Part I
Surface language

In an ideal world programmers would write perfect code with perfectly proven equalities. The surface language models this ideal, but difficult, system. Programmers should "think" in the surface language, and the machinery of later sections should reinforce an understanding of the surface type system, while being transparent to the programmer.

The surface language presented here is a minimal standard dependent type theory. Some programmatic features are allowed at the expense of logical soundness. Specifically the language allows general recursion, since general recursion is useful for general purpose functional programming. It also supports type-in-type, since it simplifies the system for programmers and makes the metatheory easier.

In contrast with later sections definitional equality is treated in a standard intentional way.

Though similar systems have been studied over the last few decades this chapter gives a self contained presentation of important meta-theoretic results sometimes simplified and with modern notation, in addition to many examples. The surface language has been an excellent platform to conduct research into "full spectrum" dependent type theory, and hopefully this exposition will be helpful for future researchers.

1 Formal Surface Language

The pre-syntax can be seen in figure 1. Location data ℓ is marked at every position in syntax where a type error might occur. When unnecessary the location information ℓ will be left implicit.

2 Examples

The surface system is extremely expressive. Church encodings are expressible.

2.1 Church Booleans

$\mathbb{B}_c \coloneqq (A:\star) \to A \to A \to A$
$true_c \coloneqq \lambda A.\lambda then.\lambda else.then$
$false_c \coloneqq \lambda A.\lambda then.\lambda else.else$

2.2 Church $\mathbb{N}$

$\mathbb{N}_c \coloneqq (A:\star) \to (A \to A) \to A \to A$
$0_c \coloneqq \lambda A.\lambda s.\lambda z.z$
$1_c \coloneqq \lambda A.\lambda s.\lambda z.s\,z$

source labels,			
ℓ			
variable contexts,			
Γ	$::=$	$\Diamond \mid \Gamma, x : M$	
expressions,			
m, n, h, M, N, H	$::=$	x	variable
	$\mid$	$m ::_{\ell} M$	annotation
	$\mid$	$\star$	type universe
	$\mid$	$(x : M_{\ell}) \to N_{\ell'}$	function type
	$\mid$	$\mathsf{fun}\, f\, x \Rightarrow m$	function
	$\mid$	$m_{\ell}\, n$	application
values,			
v	$::=$	$x \mid \star$	
	$\mid$	$(x : M_{\ell}) \to N_{\ell'}$	
	$\mid$	$\mathsf{fun}\, f\, x \Rightarrow m$	

Figure 1: Surface Language Pre-Syntax

$2_c \coloneqq \lambda A.\lambda s.\lambda z.s\ (s\, z)$
$n_c \coloneqq \lambda A.\lambda s.\lambda z.s^n\, z$
$suc_c\, x \coloneqq \lambda A.\lambda s.\lambda z.s\, (x\, A\, s\, z)$
$x +_c y \coloneqq \lambda A.\lambda s.\lambda z.x\, A\, s\ (y\, A\, s\, z)$

2.3 Unit

$Unit_c \coloneqq (A : \star) \to A \to A$
$tt_c \coloneqq \lambda A.\lambda a.a$

2.4 Void

$\bot_c \coloneqq (x : \star) \to x$

Calculus of Constructions constructions encodings are expressible,

2.5 Negation

$\neg_c A \coloneqq A \to \bot_c$

2.6 Leibniz equality

$a_1 =_A a_2 \coloneqq (C : (A \to \star)) \to C\, a_1 \to C\, a_2$
$refl_{a:A} \coloneqq \lambda C.\lambda x.x \qquad : a =_A a$
$\neg A \coloneqq A \to \bot$

2.7 Large Elimination

"Large eliminations" are possible with type-in-type.

$\lambda b.b \star Unit \perp \quad : \mathbb{B}_c \rightarrow \star$

$\lambda n.n \star (\lambda - .Unit) \perp \quad : \mathbb{N}_c \rightarrow \star$

Note that such a function is not possible in the Calculus of Constructions (CC).

large eliminations can prove standard inequalities that can be hard or impossible to express in other minimal dependent type theories such as the calculus of constructions.

