Computer-Aided Formal Reasoning

The Curry-Howard correspondence – Coq

Jérémy Ledent

Introduction

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Formula	Proof
$A \wedge B$	(p, q) where p is a proof of A and q is a proof of B

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Formula	Proof
$A \wedge B$	(p, q) where p is a proof of A and q is a proof of B
$A \vee B$	(i, p) where either $i = 0$ and p is a proof of A, or $i = 1$ and p is a proof of B

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Formula	Proof
$A \wedge B$	(p, q) where p is a proof of A and q is a proof of B
$A \vee B$	(i, p) where either $i = 0$ and p is a proof of A, or $i = 1$ and p is a proof of B
$A \Rightarrow B$	a function f which maps every proof p of A to a proof $f(p)$ of B

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Formula	Proof
$A \wedge B$	(p, q) where p is a proof of A and q is a proof of B
$A \vee B$	(i, p) where either $i = 0$ and p is a proof of A, or $i = 1$ and p is a proof of B
$A \Rightarrow B$	a function f which maps every proof p of A to a proof $f(p)$ of B
$\forall x \in S.P(x)$	a function f which maps every element $s \in S$ to a proof $f(s)$ of $P(s)$

Brouwer-Heyting-Kolmogorov Interpretation

What is a *proof* of a logial formula A?

Formula	Proof
$A \wedge B$	(p, q) where p is a proof of A and q is a proof of B
$A \vee B$	(i, p) where either $i = 0$ and p is a proof of A, or $i = 1$ and p is a proof of B
$A \Rightarrow B$	a function f which maps every proof p of A to a proof $f(p)$ of B
$\forall x \in S.P(x)$	a function f which maps every element $s \in S$ to a proof $f(s)$ of $P(s)$
$\exists x \in S.P(x)$	(s, p) where $s \in S$ and p is a proof of $P(s)$

Classical vs Intuitionistic Logic

There exist irrational numbers a and b such that a^b is rational.

Proof.

$\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.
If it is rational, we're done. Otherwise, take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$, then $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ and we're done. □

We didn't give a and b: the proof is *non-constructive*.

Classical vs Intuitionistic Logic

There exist irrational numbers a and b such that a^b is rational.

Proof.

$\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.
If it is rational, we're done. Otherwise, take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$, then $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ and we're done. □

We didn't give a and b: the proof is *non-constructive*.

In *intuitionistic* logic, the following are forbidden:

- Excluded middle: $A \vee \neg A$
- Proof by contradiction: $\neg\neg A \Rightarrow A$
- Pierce's Law: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

Classical vs Intuitionistic Logic (2)

What do we gain ? $\rightarrow$ Constructiveness

Theorem (Disjunction and witness properties)

If $\vdash_{\mathcal{I}} A \vee B$, *then either* $\vdash_{\mathcal{I}} A$ *or* $\vdash_{\mathcal{I}} B$.
If $\vdash_{\mathcal{I}} \exists x.P(x)$, *then there is* t *such that* $\vdash_{\mathcal{I}} P(t)$.

Classical vs Intuitionistic Logic (2)

What do we gain ? $\rightarrow$ Constructiveness

Theorem (Disjunction and witness properties)

If $\vdash_{\mathcal{I}} A \vee B$*, then either* $\vdash_{\mathcal{I}} A$ *or* $\vdash_{\mathcal{I}} B$*.*
If $\vdash_{\mathcal{I}} \exists x.P(x)$*, then there is* t *such that* $\vdash_{\mathcal{I}} P(t)$*.*

What do we lose ? $\rightarrow$ Nothing ! (almost)

Theorem

There is a map $(-)^{\neg}$ *from formulas to formulas, such that whenever* $\vdash_{\mathcal{C}} A$*, then* $\vdash_{\mathcal{I}} A^{\neg}$*.*
Moreover, they are classically equivalent: $\vdash_{\mathcal{C}} A \Leftrightarrow A^{\neg}$

Natural Deduction

for intuitionistic propositional logic

NJ_0 – Formulas and Sequents

Formulas (p is an atomic proposition):

$$A, B, C ::= p \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B$$

Notation: $\neg A := A \Rightarrow \bot$

NJ_0 – Formulas and Sequents

Formulas (p is an atomic proposition):

$$A, B, C ::= p \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B$$

Notation: $\neg A := A \Rightarrow \bot$

Sequents of the form $\Gamma \vdash A$, where:

- A is a formula.
- $\Gamma = A_1, \ldots, A_n$ is an unordered finite list of formulas.
- $\vdash$ stands for logical consequence.

$$\Gamma \vdash A \quad \approx \quad A_1 \wedge \cdots \wedge A_n \Rightarrow A$$

NJ_0 – Formulas and Sequents

Formulas (p is an atomic proposition):

$$A, B, C ::= p \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B$$

Notation: $\neg A := A \Rightarrow \bot$

Sequents of the form $\Gamma \vdash A$, where:

- A is a formula.
- $\Gamma = A_1, \ldots, A_n$ is an unordered finite list of formulas.
- $\vdash$ stands for logical consequence.

$$\Gamma \vdash A \quad \approx \quad A_1 \wedge \cdots \wedge A_n \Rightarrow A$$

Proof: finite tree of sequents using *deduction rules*.

