System $F_{\&}$: A Simple Core Language for Extensibility

Name1
Affiliation1
Email1

Name2 Name3
Affiliation2/3
Email2/3

Abstract

Over the years there have been various proposals for *design patterns* for improved *extensibility* of programs. Examples include *Object Algebras*, *Modular Visitors* or Torgersen's design patterns using generics. Although those design patterns give practical benefits in terms of extensibility, they also expose limitations in existing mainstream OOP languages. Some pressing limitations are: 1) lack of good mechanisms for *object-level* composition; 2) *conflation of (type) inheritance with subtyping*; 3) *heavy reliance on generics*.

This paper presents System $F_{\&}$: an extension of System F with *intersection types* and a *merge operator*. The goal of System $F_{\&}$ is to study the minimal language constructs needed to support various extensible designs, while at the same time addressing the limitations of existing OOP languages. To address the lack of good object-level composition mechanisms, System $F_{\&}$ uses the merge operator to do dynamic composition of values/objects. Moreover, in System $F_{\&}$ type inheritance is independent of subtyping, and an extension can be a supertype of a base object type. Finally, System $F_{\&}$ replaces many uses of generics by intersection types or conventional subtyping. System $F_{\&}$ is formalized and implemented. Moreover the paper shows how various extensible designs can be encoded in System $F_{\&}$.

bruno: Make all figures fit and be well-formated!

1. Introduction

There has been a remarkable number of works aimed at improving support for extensibility in programming languages. These works include: visions of new programming models [23, 34, 38]; new programming languages or language extensions []bruno: fill!, and *design patterns* that can be used with existing mainstream languages [14, 28, 39, 43].

Some of the more recent work on extensibility is focused on various proposals for design patterns. Examples include *Object Algebras* [28], *Modular Visitors* [14, 39] or Torgersen's [39] four design patterns using generics. In those approaches the idea is to use some advanced (but already available) features, such as *generics* [3], in combination with conventional OOP features to model more extensible designs. Those designs work in modern OOP languages such as Java, C# or Scala.

Although such design patterns give practical benefits in terms of extensibility, they also expose limitations in existing mainstream OOP languages. In particular there are three pressing limitations: 1) lack of good mechanisms for *object-level* composition; 2) *conflation of (type) inheritance with subtyping*; 3) *heavy reliance on generics*.

The first limitation shows up, for example, encodings of Feature-Oriented Programming [34] or Attribute Grammars [25] using Object Algebras [29, 35]. These programs are best expressed using a form of *type-safe*, *dynamic*, *delegation*-based composition. Although such form of composition can be encoded in languages like Scala, it requires the use of low-level reflection techniques, such as dynamic proxies, reflection or other forms of meta-programming. It is clear that better language support would be desirable.

The second limitation shows up in designs for modelling modular or extensible visitors [14]. The vast majority of modern OOP languages combines type inheritance and subtyping. That is a type extension induces a subtype. However as Cook et al. [11] famously argued there are programs where "*subtyping is not inheritance*". Interestingly previously not many practical programs have been reported in the literature where the distinction between subtyping and inheritance is relevant. However, as shown in this paper, it turns out that this difference does show up in practice when designing modular (extensible) visitors. We believe that modular visitors provide a compeling example where inheritance and subtyping should not be conflated!

Finally, the third limitation is prevalent in many extensible designs [14, 29, 35, 39, 43]. Such designs rely on advanced features of generics, such as *f-bounded polymorphism* [4], *variance annotations* [24], *wildcards* [40] and/or *higher-kinded types* [27] to achieve type-safety. Sadly, the amount of type-annotations, combined with the lack of un-

CONF 'yy, Month d–d, 20yy, City, ST, Country.

http://dx.doi.org/10.1145/nnnnnnn.nnnnnnn

derstanding of these features, usually deters programmers from using such designs.

This paper presents System $F_{\&}$: an extension of System F [36] with intersection types and a merge operator [18]. The goal of System $F_{\&}$ is to study the *minimal* foundational language constructs that are needed to support various extensible designs, while at the same time addressing the limitations of existing OOP languages. To address the lack of good object-level composition mechanisms, System $F_{\&}$ uses the merge operator to allow dynamic composition of values/objects. Moreover, in System $F_{\&}$ (type-level) extension is independent of subtyping, and it is possible for an extension to be a supertype of a base object type. Furthermore, intersection types and conventional subtyping can be used in many cases instead of advanced features of generics. Indeed this paper shows how many previous designs in the literature can be encoded without such advanced features of generics.

Technically speaking System $F_{\&}$ is mainly inspired by the work of Dundfield [18]. Dundfield shows how to model a simply typed calculus with intersection types and a merge operator. The presence of a merge operator adds significant expressiveness to the language, allowing encodings for many other language constructs as syntactic sugar. System $F_{\&}$ differs from Dundfield's work in a few ways. Firstly it adds parametric polymorphism and formalizes a extension for records to support a basic form of objects. Secondly, the elaboration semantics into System F is done directly from the source calculus with subtyping. In contrast Dunfield has an additional step which eliminates subtyping. Finally a non-technical difference is that System $F_{\&}$ is aimed at studying issues of OOP languages and extensibility, whereas Dunfield's work was aimed at Functional Programming and he did not consider applications to extensibility. Like many other foundational formal models for OOP (for example []bruno: fill!), System $F_{\&}$ is purely functional and it uses structural typing.

In summary, the contributions of this paper are:

- **A Minimal Core Language for Extensibility:** This paper identifies a minimal core language, System $F_{\&}$, capable of expressing various extensibility designs in the literature. System $F_{\&}$ also addresses limitations of existing OOP languages that complicate extensible designs.
- **Formalization of System $F_{\&}$:** An elaboration semantics of System $F_{\&}$ into System F is given, and type-soundness is proved.
- **Encodings of Extensible Designs:** Various encodings of extensible designs into System $F_{\&}$, including *Object Algebras* and *Modular Visitors*.
- **A Practical Example where "Inheritance is not Subtyping" Matters:** This paper shows that in modular/extensible visitors suffer from the "inheritance is not subtyping problem".
- **Implementation and Examples:** An implementation of an extension of System $F_{\&}$, as well as the examples presented in the paper, are publicly available.

2. An Overview of $F_{\&}$

george: Change the examples later to something very simple.
bruno: Mention that we use some syntactic sugar, which is part of our implementation.

This section provides the reader with necessary intuition of $F_{\&}$. In $F_{\&}$, the central addition to the type system of System F is intersection types. A number of OO languages, such as Java, C#, Scala, and Ceylongeorge: cite?, already support intersection types to different degrees. Both Java and Scala supports intersection types via `&` and `with`, respectively. For example,

	Java	Scala	$F_{\&}$
Intersection without a nominal type		✓	✓
Intersection of type parameters		✓	✓
Term-level intersection			✓

A common limitation in those languages, though, is that there is no introduction construct at the term level for intersection types.

In contrast, there are introduction construct for function types (lambdas) and universal quantification (big lambdas) in most core calculi. To fill this gap, we allow intersecting any two terms at run time using a *merge* operator, similar to Dunfield's [18] approach. The key constructs are the "merge" operator, denoted by , , at the term level and the corresponding type intersection operator, denoted by & at the type level.

The addition of intersection types to System F has a number of consequences, which we will explore one by one in the following subsections.

2.1 Intersection Types

We motivate the use of intersection types with overloaded function, as intersection types provide a simple mechanism for ad-hoc polymorphism, similar to what type classes in Haskell achieve. The benefit is that programmers can use the same operation on different types and delegate the task of choosing a concrete implementation to the type system. For example, we can define a `show` function that takes either an integer or a boolean and return its string representation. In other words, it is also *both* a function from integers to strings as well as a function from boolean to strings. Therefore, in $F_{\&}$ it should be of following type:

```
(Int -> String) & (Bool -> String)
```

Assuming we have the following two functions available,

```
let showInt : Int -> String = ...
let showBool : Bool -> String = ...
```

We may define `show` by merging the them using the merge operator (, ,):

```
let show = showInt ,, showBool
```

To illustrate the usage, consider the function application `show 100`. The type system will pick the first component of

`show`, namely `showInt`, as the implementation being applied to `100` because the type of `showInt` is compatible with `100` , but `showBool` is not. This example shows that one may regard intersections in our system as "implicit pairs" whose introduction is explicit by the merge operator and elimination is implicit (with no source-level construct for elimination).

2.2 Subtyping

bruno: Use the show example to illustrate subtyping in our language; and show other forms of subtyping. As a result of intersection types, the type system of $F_{\&}$ permits a subtyping relation naturally. The subtyping also arises from contravariant paramter types and covariant return types for functions. Subtyping in $F_{\&}$ is structual. We will explore the usefulness of such a type system in practice by showing various examples.

2.3 Intersection Types and Records

bruno: Show and talk about the record types too! bruno: we support "object/value-level composition". Contrast with class-level or trait level composition in Scala. With intersection types, we are able to regard multi-field records as just merges of single-field records, for example:

```
{ x = 1, y = 2 }
```

is just syntatic sugar for

```
{ x = 1 } ,, { y = 2 }
```

In addition, a record is just a normal type and can be merged with any other terms, for example, this is a also valid expression

```
1 ,, { x = 2 }
```

and we can further extract a field out of it, such as

```
(1 ,, { x = 2 }).x
```

That is because a record type of the form $\{l{:}\tau\}$ can be thought as a normal type `t` tagged by the label `l`. In consequence, $F_{\&}$ supports a generalization of record elimination and update that works for any type. Functional update can be done using the *with* keyword:

```
(1 ,, { x = 2 }) with { x = 1 }
```

2.4 Intersection Types and Parametric Polymorphism

The presence of both parametric polymorphism and intersection is critical, as we shall see in the next section, in solving modularity problems. The most simple example is a function that just uses the merge operator:

```
let merge [A] [B] (x: A) (y: B) : A & B = x ,, y
```

The key novel feature is that in our language we allow the intersection of type parameters. bruno: Show also how to use merge. bruno: Syntax for type applications looks uncurried.

bruno: Talk about Inheritance is not Subtyping. Describe type inheritance and subtyping, show that they don't necessarelly go along together in our language. You may need to write some Java code, to illustrate differences. *We support contravariant argument types!*

bruno: Related to the previous point, don't forget to mention that there are nominal languages, that also separate inheritance from subtyping! See Klaus Ostermann's paper & "Inheritance is not Subtyping".

3. Application

This section shows that the System F plus intersection types are enough for encoding extensible designs, and even beat the designs in languages with a much more sophisticated type system. In particular, $F_{\&}$ has two main advantages over existing languages:

1. It supports dynamic composition of intersecting values.
2. It supports contravariant parameter types in the subtyping relation.