2.8 $\neg \star =_\star \perp$

$\lambda pr.pr \ (\lambda x.x) \perp \qquad : \neg \star =_\star \perp$

2.9 $\neg Unit =_\star \perp$

$\lambda pr.pr \ (\lambda x.x) \, tt \qquad : \neg Unit =_\star \perp$

2.10 $\neg true_c =_{\mathbb{B}_c} false_c$

$\lambda pr.pr \ (\lambda b.b \star Unit \perp) \ tt \qquad : \neg true_c =_{\mathbb{B}_c} false_c$

2.11 $\neg 1_c =_{\mathbb{N}_c} 0_c$

$\lambda pr.pr \ (\lambda n.n \star (\lambda - .Unit) \perp) \ tt \qquad : \neg 1_c =_{\mathbb{N}_c} 0_c$

Such a proof is impossible in CC

2.12 $(x : \mathbb{N}_c) \rightarrow 0_c +_c x =_{\mathbb{N}_c} x +_c 0_c$ (by recursion)

$\mathsf{fun}\, f\, x \Rightarrow x \ (0_c +_c x =_{\mathbb{N}_c} x +_c 0_c) \ f \ (refl_{0_c : \mathbb{N}_c}) \qquad : (x : \mathbb{N}_c) \rightarrow 0_c +_c x =_{\mathbb{N}_c} x +_c 0_c$

TODO: check and discuss

2.13 Every type is inhabited (by recursion)

$\mathsf{fun}\, f\, x \Rightarrow f\, x \qquad :\perp$

This shows that the surface language is "logically unsound", every type is inhabited. while the surface language supports proofs, not every term typed in the surface language is a proof.

Logical soundness seems not to matter in programming practice. For instance, in ML the type `f : Int−> Int` does not imply the termination of `f 2`. While unproductive non-termination is always a bug, it seems an easy bug to detect and fix when it occurs. In mainstream languages, types help to communicate the intent of termination, even though termination is not guaranteed by the type system. Therefore, logical unsoundness seems suitable for a dependently

$$\frac{x : M \in \Gamma}{\Gamma \vdash x \,:\, M} var - ty$$

$$\frac{\Gamma \vdash m \,:\, M \quad \Gamma \vdash M \,:\, \star}{\Gamma \vdash m ::_{\ell} M \,:\, M} :: -ty$$

$$\frac{}{\Gamma \vdash \star \,:\, \star} \star -ty$$

$$\frac{\Gamma \vdash M \,:\, \star \quad \Gamma, x : M \vdash N \,:\, \star}{\Gamma \vdash (x : M) \to N \,:\, \star} \Pi - ty$$

$$\frac{\Gamma \vdash m \,:\, (x : N) \to M \quad \Gamma \vdash n \,:\, N}{\Gamma \vdash m\, n \,:\, M\,[x \coloneqq n]} \Pi - app - ty$$

$$\frac{\Gamma \vdash m \,:\, M \quad \Gamma \vdash M \equiv M' : \star}{\Gamma \vdash m \,:\, M'} conv$$

$$\frac{\Gamma, f : (x : N) \to M, x : N \vdash m \,:\, M}{\Gamma \vdash \mathsf{fun}\, f\, x \Rightarrow m \,:\, (x : N) \to M} \Pi - \mathsf{fun} - ty$$

typed programming language since proofs can still be encoded and logical unsoundness can be discovered through traditional testing, or warned about in a non-blocking way. Importantly, no desirable computation is prevented in order to preserve logical soundness.

2.14 Every type is inhabited (by Type-in-type)

It is possible to encode Gerard's paradox, producing another source of logical unsoundness. Though a subtle form of recursive behavior can be built out of Gerard's paradox, direct inclusion of recursion is much easier to work with.

...

There are more examples in [Car86] where Cardelli has studied a similar system.