NJ_0 – Deduction rules

The rules are organized in *introduction* rules and *elimination* rules:

$$\frac{}{\Gamma, A \vdash A}\,(\text{Ax})$$

$$\frac{}{\Gamma \vdash \top}\,(\top\text{-I}) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot\text{-E})$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow\text{-I}) \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow\text{-E})$$

$$\frac{\Gamma \vdash A_1 \qquad \Gamma \vdash A_2}{\Gamma \vdash A_1 \wedge A_2}\,(\wedge\text{-I}) \qquad \frac{\Gamma \vdash A_1 \wedge A_2}{\Gamma \vdash A_i}\,(\wedge_i\text{-E})$$

$$\frac{\Gamma \vdash A_i}{\Gamma \vdash A_1 \vee A_2}\,(\vee_i\text{-I}) \qquad \frac{\Gamma \vdash A_1 \vee A_2 \qquad \Gamma, A_1 \vdash B \qquad \Gamma, A_2 \vdash B}{\Gamma \vdash B}\,(\vee\text{-E})$$

Basic Properties

Weakening:

$$\text{If} \quad \Gamma \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Contraction:

$$\text{If} \quad \Gamma, A, A \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Basic Properties

Weakening:

$$\text{If} \quad \Gamma \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Contraction:

$$\text{If} \quad \Gamma, A, A \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Theorem (admitted)

The excluded middle is not provable in NJ_0*: there is a formula* A *such that* $\nvdash A \vee \neg A$*.*

Basic Properties

Weakening:

$$\text{If} \quad \Gamma \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Contraction:

$$\text{If} \quad \Gamma, A, A \vdash B \quad \text{then} \quad \Gamma, A \vdash B$$

Theorem (admitted)

The excluded middle is not provable in NJ_0*: there is a formula* A *such that* $\nvdash A \vee \neg A$.

Classical Natural Deduction (NK_0**):**
All the rules of NJ_0 + *Law of Excluded Middle*:

$$\frac{}{\Gamma \vdash A \vee \neg A}\,(\textsc{Em})$$

Simply-Typed λ-Calculus

Untyped λ-calculus

Syntax:

$$t, u ::= x \mid \lambda x.\ t \mid t\ u \qquad \text{where } x \text{ is a variable}$$

Untyped λ-calculus

Syntax:

$$t, u ::= x \mid \lambda x.\ t \mid t\ u \qquad \text{where } x \text{ is a variable}$$

λ-calculus	Haskell
$\lambda x.\ t$	`\x -> t`
$t\ u$	`t u`

Untyped λ-calculus

Syntax:

$$t, u ::= x \mid \lambda x.\ t \mid t\ u \qquad \text{where } x \text{ is a variable}$$

λ-calculus	Haskell
$\lambda x.\ t$	`\x -> t`
$t\ u$	`t u`

β-reduction:

$$(\lambda x.\ t)\ u \ \triangleright_\beta\ t[u/x]$$

Its reflexive-symmetric-transitive closure is written $\equiv_\beta$.

⚠ beware of *free* and *bound* variables:

$$\lambda x.\ z\ x = \lambda y.\ z\ y$$
$$\neq \lambda z.\ z\ z$$

Untyped λ-calculus (2)

Examples:

$$I = \lambda x.\ x \qquad K = \lambda x \lambda y.\ x \qquad S = \lambda x \lambda y \lambda z.\ x\ z\ (y\ z)$$

$$\Delta = \lambda x.\ x\ x \qquad \Omega = \Delta\ \Delta$$

Exercise: reduce the following λ-terms:

$$\Delta\ I\ I \qquad S\ K\ K \qquad \Omega \qquad K\ I\ \Omega \qquad \Delta\ (I\ I)$$

Untyped λ-calculus (2)

Examples:

$$I = \lambda x.\ x \qquad K = \lambda x \lambda y.\ x \qquad S = \lambda x \lambda y \lambda z.\ x\ z\ (y\ z)$$

$$\Delta = \lambda x.\ x\ x \qquad \Omega = \Delta\ \Delta$$

Exercise: reduce the following λ-terms:

$$\Delta\ I\ I \qquad S\ K\ K \qquad \Omega \qquad K\ I\ \Omega \qquad \Delta\ (I\ I)$$

Theorem (admitted)

The untyped λ-calculus is Turing-complete.