Various solutions have been proposed to deal with the extensibility problems and many rely on heavyweight language features such as abstract methods and classes in Java.

bruno: I would like to see a story about Church Encodings in $F_{\&}$. Can you look at Pierce's papers and try to write something along those lines? That will be a good intro for object algebras and visitors!

These two features can be used to improve existing designs of modular programs.

The expression problem refers to the difficulty of adding a new operations and a new data variant without changing or duplicating existing code.

There has been recently a lightweight solution to the expression problem that takes advantage of covariant return types in Java. We show that FI is able to solve the expression problem in the same spirit. The A)

```
trait Expr {
  def eval: Int
}

class Lit(n: Int) extends Expr {
  def eval: Int = n
}

class Add(n: Int) extends Expr {
  def eval: Int = e1.eval + e2.eval
}
```

Dunfield [18] notes that using merges as a mechanism of overloading is not as powerful as type classes.

3.1 Encoding Bounded Polymorphism

As $F_{\&}$ extends System F with intersection types, $F_{<:}$ extends System F with bounded polymorphism. $F_{<:}$ [33] allows giving an upper bound to the type variable in type abstractions. The idea of bounded universal quantification was discussed in the seminal paper by Cardelli and Wegner [7]. They show that bounded quantifiers are useful because it is able to solve the "loss of information" problem.

In fact, the extension of System F in the other direction, i.e., with intersection types, is able to address the same problem effectively. Suppose we have the following definitions:

```
let user = { name = "George", admin = true }
let id(user: {name: String}) = user
```

Under a structural type system, programmers would expect that passing the user to the function is allowed. They are correct. Note that in the source language multi-field records are just syntatic sugars for merges of single-field records. Therefore, user is of a subtype of the parameter due to subtyping introduced by intersection types. So far so good. But there is a problem: what if programmers wants to access the `admin` field later, like:

```
(id user).admin
```

They cannot do so as the above will not typecheck. After going through the function, the user now has only the type

```
{name: String}
```

This is rather undesired because it indeed has an `admin` field!

Bounded polymorphism enable the function to return the exact type of the argument so that we have no problem in accessing the `admin` field later. Consider the example below:

```
def id[A <: {name: String}] (user: A) = user
(id [{name: String, admin: Bool}] user).admin
```

We do not have bounded polymorphism in the source language. But we can encode that via intersection types:

```
let id[A] (user: A & {name: String}) = user in
(id [{admin: Bool}] user).admin
```

By requiring the type of the argument to be an intersection type of a type parameter and the upper bound and passing the type information, we make sure that we can still access the `admin` field later.

3.2 Object Algebras

Object algebras provide an alternative to *algebraic data types* (ADT).bruno: We are targeting an OO crowd. Mentioning algebraic datatypes is not going to be very useful there. For example, the following Haskell definition of the type of simple expressions

```
data Exp where
  Lit :: Int -> Exp
  Add :: Exp -> Exp -> Exp
```

can be expressed by the *interface* of an object algebra of simple expressions:

```
trait ExpAlg[E] {
  def lit(x: Int): E
  def add(e1: E, e2: E): E
}
```

Similar to ADT, data constructors in object algebras are represented by functions such as `lit` and `add` inside an interface `ExpAlg`. Different with ADT, the type of the expression itself is abtracted by a type parameter `E`.

which can be expressed similarly in $F_{\&}$ as:

```
type ExpAlg E = {
  lit : Int -> E,
  add : E -> E -> E
}
```

Scala supports intersection types via the `with` keyword. The type `A with B` expresses the combined interface of `A` and `B`. The idea is similar to

```
interface AwithB extends A, B {}
```

in Java. [1]

The value level counterpart are functions of the type `A => B => A with B`. [2]

Our type system is a simple extension of System F; yet surprisingly, it is able to solve the limitations of using object algebras in languages such as Java and Scala. We will illustrate this point with an step-by-step of solving the expression problem using a source language built on top of $F_{\&}$.

Oliveira noted that composition of object algebras can be cumbersome and intersection types provides a solution to that problem.

We first define an interface that supports the evaluation operation:

```
type IEval = { eval : Int };
type ExpAlg E = { lit : Int -> E, add : E -> E ->
    E };
let evalAlg = {
  lit = \(x : Int). { eval = x },
  add = \(x : IEval). \(y : IEval). { eval = x.eval
      + y.eval }
};
```

The interface is just a type synonym `IEval`. In $F_{\&}$, record types are structural and hence any value that satisfies this interface is of type `IEval` or of a subtype of `IEval`. [3]

In the following, `ExpAlg` is an object algebra interface of expressions with literal and addition case. And `evalAlg` is an object algebra for evluation of those expressions, which has type `ExpAlg Int`

```
type SubExpAlg E = (ExpAlg E) & { sub : E -> E ->
    E };
let subEvalAlg = evalAlg ,, { sub = \ (x : IEval).
     \ (y : IEval). { eval = x.eval - y.eval } };
```

Next, we define an interface that supports pretty printing.

```
type IPrint = { print : String };
let printAlg = {
  lit = \(x : Int). { print = x.toString() },
  add = \(x : IPrint). \(y : IPrint). { print = x.
      print.concat(" + ").concat(y.print) },
  sub = \(x : IPrint). \(y : IPrint). { print = x.
      print.concat(" - ").concat(y.print) }
};
```

[1] However, Java would require the `A` and `B` to be concrete types, whereas in Scala, there is no such restriction.

[2] FIXME

[3] Should be mentioned in S2.

Provided with the definitions above, we can then create values using the appropriate algebras. For example: defines two expressions.

The expressions are unusual in the sense that they are functions that take an extra argument `f`, the object algebras, and use the data constructors provided by the object algebra (factory) `f` such as `lit`, `add` and `sub` to create values. Moreover, The algebras themselves are abstracted over the allowed operations such as evaluation and pretty printing by requiring the expression functions to take an extra argument `E`.

```
let merge A B (f : ExpAlg A) (g : ExpAlg B) = {
  lit = \(x : Int). f.lit x ,, g.lit x,
  add = \(x : A & B). \(y : A & B).
        f.add x y ,, g.add x y
};
```

If we would like to have an expression that supports both evaluation and pretty printing, we will need a mechanism to combine the evaluation and printing algebras. Intersection types allows such composition: the `merge` function, which takes two expression algebras to create a combined algebra. It does so by constructing a new expression algebra, a record whose each field is a function that delegates the input to the two algebras taken.

```
let newAlg = merge IEval IPrint subEvalAlg
    printAlg in
let o1 = e1 (IEval & IPrint) newAlg in
o1.print
```

Note that `o1` is a single object created that supports both evaluation and printing, thus achieving full feature-oriented programming.

3.3 Visitors

Constructing instances seems clumsy!

The visitor pattern allows adding new operations to existing structures without modifying those structures. The type of expressions are defined as follows:

```
trait Exp[A] {
  def accept(f: ExpAlg[A]): A
}

trait SubExp[A] extends Exp[A] {
  override def accept(f: SubExpAlg[A]): A
}
```

The body of `Exp` and `SubExp` are almost the same: they both contain an `accept` method that takes an algebra `f` and returns a value of the carrier type `A`. The only difference is at `f` — `SubExpAlg[A]` is a subtype of `ExpAlg[A]`. Since `f` appear in parameter position of `accept` and function parameters are contravariant, naturally we would hope that `SubExp[A]` is a supertype of `Exp[A]`. However, such subtyping relation does not fit well in Scala because inheritance implies subtyping in such languages [4]. As `SubExp[A]` extends `Exp[A]`, the former becomes a subtype of the latter.

Such limitation does not exist in $F_{\&}$. For example, we can define the similar interfaces `Exp` and `SubExp`:

```
type Exp  A = { accept: forall A. ExpAlg A -> A };
type SubExp A = { accept: forall A. SubExpAlg A ->
     A };
```

Then by the typing judgment it holds that `SubExp` is a supertype of `Exp`. This relation gives desired results. To give a concrete example:

A is called is the *interpretation*. It works for any interpretation you want.

First we define two data constructors for simple expressions:

```
let lit (n : Int): Exp A = {
  accept = /\A. \(f : ExpAlg A). f.lit n
};

let add (e1 : Exp) (e2 : Exp): Exp A = {
  accept = /\A. \(f : ExpAlg A).
           f.add (e1.accept A f) (e2.accept A f)
};
```

Suppose later we decide to augment the expressions with subtraction:

```
let sub (e1 : SubExp) (e2 : SubExp): SubExp A =
  { accept = /\A. \(f : SubExpAlg A).
              f.sub (e1.accept A f) (e2.accept A f)
                   };
```

One big benefit of using the visitor pattern is that programmers is able to write in the same way that would do in Haskell. For example, `e2 = sub (lit 2)(lit 3)` defines an expression.

Another important property that does not exist in Scala is that programmer is able to pass `lit 2`, which is of type `Exp A` , to `sub`, which expects a `SubExp A` because of the subtyping relation we have. After all, it is known statically that `lit 2` can be passed into `sub` and nothing will go wrong.bruno: Subtyping needs to be much more emphasized! See Modular Visitor Components!

3.4 Mixins

bruno: Still not convinced by this section. Change to the record-based example. Mixins are useful programming technique wildly adopted in dynamic programming languages such as JavaScript and Ruby. But obviously it is the programmers' responsbility to make sure that the mixin does not try to access methods or fields that are not present in the base class.

In Haskell, one is also able to write programs in mixin style using records. However, this approach has a serious drawback: since there is no subtyping in Haskell, it is not possible to refine the mixin by adding more fields to the records. This means that the type of the family of the mixins has to be determined upfront, which undermines extensibility.

$F_{\&}$ is able to overcome both of the problems: it allows composing mixins that (1) extends the base behavior, (2)

[4] It is still possible to encode contravariant parameter types in Scala but doing so would require some technique.bruno: what technique?

$$
\begin{array}{lrcl}
\text{Types} & \tau & ::= & \alpha \mid \tau \to \tau \mid \forall\alpha.\,\tau \mid \tau \,\&\, \tau \mid \{l{:}\tau\} \\
\text{Expressions} & e & ::= & x \mid \lambda\alpha.\,e \mid e\ \tau \mid \lambda(x{:}\tau).\,e \mid e\ e \\
 & & \mid & e\ ,,e \mid \{\,l = e\,\} \mid e.l \\
 & & \mid & e \text{ with } \{l = e\} \\
\text{Contexts} & \gamma & ::= & \epsilon \mid \gamma, \alpha \mid \gamma, x{:}\tau \\
\text{Labels} & l & &
\end{array}
$$

Figure 1. Syntax of $F_{\&}$.

while ensuring type safety.