3 TAS Surface language

The type assignment system is type sound, "well typed programs don't get stuck". This can be shown with a progress and preservation style proof, with a suitable definition of the ≡ relation.The progress/preservation style proof requires ≡ be

- reflexive
- symmetric
- transitive

- closed under (well typed) substitution
- preserves typing
- $\star \not\equiv (x : N) \to M$ does not associate type constructors

it further helps if $\equiv$ is

- closed under normalization

A particularly simple definition of $\equiv$ is equating any terms that share a reduct via a system of parallel reductions

$$\frac{m \Rrightarrow_* n \quad m' \Rrightarrow_* n}{m \equiv m'} \equiv\text{-Def}$$

- reflexive if $\Rrightarrow_*$ is reflexive
- symmetric automatically
- transitive if $\Rrightarrow_*$ is confluent
- closed under substitution if $\Rrightarrow_*$ is closed under substitution
- preserves types, if $\Rrightarrow_*$ preserves types
- $\star \not\equiv (x : N) \to M$ does not associate type constructors since $(x : N) \to M \not\Rrightarrow_* \star$
- closed under normalization automatically

Parallel reductions are defined to make those properties easier to prove.

While this is a simple definition of equality and reduction, others choices are possible, for instance it is possible to extend the relation with contextual information, type information, or even explicit proofs of equality as in ITT. It is also common in the literature to assume the properties of $\equiv$ hold without proof.

3.1 Equality

3.1.1 $\Rrightarrow$, $\Rrightarrow_*$, $\equiv$ is reflexive

The following rule is admissible,

$$\frac{m}{m \Rrightarrow m} \Rrightarrow\text{-refl}$$

by induction
it follows that,

$$\frac{m}{m \Rrightarrow_* m} \Rrightarrow\text{-refl}$$

is admissible. And follows that

$$\frac{m}{m \equiv m} \equiv\text{-refl}$$

is admissible.

$$\frac{}{x \Rrightarrow x}$$

$$\frac{m \Rrightarrow m'}{m ::_{\ell} M \Rrightarrow m'}$$

$$\frac{m \Rrightarrow m' \quad M \Rrightarrow M'}{m ::_{\ell} M \Rrightarrow m' ::_{\ell} M'}$$

$$\frac{}{\star \Rrightarrow \star}$$

$$\frac{M \Rrightarrow M' \quad N \Rrightarrow N'}{(x : M_{\ell}) \to N_{\ell'} \Rrightarrow (x : M'_{\ell}) \to N'_{\ell'}}$$

$$\frac{m \Rrightarrow m' \quad n \Rrightarrow n'}{(\mathsf{fun}\, f\, x \Rightarrow m)_{\ell}\, n \Rrightarrow m' \left[f \coloneqq \mathsf{fun}\, f\, x \Rightarrow m', x \coloneqq n'\right]}$$

$$\frac{m \Rrightarrow m'}{\mathsf{fun}\, f\, x \Rightarrow m \;\Rrightarrow\; \mathsf{fun}\, f\, x \Rightarrow m'}$$

$$\frac{m \Rrightarrow m' \quad n \Rrightarrow n'}{m_{\ell}\, n \Rrightarrow m'_{\ell}\, n'}$$

3.1.2 $\Rrightarrow$, $\Rrightarrow_*$, $\equiv$ is closed under substitutions

The following rule is admissible where σ, τ is a substitution where for every x, $\sigma(x) \Rrightarrow \tau(x)$

$$\frac{m \Rrightarrow m' \quad \sigma \Rrightarrow \tau}{m[\sigma] \Rrightarrow m'[\tau]}\ {\Rrightarrow}\text{-sub}$$

by induction

$$\frac{m \Rrightarrow_* m' \quad \sigma \Rrightarrow \tau}{m[\sigma] \Rrightarrow_* m'[\tau]}\ {\Rrightarrow_*}\text{-sub}$$

is admissible. And follows that

$$\frac{m \equiv m' \quad \sigma \Rrightarrow \tau}{m[\sigma] \equiv m'[\tau]}\ {\equiv}\text{-sub}$$

is admissible.

