

Extrinsic Relational Subtyping

ACM Reference Format:

. 2025. Extrinsic Relational Subtyping. 1, 1 (January 2025), 38 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. However, one of the drawbacks of intrinsically typed languages is that they prevent reusing of constructors in contexts that are less precise than their intrinsic specifications. For instance, a *cons* constructor belonging to a list datatype could not be considered amongst a *leaf* constructor defined as belong to a tree datatype. The user would have to define a new datatype that includes both isomorphs of both *cons* and *leaf* and also write functions that translate between the isomorphs and the list and tree constructors. This not only bloats the codebase, but hurts either the runtime or compiler performance.

For various reasons that may include the reusability drawbacks, intrinsically typed languages have lost favor, and untyped or *extrinsically typed* languages, such as Javascript and Python, have increased 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

Author's address:

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM XXXX-XXXX/2025/1-ART

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

a precise type based on how constructors are used. Since the way constructors are use may overlap in 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.

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 the limitations of intrinsic type systems and expand the kinds of programs and types that can be type checked, 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

TODO: mention somewhere 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.

For a given program, type inference constructs a very precise type. Some programs are simple enough such that type inference generates singleton types.

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)

TODO: break example program into parts; inline instead of using figure

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

Path typing. Consider the function `talky`, which completes a simple English phrase:

```
let talky = (
  $ <hello> @ => <world> @
  $ <good> @ => <morning> @
  $ <thank> @ => <you> @
)
```

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

```
TOP
& (<hello> @ -> <world> @)
& (<good> @ -> <morning> @)
& (<thank> @ -> <you> @)
```

Essentially, the program is so simple, that its type has the exact same meaning merely dressed in a different syntax.

Output broadening. Consider the application `talky(x)` where `x` has the type `(<hello> @) | (<thank> @)`. Type inference breaks apart the function type's intersection into paths and constructs the strongest output type possible by expanding the output type for each viable path. Since only two of the three paths match the type of the argument, type inference determines the type of the application to be the type `(<world> @) | (<you> @)`. Broadening from the bottom up contrasts with refinement type systems, which start from the weakest type intrinsic to the constructors and refines down to a stronger type through intersections of types or conjunctions of qualifiers.

Relational typing. Consider the function `repeat` that takes a natural number and returns a list of whose length is that number.

```
let repeat = $ x => loop($ self =>
  $ <zero> @ => <nil> @
  $ <succ> n => <cons>(x,self(n))
)
```

Without specifying any requirements besides the function definition, type inference lifts the function into the definitional property as a type. To construct the type, type inference constructs a relation between nats and lists. The type of `repeat` depends on a least fixed point relation between nats and lists (parametrically named here for readability).

```
natList( $\alpha$ ) = LFP[R]( BOT
  | (<zero> @)*(<nil> @)
  | (EXI[N L ; N*L <: R](<succ> N)*(<cons> ( $\alpha$ *L))
)
```

Using the `natList` relation, type inference then lifts the function `repeat` into its precise type form.

```
ALL[T] T -> ALL[X] X -> EXI[Y ; X*Y <: natList(T)] Y
```

It may be worth noting that there could be semantically equivalent recursive type in terms of intersections instead of unions.

TODO: forward reference to correctness/model semantics

```
ALL[T] GFP[R]( TOP
  & (<zero> @) -> (<nil> @)
  & (ALL[N L ; R <: N->L] (<succ> N) -> (<cons> T*L)
)
```

Type inference reasons in terms least fixed points, but the greatest fixed point form could be handled with syntactic sugar and rewriting.

Using the precise type form, type inference can leverage solving and checking subtyping constraints to reason in a number ways: it can reason forward from inputs to outputs (just like the runtime semantics), reason backwards from outputs to inputs (like Prolog), and check against weaker specifications.

Fixed point forward broadening. Consider the application `repeat(<succ> <succ> <zero> @)(x)` where `x` has type `T`. Type inference constructs a singleton type, mirroring the results achieved by simply running the program.

```
<cons> T * <cons> T * <nil> @
```

Fixed point backwards broadening. Now suppose we have a function `foo` whose input type is inferred to be an empty list or a singleton list, `<nil> @ | <cons> T * <nil> @`. Given the application `foo(repeat(n)(x))` where `x` has type `T`, type inference can reason backwards to learn that the type of `n` must be either zero or one.

```
<zero> @ | <succ> <zero> @
```

Vertical weakening (Factoring). Now suppose we have a function `woo` whose input type is inferred to be a list over elements of type `T`.

```
LFP[R]( BOT
  | <nil> @
  | <cons> T*R
)
```

Given the application `woo(repeat(n)(x))` where `x` has type `T`, type inference discovers that the argument type depends on the relation `natList(T)`, and the relation can be factored into a weaker cross product of nats and lists. Therefore, the argument meets the requirements of `woo` and the type of `n` must be the natural numbers.

```
LFP[R]( BOT
  | <zero> @
  | <succ> R
)
```

Horizontal weakening (infilling). Now consider a function `boo` whose input type is the natural numbers. Suppose we have the application `boo(n)` where `n` guaranteed to be an even number.

```
LFP[R]( BOT
  | <zero> @
  | <succ> <succ> R
)
```

The application requires that type inference check that the `nat` type is weaker than the `even` type. Type inference sees that if both types were to unroll into an infinite sequence of values every value in `nat` would also be in `even`, therefore the application type checks. In particular, type inference leverages the inductive hypothesis, by learning that weaker types hold for all the recursive constraints of the stronger type. In the case simple recursive types as shown above, the inductive hypothesis is merely a subtyping constraint on a single variable. In the case of comparing two relations such as `natList(T)` and a corresponding `even` version, the inductive hypothesis would be a subtyping constraint on a pair of variables, which may not be decomposable into constraints on single variables, so type inference must learn relational constraints, in addition to simple constraints.

Input refinement. Consider two functions: `uno` of type $U \rightarrow V$ and `dos` of type $D \rightarrow E$. Now suppose these two functions are called on the same variable, e.g. `(uno(x), dos(x))`. Type inference learns that the type of `x` can be no weaker than the intersection of the functions' input types: $U \& D$.

Path sensitivity. Consider the function `max` that chooses the maximum of two natural numbers.

```
let lessOrEq = loop($ self =>
  $ (<zero> @), y => <true> @
  $ (<succ> x), (<succ> y) => self(x,y)
  $ (<succ> x), (<zero> @) => <false> @
) in
let max = $ (x,y) =>
  if lessOrEq(x,y) then y else x
```

The function `max` must satisfy the property that the result is greater or equal to each of the inputs. Type inference must learn constraints on the inputs to `max`: `x` and `y`, which depends on the output of `lessOrEq(x,y)`. The application `lessOrEq(x,y)` can evaluate to either `<true>@` or `<false>@`, which result from different paths taken in `lessOrEq`. Type inference considers both cases and maintains the learned constraints exist in different possible worlds, since they are learned from different paths. Finally, type inference connects the inputs to the outputs by considering the two possible paths of the `if-then-else`. It first lifts the function `lessOrEq` into a relational type. For readability, we name the relational type LED (as in "less than or equal decision").

```
LED = LFP[R] ( BOT
  | (EXI [Y] ((<zero> @)*Y)*(<true> @))
  | (EXI [X Y D ; ((X*Y)*Z) <: R] ((<succ> X)*(<succ> Y))*D)
  | (EXI [X] ((<succ> X)*(<zero> @))*(<false> @))
)
```

using the LED relation, type inference combines the constraints learned for each possible world and combines them into a function type with multiple paths.

```
TOP
& (EXI [D ; D <: (<true> @)]
  (ALL [X Y Z ; Y <: Z ; ((X*Y)*D) <: LED] (X,Y) -> Z))
& (EXI [D ; D <: (<false> @)]
  (ALL [X Y Z ; X <: Z ; ((X*Y)*D) <: LED] (X,Y) -> Z))
```

We could simplify the type by eliminating simple constraints without loss of safety or precision:

```
TOP
& (ALL [X Y ; ((X*Y)*(<true> @)) <: LED] (X,Y) -> Y)
& (ALL [X Y ; ((X*Y)*(<false> @)) <: LED] (X,Y) -> X)
```

However, we have not included this rewriting in the semantics or implementation.

TODO: show type generated from code

TODO: more motivating and elucidating examples

3 DYNAMIC SEMANTICS

The programming language is pure and applicative. A program is an expression of the form in Definition 3.1. The forms of expressions enable function abstraction, function application, tagged constructions, record construction, record projection, and pattern matching. These forms enable us to express non-trivial programs. They also allow for compositions that have no reasonable semantics.

Definition 3.1. Expressions

$$\begin{aligned}
 e &::= x \mid @ \mid \langle l \rangle e \mid \vec{r} \mid \vec{f} \mid e.l \mid e(e) \mid \text{loop}(e) \mid \dots \\
 \vec{r} &::= \epsilon \mid \vec{r} r \\
 r &::= \$l \Rightarrow e \\
 \vec{f} &::= \epsilon \mid \vec{f} f \\
 f &::= \$p \Rightarrow e \\
 p &::= x \mid @ \mid \langle l \rangle p \mid \vec{k} \\
 \vec{k} &::= \epsilon \mid \vec{k} k \\
 k &::= \$l \Rightarrow p
 \end{aligned}$$

Progression of an expression, in Definition 3.2, is a small-step operational semantics. It adheres to typical definitions of applicative languages for the most part. One slight departure is that pattern matching is merely a special case of function application. Likewise, a switch is merely a function abstraction. Records are similar to Functions, except that their entries are guarded by literal identifiers. Additionally, records may be abstracted as patterns, but functions may not. The semantics enables recursion via the fixed point combinator `loop`.

Definition 3.2. $e \rightsquigarrow e'$ Progression

$$\begin{array}{c}
 \frac{e \rightsquigarrow e'}{\langle l \rangle e \rightsquigarrow \langle l \rangle e'} \quad \frac{e \rightsquigarrow e'}{\vec{r} \$l \Rightarrow e \rightsquigarrow \vec{r} \$l \Rightarrow e'} \quad \frac{\vec{r} \rightsquigarrow \vec{r}'}{\vec{r} \$l \Rightarrow v \rightsquigarrow \vec{r}' \$l \Rightarrow v} \quad \frac{e \rightsquigarrow e'}{e.l \rightsquigarrow e'.l} \\
 \\
 \frac{\$l \Rightarrow v \in \vec{g} \quad \forall e. \$l \Rightarrow e \in \vec{g} \implies e = v}{\vec{g}.l \rightsquigarrow v} \quad \frac{e_f \rightsquigarrow e'_f}{e_f(e) \rightsquigarrow e'_f(e)} \quad \frac{e \rightsquigarrow e'}{\vec{f}(e) \rightsquigarrow \vec{f}(e')} \\
 \\
 \frac{\vec{f}(v) \rightsquigarrow e' \quad \text{FV}(e) \subseteq \text{FV}(p)}{(\vec{f} \$p \Rightarrow e)(v) \rightsquigarrow e'} \quad \frac{\exists e'. \vec{f}(v) \rightsquigarrow e' \quad p \equiv v \dashv \vec{\sigma}}{(\vec{f} \$p \Rightarrow e)(v) \rightsquigarrow e[\vec{\sigma}]} \quad \frac{e \rightsquigarrow e'}{\text{loop}(e) \rightsquigarrow \text{loop}(e')} \\
 \\
 \frac{}{\text{loop}(\$x \Rightarrow e) \rightsquigarrow e[x/\text{loop}(\$x \Rightarrow e)]}
 \end{array}$$

4 STATIC SEMANTICS

The static semantics is a system for checking if the construction of an expression is viable. The system leverages types of the forms in Definition 4.1, which allow expressing properties of expressions with varying levels of precisions.

Definition 4.1. Types

$$\begin{aligned}
\tau &::= \alpha \mid @ \mid \langle l \rangle \tau \mid l \rightarrow \tau \mid \tau \rightarrow \tau \mid \tau \mid \tau \mid \tau \& \tau \mid \tau \setminus \eta \mid &> \text{type} \\
&\quad \text{EXI}[\vec{\alpha} \Delta] \tau \mid \text{ALL}[\vec{\alpha} \Delta] \tau \mid \text{LFP}[\alpha] \tau \\
\eta &::= \text{EXI}[\vec{\alpha} \Delta] \phi \mid \phi &> \text{negative type} \\
\phi &::= \alpha \mid @ \mid \langle l \rangle \phi \mid l \rightarrow \phi \mid \phi \& \phi \mid &> \text{pattern type} \\
\vec{\alpha} &::= \epsilon \mid \vec{\alpha} \alpha &> \text{type sequence} \\
\Delta &::= \epsilon \mid \Delta ; \tau <: \tau &> \text{subtyping environment}
\end{aligned}$$

Proof typing, in Definition 4.2, checks the viability of an expression's form. Additionally, by extending the forms of expressions with type annotations, as in Definition 8.2, proof typing is also able to check that expressions meet abstract specifications. In order to check the viability of constructions and specifications, proof typing lifts expressions into types and leverages subtyping to check compatibility between types. The proof typing predicate represents a typing that holds under the assumptions of a typing environment, and a world, where a world consists of emphclosed type variables and subtyping constraints.

Whether a variable is a closed or not represents how a variable is quantified.

If proof typing holds, then its typing holds under every interpretation of its closed type variables under some interpretation of its open variables. We formalize this soundness claim in Section 5.

The proof typing predicate ($\Gamma \vdash e : \tau \dashv \Omega'$) can be interpreted as an algorithm that takes a typing environment Γ , an expression e , and a world Ω as inputs and returns a type and a world Ω' as outputs, such that the output world is an extension of the input world ($\Omega \preceq \Omega'$). The input world is not explicitly represented in the predicate, so the algorithm interprets the input world as the smallest world that can satisfy the predicate. Additionally, the outputs of the predicate are not deterministic. Therefore, the algorithm enumerates all possible outputs.

