$$

An unexpanded expression of this form defines a ueTSM named \hat{a} with *unexpanded type annotation* $\hat{\tau}$ and *parse function* e_{parse} for use within \hat{e} .

The parse function is an expanded expression because parse functions are applied statically (i.e. during typed expansion of \hat{e}), as we will discuss when describing ueTSM application below, and evaluation is defined only for closed expanded expressions. This construction simplifies our exposition, though it is not entirely practical because it provides no way for TSM providers to share values between parse functions, nor any way to use TSMs when defining other TSMs. We discuss enriching the language to eliminate these limitations in Sec. 7.3.1, but it is pedagogically simpler to leave the necessary machinery out of our calculus for now.

Rule (3.4l) defines typed expansion of ueTSM definitions (we use stylized forms for clarity):

$$\frac{\begin{array}{l} \hat{\Delta} \vdash \hat{\tau} \rightsquigarrow \tau \text{ type} \quad \emptyset \emptyset \vdash e_{\text{parse}} : \text{Body} \rightarrow \text{ParseResultExp} \\ \hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \text{uetSM}(\tau, e_{\text{parse}})} \hat{e} \rightsquigarrow e : \tau' \end{array}}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \text{syntax } \hat{a} \text{ at } \hat{\tau} \{e_{\text{parse}}\} \text{ in } \hat{e} \rightsquigarrow e : \tau'} \quad (3.4l)$$

The premises of this rule can be understood as follows, in order:

1. The first premise ensures that the unexpanded type annotation is well-formed and expands it to produce the *type annotation*, τ .
2. The second premise checks that the parse function, e_{parse} , is closed and of type

$$\text{Body} \rightarrow \text{ParseResultExp}$$

The type abbreviated `Body` classifies encodings of literal bodies, b . The mapping from literal bodies to values of type `Body` is defined by the *body encoding judgement* $b \downarrow e_{\text{body}}$. An inverse mapping is defined by the *body decoding judgement* $e_{\text{body}} \uparrow b$.

Judgement Form	Description
$b \downarrow e$	b has encoding e
$e \uparrow b$	e has decoding b

Rather than defining `Body` explicitly, and these judgements inductively against that definition (which would be tedious and uninteresting), it suffices to define the following condition, which establishes an isomorphism between literal bodies and values of type `Body` mediated by the judgements above.

Condition 3.15 (Body Isomorphism). *All of the following must hold:*

- (a) For every literal body b , we have that $b \downarrow e_{\text{body}}$ for some e_{body} such that $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$.
- (b) If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ then $e_{\text{body}} \uparrow b$ for some b .
- (c) If $b \downarrow e_{\text{body}}$ then $e_{\text{body}} \uparrow b$.
- (d) If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ and $e_{\text{body}} \uparrow b$ then $b \downarrow e_{\text{body}}$.
- (e) If $b \downarrow e_{\text{body}}$ and $b \downarrow e'_{\text{body}}$ then $e_{\text{body}} = e'_{\text{body}}$.
- (f) If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ and $e_{\text{body}} \uparrow b$ and $e_{\text{body}} \uparrow b'$ then $b = b'$.

`ParseResultExp` abbreviates a labeled sum type that distinguishes successful parses from parse errors¹:

$$\text{ParseResultExp} \triangleq [\text{Success} \hookrightarrow \text{CEExp}, \text{ParseError} \hookrightarrow \langle \rangle]$$

The type abbreviated `CEExp` classifies encodings of *candidate expansion expressions* (or *ce-expression*), \grave{e} (pronounced “grave e ”). The syntax of ce-expressions will be described in Sec. 3.2.8. The mapping from ce-expressions to values of type `CEExp` is defined by the *ce-expression encoding judgement*, $\grave{e} \downarrow_{\text{CEExp}} e$. An inverse mapping is defined by the *ce-expression decoding judgement*, $e \uparrow_{\text{CEExp}} \grave{e}$.

Judgement Form	Description
$\grave{e} \downarrow_{\text{CEExp}} e$	\grave{e} has encoding e
$e \uparrow_{\text{CEExp}} \grave{e}$	e has decoding \grave{e}

¹In VerseML, the `ParseError` constructor of `ParseResult` required an error message and an error location, but we omit these in our formalization for simplicity

Again, rather than picking a particular definition of CEE_{Exp} and defining the judgments above inductively against it, we only state the following condition, which establishes an isomorphism between values of type CEE_{Exp} and ce-expressions.

Condition 3.16 (Candidate Expansion Expression Isomorphism). *All of the following hold:*

- (a) For every \hat{e} , we have $\hat{e} \downarrow_{\text{CEE}_{\text{Exp}}} e_{\text{cand}}$ for some e_{cand} such that $\vdash e_{\text{cand}} : \text{CEE}_{\text{Exp}}$ and $e_{\text{cand}} \text{ val}$.
 - (b) If $\vdash e_{\text{cand}} : \text{CEE}_{\text{Exp}}$ and $e_{\text{cand}} \text{ val}$ then $e_{\text{cand}} \uparrow_{\text{CEE}_{\text{Exp}}} \hat{e}$ for some \hat{e} .
 - (c) If $\hat{e} \downarrow_{\text{CEE}_{\text{Exp}}} e_{\text{cand}}$ then $e_{\text{cand}} \uparrow_{\text{CEE}_{\text{Exp}}} \hat{e}$.
 - (d) If $\vdash e_{\text{cand}} : \text{CEE}_{\text{Exp}}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEE}_{\text{Exp}}} \hat{e}$ then $\hat{e} \downarrow_{\text{CEE}_{\text{Exp}}} e_{\text{cand}}$.
 - (e) If $\hat{e} \downarrow_{\text{CEE}_{\text{Exp}}} e_{\text{cand}}$ and $\hat{e} \downarrow_{\text{CEE}_{\text{Exp}}} e'_{\text{cand}}$ then $e_{\text{cand}} = e'_{\text{cand}}$.
 - (f) If $\vdash e_{\text{cand}} : \text{CEE}_{\text{Exp}}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEE}_{\text{Exp}}} \hat{e}$ and $e_{\text{cand}} \uparrow_{\text{CEE}_{\text{Exp}}} \hat{e}'$ then $\hat{e} = \hat{e}'$.
3. The final premise of Rule (3.41) extends the ueTSM context, $\hat{\Sigma}$, with the newly determined ueTSM definition, and proceeds to assign a type, τ' , and expansion, e , to \hat{e} . The conclusion of Rule (3.41) assigns this type and expansion to the ueTSM definition as a whole.

ueTSM contexts, $\hat{\Sigma}$, are of the form $\langle \mathcal{A}; \Sigma \rangle$, where \mathcal{A} is a TSM naming context and Σ is a ueTSM definition context.

A TSM naming context, \mathcal{A} , is a finite function mapping each TSM name $\hat{a} \in \text{dom}(\mathcal{A})$ to the TSM name-symbol mapping, $\hat{a} \rightsquigarrow a$, for some symbol, a . We write $\mathcal{A} \uplus \hat{a} \rightsquigarrow a$ for the ueTSM naming context that maps \hat{a} to $\hat{a} \rightsquigarrow a$, and defers to \mathcal{A} for all other TSM names (i.e. the previous mapping, if it exists, is updated).

A ueTSM definition context, Σ , is a finite function mapping each symbol $a \in \text{dom}(\Sigma)$ to an expanded ueTSM definition, $a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}})$, where τ is the ueTSM's type annotation, and e_{parse} is its parse function. We write $\Sigma, a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}})$ when $a \notin \text{dom}(\Sigma)$ for the extension of Σ that maps a to $a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}})$. We write $\Delta \vdash \Sigma$ ueTSMs when all the type annotations in Σ are well-formed assuming Δ , and the parse functions in Σ are closed and of type $\text{Body} \rightarrow \text{ParseResultExp}$.

Definition 3.17 (ueTSM Definition Context Formation). $\Delta \vdash \Sigma$ ueTSMs iff for each $\hat{a} \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}}) \in \Sigma$, we have $\Delta \vdash \tau$ type and $\emptyset \emptyset \vdash e_{\text{parse}} : \text{Body} \rightarrow \text{ParseResultExp}$.

We define $\hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}})$, when $\hat{\Sigma} = \langle \mathcal{A}; \Sigma \rangle$, as an abbreviation of

$$\langle \mathcal{A} \uplus \hat{a} \rightsquigarrow a; \Sigma, a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}}) \rangle$$

3.2.7 ueTSM Application

The stylized unexpanded expression form for applying a ueTSM named \hat{a} to a literal form with literal body b is:

$$\hat{a} / b /$$

This stylized form uses forward slashes to delimit the literal body, but stylized variants of any of the literal forms specified in Figure 3.1 could also be added to Figure 3.5. The corresponding operational form is $\text{uapuetism}[b][\hat{a}]$.

The typed expansion rule governing ueTSM application is below:

$$\frac{\begin{array}{c} b \downarrow e_{\text{body}} \quad e_{\text{parse}}(e_{\text{body}}) \Downarrow \text{Success} \cdot e_{\text{cand}} \quad e_{\text{cand}} \uparrow_{\text{CEExp}} \hat{e} \\ \emptyset \emptyset \vdash \hat{\Delta}; \hat{\Gamma}; \hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \text{uetism}(\tau; e_{\text{parse}}); b \quad \hat{e} \rightsquigarrow e : \tau \end{array}}{\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \text{uetism}(\tau; e_{\text{parse}})} \hat{a} / b / \rightsquigarrow e : \tau} \quad (3.4m)$$

The premises of Rule (3.4m) can be understood as follows, in order:

1. The first premise determines the encoding of the literal body, e_{body} (see above).
2. The second premise applies the parse function e_{parse} , which appears in the ueTSM context associated with \hat{a} , to e_{body} . If parsing succeeds, i.e. a value of the (stylized) form $\text{Success} \cdot e_{\text{cand}}$ results from evaluation, then e_{cand} will be a value of type CEEp (assuming a well-formed ueTSM context, by transitive application of the Preservation assumption). We call e_{cand} the *encoding of the candidate expansion*.
If the parse function produces a value labeled `ParseError`, then typed expansion fails. No rule is necessary to handle this case.
3. The third premise decodes the encoding of the candidate expansion to produce the *candidate expansion*, \hat{e} (see above).
4. The final premise of Rule (3.4m) *validates* the candidate expansion and simultaneously generates the *final expansion*, e . This is the topic of Sec. 3.2.9.

3.2.8 Syntax of Candidate Expansions

Figure 3.6 defines the syntax of candidate expansion types (or *ce-types*), $\hat{\tau}$, and candidate expansion expressions (or *ce-expressions*), \hat{e} . Candidate expansion types and expressions are identified up to α -equivalence in the usual manner.

Each inner core form maps onto a candidate expansion form. We refer to these as the *shared forms*. In particular:

- Each type form maps onto a ce-type form according to the metafunction $\mathcal{C}(\tau)$, defined as follows:

$$\begin{aligned} \mathcal{C}(t) &= t \\ \mathcal{C}(\text{parr}(\tau_1; \tau_2)) &= \text{ceparr}(\mathcal{C}(\tau_1); \mathcal{C}(\tau_2)) \\ \mathcal{C}(\text{all}(t.\tau)) &= \text{ceall}(t.\mathcal{C}(\tau)) \\ \mathcal{C}(\text{rec}(t.\tau)) &= \text{cerec}(t.\mathcal{C}(\tau)) \\ \mathcal{C}(\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})) &= \text{ceprod}[L](\{i \hookrightarrow \mathcal{C}(\hat{\tau}_i)\}_{i \in L}) \\ \mathcal{C}(\text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})) &= \text{cesum}[L](\{i \hookrightarrow \mathcal{C}(\hat{\tau}_i)\}_{i \in L}) \end{aligned}$$

Sort	Operational Form	Stylized Form	Description
CETyp $\tilde{\tau} ::=$	t	t	variable
	$\text{ceparr}(\tilde{\tau}; \tilde{\tau})$	$\tilde{\tau} \multimap \tilde{\tau}$	partial function
	$\text{ceall}(t.\tilde{\tau})$	$\forall t.\tilde{\tau}$	polymorphic
	$\text{cerec}(t.\tilde{\tau})$	$\mu t.\tilde{\tau}$	recursive
	$\text{ceprod}[L](\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tilde{\tau}_i\}_{i \in L} \rangle$	labeled product
	$\text{cesum}[L](\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L})$	$[\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L}]$	labeled sum
	$\text{cesplicedt}[m;n]$	$\text{spliced}\langle m,n \rangle$	spliced
CEExp $\tilde{e} ::=$	x	x	variable
	$\text{celam}\{\tilde{\tau}\}(x.\tilde{e})$	$\lambda x:\tilde{\tau}.\tilde{e}$	abstraction
	$\text{ceap}(\tilde{e}; \tilde{e})$	$\tilde{e}(\tilde{e})$	application
	$\text{cetlam}(t.\tilde{e})$	$\Lambda t.\tilde{e}$	type abstraction
	$\text{cetap}\{\tilde{\tau}\}(\tilde{e})$	$\tilde{e}[\tilde{\tau}]$	type application
	$\text{cefold}\{t.\tilde{\tau}\}(\tilde{e})$	$\text{fold}(\tilde{e})$	fold
	$\text{ceunfold}(\tilde{e})$	$\text{unfold}(\tilde{e})$	unfold
	$\text{cetpl}[L](\{i \hookrightarrow \tilde{e}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tilde{e}_i\}_{i \in L} \rangle$	labeled tuple
	$\text{cepr}[\ell](\tilde{e})$	$\tilde{e} \cdot \ell$	projection
	$\text{cein}[L][\ell]\{\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L}\}(\tilde{e})$	$\ell \cdot \tilde{e}$	injection
	$\text{cecase}[L]\{\tau\}(\tilde{e}; \{i \hookrightarrow x_i.\tilde{e}_i\}_{i \in L})$	$\text{case } \tilde{e} \{i \hookrightarrow x_i.\tilde{e}_i\}_{i \in L}$	case analysis
	$\text{cesplicede}[m;n]$	$\text{spliced}\langle m,n \rangle$	spliced

Figure 3.6: Abstract syntax of candidate expansion types and expressions in miniVerse_{UE}. Metavariables m and n range over natural numbers. Candidate expansion types and expressions are identified up to α -equivalence.

- Each expanded expression form maps onto a ce-expression form according to the metafunction $\mathcal{C}(e)$, defined as follows:

$$\begin{aligned}
\mathcal{C}(x) &= x \\
\mathcal{C}(\text{lam}\{\tau\}(x.e)) &= \text{celam}\{\mathcal{C}(\tau)\}(x.\mathcal{C}(e)) \\
\mathcal{C}(\text{ap}(e_1; e_2)) &= \text{ceap}(\mathcal{C}(e_1); \mathcal{C}(e_2)) \\
\mathcal{C}(\text{tlam}(t.e)) &= \text{cetlam}(t.\mathcal{C}(e)) \\
\mathcal{C}(\text{tap}\{\tau\}(e)) &= \text{cetap}\{\mathcal{C}(\tau)\}(\mathcal{C}(e)) \\
\mathcal{C}(\text{fold}\{t.\tau\}(e)) &= \text{cefold}\{t.\mathcal{C}(\tau)\}(\mathcal{C}(e)) \\
\mathcal{C}(\text{unfold}(e)) &= \text{ceunfold}(\mathcal{C}(e)) \\
\mathcal{C}(\text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})) &= \text{cetpl}[L](\{i \hookrightarrow \mathcal{C}(e_i)\}_{i \in L}) \\
\mathcal{C}(\text{in}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(e)) &= \text{cein}[L][\ell](\{i \hookrightarrow \mathcal{C}(\tau_i)\}_{i \in L})(\mathcal{C}(e)) \\
\mathcal{C}(\text{case}[L]\{\tau\}(e; \{i \hookrightarrow x_i.e_i\}_{i \in L})) &= \text{cecase}[L]\{\mathcal{C}(\tau)\}(\mathcal{C}(e); \{i \hookrightarrow x_i.\mathcal{C}(e_i)\}_{i \in L})
\end{aligned}$$

There are two other candidate expansion forms, highlighted in gray in Figure 3.6: a ce-type form for *references to spliced unexpanded types*, $\text{cesplicedt}[m;n]$, and a ce-expression form for *references to spliced unexpanded expressions*, $\text{cesplicede}[m;n]$.

3.2.9 Candidate Expansion Validation

The *candidate expansion validation judgements* validate ce-types and ce-expressions and simultaneously generate their final expansions.

Judgement Form	Description
$\Delta \vdash^{\mathbb{T}} \hat{\tau} \rightsquigarrow \tau \text{ type}$	Candidate expansion type $\hat{\tau}$ is well-formed and has expansion τ assuming Δ and type splicing scene \mathbb{T} .
$\Delta \Gamma \vdash^{\mathbb{E}} \hat{e} \rightsquigarrow e : \tau$	Candidate expansion expression \hat{e} has expansion e and type τ assuming Δ and Γ and expression splicing scene \mathbb{E} .

Expression splicing scenes, \mathbb{E} , are of the form $\hat{\Delta}; \hat{\Gamma}; \hat{\Sigma}; b$, and *type splicing scenes*, \mathbb{T} , are of the form $\Delta; b$. We write $\text{ts}(\mathbb{E})$ for the type splicing scene constructed by dropping the unexpanded typing context and ueTSM context from \mathbb{E} :

$$\text{ts}(\hat{\Delta}; \hat{\Gamma}; \hat{\Sigma}; b) = \hat{\Delta}; b$$

The purpose of splicing scenes is to “remember”, during the candidate expansion validation process, the unexpanded type formation context, $\hat{\Delta}$, unexpanded typing context, $\hat{\Gamma}$, ueTSM context, $\hat{\Sigma}$, and the literal body, b , from the ueTSM application site (cf. Rule (3.4m)), because these are necessary to validate references to spliced unexpanded types and expressions that appear within a candidate expansion.

Candidate Expansion Type Validation

The *candidate expansion type validation judgement*, $\Delta \vdash^{\mathbb{T}} \hat{\tau} \rightsquigarrow \tau \text{ type}$, is inductively defined by Rules (3.5) as follows.