3.1.3 $\Rrightarrow$, $\Rrightarrow_*$ is confluent, $\equiv$ is transitive

By defining normalization with parallel reductions we can show confluence using the methods shown in [Tak95]. First define an auxiliary function *max* takes the maximum possible par step, such that if $m \Rrightarrow m'$, $m' \Rrightarrow max(m)$ and $m \Rrightarrow max(m)$, referred to as the triangle property.

$$\frac{}{(\mathsf{fun}\, f\, x \Rightarrow m)_\ell\, v \rightsquigarrow m\,[f \coloneqq \mathsf{fun}\, f\, x \Rightarrow m, x \coloneqq v]}$$

$$\frac{m \rightsquigarrow m'}{m_\ell\, n \rightsquigarrow m'_\ell\, n}$$

$$\frac{n \rightsquigarrow n'}{v_\ell\, n \rightsquigarrow v_\ell\, n'}$$

$$\frac{m \rightsquigarrow m'}{m ::_\ell M \rightsquigarrow m' ::_\ell M}$$

$$\frac{}{v ::_\ell M \rightsquigarrow v}$$

$max($	$(\mathsf{fun}\, f\, x \Rightarrow m)_\ell\ n$	$) =$	$max\,(m)\,[f \coloneqq \mathsf{fun}\, f\, x \Rightarrow max\,(m)\,, x \coloneqq max\,(n)]$	otherwise
$max($	x	$) =$	x	
$max($	$m ::_\ell M$	$) =$	$max\,(m)$	
$max($	$\star$	$) =$	$\star$	
$max($	$(x : M_\ell) \to N_{\ell'}$	$) =$	$(x : max\,(M)_\ell) \to max\,(N)_{\ell'}$	
$max($	$\mathsf{fun}\, f\, x \Rightarrow m$	$) =$	$\mathsf{fun}\, f\, x \Rightarrow max\,(m)$	
$max($	$m_\ell\, n$	$) =$	$max\,(m)_\ell\ max\,(n)$	

$m \Rrightarrow\ max\,(m)$

by TODO

$m \Rrightarrow\ m'$, $m' \Rrightarrow\ max\,(m)$

by TODO

it follows that

$m \Rrightarrow\ m'$, $m \Rrightarrow\ m''$, implies $m' \Rrightarrow\ max\,(m)$,$m'' \Rrightarrow\ max\,(m)$, referred to as the diamond property, $\Rrightarrow$ is confluent.

it follows that

$\Rrightarrow_*$ is confluent

by TODO

it follows that

$\equiv$ is transitive

3.2 Context

3.3 Preservation

3.4 Progress

the following rules are admissible

$$\frac{m \rightsquigarrow m'}{m \Rrightarrow m'}$$

Thus it is is preservation preserving and we can use the

3.5 Type Soundness

The language has type soundness, well typed terms will never “get stuck” in the surface language.

3.6 Type checking is undecidable

Given a thunk $f : Unit$ defined in pcf, it can be encoded into the surface system as a thunk $f' : Unit$, such that if f reduces to the canonical unit then $f' \Rrightarrow^* \lambda A.\lambda a.a$

$\vdash \star : f' \star \star$ type-checks by conversion exactly when f halts

If there is a procedure to decide type checking we can decide exactly when any pcf function halts

3.7 the surface language is impractical as a programming language

typing is not unique up to conversion

$\lambda x.x$ has many types

TODO

4 Bi-directional Surface Language

The surface language uses bidirectional type checking to minimize the number of annotations required ([DK21] is a good survey of the technique). Bidirectional type-checking is a popular technique for implementing dependently typed programming languages because it not as complicated as more sophisticated unification strategies, while still minimizing the annotations needed. This style of type checking usually only needs top level functions to be annotated[1]. Bidirectional type-checking splits the typing judgment into 2 separate judgments: the “infer” judgment if the type can be inferred from a term, and a “check” judgment for when term will be checked against a type. Inferences can be turned into checked judgments with an explicit equality check.

4.1 ...