The figure defines a mini mixin library. The apostrophe in front of types denotes call-by-name arguments similar to the => notation in the Scala language.

```
type Mixin S = 'S -> 'S -> S;
let zero S (super : 'S) (this : 'S) : S = super;
let rec mixin S (f : Mixin S) : S
  = let m = mixin S in f (\ (_ : Unit). m f) (\ (_
      : Unit). m f);
let extends S (f : Mixin S) (g : Mixin S) : Mixin
    S
  = \ (super : 'S). \ (this : 'S). f (\ (d : Unit).
      g super this) this;
```

We define a factorial function in mixin style and make a `noisy` mixin that prints "Hello" and delegates to its superclass. Then the two functions are composed using the `mixin` and `extends` combinators. The result is the `noisyFact` function that prints "Hello" every time it is called and computes factorial.

```
let fact (super : 'Int -> Int) (this : 'Int -> Int
    ) : Int -> Int
  = \ (n : Int). if n == 0 then 1 else n * this (n
      - 1)
let noisy (super : 'Int -> Int) (this : 'Int ->
    Int) : Int -> Int
  = \ (n : Int). { println("Hello"); super n }
let noisyFact = mixin (Int -> Int) (extends (Int
    -> Int) foolish fact)
noisy 5
```

4. The $F_{\&}$ calculus

Following Dunfield's [18] work on simply-typed lambda calculus with intersection and union types, we formalize the syntax, subtyping, and typing of $F_{\&}$. In the next section, we will go through the type-directed translation from $F_{\&}$ to System F.

4.1 Syntax

Figure 1 shows the syntax of $F_{\&}$. It is System F at its core. To System F, we add two features: intersection types and single-field records. We include only single records because single record types as the multi-records can be desugared into the merge of multiple single records.

Types. The constructs in the first row of types in Figure 1 are standard in System F: type variable α, function types $\tau \to \tau$, and type abstraction $\forall\alpha.\,\tau$. The last two are novel. $\tau_1 \,\&\, \tau_1$ is the intersection of type τ_1 and τ_2, and $\{l:\tau\}$ are the types for single-field records.

Expressions. The first five constructs of expressions are also standard: variables x, and two abstraction-elimination pairs: lambda expressions $\lambda(x:\tau).\,e$ abstract expression e over values of type τ and are eliminated by application $e\ e$; Big lambdas $\lambda\alpha.\,e$ abstract expression e over types and are eliminated by type application $e\ \tau$. In the source language, lambdas are written as george: TODO and big lambdas as george: TODO.

The last four constructs are new: $e_1,,e_2$ is the *merge* of two expressions e_1 and e_2. It can be used as either e_1 or e_2. Particarly, if one regard e_1 and e_2 as objects, their merge will responds to every method that one or both of them have. Merge of expressions correspond to intersection types $\tau_1 \,\&\, \tau_2$. $\{l = e\}$ constructs a single-field record. $e.l$ accesses the field labelled l in e. Note that e does not need to be a record type in this case. For example, although the merge of two records

$$x = \{l_1 = e_1\},,\{l_1 = e_2\}$$

is of an intersection type, $x.l_1$ still gives e_1. On the other hand, $x.l_3$ does not type check. Functional update e with $\{l = e_1\}$ a *new* record which is exactly the same as e except the field labelled l is updated to become $e1$. bruno: Talking about type-checking before type-checking is discussed!

Context. Context Γ is also standard. It maps variables to their types and keeps bound type variables.

Discussion. A natural question the reader might ask is that why we have excluded union types from the language. The answer is we found that intersection types alone are enough support extensible designs. To focus on the key features that make this language interesting, we also omit other common constructs. For example, fixpoints can be added in standard ways.

4.2 Subtyping

george: Explain the subst syntax.bruno: Just say, in 1 sentence: the syntax means substitution, and the substitution function is standard and thus ommitted.

george: However, have we forbidden the interplay of subtyping relations explicitly declared by programmers as seen in class-based OO languages? bruno: Discuss somewhere (perhaps in related work) that although our system is structural, we could apply the idea of separating inheritance and subtyping to a nominal language. Point out related work.

bruno: Intersection types require a simple form of subtyping. The subtyping relation is reflexive and transitive. Our subtyping relation follows previous work. Need to cite! The main difference is the interaction with parametric polymorphism.

In some calculi such as System $F_{<:}$, the subtyping relation is orthogoal to other language features: those calculi are

indifferent with how the subtyping relation is defined. In $F_{\&}$, we take a syntatic approach, that is, subtyping is due to solely of intersection and function types.

Intersection types introduce natural subtyping relations among types. For example, `Int & Bool` should be a subtype of `Int`, since the former can be viewed as either `Int` or `Bool`. To summarize, the subtyping rules are standard except for three points listed below:

1. $\tau_1 \,\&\, \tau_2$ is a subtype of τ_3, if *either* τ_1 or τ_2 are subtypes of τ_3,
2. τ_1 is a subtype of $\tau_2 \,\&\, \tau_3$, if τ_1 is a subtype of both τ_2 and τ_3.
3. $\{l_1 : \tau_1\}$ is a subtype of $\{l_2 : \tau_2\}$, if l_1 and l_2 are identical and τ_1 is a subtype of τ_2.

The first point is captured by two rules (S-And1) and (S-And2), whereas the second point by (S-And3). Note that the last point means that record types are covariant in the type of the fields.

4.3 Typing

The typing judgment for $F_{\&}$ is of the form: $\Gamma \vdash e : \tau$. This judgment uses the context Γ. The rules for variables, abstraction, type abstraction, and type application are standard in System F. To cater to the subtyping relations and avoid having undeterministic rules, in (App), we additionally require the type of the argument be a subtype of the parameter. The rule for record construction is also standard. For record projection and update, we resort to the auxiliary "get" and "put" rules. The "get" judgment checks if a field l indeed exists in a type τ and fetches the type of the field if so. The "put" judgment is almost similar, except that it takes the intended update (both expression and type), and returns in addition a new type of the expression. In record updates, we allow refining the type of the field in question.

In particular we introduce a (T-Merge) rule that applies to *merge* constructs.

bruno: A lot more explanation needed here! You want to explain: 1) the rules which are different, and why they are different; 2) the new rules and the intuition for the new rules. For the new rules have text for each of them.

5. Type-directed Translation to System F

In this section we define the semantics of $F_{\&}$ by means of a type-directed translation to a variant of System F extended with tuples. This translation removes the labels of records and turns intersections into products, much like Dunfield's elaboration. But our translation also deals with parametric polymorphism and records.

5.1 Informal Discussion

To help the reader have a high-level understanding of how the translation works, in this subsection we present the translation informally. Take the $F_{\&}$ expression for example:

```
{ eval = 4, print = "4" }.eval
```

First, multi-field record literals are desugared into merges of single-field record literals. Therefore

```
{ eval = 4, print = "4" }
```

becomes

```
{ eval = 4 } ,, { print = "4" }
```

Merges of two values are translated into just a pair of them by (Merge) and single-field record literals lose their field labels by (RecCon). Hence `{ eval = 4 } ,, { print = "4"}` becomes `(4, "4")`.

bruno: Don't abuse inlining of examples in the text!

Finally, $e1$ and $e2$ are both coerced by a projection function $(x : (\mathtt{Int}, \mathtt{String})).\mathtt{proj}_1 x$. bruno: Show the source program, and the program that it gets translated to. Then explain how that translation works.

5.2 Target Language

The target language is System F extended with pairs. The syntax and typing is completely standard. The syntax of System F is as follows: while its semantics can be found in standard texts [33].

The main translation judgment is $\Gamma \vdash e : \tau \hookrightarrow E$ which states that with respect to the environment Γ, the $F_{\&}$ expression e is of a $F_{\&}$ type τ and its translation is a System F expression E.

We also define the type translation function $|\cdot|$ from $F_{\&}$ types τ to System F types T.

The first three rules of the translation is standard. For the last two, the intersection of two types are translated into a product of them, and the label of record types are erased.

The translation consists of four sets of rules, which are explained below:

5.3 Subtyping (Coercion)

george: Talk about η-expansion.

The coercion judgment $\Gamma \vdash \tau_1 <: \tau_2 \hookrightarrow C$ extends the subtyping judgment with a coercion on the right hand side of $\hookrightarrow$. A coercion C is an expression in the target language and has type $\tau_1 \to \tau_2$, as proved by Lemma 3. It is read "In the environment Γ, τ_1 is a subtype of τ_2; and if any expression e has a type τ_1 that is a subtype of the type of τ_2, the elaborated e, when applied to the corresponding coercion C, has exactly type $|\tau|_2$". For example, $\Gamma \vdash \mathtt{Int\&Bool} <: \mathtt{Bool} \hookrightarrow \mathtt{fst}$, where `fst` is the projection of a tuple on the first element. The coercion judgment is only used in the (App) case. As (SFun) supports contravariant parameter type and covariant return type, the coercion of the parameter types and that of the return types are used to create a coercion for the function type. (SAnd1), (SAnd2), and (SAnd3) deal with intersection types. The first two are complementary to each other. Take (SAnd1) for example, if we know τ_1 is a subtype of τ_3 and C is a coercion from τ_1 to τ_3, then we can conclude that $\tau_1 \,\&\, \tau_2$

$\boxed{\tau <: \tau}$

$$\frac{}{\alpha <: \alpha}\ \textbf{sub}\text{var} \qquad \frac{\tau_3 <: \tau_1 \qquad \tau_2 <: \tau_4}{\tau_1 \to \tau_2 <: \tau_3 \to \tau_4}\ \textbf{sub}\text{fun} \qquad \frac{\tau_1 <: [\alpha_1/\alpha_2]\tau_2}{\forall \alpha_1.\tau_1 <: \forall \alpha_2.\tau_2}\ \textbf{sub}\text{forall} \qquad \frac{\tau_1 <: \tau_2 \qquad \tau_1 <: \tau_3}{\tau_1 <: \tau_2 \,\&\, \tau_3}\ \textbf{sub}\text{and}$$

$$\frac{\tau_1 <: \tau_3}{\tau_1 \,\&\, \tau_2 <: \tau_3}\ \textbf{sub}\text{and}_1 \qquad \frac{\tau_2 <: \tau_3}{\tau_1 \,\&\, \tau_2 <: \tau_3}\ \textbf{sub}\text{and}_2 \qquad \frac{\tau_1 <: \tau_2}{\{l{:}\tau_1\} <: \{l{:}\tau_2\}}\ \textbf{sub}\text{rec}$$

Figure 2. Subtyping in $F_{\&}$.

