Extrinsic Relational Subtyping

ACM Reference Format:
. 2024. Extrinsic Relational Subtyping. 1, 1 (December 2024), 27 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Context. Automatically catching errors in programs is a hard enough problem that many languages require users to provide simple specifications to limit that space of correctness. Languages, such as Java and ML, are *intrinsically typed*, requiring nearly all terms to be associated with some type specified by the user. The clever design of ML allows annotations to be fairly sparse by having types specified at constructor definitions and relying on type inference elsewhere.

For various reasons that aren't completely clear, intrinsically typed languages have lost favor, and untyped or *extrinsically typed* languages, such as Javascript/Typescript and Python, have surged in popularity. Untyped languages place less initial burden on the programmer to define the upper bounds on specific combinations of constructors. The flexibility and reusability of writing code that doesn't have to fit some predefined restriction may be seen as one of the benefits of these extrinsically typed languages over the well-studied intrinsically-typed languages. Unfortunately, this freedom makes static analysis or type inference much more challenging.

Despite the ever increasing use of untyped languages in production systems, the need to automatically verify precise and expressive properties of systems has never been greater. To this end, researchers have extended the simple types (such as those found in ML) into *refinement types*, *predicate subtyping*, and *dependent types*.

Refinement types offer greater precision than simple types, but still rely on intrinsic type specifications. Dependent types can express detailed relations, but may require users to provide proofs along with detailed annotations. Predicate subtyping offers some of the expressivity of dependent types, but with the automatic subtyping of refinement types. All of these techniques are based on intrinsic typing and therefore require users to provide additional annotations beyond the runtime behavior of their programs.

The challenge with extrinsically typed languages is that they allow using constructors in any possible combination, rather than prescribing the upper bound of combinations as in the datatype mechanism of ML languages. Thus, the crux of typing extrinsically typed programs is to determine a precise type based on how constructors are used. Since the way constructors are use may overlap is various ways, this form of reasoning about types requires a notion of subtyping. Type systems for extrinsically typed languages have relied on unions and intersections between types to represent precise types based on how expressions are used in combination.

Author's address:

ACM XXXX-XXXX/2024/12-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Gap. Because extrinsically typed languages do not require users to specify the upper bounds of program expressions, there are many untyped programs that cannot benefit from the typing techniques of intrinsically typed languages. Furthermore, extrinsically typed languages do not require users to provide proofs, that have no runtime behavior, as is sometimes necessary in dependently typed systems to verify more expressive types. For instance, the liquid type system [] can verify and infer some relational properties, but it requires users to specify ML-style base types and a set of logical qualifiers to draw from. On the other hand, existing extrinsically typed techniques can not represent richer notions of relations beyond the mere shapes of expressions. Thus, the challenge is to bring rich expressive types to extrinsically typed languages.

Innovation. To overcome these limitations, we introduce *extrinsic relational type inference*: a novel system that automatically infers expressive properties from untyped functional programs.

The main idea behind relational typing is to leverage subtyping as a means to express relations between objects. This completely obviates the need for the two-level type language used in liquid types or predicate subtyping. There is no special first-order predicate language. In relational typing, a relation is just a type in a subtyping lattice, just as a shape is just a type in a subtyping lattice. A subtyping judgment can degenerate into a typing judgment when the left side or strong side of subtyping is a singleton type (type with a single inhabitant). **TODO: insert example of (succ zero, cons nil) subs nat list** Additionally, two separate relations may be compared via subtyping to say that one relation may hold true for a superset of inhabitants of another. **TODO: insert example of even list subs nat list** By embedding the notion of relations into subtyping the system can reuse techniques for inferring unions and intersections over simple types, which are necessary in an extrinsic setting.

In addition to checking that subtyping holds, the system is able to infer weak parameter types and strong return types of functions, which then serve as constraints to be checked according to the applications of functions.

For comparison, the meaning of subtyping relations in relational types corresponds to the meaning of implication between qualifiers in liquid types.

While the purely functional setting presented in this work is not suitable for practical programming, future work could extend it to incorporate side-effects to make it practical. Alternatively, the purely functional setting could be viewed as an alternative formal foundation more mathematics, allowing for greater proof automation by allowing reuse of proofs across the transitive closure of proposition subtyping.

2 OVERVIEW

2.1 Language of types

Parametric types. Universal types. Existential type. System F-style. Parameterization of types indexed by types (i.e. second order).

TODO: mention somwhere that the second order quantification serves two distinct purposes; 1. polymorphism as in System-F. 2. refinement as in first-order quantification of liquid types. Relational types is able to leverage second-order quantification for refinement, eschewing the first-order quantification used in other systems.

Combination types. One of the advantages of untyped programs is that they may be written in a flexible manner. Subtyping is necessary safely reflect the flexibility of compositions in programs, without too many false failures. Another main advantage of untyped programs is that users don't have to provide type specifications. Thus, a general way of constructing types from compositions encountered in the the program is necessary. Some compositions indicate that a type should

strengthen, and some compositions indicate that a type should weaken. To this end, the type language uses intersection and union combinators, whose semantics are degenerate versions of those in set-theory.

For instance, when inferring the type of a function, the system's goal is to infer the weakest valid parameter type and the strongest valid return type for a function definition. It strengthens the parameter type with intersection and weakens the return type with union according to the function body, to arrive at a valid type for the function.

By contrast, the liquid type language relies on the less flexible tagged unions of ML datatypes, which is sufficient in its setting since those types are specified by the user. Likewise, it does not rely on union to weaken to a valid return type. Instead, it weakens to the strongest valid return type by dropping conjunctions from the return type's qualifiers until a valid return type is found.

Inductive types. Similar to ML datatypes.

Constraint types. In addition to expressing the shapes of terms, the system should be able express relations between terms, such as "a list has the length of some natural number". Rather than using a distinct syntax for relational predicates, the type language treats relations as just another type thereby reusing machinery already available for types, such as existential types, union types, and inductive types. Since parametric types are second order, constraining relations requires subtyping. Thus, parametric types are extended with constraints in the form of subtyping.

2.2 Type Inference

TODO: example of a inference of intersection of function param applied to multiple arguments (not novel)
TODO: example of a inference of intersection of param with multiple functions applied to it (not novel)
TODO: example of a inference of union type of branching (not novel)

We illustrate the syntax and semantics of programs and types with the example program shown in Fig. 1.

Path typing. Consider the function `trivial` that completes an English phrase:

This program is defined by paths over hardcoded tags. The system infers the type to be an intersection of implication types:

$$\Delta \cdot \Gamma \vdash \texttt{trivial} : \texttt{(?hello -> ?world) \& (?good -> ?morning)}$$

Path selection. Suppose the function `trivial` is applied to a literal value `#hello`. The system can discard the irrelevant clauses and infer the singleton type `?world`.

$$\Delta \cdot \Gamma \vdash \texttt{trivial \#hello} : \texttt{?world}$$

Relational typing. Consider the function `repeat` that takes a natural number and returns a list of that length. Without specifying any requirements besides the function definition, the system

```
let trivial =
    path #hello => #world
    path #good => #morning in

let repeat = path x => fix(path self =>
    path #zero => #nil
    path #succ n => #cons (x, self n)) in

let fromList = fix(path self =>
    path #nil => ...
    path #cons (x, xs) => ...) in

let fromNat = path x n => fromList (repeat x n)

let fromUno = path (@uno = content) => ... in
let fromDos = path (@dos = content) => ... in
let fromBoth = path x => (fromUno x, fromDos, x)

let lessOrEq = fix(path self =>
    path (#zero, _) => #true
    path (#succ x, #succ y) => self (x, y)
    path (#succ _, #zero) => #false) in

let max = (path (x, y) =>
    if lessOrEq (x, y) then y else x) in

...
```

Fig. 1. Example program

can infer the property that the resulting list has the length of the input number.

$$\frac{\begin{array}{r} nat = \texttt{induc[N] ?zero | ?succ N} \\ nat\_list\ \alpha = \left(\begin{array}{l}\texttt{induc[NL]} \\ \quad \texttt{?zero} * \texttt{?nil} \mid \\ \quad \{\texttt{?succ N} * \texttt{?cons (}\alpha * \texttt{L) with N} * \texttt{L <: NL}\}\end{array}\right)\end{array}}{\Delta \cdot \Gamma \vdash \texttt{repeat} : \texttt{[X]X -> [F<:\{N -> L with N} * \texttt{L <:}\ nat\_list\ \texttt{X\}]F}}$$

Relational selection. Suppose the function `repeat` is applied to the hardcoded number two, represented as `(#succ #succ #zero)`. The system can infer the result to be a singleton type representing a single list, much like how Prolog evaluates logic programs.

$$\Delta \cdot \Gamma \vdash \texttt{repeat () (\#succ \#succ \#zero)} : \texttt{?cons (unit} * \texttt{?cons (unit} * \texttt{?nil))}$$

Path selection and relational selection demonstrate that the declarative type language is expressive enough to perform evaluation. However, this simply reproduces the effect of the dynamic semantics, albeit in a declarative style. For types to be useful in practice, they need to offer ways to express properties with incomplete information. The next examples illustrate how the system can compose abstract properties to infer useful properties, which are not reproducible by dynamic semantics.

Factoring. Suppose the function `fromList`, which expects a list, is applied to a list that's related to a natural number, as would be the result of `(repeat x n)`, illustrated in the body of `fromNat`. The system must verify that the type of `(repeat x n)` is a subtype of the parameter type of `(fromList)`. The argument type of `(repeat x n)` is a type projected from a relation with an abstract natural number, since its arguments are not hardcoded. This abstract type information cannot be handled by dynamic semantics. Despite these complexities, the the system is able to ensure that these abstract inferred types can safely be composed, by factoring $(nat\_list\ \alpha)$ into the weaker pair $(nat\ *\ list\ \alpha)$. Once factored out, the list type of the argument type's relation can be projected and unified with the parameter's list type.

$$\frac{list\ \alpha = \texttt{induc[L] ?nil | ?cons } (\alpha\ *\ \texttt{L}) \qquad \Delta \vdash nat\_list\ \texttt{X} \sqsubseteq nat\ *\ list\ \texttt{X} \qquad \Delta \vdash list\ \texttt{X} \sqsubseteq list\ \texttt{Y}}{\Delta \vdash \{\texttt{L with N} * \texttt{L <:}\ nat\_list\ \texttt{X}\} \sqsubseteq list\ \texttt{Y}}$$

Inductive subtyping. Consider applying a function that expects a natural number to an argument whose type is an even natural number. In order to verify that this application is allowed, the system must verify that an even number is a subtype of a natural number. The system can soundly verify this subtyping by relying on an induction hypothesis. The induction hypothesis allows weakening the inductive component of the even type to the natural number type as it unrolls.

$$\frac{\dfrac{even = \texttt{induc[N] ?zero | ?succ ?succ N} \qquad \Delta \vdash \texttt{(?zero | ?succ ?succ } nat\texttt{)} \sqsubseteq nat}{\Delta, even\ \texttt{<:}\ nat \vdash \texttt{(?zero | ?succ ?succ } even\texttt{)} \sqsubseteq nat}}{\Delta \vdash even \sqsubseteq nat}$$

Relational subtyping. Due to the precise relational types that the system infers, it may also be necessary to verify that a relation subtypes another relation, such as a list with an even length subtyping an list with a natural number length. This situation is similar to inductive subtyping of simple types, but it is complicated by relational constraints in the inductive relations, which must

be added to the context.

