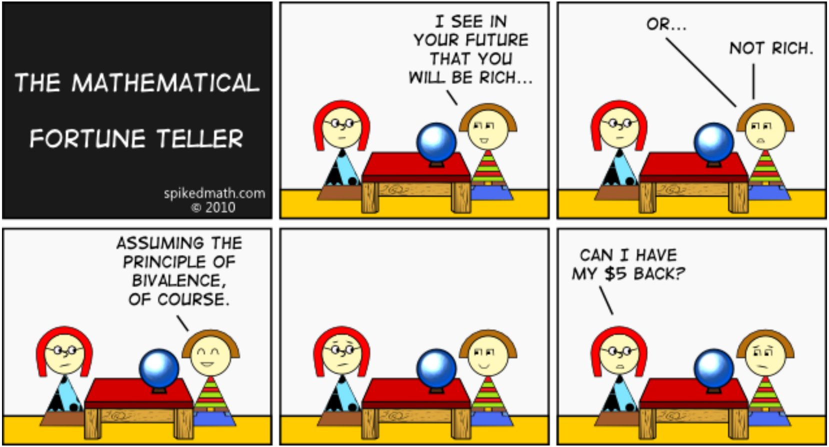
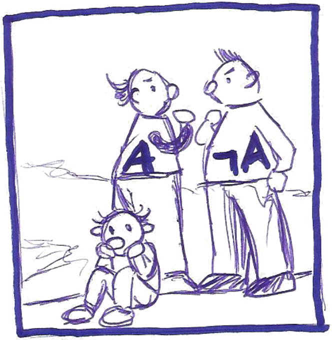


THE MATHEMATICAL FORTUNE TELLER
spikedmath.com
© 2010
I SEE IN YOUR FUTURE THAT YOU WILL BE RICH...
OR...
NOT RICH.
ASSUMING THE PRINCIPLE OF BIVALENCE, OF COURSE.
CAN I HAVE MY $5 BACK?

Double-negation translation and CPS transformation



Ingo Blechschmidt

June 3rd, 2015 at KU Leuven

Outline

Non-constructive proofs

Theorem. There exist **irrational** numbers x, y such that x^y is rational.

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational or not.

In the first case we are done.

In the second case take $x := \sqrt{2}^{\sqrt{2}}$ and $y := \sqrt{2}$. Then $x^y = 2$ is rational.

The law of excluded middle

"For any formula A, we may deduce $A \lor \neg A$."

Classical logic $=$
intuitionistic logic $+$ law of excluded middle.

Classical interpretation

$\bot$	There is a contradiction.
$A \land B$	A and B are true.
$A \lor B$	A is true or B is true.
$A \Rightarrow B$	If A holds, then also B.
$\forall x{:}X.\ A(x)$	For all $x : X$ it holds that $A(x)$.
$\exists x{:}X.\ A(x)$	There is an $x : X$ such that $A(x)$.

The law of excluded middle

"For any formula A, we may deduce $A \vee \neg A$."

Classical logic $=$
intuitionistic logic $+$ law of excluded middle.

Constructive interpretation

$\bot$	There is a contradiction.
$A \wedge B$	We have evidence for A and for B.
$A \vee B$	We have evidence for A or for B.
$A \Rightarrow B$	We can transform evidence for A into one for B.
$\forall x{:}X.\, A(x)$	Given $x : X$, we can construct evidence for $A(x)$.
$\exists x{:}X.\, A(x)$	We have an $x : X$ together with evidence for $A(x)$.

Negated statements

"$\neg A$" is syntactic sugar for $(A \Rightarrow \bot)$
and means: There can't be any evidence for A.

Constructive interpretation

$\bot$	There is a contradiction.
$A \wedge B$	We have evidence for A and for B.
$A \vee B$	We have evidence for A or for B.
$A \Rightarrow B$	We can transform evidence for A into one for B.
$\forall x{:}X.\ A(x)$	Given $x : X$, we can construct evidence for $A(x)$.
$\exists x{:}X.\ A(x)$	We have an $x : X$ together with evidence for $A(x)$.

Doubly-negated statements

"$\neg\neg A$" means: There can't be any evidence for $\neg A$.