Shared Forms Rules (3.5a) through (3.5f), which validate ce-types of shared form, are defined below.

$$\frac{}{\Delta, t \text{ type} \vdash^{\mathbb{T}} t \rightsquigarrow t \text{ type}} \quad (3.5a)$$

$$\frac{\Delta \vdash^{\mathbb{T}} \tilde{\tau}_1 \rightsquigarrow \tau_1 \text{ type} \quad \Delta \vdash^{\mathbb{T}} \tilde{\tau}_2 \rightsquigarrow \tau_2 \text{ type}}{\Delta \vdash^{\mathbb{T}} \text{ceparr}(\tilde{\tau}_1; \tilde{\tau}_2) \rightsquigarrow \text{parr}(\tau_1; \tau_2) \text{ type}} \quad (3.5b)$$

$$\frac{\Delta, t \text{ type} \vdash^{\mathbb{T}} \tilde{\tau} \rightsquigarrow \tau \text{ type}}{\Delta \vdash^{\mathbb{T}} \text{ceall}(t.\tilde{\tau}) \rightsquigarrow \text{all}(t.\tau) \text{ type}} \quad (3.5c)$$

$$\frac{\Delta, t \text{ type} \vdash^{\mathbb{T}} \tilde{\tau} \rightsquigarrow \tau \text{ type}}{\Delta \vdash^{\mathbb{T}} \text{cerec}(t.\tilde{\tau}) \rightsquigarrow \text{rec}(t.\tau) \text{ type}} \quad (3.5d)$$

$$\frac{\{\Delta \vdash^{\mathbb{T}} \tilde{\tau}_i \rightsquigarrow \tau_i \text{ type}\}_{i \in L}}{\Delta \vdash^{\mathbb{T}} \text{cprod}[L](\{i \mapsto \tilde{\tau}_i\}_{i \in L}) \rightsquigarrow \text{prod}[L](\{i \mapsto \tau_i\}_{i \in L}) \text{ type}} \quad (3.5e)$$

$$\frac{\{\Delta \vdash^{\mathbb{T}} \tilde{\tau}_i \rightsquigarrow \tau_i \text{ type}\}_{i \in L}}{\Delta \vdash^{\mathbb{T}} \text{cesum}[L](\{i \mapsto \tilde{\tau}_i\}_{i \in L}) \rightsquigarrow \text{sum}[L](\{i \mapsto \tau_i\}_{i \in L}) \text{ type}} \quad (3.5f)$$

Observe that, in each of these rules, the ce-type form and the type form in the conclusion correspond, and the premises correspond to those of the corresponding type formation rule, i.e. Rules (3.1). The type splicing scene, \mathbb{T} , passes opaquely through these rules. The following lemma establishes that each type can be expressed as a well-formed ce-type, under the same type formation context and any type splicing scene.

Lemma 3.18 (Candidate Expansion Type Expressibility). *If $\Delta \vdash \tau \text{ type}$ then $\Delta \vdash^{\mathbb{T}} \mathcal{C}(\tau) \rightsquigarrow \tau \text{ type}$.*

Proof. By rule induction over Rules (3.1). In each case, we apply the IH on or over each premise, then apply the corresponding ce-type validation rule in Rules (3.5). \square

Notice that in Rule (3.5a), only type variables tracked by the candidate expansion type formation context, Δ , are validated. Type variables in the application site unexpanded type formation context, which appears within the type splicing scene, \mathbb{T} , are not validated. Indeed, \mathbb{T} is not inspected by any of the rules above. This achieves *context-independent expansion* as described in Sec. 3.1.3 for type variables – ueTSMs cannot impose “hidden constraints” on the application site unexpanded type formation context, because the type variables bound at the application site are simply not directly available to ce-types.

References to Spliced Types The only ce-type form that does not correspond to a type form is $\text{cesplicedt}[m;n]$, which is a *reference to a spliced unexpanded type*, i.e. it indicates that an unexpanded type should be parsed out from the literal body, b , which appears in the type splicing scene, beginning at position m and ending at position n .

Rule (3.5g) governs this form:

$$\frac{\text{parseUTyp}(\text{subseq}(b; m; n)) = \hat{\tau} \quad \langle \mathcal{D}; \Delta_{\text{app}} \rangle \vdash \hat{\tau} \rightsquigarrow \tau \text{ type} \quad \Delta \cap \Delta_{\text{app}} = \emptyset}{\Delta \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle; b \text{ cesplicedt}[m; n] \rightsquigarrow \tau \text{ type}} \quad (3.5g)$$

The first premise of this rule extracts the indicated subsequence of b using the partial metafunction $\text{subseq}(b; m; n)$ and parses it using the partial metafunction $\text{parseUTyp}(b)$, described in Sec. 3.2.4, to produce the spliced unexpanded type itself, $\hat{\tau}$.

The second premise of Rule (3.5g) performs type expansion of $\hat{\tau}$ under the application site unexpanded type formation context, $\langle \mathcal{D}; \Delta_{\text{app}} \rangle$, which appears in the type splicing scene. The hypotheses in the candidate expansion type formation context, Δ , are not made available to τ .

The third premise of Rule (3.5g) imposes the constraint that the candidate expansion's type formation context, Δ , be disjoint from the application site type formation context, Δ_{app} . This premise can always be discharged by α -varying the candidate expansion that the reference to the spliced type appears within.

This achieves *expansion-independent splicing* as described in Sec. 3.1.3 for type variables – the TSM provider can choose type variable names freely within a candidate expansion, because the language prevents them from shadowing type variables at the application site (by α -varying the candidate expansion as needed).

Rules (3.5) validate the following lemma, which establishes that the final expansion of a valid ce-type is a well-formed type under the combined type formation context.

Lemma 3.19 (Candidate Expansion Type Validation). *If $\Delta \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle; b \hat{\tau} \rightsquigarrow \tau \text{ type}$ then $\Delta \cup \Delta_{\text{app}} \vdash \tau \text{ type}$.*

Proof. By rule induction over Rules (3.5).

Case (3.5a). We have

- | | |
|--|--|
| (1) $\Delta = \Delta', t \text{ type}$ | by assumption |
| (2) $\hat{\tau} = t$ | by assumption |
| (3) $\tau = t$ | by assumption |
| (4) $\Delta', t \text{ type} \vdash t \text{ type}$ | by Rule (3.1a) |
| (5) $\Delta', t \text{ type} \cup \Delta_{\text{app}} \vdash t \text{ type}$ | by Lemma 3.2 over Δ_{app} to (4) |

Case (3.5b). We have

- | | |
|---|---------------|
| (1) $\hat{\tau} = \text{ceparr}(\hat{\tau}_1; \hat{\tau}_2)$ | by assumption |
| (2) $\tau = \text{parr}(\tau_1; \tau_2)$ | by assumption |
| (3) $\Delta \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle; b \hat{\tau}_1 \rightsquigarrow \tau_1 \text{ type}$ | by assumption |
| (4) $\Delta \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle; b \hat{\tau}_2 \rightsquigarrow \tau_2 \text{ type}$ | by assumption |
| (5) $\Delta \cup \Delta_{\text{app}} \vdash \tau_1 \text{ type}$ | by IH on (3) |
| (6) $\Delta \cup \Delta_{\text{app}} \vdash \tau_2 \text{ type}$ | by IH on (4) |

(7) $\Delta \cup \Delta_{\text{app}} \vdash \text{parr}(\tau_1; \tau_2)$ type by Rule (3.1b) on (5) and (6)

Case (3.5c). We have

(1) $\hat{\tau} = \text{ceall}(t.\hat{\tau}')$	by assumption
(2) $\tau = \text{all}(t.\tau')$	by assumption
(3) $\Delta, t \text{ type} \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle;^b \hat{\tau}' \rightsquigarrow \tau' \text{ type}$	by assumption
(4) $\Delta, t \text{ type} \cup \Delta_{\text{app}} \vdash \tau' \text{ type}$	by IH on (3)
(5) $\Delta \cup \Delta_{\text{app}}, t \text{ type} \vdash \tau' \text{ type}$	by exchange over Δ_{app} on (4)
(6) $\Delta \cup \Delta_{\text{app}} \vdash \text{all}(t.\tau') \text{ type}$	by Rule (3.1c) on (5)

Case (3.5d) through (3.5f). These cases follow analagously, i.e. we apply the IH to or over all ce-type validation premises, apply exchange as needed, and then apply the corresponding type formation rule.

Case (3.5g). We have

(1) $\hat{\tau} = \text{cesplciedt}[m; n]$	by assumption
(2) $\text{parseUTyp}(\text{subseq}(b; m; n)) = \hat{\tau}$	by assumption
(3) $\langle \mathcal{D}; \Delta_{\text{app}} \rangle \vdash \hat{\tau} \rightsquigarrow \tau \text{ type}$	by assumption
(4) $\Delta_{\text{app}} \vdash \tau \text{ type}$	by Lemma 3.12 on (3)
(5) $\Delta \cup \Delta_{\text{app}} \vdash \tau \text{ type}$	by Lemma 3.2 over Δ on (4) and exchange over Δ

□

Candidate Expansion Expression Validation

The *candidate expansion expression validation judgement*, $\Delta \Gamma \vdash^{\mathbb{E}} e \rightsquigarrow e : \tau$, is defined mutually inductively with the typed expansion judgement by Rules (3.6) as follows.

Shared Forms Rules (3.6a) through (3.6k) validate ce-expressions of shared form. The first three of these rules are defined below:

$$\frac{}{\Delta \Gamma, x : \tau \vdash^{\mathbb{E}} x \rightsquigarrow x : \tau} \quad (3.6a)$$

$$\frac{\Delta \vdash^{\text{ts}(\mathbb{E})} \hat{\tau} \rightsquigarrow \tau \text{ type} \quad \Delta \Gamma, x : \tau \vdash^{\mathbb{E}} e \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash^{\mathbb{E}} \text{celam}\{\tau\}(x.\hat{e}) \rightsquigarrow \text{lam}\{\tau\}(x.e) : \text{parr}(\tau; \tau')} \quad (3.6b)$$

$$\frac{\Delta \Gamma \vdash^{\mathbb{E}} \hat{e}_1 \rightsquigarrow e_1 : \text{parr}(\tau; \tau') \quad \Delta \Gamma \vdash^{\mathbb{E}} \hat{e}_2 \rightsquigarrow e_2 : \tau}{\Delta \Gamma \vdash^{\mathbb{E}} \text{ceap}(\hat{e}_1; \hat{e}_2) \rightsquigarrow \text{ap}(e_1; e_2) : \tau'} \quad (3.6c)$$

Observe that, in each of these rules, the ce-expression form and the expanded expression form in the conclusion correspond, and the premises correspond to those of the corresponding typing rule, i.e. Rules (3.2a) through (3.2c), respectively. The expression splicing scene, \mathbb{E} , passes opaquely through these rules.

We can express this scheme more precisely with the following rule transformation. For each rule in Rules (3.2),

$$\frac{J_1 \quad \cdots \quad J_k}{J}$$

the corresponding candidate expansion expression validation rule is

$$\frac{\mathcal{C}(J_1) \quad \cdots \quad \mathcal{C}(J_k)}{\mathcal{C}(J)}$$

where

$$\begin{aligned} \mathcal{C}(\Delta \vdash \tau \text{ type}) &= \Delta \vdash^{\text{ts}(\mathbb{E})} \mathcal{C}(\tau) \rightsquigarrow \tau \text{ type} \\ \mathcal{C}(\Delta \Gamma \vdash e : \tau) &= \Delta \Gamma \vdash^{\mathbb{E}} \mathcal{C}(e) \rightsquigarrow e : \tau \\ \mathcal{C}(\{J_i\}_{i \in L}) &= \{\mathcal{C}(J_i)\}_{i \in L} \end{aligned}$$

and where:

- $\mathcal{C}(\tau)$ is defined as follows:
 - When τ is of definite form, $\mathcal{C}(\tau)$ is defined as in Sec. 3.2.8.
 - When τ is of indefinite form, $\mathcal{C}(\tau)$ is a uniquely corresponding metavariable of sort CETyp also of indefinite form. For example, $\mathcal{C}(\tau_1) = \tau_1$ and $\mathcal{C}(\tau_2) = \tau_2$.
- $\mathcal{C}(e)$ is defined as follows
 - When e is of definite form, $\mathcal{C}(e)$ is defined as in Sec. 3.2.8.
 - When e is of indefinite form, $\mathcal{C}(e)$ is a uniquely corresponding metavariable of sort CEEExp also of indefinite form. For example, $\mathcal{C}(e_1) = e_1$ and $\mathcal{C}(e_2) = e_2$.

It is instructive to use this rule transformation to generate Rules (3.6a) through (3.6c) above. We omit the remaining rules for shared forms, i.e. Rules (3.6d) through (3.6k).

The following lemma establishes that each well-typed expanded expression, e , can be expressed as a valid ce-expression, $\mathcal{C}(e)$, that is assigned the same type under any expression splicing scene.

Lemma 3.20 (Candidate Expansion Expression Expressibility). *If $\Delta \Gamma \vdash e : \tau$ then $\Delta \Gamma \vdash^{\mathbb{E}} \mathcal{C}(e) \rightsquigarrow e : \tau$.*

Proof. By rule induction over Rules (3.2). The rule transformation above guarantees that this lemma holds by construction. In particular, in each case, we apply Lemma 3.18 to or over each type formation premise, the IH to or over each typing premise, then apply the corresponding ce-expression validation rule in Rules (3.6a) through (3.6k). \square

Notice that in Rule (3.6a), only variables tracked by the candidate expansion typing context, Γ , are validated. Variables in the application site unexpanded typing context, which appears within the expression splicing scene \mathbb{E} , are not validated. Indeed, \mathbb{E} is not inspected by any of the rules above. This achieves *context-independent expansion* as described in Sec. 3.1.3 – ueTSMs cannot impose “hidden constraints” on the application site unexpanded typing context, because the variable bindings at the application site are not directly available to candidate expansions.

References to Spliced Unexpanded Expressions The only ce-expression form that does not correspond to an expanded expression form is $\text{cesplicede}[m;n]$, which is a *reference to a spliced unexpanded expression*, i.e. it indicates that an unexpanded expression should be parsed out from the literal body beginning at position m and ending at position n . Rule (3.6l) governs this form:

$$\frac{\text{parseUExp}(\text{subseq}(b;m;n)) = \hat{e} \quad \langle \mathcal{D}; \Delta_{\text{app}} \rangle \langle \mathcal{G}; \Gamma_{\text{app}} \rangle \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau \quad \Delta \cap \Delta_{\text{app}} = \emptyset \quad \text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset}{\Delta \Gamma \vdash \langle \mathcal{D}; \Delta_{\text{app}} \rangle; \langle \mathcal{G}; \Gamma_{\text{app}} \rangle; \hat{\Sigma}; b \text{ cesplicede}[m;n] \rightsquigarrow e : \tau} \quad (3.6l)$$

The first premise of this rule extracts the indicated subsequence of b using the partial metafunction $\text{subseq}(b;m;n)$ and parses it using the partial metafunction $\text{parseUExp}(b)$, described in Sec. 3.2.4, to produce the referenced spliced unexpanded expression, \hat{e} .

The second premise of Rule (3.6l) types and expands the spliced unexpanded expression \hat{e} assuming the application site contexts that appear in the expression splicing scene. The hypotheses in the candidate expansion type formation context, Δ , and typing context, Γ , are not made available to \hat{e} .

The third premise of Rule (3.6l) imposes the constraint that the candidate expansion’s type formation context, Δ , be disjoint from the application site type formation context, Δ_{app} . Similarly, the fourth premise requires that the candidate expansion’s typing context, Γ , be disjoint from the application site typing context, Γ_{app} . These two premises can always be discharged by α -varying the ce-expression that the reference to the spliced unexpanded expression appears within.

This achieves *expansion-independent splicing* as described in Sec. 3.1.3 – the TSM provider can choose variable names freely within a candidate expansion, because the language prevents them from shadowing those at the application site (by α -varying the candidate expansion as needed).

3.2.10 Metatheory

For the judgements we have defined to form a sensible language, we must have that typed expansion and candidate expansion expression validation be consistent with typing. Formally, this can be expressed as follows.

Theorem 3.21 (Typed Expansion). *Both of the following hold:*

1. If $\langle \mathcal{D}; \Delta \rangle \langle \mathcal{G}; \Gamma \rangle \vdash_{\langle \mathcal{A}; \Sigma \rangle} \hat{e} \rightsquigarrow e : \tau$ and $\Delta \vdash \Sigma$ ueTSMs then $\Delta \Gamma \vdash e : \tau$.

2. If $\Delta \Gamma \vdash \langle \mathcal{D}; \Delta_{app} \rangle; \langle \mathcal{G}; \Gamma_{app} \rangle; \langle \mathcal{A}; \Sigma \rangle; b \hat{e} \rightsquigarrow e : \tau$ and $\Delta_{app} \vdash \Sigma$ ueTSMs and $\Delta \cap \Delta_{app} = \emptyset$ and $\text{dom}(\Gamma) \cap \text{dom}(\Gamma_{app}) = \emptyset$ then $\Delta \cup \Delta_{app} \Gamma \cup \Gamma_{app} \vdash e : \tau$.

Proof. By mutual rule induction over Rules (3.4) and Rules (3.6).

The proof of part 1 proceeds by inducting over the typed expansion assumption. In the following cases, let $\hat{\Delta} = \langle \mathcal{D}; \Delta \rangle$ and $\hat{\Gamma} = \langle \mathcal{G}; \Gamma \rangle$ and $\hat{\Sigma} = \langle \mathcal{A}; \Sigma \rangle$.