$$\frac{\begin{array}{c} even\_list\ \alpha = \left(\begin{array}{l}\texttt{induc[EL]}\\ \quad \texttt{?zero * ?nil |}\\ \quad \texttt{\{?succ ?succ E * ?cons ?cons (}\alpha\ \texttt{* L) with E * L <: EL\}}\end{array}\right) \\ \Delta, \texttt{E * L <:}\ nat\_list\ \texttt{unit} \vdash \left(\begin{array}{l}\texttt{?zero * ?nil |}\\ \texttt{?succ ?succ E *}\\ \quad \texttt{?cons (unit * ?cons (unit * L))}\end{array}\right) \sqsubseteq nat\_list \end{array}}{\left(\begin{array}{l}\Delta, \\ \texttt{E * L <:}\ even\_list\ \texttt{unit}\end{array}, \begin{array}{l} even\_list\ \texttt{unit <:}\ nat\_list\ \texttt{unit}, \end{array}\right) \vdash \left(\begin{array}{l}\texttt{?zero * ?nil |}\\ \texttt{?succ ?succ E *}\\ \quad \texttt{?cons (unit * ?cons (unit * L))}\end{array}\right) \sqsubseteq nat\_list}$$

$$\Delta \vdash (even\_list\ \texttt{unit}) \sqsubseteq (nat\_list\ \texttt{unit})$$

Refinement. Consider the function `fromBoth` that calls two functions on some variable of unknown value or type. The same variable is used as an argument to two separate functions that have different parameter types. The type of the variable can be refined by intersecting both parameter types that it must satisfy.

$$\Delta \cdot \Gamma \vdash \texttt{fromBoth} : \texttt{(uno : X) \& (dos : Y) -> ...}$$

Path sensitivity. Consider the function `max` that chooses the maximum of two natural numbers. The function must satisfy the property that the result is greater or equal to each of the inputs. The system can infer this property by relying on multiple type inference mechanisms, including relational typing, path selection, refinement, and a special form of refinement that refines a type by specializing relations it belongs to. The *if-then-else* expression is merely sugar for applying a function with a *true* path and *false* path to a boolean expression. Note that the variables are used in both the condition and the bodies of the if-then-else expression. To infer a precise type for the if-then-else expression, the types of the variables need to be refined according to each path's expected type, but without leaking the refinement outside of that path. That is, the refinements must be local or path sensitive. Moreover, there must be enough paths of the applied function to handle all the possible values of the argument.

TODO: make sure inductive type (LED) is explained clearly

TODO: max type inference is wrong; should be an intersection

$$\frac{\begin{array}{c} leq\_decide = \left(\begin{array}{l}\texttt{induc[LED]}\\ \quad \texttt{\{?zero * \_ * ?true\} |}\\ \quad \texttt{\{?succ X * ?succ Y * B with X * Y * B <: LED\} |}\\ \quad \texttt{\{?succ \_ * ?zero * ?false\}}\end{array}\right) \\ max\_spec = \left(\begin{array}{l}\texttt{X * Y -> Y \& \{Z with (X * Z * ?true) <:}\ leq\_decide\texttt{\} |}\\ \texttt{X * Y -> X \& \{Z with (Z * Y * ?false) <:}\ leq\_decide\texttt{\}}\end{array}\right) \end{array}}{\Delta \cdot \Gamma \vdash \texttt{max} : max\_spec}$$

TODO: more motivating and elucidating examples

3 LANGUAGE

The programming language is pure and functional. Its syntax and dynamic semantics are fairly standard. The main departure from tradition is that its function and application rules subsume pattern matching. This departure enables a more direct correspondence between the structures of programs and their types, but it is not a necessary condition. The syntax is given in Fig. ??. It includes functions with pattern matching, records, a fixed point combinator, let binding, tags for discriminating cases, and application. A function consists of a sequence of paths, where each path maps a pattern to an expression. A record consists of a sequence of fields, where each field maps a unique label to an expression. The type language includes tag types, field types, implications, unions, intersections, inductions, existentials, universals, top, and bottom. The existential type consists of multiple bound variables, a payload containing the bound variables, and a subtyping constraint over the bound variables. If the bound variables aren't indicated, then all variables in the payload are assumed to be bound variables. If the subtyping constraint isn't indicated, then it is assumed to be a tautology, such as (`unit<:unit`). The universal type consists of a bound variable, the variable's upper bound, and a payload. If the upper bound is not indicated, it is assumed to be the top type (`top`). The typing semantics rely on a typing environment for keeping track of typings of term variables. The subtyping semantics rely on subtyping environment for keeping track of and constraints on type variables. Note that the syntax of the subtyping environment allows an upper bound constraint over a type rather than merely a type variable to allow for relational constraints.
TODO: update tag syntax: `cons;cons;e:cons//cons//T nil;():nil//unit`

3.1 Typing

The typing is given in Fig. ??. Most of the rules are fairly standard. The rule for function typing is a bit special in that it treats a function as a sequence of paths whose type is an intersection of implications, rather than having a separate pattern matching rule. Likewise, the type of a record is an intersection of field types. The let-binding rule allows for prenex polymorphism by generalizing via subtyping.

3.2 Subtyping

The subtyping is given in Fig. ??. Some of the rules are fairly standard, including implication, the union rules, and intersection rules. Note that in addition to left and right rules, union and intersection each have rules for interacting with implication's antecedent and consequent, respectively. The constraint rule checks that a subtyping relation exists as a constraint in the subtyping environment. The right induction rule is standard and simply unrolls the induction. The left induction rule relies on the induction principle to construct an inductive constraint hypothesis. The field and tag rules simply check that the labels match and subtyping holds for their constituent types. The existential rules are quite special, as they involve a subtyping constraint as part of a second-order comprehension. The left existential rule checks that subtyping holds for all variations of the payload where the subtyping constraint holds. The right existential rule checks that subtyping holds for some variation of the payload where the constraint holds. The left universal rule checks that subtyping holds for some variation of the payload consistent with the variable's upper bound. The right universal rule checks that subtyping holds for all variations of the payload consistent with the variable's upper bound.

4 ANALYSIS

The analysis consists of two main parts. The top level is type inference, which corresponds to typing and generates a type for an expression. When type inference encounters constraints that

its types must adhere to, it calls unification to solve these constraints. Note that since the types are expressive enough to represent constraints, an alternative approach of generating constraints and solving them in separate stages could also be designed using the same structures. Additional structures for the analysis are given in Fig. ??. Inference generates a solution set T, which contains triples, each with a type variable set, a subtyping environment, and a type. Unification generates a solution set C, which contains subtyping environments.

4.1 Type inference

The type inference procedure is given in Fig. ??. The procedure depends on four parameters: an type variable set, a subtyping environment, a typing environment, and an expression. The variable set indicates if a type variable's assigned type is allowed to be strengthened or weakened during unification. The subtyping environment indicates the assumed constraints on types containing type variables, including relational constraints and constraints over single type variables, which we also refer to as type assignments. The typing environment indicates the assumed constraints on term variables. The expression indicates the inhabitant of the type that is to be inferred. The procedure returns a set of triples, where each triple consists of a variable set, a subtyping environment, and a type. The unit case simply returns a singleton set with the unit type and the environments unchanged. The variable case uses the variable as a key to find its type in the typing environment. It returns a singleton set containing the found type along with the adjustment set and subtyping environment. The tag case infers the type of its constituent type and uses its label to construct a tag type. The record case infers the type of its fields and intersects the constructed field types together.

The function case is of particular importance to type inference in an untyped setting. For each path in the function, it extracts the term variables of the pattern and associates the term variables with fresh type variables. It infers the body of each path with an updated variable set and an updated typing environment containing the fresh type variables of the pattern. By adding the pattern's type variables to the adjustment variable set, it implies that the parameter type of the path can be strengthened by applications occurring in the body of the path. This enables adjusting a parameter type to reflect all of its occurrences in the body, rather than reflecting just its first occurrence and failing on subsequent occurrences. Before returning the inferred implication type for the path, the case removes the the pattern's type variables from the adjustment variable set, ensuring that those type variables cannot be strengthened or weakened from the outside. As with the record case, the inferred implications are intersected together.

The projection case infers the type of the record expression. It then calls unify to solve for the projected type by finding a single field type that is subtyped by the record type.

The application case also plays an important role in type inference of untyped programs. It creates a fresh type variable as a placeholder for the inferred type of the application result. It infers the type of the function and the argument, and then solves for the result type by unifying the function's type with an implication from the argument type to the result type. It adds the result type variable to the adjustment variable set when unifying to allow inferring types accounting for all the paths that the function might take. After unifying, it removes the result type variable from the adjustment variable set to ensure that the type cannot be modified from the outside. Additionally, since inference and unification actually return sets of solutions, the application must type check for all function types and all argument types. If even one combination cannot be unified then the inference of application fails, indicated by breaking the for-loop, which then implicitly returns an empty set.

TODO: update application to merely require some function cases to type check

the let-binding case infers the type of the argument and checks that all possible types subtype the annotation and result in a well-typed body. It generalizes type variables in the inferred argument type while maintaining the constraints indicated by the subtyping environment.

TODO: update let-binding to generalize only if something is a function-type: e.g. intersection, univeral, implication

TODO: update let-binding to merely require some bodies to type check

The fix case infers inductive types for the parameters and bodies of its target expression. Moreover, it inductively relates the parameter and body types to each other. First, it infers the type of the target and calls unify to deconstruct it into the antecedent and consequent of an implication type. According to the semantics of fix, the antecedent represents and inductive hypothesis, while the consequent represents and inductive conclusion. Thus, it uses the inferred structures of the antecedent and consequent to construct an inductive relation by ensuring that the antecedent subtypes the inductively bound variable of the resulting inductive type. Finally, the implication type is projected from the constructed relation and generalized with universal.

4.2 Subtype unification

The subtype unification procedure is given in Fig. ??. Unification depends on four parameters: a set of type variables, a subtyping environment, and two types. The set of type variables indicates the type of variables that may be adjusted (triggered by the function and application cases of inference). The subtyping environment indicates constraints on type variables. the left type indicates the stronger type, and the right type indicates the weaker type. Both types may contain type variables that are unsolved or partially solved. The procedure returns a set of subtyping environments.

The procedure begins by checking if the two types are syntactically equal. If equal then subtyping holds but there is nothing that can be unified without circular references so the assumed subtyping environment is returned unchanged in a singleton set.

The procedure then pattern matches on the left and right types. The first two cases handle assigning variables to types. The right-variable case first looks up a solution for the variable. If a solution is found, then unification proceeds between the original left type and the solution for the right type. In the case where unification fails, but the type variable is adjustable, the procedure updates the type variable with the union of the left type and the found right type (assuming the constraint is well-formed, which includes avoiding circular references). If no solution is found for the right variable, then the procedure looks for any relational constraints in the subtyping environment where the left side contains the type variable. It checks that the left type is consistent with the relational constraints. If there are no relational constraints, then the variable is assigned to the left type (if the constraint is well-formed). The left-variable rule is similar to the right-variable rule with one difference being that it uses intersection to strengthen the type variable in the case of adjustment. In the case of checking relational constraints, it ensures that the right type is weaker than what the relational constraints would allow.

The subsequent cases decompose the types into subproblems. The decomposition is given in Fig. ??. The order of the rules is critical to ensure that easier constraints are generated. To that end, cases that strengthen the left side or weaken the right side occur before rules that weaken the left side or strengthen the right side.

The left existential case first tries to unify the constraint. It's possible that the constraint cannot be solved, but also isn't invalid, in which case unifying the existential type's constraint simply updates the subtyping environment with the unsolved relational constraint. With the updated environment, the procedure then unifies the existential type's payload with the right type. It must do a safety check to ensure that the left existential's variables are merely assumed and not witnessed.

If the constraint is solved then the procedure checks that the payload subtypes the right type for every constraint solution.

The right universal case updates the subtyping environment with the universal's variable constraint and unifies the left type with the payload. As with left existential, the procedure checks that the universal's type variable is merely assumed and not instantiated.

The left induction rule first tries to factor the inductive type and unify the weakened factored type with the right type. For example, a relational type between a natural number and a list, can be factored into a cross product of a natural number type and a list type. If factoring fails, then the procedure leverages the induction principle and substitutes the right type in for the inductive variable of the left type and unifies the new left type with the right type. Note that factoring is employed for the special case where the right type has variables which cannot be unified using induction due to our circularity restriction.

The cases for antecedent union, consequent intersection, left union, and right intersection decompose into sub-problems in the same way as the declarative subtyping semantics.