Trivially, we have $A \implies \neg\neg A$.
We can't deduce $\neg\neg A \implies A$.

Constructive interpretation

$\bot$	There is a contradiction.
$A \wedge B$	We have evidence for A and for B.
$A \vee B$	We have evidence for A or for B.
$A \Rightarrow B$	We can transform evidence for A into one for B.
$\forall x{:}X.\, A(x)$	Given $x : X$, we can construct evidence for $A(x)$.
$\exists x{:}X.\, A(x)$	We have an $x : X$ together with evidence for $A(x)$.

Doubly-negated statements

"$\neg\neg A$" means: There can't be any evidence for $\neg A$.

Trivially, we have $A \implies \neg\neg A$.
We can't deduce $\neg\neg A \implies A$.

Where is the key?

$\neg\neg(\exists x.\ \text{the key is at position } x)$

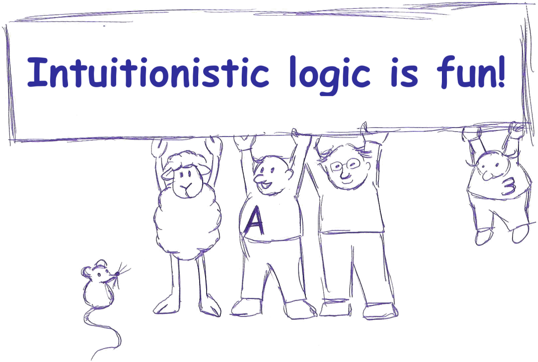
versus

$\exists x.\ \text{the key is at position } x$

Applications

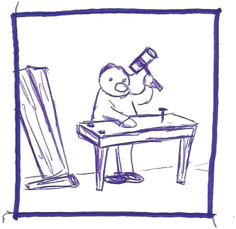
Intuitionistic logic …

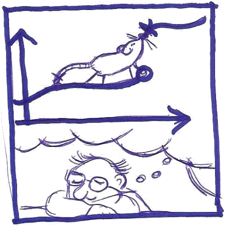
- can guide to more elegant proofs,
- is good for the mental hygiene, and
- allows to make finer distictions.



Applications

- We can **mechanically extract algorithms** from intuitionistic proofs of existence statements.
- The **internal language of toposes** is intuitionistic.
- **Dream mathematics** only works intuitionistically.





Topos power

Any finitely generated vector space does *not not* possess a basis.

$$\Downarrow$$

Any sheaf of modules of finite type on a reduced scheme is locally free on a dense open subset.

Dream mathematics

Synthetic differential geometry

Any map $\mathbb{R} \to \mathbb{R}$ is smooth. There are infinitesimal numbers ε such that $\varepsilon^2 = 0$ and $\varepsilon \neq 0$.

Synthetic domain theory

For any set X there exists a map

$$\mathsf{fix} : (X \to X) \to X$$

such that $f(\mathsf{fix}(f)) = \mathsf{fix}(f)$ for any $f : X \to X$.

Synthetic computability theory

There are only countably many subsets of $\mathbb{N}$.

The doubly-negated LEM

Even intuitionistically "$\neg\neg(A \lor \neg A)$" holds.

Proof. Assume $\neg(A \lor \neg A)$, we want to show $\bot$.

If A, then $A \lor \neg A$, thus $\bot$.

Therefore $\neg A$.

Since $\neg A$, we have $A \lor \neg A$, thus $\bot$.

The ¬¬-translation

$$
\begin{aligned}
A^{\Box} &:\equiv \neg\neg A \text{ for atomic formulas } A \\
(A \wedge B)^{\Box} &:\equiv \neg\neg(A^{\Box} \wedge B^{\Box}) \\
(A \vee B)^{\Box} &:\equiv \neg\neg(A^{\Box} \vee B^{\Box}) \\
(A \Rightarrow B)^{\Box} &:\equiv \neg\neg(A^{\Box} \Rightarrow B^{\Box}) \\
(\forall x{:}X.\, A(x))^{\Box} &:\equiv \neg\neg(\forall x{:}X.\, A^{\Box}(x)) \\
(\exists x{:}X.\, A(x))^{\Box} &:\equiv \neg\neg(\exists x{:}X.\, A^{\Box}(x))
\end{aligned}
$$

Theorem. A classically $\Longleftrightarrow$ $A^{\Box}$ intuitionistically.