Case (3.4a). We have

- | | |
|--|----------------|
| (1) $\hat{e} = \hat{x}$ | by assumption |
| (2) $e = x$ | by assumption |
| (3) $\Gamma = \Gamma', x : \tau$ | by assumption |
| (4) $\Delta \Gamma', x : \tau \vdash x : \tau$ | by Rule (3.2a) |

Case (3.4b). We have

- | | |
|--|-------------------------------|
| (1) $\hat{e} = \text{ulam}\{\hat{\tau}_1\}(\hat{x}.\hat{e}')$ | by assumption |
| (2) $e = \text{lam}\{\tau_1\}(x.e')$ | by assumption |
| (3) $\tau = \text{parr}(\tau_1; \tau_2)$ | by assumption |
| (4) $\hat{\Delta} \vdash \hat{\tau}_1 \rightsquigarrow \tau_1$ type | by assumption |
| (5) $\hat{\Delta} \hat{\Gamma}, \hat{x} \rightsquigarrow x : \tau_1 \vdash_{\hat{\Sigma}} \hat{e}' \rightsquigarrow e' : \tau_2$ | by assumption |
| (6) $\Delta \vdash \Sigma$ ueTSMs | by assumption |
| (7) $\Delta \vdash \tau_1$ type | by Lemma 3.12 on (4) |
| (8) $\Delta \Gamma, x : \tau_1 \vdash e' : \tau_2$ | by IH on (5) and (6) |
| (9) $\Delta \Gamma \vdash \text{lam}\{\tau_1\}(x.e') : \text{parr}(\tau_1; \tau_2)$ | by Rule (3.2b) on (7) and (8) |

Case (3.4c). We have

- | | |
|--|-------------------------------|
| (1) $\hat{e} = \text{uap}(\hat{e}_1; \hat{e}_2)$ | by assumption |
| (2) $e = \text{ap}(e_1; e_2)$ | by assumption |
| (3) $\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e}_1 \rightsquigarrow e_1 : \text{parr}(\tau_1; \tau)$ | by assumption |
| (4) $\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e}_2 \rightsquigarrow e_2 : \tau_1$ | by assumption |
| (5) $\Delta \vdash \Sigma$ ueTSMs | by assumption |
| (6) $\Delta \Gamma \vdash e_1 : \text{parr}(\tau_1; \tau)$ | by IH on (3) and (5) |
| (7) $\Delta \Gamma \vdash e_2 : \tau_1$ | by IH on (4) and (5) |
| (8) $\Delta \Gamma \vdash \text{ap}(e_1; e_2) : \tau$ | by Rule (3.2c) on (6) and (7) |

Case (3.4d) through (3.4k). These cases follow analogously, i.e. we apply Lemma 3.12 to or over the type expansion premises and the IH to or over the typed expression expansion premises and then apply the corresponding typing rule.

Case (3.4l). We have

- | | |
|---|---------------|
| (1) $\hat{e} = \text{usyntaxue}\{e_{\text{parse}}\}\{\hat{\tau}'\}(\hat{a}.\hat{e}')$ | by assumption |
|---|---------------|

- | | |
|---|--|
| (2) $\hat{\Delta} \vdash \hat{\tau}' \rightsquigarrow \tau'$ type | by assumption |
| (3) $\emptyset \emptyset \vdash e_{\text{parse}} : \text{parr}(\text{Body}; \text{ParseResultExp})$ | by assumption |
| (4) $\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \text{uet sm}(\tau'; e_{\text{parse}})} \hat{e}' \rightsquigarrow e : \tau$ | by assumption |
| (5) $\Delta \vdash \Sigma$ ueTSMs | by assumption |
| (6) $\Delta \vdash \tau'$ type | by Lemma 3.12 to (2) |
| (7) $\Delta \vdash \Sigma, \hat{a} \hookrightarrow \text{uet sm}(\tau'; e_{\text{parse}})$ ueTSMs | by Definition 3.17 on (5), (6) and (3) |
| (8) $\Delta \Gamma \vdash e : \tau$ | by IH on (4) and (7) |

Case (3.4m). We have

- | | |
|--|---|
| (1) $\hat{e} = \text{uapuet sm}[b][\hat{a}]$ | by assumption |
| (2) $\mathcal{A} = \mathcal{A}', \hat{a} \rightsquigarrow a$ | by assumption |
| (3) $\Sigma = \Sigma', a \hookrightarrow \text{uet sm}(\tau; e_{\text{parse}})$ | by assumption |
| (4) $b \downarrow e_{\text{body}}$ | by assumption |
| (5) $e_{\text{parse}}(e_{\text{body}}) \Downarrow \text{Success} \cdot e_{\text{cand}}$ | by assumption |
| (6) $e_{\text{cand}} \uparrow \text{CEE}_{\text{Exp}} \hat{e}$ | by assumption |
| (7) $\emptyset \emptyset \vdash \hat{\Delta}; \hat{\Gamma}; \hat{\Sigma}; b \hat{e} \rightsquigarrow e : \tau$ | by assumption |
| (8) $\Delta \vdash \Sigma$ ueTSMs | by assumption |
| (9) $\emptyset \cap \Delta = \emptyset$ | by finite set intersection identity |
| (10) $\text{dom}(\emptyset) \cap \text{dom}(\Gamma) = \emptyset$ | by finite set intersection identity |
| (11) $\emptyset \cup \Delta \emptyset \cup \Gamma \vdash e : \tau$ | by IH, part 2 on (7), (8), (9), and (10) |
| (12) $\Delta \Gamma \vdash e : \tau$ | by definition of finite set union over (11) |

The second part of the theorem proceeds by induction over the candidate expansion expression validation assumption as follows. In the following cases, let $\hat{\Delta}_{\text{app}} = \langle \mathcal{D}; \Delta_{\text{app}} \rangle$ and $\hat{\Gamma}_{\text{app}} = \langle \mathcal{G}; \Gamma_{\text{app}} \rangle$ and $\hat{\Sigma} = \langle \mathcal{A}; \Sigma \rangle$.

Case (3.6a). We have

- | | |
|--|--|
| (1) $\hat{e} = x$ | by assumption |
| (2) $e = x$ | by assumption |
| (3) $\Gamma = \Gamma', x : \tau$ | by assumption |
| (4) $\Delta \cup \Delta_{\text{app}} \Gamma', x : \tau \vdash x : \tau$ | by Rule (3.2a) |
| (5) $\Delta \cup \Delta_{\text{app}} \Gamma', x : \tau \cup \Gamma_{\text{app}} \vdash x : \tau$ | by Lemma 3.2 over Γ_{app} to (4) |

Case (3.6b). We have

- | | |
|--|---------------|
| (1) $\hat{e} = \text{celam}\{\hat{\tau}_1\}(x.\hat{e}')$ | by assumption |
|--|---------------|

(2) $e = \text{lam}\{\tau_1\}(x.e')$	by assumption
(3) $\tau = \text{parr}(\tau_1; \tau_2)$	by assumption
(4) $\Delta \vdash^{\hat{\Delta}_{\text{app}}; b} \tau_1 \rightsquigarrow \tau_1 \text{ type}$	by assumption
(5) $\Delta \Gamma, x : \tau_1 \vdash^{\hat{\Delta}_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} e' \rightsquigarrow e' : \tau_2$	by assumption
(6) $\Delta_{\text{app}} \vdash \Sigma \text{ ueTSMs}$	by assumption
(7) $\Delta \cap \Delta_{\text{app}} = \emptyset$	by assumption
(8) $\text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset$	by assumption
(9) $x \notin \text{dom}(\Gamma_{\text{app}})$	by identification convention
(10) $\text{dom}(\Gamma, x : \tau_1) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset$	by (8) and (9)
(11) $\Delta \cup \Delta_{\text{app}} \vdash \tau_1 \text{ type}$	by Lemma 3.19 on (4)
(12) $\Delta \cup \Delta_{\text{app}} \Gamma, x : \tau_1 \cup \Gamma_{\text{app}} \vdash e' : \tau_2$	by IH on (5), (6), (7) and (10)
(13) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}}, x : \tau_1 \vdash e' : \tau_2$	by exchange over Γ_{app} on (12)
(14) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash \text{lam}\{\tau_1\}(x.e') : \text{parr}(\tau_1; \tau_2)$	by Rule (3.2b) on (11) and (13)

Case (3.6c). We have

(1) $e = \text{ceap}(e_1; e_2)$	by assumption
(2) $e = \text{ap}(e_1; e_2)$	by assumption
(3) $\Delta \Gamma \vdash^{\hat{\Delta}_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} e_1 \rightsquigarrow e_1 : \text{parr}(\tau_2; \tau)$	by assumption
(4) $\Delta \Gamma \vdash^{\hat{\Delta}_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} e_2 \rightsquigarrow e_2 : \tau_2$	by assumption
(5) $\Delta_{\text{app}} \vdash \Sigma \text{ ueTSMs}$	by assumption
(6) $\Delta \cap \Delta_{\text{app}} = \emptyset$	by assumption
(7) $\text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset$	by assumption
(8) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash e_1 : \text{parr}(\tau_2; \tau)$	by IH on (3), (5), (6) and (7)
(9) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash e_2 : \tau_2$	by IH on (4), (5), (6) and (7)
(10) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash \text{ap}(e_1; e_2) : \tau$	by Rule (3.2c) on (8) and (9)

Case (3.6d). We have

(1) $e = \text{cetlam}(t.e')$	by assumption
(2) $e = \text{tlam}(t.e')$	by assumption
(3) $\tau = \text{all}(t.\tau')$	by assumption
(4) $\Delta, t \text{ type } \Gamma \vdash^{\hat{\Delta}_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} e' \rightsquigarrow e' : \tau'$	by assumption
(5) $\Delta_{\text{app}} \vdash \Sigma \text{ ueTSMs}$	by assumption
(6) $\Delta \cap \Delta_{\text{app}} = \emptyset$	by assumption
(7) $\text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset$	by assumption

(8) $t \text{ type} \notin \Delta_{\text{app}}$	by identification
(9) $\Delta, t \text{ type} \cap \Delta_{\text{app}} = \emptyset$	convention by (6) and (8)
(10) $\Delta, t \text{ type} \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash e' : \tau'$	by IH on (4), (5), (9) and (7)
(11) $\Delta \cup \Delta_{\text{app}}, t \text{ type} \Gamma \cup \Gamma_{\text{app}} \vdash e' : \tau'$	by exchange over Δ_{app} on (10)
(12) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash \text{tlam}(t.e') : \text{all}(t.\tau')$	by Rule (3.2d) on (11)

Case (3.6e) through (3.6k). These cases follow analogously, i.e. we apply the IH to all ce-expression validation judgements, Lemma 3.19 to all ce-type validation judgements, the identification convention to ensure that extended contexts remain disjoint, weakening and exchange as needed, and the corresponding typing rule.

Case (3.6l). We have

(1) $\hat{e} = \text{cesplicede}[m; n]$	by assumption
(2) $\text{parseUExp}(\text{subseq}(b; m; n)) = \hat{e}$	by assumption
(3) $\hat{\Delta}_{\text{app}} \hat{\Gamma}_{\text{app}} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau$	by assumption
(4) $\Delta_{\text{app}} \vdash \Sigma \text{ ueTSMs}$	by assumption
(5) $\Delta \cap \Delta_{\text{app}} = \emptyset$	by assumption
(6) $\text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset$	by assumption
(7) $\Delta_{\text{app}} \Gamma_{\text{app}} \vdash e : \tau$	by IH, part 1 on (3) and (4)
(8) $\Delta \cup \Delta_{\text{app}} \Gamma \cup \Gamma_{\text{app}} \vdash e : \tau$	by Lemma 3.2 over Δ and Γ and exchange on (7)

The mutual induction can be shown to be well-founded by showing that the following numeric metric on the judgements that we induct over is decreasing:

$$\begin{aligned} \|\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau\| &= \|\hat{e}\| \\ \|\Delta \Gamma \vdash_{\Delta_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} \hat{e} \rightsquigarrow e : \tau\| &= \|b\| \end{aligned}$$

where $\|b\|$ is the length of b and $\|\hat{e}\|$ is the sum of the lengths of the literal bodies in \hat{e} ,

$$\begin{aligned} \|x\| &= 0 \\ \|\text{ulam}\{\tau\}(x.\hat{e})\| &= \|\hat{e}\| \\ \|\text{uap}(\hat{e}_1; \hat{e}_2)\| &= \|\hat{e}_1\| + \|\hat{e}_2\| \\ \|\text{utlam}(t.\hat{e})\| &= \|\hat{e}\| \\ \|\text{utap}\{\tau\}(\hat{e})\| &= \|\hat{e}\| \\ \|\text{ufold}\{t.\tau\}(\hat{e})\| &= \|\hat{e}\| \\ \|\text{uunfold}(\hat{e})\| &= \|\hat{e}\| \end{aligned}$$

$$\begin{aligned}
\|\mathbf{utpl}[L](\{i \hookrightarrow \hat{e}_i\}_{i \in L})\| &= \sum_{i \in L} \|\hat{e}_i\| \\
\|\mathbf{upr}[\ell](\hat{e})\| &= \|\hat{e}\| \\
\|\mathbf{uin}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(\hat{e})\| &= \|\hat{e}\| \\
\|\mathbf{ucase}[L](\tau)(\hat{e}; \{i \hookrightarrow x_i.\hat{e}_i\}_{i \in L})\| &= \|\hat{e}\| + \sum_{i \in L} \|\hat{e}_i\| \\
\|\mathbf{usyntaxue}\{\hat{e}_{\text{parse}}\}(\tau)(\hat{a}.\hat{e})\| &= \|\hat{e}\| \\
\|\mathbf{uapuetism}[b][\hat{a}]\| &= \|b\|
\end{aligned}$$

The only case in the proof of part 1 that invokes part 2 is Case (3.4m). There, we have that the metric remains stable:

$$\begin{aligned}
&\|\hat{\Delta} \hat{\Gamma} \vdash_{\hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \mathbf{uetism}(\tau; e_{\text{parse}})} \mathbf{uapuetism}[b][\hat{a}] \rightsquigarrow e : \tau\| \\
&= \|\emptyset \emptyset \vdash_{\hat{\Delta}; \hat{\Gamma}; \hat{\Sigma}, \hat{a} \rightsquigarrow a \hookrightarrow \mathbf{uetism}(\tau; e_{\text{parse}}); b} \hat{e} \rightsquigarrow e : \tau\| \\
&= \|b\|
\end{aligned}$$

The only case in the proof of part 2 that invokes part 1 is Case (3.6l). There, we have that $\text{parseUExp}(\text{subseq}(b; m; n)) = \hat{e}$ and the IH is applied to the judgement $\hat{\Delta}_{\text{app}} \hat{\Gamma}_{\text{app}} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau$ where $\hat{\Delta}_{\text{app}} = \langle \mathcal{D}; \Delta_{\text{app}} \rangle$ and $\hat{\Gamma}_{\text{app}} = \langle \mathcal{G}; \Gamma_{\text{app}} \rangle$ and $\hat{\Sigma} = \langle \mathcal{A}; \Sigma \rangle$. Because the metric is stable when passing from part 1 to part 2, we must have that it is strictly decreasing in the other direction:

$$\|\hat{\Delta}_{\text{app}} \hat{\Gamma}_{\text{app}} \vdash_{\hat{\Sigma}} \hat{e} \rightsquigarrow e : \tau\| < \|\Delta \Gamma \vdash_{\hat{\Delta}_{\text{app}}; \hat{\Gamma}_{\text{app}}; \hat{\Sigma}; b} \mathbf{cesplicede}[m; n] \rightsquigarrow e : \tau\|$$

i.e. by the definitions above,

$$\|\hat{e}\| < \|b\|$$

This is established by appeal to the following two conditions. The first condition simply states that subsequences of b are no longer than b .

Condition 3.22 (Body Subsequences). *If $\text{subseq}(b; m; n) = b'$ then $\|b'\| \leq \|b\|$.*

The second condition states that an unexpanded expression constructed by parsing a textual sequence b is strictly smaller, as measured by the metric defined above, than the length of b , because some characters must necessarily be used to invoke a TSM on and delimit each literal body.

Condition 3.23 (Body Parsing). *If $\text{parseUExp}(b) = \hat{e}$ then $\|\hat{e}\| < \|b\|$.*

Combining Conditions 3.22 and 3.23, we have that $\|\hat{e}\| < \|b\|$ as needed. □

Chapter 4

Unparameterized Pattern TSMs

In Chapter 3, we considered situations where the programmer needed to *construct* (a.k.a. *introduce*) a value. In this chapter, we consider situations where the programmer needs to *deconstruct* (a.k.a. *eliminate*) a value. In full-scale functional languages like ML and Haskell, values are deconstructed by *pattern matching* over their structure. For example, recall the recursive labeled sum type `Rx` defined in Figure 2.1. We can pattern match over a value, `r`, of type `Rx` using VerseML's **match** construct:

```
1 fun read_example_rx(r : Rx) : (string * Rx) option =>
2   match r with
3     Seq(Str(name), Seq(Str ": ", ssn)) => Some (name, ssn)
4   | _ => None
```

Match expressions consist of a *scrutinee*, here `r`, and a sequence of *rules* separated by vertical bars, `|`, in the concrete syntax. Each rule consists of a *pattern* and an expression called the corresponding *branch*, separated by a double arrow, `=>`, in the concrete syntax. When the match expression is evaluated, the value of the scrutinee is matched against each pattern sequentially. If the value matches, evaluation takes the corresponding branch. Variables in patterns match any value of the appropriate type. In the corresponding branch, the variable stands for that value. Variables can each appear only once in a pattern. For example, on Line 3, the pattern `Seq(Str(name), Seq(Str ": ", ssn))` matches values of the form `Seq(Str(e_1), Seq(Str ": ", e_2))`, where e_1 is a value of type `string` and e_2 is a value of type `Rx`. The variables `name` and `ssn` stand for the values of e_1 and e_2 , respectively, in `Some (name, ssn)`. On Line 4, the pattern `_` is the *wildcard pattern* – it matches any value of the appropriate type and binds no variables.

The behavior of the **match** construct when no pattern in the rule sequence matches a value is to raise an exception indicating *match failure*. It is possible to statically determine whether match failure is possible (i.e. whether there exist values of the scrutinee that are not matched by any pattern in the rule sequence). In the example above, our use of the wildcard pattern ensures that match failure cannot occur. A rule sequence that cannot lead to match failure is said to be *exhaustive*. Most compilers warn the programmer when a rule sequence is non-exhaustive.

