Curry-Howard correspondence

Logic	$\longleftrightarrow$	*Type system*
propositions, ϕ	$\longleftrightarrow$	types, τ
(constructive) proofs, p	$\longleftrightarrow$	expressions, M
"p is a proof of ϕ"	$\longleftrightarrow$	"M is an expression of type τ"
simplification of proofs	$\longleftrightarrow$	reduction of expressions

Example of a non-constructive proof

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

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational, or it is not (LEM!).

Example of a non-constructive proof

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

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational, or it is not (LEM!).

If it is, we can take $a = b = \sqrt{2}$, since $\sqrt{2}$ is irrational by a well-known theorem attributed to Euclid.

Example of a non-constructive proof

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

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational, or it is not (LEM!).

If it is, we can take $a = b = \sqrt{2}$, since $\sqrt{2}$ is irrational by a well-known theorem attributed to Euclid.

If it is not, we can take $a = \sqrt{2}$ and $b = \sqrt{2}^{\sqrt{2}}$, since then $b^a = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$.

QED

Curry-Howard correspondence

Logic	$\leftrightarrow$	*Type system*
propositions, ϕ	$\leftrightarrow$	types, τ
(constructive) proofs, p	$\leftrightarrow$	expressions, M
"p is a proof of ϕ"	$\leftrightarrow$	"M is an expression of type τ"
simplification of proofs	$\leftrightarrow$	reduction of expressions

E.g.

2IPC vs PLC

Girard Reynolds

Second-order intuitionistic propositional calculus (2IPC)

2IPC propositions: $\boxed{\phi ::= p \mid \phi \to \phi \mid \forall p\,(\phi)}$, where p ranges over an infinite set of propositional variables.

2IPC sequents: $\boxed{\Phi \vdash \phi}$, where Φ is a finite set of 2IPC propositions and ϕ is a 2IPC proposition.

$\Phi \vdash \phi$ is *provable* if it is in the set of sequents inductively generated by:

$$\text{(Id)}\quad \Phi \vdash \phi \quad \text{if } \phi \in \Phi$$

$$(\to\text{I})\ \frac{\Phi, \phi \vdash \phi'}{\Phi \vdash \phi \to \phi'} \qquad (\to\text{E})\ \frac{\Phi \vdash \phi \to \phi' \quad \Phi \vdash \phi}{\Phi \vdash \phi'}$$

$$(\forall\text{I})\ \frac{\Phi \vdash \phi}{\Phi \vdash \forall p\,(\phi)} \text{ if } p \notin fv(\Phi) \qquad (\forall\text{E})\ \frac{\Phi \vdash \forall p\,(\phi)}{\Phi \vdash \phi[\phi'/p]}$$

A 2IPC proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{p \mathbin{\&} q, p, q\} \vdash p}\;(Id)}{\{p \mathbin{\&} q, p\} \vdash q \to p}\;(\to I)}{\{p \mathbin{\&} q\} \vdash p \to q \to p}\;(\to I) \qquad \dfrac{\dfrac{}{\{p \mathbin{\&} q\} \vdash \forall\, r\,((p \to q \to r) \to r)}\;(Id)}{\{p \mathbin{\&} q\} \vdash (p \to q \to p) \to p}\;(\forall E)}{\{p \mathbin{\&} q\} \vdash p}\;(\to E)}{\{\,\} \vdash p \mathbin{\&} q \to p}\;(\to I)}{\{\,\} \vdash \forall\, q\,(p \mathbin{\&} q \to p)}\;(\forall I)}{\{\,\} \vdash \forall\, p, q\,(p \mathbin{\&} q \to p)}\;(\forall I)
$$

where $p \mathbin{\&} q$ is an abbreviation for $\forall\, r\,((p \to q \to r) \to r)$.

The PLC expression corresponding to this proof is:

$$\Lambda\, p, q\,(\lambda\, z : p \mathbin{\&} q\,(z\, p\,(\lambda\, x : p, y : q\,(x)))).$$