Simply-typed λ-calculus

Types (κ is a base type):

$$T, U ::= \kappa \mid U \to T$$

Simply-typed λ-calculus

Types (κ is a base type):

$$T, U ::= \kappa \mid U \to T$$

Context: finite map from variables to types

$$\Gamma = x_1 : T_1, \ldots, x_n : T_n \qquad \text{such that } x_i \neq x_j \text{ when } i \neq j$$

Typing judgement: $\Gamma \vdash t : T$

"The term t has type T in context Γ".

Simply-typed λ-calculus

Types (κ is a base type):

$$T, U ::= \kappa \mid U \to T$$

Context: finite map from variables to types

$$\Gamma = x_1 : T_1, \ldots, x_n : T_n \qquad \text{such that } x_i \neq x_j \text{ when } i \neq j$$

Typing judgement: $\Gamma \vdash t : T$

"The term t has type T in context Γ".

Typing rules:

$$\frac{}{\Gamma, x : T \vdash x : T}(\text{Ax})$$

$$\frac{\Gamma, x : U \vdash t : T}{\Gamma \vdash \lambda x.\ t : U \to T}(\to\text{-I}) \qquad \frac{\Gamma \vdash t : U \to T \qquad \Gamma \vdash u : U}{\Gamma \vdash t\ u : T}(\to\text{-E})$$

Examples

Typing rules:

$$\frac{}{\Gamma, x : T \vdash x : T}(\text{Ax})$$

$$\frac{\Gamma, x : U \vdash t : T}{\Gamma \vdash \lambda x.\ t : U \to T}(\to\text{-I}) \qquad \frac{\Gamma \vdash t : U \to T \qquad \Gamma \vdash u : U}{\Gamma \vdash t\ u : T}(\to\text{-E})$$

Exercise: derive the following typing judgements:

- $\vdash \lambda x.\ x : T \to T$
- $x : T, y : U, z : T \to U \to V \vdash z\ x\ y : V$

Exercise: type the following terms:

- $K = \lambda x \lambda y.\ x$
- $S = \lambda x \lambda y \lambda z.\ x\ z\ (y\ z)$

Exercise: is $\Delta = \lambda x.\ x\ x$ typable?

Extension: Product types

Types:

$$T, U ::= \ldots \mid T \times U$$

Terms:

$$t, u ::= \ldots \mid \langle t, u \rangle \mid \pi_1 \ t \mid \pi_2 \ t$$

Extension: Product types

Types:

$$T, U ::= \ldots \mid T \times U$$

Terms:

$$t, u ::= \ldots \mid \langle t, u \rangle \mid \pi_1 \ t \mid \pi_2 \ t$$

λ-calculus	Haskell
$T \times U$	`(T, U)`
$\langle t, u \rangle$	`(t, u)`
$\pi_1 \ t$	`fst t`
$\pi_2 \ t$	`snd t`

Extension: Product types

Types:

$$T, U ::= \ldots \mid T \times U$$

Terms:

$$t, u ::= \ldots \mid \langle t, u \rangle \mid \pi_1\ t \mid \pi_2\ t$$

λ-calculus	Haskell
$T \times U$	`(T, U)`
$\langle t, u \rangle$	`(t, u)`
$\pi_1\ t$	`fst t`
$\pi_2\ t$	`snd t`

Typing rules:

$$\frac{\Gamma \vdash t : T \qquad \Gamma \vdash u : U}{\Gamma \vdash \langle t, u \rangle : T \times U}(\times\text{-I}) \qquad\qquad \frac{\Gamma \vdash t : T_1 \times T_2}{\Gamma \vdash \pi_i\ t : T_i}(\times_i\text{-E})$$

Extension: Product types

Types:

$$T, U ::= \dots \mid T \times U$$

Terms:

$$t, u ::= \dots \mid \langle t, u \rangle \mid \pi_1\ t \mid \pi_2\ t$$

λ-calculus	Haskell
$T \times U$	`(T, U)`
$\langle t, u \rangle$	`(t, u)`
$\pi_1\ t$	`fst t`
$\pi_2\ t$	`snd t`