A classical logic fairy tale

A classical logic fairy tale

A intuitionistically $\iff$ we can defend A in any dialog.

A classically $\iff$ we can defend $A^{\Box}$ in any dialog.

A classical logic fairy tale

$$A \text{ intuitionistically} \iff \text{we can defend } A \text{ in any dialog.}$$

$$A \text{ classically} \iff \text{we can defend } A^{\square} \text{ in any dialog.}$$

$$\iff \text{we can defend } A \text{ in any dialog with jumps back in time allowed.}$$

Curry–Howard correspondence

logic	**programming**
formula A	type A
intuitionistic proof $p : A$	term $p : A$
conjunction $A \wedge B$	product type (A, B)
disjunction $A \vee B$	sum type Either A B
implication $A \Rightarrow B$	function type $A \to B$

Curry–Howard correspondence

logic	**programming**
formula A	type A
intuitionistic proof $p : A$	term $p : A$
conjunction $A \wedge B$	product type (A, B)
disjunction $A \vee B$	sum type Either A B
implication $A \Rightarrow B$	function type $A \to B$
$\neg\neg$-translation	**CPS transformation**

Curry–Howard correspondence

logic	**programming**
formula A	type A
intuitionistic proof $p : A$	term $p : A$
conjunction $A \wedge B$	product type (A, B)
disjunction $A \vee B$	sum type Either A B
implication $A \Rightarrow B$	function type $A \rightarrow B$
$\neg\neg$-translation	**CPS transformation**
$\neg\neg A$	??

Curry–Howard correspondence

logic	programming
formula A	type A
intuitionistic proof $p : A$	term $p : A$
conjunction $A \wedge B$	product type (A, B)
disjunction $A \vee B$	sum type Either A B
implication $A \Rightarrow B$	function type $A \to B$
$\neg\neg$-translation	**CPS transformation**
$(A \Rightarrow \bot) \Rightarrow \bot$	??

Curry–Howard correspondence

logic	**programming**
formula A	type A
intuitionistic proof $p : A$	term $p : A$
conjunction $A \wedge B$	product type (A, B)
disjunction $A \vee B$	sum type Either A B
implication $A \Rightarrow B$	function type $A \to B$
$\neg\neg$-translation	**CPS transformation**
$(A \Rightarrow \bot) \Rightarrow \bot$	$(A \to r) \to r$

Computational content of classical proofs

```
type Cont r a = ((a -> r) -> r)

-- Decide an arbitrary statement a.
lem :: Cont r (Either a (a -> Cont r b))
lem k = k $ Right $ \x -> (\k' -> k (Left x))

-- Calculate the minimum of an infinite list
-- of natural numbers.
min :: [Nat] -> Cont r (Int, Int -> Cont r ())
min xs = ...
```

Outlook

- CPS transformation = Yoneda embedding
- What about delimited continuations?
- Geometrical interpretation:

$$\mathrm{Sh}(X) \models A^{\Box} \quad \Longleftrightarrow \quad \mathrm{Sh}(X_{\neg\neg}) \models A$$

- Generalize from $\neg\neg$ to arbitrary **modal operators** (monads): Relevant axioms are
  1. $A \Rightarrow \Box A$
  2. $\Box\Box A \Rightarrow \Box A$
  3. $\Box(A \wedge B) \Leftrightarrow \Box A \wedge \Box B$

Outlook

- CPS transformation = Yoneda embedding
- What about delimited continuations?
- Geometrical interpretation:

$$\mathrm{Sh}(X) \models A^{\Box} \quad \Longleftrightarrow \quad \mathrm{Sh}(X_{\neg\neg}) \models A$$

- Generalize from $\neg\neg$ to arbitrary **modal operators** (monads): Relevant axioms are
  1. $A \Rightarrow \Box A$
  2. $\Box\Box A \Rightarrow \Box A$
  3. $\Box(A \wedge B) \Leftrightarrow \Box A \wedge \Box B$

github /iblech/talk-constructive-mathematics