It is also possible to statically decide when a rule is *redundant* relative to the preceding rules, i.e. when there does not exist a value matched by that rule but not matched by

any of the preceding rules. For example, if we add another rule at the end of the match expression above, it will be redundant because all values match the wildcard pattern. Again, most compilers warn the programmer when a rule is redundant.

Nested pattern matching generalizes the projection and case analysis operators (i.e. the *eliminators*) for products and sums (cf. `miniVerseUE` from the previous section) and decreases syntactic cost in situations where eliminators would need to be nested. There remains room for improvement, however, because complex patterns sometimes individually have high syntactic cost. In Sec. 2.2.1, we considered a hypothetical dialect of ML called ML+Rx that built in derived syntax both for constructing and pattern matching over values of the recursive labeled sum type Rx. In ML+Rx, we can express the example above at lower syntactic cost as follows:

```

1 fun read_example_rx(r : Rx) : (string * Rx) option =>
2   match r with
3     /@name: %ssn/ => Some (name, ssn)
4     | _ => None

```

Dialect formation is not a modular approach, for the reasons discussed in Chapter 1, so we seek language constructs that allow us to decrease the syntactic cost of expressing complex patterns to a similar degree.

Expression TSMs – introduced in Chapter 3 – can decrease the syntactic cost of constructing a value of a specified type. However, expressions are syntactically distinct from patterns, so we cannot simply apply an expression TSM to generate a pattern.¹ For this reason, we need to introduce a new (albeit closely related) construct – the **pattern TSM**. In this chapter, we consider only **unparameterized pattern TSMs** (upTSMs), i.e. pattern TSMs that generate patterns that match values of a single specified type, like Rx. In Chapter 5, we will consider both expression and pattern TSMs that specify type and module parameters (peTSMs and ppTSMs).

4.1 Pattern TSMs By Example

The organization of the remainder of this chapter mirrors that of Chapter 3. We begin in this section with a “tutorial-style” introduction to upTSMs in VerseML. In particular, we discuss an upTSM for patterns matching values of type Rx. In the next section, we specify a reduced formal system based on `miniVerseUE` called `miniVerseU` that makes the intuitions developed here mathematically precise.

4.1.1 Usage

The VerseML function `read_example_rx` defined at the beginning of this chapter can be concretely expressed at lower syntactic cost by applying a upTSM, `$rx`, as follows:

¹The fact that certain concrete expression and pattern forms overlap is immaterial to this fundamental distinction. There are many expression forms that the expansion generated by an expression TSM might use that have no corresponding pattern form, e.g. lambda abstraction.

```

1 fun read_example_rx(r : Rx) : (string * Rx) option =>
2   match r with
3     $rx /@name: %ssn/ => Some (name, ssn)
4     | _ => None

```

Like expression TSMs, pattern TSMs are applied to *generalized literal forms* (see Figure 3.1). Generalized literal forms are left unparsed when patterns are first parsed. During the subsequent *typed expansion* process, the pattern TSM parses the body of the literal form to generate a *candidate expansion*. The language validates the candidate expansion according to criteria that we will establish in Sec. 4.1.4. If validation succeeds, the language generates the final expansion (or more concisely, simply the expansion) of the pattern. The expansion of the unexpanded pattern `$rx /@name: %ssn/` from the example above is the following pattern:

```
Seq(Str(name), Seq(Str ":", ssn))
```

The checks for exhaustiveness and redundancy can be performed post-expansion in the usual way, so we do not need to consider them further here.

4.1.2 Definition

The definition of the pattern TSM `$rx` shown being applied in the example above has the following form:

```

syntax $rx at Rx for patterns {
  static fn(body : Body) : CEPat ParseResult =>
    (* regex pattern parser here *)
}

```

This definition first names the pattern TSM. Pattern TSM names, like expression TSM names, must begin with the dollar symbol (\$) to distinguish them from labels. Pattern TSM names and expression TSM names are tracked separately, i.e. an expression TSM and a pattern TSM can have the same name without conflict (as is the case here – the expression TSM described in Sec. 3.1.2 is also named `$rx`). The *sort qualifier for patterns* indicates that this is a pattern TSM definition, rather than an expression TSM definition (the sort qualifier **for expressions** can be written for expression TSMs, though when the sort qualifier is omitted this is the default). Because defining both an expression TSM and a pattern TSM with the same name at the same type is a common idiom, VerseML provides a primitive derived form for combining their definitions:

```

syntax $rx at Rx for expressions {
  static fn(body : Body) : CEEExp ParseResult =>
    (* regex expression parser here *)
} for patterns {
  static fn(body : Body) : CEPat ParseResult =>
    (* regex pattern parser here *)
}

```

Pattern TSMs, like expression TSMs, must specify a static *parse function*, delimited by curly braces in the concrete syntax. For a pattern TSM, the parse function must be of type `Body -> CEPat ParseResult`. The input type, `Body`, gives the parse function access to

```

type CEPat = Wild
            | (* ... *)
            | Spliced of IndexRange

```

Figure 4.1: Abbreviated definition of CEPat in the VerseML prelude.

the body of the provided literal form, and is defined as in Sec. 3.1.2 as a synonym for the type string. The output type, CEPat ParseResult, is the parameterized type constructor ParseResult, defined in Figure 3.2, applied to the type CEPat defined in Figure 4.1. So if parsing succeeds, the pattern TSM returns a value of the form Success e_{cand} where e_{cand} is a value of type CEPat that we call the *encoding of the candidate expansion*. If parsing fails, then the pattern TSM returns a value constructed by ParseError and equipped with an error message and error location.

The type CEPat is analagous to the types CEEp and CETyp defined in Figure 3.3. It encodes the abstract syntax of VerseML patterns (in Figure 4.1, some constructors are elided for concision), with the exception of variable patterns (for reasons explained in Sec. 4.1.5 below), and includes an additional constructor, Spliced, for referring to spliced subpatterns by their position within the parse stream, discussed next.

4.1.3 Splicing

Patterns that appear directly within the literal body of an unexpanded pattern are called *spliced subpatterns*. For example, the patterns name and ssn appear within the unexpanded pattern \$rx /@name: %ssn/. When the parse function determines that a subsequence of the literal body should be treated as a spliced subpattern (here, by recognizing the characters @ or % followed by a variable or parenthesized pattern), it can refer to it within the candidate expansion that it construct a reference to it for use within the candidate expansion it generates using the Spliced constructor of the CEPat type shown in Figure 4.1. The Spliced constructor requires a value of type IndexRange because spliced subpatterns are referred to indirectly by their position within the literal body. This prevents pattern TSMs from “forging” a spliced subpattern (i.e. claiming that some pattern is a spliced subpattern, even though it does not appear in the literal body).

The candidate expansion generated by the pattern TSM \$rx for the example above, if written in a hypothetical concrete syntax where references to spliced subpatterns are written spliced<startIdx, endIdx>, is:

```
Seq(Str(spliced<1, 4>), Seq(Str ":", spliced<8, 10>))
```

Here, spliced<1, 4> refers to the subpattern name by position, and spliced<8, 10> refers to the subpattern ssn by position.

4.1.4 Typing

The language validates candidate expansion before a final expansion is generated. One aspect of candidate expansion validation is checking the candidate expansion against

the type annotation specified by the pattern TSM, e.g. the type Rx in the example above.

4.1.5 Hygiene

In order to check that the candidate expansion is well-typed, the language must parse, type and expand the spliced subpatterns that the candidate expansion refers to (by their position within the literal body, cf. above). To maintain a useful binding discipline, i.e. to allow programmers to reason about variable binding without examining expansions directly, the validation process allows variables (e.g. `name` and `ssn` above) to occur only in spliced subpatterns (just as variables bound at the use site can only appear in spliced subexpressions when using TSMs). Indeed, there is no constructor for the type `CEPat` corresponding to a variable pattern. This protection against “hidden bindings” is beneficial because it leaves variable naming entirely up to the client of the pattern TSM. A pattern TSM cannot inadvertently shadow a binding at the application site.

4.1.6 Final Expansion

If validation succeeds, the semantics generates the *final expansion* of the pattern from the candidate expansion by replacing the references to spliced subpatterns with their final expansions. For example, the final expansion of `$rx /@name: %ssn/` is:

```
Seq(Str(name), Seq(Str " : ", ssn))
```

4.2 miniVerse_U

To make the intuitions developed in the previous section about pattern TSMs precise, we now introduce miniVerse_U, a small language with support for both unparameterized expression TSMs and unparameterized pattern TSMs.

4.2.1 Syntax of the Inner Core

The *inner core* of miniVerse_U consists of *types*, τ , *expanded expressions*, e , *expanded rules*, r , and *expanded patterns*, p . Their syntax is specified by the syntax chart in Figure 4.2. The inner core of miniVerse_U differs from that of miniVerse_{UE} only in that the case analysis operator has been replaced by the pattern matching operator², so we will gloss some definitions that are identical to those in Sec. 3.2. The new constructs are highlighted in gray. Our formulation of the semantics of pattern matching is adapted from Harper’s formulation in *Practical Foundations for Programming Languages, First Edition* [18].³

²We do not also remove the projection operator because it has lower syntactic cost than pattern matching when only a single field from a labeled tuple is needed.

³The chapter on pattern matching has, of this writing, been removed from the draft second edition of *PFPL*, but a copy of the first edition can be found online.

Sort		Operational Form	Stylized Form	Description
Typ	$\tau ::=$	t	t	variable
		$\text{parr}(\tau; \tau)$	$\tau \rightarrow \tau$	partial function
		$\text{all}(t.\tau)$	$\forall t.\tau$	polymorphic
		$\text{rec}(t.\tau)$	$\mu t.\tau$	recursive
		$\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tau_i\}_{i \in L} \rangle$	labeled product
		$\text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$	$[\{i \hookrightarrow \tau_i\}_{i \in L}]$	labeled sum
Exp	$e ::=$	x	x	variable
		$\text{lam}\{\tau\}(x.e)$	$\lambda x:\tau.e$	abstraction
		$\text{ap}(e; e)$	$e(e)$	application
		$\text{tlam}(t.e)$	$\Lambda t.e$	type abstraction
		$\text{tap}\{\tau\}(e)$	$e[\tau]$	type application
		$\text{fold}\{t.\tau\}(e)$	$\text{fold}(e)$	fold
		$\text{unfold}(e)$	$\text{unfold}(e)$	unfold
		$\text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})$	$\langle \{i \hookrightarrow e_i\}_{i \in L} \rangle$	labeled tuple
		$\text{pr}[\ell](e)$	$e \cdot \ell$	projection
		$\text{in}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(e)$	$\ell \cdot e$	injection
		$\text{match}[n]\{\tau\}(e; \{r_i\}_{1 \leq i \leq n})$	$\text{match } e \{r_i\}_{1 \leq i \leq n}$	match
ERule	$r ::=$	$\text{rule}[n]\{p\}(\{x_i\}_{1 \leq i \leq n}.e)$	$p \Rightarrow e$	rule
EPat	$p ::=$	x	x	variable pattern
		wildp	$-$	wildcard pattern
		$\text{tplp}[L](\{i \hookrightarrow p_i\}_{i \in L})$	$\langle \{i \hookrightarrow p_i\}_{i \in L} \rangle$	labeled tuple pattern
		$\text{inp}[\ell](p)$	$\ell \cdot p$	injection pattern

Figure 4.2: Syntax of types and expanded expressions, rules and patterns (collectively, expanded terms) in $\text{miniVerse}_{\text{U}}$. We adopt the metatheoretic conventions established for our specification of $\text{miniVerse}_{\text{UE}}$ in Sec. 3.2 without restating them, unless otherwise specified. We write $\{r_i\}_{1 \leq i \leq n}$ for sequences of $n \geq 0$ rule arguments and $\{x_i\}_{1 \leq i \leq n}.e$ for expressions binding the sequence of $n \geq 0$ variables $\{x_i\}_{1 \leq i \leq n}$. Variable patterns are not pattern variables, i.e. they do not stand for terms, but rather serve as references to the bindings in the rule that the pattern appears within. The semantics below will clarify this. Types and expanded terms are identified up to α -equivalence.

4.2.2 Statics of the Inner Core

The *statics of the inner core* is specified by judgements of the following form:

Judgement Form	Description
$\Delta \vdash \tau \text{ type}$	τ is a well-formed type assuming Δ
$\Delta \Gamma \vdash e : \tau$	e has type τ assuming Δ and Γ
$\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$	r takes values of type τ to values of type τ' assuming Δ and Γ
$\Omega \Vdash p : \tau$	p matches values of type τ and generates hypotheses Ω

The types of $\text{miniVerse}_{\text{U}}$ are exactly those of $\text{miniVerse}_{\text{UE}}$, described in Sec. 3.2, so the *type formation judgement*, $\Delta \vdash \tau \text{ type}$, is inductively defined by Rules (3.1).

The *typing judgement*, $\Delta \Gamma \vdash e : \tau$, assigns types to expressions and is inductively defined by Rules (4.1), which consist of:

- Rules defined identically to Rules (3.2a) through (3.2j). We will refer to these rules as Rules (4.1a) through (4.1j).
- The following rule for match expressions:

$$\frac{\Delta \Gamma \vdash e : \tau \quad \Delta \vdash \tau' \text{ type} \quad \{\Delta \Gamma \vdash r_i : \tau \Rightarrow \tau'\}_{1 \leq i \leq n}}{\Delta \Gamma \vdash \text{match}[n]\{\tau'\}(e; \{r_i\}_{1 \leq i \leq n}) : \tau'} \quad (4.1k)$$

The first premise of Rule (4.1k) assigns a type, τ , to the scrutinee, e . The second premise checks that the type of the expression as a whole, τ' , is well-formed.⁴ The third premise then ensures that each rule r_i , for $1 \leq i \leq n$, takes values of type τ to values of the type of the match expression as a whole, τ' . This is expressed by the *rule typing judgement*, $\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$, which is defined mutually with Rules (4.1) by the following rule:

$$\frac{\Omega \Vdash p : \tau \quad \text{dom}(\Omega) = \{x_i\}_{1 \leq i \leq n} \quad \Delta \Gamma \cup \Omega \vdash e : \tau'}{\Delta \Gamma \vdash \text{rule}[n]\{p\}(\{x_i\}_{1 \leq i \leq n}.e) : \tau \Rightarrow \tau'} \quad (4.2)$$

The premises of Rule (4.2) can be understood as follows, in order:

1. The first premise invokes the *pattern typing judgement*, $\Omega \Vdash p : \tau$, to check that the pattern, p , matches values of type τ , and to gather the typing hypotheses that the pattern generates in a *pattern typing context*, Ω . Pattern typing contexts, like typing contexts, Γ , are finite functions from variables to hypotheses of the form $x : \tau$. Algorithmically, however, one should consider the pattern typing context the “output” of the pattern typing judgement.

The pattern typing judgement is inductively defined by the following rules:

$$\frac{}{x : \tau \Vdash x : \tau} \quad (4.3a)$$

$$\frac{}{\emptyset \Vdash \text{wildp} : \tau} \quad (4.3b)$$

⁴The second premise of Rule (4.1k), and the type argument in the match form, are necessary to maintain regularity, defined below, but only because when $n = 0$, the type τ' is arbitrary. In all other cases, τ' can be determined by assigning types to the branch expressions.

$$\frac{\{\Omega_i \vdash p_i : \tau_i\}_{i \in L} \quad \{\{\text{dom}(\Omega_i) \cap \text{dom}(\Omega_j) = \emptyset\}_{j \in L \setminus i}\}_{i \in L}}{\cup_{i \in L} \Omega_i \vdash \text{tplp}[L](\{i \hookrightarrow p_i\}_{i \in L}) : \text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})} \quad (4.3c)$$

$$\frac{\Omega \vdash p : \tau}{\Omega \vdash \text{inp}[\ell](p) : \text{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)} \quad (4.3d)$$

Rule (4.3a) specifies that a variable pattern, x , can match values of any type, τ , and generates the hypothesis that x has the type τ .

Rule (4.3b) specifies that a wildcard pattern can also match values of any type, τ , but wildcard patterns generate no hypotheses.

Labeled tuple patterns, $\text{tplp}[L](\{i \hookrightarrow p_i\}_{i \in L})$, specify a subpattern p_i for each label $i \in L$. Rule (4.3c) specifies that a labeled tuple pattern of this form matches values of the labeled product type $\text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$. The first premise checks each subpattern p_i against the corresponding type τ_i , generating hypotheses Ω_i . The second premise ensures that no variables are multiply bound by checking that the domains of the generated pattern typing contexts Ω_i are mutually disjoint. The hypotheses generated in the conclusion of the rule are the union of the hypotheses generated by the subpatterns.

Injection patterns, $\text{inp}[\ell](p)$, match values of labeled sum types of the form $\text{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)$, i.e. labeled sum types that define a case for the label ℓ . Rule (4.3d) checks the subpattern p against the corresponding type τ , and passes through the assumptions that p generates.

2. The second premise of Rule (4.2) ensures that pattern typing of p has generated hypotheses for all of the variables that the branch expression, e , binds. This is merely a matter of “metatheoretic bookkeeping”. In the stylized form for rules, $p \Rightarrow e$, the variables bound in e are, implicitly, exactly those mentioned in p .
3. The final premise of Rule (4.2) extends the typing context, Γ , with the hypotheses generated by pattern typing, Ω , and checks the branch expression, e , against the branch type, τ' .

The rules above are syntax-directed, so we assume an inversion lemma for each rule as needed without stating it separately or proving it explicitly. The following standard lemmas also hold.

The Weakening Lemma establishes that extending the context with unnecessary hypotheses preserves well-formedness and typing.

Lemma 4.1 (Weakening). *All of the following hold:*

1. If $\Delta \vdash \tau$ type then $\Delta, t \text{ type} \vdash \tau$ type.
2. (a) If $\Delta \Gamma \vdash e : \tau$ then $\Delta, t \text{ type} \Gamma \vdash e : \tau$.
(b) If $\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$ then $\Delta, t \text{ type} \Gamma \vdash r : \tau \Rightarrow \tau'$.
3. (a) If $\Delta \Gamma \vdash e : \tau$ and $\Delta \vdash \tau''$ type then $\Delta \Gamma, x : \tau'' \vdash e : \tau$.
(b) If $\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$ and $\Delta \vdash \tau''$ type then $\Delta \Gamma, x : \tau'' \vdash r : \tau \Rightarrow \tau'$.