$\boxed{\gamma \vdash e : \tau}$

$$\frac{(x,\tau) \in \gamma}{\gamma \vdash x : \tau}\ \textbf{E}\text{var} \qquad \frac{\gamma, x{:}\tau \vdash e : \tau_1 \qquad \gamma \vdash \tau}{\gamma \vdash \lambda(x{:}\tau).\, e : \tau \to \tau_1}\ \textbf{E}\text{lam}$$

$$\frac{\gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \gamma \vdash e_2 : \tau_3 \qquad \tau_3 <: \tau_1}{\gamma \vdash e_1\ e_2 : \tau_2}\ \textbf{E}\text{app} \qquad \frac{\gamma, \alpha \vdash e : \tau}{\gamma \vdash \lambda\alpha.\, e : \forall \alpha.\, \tau}\ \textbf{E}\text{blam} \qquad \frac{\gamma \vdash e : \forall \alpha.\, \tau_1 \qquad \gamma \vdash \tau}{\gamma \vdash e\ \tau : [\tau/\alpha]\tau_1}\ \textbf{E}\text{tapp}$$

$$\frac{\gamma \vdash e_1 : \tau_1 \qquad \gamma \vdash e_2 : \tau_2}{\gamma \vdash e_1, , e_2 : \tau_1 \,\&\, \tau_2}\ \textbf{E}\text{merge} \qquad \frac{\gamma \vdash e : \tau}{\gamma \vdash \{l = e\} : \{l{:}\tau\}}\ \textbf{E}\text{rec-con} \qquad \frac{\gamma \vdash e : \tau \qquad \tau \bullet l = \tau_1}{\gamma \vdash e.l : \tau_1}\ \textbf{E}\text{rec-proj}$$

$$\frac{\gamma \vdash e : \tau \qquad \gamma \vdash e_1 : \tau_1 \qquad \tau \blacktriangleleft \{l{:}\tau_1\} = \tau_2 \lfloor \tau_3 \rfloor \qquad \tau_1 <: \tau_3}{\gamma \vdash e \text{ with } \{l = e_1\} : \tau_2}\ \textbf{E}\text{rec-upd}$$

$\boxed{\tau_1 \bullet l = \tau_2}$

$$\frac{}{\{l{:}\tau\} \bullet l = \tau}\ \textbf{get} \qquad \frac{\tau_1 \bullet l = \tau}{\tau_1 \,\&\, \tau_2 \bullet l = \tau}\ \textbf{get}_1 \qquad \frac{\tau_2 \bullet l = \tau}{\tau_1 \,\&\, \tau_2 \bullet l = \tau}\ \textbf{get}_2$$

$\boxed{\tau \blacktriangleleft \{l{:}\tau\} = \tau_2 \lfloor \tau_3 \rfloor}$

$$\frac{}{\{l{:}\tau\} \blacktriangleleft \{l{:}\tau_1\} = \{l{:}\tau_1\} \lfloor \tau \rfloor}\ \textbf{put} \qquad \frac{\tau_1 \blacktriangleleft \{l{:}\tau\} = \tau_3 \lfloor \tau_4 \rfloor}{\tau_1 \,\&\, \tau_2 \blacktriangleleft \{l{:}\tau\} = \tau_3 \,\&\, \tau_2 \lfloor \tau_4 \rfloor}\ \textbf{put}_1$$

$$\frac{\tau_2 \blacktriangleleft \{l{:}\tau\} = \tau_3 \lfloor \tau_4 \rfloor}{\tau_1 \,\&\, \tau_2 \blacktriangleleft \{l{:}\tau\} = \tau_1 \,\&\, \tau_3 \lfloor \tau_4 \rfloor}\ \textbf{put}_2$$

Figure 3. The type system of $F_{\&}$.

Types	T	::=	$\alpha \mid T \to T \mid \forall\alpha.\, T \mid (T, T)$
Expressions	E, C	::=	$x \mid \lambda(x{:}T).\, E \mid E\ E \mid \lambda\alpha.\, E \mid E\ T$
		$\mid$	$(E, E) \mid \mathtt{proj}_k E$
Contexts	Γ	::=	$\epsilon \mid \Gamma, \alpha \mid \Gamma, x{:}T$

Figure 4. Target syntax.

$\boxed{|\tau| = T}$

$$\begin{array}{rcl} |\alpha| & = & \alpha \\ |\tau_1| \to |\tau_2| & = & |\tau_1| \to |\tau_2| \\ |\forall\alpha.\, \tau| & = & \forall\alpha.\, |\tau| \\ |\tau_1 \,\&\, \tau_2| & = & (|\tau_1|, |\tau_2|) \\ |\{l{:}\tau\}| & = & |\tau| \end{array}$$

Figure 5. Type translation.

is also a subtype of τ_3 and the new coercion is a function that takes a value x of type $\tau_1 \,\&\, \tau_2$, project x on the first item, and apply C to it. (SAnd3) uses both of two coercions and constructs a pair. bruno: Give a couple of concrete examples when explaining the rules.

5.4 Typing (Translation)

In this subsection we now present formally the translation rules that convert $F_{\&}$ expressions into System F ones. This set of rules essentially extends those in the previous section with the light-blue part for the translation.

$$\boxed{\tau <: \tau \hookrightarrow C} \qquad \frac{}{\alpha <: \alpha \hookrightarrow \lambda(x{:}|\alpha|).\, x}\ \textbf{sub}\text{var}$$

$$\frac{\tau_3 <: \tau_1 \hookrightarrow C_1 \qquad \tau_2 <: \tau_4 \hookrightarrow C_2}{\tau_1 \to \tau_2 <: \tau_3 \to \tau_4 \hookrightarrow \lambda(f{:}|\tau_1 \to \tau_2|).\, \lambda(x{:}|\tau_3|).\, C_2\ (f\ (C_1\ x))}\ \textbf{sub}\text{fun}$$

$$\frac{\tau_1 <: [\alpha_1/\alpha_2]\tau_2 \hookrightarrow C}{\forall\alpha_1.\,\tau_1 <: \forall\alpha_2.\,\tau_2 \hookrightarrow \lambda(f{:}|\forall\alpha.\,\tau_1|).\, \lambda\alpha.\, C\ (f\ \alpha)}\ \textbf{sub}\text{forall} \qquad \frac{\tau_1 <: \tau_2 \hookrightarrow C_1 \qquad \tau_1 <: \tau_3 \hookrightarrow C_2}{\tau_1 <: \tau_2 \,\&\, \tau_3 \hookrightarrow \lambda(x{:}|\tau_1|).\, (C_1\ x, C_2\ x)}\ \textbf{sub}\text{and}$$

$$\frac{\tau_1 <: \tau_3 \hookrightarrow C}{\tau_1 \,\&\, \tau_2 <: \tau_3 \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_1 x)}\ \textbf{sub}\text{and}_1 \qquad \frac{\tau_2 <: \tau_3 \hookrightarrow C}{\tau_1 \,\&\, \tau_2 <: \tau_3 \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_2 x)}\ \textbf{sub}\text{and}_2$$

$$\frac{\tau_1 <: \tau_2 \hookrightarrow C}{\{l{:}\tau_1\} <: \{l{:}\tau_2\} \hookrightarrow \lambda(x{:}|\{l{:}\tau_1\}|).\, C\ x}\ \textbf{sub}\text{rec}$$

Figure 6. Coersive subtyping.

$$\boxed{\gamma \vdash e : \tau \hookrightarrow E} \qquad \frac{(x,\tau) \in \gamma}{\gamma \vdash x : \tau \hookrightarrow x}\ \textbf{E}\text{var} \qquad \frac{\gamma, x{:}\tau \vdash e : \tau_1 \hookrightarrow E \qquad \gamma \vdash \tau}{\gamma \vdash \lambda(x{:}\tau).\, e : \tau \to \tau_1 \hookrightarrow \lambda(x{:}|\tau|).\, E}\ \textbf{E}\text{lam}$$

$$\frac{\gamma \vdash e_1 : \tau_1 \to \tau_2 \hookrightarrow E_1 \qquad \gamma \vdash e_2 : \tau_3 \hookrightarrow E_2 \qquad \tau_3 <: \tau_1 \hookrightarrow C}{\gamma \vdash e_1\ e_2 : \tau_2 \hookrightarrow E_1\ (C\ E_2)}\ \textbf{E}\text{app} \qquad \frac{\gamma, \alpha \vdash e : \tau \hookrightarrow E}{\gamma \vdash \lambda\alpha.\, e : \forall\alpha.\,\tau \hookrightarrow \lambda\alpha.\, E}\ \textbf{E}\text{blam}$$

$$\frac{\gamma \vdash e : \forall\alpha.\,\tau_1 \hookrightarrow E \qquad \gamma \vdash \tau}{\gamma \vdash e\ \tau : [\tau/\alpha]\tau_1 \hookrightarrow E\ |\tau|}\ \textbf{E}\text{tapp} \qquad \frac{\gamma \vdash e_1 : \tau_1 \hookrightarrow E_1 \qquad \gamma \vdash e_2 : \tau_2 \hookrightarrow E_2}{\gamma \vdash e_1,, e_2 : \tau_1 \,\&\, \tau_2 \hookrightarrow (E_1, E_2)}\ \textbf{E}\text{merge}$$

$$\frac{\gamma \vdash e : \tau \hookrightarrow E}{\gamma \vdash \{l = e\} : \{l{:}\tau\} \hookrightarrow E}\ \textbf{E}\text{rec-con} \qquad \frac{\gamma \vdash e : \tau \hookrightarrow E \qquad \tau \bullet l = \tau_1 \hookrightarrow C}{\gamma \vdash e.l : \tau_1 \hookrightarrow C\ E}\ \textbf{E}\text{rec-proj}$$

$$\frac{\gamma \vdash e : \tau \hookrightarrow E \qquad \gamma \vdash e_1 : \tau_1 \hookrightarrow E_1 \qquad \tau \blacktriangleleft \{l{:}\tau_1 \hookrightarrow E_1\} = \tau_2\lfloor\tau_3\rfloor \hookrightarrow C \qquad \tau_1 <: \tau_3}{\gamma \vdash e \text{ with } \{l = e_1\} : \tau_2 \hookrightarrow C\ E}\ \textbf{E}\text{rec-upd}$$

$$\boxed{\tau_1 \bullet l = \tau_2 \hookrightarrow C} \qquad \frac{}{\{l{:}\tau\} \bullet l = \tau \hookrightarrow \lambda(x{:}|\{l{:}\tau\}|).\, x}\ \textbf{get} \qquad \frac{\tau_1 \bullet l = \tau \hookrightarrow C}{\tau_1 \,\&\, \tau_2 \bullet l = \tau \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_1 x)}\ \textbf{get}_1$$