Typing rules:

$$\frac{\Gamma \vdash t : T \qquad \Gamma \vdash u : U}{\Gamma \vdash \langle t, u \rangle : T \times U}(\times\text{-I}) \qquad \frac{\Gamma \vdash t : T_1 \times T_2}{\Gamma \vdash \pi_i\ t : T_i}(\times_i\text{-E})$$

β-reduction:

$$\pi_1\ \langle t, u \rangle\ \rhd_\beta\ t \qquad \pi_2\ \langle t, u \rangle\ \rhd_\beta\ u$$

Extension: Sum types

Types:

$$T, U ::= \ldots \mid T + U$$

Terms:

$$t, u ::= \ldots \mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$$

Extension: Sum types

λ-calculus	Haskell
$T + U$	`Either T U`
$\mathsf{in}_1\ t$	`Left t`
$\mathsf{in}_2\ t$	`Right t`
case ...	`pattern matching`

Types:

$$T, U ::= \ldots \mid T + U$$

Terms:

$$t, u ::= \ldots \mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$$

Extension: Sum types

λ-calculus	Haskell
$T + U$	`Either T U`
$\mathsf{in}_1\ t$	`Left t`
$\mathsf{in}_2\ t$	`Right t`
case ...	`pattern matching`

Types:

$$T, U ::= \ldots \mid T + U$$

Terms:

$$t, u ::= \ldots \mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$$

Typing rules:

$$\frac{\Gamma \vdash t : T_i}{\Gamma \vdash \mathsf{in}_i\ t : T_1 + T_2}(+_i\text{-I})$$

$$\frac{\Gamma \vdash t : T_1 + T_2 \qquad \Gamma, x : T_1 \vdash u_1 : U \qquad \Gamma, y : T_2 \vdash u_2 : U}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u_1 \mid \mathsf{in}_2\ y \mapsto u_2\} : U}(+\text{-E})$$

Extension: Sum types

λ-calculus	Haskell
$T + U$	`Either T U`
$\mathsf{in}_1\ t$	`Left t`
$\mathsf{in}_2\ t$	`Right t`
case ...	`pattern matching`

Types:

$$T, U ::= \ldots \mid T + U$$

Terms:

$$t, u ::= \ldots \mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$$

Typing rules:

$$\frac{\Gamma \vdash t : T_i}{\Gamma \vdash \mathsf{in}_i\ t : T_1 + T_2}(+_i\text{-I})$$

$$\frac{\Gamma \vdash t : T_1 + T_2 \qquad \Gamma, x : T_1 \vdash u_1 : U \qquad \Gamma, y : T_2 \vdash u_2 : U}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u_1 \mid \mathsf{in}_2\ y \mapsto u_2\} : U}(+\text{-E})$$

β-reduction:

$$\mathsf{case}\ (\mathsf{in}_i\ t)\ \mathsf{of}\ \{\mathsf{in}_1\ x_1 \mapsto u_1 \mid \mathsf{in}_2\ x_2 \mapsto u_2\} \ \rhd_\beta\ u_i[t/x_i]$$

Extension: Unit and Void

Types:

$$T, U ::= \ldots \mid \mathsf{Unit} \mid \mathsf{Void}$$

Terms:

$$t, u ::= \ldots \mid \langle\rangle \mid \mathsf{case}\ t\ \mathsf{of}\ \{\}$$

Extension: Unit and Void

Types:

$$T, U ::= \ldots \mid \mathsf{Unit} \mid \mathsf{Void}$$

Terms:

$$t, u ::= \ldots \mid \langle\rangle \mid \mathsf{case}\ t\ \mathsf{of}\ \{\}$$

λ-calculus	Haskell
Unit	`()`
$\langle\rangle$	`()`
Void	`Void`
case t of $\{\}$	`absurd t`

Extension: Unit and Void

λ-calculus	Haskell
Unit	`()`
$\langle\rangle$	`()`
Void	`Void`
case t of $\{\}$	`absurd t`

Types:

$$T, U ::= \ldots \mid \mathsf{Unit} \mid \mathsf{Void}$$

Terms:

$$t, u ::= \ldots \mid \langle\rangle \mid \mathsf{case}\ t\ \mathsf{of}\ \{\}$$

Typing rules:

$$\frac{}{\Gamma \vdash \langle\rangle : \mathsf{Unit}}(\mathsf{Unit}\text{-}\textsc{i}) \qquad \frac{\Gamma \vdash t : \mathsf{Void}}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\} : T}(\mathsf{Void}\text{-}\textsc{e})$$