The remaining cases are continued in Fig. ??. The right existential case simply unifies the left type with the existential's payload and then unifies the existential's constraint, such that unifying the payload may bear witness to a type that leads to verifying the constraint.

TODO: consider using both forward and backtracking in unification and subtyping rules. Since it is not certain which constraint is stronger (in contrast to prolog). Union solutions together

The right existential case resembles the unification and backtracking approach in Prolog, where unification of the payload corresponds to unification of a query with the head of a horn clause, and solving the existential's constraint after the payload unification corresponds to solving the horn clause's body after the head's unification.

The left universal case also unifies in a backtracking fashion analogous to Prolog. The procedure unifies the universal's payload with the right type, possibly instantiating the universal's type variable, which may then be used to unify and check the universal's constraint.

The right induction case attempts to unroll the inductive type just enough to unify with the left type. To avoid potential infinite unrolling the procedure relies on a heuristic to see if the left type's pattern lines up with parts of the the inductive type that are guaranteed to be well-founded. If the left type is a pattern with variables that prevents it from being reduced, then the procedure checks if it is well-formed, meaning it could be solved if more information were specified, and then the unsolved relational constraint is added to the subtyping environment.

The remaining cases closely mirror their counterparts in the declarative subtyping rules.

5 EXPERIMENTS

TODO: develop 12 tree/list experiments

6 RELATED WORK

Hindley-Milner type inference. Exemplified by ML.

Logic programming. Exemplified by Prolog.
Similar: both have backchaining.
Different: RLT is fully declarative, lacks negations, but has implication.
Different: RLT allows comparing inductive relations via subtyping.

Semantic subtyping. Exemplified by XDuce and CDuce. complete subtyping.
Similar: set-like combinators: union and intersection.
Different: RLT uses rigid syntactic rules; incomplete subtyping.

The terminology "semantic subtyping" vs "syntactic subtyping" are confusing terms. "semantics subtyping" means the semantics of types is determined indirectly by the semantics of another structure. "syntactic subtyping" means the semantics of types is determined directly by the type structure

Extrinsic typing. Exemplified by Typescript, which is unsound. Maybe not as lenient? The static behavior of a program is not necessarily specified/prescribed; it may be over-approximated from the program composition. Intrinsic vs extrinsic is orthogonal to static vs dynamic, although static and dynamic are often used to mean the former. All modern languages use a combination of static and dynamic type checking. The term "dynamically typed" some times refers to a language that doesn't prescribe static meaning, even if it uses both static and dynamic type checking. The term "extrinsic typing" is less ambiguous.

Refinement Types. Exemplified by Refinement ML. Base types with intersections and subtyping.

Predicate Subtyping. Exemplified by Liquid Types. An extension of refinement types.

Similar: both use type inference to infer expressive relational properties.

Different: RLT starts with an invalid post-condition, then weakens return type to a valid post-condition from outside in by expanding unions.

Different: RLT starts with an invalid pre-condition, then strengthens parameter type to a valid pre-condition from inside out by adding intersections.

Different: Liquid types starts with an invalid post-condition, then uses iterative weakening by dropping conjunctions until a valid post-condition is reached.

Abstraction Refinement. Similar: type unification over subtyping resembles abstraction refinement where solving for variables and failing on different sides of the subtyping relation corresponds to solving with the abstractor vs solving with the refiner.

Craig interpolation. Similar: extracting an inductive type with unions and intersections from a recursive program without needing to specify a predicate universe might be similar to craig interpolation.

PDR.. exemplified by IC3.

Similar: RLT infers abstract type for return type, then safely constrains the variables in previous step (fix's antecedent) to subtype the least fixed point. This lazily propagates the type for the last step to the previous steps. This is safe as antecedent is stronger than consequent at any step. Seems similar to the notion in PDR of propagating negation of loss points to previous steps.

Different: RLT isn't cartesian

Definition 6.1. (Expression syntax)

$$
\begin{array}{rcl}
e & ::= & x \mid \texttt{@} \mid \texttt{\sim}l\ e \mid R \mid e\texttt{,}e \mid F \mid e\texttt{.}l \mid (e)(e) \mid \\
& & e\ \texttt{|>}\ e \mid \texttt{fix(}e\texttt{)} \mid \texttt{let}\ x\texttt{:}\tau\ \texttt{=}\ e\ \texttt{in}\ e \mid (e) \\
R & ::= & \epsilon \mid R\,r \\
r & ::= & l\texttt{=>}e \\
F & ::= & \epsilon \mid F\,f \\
f & ::= & *p\texttt{=>}e \\
\\
p & ::= & x \mid \texttt{@} \mid \texttt{\sim}l\ p \mid K \mid p\texttt{,}p \mid (p) \\
K & ::= & \epsilon \mid K\,k \\
k & ::= & l\texttt{=>}p \\
\\
v & ::= & \texttt{@} \mid \texttt{\sim}l\ v \mid G \mid v\texttt{,}v \mid (v) \mid F \\
G & ::= & \epsilon \mid G\,g \\
g & ::= & *l\texttt{=>}v \\
\\
\Sigma & ::= & \epsilon \mid \Sigma\,\sigma \\
\sigma & ::= & x/v
\end{array}
$$

Definition 6.2. $\boxed{e \rightsquigarrow e}$ (Progression)

$$\frac{e \rightsquigarrow e'}{\texttt{\sim}l\ e \rightsquigarrow \texttt{\sim}l\ e'} \qquad \frac{e \rightsquigarrow e'}{R{*}l\texttt{=>}e \rightsquigarrow R{*}l\texttt{=>}e'} \qquad \frac{R \rightsquigarrow R'}{R{*}l\texttt{=>}v \rightsquigarrow R'{*}l\texttt{=>}v} \qquad \frac{e \rightsquigarrow e'}{e\texttt{.}l \rightsquigarrow e'\texttt{.}l}$$

$$\frac{*l\texttt{=>}v \in G \qquad \forall\, e.\ *l\texttt{=>}e \in G \implies e = v}{G\texttt{.}l \rightsquigarrow v} \qquad \frac{e \rightsquigarrow e'}{(e)(e_a) \rightsquigarrow (e')(e_a)} \qquad \frac{e \rightsquigarrow e'}{(v)(e) \rightsquigarrow (v)(e')}$$

$$\frac{(F)(v) \rightsquigarrow e'}{(F\ \texttt{case}\ p\texttt{=>}e)(v) \rightsquigarrow e'} \qquad \frac{p \equiv v \dashv \Sigma \qquad \forall e'.\ \neg F(v) \rightsquigarrow e'}{(F\ \texttt{case}\ p\texttt{=>}e)(v) \rightsquigarrow e[\Sigma]}$$

$$\frac{e \rightsquigarrow e'}{\texttt{let}\ x\texttt{:}\tau\ \texttt{=}\ e\ \texttt{in}\ e_k \rightsquigarrow \texttt{let}\ x\texttt{:}\tau\ \texttt{=}\ e'\ \texttt{in}\ e_k} \qquad \frac{}{\texttt{let}\ x\texttt{:}\tau\ \texttt{=}\ v\ \texttt{in}\ e \rightsquigarrow e[x/v]}$$

$$\frac{e \rightsquigarrow e'}{\texttt{fix(e)} \rightsquigarrow \texttt{fix(e')}} \qquad \frac{}{\texttt{fix(case}\ x\ \texttt{=>}\ e\texttt{)} \rightsquigarrow e[x/\texttt{fix(case}\ x\ \texttt{=>}\ e\texttt{)}]}$$

$$\frac{*\texttt{left=>}e_l \quad *\texttt{right=>}e_r \rightsquigarrow e'}{e_l\texttt{,}e_r \rightsquigarrow e'} \qquad \frac{(e_b)(e_a) \rightsquigarrow e'}{e_a\ \texttt{|>}\ e_b \rightsquigarrow e'} \qquad \frac{e \rightsquigarrow e'}{(e) \rightsquigarrow e'}$$

Definition 6.3. (Type syntax)

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid \texttt{@} \mid \texttt{\textasciitilde}l\ \tau \mid l\texttt{->}\tau \mid \tau\texttt{->}\tau \mid \tau\texttt{|}\tau \mid \tau\texttt{\&}\tau \mid \tau\texttt{\textbackslash}\tau \mid \\
 & & \texttt{EXI[A}\ Q\texttt{]}\tau \mid \texttt{ALL[A}\ Q\texttt{]}\tau \mid \texttt{FIX[}\alpha\texttt{;}\tau\texttt{]} \\
\mathrm{A} & ::= & \epsilon \mid \mathrm{A}\ \alpha \\
Q & ::= & \epsilon \mid Q\ q \\
q & ::= & \texttt{.}\tau\texttt{<:}\tau \\
 & & \\
\Delta & ::= & \epsilon \mid \Delta\ \delta \\
\delta & ::= & \tau <: \tau \\
\Gamma & ::= & \epsilon \mid \Gamma\ \gamma \\
\gamma & ::= & x : \tau \\
 & & \\
M & ::= & \epsilon \mid M\ m \\
m & ::= & \alpha \\
N & ::= & \epsilon \mid N\ n \\
n & ::= & \alpha \\
 & & \\
Z & ::= & \epsilon \mid Z\ z \\
z & ::= & \langle M, \Delta \rangle \\
 & & \\
\mathrm{T} & ::= & \epsilon \mid \mathrm{T}\ \tau \\
 & & \\
\Pi & ::= & \epsilon \mid \Pi\ \pi \\
\pi & ::= & \langle M, \Delta, \tau\texttt{->}\tau \rangle \\
 & & \\
\Omega & ::= & \epsilon \mid \Omega\ \omega \\
\omega & ::= & \alpha / \tau
\end{array}
$$

Definition 6.4. $\boxed{\Gamma \vdash e : \tau \dashv Z}$ (Proof typing)

$$\frac{\langle M, \Delta \rangle \in Z}{\Gamma \vdash \texttt{@} : \texttt{@} \dashv Z} \qquad \frac{\langle M, \Delta \rangle \in Z \qquad x\texttt{:}\tau \in \Gamma}{\Gamma \vdash x : \tau \dashv Z} \qquad \frac{\Gamma \vdash e : \tau \dashv Z}{\Gamma \vdash \texttt{\textasciitilde}l\ \ e : \texttt{\textasciitilde}l\ \ \tau \dashv Z}$$

$$\frac{\Gamma \vdash R : \tau_0 \dashv Z_0 \qquad Z_0 \hookrightarrow Z_1 \qquad \Gamma \vdash e : \tau_1 \dashv Z_1}{\Gamma \vdash R\ *l\texttt{=}e : \tau_0\ \texttt{\&}\ l\texttt{:}\tau_1 \dashv Z_1} \qquad \frac{Z, \Gamma \vdash F \blacktriangle \Pi, \mathrm{T}_n \qquad \Gamma \vdash \Pi \equiv \mathrm{T}}{\Gamma \vdash F : \texttt{\&(T)} \dashv Z}$$

$$\frac{\Gamma \vdash e : \tau_0 \dashv Z_0 \qquad Z_0 \hookrightarrow Z_1 \qquad \tau_0 <: l\texttt{:}\alpha \dashv Z_1}{\Gamma \vdash e\texttt{.}l : \alpha \dashv Z_1}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \qquad Z_0 \hookrightarrow Z_1 \qquad \Gamma \vdash e_1 : \tau_1 \dashv Z_1 \qquad Z_1 \hookrightarrow Z_2 \qquad \tau_0 <: \tau_1\texttt{->}\alpha \dashv Z_2}{\Gamma \vdash e_0\texttt{(}e_1\texttt{)} : \alpha \dashv Z_2}$$

$$\frac{\begin{array}{c}\Gamma \vdash e : \tau \dashv Z_0 \qquad Z_0 \hookrightarrow Z_1 \qquad \tau <: \alpha_0\texttt{->}\alpha_1\texttt{->}\alpha_2 \dashv Z_1 \\ \mathrm{FTV}(\Gamma) \vdash \alpha_0 \circlearrowleft Z_1 \cdot \alpha_1\texttt{->}\alpha_2 \fallingdotseq \alpha_3 \circlearrowleft \mathrm{T}_{rel}\end{array}}{\Gamma \vdash \texttt{fix(}e\texttt{)} : \texttt{ALL[}\alpha_4\texttt{]}\alpha_4\texttt{->EXI[}\alpha_5\texttt{.(}\alpha_4\texttt{,}\alpha_5\texttt{)<:FIX[}\alpha_3\texttt{.|(}\mathrm{T}_{rel}\texttt{)]]}\alpha_5 \dashv Z_0}$$