Rule 4.2.1. The unit case simply returns a singleton set with the unit type and the environments unchanged.

Rule 4.2.2. 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.

Rule 4.2.3. The tag case infers the type of its constituent type and uses its label to construct a tag type.

Rule 4.2.4. The record case infers the type of its fields and intersects the constructed field types together.

Rule 4.2.5. 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. 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.

Rule 4.2.6. 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 type of a record is an intersection of field types.

Rule 4.2.7. 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.

Rule 4.2.8. The recursive 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 an inductive hypothesis, while the consequent represents an 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.

Rule 4.2.9. 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.

Definition 4.2. $\boxed{\Gamma \vdash e : \tau \dashv \Omega}$ Proof Typing

$$\begin{array}{c}
\frac{}{\Gamma \vdash @ : @ \dashv \Omega} [1] \quad \frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau \dashv \Omega} [2] \quad \frac{\Gamma \vdash e : \tau \dashv \Omega}{\Gamma \vdash \langle l \rangle e : \langle l \rangle \tau \dashv \Omega} [3] \\
\\
\frac{\Gamma \vdash R : \tau_0 \dashv \Omega \quad \Gamma \vdash e : \tau_1 \dashv \Omega' \quad \Omega \preceq \Omega'}{\Gamma \vdash R \$l \Rightarrow e : \tau_0 \& l \dashv \tau_1 \dashv \Omega'} [4] \quad \frac{\vec{\alpha}, \Delta, \Gamma \vdash \vec{f} \blacktriangle \vec{\pi}, \vec{\eta} \quad \Gamma \vdash \vec{\pi} \cong \vec{\tau}}{\Gamma \vdash \vec{f} : \text{inter}(\vec{\tau}) \dashv \vec{\alpha}, \Delta} [5] \\
\\
\frac{\Gamma \vdash e : \tau_0 \dashv \Omega \quad \tau_0 <: l \dashv \alpha \dashv \Omega' \quad \Omega \preceq \Omega'}{\Gamma \vdash e.l : \alpha \dashv \Omega'} [6] \quad \frac{\Gamma \vdash e_0 : \tau_0 \dashv \Omega \quad \Gamma \vdash e_1 : \tau_1 \dashv \Omega' \quad \Omega \preceq \Omega' \quad \tau_0 <: \tau_1 \dashv \alpha \dashv \Omega'' \quad \Omega' \preceq \Omega''}{\Gamma \vdash e_0(e_1) : \alpha \dashv \Omega''} [7] \\
\\
\frac{\begin{array}{c} \Gamma \vdash e : \alpha^+ \dashv \tau \dashv \vec{\alpha}, \Delta \\ \forall \vec{\alpha}' \Delta'. (\vec{\alpha} \vec{\alpha}', \Delta \Delta') \in \vec{\Omega} \implies \tau <: \alpha_l \dashv \alpha_r \dashv \vec{\alpha} \vec{\alpha}', \Delta \Delta' \\ \exists \Omega. \Omega \in \vec{\Omega} \quad \text{FTV}(\Gamma) \vdash \nu \alpha^+. \vec{\Omega}. \alpha_l \rightarrow \alpha_r \equiv \mu \alpha^-. \vec{\tau} \end{array}}{\Gamma \vdash \text{loop}(e) : \text{ALL}[\alpha_x] \alpha_x \dashv \text{EXI}[\alpha_y; \alpha_x * \alpha_y <: \text{LFP}[\alpha^-] \text{union}(\vec{\tau})] \alpha_y \dashv \vec{\alpha}, \Delta} [8] \\
\\
\frac{\begin{array}{c} \Gamma \vdash e : \tau \dashv \Omega \quad \tau <: \tau_a \dashv \Omega' \quad \Omega \preceq \Omega' \\ \Gamma x : \tau_x \vdash e' : \tau' \dashv \Omega'' \quad \Omega' \preceq \Omega'' \end{array}}{\Gamma \vdash \text{let } x : \tau_a = e \text{ in } e' : \tau' \dashv \Omega''} [9]
\end{array}$$

Proof subtyping, of definition 4.3, checks the viability of one type subtyping another type.

TODO: explain the overall predicate

TODO: explain the algorithmic interpretation 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.

Due to the complexity of types along with two positions for types to occur in subtyping, there are many rules needed to define the proof system of subtyping. For clarity, we show only a subset of the rules in this section in order to explain the essence of the system. We leave the remaining rules in the appendix, section 8, definition 8.6. The remaining rules include duals and other forms that adhere to similar proof strategies as the rules shown here, as well as additional rules for increased precision.

Rule 4.3.1. reflexivity up to alpha renaming.

Rule 4.3.2. left union.

Rule 4.3.3. Left Existential.

The left existential rule checks that subtyping holds for all variations of the payload where the subtyping constraint holds.

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.

dual of right universal. The right universal rule checks that subtyping holds for all variations of the payload consistent with the variable's upper bound.

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.

This is analogous to declaring a variable from an existential statement, or generalizing from an arbitrary variable to a universal statement. to choose a particular interpretation.

Rule 4.3.4. left closed variable.

Rule 4.3.5. right open variable.

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.

Rule 4.3.6. The right existential rule checks that subtyping holds for some variation of the payload where the constraint holds.

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.

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.

dual of left universal rule checks that subtyping holds for some variation of the payload consistent with the variable's upper bound.

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.

It is analogous to how variables are used in predicate logic proofs. For a universal assumption, or an existential conclusion, the prover is free to choose an interpretation for a variable.

Rule 4.3.7. right left union

Rule 4.3.8. right right union

Rule 4.3.9. left least fixed point.

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.

Rule 4.3.10. right decomposable least fixed point.

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.

Rule 4.3.11. right fixed point hypothesis utilization.

Rule 4.3.12. right fixed point hypothesis learning.

Rule 4.3.13. tags

Rule 4.3.14. records

Rule 4.3.15. implications

Rule 4.3.16. left diff

Rule 4.3.17. right diff

Definition 4.3. $\boxed{\tau <: \tau \dashv \Omega}$ Proof Subtyping

$$\begin{array}{c}
\frac{}{\tau <: \tau \dashv \Omega} [1] \qquad \frac{\tau_{ll} <: \tau_r \dashv \Omega \quad \tau_{lr} <: \tau_r \dashv \Omega' \quad \Omega \preceq \Omega'}{\tau_{ll} \mid \tau_{lr} <: \tau_r \dashv \Omega'} [2] \\
\\
\frac{\Delta \dashv \vec{\alpha}_w, \Delta_w \quad \vec{\alpha} \# \tau_r \quad (\vec{\alpha}_w \vec{\alpha}, \Delta_w) \preceq \Omega}{\text{EXI}[\vec{\alpha} \Delta] \tau_l <: \tau_r \dashv \Omega} [3] \qquad \frac{\alpha \in \vec{\alpha} \quad \text{factor}(\Delta, \alpha) = \Delta_f \quad \vec{\alpha}, (\Delta \Delta_f) \vdash \alpha <: \vec{\tau} \quad \text{inter}(\vec{\tau}) <: \tau_r \dashv \vec{\alpha}', \Delta' \quad (\vec{\alpha}, \Delta \Delta_f) \preceq (\vec{\alpha}', \Delta')}{\alpha <: \tau_r \dashv \vec{\alpha}', \Delta'} [4] \\
\\
\frac{\alpha \notin \vec{\alpha} \quad \vec{\alpha}, \Delta \vdash \alpha / \tau_l \dagger \Delta^\dagger \quad \vec{\alpha}, \Delta \vdash \alpha <: \dagger \vec{\tau} \quad \vec{\alpha}, \Delta \vdash \alpha / \tau_l <: \# \Delta^\# \quad \Delta^\dagger \tau_l <: \text{inter}(\vec{\tau}) \dashv \vec{\alpha}', \Delta' \quad (\vec{\alpha}, \Delta \Delta^\#) \preceq (\vec{\alpha}', \Delta')}{\tau_l <: \alpha \dashv (\vec{\alpha}', \Delta' \tau_l <: \alpha)} [5] \qquad \frac{\tau_l <: \tau_r \dashv \Omega \quad \Delta \dashv \Omega' \quad \Omega \preceq \Omega'}{\tau_l <: \text{EXI}[\vec{\alpha} \Delta] \tau_r \dashv \Omega'} [6] \\
\\
\frac{\tau_l <: \tau_{rl} \dashv \Omega}{\tau_l <: \tau_{rl} \mid \tau_{rr} \dashv \Omega} [7] \qquad \frac{\tau_l <: \tau_{rr} \dashv \Omega}{\tau_l <: \tau_{rl} \mid \tau_{rr} \dashv \Omega} [8] \qquad \frac{\tau_l[\alpha / \tau_r] <: \tau_r \dashv \Omega}{\text{LFP}[\alpha] \tau_l <: \tau_r \dashv \Omega} [9] \\
\\
\frac{\Omega \vdash \tau_l \cup \text{LFP}[\alpha] \tau_r \quad \tau_l <: \tau_r[\alpha / \text{LFP}[\alpha] \tau_r] \dashv \Omega' \quad \Omega \preceq \Omega'}{\tau_l <: \text{LFP}[\alpha] \dashv \Omega'} [10] \\
\\
\frac{\exists \alpha. \alpha \in \text{FTV}(\tau_l) \wedge \alpha \in \vec{\alpha} \quad \tau_l <: \text{LFP}[\alpha] \tau_r \cong \tau'_l <: \text{LFP}[\alpha] \tau'_r \quad \Delta \vdash \tau'_l <: \tau_n \sim \quad \tau_n <: \text{LFP}[\alpha] \tau'_r \dashv \Omega \quad (\vec{\alpha}, \Delta) \preceq \Omega}{\tau_l <: \text{LFP}[\alpha] \tau_r \dashv \Omega} [11] \\
\\
\frac{\vec{\alpha} \vdash \Delta \wr \text{FTV}(\tau_l) \dashv \vec{\delta} \quad \vdash \tau_l <: \text{LFP}[\alpha] \tau_r \star \quad \tau_l[\vec{\delta}] <: \text{LFP}[\alpha] \tau_r \dashv \vec{\alpha}_1, \Delta_1 \quad (\vec{\alpha}, \Delta) \preceq (\vec{\alpha}', \Delta')}{\tau_l <: \text{LFP}[\alpha] \tau_r \dashv \vec{\alpha}', \Delta' ; \tau_l <: \text{LFP}[\alpha] \tau_r} [12] \qquad \frac{\tau_l <: \tau_r \dashv \Omega}{< \! l \! > \tau_l <: < \! l \! > \tau_r \dashv \Omega} [13] \\
\\
\frac{\tau_l <: \tau_r \Omega}{l \! - \! > \tau_l <: l \! - \! > \tau_r \dashv \Omega} [14] \qquad \frac{\tau_{rl} <: \tau_{ll} \dashv \Omega \quad \tau_{lr} <: \tau_{rr} \dashv \Omega' \quad \Omega \preceq \Omega'}{\tau_{ll} \! - \! > \tau_{lr} <: \tau_{rl} \! - \! > \tau_{rr} \dashv \Omega'} [15] \qquad \frac{\tau_l <: \tau_r \mid \eta \dashv \Omega}{\tau_l \setminus \eta <: \tau_r \dashv \Omega} [16] \\
\\
\text{TODO: prove that subtyping of diff is complete} \\
\text{TODO: which implies that its negation is sound} \\
\frac{\tau_l <: \tau_r \dashv \Omega \quad \nexists \Omega'. \tau_l <: \eta \dashv \Omega' \wedge \Omega \preceq \Omega' \quad \text{FTV}(\eta) \subseteq \epsilon}{\tau_l <: \tau_r \setminus \eta \dashv \Omega} [17]
\end{array}$$

5 CORRECTNESS

TODO: introduce model typing and soundness properties

Definition 5.1. $\boxed{\vec{\delta}, \Gamma \models e : \tau}$ Model typing

$$\begin{array}{c}
\frac{\alpha/\tau \in \vec{\delta} \quad \vec{\delta}, \Gamma \models e : \tau}{\vec{\delta}, \Gamma \models e : \alpha} \quad \frac{\alpha/\tau \notin \vec{\delta} \quad \vec{\delta}, \Gamma \models e : \text{TOP}}{\vec{\delta}, \Gamma \models e : \alpha} \quad \frac{}{\vec{\delta}, \Gamma \models @ : @} \quad \frac{\vec{\delta}, \Gamma \models e : \tau}{\vec{\delta}, \Gamma \models <l>e : <l>\tau} \\
\\
\frac{\begin{array}{c} \$l \Rightarrow v \in G \quad \vec{\delta}, \Gamma \models v : \tau \\ \forall v'. \$l \Rightarrow v' \in G \implies v' = v \end{array}}{\vec{\delta}, \Gamma \models G : l \rightarrow \tau} \\
\\
\frac{\begin{array}{c} \vec{\delta}, \Gamma \sqcup \Gamma' \models p \diamond \tau_p \quad \vec{\delta}, \Gamma \sqcup \Gamma' \models e : \tau_r \\ \forall e. \vec{\delta}, \Gamma \models e : \tau_l \implies \vec{\delta}, \Gamma \models e : \tau_p \wedge (\forall \tau_n. \tau. \vec{\delta}, \Gamma \models F : \tau_n \rightarrow \tau \implies \neg(\vec{\delta}, \Gamma \models e : \tau_n)) \end{array}}{\vec{\delta}, \Gamma \models F * p \Rightarrow e : \tau_l \rightarrow \tau_r} \\
\\
\frac{\vec{\delta}, \Gamma \models F : \tau_l \rightarrow \tau_r}{\vec{\delta}, \Gamma \models F * p \Rightarrow e : \tau_l \rightarrow \tau_r} \quad \frac{\vec{\delta}, \Gamma \models e : \tau_l}{\vec{\delta}, \Gamma \models e : \tau_l | \tau_r} \quad \frac{\vec{\delta}, \Gamma \models e : \tau_r}{\vec{\delta}, \Gamma \models e : \tau_l | \tau_r} \\
\\
\frac{\vec{\delta}, \Gamma \models e : \tau_l \quad \vec{\delta}, \Gamma \models e : \tau_r}{\vec{\delta}, \Gamma \models e : \tau_l \& \tau_r} \quad \frac{\vec{\delta}, \Gamma \models e : \tau_l \quad \neg(\vec{\delta}, \Gamma \models e : \tau_r)}{\vec{\delta}, \Gamma \models e : \tau_l \setminus \tau_r} \quad \frac{\vec{\delta} \sqcup \vec{\delta}' \models Q \quad \vec{\delta} \sqcup \vec{\delta}' \models e : \tau}{\vec{\delta} \models e : \text{EXI}[A \ Q] \tau} \\
\\
\frac{\forall \vec{\delta}'. \vec{\delta} \sqcup \vec{\delta}' \models Q \implies \vec{\delta} \sqcup \vec{\delta}', \Gamma \models e : \tau}{\vec{\delta}, \Gamma \models e : \text{ALL}[A \ Q] \tau} \quad \frac{\vec{\delta} \alpha / \text{LFP}[\alpha] \tau \models e : \tau}{\vec{\delta}, \Gamma \models e : \text{LFP}[\alpha] \tau} \quad \frac{x : \tau \in \Gamma}{\vec{\delta}, \Gamma \models x : \tau} \\
\\
\frac{\vec{\delta}, \vec{\sigma} \models \Gamma \quad e[\vec{\sigma}] \rightsquigarrow e'[\vec{\sigma}'] \quad \vec{\delta}, \vec{\sigma}' \models \Gamma' \quad \vec{\delta}, \Gamma' \models e' : \tau}{\vec{\delta}, \Gamma \models e : \tau}
\end{array}$$