Curry-Howard correspondence

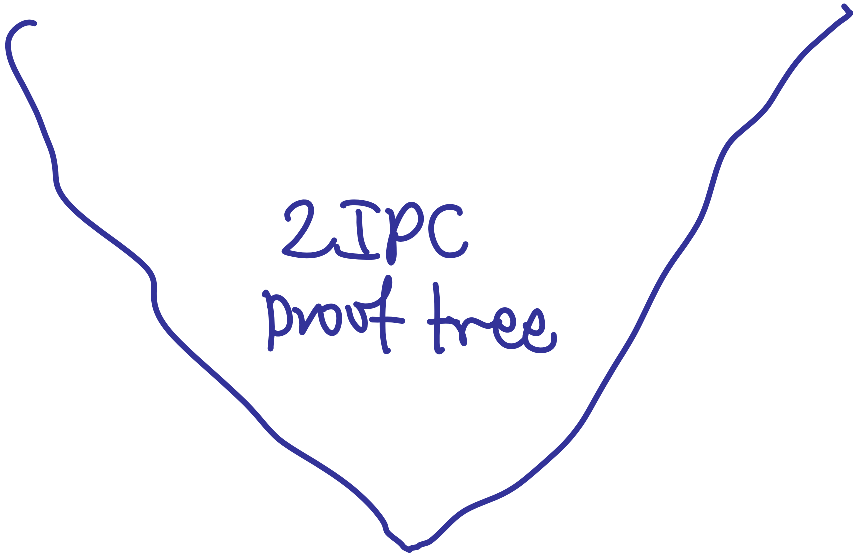
Logic 2IPC	$\leftrightarrow$	*Type system* PLC
$\varphi ::= p \mid \varphi \to \varphi \mid \forall p(\varphi)$		$\tau ::= \alpha \mid \tau \to \tau \mid \forall \alpha(\tau)$
propositions, ϕ	$\leftrightarrow$	types, τ
(constructive) proofs, p	$\leftrightarrow$	expressions, M
"p is a proof of ϕ"	$\leftrightarrow$	"M is an expression of type τ"
simplification of proofs	$\leftrightarrow$	reduction of expressions

Curry-Howard correspondence

Logic 2IPC	$\longleftrightarrow$	*Type system* PLC
$\varphi ::= p \mid \varphi \to \varphi \mid \forall p\,(\varphi)$		$\tau ::= \alpha \mid \tau \to \tau \mid \forall \alpha\,(\tau)$
propositions, ϕ	$\longleftrightarrow$	types, τ
(constructive) proofs, p	$\longleftrightarrow$	expressions, M
"p is a proof of ϕ"	$\longleftrightarrow$	"M is an expression of type τ"
simplification of proofs	$\longleftrightarrow$	reduction of expressions

proof trees for $\Phi \vdash \varphi$ $\longmapsto$ choice of labels $\bar{x} = \{x_1, \ldots, x_n\}$ for hypotheses $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ + terms M satisfying $\bar{x} : \Phi \vdash M : \varphi$

In 2IPC



$$\dfrac{\Phi, \quad \varphi \vdash \varphi'}{\Phi \vdash \varphi \to \varphi'}\ (\to I)$$

Label hypotheses with variables & recursively build up a "proof term" describing the 2IPC proof

PLC

proof tree

$$\frac{\bar{x} : \bar{\Phi},\ x : \varphi \ \vdash\ M : \varphi'}{\bar{x} : \bar{\Phi} \ \vdash \qquad\qquad \varphi \to \varphi'} \ (\to I)$$

Label hypotheses with variables & recursively build up a "proof term" describing the 2IPC proof

PLC

proof tree

$$\frac{\overline{x} : \Phi ,\ x : \varphi \ \vdash\ M : \varphi'}{\overline{x} : \Phi \ \vdash\ \lambda x : \varphi\,(M) : \varphi \to \varphi'}\ (\mathrm{fn})$$

[p 65]

$$(\mathrm{Id})\ \Phi, \phi \vdash \phi \quad \mapsto \quad (\mathrm{id})\ \overline{x} : \Phi, x : \phi \vdash x : \phi$$

$$(\to\mathrm{I})\ \frac{\Phi, \phi \vdash \phi'}{\Phi \vdash \phi \to \phi'} \quad \mapsto \quad (\mathrm{fn})\ \frac{\overline{x} : \Phi, x : \phi \vdash M : \phi'}{\overline{x} : \Phi \vdash \lambda x : \phi\,(M) : \phi \to \phi'}$$

$$(\to\mathrm{E})\ \frac{\Phi \vdash \phi \to \phi' \qquad \Phi \vdash \phi}{\Phi \vdash \phi'} \quad \mapsto \quad (\mathrm{app})\ \frac{\overline{x} : \Phi \vdash M_1 : \phi \to \phi' \qquad \overline{x} : \Phi \vdash M_2 : \phi}{\overline{x} : \Phi \vdash M_1\, M_2 : \phi'}$$

$$(\forall\mathrm{I})\ \frac{\Phi \vdash \phi}{\Phi \vdash \forall\, p\,(\phi)} \quad \mapsto \quad (\mathrm{gen})\ \frac{\overline{x} : \Phi \vdash M : \phi}{\overline{x} : \Phi \vdash \Lambda\, p\,(M) : \forall\, p\,(\phi)}$$

$$(\forall\mathrm{E})\ \frac{\Phi \vdash \forall\, p\,(\phi)}{\Phi \vdash \phi[\phi'/p]} \quad \mapsto \quad (\mathrm{spec})\ \frac{\overline{x} : \Phi \vdash M : \forall\, p\,(\phi)}{\overline{x} : \Phi \vdash M\,\phi' : \phi[\phi'/p]}$$