Definition 6.5. $\boxed{Z, \Gamma \vdash F \blacktriangle \Pi, T}$

$$\frac{Z_0, \Gamma_0 \vdash f \blacktriangle \Pi, T \qquad p : \tau_l \dashv \Gamma_1 \qquad \mathrm{neg}(\tau_l, T) = \tau_l' \qquad Z_0 \rightsquigarrow Z_1 \qquad \Gamma_0 \sqcup \Gamma_1 \vdash e : \tau_r \dashv Z_1}{Z_0, \Gamma_0 \vdash F \; *p{=}{>}e \blacktriangle \Pi \sqcup \overline{\left\langle M, \Delta, \tau_l' \text{-}{>} \tau_r \right\rangle}^{\langle M, \Delta \rangle \in Z_1}, T \; \tau_0}$$

Definition 6.6. $\boxed{Z \rightsquigarrow Z}$ (Universe ordering)

$$\frac{\forall M_1 \; \Delta_1.\; \langle M_1, \Delta_1 \rangle \in Z_1 \implies \exists M_0 \; \Delta_0.\; \langle M_0, \Delta_0 \rangle \in Z_0 \wedge M_0 \preceq M_1 \wedge \Delta_0 \preceq \Delta_1}{Z_0 \rightsquigarrow Z_1}$$

Definition 6.7. $\boxed{\tau <: \tau \dashv M, \Delta}$ (Proof subtyping)

$$\frac{}{\tau <: \tau \dashv M, \Delta} \qquad \frac{}{\texttt{BOT} <: \tau_r \dashv M, \Delta} \qquad \frac{}{\tau_l <: \texttt{TOP} \dashv M, \Delta} \qquad \frac{\tau_l <: (l : \tau_{rl}) \& (l : \tau_{rr}) \dashv M, \Delta}{\tau_l <: l : (\tau_{rl} \& \tau_{rr}) \dashv M, \Delta}$$

$$\frac{\tau_{ll} <: \tau_r \dashv M_0, \Delta_0 \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_{lr} <: \tau_r \dashv M_1, \Delta_1}{\tau_{ll} \mid \tau_{lr} <: \tau_r \dashv M_1, \Delta_1} \qquad \frac{\tau_l <: \tau_{rl} \dashv M_0, \Delta_0 \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau_{rr} \dashv M_1, \Delta_1}{\tau_l <: \tau_{rl} \& \tau_{rr} \dashv M_1, \Delta_1}$$

$$\frac{\tau_l <: (\tau_{ra} \texttt{->} \tau_{rc}) \& (\tau_{rb} \texttt{->} \tau_{rc}) \dashv M, \Delta}{\tau_l <: \tau_{ra} \mid \tau_{rb} \texttt{->} \tau_{rc} \dashv M, \Delta} \qquad \frac{\tau_l <: (\tau_{ra} \texttt{->} \tau_{rb}) \& (\tau_{ra} \texttt{->} \tau_{rc}) \dashv M, \Delta}{\tau_l <: \tau_{ra} \texttt{->} \tau_{rb} \& \tau_{rc} \dashv M, \Delta}$$

$$\frac{\begin{array}{c} Q \dashv M_0, \Delta_0 \qquad A \# \tau_r \\ M_0 \sqcup \mathrm{A} \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau_r \dashv M_1, \Delta_1 \end{array}}{\texttt{EXI[A } Q\texttt{]}\tau_l <: \tau_r \dashv M_1, \Delta_1}$$

$$\frac{\begin{array}{c} Q \dashv M_0, \Delta_0 \qquad A \# \tau_l \\ M_0 \sqcup \mathrm{A} \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau_r \dashv M_1, \Delta_1 \end{array}}{\tau_l <: \texttt{ALL[A } Q\texttt{]}\tau_r \dashv M_1, \Delta_1}$$

$$\frac{\begin{array}{c} \alpha \notin M_0 \\ M_0, \Delta_0, \Delta_0 \vdash M \lessdot \alpha \qquad M_0, \Delta_0, \Delta_0 \vdash \mathrm{T} \ll \alpha \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \overline{\texttt{.}\tau \texttt{<:} \tau_r}^{\tau \in \mathrm{T}} \dashv M_1, \Delta_1 \end{array}}{\alpha <: \tau_r \dashv M_1, \Delta_1 \sqcup \overline{z <: \tau_r}^{z \in M} \; \alpha <: \tau_r}$$

$$\frac{\begin{array}{c} \alpha \notin M_0 \\ M_0, \Delta_0, \Delta_0 \vdash \alpha \lessdot M \qquad M_0, \Delta_0, \Delta_0 \vdash \alpha \lessdot \Delta_{skol} \qquad M_0, \Delta_0, \Delta_0 \vdash \alpha \ll \mathrm{T} \qquad M_0, \Delta_0, \Delta_0 \vdash \alpha \ll \Delta_{rel} \\ M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \overline{\texttt{.}\tau_0[\alpha/\tau_l] \texttt{<:} \tau_1}^{\tau_0 <: \tau_1 \in \Delta_{rel}} \sqcup \overline{\texttt{.}\tau_l \texttt{<:} \tau}^{\tau \in \mathrm{T}} \dashv M_1, \Delta_1 \end{array}}{\tau_l <: \alpha \dashv M_1, \Delta_1 \sqcup \overline{\tau_l <: z}^{z \in M} \sqcup \overline{\tau[\alpha/\tau_l] <: z}^{\tau <: z \in \Delta_{skol}} \; \tau_l <: \alpha}$$

$$\frac{\alpha \in M_0 \qquad \alpha <: \tau \in (\Delta_0 \sqcup \mathrm{factor}(\Delta_0, \alpha)) \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau <: \tau_r \dashv M_1, \Delta_1}{\alpha <: \tau_r \dashv M_1, \Delta_1} \qquad \frac{\alpha \in M_0 \qquad \tau <: \alpha \in \Delta_0 \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau \dashv M_1, \Delta_1}{\tau_l <: \alpha \dashv M_1, \Delta_1}$$

$$\frac{\begin{array}{c} \tau_l <: \tau_r \dashv M_0, \Delta_0 \\ M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad Q \dashv M_1, \Delta_1 \end{array}}{\texttt{ALL[A } Q\texttt{]}\tau_l <: \tau_r \dashv M_1, \Delta_1} \qquad \frac{\begin{array}{c} \tau_l <: \tau_r \dashv M_0, \Delta_0 \\ M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad Q \dashv M_1, \Delta_1 \end{array}}{\tau_l <: \texttt{EXI[A } Q\texttt{]}\tau_r \dashv M_1, \Delta_1}$$

$$\frac{\tau_{ll} <: \tau_r \dashv M, \Delta}{\tau_{ll} \& \tau_{lr} <: \tau_r \dashv M, \Delta} \qquad \frac{\tau_{lr} <: \tau_r \dashv M, \Delta}{\tau_{ll} \& \tau_{lr} <: \tau_r \dashv M, \Delta} \qquad \frac{\tau_l <: \tau_{rl} \dashv M, \Delta}{\tau_l <: \tau_{rl} \mid \tau_{rr} \dashv M, \Delta} \qquad \frac{\tau_l <: \tau_{rr} \dashv M, \Delta}{\tau_l <: \tau_{rl} \mid \tau_{rr} \dashv M, \Delta}$$

Definition 6.8. $\boxed{\tau <: \tau \dashv M, \Delta}$ (Proof world subtyping)

$$\frac{\tau_l[\alpha/\tau_r] <: \tau_r \dashv M, \Delta}{\texttt{FIX[}\alpha\texttt{]}\,\tau_l <: \tau_r \dashv M, \Delta} \qquad \frac{\begin{array}{c}\text{decidable}(\Delta_0, \tau_l, \texttt{FIX[}\alpha\texttt{]}\,\tau_r) \\ \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau_r[\alpha/\texttt{FIX[}\alpha\texttt{]}\,\tau_r] \dashv M, \Delta_1\end{array}}{\tau_l <: \texttt{FIX[}\alpha\texttt{]}\,\tau_r \dashv M, \Delta_1}$$

$$\frac{\begin{array}{c}m \in \text{FTV}(\tau_l) \qquad m \in M_0 \qquad \text{norm}(\tau_l\texttt{<:FIX[}\alpha\texttt{.}\,\tau_r\texttt{]}) = \tau_l'\texttt{<:FIX[}\alpha\texttt{.}\,\tau_r'\texttt{]} \\ \tau_l'\texttt{<:}\tau \in \text{norm}(\Delta_0) \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau <: \texttt{FIX[}\alpha\texttt{.}\,\tau_r'\texttt{]} \dashv M_1, \Delta_1\end{array}}{\tau_l <: \texttt{FIX[}\alpha\texttt{.}\,\tau_r\texttt{]} \dashv M_1, \Delta_1}$$

$$\frac{\begin{array}{c}M_0, \Delta_0, \text{FV}(\tau_l) \vdash \Omega \\ M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l[\Omega] <: \texttt{FIX[}\alpha\texttt{.}\,\tau_r\texttt{]} \dashv M_1, \Delta_1 \qquad \text{WF}(\tau_l\texttt{<:FIX[}\alpha\texttt{.}\,\tau_r\texttt{]})\end{array}}{\tau_l <: \texttt{FIX[}\alpha\texttt{.}\,\tau_r\texttt{]} \dashv M_1, \Delta_1\ \tau_l <: \texttt{FIX[}\alpha\texttt{.}\,\tau_r\texttt{]}}$$

$$\frac{M, \Delta \vdash \tau_l <: \tau_r \,|\, \tau_n}{M, \Delta \vdash \tau_l \backslash \tau_n <: \tau_r} \qquad \frac{\begin{array}{c}\text{DF}(\tau_r \backslash \tau_n) \qquad \tau_l <: \tau_r \dashv M, \Delta \\ \forall M'\ \Delta'.\ M \preceq M' \implies \Delta \preceq \Delta' \implies \neg(\tau_l <: \tau_n \dashv M', \Delta')\end{array}}{\tau_l <: \tau_r \backslash \tau_n \dashv M, \Delta}$$

$$\frac{\tau_l <: \tau_r \dashv M, \Delta}{\sim l\ \ \tau_l <: \sim l\ \ \tau_r \dashv M, \Delta} \qquad \frac{\tau_l <: \tau_r \dashv M, \Delta}{l\texttt{:}\,\tau_l <: l\texttt{:}\,\tau_r \dashv M, \Delta}$$

$$\frac{\tau_{rl} <: \tau_{ll} \dashv M_0, \Delta_0 \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_{lr} <: \tau_{rr} \dashv M_1, \Delta_1}{\tau_{ll}\texttt{->}\tau_{lr} <: \tau_{rl}\texttt{->}\tau_{rr} \dashv M_1, \Delta_1}$$

Definition 6.9. $\boxed{\tau <: \tau \dashv Z}$ (Proof universe subtyping)

$$\frac{\langle M, \Delta\rangle \in Z \qquad \forall M\ \Delta.\ \tau_l <: \tau_r \dashv M, \Delta \iff \langle M, \Delta\rangle \in Z}{\tau_l <: \tau_r \dashv Z}$$

Definition 6.10. $\boxed{Q \dashv M, \Delta}$

$$\frac{Q \dashv M_0, \Delta_0 \qquad M_0 \preceq M_1 \qquad \Delta_0 \preceq \Delta_1 \qquad \tau_l <: \tau_r \dashv M_1, \Delta_1}{Q\texttt{.}\,\tau_l\texttt{<:}\,\tau_r \dashv M_1, \Delta_1} \qquad \frac{}{M, \Delta \vdash \epsilon}$$