Definition 5.2. $\boxed{\vec{\delta} \models \tau <: \tau}$ Model Subtyping

$$\frac{\forall e. \vec{\delta}, \Gamma \models e : \tau_l \implies \vec{\delta}, \Gamma \models e : \tau_r}{\vec{\delta} \models \tau_l <: \tau_r}$$

Definition 5.3. $\boxed{\vec{\delta} \models Q}$ Model Sequence Subtyping

$$\frac{}{\vec{\delta} \models \epsilon} \quad \frac{\vec{\delta} \models Q \quad \vec{\delta} \models \tau_l <: \tau_r}{\vec{\delta} \models Q . \tau_l <: \tau_r}$$

6 EXPERIMENTS

TODO: develop 12 tree/list experiments

7 RELATED WORK

Tree interpolation. Exemplified by CHC duality solver.

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

8 APPENDIX

Definition 8.1. Internals

$$\Gamma ::= \epsilon \mid \Gamma x : \tau$$

$$\begin{aligned}\vec{\Omega} &::= \epsilon \mid \vec{\Omega} \Omega \\ \Omega &::= \vec{\alpha}, \Delta\end{aligned}$$

$$\begin{aligned}\vec{\tau} &::= \epsilon \mid \vec{\tau} \tau \\ \vec{\phi} &::= \epsilon \mid \vec{\phi} \phi\end{aligned}$$

$$\begin{aligned}\vec{\pi} &::= \epsilon \mid \vec{\pi} \pi \\ \pi &::= \vec{\alpha}, \Delta, \tau \multimap \tau\end{aligned}$$

$$\begin{aligned}\vec{\delta} &::= \epsilon \mid \vec{\delta} \delta \\ \delta &::= \alpha / \tau\end{aligned}$$

Definition 8.2. Sugared Expressions

$$\begin{aligned}e &::= \dots \mid e, e \mid e \mid e \mid \text{let } x z = e \text{ in } e \mid (e) \\ z &::= \epsilon \mid : \tau \\ p &::= \dots \mid p, p \mid (p)\end{aligned}$$

Definition 8.3. Values

$$\begin{aligned}v &::= @ \mid \langle l \rangle v \mid \vec{g} \mid v, v \mid (v) \mid \vec{f} \\ \vec{g} &::= \epsilon \mid \vec{g} g \\ g &::= \$l \Rightarrow v \\ \vec{\sigma} &::= \epsilon \mid \vec{\sigma} \sigma \\ \sigma &::= x / v\end{aligned}$$

Definition 8.4. $\boxed{e \rightsquigarrow e}$ Sugared Progression

$$\begin{array}{c} \frac{e_b(e_a) \rightsquigarrow e'}{e_a \mid e_b \rightsquigarrow e'} \quad \frac{e \rightsquigarrow e'}{(e) \rightsquigarrow e'} \quad \frac{\$left \Rightarrow e_l \$right \Rightarrow e_r \rightsquigarrow e'}{e_l, e_r \rightsquigarrow e'} \\[10pt] \frac{(\$ \langle \text{true} \rangle @ \Rightarrow e_t \$ \langle \text{false} \rangle @ \Rightarrow e_f)(e_c) \rightsquigarrow e'}{\text{if } e_c \text{ then } e_t \text{ else } e_f \rightsquigarrow e'} \quad \frac{(\$x \Rightarrow e_k)(e) \rightsquigarrow e'}{\text{let } x : \tau = e \text{ in } e_k \rightsquigarrow e'} \end{array}$$

Definition 8.5. Sugared Types

$$\begin{aligned}\tau &::= \dots \mid \text{TOP} \mid \text{BOT} \mid (\tau) \\ \phi &::= \dots \mid (\phi)\end{aligned}$$

Definition 8.6. $\boxed{\tau <: \tau \vdash M, \Delta}$ Continued Proof Subtyping

$$\begin{array}{c}
\frac{}{\text{BOT} <: \tau_r \vdash M, \Delta} \quad \frac{}{\tau_l <: \text{TOP} \vdash M, \Delta} \quad \frac{\tau_l <: (l : \tau_{rl}) \& (l : \tau_{rr}) \vdash M, \Delta}{\tau_l <: l : (\tau_{rl} \& \tau_{rr}) \vdash M, \Delta} \\
\\
\frac{\tau_l <: \tau_{rl} \vdash M_0, \Delta_0 \quad M_0 \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \tau_{rr} \vdash M_1, \Delta_1}{\tau_l <: \tau_{rl} \& \tau_{rr} \vdash M_1, \Delta_1} \quad \frac{\tau_l <: (\tau_{ra} \rightarrow \tau_{rc}) \& (\tau_{rb} \rightarrow \tau_{rc}) \vdash M, \Delta}{\tau_l <: \tau_{ra} \mid \tau_{rb} \rightarrow \tau_{rc} \vdash M, \Delta} \\
\\
\frac{\tau_l <: (\tau_{ra} \rightarrow \tau_{rb}) \& (\tau_{ra} \rightarrow \tau_{rc}) \vdash M, \Delta}{\tau_l <: \tau_{ra} \rightarrow \tau_{rb} \& \tau_{rc} \vdash M, \Delta} \quad \frac{Q \vdash M_0, \Delta_0 \quad A \# \tau_l \quad M_0 \sqcup A \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \tau_r \vdash M_1, \Delta_1}{\tau_l <: \text{ALL}[A \ Q] \tau_r \vdash M_1, \Delta_1} \\
\\
\frac{\alpha \in M_0 \quad \Delta_0 \vdash T <: \alpha \quad M_0 \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \mid (T) \vdash M_1, \Delta_1}{\tau_l <: \alpha \vdash M_1, \Delta_1} \\
\\
\frac{M_0, \Delta_0 \vdash T <: \dagger \alpha \quad \alpha \notin M_0 \quad M_0, \Delta_0 \vdash \Delta_m <: \# \alpha / \tau_r \quad M_0 \preceq M_1 \quad \Delta_0 \sqcup \Delta_m \preceq \Delta_1 \quad \mid (T) <: \tau_r \vdash M_1, \Delta_1}{\alpha <: \tau_r \vdash M_1, \Delta_1 \quad \alpha <: \tau_r}
\end{array}$$

$$\frac{M_0 \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \tau_r \vdash M_0, \Delta_0}{\text{ALL}[A \ Q] \tau_l <: \tau_r \vdash M_1, \Delta_1} \quad \frac{\tau_{ll} <: \tau_r \vdash M, \Delta}{\tau_{ll} \& \tau_{lr} <: \tau_r \vdash M, \Delta} \quad \frac{\tau_{lr} <: \tau_r \vdash M, \Delta}{\tau_{ll} \& \tau_{lr} <: \tau_r \vdash M, \Delta}$$

Definition 8.7. $\boxed{\Omega \preceq \Omega}$ World Ordering

$$(\vec{\alpha}, \Delta) \preceq (\vec{\alpha} \vec{\alpha}', \Delta \Delta')$$

Definition 8.8. $\boxed{\vec{\alpha}, \Delta, \Gamma \vdash \vec{f} \blacktriangle \vec{\pi}, \vec{\eta}}$ Function Lifting

$$\frac{\vec{\alpha}, \Delta, \Gamma \vdash \vec{f} \blacktriangle \vec{\pi}, \vec{\eta} \quad p : \phi \vdash \Gamma' \quad \text{diff}(\phi, \vec{\eta}) = \tau_l \quad \forall \vec{\alpha}' \Delta' \tau_r. (\vec{\alpha} \vec{\alpha}', \Delta \Delta', \tau_l \rightarrow \tau_r) \in \vec{\pi}' \implies \Gamma \Gamma' \vdash e : \tau_r \vdash \vec{\alpha} \vec{\alpha}', \Delta \Delta' \quad \exists \pi. \pi \in \vec{\pi}' \quad \text{close}(\phi) = \eta}{\vec{\alpha}, \Delta, \Gamma \vdash \vec{f} \$p \Rightarrow e \blacktriangle \vec{\pi} \vec{\pi}', \vec{\eta} \eta}$$

Definition 8.9. $\boxed{\Omega \vdash \tau \cup \tau}$ Decomposable

$$\frac{\text{TODO: ...}}{\Omega \vdash \tau \cup \tau}$$

Definition 8.10. $\boxed{\tau <: \tau \cong \tau <: \tau}$ Normal Constraint Congruence

$$\frac{\text{TODO: ...}}{\tau <: \tau \cong \tau <: \tau}$$

Definition 8.11. $\boxed{\Delta \vdash \tau' <: \tau \sim}$ Normal Constraint Entailment

$$\frac{\text{TODO: ...}}{\Delta \vdash \tau' <: \tau \sim}$$

Definition 8.12. $\boxed{\vec{\alpha} \vdash \Delta \wr \vec{\alpha} \dashv \vec{\delta}}$ Modulo Type Solution

$$\frac{\text{TODO: ...}}{\vec{\alpha} \vdash \Delta \wr \vec{\alpha} \dashv \vec{\delta}}$$

Definition 8.13. $\boxed{\vdash \tau_l <: \tau \star}$ Constraint Consistency

$$\frac{\text{TODO: ...}}{\vdash \tau_l <: \text{LFP}[\alpha] \tau_r \star}$$

Definition 8.14. $\boxed{A \# \tau}$ Fresh variables

$$\frac{\forall \alpha. \alpha \in A \implies \alpha \notin \text{FV}(\tau)}{A \# \tau}$$

Definition 8.15. $\boxed{\tau <: \tau \dashv Z}$ (Proof universe subtyping)

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

Definition 8.16. $\boxed{Q \dashv M, \Delta}$

$$\frac{Q \dashv M_0, \Delta_0 \quad M_0 \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \tau_r \dashv M_1, \Delta_1}{Q \cdot \tau_l <: \tau_r \dashv M_1, \Delta_1} \quad \overline{M, \Delta \vdash \epsilon}$$

Definition 8.17. (Collection)

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

Definition 8.18. $\boxed{C \ C = C}$ Concatenation

$$\begin{aligned} C \ \epsilon &= C && \triangleright \text{empty} \\ C \ (C' \ c) &= (C \ C') \ c && \triangleright \text{step} \end{aligned}$$

Definition 8.19. $\boxed{C \diamond C = C}$ Filter

$$\begin{aligned} C \diamond \epsilon &= \epsilon \\ C \diamond (C' \ c) &= \begin{cases} (C \diamond C') \ c & \text{if } c \in C \\ (C \diamond C') & \text{otherwise} \end{cases} \end{aligned}$$

Definition 8.20. $\boxed{c \in C}$ Collection Containment

$$\frac{}{c \in C \ c} \quad \frac{c \neq c' \quad c \in C}{c \in C \ c'}$$

Definition 8.21. $\boxed{C \preceq C}$

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

Definition 8.22. $\boxed{\text{union}(T) = \tau}$ Collective Union

$$\begin{aligned} \text{union}(\epsilon) &= \text{BOT} &> \text{empty} \\ \text{union}(T \ \tau) &= \text{union}(T) \mid \tau &> \text{step} \end{aligned}$$

Definition 8.23. $\boxed{\text{inter}(T) = \tau}$ Collective Intersection

$$\begin{aligned} \text{inter}(\epsilon) &= \text{TOP} &> \text{empty} \\ \text{inter}(T \ \tau) &= \text{inter}(T) \& \tau &> \text{step} \end{aligned}$$

Definition 8.24. $\boxed{M, \Delta \vdash m <:^{\#} \alpha}$ Lower closed subtyping

$$\frac{m \in M \quad m <: \alpha \in \Delta}{M, \Delta \vdash m <:^{\#} \alpha}$$

Definition 8.25. $\boxed{M, \Delta \vdash \Delta' <:^{\#} \alpha / \tau}$ Universal lower closed subtyping

$$\frac{\forall \tau. m <: \tau \in \Delta' \iff M, \Delta \vdash m \in M \wedge m <: \alpha \in \Delta}{M, \Delta \vdash \Delta' <:^{\#} \alpha / \tau}$$