Proof Sketch.

1. By rule induction over Rules (3.1).

2. By mutual rule induction over Rules (4.1) and Rule (4.2).
3. By mutual rule induction over Rules (4.1) and Rule (4.2).

□

The pattern typing judgement is a *linear hypothetical judgement*, i.e. it does *not* obey weakening of the pattern typing context. This is to ensure that the pattern typing context captures exactly those hypotheses generated by a pattern, and no others.

We assume that renaming of bound variables, α -equivalence and substitution are defined as in *PFPL* [19], with the additional stipulation that the variables that are bound by the branch expression in an expanded rule are renamed together with those in the corresponding expanded pattern. The Substitution Lemma establishes that substitution of a well-formed type for a type variable, or an expanded expression of the appropriate type for an expanded expression variable, preserves well-formedness and typing.

Lemma 4.2 (Substitution). *All of the following hold:*

1. If $\Delta, t \text{ type} \vdash \tau \text{ type}$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta \vdash [\tau'/t]\tau \text{ type}$.
2. (a) If $\Delta, t \text{ type} \Gamma \vdash e : \tau$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$.
 (b) If $\Delta, t \text{ type} \Gamma \vdash r : \tau \Rightarrow \tau''$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]r : [\tau'/t]\tau \Rightarrow [\tau'/t]\tau''$.
3. (a) If $\Delta \Gamma, x : \tau' \vdash e : \tau$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma \vdash [e'/x]e : \tau$.
 (b) If $\Delta \Gamma, x : \tau' \vdash r : \tau \Rightarrow \tau''$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma \vdash [e'/x]r : \tau \Rightarrow \tau''$.

Proof Sketch.

1. By rule induction over Rules (3.1).
2. By mutual rule induction over Rules (4.1) and Rule (4.2).
3. By mutual rule induction over Rules (4.1) and Rule (4.2).

□

The Decomposition Lemma is the converse of the Substitution Lemma.

Lemma 4.3 (Decomposition). *All of the following hold:*

1. If $\Delta \vdash [\tau'/t]\tau \text{ type}$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta, t \text{ type} \vdash \tau \text{ type}$.
2. (a) If $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta, t \text{ type} \Gamma \vdash e : \tau$.
 (b) If $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]r : [\tau'/t]\tau \Rightarrow [\tau'/t]\tau''$ and $\Delta \vdash \tau' \text{ type}$ then $\Delta, t \text{ type} \Gamma \vdash r : \tau \Rightarrow \tau''$.
3. (a) If $\Delta \Gamma \vdash [e'/x]e : \tau$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma, x : \tau' \vdash e : \tau$.
 (b) If $\Delta \Gamma \vdash [e'/x]r : \tau \Rightarrow \tau''$ and $\Delta \Gamma \vdash e' : \tau'$ then $\Delta \Gamma, x : \tau' \vdash r : \tau \Rightarrow \tau''$.

Proof Sketch.

1. By rule induction over Rules (3.1) and case analysis over the definition of substitution. In all cases, the derivation of $\Delta \vdash [\tau'/t]\tau \text{ type}$ does not depend on the form of τ' .
2. By mutual rule induction over Rules (4.1) and Rule (4.2) and case analysis over the definition of substitution. In all cases, the derivation of $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]e : [\tau'/t]\tau$ or $\Delta [\tau'/t]\Gamma \vdash [\tau'/t]r : [\tau'/t]\tau \Rightarrow [\tau'/t]\tau''$ does not depend on the form of τ' .
3. By mutual rule induction over Rules (4.1) and Rule (4.2) and case analysis over the definition of substitution. In all cases, the derivation of $\Delta \Gamma \vdash [e'/x]e : \tau$ or

$\Delta \Gamma \vdash [e'/x]r : \tau \Rightarrow \tau''$ does not depend on the form of e' . □

The Pattern Regularity Lemma establishes that the hypotheses generated by checking a pattern against a well-formed type involve only well-formed types.

Lemma 4.4 (Pattern Regularity). *If $\Omega \Vdash p : \tau$ and $\Delta \vdash \tau$ type then $\Delta \vdash \tau_i$ type for each assumption $x_i : \tau_i$ in Ω .*

Proof. By rule induction over Rules (4.3).

Case (4.3a). We have:

- | | |
|-------------------------------|---------------|
| (1) $p = x$ | by assumption |
| (2) $\Omega = x : \tau$ | by assumption |
| (3) $\Delta \vdash \tau$ type | by assumption |

Case (4.3b). We have $\Omega = \emptyset$ by assumption, so the conclusion trivially holds.

Case (4.3c). We have:

- | | |
|---|--|
| (1) $p = \mathbf{tplp}[L](\{i \hookrightarrow p_i\}_{i \in L})$ | by assumption |
| (2) $\tau = \mathbf{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ | by assumption |
| (3) $\Omega_i \Vdash p_i : \tau_i$ for each $i \in L$ | by assumption |
| (4) $\Omega = \cup_{i \in L} \Omega_i$ | by assumption |
| (5) $\Delta \vdash \mathbf{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ type | by assumption |
| (6) $\Delta \vdash \tau_i$ type for each $i \in L$ | by Inversion of Rule (3.1e) on (5) |
| (7) $\Delta \vdash \tau_{ij}$ type for each $x_{ij} : \tau_{ij}$ in Ω_i , for each $i \in L$ | by IH on (3) and (6) for each $i \in L$ |
| (8) $\Delta \vdash \tau_{ij}$ type for each $x_{ij} : \tau_{ij}$ in $\cup_{i \in L} \Omega_i$ | by the definition of pattern context union and (7) |

Case (4.3d). We have:

- | | |
|--|------------------------------------|
| (1) $p = \mathbf{inp}[\ell](p')$ | by assumption |
| (2) $\tau = \mathbf{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau')$ | by assumption |
| (3) $\Delta \vdash \mathbf{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau')$ type | by assumption |
| (4) $\Omega \Vdash p' : \tau'$ | by assumption |
| (5) $\Delta \vdash \tau'$ type | by Inversion of Rule (3.1f) on (3) |
| (6) $\Delta \vdash \tau_i$ type for each assumption $x : \tau_i$ in Ω | by IH on (4) and (5) |

□

Finally, the Regularity Lemma establishes that the type assigned to an expression under a well-formed typing context is well-formed.

Lemma 4.5 (Regularity). *All of the following hold:*

1. *If $\Delta \Gamma \vdash e : \tau$ and $\Delta \vdash \tau_i$ type for each assumption $x_i : \tau_i$ in Γ then $\Delta \vdash \tau$ type.*

2. If $\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$ and $\Delta \vdash \tau$ type and $\Delta \vdash \tau_i$ type for each assumption $x_i : \tau_i$ in Γ then $\Delta \vdash \tau'$ type.

Proof Sketch. By mutual rule induction over Rules (4.1) and Rule (4.2), and Lemma 4.2 and Lemma 4.4. \square

4.2.3 Structural Dynamics

The *structural dynamics* of $\text{miniVerse}_{\mathcal{U}}$ is specified as a transition system, and is organized around judgements of the following form:

Judgement Form	Description
$e \mapsto e'$	e transitions to e'
$e \text{ val}$	e is a value
$e \text{ matchfail}$	e raises match failure

We also define auxiliary judgements for *iterated transition*, $e \mapsto^* e'$, and *evaluation*, $e \Downarrow e'$.

Definition 4.6 (Iterated Transition). *Iterated transition, $e \mapsto^* e'$, is the reflexive, transitive closure of the transition judgement, $e \mapsto e'$.*

Definition 4.7 (Evaluation). *$e \Downarrow e'$ iff $e \mapsto^* e'$ and $e' \text{ val}$.*

As in Sec. 3.2.3, our subsequent developments do not make mention of particular rules in the dynamics, nor do they make mention of judgements that are used only for defining the dynamics of the match operator, so we do not provide these details here. Instead, it suffices to state the following conditions.

The Canonical Forms condition characterizes well-typed values. Satisfying this condition requires an *eager* (i.e. *by-value*) formulation of the dynamics. This condition is identical to Condition 3.8.

Condition 4.8 (Canonical Forms). *If $\vdash e : \tau$ and $e \text{ val}$ then:*

1. If $\tau = \text{parr}(\tau_1; \tau_2)$ then $e = \text{lam}\{\tau_1\}(x.e')$ and $x : \tau_1 \vdash e' : \tau_2$.
2. If $\tau = \text{all}(t.\tau')$ then $e = \text{tlam}(t.e')$ and $t \text{ type} \vdash e' : \tau'$.
3. If $\tau = \text{rec}(t.\tau')$ then $e = \text{fold}\{t.\tau'\}(e')$ and $\vdash e' : [\text{rec}(t.\tau')/t]\tau'$ and $e' \text{ val}$.
4. If $\tau = \text{prod}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ then $e = \text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})$ and $\vdash e_i : \tau_i$ and $e_i \text{ val}$ for each $i \in L$.
5. If $\tau = \text{sum}[L](\{i \hookrightarrow \tau_i\}_{i \in L})$ then for some label set L' and label ℓ , we have that $L = L', \ell$ and $\tau = \text{sum}[L', \ell](\{i \hookrightarrow \tau_i\}_{i \in L'; \ell \hookrightarrow \tau_\ell})$ and $e = \text{in}[L', \ell][\ell]\{\{i \hookrightarrow \tau_i\}_{i \in L'; \ell \hookrightarrow \tau_\ell}\}(e')$ and $\vdash e' : \tau_\ell$ and $e' \text{ val}$.

The Preservation condition ensures that evaluation preserves typing.

Condition 4.9 (Preservation). *If $\vdash e : \tau$ and $e \mapsto e'$ then $\vdash e' : \tau$.*

The Progress condition ensures that evaluation of a well-typed expression preserves typing and cannot “get stuck”.

Condition 4.10 (Progress). *If $\vdash e : \tau$ then either $e \text{ val}$ or $e \text{ matchfail}$ or there exists an e' such that $e \mapsto e'$.*

The Preservation and Progress conditions together establish type safety.

Sort	Operational Form	Stylized Form	Description
UExp	$\hat{e} ::= x$	x	variable
	$\text{ulam}\{\tau\}(x.\hat{e})$	$\lambda x:\tau.\hat{e}$	abstraction
	$\text{uap}(\hat{e};\hat{e})$	$\hat{e}(\hat{e})$	application
	$\text{utlam}(t.\hat{e})$	$\Lambda t.\hat{e}$	type abstraction
	$\text{utap}\{\tau\}(\hat{e})$	$\hat{e}[\tau]$	type application
	$\text{ufold}\{t.\tau\}(\hat{e})$	$\text{fold}(\hat{e})$	fold
	$\text{uunfold}(\hat{e})$	$\text{unfold}(\hat{e})$	unfold
	$\text{utpl}[L](\{i \hookrightarrow \hat{e}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \hat{e}_i\}_{i \in L} \rangle$	labeled tuple
	$\text{upr}[\ell](\hat{e})$	$\hat{e} \cdot \ell$	projection
	$\text{uin}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(\hat{e})$	$\ell \cdot \hat{e}$	injection
	$\text{umatch}[n]\{\tau\}(\hat{e}; \{\hat{r}_i\}_{1 \leq i \leq n})$	$\text{match } \hat{e} \{ \hat{r}_i \}_{1 \leq i \leq n}$	match
	$\text{usyntaxue}\{e\}\{\tau\}(\hat{a}.\hat{e})$	syntax a at τ for expressions $\{e\}$ in \hat{e}	ueTSM definition
	$\text{uapuetism}[b][\hat{a}]$	$\hat{a} / b /$	ueTSM application
	$\text{usyntaxup}\{e\}\{\tau\}(\hat{a}.\hat{e})$	syntax a at τ for patterns $\{e\}$ in \hat{e}	upTSM definition
URule	$\hat{r} ::= \text{urule}[n]\{\hat{p}\}(\{x_i\}_{1 \leq i \leq n}.\hat{e})$	$\hat{p} \Rightarrow \hat{e}$	match rule
UPat	$\hat{p} ::= x$	x	variable pattern
	uwildp	$-$	wildcard pattern
	$\text{utplp}[L](\{i \hookrightarrow \hat{p}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \hat{p}_i\}_{i \in L} \rangle$	labeled tuple pattern
	$\text{uinp}[\ell](\hat{p})$	$\ell \cdot \hat{p}$	injection pattern
	$\text{uapuptism}[b][\hat{a}]$	$\hat{a} / b /$	upTSM application

Figure 4.3: Abstract syntax of unexpanded expressions, rules and patterns in $\text{miniVerse}_{\text{U}}$. Metavariable \hat{a} ranges over TSM names and b ranges over literal bodies. Literal bodies might contain unparsed terms, so variable renaming and substitution cannot be defined in the usual manner over unexpanded terms.

We do not define exhaustiveness and redundancy properties here, because these can be checked post-expansion and so are also not relevant to our subsequent developments (but see [18] for a formal account).

4.2.4 Syntax of the Outer Surface

Programs ultimately evaluate as expanded expressions, but programmers do not write expanded terms directly. Instead, the *outer surface* of $\text{miniVerse}_{\text{U}}$ consists of types, defined above, and *unexpanded expressions*, \hat{e} , *unexpanded rules*, \hat{r} , and *unexpanded patterns*, \hat{p} (collectively, *unexpanded terms*). The syntax of unexpanded terms is specified in Figure 4.3. Notice that each expanded term form corresponds to an unexpanded term form. We refer to these as the *shared forms*. In addition, four unexpanded term forms do not correspond to expanded term forms: the ueTSM definition form, the ueTSM application form, the upTSM definition form and the upTSM application form. The forms related to ueTSMs are highlighted in dark gray, and the forms related to upTSMs are highlighted

in light gray.

4.2.5 Typed Expansion

Unexpanded terms are typed and expanded according to the *typed expansion judgements*:

Judgement Form	Description
$\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{e} \rightsquigarrow e : \tau$	\hat{e} has expansion e and type τ under ueTSM context $\hat{\Sigma}$ and upTSM context Φ assuming Δ and Γ
$\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$	\hat{r} has expansion r and takes values of type τ to values of type τ' under TSM environments $\hat{\Sigma}$ and Φ assuming Δ and Γ
$\Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau$	\hat{p} has expansion p and type τ and generates hypotheses Ω under upTSM context Φ

The *typed expression expansion judgement*, $\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{e} \rightsquigarrow e : \tau$, and the *typed rule expansion judgement*, $\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$ are defined mutually inductively by Rules (4.4) and Rule (4.5), respectively, and the *typed pattern expansion judgement*, $\Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau$, is inductively defined by Rules (4.6) as follows.

Shared Forms Rules (4.4a) through (4.4k) define typed expansion of unexpanded expressions of shared form. The first three of these rules are shown below:

$$\frac{}{\Delta \Gamma, x : \tau \vdash_{\hat{\Sigma}; \Phi} x \rightsquigarrow x : \tau} \quad (4.4a)$$

$$\frac{\Delta \vdash \tau \text{ type} \quad \Delta \Gamma, x : \tau \vdash_{\hat{\Sigma}; \Phi} \hat{e} \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash_{\Sigma; \Phi} \text{ulam}\{\tau\}(x.\hat{e}) \rightsquigarrow \text{lam}\{\tau\}(x.e) : \text{parr}(\tau; \tau')} \quad (4.4b)$$

$$\frac{\Delta \Gamma \vdash_{\Sigma; \Phi} \hat{e}_1 \rightsquigarrow e_1 : \text{parr}(\tau; \tau') \quad \Delta \Gamma \vdash_{\Sigma; \Phi} \hat{e}_2 \rightsquigarrow e_2 : \tau}{\Delta \Gamma \vdash_{\Sigma; \Phi} \text{uap}(\hat{e}_1; \hat{e}_2) \rightsquigarrow \text{ap}(e_1; e_2) : \tau'} \quad (4.4c)$$

Observe that, in each of these rules, the unexpanded and expanded expression forms in the conclusion correspond, and the premises correspond to those of the typing rule for the expanded expression form, i.e. Rules (4.1a), (4.1b) and (4.1c), respectively. In particular, the type formation premises correspond directly, and the typed expansion premises correspond to the typing premises. The ueTSM context, $\hat{\Sigma}$, and upTSM context, Φ , pass opaquely through these rules.