Full Type System

Terms: $t, u ::= x \mid \lambda x.\ t \mid t\ u \mid \langle t, u \rangle \mid \pi_1\ t \mid \pi_2\ t \mid \langle\rangle \mid \mathsf{case}\ t\ \mathsf{of}\ \{\}$
$\mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$

$$\frac{}{\Gamma, x : T \vdash x : T}(\mathrm{Ax}) \qquad \frac{}{\Gamma \vdash \langle\rangle : \mathsf{Unit}}(\mathsf{Unit}\text{-}\mathrm{I}) \qquad \frac{\Gamma \vdash t : \mathsf{Void}}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\} : T}(\mathsf{Void}\text{-}\mathrm{E})$$

$$\frac{\Gamma, x : U \vdash t : T}{\Gamma \vdash \lambda x.\ t : U \to T}(\to\text{-}\mathrm{I}) \qquad \frac{\Gamma \vdash t : U \to T \qquad \Gamma \vdash u : U}{\Gamma \vdash t\ u : T}(\to\text{-}\mathrm{E})$$

$$\frac{\Gamma \vdash t : T \qquad \Gamma \vdash u : U}{\Gamma \vdash \langle t, u \rangle : T \times U}(\times\text{-}\mathrm{I}) \qquad \frac{\Gamma \vdash t : T_1 \times T_2}{\Gamma \vdash \pi_i\ t : T_i}(\times_i\text{-}\mathrm{E})$$

$$\frac{\Gamma \vdash t : T_i}{\Gamma \vdash \mathsf{in}_i\ t : T_1 + T_2}(+_i\text{-}\mathrm{I})$$

$$\frac{\Gamma \vdash t : T_1 + T_2 \qquad \Gamma, x : T_1 \vdash u_1 : U \qquad \Gamma, y : T_2 \vdash u_2 : U}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u_1 \mid \mathsf{in}_2\ y \mapsto u_2\} : U}(+\text{-}\mathrm{E})$$

Properties

Inversion:

- If $\Gamma \vdash \lambda x.\ t : T$ then $T = U \to V$ and $\Gamma, x : U \vdash t : V$
- If $\Gamma \vdash \langle t_1, t_2 \rangle : T$ then $T = T_1 \times T_2$ and $\Gamma \vdash t_i : T_i$
- If $\Gamma \vdash \mathsf{in}_i\ t : T$ then $T = T_1 + T_2$ and $\Gamma \vdash t : T_i$
- $\ldots$

Properties

Inversion:

- If $\Gamma \vdash \lambda x.\ t : T$ then $T = U \to V$ and $\Gamma, x : U \vdash t : V$
- If $\Gamma \vdash \langle t_1, t_2 \rangle : T$ then $T = T_1 \times T_2$ and $\Gamma \vdash t_i : T_i$
- If $\Gamma \vdash \mathsf{in}_i\ t : T$ then $T = T_1 + T_2$ and $\Gamma \vdash t : T_i$
- $\ldots$

Substitution:

If $\Gamma, x : U \vdash t : T$ and $\Gamma \vdash u : U$ then $\Gamma \vdash t[u/x] : T$

Properties

Inversion:

- If $\Gamma \vdash \lambda x.\, t : T$ then $T = U \to V$ and $\Gamma, x : U \vdash t : V$
- If $\Gamma \vdash \langle t_1, t_2 \rangle : T$ then $T = T_1 \times T_2$ and $\Gamma \vdash t_i : T_i$
- If $\Gamma \vdash \mathsf{in}_i\ t : T$ then $T = T_1 + T_2$ and $\Gamma \vdash t : T_i$
- $\ldots$

Substitution:

If $\Gamma, x : U \vdash t : T$ and $\Gamma \vdash u : U$ then $\Gamma \vdash t[u/x] : T$

Theorem (Subject Reduction)

If $\Gamma \vdash t : T$ *and* $t \rhd_\beta u$ *then* $\Gamma \vdash u : T$.

Properties

Inversion:

- If $\Gamma \vdash \lambda x.\, t : T$ then $T = U \to V$ and $\Gamma, x : U \vdash t : V$
- If $\Gamma \vdash \langle t_1, t_2 \rangle : T$ then $T = T_1 \times T_2$ and $\Gamma \vdash t_i : T_i$
- If $\Gamma \vdash \mathsf{in}_i\ t : T$ then $T = T_1 + T_2$ and $\Gamma \vdash t : T_i$
- $\ldots$

Substitution:

If $\Gamma, x : U \vdash t : T$ and $\Gamma \vdash u : U$ then $\Gamma \vdash t[u/x] : T$

Theorem (Subject Reduction)

If $\Gamma \vdash t : T$ *and* $t \rhd_\beta u$ *then* $\Gamma \vdash u : T$.