Definition 8.26. $\boxed{M, \Delta \vdash \alpha / \tau <:^{\#} \Delta}$ Universal upper closed subtyping

$$\frac{\forall \tau. m. \tau <: m \in \Delta' \iff m \in M \wedge \alpha <: m \in \Delta}{M, \Delta \vdash \alpha <:^{\#} \Delta'}$$

Definition 8.27. $\boxed{M, \Delta \vdash \tau <:^{\dagger} \alpha}$ Lower transitive subtyping

$$\frac{\tau \notin M \quad \tau <: \alpha \in \Delta}{M, \Delta \vdash \tau <:^{\dagger} \alpha} \quad \frac{m \in M \quad M, \Delta \vdash \tau <:^{\dagger} m \quad m <: \alpha \in \Delta}{M, \Delta \vdash \tau <:^{\dagger} \alpha}$$

Definition 8.28. $\boxed{M, \Delta \vdash T <:^{\dagger} \alpha}$ Universal lower transitive subtyping

$$\frac{\forall \tau. \tau \in T \iff M, \Delta \vdash \tau <:^{\dagger} \alpha}{M, \Delta \vdash T <:^{\dagger} \alpha}$$

Definition 8.29. $\boxed{M, \Delta \vdash \alpha <:^{\dagger} \tau}$ Upper transitive subtyping

$$\frac{\tau \notin M \quad \alpha <: \tau \in \Delta}{M, \Delta \vdash \alpha <:^{\dagger} \tau} \quad \frac{m \in M \quad \alpha <: m \in \Delta \quad M, \Delta \vdash m <:^{\dagger} \tau}{M, \Delta \vdash \alpha <:^{\dagger} \tau}$$

Definition 8.30. $\boxed{M, \Delta \vdash \alpha <:^{\dagger} T}$ Universal upper transitive subtyping

$$\frac{\forall \tau. \tau \in T \iff M, \Delta \vdash \alpha <:^{\dagger} \tau}{M, \Delta \vdash \alpha <:^{\dagger} T}$$

Definition 8.31. $\boxed{M, \Delta \vdash \alpha \dagger \tau <: \tau}$ Relational subtyping

$$\frac{\alpha \neq \tau_l \quad \alpha \in \text{FTV}(\tau_l)}{\Delta \vdash \alpha \dagger \tau_l <: \tau_r}$$

Definition 8.32. $\boxed{M, \Delta \vdash \alpha/\tau \dagger \Delta}$ Relational substitution

$$\frac{\forall \tau_l \tau_r. \tau_l[\alpha/\tau] <: \tau_r \in \Delta' \iff M, \Delta \vdash \alpha \dagger \tau_l <: \tau_r}{M, \Delta \vdash \alpha/\tau \dagger \Delta'}$$

Definition 8.33. $\boxed{M, \Delta, A \vdash \vec{\delta}}$

$$\frac{}{M, \Delta, \epsilon \vdash \epsilon} \quad \frac{\alpha \notin M \quad \forall \tau. \tau <: \alpha \notin \Delta \quad M, \Delta, A \vdash \vec{\delta}}{M, \Delta, A \alpha \vdash \vec{\delta}}$$

$$\frac{\alpha \notin M \quad \exists \tau. \tau <: \alpha \in \Delta \quad M, \Delta, A \vdash \vec{\delta}}{M, \Delta, A \alpha \vdash \vec{\delta} \alpha / | (\overline{\tau}^{\tau <: \alpha \in \Delta})}$$

Definition 8.34. $\boxed{\vec{\alpha}, \vec{\alpha}' \vdash \vec{\pi} \cong \vec{\tau}}$ Constrained Implication Congruence

$$\frac{}{\vec{\alpha}_f, \vec{\alpha}_m \vdash \epsilon \cong \epsilon} \quad \frac{\vec{\alpha}_f, \vec{\alpha}_m \vdash \vec{\pi} \cong \vec{\tau} \quad \text{FTV}(\tau_l) = \vec{\alpha}_l \quad \text{FTV}(\tau_r) = \vec{\alpha}_r \quad \Delta \vdash \vec{\alpha}_f \vec{\alpha}_m \vec{\alpha}_l \vec{\alpha}_r \dot{\cap} \Delta' \quad \vec{\alpha}_f, \vec{\alpha}_m, \Delta' \vdash \tau_l \text{-}> \tau_r \cong^+ \tau}{\vec{\alpha}_f, \vec{\alpha}_m \vdash \vec{\pi} \langle M, \Delta, \tau_l \text{-}> \tau_r \rangle \cong \vec{\tau} \tau}$$

Definition 8.35. $\boxed{\vec{\alpha} \vdash v\alpha.Z.\alpha \rightarrow \alpha \equiv \mu\alpha.\vec{\tau}}$ Fixpoint Duality

TODO: Note the reason for excluding rigids and closedes from quantification is a way to improve precision, but not necessary for soundness. (Right?). Need to conjure up an example to support this idea.

$$\frac{}{\vec{\alpha}_f \vdash \alpha_{h^+} \cdot \epsilon \cdot \alpha_l \text{-}> \alpha_r \equiv \alpha_{h^-} \cdot \epsilon} \quad \frac{\vec{\alpha}_f \vdash \alpha_{h^+} \cdot Z \cdot \alpha_l \text{-}> \alpha_r \equiv \alpha_{h^-} \cdot T \quad \Delta \vdash \alpha_{h^+} <: T_h \quad \Delta \vdash \alpha_l <: T_l \quad \Delta \vdash T_r <: \alpha_r \quad \frac{\tau_l * \tau_r <: \alpha_{h^-} \tau_l \text{-}> \tau_r \in T_h = \Delta_h}{\vec{\alpha}_f \sqcup M \sqcup \text{FTV}(T_l) \sqcup \text{FTV}(T_r) \alpha_{h^-} = A \quad \Delta \vdash A \dot{\cap} \Delta_i \quad \vec{\alpha}_f \alpha_{h^-}, M, \Delta_i \sqcup \Delta_h \vdash \&(T_l) * | (T_r) \cong^- \tau}}{\vec{\alpha}_f \vdash \alpha_{h^+} \cdot Z \langle M, \Delta \rangle \cdot \alpha_l \text{-}> \alpha_r \equiv \alpha_{h^-} \cdot T \tau}$$

Definition 8.36. $\boxed{\Delta \vdash A \dot{\cap} \Delta}$ Influential Filter

$$\frac{}{\epsilon \vdash A \dot{\cap} \epsilon} \quad \frac{\alpha \in A \quad \alpha \in \text{FTV}(\tau_l) \sqcup \text{FTV}(\tau_r) \quad \Delta \vdash A \dot{\cap} \Delta'}{\Delta \tau_l <: \tau_r \vdash N \dot{\cap} \Delta' \tau_l <: \tau_r}$$

$$\frac{\forall \alpha. \alpha \in A \implies \alpha \notin \text{FTV}(\tau_l) \sqcup \text{FTV}(\tau_r) \quad \Delta \vdash A \dot{\cap} \Delta'}{\Delta \tau_l <: \tau_r \vdash A \dot{\cap} \Delta'}$$

Definition 8.37. $\boxed{\Delta \vdash T <: \alpha}$

$$\frac{}{\epsilon \vdash \epsilon <: \alpha} \quad \frac{\Delta \vdash T <: \alpha}{\Delta \tau <: \alpha \vdash T \tau <: \alpha} \quad \frac{\tau_r \neq \alpha \quad \Delta \vdash T <: \alpha}{\Delta \tau_l <: \tau_r \vdash T <: \alpha}$$

Definition 8.38. $\boxed{\Delta \vdash \alpha <: T}$

$$\frac{}{\epsilon \vdash \alpha <: \epsilon} \quad \frac{\Delta \vdash \alpha <: T}{\Delta \alpha <: \tau \vdash \alpha <: T \tau} \quad \frac{\tau_l \neq \alpha \quad \Delta \vdash \alpha <: T}{\Delta \tau_l <: \tau_r \vdash \alpha <: T}$$

Definition 8.39. $\boxed{\text{outer}(+|-) = \text{ALL}|\text{EXI}}$

$$\begin{aligned}\text{outer}(+) &= \text{EXI} \triangleright \text{positive} \\ \text{outer}(-) &= \text{ALL} \triangleright \text{negative}\end{aligned}$$

Definition 8.40. $\boxed{\text{inner}(+|-) = \text{ALL}|\text{EXI}}$

$$\begin{aligned}\text{inner}(+) &= \text{ALL} \triangleright \text{positive} \\ \text{inner}(-) &= \text{EXI} \triangleright \text{negative}\end{aligned}$$

Definition 8.41. $\boxed{\text{quantify}^{+|-}(\mathbf{A}, \Delta, \mathbf{A}, \Delta, \tau) = \tau}$

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

Definition 8.42. $\boxed{\mathbf{A}, \mathbf{A}, \Delta \vdash \tau \cong^{+|-} \tau'}$

$$\frac{\begin{array}{c} \mathbf{A}_z, \Delta \vdash \Delta_o \wr \Delta_i \\ (\text{FTV}(\Delta) \text{FTV}(\tau)) \diamond \mathbf{A}_z = \mathbf{A}_o \quad (\text{FTV}(\Delta_i) \text{FTV}(\tau)) \setminus \mathbf{A}_z \setminus \mathbf{A}_r = \mathbf{A}_i \\ \text{quantify}^{+|-}(\mathbf{A}_o, \Delta_o, \mathbf{A}_i, \Delta_i, \tau) = \tau' \end{array}}{\mathbf{A}_r, \mathbf{A}_z, \Delta \vdash \tau \cong^{+|-} \tau'}$$

Definition 8.43. $\boxed{\mathbf{A}, \Delta \vdash \Delta \wr \Delta}$

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

Definition 8.44. $\boxed{\models e}$

$$\frac{e = v}{\models e} \qquad \frac{e \rightsquigarrow e' \quad \models e'}{\models e}$$

Theorem 8.1. (Typing Soundness)

$$\frac{\vdash e : \tau \dashv Z}{\models e}$$

Proof:

assume $\vdash e : \tau \dashv Z$

. **let** $\vec{\delta} \Gamma' \tau'$ **s.t.** $\vec{\delta}, \Gamma' \models e : \tau'$ by LEMMA 8.3

. $\vec{\delta}, \vec{\sigma} \models \Gamma'$ by ...

. $\models e[\vec{\sigma}]$ by theorem 8.51

. $e[\vec{\sigma}] = e$ by ...

. $\models e$ by substitution

□

Theorem 8.2. (Proof typing consistency)

$$\frac{\Gamma \vdash e : \tau \dashv Z}{\exists \vec{\delta}. \vec{\delta} \models Z}$$

TODO: ...

Theorem 8.3. (Proof typing soundness)

$$\frac{\Gamma \vdash e : \tau \dashv Z}{\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau}$$

TODO: ...

Theorem 8.4. (Proof typing weak soundness)

$$\frac{\Gamma \vdash e : \tau \dashv Z}{\forall \vec{\delta}. \vec{\delta} \models Z \implies \vec{\delta}, \Gamma \models e : \tau}$$

TODO: rewrite inductive hypotheses with just the conclusion implied by the case conditions

TODO: rewrite cases with universal/implication in conclusion/hypotheses

Proof:

```

assume  $\Gamma \vdash e : \tau \dashv Z$ 
.   induct on  $\Gamma \vdash e : \tau \dashv Z$ 
.   case  $e = @ \quad \tau = @$ 
.   .   let  $\vec{\delta}$  by definition
.   .    $\vec{\delta}, \Gamma \models @ : @$  by definition
.   .    $\vec{\delta}, \Gamma \models e : \tau$  by substitution
.   .    $\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau$  by witness
.   case  $e = x \quad x : \tau \in \Gamma$ 
.   wrt  $x$ 
.   .   let  $\vec{\delta}$  by definition
.   .    $\vec{\delta}, \Gamma \models x : \tau$  by definition
.   .    $\vec{\delta}, \Gamma \models e : \tau$  by substitution
.   .    $\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau$  by witness
.   case  $\Gamma \vdash e' : \tau' \dashv Z \quad \tau = \langle l \rangle \tau' \quad e = \langle l \rangle e'$ 
.   hypo  $\Gamma \vdash e' : \tau' \dashv Z \implies \vec{\delta}, \Gamma \models e' : \tau'$ 
.   wrt  $e' \tau'$ 
.   .   let  $\vec{\delta}$  by definition
.   .    $\vec{\delta}, \Gamma \models e' : \tau'$  by application
.   .    $\vec{\delta}, \Gamma \models \langle l \rangle e' : \langle l \rangle \tau'$  by definition
.   .    $\vec{\delta}, \Gamma \models e : \tau$  by substitution
.   .    $\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau$  by witness
.   TODO: remaining trivial introduction cases
.   case
.   hypo
.   wrt
.   case  $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \quad Z_0 \rightsquigarrow Z_1 \quad \tau_0 <: l \dashv \alpha \dashv Z_1 \quad e = e_0.l \quad \tau = \alpha \quad Z = Z_1$ 
.   hypo  $\Gamma \vdash e_0 : \tau_0 \dashv Z_0 \implies \vec{\delta}, \Gamma \models e_0 : \tau_0$ 