$$\frac{\tau_2 \bullet l = \tau \hookrightarrow C}{\tau_1 \,\&\, \tau_2 \bullet l = \tau \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_2 x)}\ \textbf{get}_2$$

$$\boxed{\tau \blacktriangleleft \{l{:}\tau \hookrightarrow E\} = \tau_2\lfloor\tau_3\rfloor \hookrightarrow C} \qquad \frac{}{\{l{:}\tau\} \blacktriangleleft \{l{:}\tau_1 \hookrightarrow E\} = \{l{:}\tau_1\}\lfloor\tau\rfloor \hookrightarrow \lambda(\_{:}|\{l{:}\tau\}|).\, E}\ \textbf{put}$$

$$\frac{\tau_1 \blacktriangleleft \{l{:}\tau \hookrightarrow E\} = \tau_3\lfloor\tau_4\rfloor \hookrightarrow C}{\tau_1 \,\&\, \tau_2 \blacktriangleleft \{l{:}\tau \hookrightarrow E\} = \tau_3 \,\&\, \tau_2\lfloor\tau_4\rfloor \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_1 x)}\ \textbf{put}_1$$

$$\frac{\tau_2 \blacktriangleleft \{l{:}\tau \hookrightarrow E\} = \tau_3\lfloor\tau_4\rfloor \hookrightarrow C}{\tau_1 \,\&\, \tau_2 \blacktriangleleft \{l{:}\tau \hookrightarrow E\} = \tau_1 \,\&\, \tau_3\lfloor\tau_4\rfloor \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\, C\ (\mathtt{proj}_2 x)}\ \textbf{put}_2$$

Figure 7. Elaboration typing from $F_{\&}$ to System F.

Translation The elaboration judgment $\Gamma \vdash e : \tau \hookrightarrow E$ extends the typing judgment with an elaborated expression on the right hand side of $\hookrightarrow$. The translation ensures that E has type $|\tau|$. It is also standard, except for the case of (App), in which a coercion from the inferred type of the argument, e_2 , to the expected type of the parameter, τ_1, is inserted before the argument; (Merge) translates merges into pairs. (RecCon) uses the same System F expression E for e as for $\{l = e\}$. And in (RecEim) and (RecUpd) the coercions generated by the "get" and "put" rules will be used to coece the main $F_{\&}$ expression.

(RecProj) typechecks e and use the "get" rule to return the type of the field τ_1 and the coecion C. The type of the whole expression is τ_1 and its translation of $C\ E$.

(RecUpd) is similar to (RecProj) in that it uses the auxiliary "put" rule. This rule typechecks e and e_1, and uses the "put" rule. Note that it allows refining of types by an e_1 that is of a subtype of τ_1', which is the type of the field l in e. The type of the updated expression then takes the type τ' returned by the "put" rule, while its translation is E, applied to the coercion generated by the "put" rule, C.

The two set of rules are explained below.

"get" Rules The "get" judgment deals spefically with record elimination and yields a coercion can be thought as a field accessor. For example:bruno: Still not showing the derivations!

$\Gamma \vdash_{\text{get}} (\{\texttt{eval} : \texttt{Int}\}, \texttt{eval}) : \{\texttt{eval} : \texttt{Int}\} \hookrightarrow \lambda(x:).\, \texttt{Int}x$

The lambda is the field accessor and when applied to a translated expression of type $\{\texttt{eval} : \texttt{Int}\}$, it is able to give the desired field. (GetBase) is the base case: the type of the field labelled l in a $\{l : \tau\}$ is just τ and the coercion is an identity function specialized to type $|\{l : \tau\}|$ (GetLeft) and (GetRight) are complementary to each other.

Consider the source program:

```
({ name = "Isaac", age = 10 }).name
```

Multi-field records are desugared into merge of single-field records:

```
({ name = "Isaac"} ,, { age = 10 }).name
```

By (GetBase),

$$\vdash_{\text{get}} (\{name{:}String\}; name) : String$$

we have the coercion

$$\lambda(x{:}|\{name{:}String\}|).\, x$$

which is just $\lambda(x : String).\, x$ according to type translation.

By (GetLeft),

$$\vdash_{\text{get}} (\{name{:}String\} \,\&\, \{age{:}Int\}; name) : String$$

By typing rules, the translation of the program is

$$(\text{"Isaac"}, 10)$$

. If we apply the coercion to it, we get

$$\text{"Isaac"}$$

"put" Rules bruno: Missing example (and derivation)

The "put" judgment deals spefically with record update can be thought as producing a field updater. Compared to the "get" rules, the "put" rules take an extra input e, which is the desired expression to replace the field lablled l in values of type τ. (PutBase) is the base case. This rule allows refinement of record fields in the sense that the type of e can be a subtype of the type of the field labelled by l. The resulting type is $\{l : \tau'\}$ and the generated coercion is a constant function that always returns E. (PutLeft) and (PutRight) are complementary to each other: the idea is exactly the same as (GetLeft) and (GetRight) except that the refined type τ_1' and τ_2' is used.

5.5 Meta-theory

Lemma 1 (Subtyping is reflexive.)**.** *Given a type* τ, $\tau <: \tau$.

Lemma 2 (Subtyping is transitive.)**.** *If* $\tau_1 <: \tau_2$ *and* $\tau_2 <: \tau_3$, *then* $\tau_1 <: \tau_3$.

Lemma 3. *If*

$$\Gamma \vdash \tau_1 <: \tau_2 \hookrightarrow C$$

then

$$|\Gamma| \vdash C : |\tau_1| \to |\tau_2|$$

Lemma 4 (Get rules produce the type-correct coercion.)**.** *If*

$$\Gamma \vdash_{get} \tau; l = C; \tau_1$$

then

$$|\Gamma| \vdash C : |\tau| \to |\tau_1|$$

Proof. By induction on the given derivation. □

Lemma 5 (Put rules produce the type-correct coercion.)**.** *If*

$$\Gamma \vdash_{put} \tau; l; E = C; \tau_1$$

then

$$|\Gamma| \vdash C : |\tau| \to |\tau|$$

Proof. By induction on the given derivation. □

Lemma 6 (Translation preserves well-formedness.)**.** *If*

$$\Gamma \vdash \tau$$

then

$$|\Gamma| \vdash |\tau|$$

Proof. By induction on the given derivation. □

Theorem 1 (Type preserving translation.)**.** *If*

$$\Gamma \vdash e : \tau \hookrightarrow E$$

then

$$|\Gamma| \vdash E : |\tau|$$

Proof. (Sketch) By structural induction on the expression and the corresponding inference rule. The full proof can be found in the appendix. □

Type-Directed Translation to System F. Main results: type-preservation + coherence.

6. Implementation

We implemented all the functionalities of the $F_{\&}$ as a contribution to the open source community. Besides, we built a language on top of $F_{\&}$ to facilitate programming. We adopted a three-phase design to compile source programs built into System F terms.

1. A *type checking* phase that checks the usage of $F_{\&}$ and other source features against an abstract syntax tree that follows strictly with the source syntax. We intentionally made type checking happen first, so as to make the error messages relevant for programmers, although such an approach has obviously complicated the implementation.
2. A *desugaring* phase that translates well-typed source terms into $F_{\&}$ terms. A number of source-level features such as multi-field records, recursive `let` definitions, type synonyms are rewritten at this phase. The resulting program is just $F_{\&}$ expressions with other minor features.
3. A *compilation* phase that translates well-typed $F_{\&}$ terms into System F ones.

Phase 3 is what we have formalized in this paper.

Type synonyms. We implement *type synonym* as in Scala and Haskell.

In fact, to make future adaptations easier, we implemented this feature on top of the more general System F_{ω}.

```
type T[A, B] = t; e
```

6.1 Optimization.

The reader might argue that translating merges as pairs can be inefficient in practice. That is indeed the case. For example, the ternary merge

```
1,,2,,3
```

is elaborated into a nested tuple

```
((1,2),3)
```

as the merge operator associates to the left.

Another issue is that every time a coercion is generated, an application will be incurred at run-time.

7. Related work

Intersection types with polymorphism. Intersection types date back to as early as Coppo et al. [12]. Recently, some form of intersection types have been adopted in object-oriented languages such as Scala, Ceylon, and Grace. One defining difference, among others, is that all those languages only allow intersections of concrete types (classes), whereas our language allows intersections of type variables, such as `A & B`. Without that vehicle, we would not be able to define the generic `merge` function (below) for all interpretations of a given algebra, and would incur boilerplate code:

```
let merge [A, B] (f: ExpAlg A) (g: ExpAlg B) = {
  lit (x : Int) = f.lit x ,, g.lit x,
  add (x : A & B) (y : A & B) =
    f.add x y ,, g.add x y
}
```

In Scala community, there have been attempts to provide a foundational calculus for Scala that incorporates intersection types [1, 2].

Our type system combines intersection types and polymorphism. The closest to ours is Pierce's work [30] on a prototype compiler for a language with both intersection types, union types, and parametric polymorphism. The important difference with our system is that in his language there is no explicit introduction construct like our merge operator. As shown in Section 3, this feature is pivotal in supporting modularity and extensibility because it allows dynamic composition of values. Pierce has also studied a system where both intersection types and bounded polymorphism are present in his Ph.D dissertation [31] and a 1997 report [32]. Going in the direction of higher kinds, Compagnoni and Pierce [10] add intersection types to System F^{ω} and use the new calculus, $F^{\omega}_{\wedge}$, to model multiple inheritance. In their system, types include the construct of intersection of types of the same kind K. Compared to our work, they do not have a term-level construct for intersection introduction. Davies and Pfenning [16] study the interactions between intersection types and effects in call-by-value languages. And they propose a "value restriction" for intersection types, similar to value restriction on parametric polymorphism.

Other type systems with intersection types. Dunfield [18] describes a similar approach to ours: compiling a system with intersection types into ordinary λ-calculus terms. The major difference is that his system does not include parametric polymorphism, while ours does not include unions. Besides, our rules are algorithmic.

Reynolds invented Forsythe [37] in the 1980s. Our merge operator is analogous to his p_1, p_2. Castagna, and Dunfield describe elaborating multi-fields records into merge of single-field records. As Dunfield has noted, in Forsythe merges can be only used unambiguously. [5] For instance, it is not allowed in Forsythe to merge two functions.

Refinement intersection [15, 17, 20] is the more conservative approach of adopting intersection types. It increases only the expressiveness of types but not terms. But without a term-level construct like "merge", it is not possible to encode various language features. As an alternative to syntatic subtyping described in this paper, Frisch et al. [21] study semantic subtyping.

[5] Why the restriction?