Rule (4.4k), below, defines typed expansion of unexpanded match expressions and corresponds analogously to Rule (4.1k).

$$\frac{\Delta \Gamma \vdash_{\Sigma; \Phi} \hat{e} \rightsquigarrow e : \tau \quad \Delta \vdash \tau' \text{ type} \quad \{\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{r}_i \rightsquigarrow r_i : \tau \Rightarrow \tau'\}_{1 \leq i \leq n}}{\Delta \Gamma \vdash_{\Sigma; \Phi} \text{umatch}[n]\{\tau'\}(\hat{e}; \{\hat{r}_i\}_{1 \leq i \leq n}) \rightsquigarrow \text{match}[n]\{\tau'\}(e; \{r_i\}_{1 \leq i \leq n}) : \tau'} \quad (4.4k)$$

We can express this scheme more precisely with the following rule transformation. For each rule in Rules (4.1),

$$\frac{J_1 \quad \cdots \quad J_k}{J}$$

the corresponding typed expansion rule is

$$\frac{\mathcal{U}(J_1) \quad \cdots \quad \mathcal{U}(J_k)}{\mathcal{U}(J)}$$

where

$$\begin{aligned} \mathcal{U}(\Delta \vdash \tau \text{ type}) &= \Delta \vdash \tau \text{ type} \\ \mathcal{U}(\Gamma \Delta \vdash e : \tau) &= \Gamma \Delta \vdash_{\hat{\Sigma}; \Phi} \mathcal{U}(e) \rightsquigarrow e : \tau \\ \mathcal{U}(\Gamma \Delta \vdash r : \tau \Rightarrow \tau') &= \Gamma \Delta \vdash_{\hat{\Sigma}; \Phi} \mathcal{U}(r) \rightsquigarrow r : \tau \Rightarrow \tau' \\ \mathcal{U}(\{J_i\}_{i \in L}) &= \{\mathcal{U}(J_i)\}_{i \in L} \end{aligned}$$

and where $\mathcal{U}(e)$, when e is a metapattern of sort Exp, is a metapattern of sort UExp defined as follows:

- When e is of definite form, $\mathcal{U}(e)$ is defined as follows:

$$\begin{aligned} \mathcal{U}(x) &= x \\ \mathcal{U}(\text{lam}\{\tau\}(x.e)) &= \text{ulam}\{\tau\}(x.\mathcal{U}(e)) \\ \mathcal{U}(\text{ap}(e_1; e_2)) &= \text{uap}(\mathcal{U}(e_1); \mathcal{U}(e_2)) \\ \mathcal{U}(\text{tlam}(t.e)) &= \text{utlam}(t.\mathcal{U}(e)) \\ \mathcal{U}(\text{tap}\{\tau\}(e)) &= \text{utap}\{\tau\}(\mathcal{U}(e)) \\ \mathcal{U}(\text{fold}\{t.\tau\}(e)) &= \text{ufold}\{t.\tau\}(e) \\ \mathcal{U}(\text{unfold}(e)) &= \text{uunfold}(\mathcal{U}(e)) \\ \mathcal{U}(\text{tpl}[L](\{i \hookrightarrow e_i\}_{i \in L})) &= \text{utpl}[L](\{i \hookrightarrow \mathcal{U}(e_i)\}_{i \in L}) \\ \mathcal{U}(\text{in}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(e)) &= \text{uin}[L][\ell](\{i \hookrightarrow \tau_i\}_{i \in L})(\mathcal{U}(e)) \\ \mathcal{U}(\text{match}[n]\{\tau\}(e; \{r_i\}_{1 \leq i \leq n})) &= \text{umatch}[n]\{\tau\}(\mathcal{U}(e); \{\mathcal{U}(r_i)\}_{1 \leq i \leq n}) \end{aligned}$$

- When e is of indefinite form, $\mathcal{U}(e)$ is a uniquely corresponding metapattern of indefinite form.

and where $\mathcal{U}(r)$, when r is a metapattern of sort ERule of indefinite form, is a uniquely corresponding metapattern of sort URule of indefinite form.

It is instructive to use this rule transformation to generate Rules (4.4a) through (4.4c) and Rule (4.4k) above. We omit the remaining rules generated by this transformation, i.e. Rules (4.4d) through (4.4j).

The typed rule expansion judgement is defined by Rule (4.5), below.

$$\frac{\Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau \quad \text{dom}(\Omega) = \{x_i\}_{1 \leq i \leq n} \quad \Delta \Gamma \cup \Omega \vdash_{\hat{\Sigma}; \Phi} \hat{e} \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \text{urule}[n]\{\hat{p}\}(\{x_i\}_{1 \leq i \leq n}.\hat{e}) \rightsquigarrow \text{rule}[n]\{p\}(\{x_i\}_{1 \leq i \leq n}.e) : \tau \Rightarrow \tau'} \quad (4.5)$$

As in the typed expression expansion judgements, the unexpanded and expanded forms in the conclusion of the rule above correspond. The premises correspond to those of the rule typing rule, i.e. Rule (4.2). In particular, the typed pattern expansion premise above

corresponds to the pattern typing premise of Rule (4.2), the second premise corresponds directly, and the typed expression expansion premise in the rule above corresponds to the typing premise of Rule (4.2).

The typed pattern expansion judgement for patterns of shared form is defined by the following rules.

$$\frac{}{x : \tau \vdash_{\Phi} x \rightsquigarrow x : \tau} \quad (4.6a)$$

$$\frac{}{\emptyset \vdash_{\Phi} \text{uwildp} \rightsquigarrow \text{wildp} : \tau} \quad (4.6b)$$

$$\frac{\{\Omega_i \vdash_{\Phi} \hat{p}_i \rightsquigarrow p_i : \tau_i\}_{i \in L} \quad \{\{\text{dom}(\Omega_i) \cap \text{dom}(\Omega_j) = \emptyset\}_{j \in L \setminus i}\}_{i \in L}}{\left(\frac{\bigcup_{i \in L} \Omega_i \vdash_{\Phi} \text{utplp}[L](\{i \hookrightarrow \hat{p}_i\}_{i \in L})}{\rightsquigarrow} \right)} \quad (4.6c)$$

$$\frac{\Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau}{\Omega \vdash_{\Phi} \text{uinp}[\ell](\hat{p}) \rightsquigarrow \text{inp}[\ell](p) : \text{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)} \quad (4.6d)$$

Again, the unexpanded and expanded pattern forms in the conclusion correspond and the premises correspond to those of the corresponding pattern typing rule, i.e. Rules (4.3a) through (4.3d), respectively. The upTSM context, Φ , passes through these rules opaquely.

ueTSM Definition and Application Rules (4.4l) and (4.4m) define typed expansion of ueTSM definitions and ueTSM application, respectively.

$$\frac{\Delta \vdash \tau \text{ type} \quad \emptyset \emptyset \vdash e_{\text{parse}} : \text{parr}(\text{Body}; \text{ParseResultExp}) \quad \Delta \Gamma \vdash_{\hat{\Sigma}, \hat{a} \hookrightarrow \text{uetSM}(\tau; e_{\text{parse}}); \Phi} \hat{e} \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash_{\Sigma; \Phi} \text{syntax } \hat{a} \text{ at } \tau \{e_{\text{parse}}\} \text{ in } \hat{e} \rightsquigarrow e : \tau'} \quad (4.4l)$$

$$\frac{b \downarrow e_{\text{body}} \quad e_{\text{parse}}(e_{\text{body}}) \Downarrow \text{Success} \cdot e_{\text{cand}} \quad e_{\text{cand}} \uparrow_{\text{CEExp}} \hat{e} \quad \emptyset \emptyset \vdash \Delta; \Gamma; \hat{\Sigma}, \hat{a} \hookrightarrow \text{uetSM}(\tau; e_{\text{parse}}); \Phi; b \hat{e} \rightsquigarrow e : \tau}{\Delta \Gamma \vdash_{\hat{\Sigma}, \hat{a} \hookrightarrow \text{uetSM}(\tau; e_{\text{parse}}); \Phi} \hat{a} / b / \rightsquigarrow e : \tau} \quad (4.4m)$$

These rules are nearly identical to Rules (3.4l) and (3.4m), respectively, differing only in that the upTSM context, Φ , passes through them opaquely. The premises of these rules, and the following auxiliary definitions and conditions, can be understood as described in Sec. 3.2.6 and 3.2.7, respectively.

The type `ParseResultExp` is defined as follows:

$$\text{ParseResultExp} \triangleq [\text{Success} \hookrightarrow \text{CEExp}, \text{ParseError} \hookrightarrow \langle \rangle]$$

The *body encoding judgement* $b \downarrow e_{\text{body}}$ specifies a mapping from the literal body, b , to an expanded value, e_{body} , of type `Body`. An inverse mapping is specified by the *body*

decoding judgement $e_{\text{body}} \uparrow b$.

Judgement Form	Description
$b \downarrow e$	b has encoding e
$e \uparrow b$	e has decoding b

The following condition establishes an isomorphism between literal bodies and values of type `Body`.

Condition 4.11 (Body Isomorphism). *All of the following hold:*

1. For every literal body b , we have that $b \downarrow e_{\text{body}}$ and $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$.
2. If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ then $e_{\text{body}} \uparrow b$ for some b .
3. If $b \downarrow e_{\text{body}}$ then $e_{\text{body}} \uparrow b$.
4. If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ and $e_{\text{body}} \uparrow b$ then $b \downarrow e_{\text{body}}$.
5. If $b \downarrow e_{\text{body}}$ and $b \downarrow e'_{\text{body}}$ then $e_{\text{body}} = e'_{\text{body}}$.
6. If $\vdash e_{\text{body}} : \text{Body}$ and $e_{\text{body}} \text{ val}$ and $e_{\text{body}} \uparrow b$ and $e_{\text{body}} \uparrow b'$ then $b = b'$.

The candidate expansion expression decoding judgement, $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}$, decodes e_{cand} to produce a candidate expansion expression, \grave{e} (pronounced “grave e ”). The inverse mapping is specified by the judgement $\grave{e} \downarrow_{\text{CEExp}} e_{\text{cand}}$.

Judgement Form	Description
$\grave{e} \downarrow_{\text{CEExp}} e$	\grave{e} has encoding e
$e \uparrow_{\text{CEExp}} \grave{e}$	e has decoding \grave{e}

The syntax of candidate expansion terms is defined in Figure 4.4, and described in Sec. 4.2.8 below. The follow condition establishes an isomorphism between values of type `CEExp` and candidate expansion expressions.

Condition 4.12 (Candidate Expansion Expression Isomorphism). *All of the following hold:*

1. If $\vdash e_{\text{cand}} : \text{CEExp}$ and $e_{\text{cand}} \text{ val}$ then $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}$ for some \grave{e} .
2. For every \grave{e} , we have $\grave{e} \downarrow_{\text{CEExp}} e_{\text{cand}}$ such that $\vdash e_{\text{cand}} : \text{CEExp}$ and $e_{\text{cand}} \text{ val}$.
3. If $\vdash e_{\text{cand}} : \text{CEExp}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}$ then $\grave{e} \downarrow_{\text{CEExp}} e_{\text{cand}}$.
4. If $\grave{e} \downarrow_{\text{CEExp}} e_{\text{cand}}$ then $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}$.
5. If $\vdash e_{\text{cand}} : \text{CEExp}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}$ and $e_{\text{cand}} \uparrow_{\text{CEExp}} \grave{e}'$ then $\grave{e} = \grave{e}'$.
6. If $\grave{e} \downarrow_{\text{CEExp}} e_{\text{cand}}$ and $\grave{e} \downarrow_{\text{CEExp}} e'_{\text{cand}}$ then $e_{\text{cand}} = e'_{\text{cand}}$.

ueTSM contexts, $\hat{\Sigma}$, are finite functions from TSM names, \hat{a} , to ueTSM definitions, $\text{uetSM}(\tau; e_{\text{parse}})$, where τ is the ueTSM’s type annotation and e_{parse} is its parse function. The ueTSM context formation judgement, $\Delta \vdash \hat{\Sigma}$ ueTSMs, ensures that the type annotations in $\hat{\Sigma}$ are well-formed assuming Δ , and that the parse functions in $\hat{\Sigma}$ are of type $\text{parr}(\text{Body}; \text{ParseResultExp})$.

Judgement Form	Description
$\Delta \vdash \hat{\Sigma}$ ueTSMs	$\hat{\Sigma}$ is well-formed assuming Δ

This judgement is inductively defined by the following rules:

$$\frac{}{\Delta \vdash \emptyset \text{ ueTSMs}} \quad (4.7a)$$

$$\frac{\Delta \vdash \hat{\Sigma} \text{ ueTSMs} \quad \Delta \vdash \tau \text{ type} \quad \emptyset \emptyset \vdash e_{\text{parse}} : \text{parr}(\text{Body}; \text{ParseResultExp})}{\Delta \vdash \hat{\Sigma}, \hat{a} \hookrightarrow \text{uetism}(\tau; e_{\text{parse}}) \text{ ueTSMs}} \quad (4.7b)$$

upTSM Definition and Application Rules (4.4n) and (4.6e) define upTSM definition and application, and are defined in the next two subsections, respectively.

4.2.6 upTSM Definition

The *upTSM definition form*:

syntax \hat{a} at τ for patterns $\{e_{\text{parse}}\}$ in \hat{e}

allows the programmer to introduce a upTSM named \hat{a} at type τ with parse function e_{parse} into the upTSM context of \hat{e} . The operational form corresponding to this stylized form is $\text{usyntaxup}\{e_{\text{parse}}\}\{\tau\}(\hat{a}.\hat{e})$. Rule (4.4n), defines typed expansion of upTSM definitions (for clarity, we use the stylized form in the conclusion of the rule):

$$\frac{\Delta \vdash \tau \text{ type} \quad \emptyset \emptyset \vdash e_{\text{parse}} : \text{parr}(\text{Body}; \text{ParseResultPat}) \quad \Delta \Gamma \vdash_{\hat{\Sigma}; \Phi, \hat{a} \hookrightarrow \text{uptsm}(\tau; e_{\text{parse}})} \hat{e} \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \text{syntax } \hat{a} \text{ at } \tau \text{ for patterns } \{e_{\text{parse}}\} \text{ in } \hat{e} \rightsquigarrow e : \tau'} \quad (4.4n)$$

This rule is similar to Rule (4.4l), which governs ueTSM definitions. Its premises can be understood as follows, in order:

1. The first premise ensures that the type annotation is well-formed.
2. The second premise checks that the parse function, e_{parse} , is of type

$\text{parr}(\text{Body}; \text{ParseResultPat})$

Parse functions are applied statically (i.e. during typed expansion), as we will discuss when describing ueTSM application below, and evaluation is defined only for closed expanded expressions, so the parse function must be closed.

The type abbreviated Body is characterized above.

ParseResultPat abbreviates a labeled sum type that distinguishes successful parses from parse errors:

$$\text{ParseResultPat} \triangleq [\text{Success} \hookrightarrow \text{CEPat}, \text{ParseError} \hookrightarrow \langle \rangle]$$

The type abbreviated CEPat classifies encodings of *candidate expansion patterns* (or *ce-patterns*), \hat{p} (pronounced “grave p ”). The syntax of ce-patterns will be described in Sec. 4.2.8. The mapping from ce-patterns to values of type CEPat is defined by the *ce-pattern encoding judgement*, $\hat{p} \downarrow_{\text{CEPat}} e$. The inverse mapping is defined by the *ce-pattern decoding judgement*, $e \uparrow_{\text{CEPat}} \hat{p}$.

Judgement Form	Description
$\hat{p} \downarrow_{\text{CEPat}} e$	\hat{p} has encoding e
$e \uparrow_{\text{CEPat}} \hat{p}$	e has decoding \hat{p}

Again, rather than picking a particular definition of CEPat and defining the judgements above inductively against it, we only state the following condition, which establishes an isomorphism between values of type CEPat and ce-patterns.

Condition 4.13 (Candidate Expansion Pattern Isomorphism). *All of the following must hold:*

- (a) If $\vdash e_{\text{cand}} : \text{CEPat}$ and $e_{\text{cand}} \text{ val}$ then $e_{\text{cand}} \uparrow_{\text{CEPat}} \hat{p}$ for some \hat{p} .
 - (b) For every \hat{p} , we have $\hat{p} \downarrow_{\text{CEPat}} e_{\text{cand}}$ such that $\vdash e_{\text{cand}} : \text{CEPat}$ and $e_{\text{cand}} \text{ val}$.
 - (c) If $\vdash e_{\text{cand}} : \text{CEPat}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEPat}} \hat{p}$ then $\hat{p} \downarrow_{\text{CEPat}} e_{\text{cand}}$.
 - (d) If $\hat{p} \downarrow_{\text{CEPat}} e_{\text{cand}}$ then $e_{\text{cand}} \uparrow_{\text{CEPat}} \hat{p}$.
 - (e) If $\vdash e_{\text{cand}} : \text{CEPat}$ and $e_{\text{cand}} \text{ val}$ and $e_{\text{cand}} \uparrow_{\text{CEPat}} \hat{p}$ and $e_{\text{cand}} \uparrow_{\text{CEPat}} \hat{p}'$ then $\hat{p} = \hat{p}'$.
 - (f) If $\hat{p} \downarrow_{\text{CEPat}} e_{\text{cand}}$ and $\hat{p} \downarrow_{\text{CEPat}} e'_{\text{cand}}$ then $e_{\text{cand}} = e'_{\text{cand}}$.
3. The final premise of Rule (4.4n) extends the upTSM context with the newly determined upTSM definition, and proceeds to assign a type, τ' , and expansion, e , to \hat{e} . The conclusion of Rule (4.4n) assigns this type and expansion to the ueTSM definition as a whole.

upTSM contexts, Φ , are finite functions from TSM names, \hat{a} , to upTSM definitions, $\text{uptsm}(\tau; e_{\text{parse}})$, where τ is the upTSM's type annotation and e_{parse} is the upTSM's parse function. The upTSM context formation judgement, $\Delta \vdash \Phi \text{ ok}$, ensures that the type annotations in Φ are well-formed assuming Δ and the parse functions in Φ are of type $\text{parr}(\text{Body}; \text{ParseResultPat})$.

Judgement Form	Description
$\Delta \vdash \Phi \text{ ok}$	upTSM context Φ is well-formed assuming Δ

This judgement is inductively defined by the following rules:

$$\frac{}{\Delta \vdash \emptyset \text{ ok}} \quad (4.8a)$$

$$\frac{\Delta \vdash \Phi \text{ ok} \quad \Delta \vdash \tau \text{ type} \quad \emptyset \emptyset \vdash e_{\text{parse}} : \text{parr}(\text{Body}; \text{ParseResultPat})}{\Delta \vdash \hat{\Sigma}, \hat{a} \hookrightarrow \text{uptsm}(\tau; e_{\text{parse}}) \text{ ok}} \quad (4.8b)$$

4.2.7 upTSM Application

The stylized unexpanded pattern form for applying a upTSM named \hat{a} to a literal form with literal body b is:

$$\hat{a} / b /$$

This stylized form is identical to the stylized form for ueTSM application, differing in that appears within the syntax of unexpanded patterns, \hat{p} , rather than unexpanded expressions, \hat{e} . The corresponding operational form is $\text{uapuptsm}[b][\hat{a}]$.