```

\cdot **wrt** $\vec{\delta} \ e' \ l \ \alpha \ \tau_0 \ Z_0 \ Z_1$
 \cdot \cdot $\vec{\delta}, \Gamma \models e_0 : \tau_0$ by application
 \cdot \cdot **let** $M \Delta$ **s.t.** $\tau_0 <: l \rightarrow \alpha \vdash M, \Delta$ by theorem 8.18
 \cdot \cdot $\vec{\delta} \models \tau_0 <: l \rightarrow \alpha$ by theorem 8.23
 \cdot \cdot $\vec{\delta}, \Gamma \models e_0 : l \rightarrow \alpha$ by theorem 8.19
 \cdot \cdot $\vec{\delta}, \Gamma \models e_0.l : \alpha$ by theorem 8.20
 \cdot \cdot $\vec{\delta}, \Gamma \models e : \tau$ by substitution
 \cdot \cdot $\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau$ by witness
 \cdot **case** $\Gamma \vdash e_0 : \tau_0 \vdash Z_0 \quad Z_0 \rightsquigarrow Z_1 \quad \Gamma \vdash e_1 : \tau_1 \vdash Z_1 \quad e = e_0(e_1) \quad \tau = \alpha \quad Z = Z_2$
 \cdot $Z_1 \rightsquigarrow Z_2 \quad \tau_0 <: \tau_1 \rightarrow \alpha \vdash Z_2$
 \cdot **hypo** $\Gamma \vdash e_0 : \tau_0 \vdash Z_0 \implies \vec{\delta}, \Gamma \models e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \vdash Z_1 \implies \vec{\delta}, \Gamma \models e_1 : \tau_1$
 \cdot **wrt** $e_0 \ e_1 \ \alpha \ \tau_0 \ \tau_1 \ Z_0 \ Z_1 \ Z_2$
 \cdot \cdot $\vec{\delta}, \Gamma \models e_0 : \tau_0$ by application
 \cdot \cdot $\vec{\delta}, \Gamma \models e_1 : \tau_1$ by application
 \cdot \cdot **let** $M \Delta$ **s.t.** $\tau_0 <: \tau_1 \rightarrow \alpha \vdash \langle M, \Delta \rangle$ by theorem 8.18
 \cdot \cdot $\vec{\delta}, \Gamma \models \tau_0 <: \tau_1 \rightarrow \alpha$ by theorem 8.23
 \cdot \cdot $\vec{\delta} \models e_0 : \tau_1 \rightarrow \alpha$ by theorem 8.19
 \cdot \cdot $\vec{\delta}, \Gamma \models e_0(e_1) : \alpha$ by theorem 8.39
 \cdot \cdot $\vec{\delta}, \Gamma \models e : \tau$ by substitution
 \cdot \cdot $\exists \vec{\delta}. \vec{\delta}, \Gamma \models e : \tau$ by substitution
 \cdot **case** $e = \text{loop}(e')$
 \cdot $\mid \quad \tau = \text{ALL}[\alpha'_l] \alpha'_l \rightarrow \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFLFP}[\alpha_{h^-}]] \mid (T)] \alpha_r$
 \cdot $\mid \quad Z = Z_0$
 \cdot $\mid \quad \Gamma \vdash e' : \alpha_{h^+} \rightarrow \tau' \vdash Z_0 \quad Z_0 \rightsquigarrow Z_1 \quad \tau' <: \alpha_l \rightarrow \alpha_r \vdash Z_1$
 \cdot $\mid \quad \text{FTV}(\Gamma) \vdash \alpha_{h^+} \cdot Z_1 \cdot \alpha_l \rightarrow \alpha_r \doteq \alpha_{h^-} \cdot T$
 \cdot **hypo** $\forall \vec{\delta}. \vec{\delta} \models Z_0 \implies \vec{\delta}, \Gamma \models e' : \alpha_{h^+} \rightarrow \tau'$
 \cdot **wrt** $e' \ \tau' \ \alpha_{h^+} \ \alpha_l \ \alpha_r \ \alpha_{h^-} \ \alpha'_l \ \alpha'_r \ T \ Z_0 \ Z_1$
 \cdot \cdot **for** $\vec{\delta}$ **assume** $\vec{\delta} \models Z$
 \cdot \cdot \cdot $\vec{\delta} \models Z_0$ by substitution
 \cdot \cdot \cdot $\vec{\delta}, \Gamma \models e' : \alpha_{h^+} \rightarrow \tau'$ by instantiation and application
 \cdot \cdot \cdot $\vec{\delta} \models \tau' <: \text{ALL}[\alpha'_l] \alpha'_l \rightarrow \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFP}[\alpha_{h^-}]] \mid (T)] \alpha_r$ by theorem 8.5
 \cdot \cdot \cdot $\vec{\delta} \models \tau' <: \tau$ by substitution
 \cdot \cdot \cdot $\vec{\delta} \models e' : \alpha_{h^+} \rightarrow \tau$ by theorem 8.19
 \cdot \cdot \cdot $\vec{\delta} \models \text{loop}(e') : \tau$ by theorem 8.16
 \cdot \cdot \cdot $\vec{\delta} \models e : \tau$ by substitution
 \cdot \cdot $\forall \vec{\delta}. \vec{\delta} \models Z \implies \vec{\delta} \models e : \tau$ by implication and generalization
 \cdot $\vec{\delta}, \Gamma \models e : \tau$ by induction

□

Theorem 8.5. (Fixpoint duality soundness (new))

$$\frac{\tau <: \alpha_l \rightarrow \alpha_r \vdash Z_1 \quad \text{FTV}(\tau) \subseteq N \quad \alpha_l \notin N \quad \alpha_r \notin N \quad N \vdash \alpha_{h^+} \cdot Z_1 \cdot \alpha_l \rightarrow \alpha_r \doteq \alpha_{h^-} \cdot T}{\vec{\delta} \models \tau <: \text{ALL}[\alpha'_l] \alpha'_l \rightarrow \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFP}[\alpha_{h^-}]] \mid (T)] \alpha'_r}$$

TODO: ...

TODO: Cretin's corresponding theorem is Theorem 101 on p. 134

TODO: See how Cretin proves this without using subject reduction

Theorem 8.6. (Fixpoint duality soundness old)

$$\frac{Z_0 \rightsquigarrow Z_1 \quad N \vdash \alpha_{h^+} \cdot Z_1 \cdot \alpha_l \text{->} \alpha_r \equiv \alpha_{h^-} \cdot T}{\forall \tau. \tau <: \alpha_l \text{->} \alpha_r \vdash Z_1 \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFP}[\alpha_{h^-}] \mid (T)] \alpha'_r \vdash Z_0}$$

Proof:

assume $Z_0 \rightsquigarrow Z_1 \quad N \vdash \alpha_{h^+} \cdot Z_1 \cdot \alpha_l \text{->} \alpha_r \equiv \alpha_{h^-} \cdot T$

. **induct on** $N \vdash \alpha_{h^+} \cdot Z_1 \cdot \alpha_l \text{->} \alpha_r \equiv \alpha_{h^-} \cdot T$

. **case** $Z_1 = \epsilon \quad T = \epsilon$

. . **for** τ

. . . **assume** $\tau <: \alpha_l \text{->} \alpha_r \vdash Z_1$

. . . . $\tau <: \alpha_l \text{->} \alpha_r \vdash \epsilon$ by substitution

. . . . **let** $M \Delta$ **s.t.** $\langle M, \Delta \rangle \in \epsilon$ by theorem 8.14

. . . . \perp by theorem 8.15

. . . $\tau <: \alpha_l \text{->} \alpha_r \vdash Z_1 \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFP}[\alpha_{h^-}] \mid (T)] \alpha'_r \vdash Z_0$ by implication

. . $\forall \tau. \tau <: \alpha_l \text{->} \alpha_r \vdash Z_1 \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. \alpha'_l * \alpha'_r <: \text{LFP}[\alpha_{h^-}] \mid (T)] \alpha'_r \vdash Z_0$ by generalization

. **case** $Z_1 = Z \quad \langle M, \Delta \rangle \quad T = T_i \tau_i$

. | $N \vdash \alpha_{h^+} \cdot Z \cdot \alpha_l \text{->} \alpha_r \equiv \alpha_{h^-} \cdot T_i$

. | $M, \Delta, \Delta \vdash \alpha_{h^+} <: T_h \quad M, \Delta, \Delta \vdash \alpha_l <: T_l \quad M, \Delta, \Delta \vdash T_r <: \alpha_r$

. | $\frac{\tau_l * \tau_r <: \alpha_{h^-}}{\tau_l * \tau_r <: \alpha_{h^-}} \tau_l \tau_r. \tau_l \text{->} \tau_r \in T_h = \Delta_h$

. | $N \sqcup M \sqcup \text{FTV}(T_l) \sqcup \text{FTV}(T_r) \quad \alpha_{h^-} = A \quad \Delta \vdash A \text{ } \text{ } \Delta_i$

. | $N \alpha_{h^-}, M, \Delta_i \sqcup \Delta_h \vdash \&(T_l) * \mid (T_r) \cong^- \tau_i$

. **hypo** $N \vdash \alpha_{h^+} \cdot Z \cdot \alpha_l \text{->} \alpha_r \equiv \alpha_{h^-} \cdot T_i \implies$

$\forall \tau. \tau <: \alpha_l \text{->} \alpha_r \vdash Z \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. (\alpha'_l, \alpha'_r) <: \text{LFP}[\alpha_{h^-}] \mid (T_i)] \alpha'_r \vdash Z_0$

. **wrt** $Z \quad M \Delta \quad T_i \tau_i$

. . **for** τ **assume** $\tau <: \alpha_l \text{->} \alpha_r \vdash Z_1$

. . . $\tau <: \alpha_l \text{->} \alpha_r \vdash Z \quad \langle M, \Delta \rangle$ by substitution

. . . $\tau <: \alpha_l \text{->} \alpha_r \vdash \langle M, \Delta \rangle$ by theorem 8.17

. . . $\tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. (\alpha'_l, \alpha'_r) <: \text{LFP}[\alpha_{h^-}] \mid (T_i)] \alpha'_r \vdash Z_0$ by instantiation and application

. . . $\tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. (\alpha'_l, \alpha'_r) <: \text{LFP}[\alpha_{h^-}] \mid (T_i \tau_i)] \alpha'_r \vdash Z_0$ by theorem 8.7

. . $\forall \tau. \tau <: \alpha_l \text{->} \alpha_r \vdash Z_1 \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. (\alpha'_l, \alpha'_r) <: \text{LFP}[\alpha_{h^-}] \mid (T)] \alpha'_r \vdash Z_0$ by implication and generalization

. $\forall \tau. \tau <: \alpha_l \text{->} \alpha_r \vdash Z_1 \implies \tau <: \text{ALL}[\alpha'_l] \alpha'_l \text{->} \text{EXI}[\alpha'_r. (\alpha'_l, \alpha'_r) <: \text{LFP}[\alpha_{h^-}] \mid (T)] \alpha'_r \vdash Z_0$ by induction

□ by implication

Theorem 8.7. (Universe proof typing fixpoint extension)

$$\begin{array}{c} \vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \text{->} \text{EXI}[\alpha_r. (\alpha_l, \alpha_r) <: \text{LFP}[\alpha_{h^-}] \mid (T_i)] \alpha_r \\ \tau <: \alpha_l \text{->} \alpha_r \vdash \langle M, \Delta \rangle \\ \frac{\Delta \vdash \alpha_{h^+} <: T_h \quad \Delta \vdash \alpha_l <: T_l \quad \Delta \vdash T_r <: \alpha_r}{\frac{\tau_l * \tau_r <: \alpha_{h^-}}{\tau_l * \tau_r <: \alpha_{h^-}} \tau_l \tau_r. \tau_l \text{->} \tau_r \in T_h = \Delta_h \quad N \sqcup M \sqcup \text{FTV}(T_l) \sqcup \text{FTV}(T_r) \quad \alpha_{h^-} = A}{\Delta \vdash A \text{ } \text{ } \Delta_i \quad N \alpha_{h^-}, M, \Delta_i \sqcup \Delta_h \vdash \&(T_l) * \mid (T_r) \cong^- \tau_i} \\ \vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \text{->} \text{EXI}[\alpha_r. \alpha_l * \alpha_r <: \text{LFP}[\alpha_{h^-}] \mid (T_i \tau_i)] \alpha_r \end{array}$$

Proof:

TODO: ...

□

Theorem 8.8. (Universe proof typing case soundness)

$$\frac{\begin{array}{c} \tau <: \alpha_l \rightarrow \alpha_r \vdash \langle M, \Delta \rangle \\ \Delta \vdash \alpha_{h^+} <: T_h \quad \Delta \vdash \alpha_l <: T_l \quad \Delta \vdash T_r <: \alpha_r \\ \frac{\tau_l * \tau_r <: \alpha_{h^-} \rightarrow \tau_r \in T_h = \Delta_h \quad N \sqcup M \sqcup \text{FTV}(T_l) \sqcup \text{FTV}(T_r) \quad \alpha_{h^-} = A}{\Delta \vdash A \text{ th } \Delta_i \quad N \alpha_{h^-}, M, \Delta_i \sqcup \Delta_h \vdash \&(T_l) * | (T_r) \cong^- \tau_i} \end{array}}{\vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \rightarrow \text{EXI}[\alpha_r . \alpha_l * \alpha_r <: \text{LFP}[\alpha_{h^-}] \tau_i] \alpha_r}$$

Proof:

TODO: ...

□

Theorem 8.9. (Universe proof typing fixpoint union)

$$\frac{\begin{array}{c} \vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \rightarrow \text{EXI}[\alpha_r . \alpha_l * \alpha_r <: \text{LFP}[\alpha_{h^-}] | (T)] \alpha_r \\ \vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \rightarrow \text{EXI}[\alpha_r . \alpha_l * \alpha_r <: \text{LFP}[\alpha_{h^-}] \tau] \alpha_r \end{array}}{\vec{\delta} \models \tau <: \text{ALL}[\alpha_l] \alpha_l \rightarrow \text{EXI}[\alpha_r . \alpha_l * \alpha_r <: \text{LFP}[\alpha_{h^-}] | (T \ \tau)] \alpha_r}$$

Proof:

TODO: ...