Theorem (Strong Normalization)

If $\Gamma \vdash t : T$ *then* t *is strongly normalizing.*

Curry-Howard Correspondence

for intuitionistic propositional logic

Propositions	$\leftrightarrow$	Types
Proofs	$\leftrightarrow$	Programs

Propositions as Types

Propositions:

$$A, B ::= p \mid A \Rightarrow B \mid A \wedge B \mid A \vee B \mid \top \mid \bot$$

Types:

$$T, U ::= \kappa \mid U \to T \mid T \times U \mid T + U \mid \text{Unit} \mid \text{Void}$$

Proposition A	Type T
$A \Rightarrow B$	$T \to U$
$A \wedge B$	$T \times U$
$A \vee B$	$T + U$
$\top$	Unit
$\bot$	Void

Proofs as Programs

Terms: $t, u ::= x \mid \lambda x.\ t \mid t\ u \mid \langle t, u \rangle \mid \pi_1\ t \mid \pi_2\ t \mid \langle\rangle \mid \mathsf{case}\ t\ \mathsf{of}\ \{\}$
$\mid \mathsf{in}_1\ t \mid \mathsf{in}_2\ t \mid \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u \mid \mathsf{in}_2\ y \mapsto v\}$

$$\frac{}{\Gamma, x : T \vdash x : T}(\text{Ax}) \qquad \frac{}{\Gamma \vdash \langle\rangle : \mathsf{Unit}}(\mathsf{Unit}\text{-I}) \qquad \frac{\Gamma \vdash t : \mathsf{Void}}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\} : T}(\mathsf{Void}\text{-E})$$

$$\frac{\Gamma, x : U \vdash t : T}{\Gamma \vdash \lambda x.\ t : U \to T}(\to\text{-I}) \qquad \frac{\Gamma \vdash t : U \to T \qquad \Gamma \vdash u : U}{\Gamma \vdash t\ u : T}(\to\text{-E})$$

$$\frac{\Gamma \vdash t : T \qquad \Gamma \vdash u : U}{\Gamma \vdash \langle t, u \rangle : T \times U}(\times\text{-I}) \qquad \frac{\Gamma \vdash t : T_1 \times T_2}{\Gamma \vdash \pi_i\ t : T_i}(\times_i\text{-E})$$

$$\frac{\Gamma \vdash t : T_i}{\Gamma \vdash \mathsf{in}_i\ t : T_1 + T_2}(+_i\text{-I})$$

$$\frac{\Gamma \vdash t : T_1 + T_2 \qquad \Gamma, x : T_1 \vdash u_1 : U \qquad \Gamma, y : T_2 \vdash u_2 : U}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \{\mathsf{in}_1\ x \mapsto u_1 \mid \mathsf{in}_2\ y \mapsto u_2\} : U}(+\text{-E})$$

Proofs as Programs

Terms: $t, u \ ::= x \mid \lambda x.\ t \mid t\ u \mid \langle t, u \rangle \mid \pi_1\ t \mid \pi_2\ t \mid \langle\rangle \mid \textsf{case}\ t\ \textsf{of}\ \{\}$
$\mid \textsf{in}_1\ t \mid \textsf{in}_2\ t \mid \textsf{case}\ t\ \textsf{of}\ \{\textsf{in}_1\ x \mapsto u \mid \textsf{in}_2\ y \mapsto v\}$

$$\frac{}{\Gamma, x : A \vdash x : A}(\text{Ax}) \qquad \frac{}{\Gamma \vdash \langle\rangle : \top}(\top\text{-I}) \qquad \frac{\Gamma \vdash t : \bot}{\Gamma \vdash \textsf{case}\ t\ \textsf{of}\ \{\} : A}(\bot\text{-E})$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.\ t : A \Rightarrow B}(\Rightarrow\text{-I}) \qquad \frac{\Gamma \vdash t : A \Rightarrow B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B}(\Rightarrow\text{-E})$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \wedge B}(\wedge\text{-I}) \qquad \frac{\Gamma \vdash t : A_1 \wedge A_2}{\Gamma \vdash \pi_i\ t : A_i}(\wedge_i\text{-E})$$

$$\frac{\Gamma \vdash t : A_i}{\Gamma \vdash \textsf{in}_i\ t : A_1 \vee A_2}(\vee_i\text{-I})$$

$$\frac{\Gamma \vdash t : A_1 \vee A_2 \qquad \Gamma, x : A_1 \vdash u_1 : B \qquad \Gamma, y : A_2 \vdash u_2 : B}{\Gamma \vdash \textsf{case}\ t\ \textsf{of}\ \{\textsf{in}_1\ x \mapsto u_1 \mid \textsf{in}_2\ y \mapsto u_2\} : B}(\vee\text{-E})$$