Definition 6.11. (Collection)

$$C ::= \epsilon \mid C\ c$$

Definition 6.12. $\boxed{C \sqcup C = C}$

$$\begin{array}{rcll} C \sqcup \epsilon & = & C & \triangleright\ \textit{empty} \\ C \sqcup (C'\ c) & = & (C \sqcup C')\ c & \triangleright\ \textit{step} \end{array}$$

Definition 6.13. $\boxed{C \sqcap C = C}$

$$\begin{array}{rcll} C \sqcap \epsilon & = & \epsilon & \triangleright\ \textit{empty} \\ C \sqcap (C'\ c) & = & \begin{cases}(C \sqcap C')\ c & \text{if } c \in C \\ (C \sqcap C') & \text{otherwise}\end{cases} & \textsc{Step} \end{array}$$

Definition 6.14. $\boxed{\mathrm{map}(C, t) = C}$

$$\begin{array}{rcll} \mathrm{map}(\epsilon, t) & = & \epsilon & \triangleright \textit{ empty} \\ \mathrm{map}(C\ c, t) & = & \mathrm{map}(C, t) \sqcup t(c) & \triangleright \textit{ step} \end{array}$$

Definition 6.15. $\boxed{\overline{c}^{c \in C} \triangleq C}$

$$\overline{c'}^{c \in C} \triangleq \mathrm{map}(C, \lambda c.c') \quad \triangleright \textit{ comprehension}$$

Definition 6.16. $\boxed{c \in C}$

$$\frac{c \notin C}{c \in C\ c} \qquad \frac{c \in C}{c \in C\ c'}$$

Definition 6.17. $\boxed{C \preceq C}$

$$\frac{}{C \preceq C} \qquad \frac{C \preceq C'}{C \preceq C'\ c}$$

Definition 6.18. $\boxed{|(\mathrm{T}) = \tau}$

$$\begin{array}{rcll} |(\epsilon) & = & \texttt{BOT} & \triangleright \textit{ empty} \\ |(\mathrm{T}\ \tau) & = & |(\mathrm{T})|\tau & \triangleright \textit{ step} \end{array}$$

Definition 6.19. $\boxed{\&(\mathrm{T}) = \tau}$

$$\begin{array}{rcll} \&(\epsilon) & = & \texttt{TOP} & \triangleright \textit{ empty} \\ \&(\mathrm{T}\ \tau) & = & \&(\mathrm{T})\&\tau & \triangleright \textit{ step} \end{array}$$

Definition 6.20. $\boxed{M, \Delta, \Delta \vdash M \lessdot \alpha}$

$$\frac{}{M, \Delta, \epsilon \vdash \epsilon \lessdot \alpha} \qquad \frac{m \in M_0 \qquad M_0, \Delta_0, \Delta_1 \vdash M_1 \lessdot \alpha \qquad M_0, \Delta_0, \Delta_0 \vdash M_2 \lessdot m}{M_0, \Delta_0, \Delta_1\ m <: \alpha \vdash M_1 \sqcup M_2\ m \lessdot \alpha} \qquad \frac{\neg(\tau_l \in M_0 \wedge \tau_r = \alpha) \qquad M_0, \Delta_0, \Delta_1 \vdash M_1 \lessdot \alpha}{M_0, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash M_1 \lessdot \alpha}$$

Definition 6.21. $\boxed{M, \Delta, \Delta \vdash \mathrm{T} \ll \alpha}$

$$\frac{}{M, \Delta, \epsilon \vdash \epsilon \ll \alpha} \qquad \frac{\tau \notin M \qquad M, \Delta_0, \Delta_1 \vdash \mathrm{T} \ll \alpha}{M, \Delta_0, \Delta_1\ \tau <: \alpha \vdash \mathrm{T}\ \tau \ll \alpha}$$

$$\frac{m \in M \qquad M, \Delta_0, \Delta_1 \vdash \mathrm{T}_0 \ll \alpha \qquad M, \Delta_0, \Delta_0 \vdash \mathrm{T}_1 \ll z}{M, \Delta_0, \Delta_1\ m <: \alpha \vdash \mathrm{T}_0 \sqcup \mathrm{T}_1 \ll \alpha} \qquad \frac{\tau_r \neq \alpha \qquad M, \Delta_0, \Delta_1 \vdash \mathrm{T} \ll \alpha}{M, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \mathrm{T} \ll \alpha}$$

Definition 6.22. $\boxed{M, \Delta, \Delta \vdash \alpha \lessdot M}$

$$\frac{}{M, \Delta, \epsilon \vdash \alpha \lessdot \epsilon} \qquad \frac{m \in M_0 \qquad M_0, \Delta_0, \Delta_1 \vdash \alpha \lessdot M_1 \qquad M_0, \Delta_0, \Delta_0 \vdash m \lessdot M_2}{M_0, \Delta_0, \Delta_1\ \alpha <: m \vdash \alpha \lessdot M_1 \sqcup M_2\ m} \qquad \frac{\neg(\tau_r \in M_0 \wedge \tau_l = \alpha) \qquad M_0, \Delta_0, \Delta_1 \vdash \alpha \lessdot M_1}{M_0, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \alpha \lessdot M_1}$$

Definition 6.23. $\boxed{M, \Delta, \Delta \vdash \alpha \ll \mathrm{T}}$

$$\frac{}{M, \Delta, \epsilon \vdash \alpha \ll \epsilon} \qquad \frac{\tau \notin M \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \mathrm{T}}{M, \Delta_0, \Delta_1\ \alpha <: \tau \vdash \alpha \ll \mathrm{T}\ \tau}$$

$$\frac{m \in M \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \mathrm{T}_0 \qquad M, \Delta_0, \Delta_0 \vdash m \ll \mathrm{T}_1}{M, \Delta_0, \Delta_1\ \alpha <: m \vdash \alpha \ll \mathrm{T}_0 \sqcup \mathrm{T}_1} \qquad \frac{\tau_l \neq \alpha \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \mathrm{T}}{M, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \alpha \ll \mathrm{T}}$$

Definition 6.24. $\boxed{M, \Delta, \Delta \vdash \alpha \lessdot \Delta}$

$$\frac{}{M, \Delta, \epsilon \vdash \alpha \lessdot \epsilon} \qquad \frac{\alpha \in \mathrm{FTV}(\tau) \qquad m_0 \in M_0 \qquad M_0, \Delta_0, \Delta_1 \vdash \alpha \lessdot \Delta_2 \qquad M_0, \Delta_0, \Delta_0 \vdash m_0 \lessdot M_1}{M_0, \Delta_0 \vdash \Delta_1\ \tau <: m_0 \vdash \alpha \lessdot \Delta_2 \sqcup \overline{\tau <: m_1}^{m_1 \in M_1}\ \tau <: m_0}$$

$$\frac{\neg(\tau_r \in M_0 \wedge \alpha \in \mathrm{FTV}(\tau_l)) \qquad M_0, \Delta_0, \Delta_1 \vdash \alpha \lessdot \Delta_2}{M_0, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \alpha \lessdot \Delta_2}$$

Definition 6.25. $\boxed{M, \Delta, \Delta \vdash \alpha \ll \Delta}$

$$\frac{}{M, \Delta, \epsilon \vdash \alpha \ll \epsilon} \qquad \frac{\alpha \in \mathrm{FTV}(\tau_l) \qquad \tau \notin M \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \Delta_2}{M, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \alpha \ll \Delta_2\ \tau_l <: \tau_r}$$

$$\frac{\alpha \in \mathrm{FTV}(\tau) \qquad m \in M \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \Delta_2 \qquad M, \Delta_0, \Delta_0 \vdash z \ll \Delta_3}{M, \Delta_0, \Delta_1\ \tau <: z \vdash \alpha \ll \Delta_2 \sqcup \Delta_3} \qquad \frac{\alpha \notin \mathrm{FTV}(\tau_l) \qquad M, \Delta_0, \Delta_1 \vdash \alpha \ll \Delta_2}{M, \Delta_0, \Delta_1\ \tau_l <: \tau_r \vdash \alpha \ll \Delta_2}$$

Definition 6.26. $\boxed{M, \Delta, \mathrm{A} \vdash \Omega}$

$$\frac{}{M, \Delta, \epsilon \vdash \epsilon} \qquad \frac{\alpha \notin M \qquad \forall \tau.\ \tau <: \alpha \notin \Delta \qquad M, \Delta, A \vdash \Omega}{M, \Delta, A\ \alpha \vdash \Omega}$$

$$\frac{\alpha \notin M \qquad \exists \tau.\ \tau <: \alpha \in \Delta \qquad M, \Delta, \mathrm{A} \vdash \Omega}{M, \Delta, \mathrm{A}\ \alpha \vdash \Omega\ \alpha / \lfloor (\overline{\tau}^{\tau <: \alpha \in \Delta}) \rfloor}$$

Definition 6.27. $\boxed{N, M \vdash \Pi \equiv \mathrm{T}}$

$$\frac{}{N, M \vdash \epsilon \equiv \epsilon} \qquad \frac{\begin{array}{c} N, M \vdash \Pi \equiv \mathrm{T} \qquad \mathrm{FTV}(\tau_l) = A_l \qquad \mathrm{FTV}(\tau_r) = A_r \\ \Delta \vdash N \sqcup M \sqcup A_l \sqcup A_r \Uparrow \Delta' \qquad N, M, \Delta' \vdash \tau_l \text{->} \tau_r \equiv^{+} \tau \end{array}}{N, M \vdash \Pi\ \langle M, \Delta, \tau_l \text{->} \tau_r \rangle \equiv \mathrm{T}\ \tau}$$

Definition 6.28. $\boxed{N \vdash \alpha \circlearrowleft Z \cdot \alpha \text{->} \alpha \coloneqq \alpha \circlearrowright \mathrm{T}}$

$$\frac{}{N \vdash \alpha_0 \circlearrowleft \epsilon \cdot \alpha_1 \text{->} \alpha_2 \coloneqq \alpha_3 \circlearrowright \epsilon}$$

$$\frac{\begin{array}{c} M, \Delta, \Delta \vdash \alpha_1 <: \mathrm{T}_l \qquad M, \Delta, \Delta \vdash \mathrm{T}_r <: \alpha_2 \qquad (\&(\mathrm{T}_l), \lfloor(\mathrm{T}_r)) = \tau_p \\ \mathrm{FTV}(\tau_p) = \mathrm{A}_p \qquad \Delta \vdash N \sqcup M \sqcup A_p\ \alpha_3 \Uparrow \Delta_i \qquad N\ \alpha_3, M, \Delta_i \vdash \tau_p \equiv^{-} \tau \end{array}}{N \vdash \alpha_0 \circlearrowleft Z\ \langle M, \Delta \rangle \cdot \alpha_1 \text{->} \alpha_2 \coloneqq \alpha_3 \circlearrowright \mathrm{T}\ \tau}$$

Definition 6.29. $\boxed{\Delta \vdash N \Uparrow \Delta}$

$$\frac{}{\epsilon \vdash N \Uparrow \epsilon} \qquad \frac{\alpha \in N \qquad \alpha \in \mathrm{FTV}(\tau_l) \sqcup \mathrm{FTV}(\tau_r) \qquad \Delta \vdash N \Uparrow \Delta_i}{\Delta\ \tau_l <: \tau_r \vdash N \Uparrow \Delta_i\ \tau_l <: \tau_r}$$

$$\frac{\forall \alpha.\ \alpha \in N \implies \alpha \notin \mathrm{FTV}(\tau_l) \sqcup \mathrm{FTV}(\tau_r) \qquad \Delta \vdash N \Uparrow \Delta'}{\Delta\ \tau_l <: \tau_r \vdash N \Uparrow \Delta'}$$