□

Theorem 8.10. Influential soundness

TODO: Prove that any constraints on non-influential variables with have been transitively applied to the influential variables

$$\frac{\begin{array}{c} \tau <: \alpha_l \rightarrow \alpha_r \vdash M, \Delta \quad \Delta \vdash \alpha_l <: T_l \quad \Delta \vdash T_r <: \alpha_r \\ \Delta \vdash A \text{ th } \Delta_i \quad \text{FTV}(\tau) \subseteq A \\ N, M, \Delta \sqcup \Delta' \vdash \&(T_l) * | (T_r) \cong^- \tau \quad N, M, \Delta_i \sqcup \Delta' \vdash \&(T_l) * | (T_r) \cong^- \tau_i \end{array}}{\vec{\delta} \models \tau <: \tau_i \wedge \vec{\delta} \models \tau_i <: \tau}$$

Proof:

TODO: ...

□

Theorem 8.11. (Universe proof typing implication expansion)

$$\frac{}{\tau_l \rightarrow \tau_r <: \text{ALL}[\alpha_l] \alpha_l \rightarrow \text{EXI}[\alpha_r . (\alpha_l, \alpha_r) <: (\tau_l, \tau_r)] \alpha_r \vdash M, \Delta}$$

Proof:

TODO: $P \implies Q$ is equivalent to $\neg(P \wedge \neg Q)$

TODO: $X \rightarrow Y$ is equivalent to $\forall x \in X. \exists y. (x, y) \in (X \times Y)$

TODO: $X \rightarrow Y$ is equivalent to $\neg(\exists x \in X \wedge \nexists y \in Y)$

□

Theorem 8.12. (Upper bound interpretation sound)

$$\frac{M, \Delta, \Delta \vdash \alpha <: T}{\alpha <: \&(T) \vdash \langle M, \Delta \rangle}$$

Proof:

TODO: ...

□

Theorem 8.13. (Lower bound interpretation sound)

$$\frac{M, \Delta, \Delta \vdash T <: \alpha}{|\langle T \rangle <: \alpha \dashv \langle M, \Delta \rangle}$$

Proof:

TODO: ...

□

Theorem 8.14. (Universe proof typing worldly)

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

Proof:

TODO: ...

□

Theorem 8.15. (Empty containment absurd)

$$\frac{\langle M, \Delta \rangle \in \epsilon}{\perp}$$

Proof:

TODO: ...

□

Theorem 8.16. (Model typing implication independence)

$$\frac{\vec{\delta}, \Gamma \models e : \tau_l \dashv \tau_r \quad \vec{\delta} \models \tau_r}{\vec{\delta}, \Gamma \models \text{loop}(e) : \tau_r}$$

Proof:

TODO: ...

□

Theorem 8.17. (Proof subtyping decomposition)

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

Proof:

TODO: ...

□

Theorem 8.18. (Proof subtyping choice)

$$\frac{\tau_l <: \tau_r \dashv Z}{\exists M \Delta . \tau_l <: \tau_r \dashv M, \Delta}$$

Proof:

TODO: ...

□

Theorem 8.19. (Model subtyping elimination)

$$\frac{\vec{\delta} \models \tau_l <: \tau_r \quad \vec{\delta}, \Gamma \models e : \tau_l}{\vec{\delta}, \Gamma \models e : \tau_r}$$

Proof:

assume $\vec{\delta} \models \tau_l <: \tau_r \quad \vec{\delta}, \Gamma \models e : \tau_l$
 . **invert on** $\vec{\delta} \models \tau_l <: \tau_r$
 . **case** $\forall e' \Gamma'. \vec{\delta}, \Gamma' \models e' : \tau_l \implies \vec{\delta}, \Gamma' \models e' : \tau_r$
 . . $\vec{\delta}, \Gamma \models e : \tau_l \implies \vec{\delta}, \Gamma \models e : \tau_r$ by instantiation
 . . $\vec{\delta}, \Gamma \models e : \tau_r$ by application
 . $\vec{\delta}, \Gamma \models e : \tau_r$ by inversion
 \square by implication

Theorem 8.20. (Model typing record elimination)

$$\frac{\vec{\delta}, \Gamma \models e : l \rightarrow \tau}{\vec{\delta}, \Gamma \models e.l : \tau}$$

Proof:

assume $\vec{\delta}, \Gamma \models e : l \rightarrow \tau$
 . **induct on** $\vec{\delta}, \Gamma \models e : l \rightarrow \tau$
 . **case** $e = G \quad \$l \Rightarrow v \in G \quad \vec{\delta}, \Gamma \models v : \tau \quad \forall v'. \$l \Rightarrow v' \in G \implies v' = v$
 . **wrt** $G v$
 . . $\vec{\delta}, \Gamma \models G : l \rightarrow \tau$ by substitution
 . . $G.l \rightsquigarrow v$ by definition
 . . **let** $\vec{\sigma}$ s.t. $\vec{\delta}, \Gamma \models \vec{\sigma}$ by theorem ??
 . . $G.l[\vec{\sigma}] \rightsquigarrow v$ by definition
 . . $v = v[\vec{\sigma} \sqcup \epsilon]$ by definition
 . . $G.l[\vec{\sigma}] \rightsquigarrow v[\vec{\sigma} \sqcup \epsilon]$ by substitution
 . . $\vec{\delta}, \epsilon \models \epsilon$ by definition
 . . $\vec{\delta}, \Gamma \sqcup \epsilon \models v : \tau$ by definition
 . . $\vec{\delta}, \Gamma \models G.l : \tau$ by definition
 . . $\vec{\delta}, \Gamma \models e.l : \tau$ by substitution
 . **case** $\vec{\delta}, \vec{\sigma} \models \Gamma \quad e[\vec{\sigma}] \rightsquigarrow e'[\vec{\sigma} \sqcup \vec{\sigma}'] \quad \vec{\delta}, \vec{\sigma}' \models \Gamma' \quad \vec{\delta}, \Gamma \sqcup \Gamma' \models e' : l \rightarrow \tau$
 . **hypo** $\vec{\delta}, \Gamma \sqcup \Gamma' \models e' : l \rightarrow \tau \implies \vec{\delta}, \Gamma \sqcup \Gamma' \models e'.l : \tau$
 . **wrt** $\vec{\sigma} e' \vec{\sigma}' \Gamma'$
 . . $\vec{\delta}, \Gamma \sqcup \Gamma' \models e'.l : \tau$ by application
 . . $e[\vec{\sigma}].l \rightsquigarrow e'[\vec{\sigma} \sqcup \vec{\sigma}'].l$ by definition
 . . $e[\vec{\sigma}].l = e.l[\vec{\sigma}]$ by definition
 . . $e'[\vec{\sigma} \sqcup \vec{\sigma}'].l = e'.l[\vec{\sigma} \sqcup \vec{\sigma}']$ by definition
 . . $e.l[\vec{\sigma}] \rightsquigarrow e'.l[\vec{\sigma} \sqcup \vec{\sigma}']$ by substitution
 . . $\vec{\delta}, \Gamma \models e.l : \tau$ by definition
 . $\vec{\delta}, \Gamma \models e.l : \tau$ by induction
 \square

Theorem 8.21. (Proof subtyping consistency)

$$\frac{\tau_l <: \tau_r \dashv M, \Delta}{\exists \vec{\delta}. \vec{\delta} \models \Delta}$$

Theorem 8.22. (Proof subtyping soundness)

$$\frac{\tau_l <: \tau_r \dashv M, \Delta}{\exists \vec{\delta}. \vec{\delta} \models \tau_l <: \tau_r}$$

Theorem 8.23. (Proof subtyping weak soundness)

$$\frac{\tau_l <: \tau_r \dashv M, \Delta}{\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r}$$

TODO: closed variableless simply remove variables from soundness consideration Proof:

TODO: think about how to handle the mutually recursive definition

assume $\tau_l <: \tau_r \dashv M, \Delta$

- . **induct on** $\tau_l <: \tau_r \dashv M, \Delta$
- . **case** $\tau_l = \tau \quad \tau_r = \tau$
- . **wrt** τ
- . . **for** $\vec{\delta}$ **assume** $\vec{\delta} \models \Delta$
- . . . $\vec{\delta} \models \tau <: \tau$ by theorem 8.37
- . . . $\vec{\delta} \models \tau_l <: \tau_r$ by substitution
- . . $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$ by implication and generalization
- . **case** $\tau_l = \text{BOT}$
- . . **for** $\vec{\delta}$ **assume** $\vec{\delta} \models \Delta$
- . . . $\vec{\delta} \models \text{BOT} <: \tau_r$ by definition
- . . . $\vec{\delta} \models \tau_l <: \tau_r$ by substitution
- . . $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$ by implication and generalization
- . **case** $\tau_r = \text{TOP}$
- . . **for** $\vec{\delta}$ **assume** $\vec{\delta} \models \Delta$
- . . . $\vec{\delta} \models \tau_l <: \text{TOP}$ by definition
- . . . $\vec{\delta} \models \tau_l <: \tau_r$ by substitution
- . . $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$ by implication and generalization
- . **case** $\tau_r = l \rightarrow (\tau_{rl} \& \tau_{rr}) \quad \tau_l <: (l \rightarrow \tau_{rl}) \& (l \rightarrow \tau_{rr}) \dashv M, \Delta$
- . **hypo** $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: (l \rightarrow \tau_{rl}) \& (l \rightarrow \tau_{rr})$
- . **wrt** $l \ \tau_{rl} \ \tau_{rr}$
- . . **for** $\vec{\delta}$ **assume** $\vec{\delta} \models \Delta$
- . . . $\vec{\delta} \models \tau_l <: (l \rightarrow \tau_{rl}) \& (l \rightarrow \tau_{rr})$ by application
- . . . **for** $e \ \Gamma$ **assume** $\vec{\delta}, \Gamma \models e : \tau_l$
- $\vec{\delta}, \Gamma \models e : (l \rightarrow \tau_{rl}) \& (l \rightarrow \tau_{rr})$ by theorem 8.38
- $\vec{\delta}, \Gamma \models e : l \rightarrow \tau_{rl}$ by theorem 8.36
- $\vec{\delta}, \Gamma \models e : l \rightarrow \tau_{rr}$ by theorem 8.36
- $\vec{\delta}, \Gamma \models e.l : \tau_{rl}$ by theorem 8.20
- $\vec{\delta}, \Gamma \models e.l : \tau_{rr}$ by theorem 8.20
- $\vec{\delta}, \Gamma \models e.l : \tau_{rl} \& \tau_{rr}$ by definition
- $\vec{\delta}, \Gamma \models e : l \rightarrow (\tau_{rl} \& \tau_{rr})$ by theorem 8.34

```

. . .  $\vec{\delta}, \Gamma \models e : \tau_r$  by substitution
. . .  $\forall e \Gamma. \vec{\delta}, \Gamma \models e : \tau_l \implies \vec{\delta}, \Gamma \models e : \tau_r$  by implication and generalization
. . .  $\vec{\delta} \models \tau_l <: \tau_r$  by definition
. .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. case  $\tau_l = \tau_{ll} \mid \tau_{lr}$   $M = M_1$   $\Delta = \Delta_1$ 
. |  $\tau_{ll} <: \tau_r \dashv M_0, \Delta_0$   $M_0 \preceq M_1$   $\Delta_0 \preceq \Delta_1$   $\tau_{lr} <: \tau_r \dashv M_1, \Delta_1$ 
. hypo  $\forall \vec{\delta}. \vec{\delta} \models \Delta_0 \implies \vec{\delta} \models \tau_{ll} <: \tau_r$   $\forall \vec{\delta}. \vec{\delta} \models \Delta_1 \implies \vec{\delta} \models \tau_{lr} <: \tau_r$ 
. wrt  $\tau_{ll} \tau_{lr}$ 
. . for  $\vec{\delta}$  assume  $M, \vec{\delta} \models \Delta$ 
. . .  $\vec{\delta} \models \Delta_1$  by substitution
. . .  $\vec{\delta} \models \tau_{lr} <: \tau_r$  by application
. . .  $\vec{\delta} \models \Delta_0$  by theorem ?? TODO: ...
. . .  $\vec{\delta} \models \tau_{ll} <: \tau_r$  by application
. . .  $\vec{\delta} \models \tau_{ll} \mid \tau_{lr} <: \tau_r$  by definition
. . .  $\vec{\delta} \models \tau_l <: \tau_r$  by substitution
. .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. case  $\tau_r = \tau_{rl} \& \tau_{rr}$   $M = M_1$   $\Delta = \Delta_1$ 
. |  $\tau_l <: \tau_{rl} \dashv M_0, \Delta_0$   $M_0 \preceq M_1$   $\Delta_0 \preceq \Delta_1$   $\tau_l <: \tau_{rr} \dashv M_1, \Delta_1$ 
. hypo  $\forall \vec{\delta}. \vec{\delta} \models \Delta_0 \implies \vec{\delta} \models \tau_l <: \tau_{rl}$   $\forall \vec{\delta}. \vec{\delta} \models \Delta_1 \implies \vec{\delta} \models \tau_l <: \tau_{rr}$ 
. wrt
. . for  $\vec{\delta}$  assume  $\vec{\delta} \models \Delta$ 
. . .  $\vec{\delta} \models \Delta_1$  by substitution
. . .  $\vec{\delta} \models \tau_l <: \tau_{rr}$  by instantiation and application
. . .  $\vec{\delta} \models \Delta_0$  by theorem ?? TODO: ...
. . .  $\vec{\delta} \models \tau_l <: \tau_{rl}$  by instantiation and application
. . .  $\vec{\delta} \models \tau_l <: \tau_{rl} \& \tau_{rr}$  by definition
. . .  $\vec{\delta} \models \tau_l <: \tau_r$  by substitution
. .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. case
. hypo
. wrt
. . TODO: ...
. case
. hypo
. wrt
. . TODO: ...
. case  $\tau_l = \text{EXI}[A \ Q] \tau_b$   $M = M_1$   $\Delta = \Delta_1$ 
. |  $Q \dashv M_0, \Delta_0$   $A \# \tau_r$   $M_0 \sqcup A \preceq M_1$   $\Delta_0 \preceq \Delta_1$   $\tau_b <: \tau_r \dashv M_1, \Delta_1$ 
. hypo  $\forall \vec{\delta}. \vec{\delta} \models \Delta_1 \implies \vec{\delta} \models M_1, \tau_b <: \tau_r$ 
. mutu  $\forall \vec{\delta}. \vec{\delta} \models \Delta_0 \implies \vec{\delta} \models Q$  by theorem ?? TODO: sequence soundness / mutual
dependence
. wrt  $A \ Q \ \tau_b \ M_1 \ \Delta_1 \ M_0 \ \Delta_0$ 
. . for  $\vec{\delta}$  assume  $\vec{\delta} \models \Delta$ 
. . .  $\vec{\delta} \models \Delta_1$  by substitution
. . .  $\vec{\delta} \models \tau_b <: \tau_r$  by application