Computation is Proof Simplification

β-**reduction:** $(\lambda x.\ t)\ u \quad \triangleright_\beta \quad t[u/x]$

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi_1}{\Gamma, x : U \vdash t : T}}{\Gamma \vdash \lambda x.\ t : U \to T} \qquad \dfrac{\vdots\ \Xi_2}{\Gamma \vdash u : U}}{\Gamma \vdash (\lambda x.\ t)\ u : T} \qquad \triangleright_\beta \qquad \dfrac{\vdots\ \Xi_1[\Xi_2/x]}{\Gamma \vdash t[u/x] : T}$$

Computation is Proof Simplification

β-reduction: $(\lambda x.\ t)\ u \quad \rhd_\beta \quad t[u/x]$

$$\dfrac{\dfrac{\dfrac{\vdots}{\Xi_1}}{\Gamma, x : U \vdash t : T}}{\Gamma \vdash \lambda x.\ t : U \to T} \quad \dfrac{\dfrac{\vdots}{\Xi_2}}{\Gamma \vdash u : U} \Big/ \; \Gamma \vdash (\lambda x.\ t)\ u : T \qquad \rhd_\beta \qquad \dfrac{\dfrac{\vdots}{\Xi_1[\Xi_2/x]}}{\Gamma \vdash t[u/x] : T}$$

corresponds in natural deduction to:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Xi_1}}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \quad \dfrac{\dfrac{\vdots}{\Xi_2}}{\Gamma \vdash A}}{\Gamma \vdash B} \qquad \rhd \qquad \dfrac{\dfrac{\vdots}{\Xi_1[\Xi_2/A]}}{\Gamma \vdash B}$$

Computation is Proof Simplification (2)

β-**reduction:** $\pi_i \; \langle t_1, t_2 \rangle \quad \triangleright_\beta \quad t_i$

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ \Xi_1\end{matrix}}{\Gamma \vdash t_1 : T_1} \qquad \dfrac{\begin{matrix}\vdots \\ \Xi_2\end{matrix}}{\Gamma \vdash t_2 : T_2}}{\dfrac{\Gamma \vdash \langle t_1, t_2 \rangle : T_1 \times T_2}{\Gamma \vdash \pi_i \; \langle t_1, t_2 \rangle : T_i}} \qquad \triangleright_\beta \qquad \dfrac{\begin{matrix}\vdots \\ \Xi_i\end{matrix}}{\Gamma \vdash t_i : T_i}$$

Computation is Proof Simplification (2)

β-**reduction:** $\pi_i\ \langle t_1, t_2 \rangle \quad \rhd_\beta \quad t_i$

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi_1}{\Gamma \vdash t_1 : T_1} \qquad \dfrac{\vdots\ \Xi_2}{\Gamma \vdash t_2 : T_2}}{\Gamma \vdash \langle t_1, t_2 \rangle : T_1 \times T_2}}{\Gamma \vdash \pi_i\ \langle t_1, t_2 \rangle : T_i} \qquad \rhd_\beta \qquad \dfrac{\vdots\ \Xi_i}{\Gamma \vdash t_i : T_i}$$

corresponds in natural deduction to:

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi_1}{\Gamma \vdash A_1} \qquad \dfrac{\vdots\ \Xi_2}{\Gamma \vdash A_2}}{\Gamma \vdash A_1 \wedge A_2}}{\Gamma \vdash A_i} \qquad \rhd \qquad \dfrac{\vdots\ \Xi_i}{\Gamma \vdash A_i}$$

Computation is Proof Simplification (3)

β**-reduction:** $\quad \mathsf{case}\ (\mathsf{in}_i\ t)\ \mathsf{of}\ \{\mathsf{in}_1\ x_1 \mapsto u_1 \mid \mathsf{in}_2\ x_2 \mapsto u_2\} \quad \rhd_\beta \quad u_i[t/x_i]$

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi}{\Gamma \vdash t : T_i}}{\Gamma \vdash \mathsf{in}_i\ t : T_1 + T_2} \qquad \dfrac{\vdots\ \Xi_j}{\Gamma, x_j : T_j \vdash u_j : U}\ (j = 1,2)}{\Gamma \vdash \mathsf{case}\ (\mathsf{in}_i\ t)\ \mathsf{of}\ \{\mathsf{in}_1\ x_1 \mapsto u_1 \mid \mathsf{in}_2\ x_2 \mapsto u_2\} : U} \quad \rhd_\beta \quad \dfrac{\vdots\ \Xi_i[\Xi/x_i]}{\Gamma \vdash u_i[t/x_i] : U}$$