Rule (4.6e), below, governs upTSM application.

$$\frac{
 \begin{array}{c}
 b \downarrow e_{\text{body}} \quad e_{\text{parse}}(e_{\text{body}}) \Downarrow \text{Success} \cdot e_{\text{cand}} \quad e_{\text{cand}} \uparrow_{\text{CEPat}} \dot{p} \\
 \vdash \Omega; \Phi, \hat{a} \hookrightarrow \text{uptsm}(\tau; e_{\text{parse}}); b \quad \dot{p} \rightsquigarrow p : \tau
 \end{array}
 }{
 \Omega \vdash \Phi, \hat{a} \hookrightarrow \text{uptsm}(\tau; e_{\text{parse}}) \quad \text{uapuptsm}[b][\hat{a}] \rightsquigarrow p : \tau
 } \quad (4.6e)$$

This rule is similar to Rule (4.4m), which governs ueTSM application. Its premises can be understood as follows, in order:

1. The first premise determines the encoding of the literal body, e_{body} (see above).
2. The second premise applies the parse function e_{parse} to e_{body} . If parsing succeeds, i.e. a value of the (stylized) form $\text{Success} \cdot e_{\text{cand}}$ results from evaluation, then e_{cand} will be a value of type CEPat (assuming a well-formed upTSM context, by transitive application of Assumption 4.9). We call e_{cand} the *encoding of the candidate expansion*.
3. The third premise decodes the encoding of the candidate expansion to produce *candidate expansion*, \dot{p} (see above).
4. The final premise of Rule (4.6e) *validates* the candidate expansion and simultaneously generates its final expansion, p , and its pattern typing context, Ω . This is the topic of Sec. 4.2.9.

4.2.8 Syntax of Candidate Expansions

Figure 4.4 defines the syntax of candidate expansion types (or *ce-types*), τ , candidate expansion expressions (or *ce-expressions*), e , candidate expansion rules (or *ce-rules*), \dot{r} , and candidate expansion patterns (or *ce-patterns*), \dot{p} . The syntax of ce-types is identical to that given in Figure 3.6, which was described in Sec. 3.2.8.

Observe that for each expanded term form, except for the form for variable patterns, there is a corresponding ce-term form. We refer to these as the *shared forms*. There are two other ce-term forms: a ce-expression form for *references to spliced unexpanded expressions*, $\text{cespliced}[m;n]$, highlighted in dark gray, and a ce-pattern form for *references to spliced unexpanded patterns*, $\text{cesplicedp}[m;n]$, highlighted in light gray.

Sort	Operational Form	Stylized Form	Description
CETyp $\tilde{\tau} ::=$	t	t	variable
	$\text{ceparr}(\tilde{\tau}; \tilde{\tau})$	$\tilde{\tau} \rightarrow \tilde{\tau}$	partial function
	$\text{ceall}(t.\tilde{\tau})$	$\forall t.\tilde{\tau}$	polymorphic
	$\text{cerec}(t.\tilde{\tau})$	$\mu t.\tilde{\tau}$	recursive
	$\text{ceprod}[L](\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tilde{\tau}_i\}_{i \in L} \rangle$	labeled product
	$\text{cesum}[L](\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L})$	$[\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L}]$	labeled sum
	$\text{cesplicedt}[m; n]$	$\text{spliced}\langle m, n \rangle$	spliced
CEExp $\tilde{e} ::=$	x	x	variable
	$\text{celam}\{\tilde{\tau}\}(x.\tilde{e})$	$\lambda x:\tilde{\tau}.\tilde{e}$	abstraction
	$\text{ceap}(\tilde{e}; \tilde{e})$	$\tilde{e}(\tilde{e})$	application
	$\text{cetlam}(t.\tilde{e})$	$\Lambda t.\tilde{e}$	type abstraction
	$\text{cetap}\{\tilde{\tau}\}(\tilde{e})$	$\tilde{e}[\tilde{\tau}]$	type application
	$\text{cefold}\{t.\tilde{\tau}\}(\tilde{e})$	$\text{fold}(\tilde{e})$	fold
	$\text{ceunfold}(\tilde{e})$	$\text{unfold}(\tilde{e})$	unfold
	$\text{cetpl}[L](\{i \hookrightarrow \tilde{e}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tilde{e}_i\}_{i \in L} \rangle$	labeled tuple
	$\text{cepr}[\ell](\tilde{e})$	$\tilde{e} \cdot \ell$	projection
	$\text{cein}[L][\ell](\{i \hookrightarrow \tilde{\tau}_i\}_{i \in L})(\tilde{e})$	$\ell \cdot \tilde{e}$	injection
	$\text{cematch}[n](\{\tau\}(\tilde{e}; \{\tilde{r}_i\}_{1 \leq i \leq n}))$	$\text{match } \tilde{e} \{ \tilde{r}_i \}_{1 \leq i \leq n}$	match
	$\text{cesplicede}[m; n]$	$\text{spliced}\langle m, n \rangle$	spliced
CERule $\tilde{r} ::=$	$\text{cerule}[n](\{p\}(\{x_i\}_{1 \leq i \leq n}.\tilde{e}))$	$p \Rightarrow \tilde{e}$	rule
CEPat $\tilde{p} ::=$	cewildp	$-$	wildcard pattern
	$\text{cetplp}[L](\{i \hookrightarrow \tilde{p}_i\}_{i \in L})$	$\langle \{i \hookrightarrow \tilde{p}_i\}_{i \in L} \rangle$	labeled tuple pattern
	$\text{ceinp}[\ell](\tilde{p})$	$\ell \cdot \tilde{p}$	injection pattern
	$\text{cesplicedp}[m; n]$	$\text{spliced}\langle m, n \rangle$	spliced

Figure 4.4: Abstract syntax of candidate expansion types and candidate expansion expressions, rules and patterns (collectively, candidate expansion terms) in miniVerse_{UE}. Candidate expansion types and terms are identified up to α -equivalence.

4.2.9 Candidate Expansion Validation

The *candidate expansion validation judgements* validate ce-types and ce-terms and simultaneously generate their final expansions.

Judgement Form	Description
$\Delta \vdash^{\mathbb{T}} \hat{\tau} \rightsquigarrow \tau \text{ type}$	$\hat{\tau}$ is well-formed and has expansion τ assuming Δ and type splicing scene \mathbb{T}
$\Delta \Gamma \vdash^{\mathbb{E}} \hat{e} \rightsquigarrow e : \tau$	\hat{e} has expansion e and type τ assuming Δ and Γ and expression splicing scene \mathbb{E}
$\Delta \Gamma \vdash^{\mathbb{E}} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$	\hat{r} has expansion r and takes values of type τ to values of type τ' assuming Δ and Γ and expression splicing scene \mathbb{E}
$\vdash^{\Omega; \mathbb{P}} \hat{p} \rightsquigarrow p : \tau$	\hat{p} expands to p and matches values of type τ generating assumptions Ω assuming pattern splicing scene \mathbb{P}

Expression splicing scenes, \mathbb{E} , are of the form $\Delta; \Gamma; \hat{\Sigma}; \Phi; b$, *type splicing scenes*, \mathbb{T} , are of the form $\Delta; b$, and *pattern splicing scenes*, \mathbb{P} , are of the form $\Phi; b$. Their purpose is to “remember”, during candidate expansion validation, the contexts, TSM environments and literal bodies from the TSM application site (cf. Rules (4.4m) and (4.6e)), because these are necessary to validate references to spliced types and terms. We write $\text{ts}(\mathbb{E})$ for the type splicing scene constructed by dropping the typing context and TSM environments from \mathbb{E} :

$$\text{ts}(\Delta; \Gamma; \hat{\Sigma}; \Phi; b) = \Delta; b$$

Candidate Expansion Type Validation

The *candidate type validation judgement*, $\Delta \vdash^{\mathbb{T}} \hat{\tau} \rightsquigarrow \tau \text{ type}$, is inductively defined by Rules (3.5), which were defined in Sec. 3.2.9.

Candidate Expansion Expression and Rule Validation

The *ce-expression validation judgement*, $\Delta \Gamma \vdash^{\mathbb{E}} \hat{e} \rightsquigarrow e : \tau$, and the *ce-rule validation judgement*, $\Delta \Gamma \vdash^{\mathbb{E}} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$, are defined mutually inductively with Rules (4.4) and Rule (4.5) by Rules (4.8) and Rule (4.9), respectively, as follows.

Rules (4.8) define ce-expression validation and consist of the following rules:

- Rules defined identically to Rules (3.6a) through (3.6j). We will refer to these as Rules (4.8a) through (4.8j).
- The following rule for match ce-expressions:

$$\frac{\Delta \Gamma \vdash^{\mathbb{E}} \hat{e} \rightsquigarrow e : \tau \quad \Delta \vdash^{\text{ts}(\mathbb{E})} \hat{\tau}' \rightsquigarrow \tau' \text{ type} \quad \{\Delta \Gamma \vdash^{\mathbb{E}} \hat{r}_i \rightsquigarrow r_i : \tau \Rightarrow \tau'\}_{1 \leq i \leq n}}{\Delta \Gamma \vdash^{\mathbb{E}} \text{cmatch}[n]\{\hat{\tau}'\}(\hat{e}; \{\hat{r}_i\}_{1 \leq i \leq n}) \rightsquigarrow \text{match}[n]\{\tau'\}(e; \{r_i\}_{1 \leq i \leq n}) : \tau'} \quad (4.8k)$$

- The following rule for references to spliced unexpanded expressions, which can be understood as described in Sec. 3.2.9.

$$\frac{\Delta_{\text{app}} \Gamma_{\text{app}} \vdash_{\hat{\Sigma}; \Phi_S} \hat{e} \rightsquigarrow e : \tau \quad \Delta \cap \Delta_{\text{app}} = \emptyset \quad \text{dom}(\Gamma) \cap \text{dom}(\Gamma_{\text{app}}) = \emptyset}{\Delta \Gamma \vdash_{\Delta_{\text{app}}; \Gamma_{\text{app}}; \hat{\Sigma}; \Phi_S; b} \text{cesplicede}[m; n] \rightsquigarrow e : \tau} \quad (4.8l)$$

Rule (4.9) defines ce-rule validation and is defined as follows:

$$\frac{\Omega \Vdash p : \tau \quad \text{dom}(\Omega) = \{x_i\}_{1 \leq i \leq n} \quad \Delta \Gamma \cup \Omega \vdash^{\mathbb{E}} \hat{e} \rightsquigarrow e : \tau'}{\Delta \Gamma \vdash^{\mathbb{E}} \text{cerule}[n]\{p\}(\{x_i\}_{1 \leq i \leq n}. \hat{e}) \rightsquigarrow \text{rule}[n]\{p\}(\{x_i\}_{1 \leq i \leq n}. e) : \tau \Rightarrow \tau'} \quad (4.9)$$

Notice that expanded patterns, p , not ce-patterns, \hat{p} , appear in ce-rules. This is because ce-expressions are generated only by ueTSMs. It would not be sensible for a ueTSM to extract a spliced subpattern from a literal body.

Candidate Expansion Pattern Validation

upTSMs generate candidate expansions of ce-pattern form, as described in Sec. 4.2.7. The *ce-pattern validation judgement*, $\vdash^{\Omega; \mathbb{P}} \hat{p} \rightsquigarrow p : \tau$, which appears as the final premise of Rule (4.4m), validates ce-patterns by checking that the pattern matches values of type τ , and simultaneously generates the final expansion, p , and the hypotheses Ω . Hypotheses can be generated only by spliced subpatterns, so there is no ce-pattern form corresponding to variable patterns (this is also why Ω does not appear to the left of the turnstile in the judgement form). The pattern splicing scene, \mathbb{P} , is used to “remember” the upTSM context and literal body from the upTSM application site.

The ce-pattern validation judgement is defined mutually inductively with Rules (4.6) by the following rules.

$$\overline{\vdash^{\emptyset; \mathbb{P}} \text{cewildp} \rightsquigarrow \text{wildp} : \tau} \quad (4.10a)$$

$$\frac{\{\vdash^{\Omega_i; \mathbb{P}} \hat{p}_i \rightsquigarrow p_i : \tau_i\}_{i \in L} \quad \{\{\text{dom}(\Omega_i) \cap \text{dom}(\Omega_j) = \emptyset\}_{j \in L \setminus i}\}_{i \in L}}{\left(\frac{\vdash^{\cup_{i \in L} \Omega_i; \mathbb{P}} \text{cetplp}[L](\{i \hookrightarrow \hat{p}_i\}_{i \in L})}{\rightsquigarrow} \right)} \quad (4.10b)$$

$$\frac{\vdash^{\Omega; \mathbb{P}} \hat{p} \rightsquigarrow p : \tau}{\vdash^{\Omega; \mathbb{P}} \text{ceinp}[\ell](\hat{p}) \rightsquigarrow \text{inp}[\ell](p) : \text{sum}[L, \ell](\{i \hookrightarrow \tau_i\}_{i \in L}; \ell \hookrightarrow \tau)} \quad (4.10c)$$

$$\frac{\text{parseUPat}(\text{subseq}(b; m; n)) = \hat{p} \quad \Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau}{\vdash^{\Omega; \Phi; b} \text{cesplicedp}[m; n] \rightsquigarrow p : \tau} \quad (4.10d)$$

Rules (4.10a) through (4.10c) handle ce-patterns of shared form, and correspond to Rules (4.3b) through (4.3d). Rule (4.10d) handles references to spliced unexpanded patterns. The first premise parses the indicated subsequence of the literal body, b , to produce the referenced unexpanded pattern, \hat{p} , and the second premise types and expands

\hat{p} under the upTSM context Φ from the upTSM application site, producing the hypotheses Ω . These are the hypotheses generated in the conclusion of the rule.

Notice that none of these rules explicitly add any hypotheses to the pattern typing context, so upTSMs cannot introduce any hypotheses other than those that come from such spliced subpatterns. This achieves the “no hidden assumptions” hygiene property described in Sec. 4.1.5.

4.2.10 Metatheory

Theorem 4.14 (Typed Pattern Expansion). *Both of the following hold:*

1. *If $\Omega \vdash_{\Phi} \hat{p} \rightsquigarrow p : \tau$ and $\Delta \vdash \Phi \text{ ok}$ then $\Omega \Vdash p : \tau$.*
2. *If $\vdash^{\Omega; \Phi; b} \hat{p} \rightsquigarrow p : \tau$ and $\Delta \vdash \Phi \text{ ok}$ then $\Omega \Vdash p : \tau$.*

Proof. By mutual rule induction on Rules (4.6) and (4.10). □

Theorem 4.15 (Typed Expansion). *All of the following hold:*

1. (a) *If $\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{e} \rightsquigarrow e : \tau$ and $\Delta \vdash \hat{\Sigma} \text{ ueTSMs}$ and $\Delta \vdash \Phi \text{ ok}$ then $\Delta \Gamma \vdash e : \tau$.*
 (b) *If $\Delta \Gamma \vdash_{\hat{\Sigma}; \Phi} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$ and $\Delta \vdash \hat{\Sigma} \text{ ueTSMs}$ and $\Delta \vdash \Phi \text{ ok}$ then $\Delta \Gamma \vdash r : \tau \Rightarrow \tau'$.*
2. (a) *If $\Delta \Gamma \vdash^{\Delta_{app}; \Gamma_{app}; \hat{\Sigma}; \Phi_S; b} \hat{e} \rightsquigarrow e : \tau$ and $\Delta_{app} \vdash \hat{\Sigma} \text{ ueTSMs}$ and $\Delta_{app} \vdash \Phi_S \text{ ok}$ then $\Delta \cup \Delta_{app} \Gamma \cup \Gamma_{app} \vdash e : \tau$.*
 (b) *If $\Delta \Gamma \vdash^{\Delta_{app}; \Gamma_{app}; \hat{\Sigma}; \Phi_S; b} \hat{r} \rightsquigarrow r : \tau \Rightarrow \tau'$ and $\Delta_{app} \vdash \hat{\Sigma} \text{ ueTSMs}$ and $\Delta_{app} \vdash \Phi_S \text{ ok}$ then $\Delta \cup \Delta_{app} \Gamma \cup \Gamma_{app} \vdash r : \tau \Rightarrow \tau'$.*

Proof. By mutual rule induction on Rules (4.4), Rule (4.5), Rules (4.8) and Rule (4.9). □

Chapter 5

Parameterized TSMs

5.1 Parameterized TSMs By Example

5.1.1 Type Parameters By Example

5.1.2 Module Parameters By Example

5.2 miniVerse_∀

5.2.1 Signatures, Types and Expanded Expressions

5.2.2 Parameter Application and Deferred Substitution

5.2.3 Macro Expansion and Validation

5.2.4 Metatheory

Chapter 6

Type-Specific Languages (TSLs)

With TSMs, library providers can control the expansion of arbitrary syntax that appears between delimiters, but clients must explicitly identify the TSM and provide the required type and module parameters at each use site. To further lower the syntactic cost of using TSMs, so that it compares to the syntactic cost of derived syntax built in primitively (e.g. list syntax), we will now discuss how VerseML allows library providers to define *type-specific languages* (TSLs) by associating a TSM directly with an abstract type or datatype. When the type system encounters a delimited form not prefixed by a TSM name, it applies the TSM associated with the type it is being analyzed against implicitly.

6.1 TSLs By Example

For example, a module `P` can associate the TSM `rx` defined in the previous section with the abstract type `R.t` by qualifying the definition of the sealed module it is defined by as follows:

```
module R = mod {  
  type t = (* ... *)  
  (* ... *)  
} :> RX with syntax rx
```

More generally, when sealing a module expression against a signature, the programmer can specify, for each abstract type that is generated, at most one previously defined TSMs. This TSM must take as its first parameter the module being sealed.

The following function has the same expansion as `example_using_tsm` but, by using the TSL just defined, it is more concise. Notice the return type annotation, which is necessary to ensure that the TSL can be unambiguously determined:

```
fun example_using_tsl(name : string) : R.t => /@name: %ssn/
```

As another example, let us consider the standard list datatype. We can use TSLs to express derived list syntax, for both expressions and patterns:

```
datatype list('a) { Nil | Cons of 'a * list('a) } with syntax {  
  static fn (body : Body) =>  
    (* ... comma-delimited spliced exps ... *)
```

```

} with pattern syntax {
  static fn (body : Body) : Pat =>
    (* ... list pattern parser ... *)
}

```

Together with the TSL for regular expression patterns, this allows us to write lists like this:

```

let val x : list(R.t) = [/\\d/, /\\d\\d/, /\\d\\d\\d/]

```

From the client’s perspective, it is essentially as if the language had built in derived syntax for lists and regular expression patterns directly.