A 2IPC proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{p \mathbin{\&} q, p, q\} \vdash p}\,(Id)}{\{p \mathbin{\&} q, p\} \vdash q \to p}\,(\to I)}{\{p \mathbin{\&} q\} \vdash p \to q \to p}\,(\to I)
\qquad
\dfrac{\dfrac{}{\{p \mathbin{\&} q\} \vdash \forall\, r\,((p \to q \to r) \to r)}\,(Id)}{\{p \mathbin{\&} q\} \vdash (p \to q \to p) \to p}\,(\forall E)}{\{p \mathbin{\&} q\} \vdash p}\,(\to E)}{\{\,\} \vdash p \mathbin{\&} q \to p}\,(\to I)}{\{\,\} \vdash \forall\, q\,(p \mathbin{\&} q \to p)}\,(\forall I)}{\{\,\} \vdash \forall\, p, q\,(p \mathbin{\&} q \to p)}\,(\forall I)
$$

where $p \mathbin{\&} q$ is an abbreviation for $\forall\, r\,((p \to q \to r) \to r)$.

The PLC expression corresponding to this proof is:

$$
\Lambda\, p, q\,(\lambda\, z : p \mathbin{\&} q\,(z\, p\,(\lambda\, x : p, y : q\,(x)))).
$$

$$\dfrac{}{\{z:p\&q,\ x:p,\ y:q\}\vdash x:p}\ (\mathrm{id})$$

$$\dfrac{\dfrac{\{z:p\&q,\ x:p,\ y:q\}\vdash x:p}{}}{\{z:p\&q\}\vdash \lambda x:p,y:q(x):p\to q\to p}\ (\mathrm{fn})^2$$

$$\dfrac{}{\{z:p\&q\}\vdash z:\forall r((p\to q\to r)\to r)}\ (\mathrm{id})$$

$$\dfrac{\{z:p\&q\}\vdash z:\forall r((p\to q\to r)\to r)}{\{z:p\&q\}\vdash zp:(p\to q\to p)\to p}\ (\mathrm{spec})$$

$$\dfrac{\{z:p\&q\}\vdash \lambda x:p,y:q(x):p\to q\to p \qquad \{z:p\&q\}\vdash zp:(p\to q\to p)\to p}{\{z:p\&q\}\vdash zp(\lambda x:p,y:q(x)):p}\ (\mathrm{app})$$

$$\dfrac{\{z:p\&q\}\vdash zp(\lambda x:p,y:q(x)):p}{\{\}\vdash \lambda z:p\&q(zp(\lambda x:p,y:q(x))):p\&q\to p}\ (\mathrm{fn})$$

$$\dfrac{\dfrac{\{\}\vdash \lambda z:p\&q(zp(\lambda x:p,y:q(x))):p\&q\to p}{}}{\{\}\vdash \Lambda p,q(\lambda z:p\&q(zp(\lambda x:p,y:q(x)))):\forall p,q(p\&q\to p)}\ (\mathrm{gen})^2$$

this PLC term captures the structure of the original 2IPC proof of $\{\}\vdash\forall p,q(p\&q\to p)$

Logical operations definable in 2IPC

- *Truth*: $\boldsymbol{true} \stackrel{\text{def}}{=} \forall\, p\,(p \rightarrow p)$.
- *Falsity*: $\boldsymbol{false} \stackrel{\text{def}}{=} \forall\, p\,(p)$.
- *Conjunction*: $\phi \,\&\, \phi' \stackrel{\text{def}}{=} \forall\, p\,((\phi \rightarrow \phi' \rightarrow p) \rightarrow p)$ (where $p \notin fv(\phi, \phi')$).
- *Disjunction*: $\phi \vee \phi' \stackrel{\text{def}}{=} \forall\, p\,((\phi \rightarrow p) \rightarrow (\phi' \rightarrow p) \rightarrow p)$ (where $p \notin fv(\phi, \phi')$).
- *Negation*: $\neg\phi \stackrel{\text{def}}{=} \phi \rightarrow \boldsymbol{false}$.
- *Existential quantification*:
  $\exists\, p\,(\phi) \stackrel{\text{def}}{=} \forall\, p'\,(\forall\, p\,(\phi \rightarrow p') \rightarrow p')$
  (where $p' \notin fv(\phi, p)$).

