Definition A __context__ $\Gamma = x_1 : A_1, \ldots, x_n : A_n$ is a function from some finite set of variables to types.

A __typing judgement__ is a triple $\Gamma \vdash M : A$, where Γ is a context, M is a term, and A is a type.

The set of __valid__ typing judgements is the smallest set closed under the following rules:

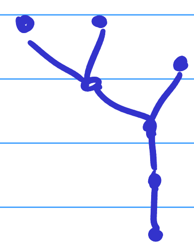
$$\frac{}{\Gamma, x : A \vdash x : A} \qquad \frac{\Gamma \vdash M : A \qquad \Gamma \vdash N : B}{\Gamma \vdash (M, N) : A \times B}$$

$$\frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \mathrm{fst}\, M : A} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \mathrm{snd}\, M : B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A . M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x:A, y:A\to A\to B \vdash y : A\to A\to B} \qquad \dfrac{}{x:A, y:A\to A\to B \vdash x : A}}{x:A, y:A\to A\to B \vdash yx : A\to B} \qquad \dfrac{}{x:A, y:A\to A\to B \vdash x : A}}{x:A,\ y:A\to A\to B \vdash (yx)x : B}}{x:A \vdash \lambda y:A\to A\to B.(yx)x : (A\to A\to B)\to B}}{\vdash \lambda x:A.(\lambda y:A\to A\to B.(yx)x) : A\to (A\to A\to B)\to B}$$



The Curry-Howard Isomorphism

or

the Propositions-as-types paradigm

What is a proof?

Propositional Logic

and ↓ implies ↓

Propositions : $A, B ::= \alpha \mid A \wedge B \mid A \Rightarrow B$

Types : $A, B ::= \alpha \mid A \times B \mid A \to B$

What is a proof of $A \wedge B$?

A proof of $A \wedge B$ is a pair of a proof of A and a proof of B.

What is a proof of $A \Rightarrow B$?

Brower-Heyting-Kolmogorov interpretation

A proof of $A \Rightarrow B$ is a function that maps proofs of A to proofs of B.

Example Prove $A \wedge B \Rightarrow B \wedge A$

$z : A$

"z is a proof of A".

$$(\lambda z : A \wedge B . (\text{snd } z, \text{fst } z)) : A \wedge B \Rightarrow B \wedge A$$

$$A \times B \to B \times A$$

$x_1 : A_1, \ldots, x_n : A_n \vdash M : B$

Means: Given proofs $x_1, \ldots, x_n$ of $A_1, \ldots, A_n$, we have a proof of B.

In other words: We have a proof of B from assumptions $A_1, \ldots, A_n$.

There are two ways of formally fitting the B-H-K interpretation into the syntax of lambda calculus:

(1) Reinterpret $M : A$ to mean "M is a proof of A"

(2) Identify a proposition A with the set of all of its proofs.

For example, $A \wedge B = \{ M \mid M \text{ is a proof of } A \wedge B \}$

$= \{ (N, P) \mid N \text{ is a proof of } A, P \text{ is a proof of } B \}$

$= \{ N \mid N \text{ is a proof } A \} \times \{ P \mid P \text{ is a proof of } B \}$

$= A \times B$

Example

A proposition with more than one proof.

Prove: $A \wedge A \Rightarrow A$

$(\lambda z : A \wedge A.\ \mathrm{fst}\ z) : A \times A \to A$

$(\lambda z : A \wedge A.\ \mathrm{snd}\ z) : A \times A \to A$

Truth table for "and"

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

N: non-empty
E: empty

A	B	$A \times B$
N	N	N
N	E	E
E	N	E
E	E	E

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

A	B	$A \to B$
N	N	N
N	E	E
E	N	N
E	E	N

Some of the other logical connectives

Boolean constants

"top" "true" $\top$ = Truth

"bottom" "false" $\bot$ = Falsity

$\top = \{*\}$ a singleton set.

$*$ is the unique proof of $\top$

$\bot = \emptyset$ "False" has no proof.

Negation

We write $\neg A$ for "not A".

We regard $\neg A$ as an abbreviation for $A \to \bot$

BHK-interpretation: A proof of $\neg A$ is a function that maps a proof of A to a contradiction. (A contradiction is a proof of $\bot$).

Disjunction

We write $A \vee B$ for "A or B".

BHK-interpretation: "A proof of $A \vee B$ is either a proof of A, or a proof of B, together with an indication of which of the two it is."

Identify $A \vee B$ with the disjoint union $A + B$.

In lambda calculus:

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \mathrm{left}\ M : A+B} \qquad \frac{\Gamma \vdash N : B}{\Gamma \vdash \mathrm{right}\ N : A+B}$$

$$\frac{\Gamma, x:A \vdash N : C \quad \Gamma, y:B \vdash P : C \quad \Gamma \vdash M : A+B}{\Gamma \vdash \mathrm{case}\ M\ \mathrm{of}\ \{\mathrm{left}\ x \to N;\ \mathrm{right}\ y \to P\} : C}$$

Example Prove $A \vee B \Rightarrow B \vee A$

Equivalently: $A + B \to B + A$

$$\lambda z : A+B.\ \mathrm{case}\ z\ \mathrm{of}\ \{\mathrm{left}\ \underset{x:A}{x} \to \underbrace{\mathrm{right}\ x}_{B+A};\ \mathrm{right}\ \underset{y:B}{y} \to \mathrm{left}\ y\}$$

If and only if

We regard $A \Leftrightarrow B$ as an abbreviation for $(A \Rightarrow B) \wedge (B \Rightarrow A)$

Quantifiers

Universal Quantifier

We write $\forall x : X .\ P(x)$

for "for all $x : X$, $P(x)$"

BHK-interpretation: "A proof of $\forall x : X . P(x)$ is a <u>function</u> that maps any element $x \in X$ to a proof of $P(x)$".

Existential Quantifier

We write $\exists x : X .\ P(x)$

for "there exists an $x : X$ such that $P(x)$".

BHK-interpretation: "A proof of $\exists x : X . P(x)$ is a pair of a <u>witness</u> $x : X$ and <u>evidence</u> $P(x)$."

<u>Prove</u>. there exists a prime greater than 100.

$$\exists x \in \mathbb{N} .\ \mathrm{prime}(x) \wedge x > 100$$

<u>BHK</u>: $(101,$ a proof of "$\mathrm{prime}(101) \wedge 101 > 100$"$)$