Definition 6.30. $\boxed{M, \Delta \vdash \mathrm{T} <: \alpha}$

$$\frac{}{M, \epsilon \vdash \epsilon <: \alpha} \qquad \frac{\tau \notin M \qquad M, \Delta \vdash \mathrm{T} <: \alpha}{M, \Delta\ \tau <: \alpha \vdash \mathrm{T}\ \tau <: \alpha} \qquad \frac{\tau_r \neq \alpha \qquad M, \Delta \vdash \mathrm{T} <: \alpha}{M, \Delta\ \tau_l <: \tau_r \vdash \mathrm{T} <: \alpha}$$

Definition 6.31. $\boxed{M, \Delta \vdash \mathrm{T} <: \alpha}$

$$\frac{}{M, \epsilon \vdash \alpha <: \epsilon} \qquad \frac{\tau \notin M \qquad M, \Delta \vdash \alpha <: \mathrm{T}}{M, \Delta\ \tau <: \alpha \vdash \alpha <: \mathrm{T}\ \tau} \qquad \frac{\tau_r \neq \alpha \qquad M, \Delta \vdash \alpha <: \mathrm{T}}{M, \Delta\ \tau_l <: \tau_r \vdash \alpha <: \mathrm{T}}$$

Definition 6.32. $\boxed{\mathrm{outer}(+|-) = \texttt{ALL}|\texttt{EXI}}$

$$\begin{array}{rcll} \mathrm{outer}(+) & = & \texttt{EXI} & \triangleright \textit{ positive} \\ \mathrm{outer}(-) & = & \texttt{ALL} & \triangleright \textit{ negative} \end{array}$$

Definition 6.33. $\boxed{\mathrm{inner}(+|-) = \texttt{ALL}|\texttt{EXI}}$

$$\begin{array}{rcll} \mathrm{inner}(+) & = & \texttt{ALL} & \triangleright \textit{ positive} \\ \mathrm{inner}(-) & = & \texttt{EXI} & \triangleright \textit{ negative} \end{array}$$

Definition 6.34. $\boxed{\mathrm{quantify}^{+|-}(\mathrm{A}, \Delta, \mathrm{A}, \Delta, \tau) = \tau}$

$$\begin{array}{rcl} \mathrm{quantify}^{+|-}(\epsilon, \epsilon, \epsilon, \epsilon, \tau) & = & \tau \\ \mathrm{quantify}^{+|-}(\epsilon, \epsilon, \mathrm{A}_i, \Delta_i, \tau) & = & \mathrm{inner}(+|-)\,[\mathrm{A}_i\ \ \Delta_i]\,\tau \\ \mathrm{quantify}^{+|-}(\mathrm{A}_o, \Delta_o, \epsilon, \epsilon, \tau) & = & \mathrm{outer}(+|-)\,[\mathrm{A}_o\ \ \Delta_o]\,\tau \\ \mathrm{quantify}^{+|-}(\mathrm{A}_o, \Delta_o, \mathrm{A}_i, \Delta_i, \tau) & = & \mathrm{outer}(+|-)\,[\mathrm{A}_o\ \ \Delta_o]\,\mathrm{inner}(+|-)\,[\mathrm{A}_i\ \ \Delta_i]\,\tau \end{array}$$

Definition 6.35. $\boxed{\mathrm{A}, \mathrm{A}, \Delta \vdash \tau \equiv^{+|-} \tau}$

$$\frac{\begin{array}{c}\mathrm{A}_z, \Delta \vdash \Delta_o \wr \Delta_i \\ (\mathrm{FTV}(\Delta)\ \mathrm{FTV}(\tau)) \sqcap \mathrm{A}_z = \mathrm{A}_o \qquad (\mathrm{FTV}(\Delta_i)\ \mathrm{FTV}(\tau)) \setminus \mathrm{A}_z \setminus \mathrm{A}_r = \mathrm{A}_i \\ \mathrm{quantify}^{+|-}(\mathrm{A}_o, \Delta_o, \mathrm{A}_i, \Delta_i, \tau) = \tau'\end{array}}{\mathrm{A}_r, \mathrm{A}_z, \Delta \vdash \tau \equiv^{+|-} \tau'}$$

Definition 6.36. $\boxed{\mathrm{A}, \Delta \vdash \Delta \wr \Delta}$

$$\frac{}{\mathrm{A}_z, \epsilon \vdash \epsilon \wr \epsilon} \qquad \frac{\mathrm{FTV}(\tau_l)\ \mathrm{FTV}(\tau_r) = \mathrm{A}_q \qquad \forall \alpha.\ \alpha \in \mathrm{A}_q \implies \alpha \in \mathrm{A}_z \qquad \mathrm{A}_z, \Delta \vdash \Delta_o \wr \Delta_i}{\mathrm{A}_z, \Delta\ \tau_l <: \tau_r \vdash \Delta_o\ \tau_l <: \tau_r \wr \Delta_i}$$

$$\frac{\mathrm{FTV}(\tau_l)\ \mathrm{FTV}(\tau_r) = \mathrm{A}_q \qquad \alpha \in \mathrm{A}_q \qquad \alpha \notin \mathrm{A}_z \qquad \mathrm{A}_z, \Delta \vdash \Delta_o \wr \Delta_i}{\mathrm{A}_z, \Delta\ \tau_l <: \tau_r \vdash \Delta_o \wr \Delta_i\ \tau_l <: \tau_r}$$

Definition 6.37. $\boxed{e \textbf{ wellformed}}$

$$\frac{e = v}{e \textbf{ wellformed}} \qquad \frac{e \rightsquigarrow e' \qquad e' \textbf{ wellformed}}{e \textbf{ wellformed}}$$

Theorem 6.1. (Typing Soundness)

$$\frac{\vdash e : \tau \dashv Z}{e \textbf{ wellformed}}$$

Proof:
assume $\vdash e : \tau \dashv Z$
  let $\Omega\ \Gamma'\ \tau'$ **s.t.** $\Omega, \Gamma' \vDash e : \tau'$ by Lemma 6.2
  $\Omega, \Sigma \vDash \Gamma'$ by ...
  $e[\Sigma]$ **wellformed** by theorem 6.17
  $e[\Sigma] = e$ by ...
  e **wellformed** by substitution
□

Theorem 6.2. (Proof typing soundness)

$$\frac{\Gamma \vdash e : \tau \dashv Z \qquad \langle M, \Delta \rangle \in Z \qquad \langle M, \Delta \rangle \rightsquigarrow \Omega}{\Omega, \Gamma \vDash e : \tau}$$

Proof:
assume $\Gamma \vdash e : \tau \dashv Z \quad \langle M, \Delta \rangle \in Z \quad \langle M, \Delta \rangle \rightsquigarrow \Omega$
. **induct on** $\Gamma \vdash e : \tau \dashv Z$
. **case** $e = @ \quad \tau = @$
. . $\Omega, \Gamma \vDash @ : @$ by definition
. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. **case** $e = x \quad x : \tau \in \Gamma$
. **wrt** x
. . $\Omega, \Gamma \vDash x : \tau$ by definition
. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. **case** $\Gamma \vdash e' : \tau' \dashv Z \quad \tau = \sim l\ \ \tau' \quad e = \sim l\ \ e'$
. **hypo** $\Gamma \vdash e' : \tau' \dashv Z \implies \Omega, \Gamma \vDash e' : \tau'$
. **wrt** $e'\ \tau'$
. . $\Omega, \Gamma \vDash e' : \tau'$ by application
. . $\Omega, \Gamma \vDash \sim l\ \ e' : \sim l\ \ \tau'$ by definition
. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. **TODO: remaining trivial introduction cases**
. **case**
. **hypo**
. **wrt**
. **case** $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \quad Z_0 \nrightarrow Z_1 \quad \tau_0 <: l\text{->}\alpha \dashv Z_1 \quad e = e_0\,.\,l \quad \tau = \alpha \quad Z = Z_1$
. **hypo** $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \implies \Omega, \Gamma \vDash e_0 : \tau_0$
. **wrt** $e'\ l\ \alpha\ \tau_0\ Z_0\ Z_1$
. . $\Omega, \Gamma \vDash e_0 : \tau_0$ by application
. . $\langle M, \Delta \rangle \in Z_1$ by substitution
. . $\tau_0 <: l\text{->}\alpha \dashv M, \Delta$ by theorem 6.3
. . $\Omega \vDash \tau_0 <: l\text{->}\alpha$ by theorem 6.6

. . $\forall e\ \Gamma.\ \Omega, \Gamma \vDash e : \tau_0 \implies \Omega, \Gamma \vDash e : l\text{->}\alpha$ by theorem 6.4
. . $\Omega, \Gamma \vDash e_0 : \tau_0 \implies \Omega, \Gamma \vDash e_0 : l\text{->}\alpha$ by instantiation
. . $\Omega, \Gamma \vDash e_0 : l\text{->}\alpha$ by application
. . $\Omega, \Gamma \vDash e_0.l : \alpha$ by theorem 6.5
. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. **case** $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \quad Z_0 \hookrightarrow Z_1 \quad \Gamma \vdash e_1 : \tau_1 \dashv Z_1 \quad e = e_0(e_1) \quad \tau = \alpha \quad Z = Z_2$
. $Z_1 \hookrightarrow Z_2 \quad \tau_0 <: \tau_1\text{->}\alpha \dashv Z_2$
. **hypo** $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \implies \Omega, \Gamma \vDash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \dashv Z_1 \implies \Omega, \Gamma \vDash e_1 : \tau_1$
. **wrt** $e_0\ e_1\ \alpha\ \tau_0\ \tau_1\ Z_0\ Z_1\ Z_2$
. . $\Omega, \Gamma \vDash e_0 : \tau_0$ by application
. . $\Omega, \Gamma \vDash e_1 : \tau_1$ by application
. . $\langle M, \Delta \rangle \in Z_2$ by substitution
. . $\tau_0 <: \tau_1\text{->}\alpha \dashv \langle M, \Delta \rangle$ by theorem 6.3
. . $\Omega, \Gamma \vDash \tau_0 <: \tau_1\text{->}\alpha$ by theorem 6.6
. . $\forall e.\ \Omega, \Gamma \vDash e : \tau_0 \implies e : \tau_1\text{->}\alpha$ by theorem 6.4
. . $\Omega, \Gamma \vDash e_0 : \tau_0 \implies e_0 : \tau_1\text{->}\alpha$ by instantiation
. . $e_0 : \tau_1\text{->}\alpha$ by application
. . $\Omega, \Gamma \vDash e_0(e_1) : \alpha$ by theorem 6.8
. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. **case** $\Gamma \vdash e' : \tau' \dashv Z_0 \quad Z_0 \hookrightarrow Z_1 \quad \tau' <: \alpha_0\text{->}\alpha_1\text{->}\alpha_2 \dashv Z_1$
. $\mathrm{FTV}(\Gamma) \vdash \alpha_0 \circlearrowleft Z_1 \cdot \alpha_1\text{->}\alpha_2 \fallingdotseq \alpha_3 \circlearrowleft \mathrm{T}_{rel} \quad e = \texttt{fix(}e'\texttt{)}$
. $\tau = \texttt{ALL[}\alpha_4\texttt{]}\alpha_4\texttt{->EXI[}\alpha_5\texttt{.(}\alpha_4\texttt{,}\alpha_5\texttt{)<:FIX[}\alpha_3\texttt{.|(}\mathrm{T}_{rel}\texttt{)]]}\alpha_5$
. $Z = Z_1$
. **hypo** $\Gamma \vdash e' : \tau' \dashv Z_0 \implies \Omega, \Gamma \vDash e' : \tau'$
. **wrt** $e'\ \tau'\ \alpha_0 \ldots \alpha_5\ T_{rel}\ Z_0\ Z_1$
. . $\Omega, \Gamma \vDash e' : \tau'$ by application
. . $\langle M, \Delta \rangle \in Z_1$ by substitution
. . $\tau' <: \alpha_0\text{->}\alpha_1\text{->}\alpha_2 \dashv \langle M, \Delta \rangle$ by theorem 6.3
. . $\Omega \vDash \tau' <: \alpha_0\text{->}\alpha_1\text{->}\alpha_2$ by theorem 6.6
. . $\forall e.\ \Omega, \Gamma \vDash e : \tau' \implies \Omega\Gamma \vDash e : \alpha_0\text{->}\alpha_1\text{->}\alpha_2$ by theorem 6.4
. . $\Omega, \Gamma \vDash e' : \tau' \implies \Omega, \Gamma.\ e' : \alpha_0\text{->}\alpha_1\text{->}\alpha_2$ by instantiation
. . $\Omega, \Gamma \vDash e' : \alpha_0\text{->}\alpha_1\text{->}\alpha_2$ by application
. . $\Omega, \Gamma \vDash \texttt{fix(}e'\texttt{)} : \texttt{ALL[}\alpha_4\texttt{]}\alpha_4\texttt{->EXI[}\alpha_5\texttt{.(}\alpha_4\texttt{,}\alpha_5\texttt{)<:FIX[}\alpha_3\texttt{.|(}\mathrm{T}_{rel}\texttt{)]]}\alpha_5$ by theorem ??