Type systems for modularity. To address the problem of extensibility, some researchers have designed new type system features such as virtual classes [19], polymorphic variants [22], while others have shown employing programming pattern such as object algebras [28] by using features within existing programming languages. Both of the two approaches have drawbacks of some kind. The first approach often involves heavyweight designs, while the second approach still sacrifices the readability for extensibility. bruno: fill me in with more details and more references!

Extensible records. Understanding records is important for understanding object-oriented languages. And we are the first to elaborate records to System F. Encoding records using intersection types appear in Reynolds [37] and Castagna et al. [8]. Although Dunfield also discusses this idea in his paper [18], he only provides an implementation but not formalization. Very similar to our treatment of elaborating records is Cardelli's work [5] on translating a calculus, named $F_{<:\rho}$, with extensible records to a simpler calculus that without records primitives (in which case is $F_{<:}$). But he does not consider encoding multi-field records as intersections; hence his translation is more heavyweight. Crary [13] uses intersection types and existential types to address the problem that arises when interpreting method dispatch as self-application. But in his paper, intersection types are not used to encode multi-field records.

Wand [41] started the work on extensible records and proposes row types [42] for records. Cardelli and Mitchell [6] define three primitive operations on records that are different from ours: *selection*, *restriction*, and *extension*. Following this approach, Leijen [26] define record update in terms of restriction and extension, while in our record system record update is a primitive operation. Both Leijen's system and ours allows records that contain duplicate labels. Arguably Leijen's system is stronger. For example, it supports passing record labels as arguments to functions. He also shows encoding an intersection type using first-class labels. Chlipala's `Ur` [9] explains record as type level constructs.

Indeed, our system can be adapted to simulate systems that support extensible records but not intersection of ordinary types like `Int` and `Float` by allowing only intersection of record types.

$\vdash_{\text{rec}} \tau$ states that τ is a record type, or the intersection of record types, and so forth.

RecBase

$$\vdash_{\text{rec}} \{l{:}\tau\}$$

RecStep

$$\frac{\vdash_{\text{rec}} \tau_1 \qquad \vdash_{\text{rec}} \tau_2}{\vdash_{\text{rec}} \tau_1 \,\&\, \tau_2}$$

Merge'

$$\frac{\Gamma \vdash e_1 : \tau_1 \hookrightarrow E_1 \qquad \vdash_{\text{rec}} \tau_1 \quad \Gamma \vdash e_2 : \tau_2 \hookrightarrow E_2 \qquad \vdash_{\text{rec}} \tau_2}{\Gamma \vdash e_1 ,, e_2 : \tau_1 \,\&\, \tau_2 \hookrightarrow (E_1, E_2)}$$

Of course our approach has its limitation as duplicated labels in a record are allowed. This has been discussed in a larger issue by Dunfield [18].

8. Conclusion and Further Work

We have described a simple type system suitable for extensible designs. As future work, we would like to explore extending our structural type system with nominal subtyping to allow more familiar programming experience and investigate type inference.

References

[1] N. Amin, A. Moors, and M. Odersky. Dependent object types. In *19th International Workshop on Foundations of Object-Oriented Languages*, number EPFL-CONF-183030, 2012.

[2] N. Amin, T. Rompf, and M. Odersky. Foundations of path-dependent types. In *Proceedings of the 2014 ACM International Conference on Object Oriented Programming Systems Languages & Applications*, pages 233–249. ACM, 2014.

[3] G. Bracha, M. Odersky, D. Stoutamire, and P. Wadler. Making the future safe for the past: Adding genericity to the java programming language. In *Proceedings of the 13th ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages, and Applications*, OOPSLA '98, pages 183–200, 1998.

[4] P. Canning, W. Cook, W. Hill, W. Olthoff, and J. C. Mitchell. F-bounded polymorphism for object-oriented programming. In *Proceedings of the Fourth International Conference on Functional Programming Languages and Computer Architecture*, FPCA '89, pages 273–280, New York, NY, USA, 1989. ACM. ISBN 0-89791-328-0. . URL `http://doi.acm.org/10.1145/99370.99392`.

[5] L. Cardelli. *Extensible records in a pure calculus of subtyping*. Digital. Systems Research Center, 1992.

[6] L. Cardelli and J. C. Mitchell. Operations on records. In *Mathematical foundations of programming semantics*, pages 22–52. Springer, 1990.

[7] L. Cardelli and P. Wegner. On understanding types, data abstraction, and polymorphism. *ACM Computing Surveys (CSUR)*, 17(4):471–523, 1985.

[8] G. Castagna, G. Ghelli, and G. Longo. A calculus for overloaded functions with subtyping. *Information and Computation*, 117(1):115–135, 1995.

[9] A. Chlipala. Ur: statically-typed metaprogramming with type-level record computation. In *ACM Sigplan Notices*, volume 45, pages 122–133. ACM, 2010.

[10] A. B. Compagnoni and B. C. Pierce. Higher-order intersection types and multiple inheritance. *Mathematical Structures in Computer Science*, 6(5):469–501, 1996.

[11] W. R. Cook, W. Hill, and P. S. Canning. Inheritance is not subtyping. In *Proceedings of the 17th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 125–135. ACM, 1989.

[12] M. Coppo, M. Dezani-Ciancaglini, and B. Venneri. Functional characters of solvable terms. *Mathematical Logic Quarterly*,

27(2-6):45–58, 1981.

[13] K. Crary. Simple, efficient object encoding using intersection types. Technical report, Cornell University, 1998.

[14] B. C. d. S. Oliveira. Modular visitor components: A practical solution to the expression families problem. In S. Drossopoulou, editor, *23rd European Conference on Object Oriented Programming (ECOOP)*, July 2009.

[15] R. Davies. *Practical refinement-type checking*. PhD thesis, University of Western Australia, 2005.

[16] R. Davies and F. Pfenning. Intersection types and computational effects. In *ACM Sigplan Notices*, volume 35, pages 198–208. ACM, 2000.

[17] J. Dunfield. Refined typechecking with stardust. In *Proceedings of the 2007 workshop on Programming languages meets program verification*, pages 21–32. ACM, 2007.

[18] J. Dunfield. Elaborating intersection and union types. *Journal of Functional Programming*, 24(2-3):133–165, 2014.

[19] E. Ernst, K. Ostermann, and W. R. Cook. A virtual class calculus. *POPL 2006*, pages 270–282.

[20] T. Freeman and F. Pfenning. *Refinement types for ML*, volume 26. ACM, 1991.

[21] A. Frisch, G. Castagna, and V. Benzaken. Semantic subtyping: Dealing set-theoretically with function, union, intersection, and negation types. *Journal of the ACM (JACM)*, 55(4):19, 2008.

[22] J. Garrigue. Programming with polymorphic variants. In *ML Workshop*, volume 13. Baltimore, 1998.

[23] W. Harrison and H. Ossher. Subject-oriented programming: A critique of pure objects. In *Proceedings of the Eighth Annual Conference on Object-oriented Programming Systems, Languages, and Applications*, OOPSLA '93, pages 411–428, 1993.

[24] A. Igarashi and M. Viroli. Variant parametric types: A flexible subtyping scheme for generics. *ACM Trans. Program. Lang. Syst.*, 28(5):795–847, Sept. 2006.

[25] D. Knuth. Semantics of Context-Free Languages. *Mathematical Systems Theory*, 2:127–145, 1968.

[26] D. Leijen. Extensible records with scoped labels. *Trends in Functional Programming*, 5:297–312, 2005.

[27] A. Moors, F. Piessens, and M. Odersky. Generics of a higher kind. In *Proceedings of the 23rd ACM SIGPLAN Conference on Object-oriented Programming Systems Languages and Applications*, OOPSLA '08, pages 423–438, 2008.

[28] B. C. d. S. Oliveira and W. R. Cook. Extensibility for the masses. In *ECOOP 2012–Object-Oriented Programming*, pages 2–27. Springer, 2012.

[29] B. C. d. S. Oliveira, T. Van Der Storm, A. Loh, and W. R. Cook. Feature-oriented programming with object algebras. In *ECOOP 2013–Object-Oriented Programming*, pages 27–51. Springer, 2013.

[30] B. C. Pierce. Programming with intersection types, union types, and polymorphism. 1991.

[31] B. C. Pierce. *Programming with intersection types and bounded polymorphism*. PhD thesis, Carnegie Mellon University Pittsburgh, PA, 1991.

[32] B. C. Pierce. Intersection types and bounded polymorphism. *Mathematical Structures in Computer Science*, 7(02):129–193, 1997.

[33] B. C. Pierce. *Types and programming languages*. MIT press, 2002.

[34] C. Prehofer. Feature-oriented programming: A fresh look at objects. In *ECOOP '97 — Object-Oriented Programming 11th European Conference, Jyväskylä, Finland*. Springer-Verlag, 1997.

[35] T. Rendel, J. I. Brachthäuser, and K. Ostermann. From object algebras to attribute grammars. In *Proceedings of the 2014 ACM International Conference on Object Oriented Programming Systems Languages & Applications*, OOPSLA '14, pages 377–395, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2585-1. . URL `http://doi.acm.org/10.1145/2660193.2660237`.

[36] J. C. Reynolds. Towards a theory of type structure. In *Programming Symposium, Proceedings Colloque Sur La Programmation*, pages 408–423, London, UK, UK, 1974. Springer-Verlag. ISBN 3-540-06859-7. URL `http://dl.acm.org/citation.cfm?id=647323.721503`.

[37] J. C. Reynolds. *Design of the programming language Forsythe*. Springer, 1997.

[38] P. Tarr, H. Ossher, W. Harrison, and S. M. Sutton, Jr. N degrees of separation: Multi-dimensional separation of concerns. In *Proceedings of the 21st International Conference on Software Engineering*, ICSE '99, pages 107–119, 1999.

[39] M. Torgersen. The Expression Problem Revisited. In M. Odersky, editor, *Proc. of the 18th European Conference on Object-Oriented Programming*, volume 3086 of *Lecture Notes in Computer Science*, pages 123–143, Oslo (Norway), June 2004.

[40] M. Torgersen, C. P. Hansen, E. Ernst, P. von der Ahé, G. Bracha, and N. Gafter. Adding wildcards to the java programming language. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, SAC '04, pages 1289–1296, 2004.

[41] M. Wand. Complete type inference for simple objects. In *LICS*, volume 87, pages 37–44, 1987.

[42] M. Wand. Type inference for record concatenation and multiple inheritance. In *Logic in Computer Science, 1989. LICS'89, Proceedings., Fourth Annual Symposium on*, pages 92–97. IEEE, 1989.

[43] M. Zenger and M. Odersky. Independently extensible solutions to the expression problem. In *FOOL*, Jan. 2005.