The surface language supports bidirectional type-checking over the pre-syntax with the rules in figure 2. Bidirectional type-checking is a form of lightweight type inference, and strikes a good compromise between the needed type annotations and the simplicity of the theory. This is accomplished by breaking typing judgments into 2 forms:

- Inference judgments where type information propagates out of a term, $\overset{\rightarrow}{:}$ in our notation.

[1] Even in Haskell, with full Hindley-Milner type inference, top level type annotations are encouraged.

$$\frac{x : M \in \Gamma}{\Gamma \vdash x \overset{\rightarrow}{:} M}\ \text{var-}\overrightarrow{ty}$$

$$\frac{\Gamma \vdash}{\Gamma \vdash \star \overset{\rightarrow}{:} \star}\ \star\text{-}\overrightarrow{ty}$$

$$\frac{\Gamma \vdash m \overset{\leftarrow}{:} M \quad \Gamma \vdash M \overset{\leftarrow}{:} \star}{\Gamma \vdash m ::_{\ell} M \overset{\rightarrow}{:} M}\ ::\text{-}\overrightarrow{ty}$$

$$\frac{\Gamma \vdash M \overset{\leftarrow}{:} \star \quad \Gamma, x : M \vdash N \overset{\leftarrow}{:} \star}{\Gamma \vdash (x : M) \to N \overset{\rightarrow}{:} \star}\ \Pi\text{-}\overrightarrow{ty}$$

$$\frac{\Gamma \vdash m \overset{\rightarrow}{:} (x : N) \to M \quad \Gamma \vdash n \overset{\leftarrow}{:} N}{\Gamma \vdash m\, n \overset{\rightarrow}{:} M\, [x \coloneqq n]}\ \Pi\text{-app-}\overrightarrow{ty}$$

$$\frac{\Gamma \vdash m \overset{\rightarrow}{:} M \quad \Gamma \vdash M \equiv M' : \star}{\Gamma \vdash m \overset{\leftarrow}{:} M'}\ \text{conv-}\overrightarrow{ty}$$

$$\frac{\Gamma, f : (x : N) \to M, x : N \vdash m \overset{\leftarrow}{:} M}{\Gamma \vdash \mathsf{fun}\, f\, x \Rightarrow m \overset{\leftarrow}{:} (x : N) \to M}\ \Pi\text{-}\mathsf{fun}\text{-}\overrightarrow{ty}$$

Figure 2: Surface Language Bidirectional Typing Rules

- And Checking judgments where a type is checked against a term, $\overset{\leftarrow}{:}$ in our notation.

Unfortunately, the system is logically unsound (every type is trivially inhabited with recursion), since our language attempts to be more oriented to programs than proofs. We expect this is acceptable.

It might seem restrictive that the surface language only supports dependent recursive functions. However, this is extremely expressive: church style data can be encoded, as can calculus of construction style predicates, recursion can simulate induction, and type-in-type allows large elimination (see [Car86] for examples). This is still inconvenient, so we have implemented dependent data in our prototype. We suggest ways dependent data could be added to the theory in Section 4.

4.2 If it types in the bidirectional system then it types in the TAS system

...

4.3 If it types in the TAS system annotations can be added such that an equivalent term types in the bidirectional system

...

4.4 Type-checking in the Bi-directional system is still undecidable

Type checking remains undecidable because of general recursion and type-in-type. However, since the user is not expected to type-check their program directly this should not cause any issues in practice. Even decidable type-checking in dependent type theory is computationally intractable.

4.5 Bi-directional errors are local

...

5 Implementation

Implemented in Haskell. We have mechanized the type soundness of the type assignment system (without location data) in Coq.

6 Related work

Unsound logical systems that are acceptable programming languages go back to at least Church's lambda calculus which was originally intended to be a logical foundation for mathematics. In the 1970s, Martin-Löf proposed a system with Type-in-Type that was shown logically unsound by Girard (as described in the introduction in [ML72]). In the 1980s, Cardelli explored the domain semantics of a system with general recursive dependent functions and Type-in-Type[Car86].