TODO: ...

. . $\Omega, \Gamma \vDash e : \tau$ by substitution
. $\Omega, \Gamma \vDash e : \tau$ by induction

□

TODO: Cretin's corresponding theorem is Theorem 101 on p. 134
TODO: See how Cretin proves this without using subject reduction

Theorem 6.3. (Proof subtyping choice)

$$\frac{\tau_l <: \tau_r \dashv Z \qquad \langle M, \Delta \rangle \in Z}{\tau_l <: \tau_r \dashv M, \Delta}$$

Proof:

TODO: ...

□

Theorem 6.4. (Model subtyping inversion)

$$\frac{\Omega \vDash \tau_l <: \tau_r}{\forall e\ \Gamma.\ \Omega, \Gamma \vDash e : \tau_l \implies \Omega, \Gamma \vDash e : \tau_r}$$

Proof:
TODO: ...
$\forall e\ \Gamma.\ \Omega, \Gamma \vDash e : \tau_l \implies \Omega, \Gamma \vDash e : \tau_r$ by inversion
□

Theorem 6.5. (Model typing record elimination)

$$\frac{\Omega, \Gamma \vDash e : l\text{->}\tau}{\Omega, \Gamma \vDash e.l : \tau}$$

Proof:
assume $\Omega, \Gamma \vDash e : l\text{->}\tau$
. **induct on** $\Omega, \Gamma \vDash e : l\text{->}\tau$
. **case** $*l\text{=>}v \in G \quad \Omega, \Gamma \vDash v : \tau \quad \forall e'.\ *l\text{=>}e' \in G \implies e' = v \quad e = R$
. **wrt** $v\ R$
. . $\Omega, \Gamma \vDash G : l\text{->}\tau$ by substitution
. . $G.l \rightsquigarrow v$ by definition
. . $\exists \Sigma.\ \Omega, \Gamma \vDash \Sigma$ by theorem **??**
. . **let** Σ **s.t.** $\Omega, \Gamma \vDash \Sigma$ by declaration
. . $G.l[\Sigma] \rightsquigarrow v$ by definition
. . $G.l[\Sigma] \rightsquigarrow v[\Sigma \sqcup \epsilon]$ by definition
. . $\Omega, \epsilon \vDash \epsilon$ by definition
. . $\Omega, \Gamma \sqcup \epsilon \vDash v : \tau$ by definition
. . $\Omega, \Gamma \vDash G.l : \tau$ by definition
. . $\Omega, \Gamma \vDash e.l : \tau$ by substitution
. **case** $\Omega, \Sigma \vDash \Gamma \quad e[\Sigma] \rightsquigarrow e'[\Sigma \sqcup \Sigma'] \quad \Omega, \Sigma' \vDash \Gamma' \quad \Omega, \Gamma \sqcup \Gamma' \vDash e' : l\text{->}\tau$
. **hypo** $\Omega, \Gamma \sqcup \Gamma' \vDash e' : l\text{->}\tau \implies \Omega, \Gamma \sqcup \Gamma' \vDash e'.l : \tau$
. **wrt** $\Sigma\ e'\ \Sigma'\ \Gamma'$
. . $\Omega, \Gamma \sqcup \Gamma' \vDash e'.l : \tau$ by application
. . $e[\Sigma].l \rightsquigarrow e'[\Sigma \sqcup \Sigma'].l$ by definition
. . $e.l[\Sigma] \rightsquigarrow e'.l[\Sigma \sqcup \Sigma']$ by definition
. . $\Omega, \Gamma \vDash e.l : \tau$ by definition
. $\Omega, \Gamma \vDash e.l : \tau$ by induction
□

Theorem 6.6. (Proof subtyping soundness)

$$\frac{\tau_l <: \tau_r \dashv M, \Delta \qquad \langle M, \Delta \rangle \rightsquigarrow \Omega}{\Omega \vDash \tau_l <: \tau_r}$$

Proof:
TODO: ...
□

Theorem 6.7. (Model typing subsumption)

$$\frac{\Omega, \Gamma \vDash e : \tau_l \qquad \Omega, \Gamma \vDash \tau_l <: \tau_r}{\Omega, \Gamma \vDash e : \tau_r}$$

Proof:
assume $\Omega, \Gamma \vDash e : \tau_l \quad \Omega, \Gamma \vDash \tau_l <: \tau_r$
. **invert on** $\Omega, \Gamma \vDash \tau_l <: \tau_r$
. **case** $\forall e'.\ \Omega, \Gamma \vDash e' : \tau_l \implies \Omega, \Gamma \vDash e' : \tau_r$
. . $\forall e'.\ \Omega, \Gamma \vDash e' : \tau_l \implies \Omega, \Gamma \vDash e' : \tau_r$ by identity
. $\forall e'.\ \Omega, \Gamma \vDash e' : \tau_l \implies \Omega, \Gamma \vDash e' : \tau_r$ by inversion
. $\Omega, \Gamma \vDash e : \tau_l \implies \Omega, \Gamma \vDash e : \tau_r$ by instantiation
. $\Omega, \Gamma \vDash e : \tau_r$ by application
□

Theorem 6.8. (Model typing implication elimination)

$$\frac{\Omega, \Gamma \vDash e_0 : \tau_l \text{->} \tau_r \qquad \Omega, \Gamma \vDash e_1 : \tau_l}{\Omega, \Gamma \vDash e_0\,(e_1) : \tau_r}$$

Proof:
assume $\Omega, \Gamma \vDash e_0 : \tau_l \text{->} \tau_r \quad \Omega, \Gamma \vDash e_1 : \tau_l$
. **induct on** $\Omega, \Gamma \vDash e_0 : \tau_l \text{->} \tau_r$
. **case** $\Omega, \Gamma \sqcup \Gamma' \vDash p : \tau_l \quad \Omega, \Gamma \sqcup \Gamma' \vDash e : \tau_r$
. $F = \epsilon \vee \Omega, \Gamma \vDash F : \tau_l \text{->} \tau_r \quad e_0 = (F{*}p{=>}e)$
. **hypo** $\Omega, \Gamma \vDash F : \tau_l \text{->} \tau_r \implies \Omega, \Gamma \vDash F\,(e_1) : \tau_r$
. **wrt** $F\ p\ e\ \Gamma'$
. . $\exists \Sigma.\ \Omega, \Sigma \vDash \Gamma$ by theorem 6.16
. . **let** Σ **s.t.** $\Omega, \Sigma \vDash \Gamma$ by declaration
. . $e_1[\Sigma]$ **wellformed** by theorem 6.17
. . **induct on** $e_1[\Sigma]$ **wellformed**
. . **case** $e_1[\Sigma] = v_1$ **for** v_1
. . . $\Omega \vDash e_1[\Sigma] : \tau_l$ by theorem 6.10
. . . $\Omega \vDash v_1 : \tau_l$ by substitution
. . . **invert on** $F = \epsilon \vee \Omega, \Gamma \vDash F : \tau_l \text{->} \tau_r$
. . . **case** $F = \epsilon$
. . . . $\Omega, \Gamma \vDash (F{*}p{=>}e) : \tau_l \text{->} \tau_r$ by substitution
. . . . $\Omega, \Gamma \vDash F{*}p{=>}e : \tau_l \text{->} \tau_r$ by theorem 6.9
. . . . $\Omega, \Gamma \vDash *p{=>}e : \tau_l \text{->} \tau_r$ by substitution
. . . . $\exists \Sigma'.\ p \equiv v_1 \dashv \Sigma'$ by theorem 6.11
. . . . **let** Σ' **s.t.** $p \equiv v_1 \dashv \Sigma'$ by declaration
. . . . **for** e'
. . . . . $\neg\epsilon[\Sigma]\,(v_1) \rightsquigarrow e'$ by definition
. . . . . $\neg F[\Sigma]\,(v_1) \rightsquigarrow e'$ by substitution
. . . . $\forall e'.\ \neg F[\Sigma]\,(v_1) \rightsquigarrow e'$ by generalization
. . . . $(F[\Sigma]{*}p{=>}e[\Sigma])\,(v_1) \rightsquigarrow e[\Sigma][\Sigma']$ by definition
. . . . $(F[\Sigma]{*}p{=>}e[\Sigma])\,(v_1) \rightsquigarrow e[\Sigma \sqcup \Sigma']$ by theorem ?? **TODO: subbing with concat**
. . . . $(F{*}p{=>}e)\,[\Sigma]\,(v_1) \rightsquigarrow e[\Sigma \sqcup \Sigma']$ by definition
. . . . $(F{*}p{=>}e)\,[\Sigma]\,(e_1[\Sigma]) \rightsquigarrow e[\Sigma \sqcup \Sigma']$ by substitution
. . . . $((F{*}p{=>}e)\,(e_1))[\Sigma] \rightsquigarrow e[\Sigma \sqcup \Sigma']$ by definition
. . . . $\Omega, \Gamma \vDash (F{*}p{=>}e)\,(e_1) : \tau_r$ by definition
. . . **case** $\Omega, \Gamma \vDash F : \tau_l \text{->} \tau_r$
. . . . $\Omega, \Gamma \vDash F\,(e_1) : \tau_r$ by application
. . . . **let** e' **s.t.** $(F\,(e_1))[\Sigma] \rightsquigarrow e' \wedge \Omega, \Gamma \vDash e' : \tau_r$ by theorem 6.13

. . . . $((F{*}p{=>}e)(e_1))[\Sigma] \rightsquigarrow e'$ by definition
. . . . $\Omega, \Gamma \vDash (F{*}p{=>}e)(e_1) : \tau_r$ by definition
. . . $\Omega, \Gamma \vDash (F{*}p{=>}e)(e_1) : \tau_r$ by induction
. . **case** $e_1[\Sigma] \rightsquigarrow e_1'$ e_1' **wellformed**
. . **hypo** e_1' **wellformed** $\implies \Omega, \Gamma \vDash (F{*}p{=>}e)(e_1') : \tau_r$
. . **wrt** e_1'
. . . $\Omega, \Gamma \vDash (F{*}p{=>}e)(e_1') : \tau_r$ by application
. . . $(F{*}p{=>}e)[\Sigma](e_1[\Sigma]) \rightsquigarrow (F{*}p{=>}e)[\Sigma](e_1')$ by definition
. . . $\forall x.\ x \notin \mathbf{FV}(e_1')$ by theorem 6.14
. . . $e_1' = e_1'[\Sigma]$ by by theorem 6.15
. . . $(F{*}p{=>}e)[\Sigma](e_1[\Sigma]) \rightsquigarrow (F{*}p{=>}e)[\Sigma](e_1'[\Sigma])$ by substitution
. . . $((F{*}p{=>}e)(e_1))[\Sigma] \rightsquigarrow ((F{*}p{=>}e)(e_1'))[\Sigma]$ by definition
. . . $\Sigma \sqcup \epsilon = \Sigma$ by definition
. . . $((F{*}p{=>}e)(e_1))[\Sigma] \rightsquigarrow ((F{*}p{=>}e)(e_1'))[\Sigma \sqcup \epsilon]$ by substitution
. . . $\Gamma \sqcup \epsilon = \Gamma$ by definition
. . . $\Omega, \epsilon \vDash \epsilon$ by definition
. . . $\Omega, \Gamma \sqcup \epsilon \vDash (F{*}p{=>}e)(e_1')$ by substitution
. . . $\Omega, \Gamma \vDash (F{*}p{=>}e)(e_1) : \tau_r$ by definition
. . $\Omega, \Gamma \vDash (F{*}p{=>}e)(e_1) : \tau_r$ by induction
. . $\Omega, \Gamma \vDash e_0(e_1) : \tau_r$ by substitution
. **case** $\Omega, \Sigma \vDash \Gamma$ $e_0[\Sigma] \rightsquigarrow e_0'$ $\Omega, \Gamma \vDash e_0' : \tau_l \text{->} \tau_r$
. **hypo** $\Omega, \Gamma \vDash e_0' : \tau_l \text{->} \tau_r \implies \Omega, \Gamma \vDash e_0'(e_1) : \tau_r$
. **wrt** Σ e_0'
. . $\Omega, \Gamma \vDash e_0'(e_1) : \tau_r$ by application
. . $e_0[\Sigma](e_1) \rightsquigarrow e_0'(e_1)$
. . $(e_0(e_1))[\Sigma] \rightsquigarrow e_0'(e_1)$
. . $\Omega, \Gamma \vDash e_0(e_1) : \tau_r$
. $\Omega, \Gamma \vDash e_0(e_1) : \tau_r$ by induction
□