Acknowledgments

Acknowledgments, if needed.

A. Type Well-formedness

george: Or just use FTV.

$\boxed{\gamma \vdash \tau}$

$$\frac{\alpha \in \gamma}{\gamma \vdash \alpha} \qquad \frac{\gamma \vdash \tau_1 \qquad \gamma \vdash \tau_2}{\gamma \vdash \tau_1 \to \tau_2} \qquad \frac{\gamma, \alpha \vdash \tau}{\gamma \vdash \forall \alpha.\, \tau} \qquad \frac{\gamma \vdash \tau_1 \qquad \gamma \vdash \tau_2}{\gamma \vdash \tau_1 \,\&\, \tau_2} \qquad \frac{\gamma \vdash \tau}{\gamma \vdash \{l{:}\tau\}}$$

Figure 8. Type well-formedness in $F_{\&}$.

$\boxed{\Gamma \vdash T}$

$$\frac{\alpha \in T}{T \vdash \alpha} \qquad \frac{\Gamma \vdash T_1 \qquad \Gamma \vdash T_2}{\Gamma \vdash T_1 \to T_2} \qquad \frac{\Gamma, \alpha \vdash T}{\Gamma \vdash \forall \alpha.\, T} \qquad \frac{\Gamma \vdash T_1 \qquad \Gamma \vdash T_2}{\Gamma \vdash (T_1, T_2)}$$

Figure 9. Type well-formedness in the target type system.

B. Target Type System

george: TODO

C. Proofs

Notation. We present our proofs in two-column style: on the left are the intermediate results and on the right are the justification (for the previous intermediate result to reach the corresponding left-hand side).

C.1 Elaboration

Lemma 7 (**sub** rules produce type-correct coercion)**.** *If* $\tau_1 <: \tau_2 \hookrightarrow C$*, then* $\epsilon \vdash C : |\tau_1| \to |\tau_2|$.

Proof. By structural induction of the derivation.

- **Case**

$$\frac{}{\alpha <: \alpha \hookrightarrow \lambda(x{:}|\alpha|).\, x}\ \textbf{sub}\text{var}$$

$\epsilon \vdash \lambda(x{:}|\alpha|).\, x : \alpha \to \alpha$ By **T**var and **T**lam

- **Case**

$$\frac{\tau_3 <: \tau_1 \hookrightarrow C_1 \qquad \tau_2 <: \tau_4 \hookrightarrow C_2}{\tau_1 \to \tau_2 <: \tau_3 \to \tau_4 \hookrightarrow \lambda(f{:}|\tau_1 \to \tau_2|).\, \lambda(x{:}|\tau_3|).\, C_2\ (f\ (C_1\ x))}\ \textbf{sub}\text{fun}$$

$\tau_3 <: \tau_1 \hookrightarrow C_1$	Premise
$\epsilon \vdash C_1 : \|\tau_3\| \to \|\tau_1\|$	By i.h.
$\epsilon \vdash C_2 : \|\tau_2\| \to \|\tau_4\|$	Similar to the above

george: TODO

- **Case**

$$\frac{\tau_1 <: [\alpha_1/\alpha_2]\tau_2 \hookrightarrow C}{\forall \alpha_1.\, \tau_1 <: \forall \alpha_2.\, \tau_2 \hookrightarrow \lambda(f{:}|\forall \alpha.\, \tau_1|).\, \lambda \alpha.\, C\ (f\ \alpha)}\ \textbf{sub}\text{forall}$$

george: TODO

- **Case**

$$\frac{\tau_1 <: \tau_2 \hookrightarrow C_1 \qquad \tau_1 <: \tau_3 \hookrightarrow C_2}{\tau_1 <: \tau_2 \,\&\, \tau_3 \hookrightarrow \lambda(x{:}|\tau_1|).\,(C_1\ x, C_2\ x)}\ \textbf{sub}\text{and}$$

george: TODO

- **Case**

$$\frac{\tau_1 <: \tau_3 \hookrightarrow C}{\tau_1 \,\&\, \tau_2 <: \tau_3 \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\,C\ (\mathtt{proj}_1\, x)}\ \textbf{sub}\text{and}_1$$

george: TODO

- **Case**

$$\frac{\tau_2 <: \tau_3 \hookrightarrow C}{\tau_1 \,\&\, \tau_2 <: \tau_3 \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\,C\ (\mathtt{proj}_2 x)}\ \textbf{sub}\text{and}_2$$

By symmetry with the above case.

- **Case**

$$\frac{\tau_1 <: \tau_2 \hookrightarrow C}{\{l{:}\tau_1\} <: \{l{:}\tau_2\} \hookrightarrow \lambda(x{:}|\{l{:}\tau_1\}|).\,C\ x}\ \textbf{sub}\text{rec}$$

	$\tau_1 <: \tau_2 \hookrightarrow C$	Premise
(a)	$\epsilon \vdash C : \|\tau_1\| \to \|\tau_2\|$	By i.h.
	$\epsilon, x{:}\|\{l{:}\tau_1\}\| \vdash x : \|\{l{:}\tau_1\}\|$	By Tvar
	$\epsilon, x{:}\|\{l{:}\tau_1\}\| \vdash x : \|\tau_1\|$	By the definition of $\|\cdot\|$
	$\epsilon, x{:}\|\{l{:}\tau_1\}\| \vdash C\ x : \|\tau_2\|$	By Tapp and (a)
	$\epsilon, x{:}\|\{l{:}\tau_1\}\| \vdash C\ x : \|\{l{:}\tau_2\}\|$	By the definition of $\|\cdot\|$
	$\epsilon \vdash \lambda(x{:}\|\{l{:}\tau_1\}\|).\,C\ x : \|\{l{:}\tau_1\}\| \to \|\{l{:}\tau_2\}\|$	By Tlam

□

Lemma 8 (get rules produce type-correct coercion)**.** *If* $\tau \bullet l = \tau_1 \hookrightarrow C$*, then* $\epsilon \vdash C : |\tau| \to |\tau_1|$.

Proof. By structural induction of the derivation.

- **Case**

$$\frac{}{\{l{:}\tau\} \bullet l = \tau \hookrightarrow \lambda(x{:}|\{l{:}\tau\}|).\,x}\ \mathtt{get}$$

$\epsilon \vdash \lambda(x{:}\|\{l{:}\tau\}\|).\,x : \|\{l{:}\tau\}\| \to \|\{l{:}\tau\}\|$	By Tlam and Tvar
$\epsilon \vdash \lambda(x{:}\|\{l{:}\tau\}\|).\,x : \|\{l{:}\tau\}\| \to \|\tau\|$	By the definition of $\|\cdot\|$

- **Case**

$$\frac{\tau_1 \bullet l = \tau \hookrightarrow C}{\tau_1 \,\&\, \tau_2 \bullet l = \tau \hookrightarrow \lambda(x{:}|\tau_1 \,\&\, \tau_2|).\,C\ (\mathtt{proj}_1 x)}\ \mathtt{get}_1$$

$\epsilon, x{:}\|\tau_1 \,\&\, \tau_2\| \vdash x : \|\tau_1 \,\&\, \tau_2\|$	By Tvar
$\epsilon, x{:}\|\tau_1 \,\&\, \tau_2\| \vdash x : (\|\tau_1\|, \|\tau_2\|)$	By the definition of $\|\cdot\|$
$\epsilon, x{:}\|\tau_1 \,\&\, \tau_2\| \vdash \mathtt{proj}_1 x : \|\tau_1\|$	By Tproj$_1$
$\epsilon \vdash C : \|\tau_1\| \to \|\tau\|$	By i.h.
$\epsilon, x{:}\|\tau_1 \,\&\, \tau_2\| \vdash C : \|\tau_1\| \to \|\tau\|$	george: What should this be called?
$\epsilon, x{:}\|\tau_1 \,\&\, \tau_2\| \vdash C\ (\mathtt{proj}_1 x) : \|\tau\|$	By Tapp
$\epsilon \vdash \lambda(x{:}\|\tau_1 \,\&\, \tau_2\|).\,C\ (\mathtt{proj}_1 x) : \|\tau_1 \,\&\, \tau_2\| \to \|\tau\|$	By Tlam

- **Case**

$$\frac{\tau_2 \bullet \mathsf{l} = \tau \hookrightarrow \mathsf{C}}{\tau_1 \mathbin{\&} \tau_2 \bullet \mathsf{l} = \tau \hookrightarrow \lambda(\mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2|).\, \mathsf{C}\ (\mathtt{proj}_2\, \mathsf{x})}\ \mathtt{get}_2$$

By symmetry with the above case.

□

Lemma 9 (**put** rules produce type-correct coercion)**.** *If* $\tau \blacktriangleleft \{\mathsf{l}:\tau_1 \hookrightarrow \mathsf{E}\} = \tau_2 \lfloor \tau_3 \rfloor \hookrightarrow \mathsf{C}$ *and* $\Gamma \vdash \mathsf{E} : |\tau_1|$ *for some* Γ*, then* $\Gamma \vdash \mathsf{C} : |\tau| \to |\tau_2|$.

Proof. By structural induction of the derivation.