```

```

. . .  $\vec{\delta} \models \Delta_0$  by theorem 8.28
. . .  $\vec{\delta} \models Q$  by application
. . . for  $e$  assume  $\vec{\delta} \models e : \tau_l$ 
. . . .  $\vec{\delta} \models e : \text{EXI}[A \ Q] \tau_b$  by substitution
. . . .  $\vec{\delta} \models e : \tau_r$  by theorem 8.24
. . . .  $\forall e. \vec{\delta} \models e : \tau_l \implies \vec{\delta} \models e : \tau_r$ 
. . . .  $\vec{\delta} \models \tau_l <: \tau_r$  by definition
. . .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. case  $\tau_r = \text{ALL}[A \ Q] \tau_b \quad M = M_1 \quad \Delta = \Delta_1$ 
. |  $Q \dashv M_0, \Delta_0 \quad A \# \tau_l \quad M_0 \sqcup A \preceq M_1 \quad \Delta_0 \preceq \Delta_1 \quad \tau_l <: \tau_b \dashv M_1, \Delta_1$ 
. hypo  $\forall \vec{\delta}. \vec{\delta} \models \Delta_1 \implies \vec{\delta} \models \tau_l <: \tau_b$ 
. mutu  $\forall \vec{\delta}. \vec{\delta} \models \Delta_0 \implies \vec{\delta} \models Q$  by theorem ?? TODO: sequence soundness / mutual
dependence
. wrt  $A \ Q \ \tau_b \ M_1 \ \Delta_1 \ M_0 \ \Delta_0$ 
. . for  $\vec{\delta}$  assume  $\vec{\delta} \models \Delta$ 
. . .  $\vec{\delta} \models \Delta_1$  by substitution
. . .  $\vec{\delta} \models \tau_l <: \tau_b$  by application
. . .  $\vec{\delta} \models \Delta_0$  by theorem 8.28
. . .  $\vec{\delta} \models Q$  by application
. . . for  $e$  assume  $\vec{\delta} \models e : \tau_l$ 
. . . .  $\vec{\delta} \models e : \text{ALL}[A \ Q] \tau_b$  by theorem 8.25
. . . .  $\vec{\delta} \models e : \tau_r$  by substitution
. . . .  $\forall e. \vec{\delta} \models e : \tau_l \implies \vec{\delta} \models e : \tau_r$ 
. . . .  $\vec{\delta} \models \tau_l <: \tau_r$  by definition
. . .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. . TODO: ...
. case  $\tau_l = \alpha \quad M = M_1 \quad \Delta = \Delta_1 \quad \alpha <: \tau_r$ 
. |  $\alpha \notin M_0 \quad M_0, \Delta_0 \vdash \Delta_m <:^\# \alpha / \tau_r \quad M_0, \Delta_0 \vdash T <:^\dagger \alpha \quad M_0 \preceq M_1$ 
. |  $\Delta_0 \sqcup \Delta_m \preceq \Delta_1 \quad |(T) <: \tau_r \dashv M_1, \Delta_1$ 
. hypo  $\forall \vec{\delta}. \vec{\delta} \models \Delta_1 \implies \vec{\delta} \models |(T) <: \tau_r$ 
. wrt  $\alpha \ M_1 \ \Delta_1 \ M_0 \ \Delta_0 \ \Delta_m \ T$ 
. . for  $\vec{\delta}$  assume  $\vec{\delta} \models \Delta$ 
. . .  $\vec{\delta} \models \Delta_1 (\alpha <: \tau_r)$  by substitution
. . .  $\vec{\delta} \models \alpha <: \tau_r$  by theorem 8.26
. . .  $\vec{\delta} \models \tau_l <: \tau_r$  by substitution
. . .  $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$  by implication and generalization
. . TODO: ...
. case
. hypo
. wrt
. . TODO: ...
. case
. hypo
. wrt
. . TODO: ...

```

. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. case
. hypo
. wrt
. . **TODO: ...**
. $\forall \vec{\delta}. \vec{\delta} \models \Delta \implies \vec{\delta} \models \tau_l <: \tau_r$ by induction
□ by implication

Theorem 8.24. Model typing existential elimination

$$\frac{\vec{\delta} \models e : \text{EXI}[A \ Q] \tau_l \quad \vec{\delta} \models Q \quad \vec{\delta} \models \tau_l <: \tau_r \quad A \# \tau_r}{\vec{\delta} \models e : \tau_r}$$

Proof:

TODO: depends on proof subtyping. can we abstract away proof subtyping?

Theorem 8.25. Model typing universal introduction

$$\frac{\vec{\delta} \models e : \tau_l \quad \vec{\delta} \models Q \quad \vec{\delta} \models \tau_l <: \tau_r \quad A \# \tau_l}{\vec{\delta} \models e : \text{ALL}[A \ Q] \tau_r}$$

Proof:

TODO: depends on proof subtyping. can we abstract away proof subtyping?

Theorem 8.26. Model subtyping sequence last

$$\frac{\vec{\delta} \models \Delta \ (\tau_l <: \tau_r)}{\vec{\delta} \models \tau_l <: \tau_r}$$

Proof:

TODO: ...

Theorem 8.27. Model subtyping sequence reduction

$$\frac{\vec{\delta} \models \Delta \ \delta}{\vec{\delta} \models \Delta}$$

Proof:

TODO: ...

Theorem 8.28. Model subtyping sequence prefix

$$\frac{\vec{\delta} \models \Delta' \quad \Delta \preceq \Delta'}{\vec{\delta} \models \Delta}$$

Proof:

TODO: ...

Theorem 8.29. Model subtyping sequence uncat

$$\frac{\vec{\delta} \models \Delta \sqcup \Delta'}{\vec{\delta} \models \Delta}$$

Proof:

TODO: ...

Theorem 8.30. concatenation prefix

$$\overline{\Delta \preceq \Delta \sqcup \Delta'}$$

Proof:

TODO: ...

Theorem 8.31. Model subtyping unsub left

$$\frac{\vec{\delta} \models \tau_l <: \tau_r \quad \alpha / \tau_l \in \vec{\delta}}{\vec{\delta} \models \alpha <: \tau_r}$$

Proof:

TODO: ...

Theorem 8.32. Model subtyping unsub right

$$\frac{\vec{\delta} \models \tau_l <: \tau_r \quad \alpha / \tau_r \in \vec{\delta}}{\vec{\delta} \models \tau_l <: \alpha}$$

Proof:

TODO: ...

Theorem 8.33. Model subtyping something

$$\frac{\vec{\delta} \models \Delta \quad M, \Delta \vdash T <:^\# \alpha}{\alpha / \mid (T) \in \vec{\delta}}$$

Proof:

TODO: ...

Theorem 8.34. Model typing record introduction

$$\frac{\vec{\delta} \models e.l : \tau}{\vec{\delta} \models e : l \rightarrow \tau}$$

Proof:

TODO: ...

Theorem 8.35. Model typing implication introduction **TODO: this is really messed up**

$$\frac{\vec{\delta} \models e_0(e_1) : \tau_r \quad \vec{\delta} \models e_1 : \tau_l \quad \forall \tau. \vec{\delta} \models e_1 : \tau \implies \tau_l <: \tau}{\vec{\delta} \models e_0 : \tau_l \rightarrow \tau_r}$$

Proof:

TODO: ...

Theorem 8.36. Model typing intersection elimination

$$\frac{\vec{\delta} \models e : \tau_l \& \tau_r}{\vec{\delta} \models e : \tau_l \wedge \vec{\delta} \models e : \tau_r}$$

Proof:

TODO: ...

Theorem 8.37. Model typing reflexivity

$$\overline{\vec{\delta} \models \tau <: \tau}$$

Proof:

for $e \in \Gamma$ **assume** $\vec{\delta}, \Gamma \models e : \tau$

. $\vec{\delta}, \Gamma \models e : \tau$ by identity

$\forall e \in \Gamma. \vec{\delta}, \Gamma \models e : \tau \implies \vec{\delta}, \Gamma \models e : \tau$ by implication and generalization

□ by definition

Theorem 8.38. (Model typing subsumption)

$$\frac{\vec{\delta}, \Gamma \models e : \tau_l \quad \vec{\delta}, \Gamma \models \tau_l <: \tau_r}{\vec{\delta}, \Gamma \models e : \tau_r}$$

Proof:

assume $\vec{\delta}, \Gamma \models e : \tau_l \quad \vec{\delta}, \Gamma \models \tau_l <: \tau_r$

. **invert on** $\vec{\delta}, \Gamma \models \tau_l <: \tau_r$

. **case** $\forall e'. \vec{\delta}, \Gamma \models e' : \tau_l \implies \vec{\delta}, \Gamma \models e' : \tau_r$

. . $\forall e'. \vec{\delta}, \Gamma \models e' : \tau_l \implies \vec{\delta}, \Gamma \models e' : \tau_r$ by identity

. $\forall e'. \vec{\delta}, \Gamma \models e' : \tau_l \implies \vec{\delta}, \Gamma \models e' : \tau_r$ by inversion

. $\vec{\delta}, \Gamma \models e : \tau_l \implies \vec{\delta}, \Gamma \models e : \tau_r$ by instantiation

. $\vec{\delta}, \Gamma \models e : \tau_r$ by application

□ by implication

Theorem 8.39. (Model typing implication elimination)

$$\frac{\vec{\delta}, \Gamma \models e_0 : \tau_l \multimap \tau_r \quad \vec{\delta}, \Gamma \models e_1 : \tau_l}{\vec{\delta}, \Gamma \models e_0(e_1) : \tau_r}$$

assume $\vec{\delta}, \Gamma \models e_0 : \tau_l \multimap \tau_r \quad \vec{\delta}, \Gamma \models e_1 : \tau_l$

- . **let** $\vec{\sigma}$ **s.t.** $\vec{\delta}, \vec{\sigma} \models \Gamma$ by theorem ??
- . **induct on** $\vec{\delta}, \Gamma \models e_0 : \tau_l \multimap \tau_r$
- . **case** **TODO: ...**
- . **case** $e_0 = F\$p \Rightarrow e_2 \quad \vec{\delta}, \Gamma \models F : \tau_l \multimap \tau_r$
- . **hypo** $\vec{\delta}, \Gamma \models F(e_1) : \tau_r$
- . **wrt** $F \ p \ e_2$
 - . $\models F(e_1)[\vec{\sigma}]$ by theorem 8.51
 - . **invert on** $\models F(e_1)[\vec{\sigma}]$
 - . **case** $F(e_1)[\vec{\sigma}] = v$
 - . **wrt** v
 - . $F(e_1)[\vec{\sigma}] \neq v$ by definition
 - . \perp by application
 - . **case** $(F(e_1))[\vec{\sigma}] \rightsquigarrow e_3 \quad \vec{\delta}, \Gamma \models e_3 : \tau_r$
 - . **wrt** e_3
 - . $(F(e_1))[\vec{\sigma}] = F[\vec{\sigma}](e_1[\vec{\sigma}])$ by definition
 - . $F[\vec{\sigma}](e_1[\vec{\sigma}]) \rightsquigarrow e_3$ by substitution
 - . **let** F' **s.t.** $F[\vec{\sigma}] = F'$ by theorem ?? **TODO: ...**
 - . **let** e'_1 **s.t.** $e_1[\vec{\sigma}] = e'_1$ by theorem ?? **TODO: ...**
 - . $FV(e_2[\vec{\sigma} \setminus FV(p)]) \subseteq FV(p)$ by theorem ?? **TODO: ...**
 - . $F'(e'_1) \rightsquigarrow e_3$ by substitution
 - . $(F' \$p \Rightarrow e_2[\vec{\sigma} \setminus FV(p)])(e'_1) \rightsquigarrow e_3$ by definition
 - . $(F[\vec{\sigma}] \$p \Rightarrow e_2[\vec{\sigma} \setminus FV(p)])(e_1[\vec{\sigma}]) \rightsquigarrow e_3$ by substitution
 - . $((F \$p \Rightarrow e_2)(e_1))[\vec{\sigma}] = (F[\vec{\sigma}] \$p \Rightarrow e[\vec{\sigma} \setminus FV(p)])(e_1[\vec{\sigma}])$ by definition
 - . $((F \$p \Rightarrow e_2)(e_1))[\vec{\sigma}] \rightsquigarrow e_3$ by substitution
 - . $\vec{\delta}, \Gamma \models (F \$p \Rightarrow e)(e_1) : \tau_r$ by definition
 - . $\vec{\delta}, \Gamma \models (F \$p \Rightarrow e)(e_1) : \tau_r$ by inversion
 - . **case** $\vec{\delta}, \vec{\sigma} \models \Gamma \quad e_0[\vec{\sigma}] \rightsquigarrow e'_0 \quad \vec{\delta}, \Gamma \models e'_0 : \tau_l \multimap \tau_r$
 - . **hypo** $\vec{\delta}, \Gamma \models e'_0 : \tau_l \multimap \tau_r \implies \vec{\delta}, \Gamma \models e'_0(e_1) : \tau_r$
 - . **wrt** $\vec{\sigma} \ e'_0$
 - . $\vec{\delta}, \Gamma \models e'_0(e_1) : \tau_r$ by application
 - . $e_0[\vec{\sigma}](e_1) \rightsquigarrow e'_0(e_1)$
 - . $(e_0(e_1))[\vec{\sigma}] \rightsquigarrow e'_0(e_1)$
 - . $\vec{\delta}, \Gamma \models e_0(e_1) : \tau_r$
 - . $\vec{\delta}, \Gamma \models e_0(e_1) : \tau_r$ by induction