The first direct proof of type soundness for a language with general recursive dependent functions, Type-in-Type, and dependent data that I am aware of came form the Trellys Project [SCA$^+$12]. At the time their language had several additional features not included in my surface language. Additionally, my surface language uses a simpler notion of equality and dependent data resulting in an arguably simpler proof of type soundness. Later work in the Trellys Project[CSW14, Cas14] used modalities to separate terminating and non-terminating fragments of the language, to allow both general recursion and logically sound reasoning. In general, the base language has been deeply informed by the Trellys project[KSEI$^+$12][SCA$^+$12][CSW14, Cas14] [SW15] [Sjö15] and the Zombie language[2] it produced.

Several implementations support this combination of features without proofs of type soundness. Coquand presented an early bidirectional algorithm to type-check a similar language [Coq96]. Cayenne [Aug98] is a Haskell like language that combined dependent types with Type-in-Type, data and non-termination. Agda supports general recursion and type-in-type with compiler flags. Idris supports similar "unsafe" features.

A similar "partial correctness" criterion for dependent languages with non-termination run with Call-by-Value is presented in [JZSW10].

[2] https://github.com/sweirich/trellys

7 TODO

discuss

g : (f : nat -> bool) -> (fpr : (x :Nat -> IsEven x -> f x = Bool) -> Bool

g f _ = f 2

in the presence of non terminating proof functions

g : (n : Nat) -> (fpn : (x : IsEven n) -> Bool

g f _ = f 2

example of non-terminating functions being equal

what is the deal with bidirecitonal type checking?!?!

contact guy about presentations.

caveat about unsupported features

go through prevous stack overflow questions to remindmyself about past confusion.

References

[Aug98] Lennart Augustsson. Cayenne a language with dependent types. In *Proceedings of the Third ACM SIGPLAN International Conference on Functional Programming*, ICFP '98, pages 239–250, New York, NY, USA, 1998. Association for Computing Machinery.

[Car86] Luca Cardelli. A polymorphic [lambda]-calculus with type: Type. Technical report, DEC System Research Center, 130 Lytton Avenue, Palo Alto, CA 94301, May 1986.

[Cas14] Chris Casinghino. Combining proofs and programs. 2014.

[Coq96] Thierry Coquand. An algorithm for type-checking dependent types. *Science of Computer Programming*, 26(1):167–177, 1996.

[CSW14] Chris Casinghino, Vilhelm Sjöberg, and Stephanie Weirich. Combining proofs and programs in a dependently typed language. *ACM SIGPLAN Notices*, 49(1):33–45, 2014.

[DK21] Jana Dunfield and Neel Krishnaswami. Bidirectional typing. *ACM Comput. Surv.*, 54(5), May 2021.

[JZSW10] Limin Jia, Jianzhou Zhao, Vilhelm Sjöberg, and Stephanie Weirich. Dependent types and program equivalence. *SIGPLAN Not.*, 45(1):275–286, January 2010.

[KSEI$^+$12] Garrin Kimmell, Aaron Stump, Harley D Eades III, Peng Fu, Tim Sheard, Stephanie Weirich, Chris Casinghino, Vilhelm Sjöberg, Nathan Collins, and Ki Yung Ahn. Equational reasoning about programs with general recursion and call-by-value semantics. In *Proceedings of the sixth workshop on Programming languages meets program verification*, pages 15–26, 2012.

[ML72] Per Martin-Löf. An intuitionistic theory of types. Technical report, University of Stockholm, 1972.

[SCA$^+$12] Vilhelm Sjöberg, Chris Casinghino, Ki Yung Ahn, Nathan Collins, Harley D Eades III, Peng Fu, Garrin Kimmell, Tim Sheard, Aaron Stump, and Stephanie Weirich. Irrelevance, heterogeneous equality, and call-by-value dependent type systems. *Mathematically Structured Functional Programming*, 76:112–162, 2012.

[Sjö15] Vilhelm Sjöberg. A dependently typed language with nontermination. 2015.

[SW15] Vilhelm Sjöberg and Stephanie Weirich. Programming up to congruence. In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 369–382, 2015.

[Tak95] M. Takahashi. Parallel reductions in λ-calculus. *Information and Computation*, 118(1):120–127, 1995.