Theorem 6.9. (Model typing unwrapping)

$$\frac{\Omega, \Gamma \vDash (e) : \tau}{\Omega, \Gamma \vDash e : \tau}$$

Proof:
assume $\Omega, \Gamma \vDash (e) : \tau$
TODO: ...
□

Theorem 6.10. (Model typing valuation)

$$\frac{\Omega, \Gamma \vDash e : \tau \qquad \Omega, \Sigma \vDash \Gamma}{\Omega \vDash e[\Sigma] : \tau}$$

Proof:
assume $\Omega, \Gamma \vDash e : \tau$ $\Omega, \Sigma \vDash \Gamma$
TODO: ...
□

Theorem 6.11. (Model typing pattern matching)

$$\frac{\Omega, \Gamma \vDash *p{=>}e : \tau_l \text{->} \tau_r \qquad \Omega \vDash v : \tau_l}{\exists \Sigma.\ p \equiv v \dashv \Sigma}$$

Proof:
assume $\Omega, \Gamma \vDash *p{=>}e : \tau_l \text{->} \tau_r \quad \Omega \vDash v : \tau_l$
TODO: ...
□

Theorem 6.12. (Well-formed function valuation)

$$\frac{F \textbf{ wellformed}}{\exists v.\ v = F}$$

Proof:
assume F **wellformed**
. **invert on** F **wellformed**
. **case** $v = F$
. . $v = F$ by identity
. **case** $F \rightsquigarrow e$
. **wrt** e
. . $\neg F \rightsquigarrow e$ by definition
. . $\bot$ by application
. $v = F$ by inversion
□

Theorem 6.13. (Model typing function progress)

$$\frac{\Omega, \Gamma \vDash F(e) : \tau_r}{\exists e'.\ F(e) \rightsquigarrow e' \wedge \Omega, \Gamma \vDash e' : \tau_r}$$

Proof:
assume $\Omega, \Gamma \vDash F(e) : \tau_r$
. **invert on** $\Omega, \Gamma \vDash F(e) : \tau_r$
. **case** ...
. **TODO: vacuous cases**
. **case** $F(e) \rightsquigarrow e' \quad \Omega, \Gamma \vDash e' : \tau_r$
. **wrt** e'
. . $F(e) \rightsquigarrow e' \wedge \Omega, \Gamma \vDash e' : \tau_r$ by conjunction
. . $\exists e'.\ F(e) \rightsquigarrow e' \wedge \Omega, \Gamma \vDash e' : \tau_r$ by witness
. $\exists e'.\ F(e) \rightsquigarrow e' \wedge \Omega, \Gamma \vDash e' : \tau_r$ by inversion
□

Theorem 6.14. (Reduction closed)

$$\frac{e \rightsquigarrow e'}{\forall x.\ x \notin \mathbf{FV}(e')}$$

Proof:
assume $e \rightsquigarrow e'$
TODO: ...
□

Theorem 6.15. (Closed substitution)

$$\frac{\forall x.\ x \notin \mathbf{FV}(e)}{e = e[\Sigma]}$$

Proof:
assume $\forall x.\ x \notin \mathbf{FV}(e)$
TODO: ...
□

Theorem 6.16. (Model typing assignability)

$$\frac{\Omega, \Gamma \vDash e : \tau}{\exists \Sigma.\ \Omega, \Sigma \vDash \Gamma}$$

Proof:
TODO: ...

Theorem 6.17. (Model typing soundness)

$$\frac{\Omega, \Sigma \vDash \Gamma \qquad \Omega, \Gamma \vDash e : \tau}{e[\Sigma]\ \mathbf{wellformed}}$$

Proof:
assume $\Omega, \Sigma \vDash \Gamma \quad \Omega, \Gamma \vDash e : \tau$
. **case** $e = @$
. . **let** v **s.t.** $@ = v$
. . $e[\Sigma] = v$
. . $e[\Sigma]$ **wellformed**
. **case** $\Omega, \Gamma \vDash e' : \tau' \quad e = \sim l\ e' \quad \tau = \sim l\ \tau'$
. . e' **wellformed** by induction hypothesis
. . **case** $e'[\Sigma] = v$
. . . **let** v' **s.t.** $\sim l\ v = v'$
. . . $\sim l\ e'[\Sigma] = v'$
. . . $(\sim l\ e')[\Sigma] = v'$
. . . $e[\Sigma] = v'$
. . . $e[\Sigma]$ **wellformed**
. . **case** $e'[\Sigma] \rightsquigarrow e'' \quad e''$ **wellformed**
. . . $\sim l\ e'[\Sigma] \rightsquigarrow \sim l\ e''$
. . . $\sim l\ e''$ **wellformed**
. . . $\sim l\ e'[\Sigma]$ **wellformed**
. . . $(\sim l\ e')[\Sigma]$ **wellformed**
. . . $e[\Sigma]$ **wellformed**
. . $e[\Sigma]$ **wellformed** by cases on e' **wellformed**
. **TODO: remaining introduction cases**
. **case** $x : \tau \in \Gamma \quad x/v \in \Sigma \quad e = x$
. . $x[\Sigma] = v$
. . $e[\Sigma] = v$
. . $e[\Sigma]$ **wellformed**
. **case** $e[\Sigma] \rightsquigarrow e' \quad \Omega, \Gamma \vDash e' : \tau$
. . $e'[\Sigma]$ **wellformed** by induction hypothesis
. . $e[\Sigma]$ **wellformed**

. $e[\Sigma]$ **wellformed** by induction on $\Omega, \Gamma \vDash e : \tau$

□

TODO: Cretin's corresponding theorem is by definition of pretypes on p. 125

NOTE: The induction hypothesis includes the generalized assumption, e.g. $\forall e'.\ e' < e \implies Q(e')$ if inducting on e or $\forall e'.\ (P(e') \implies P(e)), P(e') \implies Q(e')$ if inducting on predicate P

NOTE: we induct on $\Omega, \Gamma \vDash e : \tau$ instead of e, as the predicate acts as a guard/ordering in lieu of a decreasing e. This allows us to use the induction hypothesis on the reduction step result in the elimination case.

NOTE: Kozen says, "Intuitively, one can appeal to the coinductive hypothesis as long as there has been progress in observing the elements of the stream (guardedness) and there is no further analysis of the tails (opacity)". Kozen demonstrates a legal proof by induction on infinite streams too

Definition 6.38. $\boxed{\Omega, \Gamma \vDash e : \tau}$ (Model Typing)

$$\frac{\alpha/\tau \in \Omega \qquad \Omega, \Gamma \vDash e : \tau}{\Omega, \Gamma \vDash e : \alpha} \qquad \frac{}{\Omega, \Gamma \vDash @ : @} \qquad \frac{\Omega, \Gamma \vDash v : \tau}{\Omega, \Gamma \vDash \sim l\ \ v : \sim l\ \ \tau} \qquad \frac{*l{=>}v \in G \qquad \Omega, \Gamma \vDash e : \tau \qquad \forall e.\ *l{=>}e \in G \implies e = v}{\Omega, \Gamma \vDash G : l\text{->}\tau}$$

$$\frac{F = \epsilon \vee \Omega, \Gamma \vDash F : \tau_l\text{->}\tau_r \qquad \Omega, \Gamma \sqcup \Gamma' \vDash p : \tau_l \qquad \Omega, \Gamma \sqcup \Gamma' \vDash e : \tau_r}{\Omega, \Gamma \vDash F{*}p{=>}e : \tau_l\text{->}\tau_r} \qquad \frac{\Omega, \Gamma \vDash e : \tau_l}{\Omega, \Gamma \vDash e : \tau_l \,|\, \tau_r}$$

$$\frac{\Omega, \Gamma \vDash e : \tau_r}{\Omega, \Gamma \vDash e : \tau_l \,|\, \tau_r} \qquad \frac{\Omega, \Gamma \vDash e : \tau_l \qquad \Omega, \Gamma \vDash e : \tau_r}{\Omega, \Gamma \vDash e : \tau_l \& \tau_r} \qquad \frac{\Omega, \Gamma \vDash e : \tau_l \qquad \neg\, (\Omega, \Gamma \vDash e : \tau_r)}{\Omega, \Gamma \vDash e : \tau_l \backslash \tau_r}$$

$$\frac{\Omega \sqcup \Omega' \vDash Q \qquad \Omega \sqcup \Omega' \vDash e : \tau}{\Omega \vDash e : \texttt{EXI[A}\ Q\texttt{]}\tau} \qquad \frac{\forall \Omega'.\ \Omega \sqcup \Omega' \vDash Q \implies \Omega \sqcup \Omega', \Gamma \vDash e : \tau}{\Omega, \Gamma \vDash e : \texttt{ALL[A}\ Q\texttt{]}\tau}$$

$$\frac{\Omega\ \alpha/\texttt{FIX[}\alpha\texttt{.}\tau\texttt{]} \vDash e : \tau}{\Omega, \Gamma \vDash e : \texttt{FIX[}\alpha\texttt{.}\tau\texttt{]}} \qquad \frac{x : \tau \in \Gamma}{\Omega, \Gamma \vDash x : \tau}$$

$$\frac{\Omega, \Sigma \vDash \Gamma \qquad e[\Sigma] \rightsquigarrow e'[\Sigma \sqcup \Sigma'] \qquad \Omega, \Sigma' \vDash \Gamma' \qquad \Omega, \Gamma \sqcup \Gamma' \vDash e' : \tau}{\Omega, \Gamma \vDash e : \tau}$$

Definition 6.39. $\boxed{\Omega, \Sigma \vDash \Gamma}$

$$\frac{}{\Omega, \Sigma \vDash \epsilon} \qquad \frac{\Omega, \Sigma \vDash \Gamma \qquad \Omega \vDash v : \tau}{\Omega, \Sigma\ x/v \vDash \Gamma\ x : \tau}$$

Definition 6.40. $\boxed{\Omega \vDash \tau <: \tau}$

$$\frac{\forall e\ \Gamma.\ \Omega, \Gamma \vDash e : \tau_l \implies \Omega, \Gamma \vDash e : \tau_r}{\Omega \vDash \tau_l <: \tau_r}$$

Definition 6.41. $\boxed{\Omega \vDash Q}$

$$\frac{}{\Omega \vDash \epsilon} \qquad \frac{\Omega \vDash Q \qquad \Omega \vDash \tau_l <: \tau_r}{\Omega \vDash Q\ .\tau_l{<:}\tau_r}$$