□

Theorem 8.40. Model typing reduced implication elimination

$$\frac{\vec{\delta}, \Gamma \models (F \$p \Rightarrow e) : \tau_l \multimap \tau_r \quad \vec{\delta}, \Gamma \models e_1 : \tau_l \quad F = \epsilon \vee \vec{\delta}, \Gamma \models F(e_1) : \tau_r}{\vec{\delta}, \Gamma \models (F \$p \Rightarrow e)(e_1) : \tau_r}$$

assume $\models e_1[\vec{\sigma}]$
 . **let** $\vec{\sigma}$ **s.t.** $\vec{\delta}, \vec{\sigma} \models \Gamma$ by theorem 8.50
 . $\models e_1[\vec{\sigma}]$ by theorem 8.51
 . **induct on** $\models e_1[\vec{\sigma}]$
 . **case** $e_1[\vec{\sigma}] = v_1$
 . **wrt** v_1
 . . $\vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e_1) : \tau_r$ by theorem 8.41
 . **case** $e_1[\vec{\sigma}] \rightsquigarrow e'_1 \models e'_1$
 . **hypo** $\models e'_1 \implies \vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e'_1) : \tau_r$
 . **wrt** e'_1
 . . $\vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e'_1) : \tau_r$ by application
 . . $(F\$p \Rightarrow e)[\vec{\sigma}](e_1[\vec{\sigma}]) \rightsquigarrow (F\$p \Rightarrow e)[\vec{\sigma}](e'_1)$ by definition
 . . $\forall x. x \notin \mathbf{FV}(e'_1)$ by theorem 8.48
 . . $e'_1 = e'_1[\vec{\sigma}]$ by theorem 8.49
 . . $(F\$p \Rightarrow e)[\vec{\sigma}](e_1[\vec{\sigma}]) \rightsquigarrow (F\$p \Rightarrow e)[\vec{\sigma}](e'_1[\vec{\sigma}])$ by substitution
 . . $((F\$p \Rightarrow e)(e_1))[\vec{\sigma}] \rightsquigarrow ((F\$p \Rightarrow e)(e'_1))[\vec{\sigma}]$ by definition
 . . $\vec{\sigma} \sqcup \epsilon = \vec{\sigma}$ by definition
 . . $((F\$p \Rightarrow e)(e_1))[\vec{\sigma}] \rightsquigarrow ((F\$p \Rightarrow e)(e'_1))[\vec{\sigma} \sqcup \epsilon]$ by substitution
 . . $\Gamma \sqcup \epsilon = \Gamma$ by definition
 . . $\vec{\delta}, \epsilon \models \epsilon$ by definition
 . . $\vec{\delta}, \Gamma \sqcup \epsilon \models (F\$p \Rightarrow e)(e'_1)$ by substitution
 . . $\vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e_1) : \tau_r$ by definition
 . $\vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e_1) : \tau_r$ by induction
 □ by implication

Theorem 8.41. Model typing fully reduced implication elimination

$$\frac{\vec{\delta}, \Gamma \models (F\$p \Rightarrow e) : \tau_l \multimap \tau_r \quad F = \epsilon \vee \vec{\delta}, \Gamma \models F(e_1) : \tau_r \quad \vec{\delta} \models e_1 : \tau_l \quad \vec{\delta}, \vec{\sigma} \models \Gamma \quad e_1[\vec{\sigma}] = v_1}{\vec{\delta}, \Gamma \models (F\$p \Rightarrow e)(e_1) : \tau_r}$$

Proof:

assume $F = \epsilon \vee \vec{\delta}, \Gamma \models F : \tau_l \multimap \tau_r$ **TODO: add more assumptions**
 . $\vec{\delta} \models e_1[\vec{\sigma}] : \tau_l$ by theorem 8.45
 . $\vec{\delta} \models v_1 : \tau_l$ by substitution
 . **invert on** $F = \epsilon \vee \vec{\delta}, \Gamma \models F : \tau_l \multimap \tau_r$
 . **case** $F = \epsilon$
 . . $\vec{\delta}, \Gamma \models F\$p \Rightarrow e : \tau_l \multimap \tau_r$ by theorem ??
 . . $\vec{\delta}, \Gamma \models \$p \Rightarrow e : \tau_l \multimap \tau_r$ by substitution
 . . **let** $\vec{\sigma}'$ **s.t.** $p \equiv v_1 \dashv \vec{\sigma}'$ by theorem 8.46
 . . **for** e'
 . . . $\neg \epsilon[\vec{\sigma}](v_1) \rightsquigarrow e'$ by definition
 . . . $\neg F[\vec{\sigma}](v_1) \rightsquigarrow e'$ by substitution
 . . $\forall e'. \neg F[\vec{\sigma}](v_1) \rightsquigarrow e'$ by generalization
 . . $(F[\vec{\sigma}] \$p \Rightarrow e[\vec{\sigma} \setminus \mathbf{FV}(p)])(v_1) \rightsquigarrow e[\vec{\sigma} \setminus \mathbf{FV}(p)][\vec{\sigma}]$ by definition
 . . $\forall x. x \in \mathbf{FV}(p) \iff x \in \mathbf{dom}(\vec{\sigma}')$ by theorem 8.42
 . . $\vec{\sigma} \setminus \mathbf{FV}(p) = \vec{\sigma} \setminus \mathbf{dom}(\vec{\sigma}')$ by theorem 8.43

. . $e[\vec{\sigma} \backslash \mathbf{dom}(\vec{\sigma}')][\vec{\sigma}'] = e[\vec{\sigma} \sqcup \vec{\sigma}']$ by theorem 8.44
 . . $(F[\vec{\sigma}] \$ p \Rightarrow e[\vec{\sigma} \backslash \mathbf{FV}(p)])(v_1) \rightsquigarrow e[\vec{\sigma} \backslash \mathbf{dom}(\vec{\sigma}')][\vec{\sigma}]$ by substitution
 . . $(F[\vec{\sigma}] \$ p \Rightarrow e[\vec{\sigma} \backslash \mathbf{FV}(p)])(v_1) \rightsquigarrow e[\vec{\sigma} \sqcup \vec{\sigma}']$ by substitution
 . . $(F \$ p \Rightarrow e)[\vec{\sigma}](v_1) \rightsquigarrow e[\vec{\sigma} \sqcup \vec{\sigma}']$ by definition
 . . $(F \$ p \Rightarrow e)[\vec{\sigma}](e_1[\vec{\sigma}]) \rightsquigarrow e[\vec{\sigma} \sqcup \vec{\sigma}']$ by substitution
 . . $(F \$ p \Rightarrow e)[\vec{\sigma}](e_1[\vec{\sigma}]) = ((F \$ p \Rightarrow e)(e_1))[\vec{\sigma}]$ by definition
 . . $((F \$ p \Rightarrow e)(e_1))[\vec{\sigma}] \rightsquigarrow e[\vec{\sigma} \sqcup \vec{\sigma}']$ by substitution
 . . $\vec{\delta}, \Gamma \models (F \$ p \Rightarrow e)(e_1) : \tau_r$ by definition
 . **case** $\vec{\delta}, \Gamma \models F(e_1) : \tau_r$
 . . **let** e' **s.t.** $(F(e_1))[\vec{\sigma}] \rightsquigarrow e' \wedge \vec{\delta}, \Gamma \models e' : \tau_r$ by theorem ??
 . . $((F \$ p \Rightarrow e)(e_1))[\vec{\sigma}] \rightsquigarrow e'$ by definition
 . . $\vec{\delta}, \Gamma \models (F \$ p \Rightarrow e)(e_1) : \tau_r$ by definition
 . $\vec{\delta}, \Gamma \models (F \$ p \Rightarrow e)(e_1) : \tau_r$ by inversion
 □ by implication

Theorem 8.42. (Pattern matching consistency)

$$\frac{p \equiv v \dashv \vec{\sigma}}{\forall x. x \in \mathbf{FV}(p) \iff x \in \mathbf{dom}(\vec{\sigma})}$$

Proof:

TODO: ...

□

Theorem 8.43. (Consistency diffing)

$$\frac{\forall x. x \in X_l \iff x \in X_r}{\vec{\sigma} \backslash X_l = \vec{\sigma} \backslash X_r}$$

Proof:

TODO: ...

□

Theorem 8.44. (Concatenation Substitution)

$$\overline{e[\vec{\sigma} \backslash \mathbf{dom}(\vec{\sigma}')][\vec{\sigma}'] = e[\vec{\sigma} \sqcup \vec{\sigma}']}$$

Proof:

TODO: ...

□

Theorem 8.45. (Model typing valuation)

$$\frac{\vec{\delta}, \Gamma \models e : \tau \quad \vec{\delta}, \vec{\sigma} \models \Gamma}{\vec{\delta} \models e[\vec{\sigma}] : \tau}$$

Proof:

assume $\vec{\delta}, \Gamma \models e : \tau \quad \vec{\delta}, \vec{\sigma} \models \Gamma$

TODO: ...

□

Theorem 8.46. (Model typing pattern matching)

$$\frac{\vec{\delta}, \Gamma \models \$p \Rightarrow e : \tau_l \rightarrow \tau_r \quad \vec{\delta} \models v : \tau_l}{\exists \vec{\sigma}. p \equiv v \dashv \vec{\sigma}}$$

Proof:

assume $\vec{\delta}, \Gamma \models \$p \Rightarrow e : \tau_l \rightarrow \tau_r \quad \vec{\delta} \models v : \tau_l$

TODO: ...

□

Theorem 8.47. (Well-formed function valuation)

$$\frac{\models F}{\exists v. v = F}$$

PROOF.

assume $\models F$

. **invert on** $\models F$

. **case** $v = F$

. . $v = F$ by identity

. **case** $F \rightsquigarrow e$

. **wrt** e

. . $\neg F \rightsquigarrow e$ by definition

. . \perp by application

. $v = F$ by inversion

□

□

Theorem 8.48. (Reduction closed)

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

Proof:

assume $e \rightsquigarrow e'$

TODO: ...

□

Theorem 8.49. (Closed substitution)

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

Proof:

assume $\forall x. x \notin \mathbf{FV}(e)$

TODO: ...

□

Theorem 8.50. (Model typing assignability)

$$\frac{\vec{\delta}, \Gamma \models e : \tau}{\exists \vec{\sigma}. \vec{\delta}, \vec{\sigma} \models \Gamma}$$

Proof:

TODO: ...

Theorem 8.51. (Model typing soundness)

$$\frac{\vec{\delta}, \Gamma \models e : \tau}{\forall \vec{\sigma}. \vec{\delta}, \vec{\sigma} \models \Gamma \implies \models e[\vec{\sigma}]}$$

Proof:

TODO: redo using universal/implication

assume $\vec{\delta}, \vec{\sigma} \models \Gamma \quad \vec{\delta}, \Gamma \models e : \tau$

- . **case** $e = @$
 - . . **let** v **s.t.** $@ = v$
 - . . $e[\vec{\sigma}] = v$
 - . . $\models e[\vec{\sigma}]$
- . **case** $\vec{\delta}, \Gamma \models e' : \tau' \quad e = \langle l \rangle e' \quad \tau = \langle l \rangle \tau'$
 - . . $\models e'$ by induction hypothesis
 - . . **case** $e'[\vec{\sigma}] = v$
 - . . . **let** v' **s.t.** $\langle l \rangle v = v'$
 - . . . $\langle l \rangle e'[\vec{\sigma}] = v'$
 - . . . $(\langle l \rangle e')[\vec{\sigma}] = v'$
 - . . . $e[\vec{\sigma}] = v'$
 - . . . $\models e[\vec{\sigma}]$
 - . . **case** $e'[\vec{\sigma}] \rightsquigarrow e'' \quad \models e''$
 - . . . $\langle l \rangle e'[\vec{\sigma}] \rightsquigarrow \langle l \rangle e''$
 - . . . $\models \langle l \rangle e''$
 - . . . $\models \langle l \rangle e'[\vec{\sigma}]$
 - . . . $\models (\langle l \rangle e')[\vec{\sigma}]$
 - . . . $\models e[\vec{\sigma}]$
 - . . $\models e[\vec{\sigma}]$ by cases on $\models e'$
- . **TODO: remaining introduction cases**
- . **case** $x : \tau \in \Gamma \quad x/v \in \vec{\sigma} \quad e = x$
 - . . $x[\vec{\sigma}] = v$
 - . . $e[\vec{\sigma}] = v$
 - . . $\models e[\vec{\sigma}]$
- . **case** $e[\vec{\sigma}] \rightsquigarrow e' \quad \vec{\delta}, \Gamma \models e' : \tau$
 - . . $\models e'[\vec{\sigma}]$ by induction hypothesis
 - . . $\models e[\vec{\sigma}]$
- . $\models e[\vec{\sigma}]$ by induction on $\vec{\delta}, \Gamma \models e : \tau$

□

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 $\vec{\delta}, \Gamma \models e : \tau$ 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 8.45.

$$\boxed{\vec{\delta}, \vec{\sigma} \models \Gamma}$$

$$\frac{}{\vec{\delta}, \vec{\sigma} \models \epsilon}$$

$$\frac{\vec{\delta}, \vec{\sigma} \models \Gamma \quad \vec{\delta} \models v : \tau}{\vec{\delta}, \vec{\sigma} \ x/v \models \Gamma \ x : \tau}$$