Computation is Proof Simplification (3)

β-reduction: $\text{case } (\text{in}_i\ t) \text{ of } \{\text{in}_1\ x_1 \mapsto u_1 \mid \text{in}_2\ x_2 \mapsto u_2\} \quad \rhd_\beta \quad u_i[t/x_i]$

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi}{\Gamma \vdash t : T_i}}{\Gamma \vdash \text{in}_i\ t : T_1 + T_2} \qquad \dfrac{\vdots\ \Xi_j}{\Gamma, x_j : T_j \vdash u_j : U}\ (j = 1, 2)}{\Gamma \vdash \text{case } (\text{in}_i\ t) \text{ of } \{\text{in}_1\ x_1 \mapsto u_1 \mid \text{in}_2\ x_2 \mapsto u_2\} : U} \quad \rhd_\beta \quad \dfrac{\vdots\ \Xi_i[\Xi/x_i]}{\Gamma \vdash u_i[t/x_i] : U}$$

corresponds in natural deduction to:

$$\dfrac{\dfrac{\dfrac{\vdots\ \Xi}{\Gamma \vdash A_i}}{\Gamma \vdash A_1 \vee A_2} \qquad \dfrac{\vdots\ \Xi_1}{\Gamma, A_1 \vdash B} \qquad \dfrac{\vdots\ \Xi_2}{\Gamma, A_2 \vdash B}}{\Gamma \vdash B} \quad \rhd \quad \dfrac{\vdots\ \Xi_i[\Xi/A_i]}{\Gamma \vdash B}$$

Curry-Howard Correspondence for NJ_0

Theorem (Curry-Howard Correspondence)

$A_1, \ldots, A_n \vdash A$ *is derivable in* NJ_0 *iff there is a term* t *with* $\mathsf{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ *such that* $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$.

Curry-Howard Correspondence for NJ_0

Theorem (Curry-Howard Correspondence)

$A_1, \ldots, A_n \vdash A$ *is derivable in* NJ_0 *iff there is a term* t *with* $\mathsf{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ *such that* $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$.

Reminder: some properties of $\triangleright_\beta$:

- Subject reduction: if $\Gamma \vdash t : T$ and $t \triangleright_\beta u$ then $\Gamma \vdash u : T$.
- If t is typable, then it is strongly normalizing.

Curry-Howard Correspondence for NJ_0

Theorem (Curry-Howard Correspondence)

$A_1, \ldots, A_n \vdash A$ is derivable in NJ_0 iff there is a term t with $\mathsf{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ such that $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$.

Reminder: some properties of $\triangleright_\beta$:

- Subject reduction: if $\Gamma \vdash t : T$ and $t \triangleright_\beta u$ then $\Gamma \vdash u : T$.
- If t is typable, then it is strongly normalizing.

Lemma (Closed normal forms)

If t is typed, closed, and in $\triangleright_\beta$-normal form, then t is of the form:

$$\langle\rangle \quad \text{or} \quad \lambda x.\ u \quad \text{or} \quad \langle u, v\rangle \quad \text{or} \quad \mathsf{in}_i\ u$$

Curry-Howard Correspondence for NJ_0

Theorem (Curry-Howard Correspondence)

$A_1, \ldots, A_n \vdash A$ is derivable in NJ_0 iff there is a term t with $\mathsf{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ such that $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$.

Reminder: some properties of $\rhd_\beta$:

- Subject reduction: if $\Gamma \vdash t : T$ and $t \rhd_\beta u$ then $\Gamma \vdash u : T$.
- If t is typable, then it is strongly normalizing.

Lemma (Closed normal forms)

If t is typed, closed, and in $\rhd_\beta$-normal form, then t is of the form:

$$\langle\rangle \quad \text{or} \quad \lambda x.\ u \quad \text{or} \quad \langle u, v\rangle \quad \text{or} \quad \mathsf{in}_i\ u$$

Corollary: in intuitionistic propositional logic (NJ_0),

- $\vdash \bot$ is not provable.
- if $\vdash A \vee B$, then either $\vdash A$ or $\vdash B$.

Beyond NJ_0 and simple types

The correspondence can be extended in many ways:

- System F $\rightarrow$ second-order logic
- Martin-Löf Type Theory $\rightarrow$ dependent types (quantifiers)
- Calculus of Constructions
- Calculus of Inductive Constructions $\rightarrow$ Coq
- Homotopy Type Theory
- ...

Other approaches to the "Proofs as Programs" paradigm:

- Realizability
- Classical Realizability