2IPC is a constructive logic

For example, there is no proof of the *Law of Excluded Middle*

$$\forall\, p\,(p \lor \neg p)$$

Using the definitions on Slide 65, this is an abbreviation for

$$\forall\, p, q\,((p \to q) \to ((p \to \forall\, r\,(r)) \to q) \to q)$$

(The fact that there is no closed PLC term of type $\forall\, p\,(p \lor \neg p)$ can be proved using the technique developed in the Tripos question 13 on paper 9 in 2000.)

Curry-Howard correspondence

Logic	$\leftrightarrow$	*Type system*
propositions, ϕ	$\leftrightarrow$	types, τ
(constructive) proofs, p	$\leftrightarrow$	expressions, M
"p is a proof of ϕ"	$\leftrightarrow$	"M is an expression of type τ"
simplification of proofs	$\leftrightarrow$	reduction of expressions

2IPC

$\Phi, \varphi \vdash \varphi'$

$\Phi \vdash \varphi$

PLC

$\bar{x} : \Phi, x : \varphi \vdash M : \varphi'$

$\bar{x} : \Phi \vdash N : \varphi$

2IPC

$$\dfrac{\dfrac{\Phi, \varphi \vdash \varphi'}{\Phi \vdash \varphi \to \varphi'}\,(\to I) \qquad \Phi \vdash \varphi}{\Phi \vdash \varphi'}\,(\to E)$$

PLC

$$\bar{x} : \Phi, x : \varphi \vdash M : \varphi'$$

$$\bar{x} : \Phi \vdash N : \varphi$$

2IPC

$$\dfrac{\dfrac{\Phi, \varphi \vdash \varphi'}{\Phi \vdash \varphi \to \varphi'}\,(\to I) \qquad \Phi \vdash \varphi}{\Phi \vdash \varphi'}\,(\to E)$$

PLC

$$\dfrac{\bar{x}:\Phi, x:\varphi \vdash M : \varphi'}{\bar{x}:\Phi \vdash \lambda x:\varphi(M) : \varphi \to \varphi' \qquad \bar{x}:\Phi \vdash N : \varphi}$$

$$\bar{x}:\Phi \vdash (\lambda x:\varphi(M))N : \varphi'$$

2IPC

$$\dfrac{\dfrac{\Phi, \varphi \vdash \varphi'}{\Phi \vdash \varphi \to \varphi'}\,(\to I) \qquad \Phi \vdash \varphi}{\Phi \vdash \varphi'}\,(\to E)$$

PLC

$$\dfrac{\dfrac{\bar{x}:\Phi, x:\varphi \vdash M : \varphi'}{\bar{x}:\Phi \vdash \lambda x:\varphi(M) : \varphi \to \varphi'} \qquad \bar{x}:\Phi \vdash N : \varphi}{\bar{x}:\Phi \vdash (\lambda x:\varphi(M))N : \varphi'}$$

$$\Big\downarrow \ \beta\text{-reduces}$$

$$\bar{x}:\Phi \vdash M[N/x] : \varphi'$$

$$\text{2IPC} \xleftrightarrow[\text{Howard}]{\text{Curry-}} \text{PLC}$$

$$\dfrac{\dfrac{\Phi, \varphi \vdash \varphi'}{\Phi \vdash \varphi \to \varphi'}(\to I) \qquad \Phi \vdash \varphi}{\Phi \vdash \varphi'}(\to E)$$

$$\dfrac{\dfrac{\bar{x}:\Phi, x:\varphi \vdash M : \varphi'}{\bar{x}:\Phi \vdash \lambda x{:}\varphi(M) : \varphi \to \varphi'} \qquad \bar{x}:\Phi \vdash N : \varphi}{\bar{x}:\Phi \vdash (\lambda x{:}\varphi(M))N : \varphi'}$$

$$\Big\downarrow \ \beta\text{-reduces}$$

$$\bar{x}:\Phi \vdash M[N/x] : \varphi'$$

Can simplify this proof to a prove of

$$\Phi \vdash \varphi'$$

("CUT RULE")

Type-inference versus proof search

Type-inference: "given Γ and M, is there a type τ such that $\Gamma \vdash M : \tau$?"

(For PLC/2IPC this is decidable.)

Proof-search: "given Γ and ϕ, is there a proof term M such that $\Gamma \vdash M : \phi$?"

(For PLC/2IPC this is undecidable.)