- **Case**

$$\frac{}{\{\mathsf{l}{:}\tau\} \blacktriangleleft \{\mathsf{l}{:}\tau_1 \hookrightarrow \mathsf{E}\} = \{\mathsf{l}{:}\tau_1\} \lfloor \tau \rfloor \hookrightarrow \lambda(\_{:}|\{\mathsf{l}{:}\tau\}|).\, \mathsf{E}}\ \mathtt{put}$$

$\Gamma \vdash \lambda(\_{:}|\{\mathsf{l}{:}\tau\}|).\, \mathsf{E} : |\{\mathsf{l}{:}\tau\}| \to |\tau_1|$ By Tlam, Tvar, and the hypothesis

- **Case**

$$\frac{\tau_1 \blacktriangleleft \{\mathsf{l}{:}\tau \hookrightarrow \mathsf{E}\} = \tau_3 \lfloor \tau_4 \rfloor \hookrightarrow \mathsf{C}}{\tau_1 \mathbin{\&} \tau_2 \blacktriangleleft \{\mathsf{l}{:}\tau \hookrightarrow \mathsf{E}\} = \tau_3 \mathbin{\&} \tau_2 \lfloor \tau_4 \rfloor \hookrightarrow \lambda(\mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2|).\, \mathsf{C}\ (\mathtt{proj}_1\, \mathsf{x})}\ \mathtt{put}_1$$

$\Gamma, \mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2| \vdash \mathsf{x} : |\tau_1 \mathbin{\&} \tau_2|$	By Tvar
$\Gamma, \mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2| \vdash \mathsf{x} : (|\tau_1|, |\tau_2|)$	By the definition of $\lvert\cdot\rvert$
$\Gamma, \mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2| \vdash \mathtt{proj}_1\, \mathsf{x} : |\tau_1|$	By $\mathtt{T}\mathtt{proj}_1$
$\Gamma \vdash \mathsf{C} : |\tau_1| \to |\tau_3|$	By i.h.
$\Gamma, \mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2| \vdash \mathsf{C} : |\tau_1| \to |\tau_3|$	george: Seems to need to assume x fresh
$\Gamma, \mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2| \vdash \mathsf{C}\ (\mathtt{proj}_1\, \mathsf{x}) : |\tau_3|$	By Tapp
$\Gamma \vdash \lambda(\mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2|).\, \mathsf{C}\ (\mathtt{proj}_1\, \mathsf{x}) : |\tau_1 \mathbin{\&} \tau_2| \to |\tau_3|$	By Tlam

- **Case**

$$\frac{\tau_2 \blacktriangleleft \{\mathsf{l}{:}\tau \hookrightarrow \mathsf{E}\} = \tau_3 \lfloor \tau_4 \rfloor \hookrightarrow \mathsf{C}}{\tau_1 \mathbin{\&} \tau_2 \blacktriangleleft \{\mathsf{l}{:}\tau \hookrightarrow \mathsf{E}\} = \tau_1 \mathbin{\&} \tau_3 \lfloor \tau_4 \rfloor \hookrightarrow \lambda(\mathsf{x}{:}|\tau_1 \mathbin{\&} \tau_2|).\, \mathsf{C}\ (\mathtt{proj}_2\, \mathsf{x})}\ \mathtt{put}_2$$

By symmetry with the above case.

□

Lemma 10 (Preservation of well-formedness under type translation)**.** *If* $\gamma \vdash \tau$*, then* $|\gamma| \vdash |\tau|$.

Proof. Standard. □

Theorem 2 (Type-preserving translation)**.** *If* $\gamma \vdash e : \tau \hookrightarrow \mathsf{E}$*, then* $|\gamma| \vdash \mathsf{E} : |\tau|$.

Proof. By structural induction of the derivation.

- **Case**

$$\frac{(\mathsf{x}, \tau) \in \gamma}{\gamma \vdash \mathsf{x} : \tau \hookrightarrow \mathsf{x}}\ \mathtt{E}\mathtt{var}$$

$(\mathsf{x}, \tau) \in \gamma$	Premise
$(\mathsf{x}, |\tau|) \in |\gamma|$	
$|\gamma| \vdash \mathsf{x} : |\tau|$	By Tvar

- **Case**

$$\frac{\gamma, x{:}\tau \vdash e : \tau_1 \hookrightarrow E \qquad \gamma \vdash \tau}{\gamma \vdash \lambda(x{:}\tau).\, e : \tau \to \tau_1 \hookrightarrow \lambda(x{:}|\tau|).\, E}\ \textsc{E}\text{lam}$$

$\gamma, x{:}\tau \vdash e : \tau_1 \hookrightarrow E$	Premise
$\lvert\gamma, x{:}\tau\rvert \vdash E : \lvert\tau_1\rvert$	By i.h.
$\lvert\gamma\rvert, x{:}\lvert\tau\rvert \vdash E : \lvert\tau_1\rvert$	
$\lvert\gamma\rvert \vdash \lambda(x{:}\lvert\tau\rvert).\, E : \lvert\tau\rvert \to \lvert\tau_1\rvert$	By Tlam
$\lvert\gamma\rvert \vdash \lambda(x{:}\lvert\tau\rvert).\, E : \lvert\tau \to \tau_1\rvert$	By the definition of $\lvert\cdot\rvert$

- **Case**

$$\frac{\gamma \vdash e_1 : \tau_1 \to \tau_2 \hookrightarrow E_1 \qquad \gamma \vdash e_2 : \tau_3 \hookrightarrow E_2 \qquad \tau_3 <: \tau_1 \hookrightarrow C}{\gamma \vdash e_1\ e_2 : \tau_2 \hookrightarrow E_1\ (C\ E_2)}\ \textsc{E}\text{app}$$

$\gamma \vdash e_1 : \tau_1 \to \tau_2 \hookrightarrow E_1$	Premise
$\lvert\gamma\rvert \vdash E_1 : \lvert\tau_1 \to \tau_2\rvert$	By i.h.
$\gamma \vdash e_2 : \tau_3 \hookrightarrow E_2$	Premise
$\lvert\gamma\rvert \vdash E_2 : \lvert\tau_3\rvert$	By i.h.
$\tau_3 <: \tau_1 \hookrightarrow C$	Premise
$\epsilon \vdash C : \lvert\tau_3\rvert \to \lvert\tau_1\rvert$	george: one lemma about coercion
$\lvert\gamma\rvert \vdash E_1\ (C\ E_2) : \lvert\tau_2\rvert$	By Tapp and the definition of $\lvert\cdot\rvert$

- **Case**

$$\frac{\gamma, \alpha \vdash e : \tau \hookrightarrow E}{\gamma \vdash \lambda\alpha.\, e : \forall\alpha.\, \tau \hookrightarrow \lambda\alpha.\, E}\ \textsc{E}\text{blam}$$

$\gamma, \alpha \vdash e : \tau \hookrightarrow E$	Premise
$\lvert\gamma, \alpha\rvert \vdash E : \lvert\tau\rvert$	By i.h.
$\lvert\gamma\rvert, \alpha \vdash E : \lvert\tau\rvert$	
$\lvert\gamma\rvert \vdash \lambda\alpha.\, E : \forall\alpha.\, \lvert\tau\rvert$	By Tblam
$\lvert\gamma\rvert \vdash \lambda\alpha.\, E : \lvert\forall\alpha.\, \tau\rvert$	By the definition of $\lvert\cdot\rvert$

- **Case**

$$\frac{\gamma \vdash e : \forall\alpha.\, \tau_1 \hookrightarrow E \qquad \gamma \vdash \tau}{\gamma \vdash e\ \tau : [\tau/\alpha]\tau_1 \hookrightarrow E\ \lvert\tau\rvert}\ \textsc{E}\text{tapp}$$

$\gamma \vdash e : \forall\alpha.\, \tau_1 \hookrightarrow E$	Premise
$\lvert\gamma\rvert \vdash E : \lvert\forall\alpha.\, \tau_1\rvert$	By i.h.
$\lvert\gamma\rvert \vdash E : \forall\alpha.\, \lvert\tau_1\rvert$	By the definition of $\lvert\cdot\rvert$
$\gamma \vdash \tau$	Premise
$\lvert\gamma\rvert \vdash \lvert\tau\rvert$	By Lemma 10
$\gamma \vdash E\ \lvert\tau\rvert : [\lvert\tau\rvert/\alpha]\lvert\tau_1\rvert$	By Ttapp
$\gamma \vdash E\ \lvert\tau\rvert : \lvert[\tau/\alpha]\tau_1\rvert$	

- **Case**

$$\frac{\gamma \vdash e_1 : \tau_1 \hookrightarrow E_1 \qquad \gamma \vdash e_2 : \tau_2 \hookrightarrow E_2}{\gamma \vdash e_1, , e_2 : \tau_1 \,\&\, \tau_2 \hookrightarrow (E_1, E_2)}\ \textsc{E}\text{merge}$$

$\gamma \vdash e_1 : \tau_1 \hookrightarrow E_1$	Premise
$\lvert\gamma\rvert \vdash E_1 : \lvert\tau_1\rvert$	By i.h.
$\lvert\gamma\rvert \vdash E_2 : \lvert\tau_2\rvert$	Similar to the above
$\lvert\gamma\rvert \vdash (E_1, E_2) : (\lvert\tau_1\rvert, \lvert\tau_2\rvert)$	By Tpair
$\lvert\gamma\rvert \vdash (E_1, E_2) : \lvert\tau_1 \,\&\, \tau_2\rvert$	By the definition of $\lvert\cdot\rvert$

- **Case**

$$\frac{\gamma \vdash e : \tau \hookrightarrow E}{\gamma \vdash \{l = e\} : \{l{:}\tau\} \hookrightarrow E}\ \textsc{Erec-con}$$

$\gamma \vdash e : \tau \hookrightarrow E$	Premise
$\lvert\gamma\rvert \vdash E : \lvert\tau\rvert$	By i.h.
$\lvert\gamma\rvert \vdash E : \lvert\{l{:}\tau\}\rvert$	By the definition of $\lvert\cdot\rvert$

- **Case**

$$\frac{\gamma \vdash e : \tau \hookrightarrow E \qquad \tau \bullet l = \tau_1 \hookrightarrow C}{\gamma \vdash e.l : \tau_1 \hookrightarrow C\ E}\ \textsc{Erec-proj}$$

$\tau \bullet l = \tau_1 \hookrightarrow C$	Premise
$\epsilon \vdash C : \lvert\tau\rvert \to \lvert\tau_1\rvert$	By Lemma 8
$\lvert\gamma\rvert \vdash C : \lvert\tau\rvert \to \lvert\tau_1\rvert$	
$\gamma \vdash e : \tau \hookrightarrow E$	Premise
$\lvert\gamma\rvert \vdash E : \lvert\tau\rvert$	By i.h.
$\lvert\gamma\rvert \vdash C\ E : \lvert\tau_1\rvert$	By Tapp

- **Case**

$$\frac{\gamma \vdash e : \tau \hookrightarrow E \qquad \gamma \vdash e_1 : \tau_1 \hookrightarrow E_1 \qquad \tau \blacktriangleleft \{l{:}\tau_1 \hookrightarrow E_1\} = \tau_2 \lfloor \tau_3 \rfloor \hookrightarrow C \qquad \tau_1 <: \tau_3}{\gamma \vdash e \text{ with } \{l = e_1\} : \tau_2 \hookrightarrow C\ E}\ \textsc{Erec-upd}$$

$\gamma \vdash e_1 : \tau_1 \hookrightarrow E_1$	Premise
$\lvert\gamma\rvert \vdash E_1 : \lvert\tau_1\rvert$	By i.h.
$\tau \blacktriangleleft \{l{:}\tau_1 \hookrightarrow E_1\} = \tau_2 \lfloor \tau_3 \rfloor \hookrightarrow C$	Premise
$\lvert\gamma\rvert \vdash C : \lvert\tau\rvert \to \lvert\tau_2\rvert$	By Lemma 9
$\gamma \vdash e : \tau \hookrightarrow E$	Premise
$\lvert\gamma\rvert \vdash E : \lvert\tau\rvert$	By i.h.
$\lvert\gamma\rvert \vdash C\ E : \lvert\tau_2\rvert$	By Tapp

□