6.2 Parameterized Modules

TSLs can be associated with abstract types that are generated by parameterized modules (i.e. generative functors in Standard ML) as well. For example, consider a trivially parameterized module that creates modules sealed against RX:

```

module F() => mod {
  type t = (* ... *)
  (* ... *)
} :> RX with syntax rx

```

Each application of F generates a distinct abstract type. The semantics associates the appropriately parameterized TSM with each of these as they are generated:

```

module F1 = F() (* F1.t has TSL rx(F1) *)
module F2 = F() (* F2.t has TSL rx(F2) *)

```

As a more complex example, let us define two signatures, A and B, a TSM \$G and a parameterized module G : A -> B:

```

signature A = sig { type t; val x : t }
signature B = sig { type u; val y : u }
syntax $G(M : A)(G : B) at G.u { (* ... *) }
module G(M : A) => mod {
  type u = M.t; val y = M.x } :> B with syntax $G(M)

```

Both G and \$G take a parameter M : A. We associate the partially applied TSM \$G(M) with the abstract type that G generates. Again, this satisfies the requirement that one must be able to apply the TSM being associated with the abstract type to the module being sealed.

Only fully abstract types can have TSLs associated with them. Within the definition of G, type u does not have a TSL available to it because it is synonymous to M.t. More generally, TSL lookup respects type equality, so any synonyms of a type with a TSL will also have that TSL. We can see this in the following example, where the type u has a different TSL associated with it inside and outside the definition of the module N:

```

module M : A = mod { type t = int; val x = 0 }
module G1 = G(M) (* G1.t has TSL $G(M), per above *)
module N = mod {

```

```

type u = G1.t (* u = G1.t in this scope, so u also has TSL  $G(M)$  *)
val y = /asdf/ (* we can use it to create a value of that type *)
} :> B (* did not specify a TSL for N.u at the point where it is sealed,
        so N.u has no TSL in the outer scope *)
val z : N.u = /asdf/ (* ERROR: no TSL for type N.u *)

```

6.3 miniVerse_{TSL}

A formal specification of TSLs in a language that supports only non-parametric datatypes is available in a paper published in ECOOP 2014 [30].

Chapter 7

Discussion & Future Directions

7.1 Interesting Applications

Most of the examples in Sec. 2.2 can be expressed straightforwardly using the constructs introduced in the previous chapters. Here, let us highlight certain interesting examples and exceptions.

7.1.1 TSMs For Defining TSMs

Static functions can also make use of TSMs. In this section, we will show how quasiquotation syntax and grammar-based parser generators can be expressed using TSMs. These TSMs are quite useful for writing other TSMs.

Quasiquotation

TSMs must generate values of type `CEExp`. Doing so explicitly can have high syntactic cost. To decrease the syntactic cost of constructing values of this type, the prelude includes a TSM that provides quasiquotation syntax (cf. Sec. 2.2.7):

```
syntax $qqexp at CEExp {  
  static fn(body : Body) : ParseResult => (* expression parser here *)  
}  
  
syntax $qqtype at CETyp {  
  static fn(body : Body) : ParseResult => (* type parser here *)  
}
```

For example, the following expression:

```
let gx = $qqexp 'g(x)'
```

is more concise than its expansion:

```
let gx = App(Var 'g', Var 'x')
```

The full concrete syntax of the language can be used. Anti-quotation, i.e. splicing in an expression of type `MarkedExp`, is indicated by the prefix `%`:


```
let fgx = $qqexp 'f(%gx)'
```

The expansion of this expression is:

```
let fgx = App(Var 'f', gx)
```

Parser Generators

TODO: grammars, compile function, TSM for grammar, example of IP address

7.1.2 Monadic Commands

7.2 Summary

TODO: Write summary

7.3 Future Directions

7.3.1 Static Language

We have assumed throughout this work that parse functions are fully self-contained, i.e. they are closed. This simplifies our exposition and metatheory, but it is not a realistic constraint – in practice, one would want to be able to share helper code between parse functions. To allow this, VerseML allows programmers to introduce *static blocks*, which introduce bindings available only in other static blocks and static functions. For example, the following static block defines a helper function for use in the subsequent parse function.

```
1 static
2   val parseInt : Body -> Exp option = (* ... *)
3 end
4 syntax $rx at Rx {
5   static fn(body : Body) : ParseResultExp =>
6     (* ... parseInt is available here ... *)
7 }
8 val x = parseInt("34") (* error: parseInt is not bound here *)
```

7.3.2 TSM Packaging

In the exposition thusfar, we have assumed that TSMs have delimited scope. However, ideally, we would like to be able to define TSMs within a module:

```
structure Rxlib = struct
  type Rx = (* ... *)
  syntax $rx at Rx { (* ... *) }
  (* ... *)
end
```

However, this leads to an important question: how can we write down a signature for the module `Rxlib`? One approach would be to simply duplicate the full definition of the TSM in the signature, but this leads to inelegant code duplication and raises the difficult question of how the language should decide whether one TSM is a duplicate of another. For this reason, in VerseML, a signature can only refer to a previously defined TSM. So, for example, we can write down a signature for `Rxlib` after it has been defined:

```
signature RXLIB = sig
  type Rx = (* ... *)
  syntax $rx = Rxlib.$rx
  (* ... *)
end
Rxlib : RXLIB (* check Rxlib against RXLIB after the fact *)
```

Alternatively, we can define the type `Rx` and the TSM `$rx` before defining `Rxlib`:

```
local
  type Rx = (* ... *)
  syntax $rx at Rx { (* ... *) }
in
  structure Rxlib :
  sig
    type Rx = Rx
    syntax $rx = $rx
    (* ... *)
  end = struct
    type Rx = Rx
    syntax $rx = $rx
    (* ... *)
  end
end
```

Another important question is: how does a TSM defined within a module at a type that is held abstract outside of that module operate? For example, consider the following:

```
local
  type Rx = (* ... *)
  syntax $rx at Rx { (* ... *) }
in
  structure Rxlib :
  sig
    type Rx (* held abstract *)
    syntax $rx = $rx
    (* ... *)
  end = struct
    type Rx = Rx
    syntax $rx = $rx
    (* ... *)
  end
end
```

If we apply `Rxlib.$rx`, it may generate an expansion that uses the constructors of the `Rx` type. However, because the type is being held abstract, these constructors may not be visible at the application site. **TODO: actually, this is why doing this is a bad idea. export TSMs only from units, not modules**

7.3.3 TSMs and TSLs In Candidate Expansions

Candidate expansions cannot themselves define or apply TSMs. This simplifies our metatheory, though it can be inconvenient at times for TSM providers. We discuss adding the ability to use TSMs within candidate expansions here. **TODO: write this**

7.3.4 Pattern Matching Over Values of Abstract Type

ML does not presently support pattern matching over values of an abstract data type. However, there have been proposals for adding support for pattern matching over abstract data types defined by modules having a “datatype-like” shape, e.g. those that define a case analysis function like the one specified by `RX`,

7.3.5 Integration Into Other Languages

We conjecture that the constructs we describe could be integrated into dependently typed functional languages, e.g. Coq, but leave the technical developments necessary for doing so as future work.

Some of the constructs in Chapter 3, Chapter 5 and Chapter 6 could also be adapted for use in imperative languages with non-trivial type structure, like Java. Similarly, some of the constructs we discuss could also be adapted into “dynamic languages” like Racket or Python, though the constructs in Chapter 6 are not relevant to such languages.

7.3.6 Mechanically Verifying TSM Definitions

Finally, VerseML is not designed for advanced theorem proving tasks where languages like Coq, Agda or Idris might be used today. That said, we conjecture that the primitives we describe could be integrated into languages like Gallina (the “external language” of the Coq proof assistant [26]) with modifications, but do not plan to pursue this line of research here.

In such a setting, you could verify TSM definitions **TODO: finish writing this**

7.3.7 Improved Error Reporting

7.3.8 Controlled Binding

7.3.9 Type-Aware Splicing

7.3.10 Integration With Code Editors

7.3.11 Resugaring

TODO: Cite recent work at PLDI (?) and ICFP from Brown

7.3.12 Non-Textual Display Forms

TODO: Talk about active code completion work and future ideas

L^AT_EX Source Code and Updates

The L^AT_EX sources for this document can be found at the following URL:

<https://github.com/cyrus-/thesis>

The latest version of this document can be downloaded from the following URL:

<https://github.com/cyrus-/thesis/raw/master/omar-thesis.pdf>

Any errors or omissions can be reported to the author by email at the following address:

comar@cs.cmu.edu

The author will also review and accept pull requests on GitHub.

Bibliography

TODO (Later): List conference abbreviations.

TODO (Later): Remove extraneous nonsense from entries.

- [1] [Rust] Macros. <https://doc.rust-lang.org/book/macros.html>. Retrieved Nov. 3, 2015. 3.1.2
- [2] The Visible Compiler. <http://www.smlnj.org/doc/Compiler/pages/compiler.html>. 2.3.3
- [3] Information technology portable operating system interface (posix) base specifications, issue 7. *Information technology Portable Operating System Interface (POSIX) Base Specifications, Issue 7*. 2.2.1
- [4] OWASP Top 10 2013. https://www.owasp.org/index.php/Top_10_2013-Top_10_2013. 3
- [5] Alan Bawden. Quasiquotation in Lisp. In *Partial Evaluation and Semantic-Based Program Manipulation*, pages 4–12, 1999. URL <http://repository.readscheme.org/ftp/papers/pepm99/bawden.pdf>. 2.3.3
- [6] Martin Bravenboer, Eelco Dolstra, and Eelco Visser. Preventing Injection Attacks with Syntax Embeddings. In *GPCE '07*, pages 3–12, 2007. ISBN 978-1-59593-855-8. doi: 10.1145/1289971.1289975. URL <http://doi.acm.org/10.1145/1289971.1289975>. 2.3.1
- [7] Eugene Burmako. Scala Macros: Let Our Powers Combine!: On How Rich Syntax and Static Types Work with Metaprogramming. In *Proceedings of the 4th Workshop on Scala (SCALA '13)*, pages 3:1–3:10, 2013. 2.3.3
- [8] Adam Chlipala. Ur: statically-typed metaprogramming with type-level record computation. In Benjamin G. Zorn and Alexander Aiken, editors, *Proceedings of the 2010 ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2010, Toronto, Ontario, Canada, June 5-10, 2010*, pages 122–133. ACM, 2010. ISBN 978-1-4503-0019-3. URL <http://doi.acm.org/10.1145/1806596.1806612>. 1.1
- [9] Adam Chlipala. Ur/Web: A simple model for programming the web. In *POPL '15*, pages 153–165, 2015. ISBN 978-1-4503-3300-9. URL <http://dl.acm.org/citation.cfm?id=2676726>. 1.1
- [10] Tom Christiansen, Brian D. Foy, and Larry Wall. *Programming Perl - Unmatched power for text processing and scripting: covers Version 5.14, 4th Edition*. O'Reilly, 2012.

ISBN 978-0-596-00492-7. URL <http://www.oreilly.de/catalog/9780596004927/index.html>. 2.2.1

- [11] Sebastian Erdweg and Felix Rieger. A framework for extensible languages. In *GPCE '13*, pages 3–12, 2013. 1.1, 2.3.2
- [12] Sebastian Erdweg, Tillmann Rendel, Christian Kastner, and Klaus Ostermann. SugarJ: Library-based syntactic language extensibility. In *OOPSLA '11*, pages 187–188, 2011. 1.1
- [13] Matthew Flatt. Creating languages in Racket. *Commun. ACM*, 55(1):48–56, January 2012. ISSN 0001-0782. doi: 10.1145/2063176.2063195. URL <http://doi.acm.org/10.1145/2063176.2063195>. 1.1, 1.1.1, 2.3.2
- [14] Steven Ganz, Amr Sabry, and Walid Taha. Macros as multi-stage computations: Type-safe, generative, binding macros in MacroML. In *ICFP '01*, pages 74–85, 2001. 2.3.3
- [15] T.G. Griffin. Notational definition-a formal account. In *Logic in Computer Science (LICS '88)*, pages 372–383, 1988. doi: 10.1109/LICS.1988.5134. 2.3.2
- [16] Cordelia V. Hall, Kevin Hammond, Simon L. Peyton Jones, and Philip L. Wadler. Type classes in Haskell. *ACM Trans. Program. Lang. Syst.*, 18(2):109–138, March 1996. ISSN 0164-0925. doi: 10.1145/227699.227700. URL <http://doi.acm.org/10.1145/227699.227700>. 1.3
- [17] Robert Harper. *Programming in Standard ML*. 1997. URL <http://www.cs.cmu.edu/~rwh/smlbook/book.pdf>. Working draft, retrieved June 21, 2015. 1.1, 2.1
- [18] Robert Harper. *Practical Foundations for Programming Languages*. Cambridge University Press, 2012. 4.2.1, 4.2.3
- [19] Robert Harper. *Practical Foundations for Programming Languages*. Second edition, 2015. URL <https://www.cs.cmu.edu/~rwh/plbook/2nded.pdf>. (Working Draft, Retrieved Nov. 19, 2015). 2.1, 2.2.1, 3.1.2, 3.2.1, 3.4, 3.2.2, 4.2.2
- [20] T. P. Hart. MACRO definitions for LISP. Report A. I. MEMO 57, Massachusetts Institute of Technology, A.I. Lab., Cambridge, Massachusetts, October 1963. 2.3.3
- [21] David Herman. *A Theory of Typed Hygienic Macros*. PhD thesis, Northeastern University, Boston, MA, May 2010. 2.3.3
- [22] Neil D. Jones, Carsten K. Gomard, and Peter Sestoft. *Partial Evaluation and Automatic Program Generation*. Prentice Hall International, International Series in Computer Science, June 1993. ISBN number 0-13-020249-5 (pbk). 4
- [23] Simon L Peyton Jones. *Haskell 98 language and libraries: the revised report*. Cambridge University Press, 2003. 1.1
- [24] Eugene E. Kohlbecker, Daniel P. Friedman, Matthias Felleisen, and Bruce Duba. Hygienic macro expansion. In *Symposium on LISP and Functional Programming*, pages 151–161, August 1986. 2.3.3
- [25] Xavier Leroy, Damien Doligez, Alain Frisch, Jacques Garrigue, Didier Rémy, and

- Jérôme Vouillon. *The OCaml system release 4.01 Documentation and user's manual*. Institut National de Recherche en Informatique et en Automatique, September 2013. 1.1, 1.1, 2.3.2
- [26] The Coq development team. *The Coq proof assistant reference manual*. LogiCal Project, 2004. URL <http://coq.inria.fr>. Version 8.0. 2.3.2, 7.3.6
 - [27] Robin Milner, Mads Tofte, Robert Harper, and David MacQueen. *The Definition of Standard ML (Revised)*. The MIT Press, 1997. 1.1, 1.2
 - [28] Odersky, Zenger, and Zenger. Colored local type inference. In *POPL: 28th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*, 2001. 1.2
 - [29] Cyrus Omar, YoungSeok Yoon, Thomas D. LaToza, and Brad A. Myers. Active Code Completion. In *Proceedings of the 2012 International Conference on Software Engineering (ICSE '12)*, pages 859–869, 2012. ISBN 978-1-4673-1067-3. URL <http://dl.acm.org/citation.cfm?id=2337223.2337324>. 1
 - [30] Cyrus Omar, Darya Kurilova, Ligia Nistor, Benjamin Chung, Alex Potanin, and Jonathan Aldrich. Safely composable type-specific languages. In *ECOOP '14*, 2014. 3.1, 6.3
 - [31] Cyrus Omar, Chenglong Wang, and Jonathan Aldrich. Composable and hygienic typed syntax macros. In *ACM Symposium on Applied Computing (SAC '15)*, 2015. 3.1
 - [32] Benjamin C. Pierce. *Types and Programming Languages*. MIT Press, 2002. 2.1, 3.2.1
 - [33] Benjamin C. Pierce and David N. Turner. Local type inference. *ACM Trans. Program. Lang. Syst.*, 22(1):1–44, January 2000. ISSN 0164-0925. doi: 10.1145/345099.345100. URL <http://doi.acm.org/10.1145/345099.345100>. 1.2
 - [34] J. C. Reynolds. GEDANKEN - a simple typless language based on the principle of completeness and reference concept. *Comm. A.C.M.*, 13(5), May 1970. 1
 - [35] August Schwerdfeger and Eric Van Wyk. Verifiable composition of deterministic grammars. In *PLDI '09*, pages 199–210, 2009. ISBN 978-1-60558-392-1. URL <http://doi.acm.org/10.1145/1542476.1542499>. 1.1.1, 2.3.2
 - [36] Denys Shabalin, Eugene Burmako, and Martin Odersky. Quasiquotes for Scala. Technical Report EPFL-REPORT-185242, 2013. 2.3.3
 - [37] Eric Spishak, Werner Dietl, and Michael D Ernst. A type system for regular expressions. In *Proceedings of the 14th Workshop on Formal Techniques for Java-like Programs (FTfJP '12)*, pages 20–26, 2012. 4
 - [38] Guy L Steele. *Common LISP: the language*. Digital press, 1990. 2.3.2
 - [39] Ken Thompson. Programming techniques: Regular expression search algorithm. *Commun. ACM*, 11(6):419–422, June 1968. ISSN 0001-0782. doi: 10.1145/363347.363387. URL <http://doi.acm.org/10.1145/363347.363387>. 2.2.1
 - [40] Todd L. Veldhuizen. *Active Libraries and Universal Languages*. PhD thesis, Indiana University, 2004. 2.3.4
 - [41] Martin P. Ward. Language-oriented programming. *Software - Concepts and Tools*, 15

(4):147–161, 1994. [1.1.1](#)

- [42] Xi, Chen, and Chen. Guarded recursive datatype constructors. In *POPL '03*, 2003. [1.1.3](#)