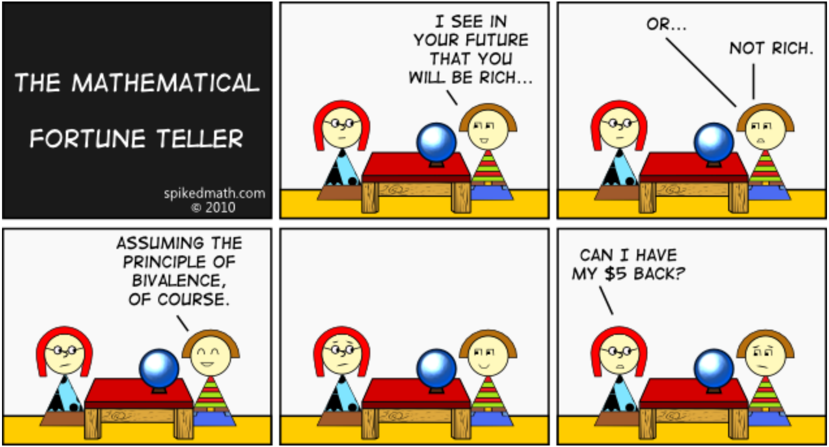
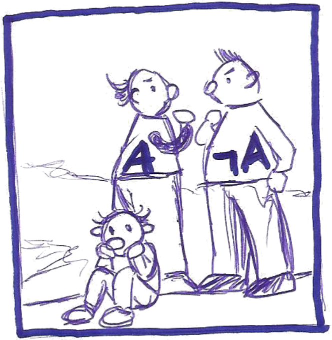

THE MATHEMATICAL FORTUNE TELLER
spikedmath.com
© 2010
I SEE IN YOUR FUTURE THAT YOU WILL BE RICH...
OR...
NOT RICH.
ASSUMING THE PRINCIPLE OF BIVALENCE, OF COURSE.
CAN I HAVE MY $5 BACK?

Double-negation translation and CPS transformation



Ingo Blechschmidt

June 3rd, 2015 at KU Leuven

This annotated version of the slides is not yet finished.

Expect references and more explanations in the next few days.

Abstract

Constructive mathematicians don't use the law of excluded middle, which approximately says that for any proposition P, either P is true or $\neg P$ is true. Several advantages emerge from this rejection, for instance one can mechanically extract algorithms from constructive proofs of existence statements and rigorously work with non-standard *dream axioms* which are plainly false in classical mathematics, such as *any function is smooth*.

For communicating with classicial mathematicians, constructive mathematicians can employ the *double-negation translation*. This device associates to any formula a translated formula in such a way that a given formula holds classically if and only if its translation holds constructively.

The talk will give an introduction to these topics and discuss the intriguing relationship of the double-negation translation with the well-known continuation-passing style transformation: In some sense, they are the same. This is a beautiful facet of *computational trinitarianism*.

For the first part of the talk, no background in formal logic or constructive mathematics is required. For the second part of the talk, one should be vaguely familiar with the continuation-passing style transformation.

Outline

1. Constructive mathematics
    - The law of excluded middle
    - Interpretation of intuitionistic logic
    - Applications

2. The double-negation translation
    - The doubly-negated law of excluded middle
    - The fundamental result
    - Game-theoretical interpretation

3. Continuations
    - The Curry–Howard correspondence
    - Computational content of classical proofs

4. Outlook

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 $A \vee \neg A$."

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

Classical interpretation

$\bot$	There is a contradiction.
$A \wedge B$	A and B are true.
$A \vee B$	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 $A(x)$.

More precisely, one should say: Classical mathematics = intuitionistic logic + law of excluded middle + a set theory including the axiom of choice.

The constructive interpretation of the axiom of excluded middle is: For any formula A, we have evidence for A or for $\neg A$. This is an absurd statement.

Several years ago a video showing Kate Moss consuming drugs surfaced. From the video it was clear that the drugs were either of some type A or of some type B, but there was no direct evidence for either type. Kate Moss was not prosecuted; in this sense, Great Britain's judicial system operated intuitionistically.

Note that constructive mathematicians do *not* claim that the law of excluded middle is false (that is, that its negation holds). In fact, some instances of the law of excluded middle are true intuitionistically: For example one can show by induction that any natural number is zero or is not zero. Constructive mathematicians simply don't suppose that the law of excluded holds generally.

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 $A(x)$.

Note that the word “contradiction” is not generally forbidden in intuitionistic logic. For instance, the usual proof that $\sqrt{2}$ is not rational, deducing $\bot$ from the assumption that $\sqrt{2}$ were rational, is perfectly fine intuitionistically.

Colloquially, those proofs are called “proof by contradiction”, but this labeling is deceptive. A true proof by contradiction runs like this:

> *We want to show A. Assume $\neg A$. Then . . ., so $\bot$. Therefore $\neg\neg A$. Thus A.*

The last step needs the axiom of double negation elimination, $\neg\neg A \Rightarrow A$, which is not available in intuitionistic logic. (In fact, the statement that double negation elimination holds for all A is equivalent to the statement that the law of excluded middle holds for all A.)

Doubly-negated statements

“$\neg\neg A$” means: There can’t be any evidence for $\neg A$.

Trivially, we have $A \Longrightarrow \neg\neg A$.
We can’t deduce $\neg\neg A \Longrightarrow A$.

Constructive interpretation

$\perp$	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

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

If we know that the key to our apartment has to be somewhere in the apartment (since we used it to enter last night) but we can't find it, we can constructively only justify

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

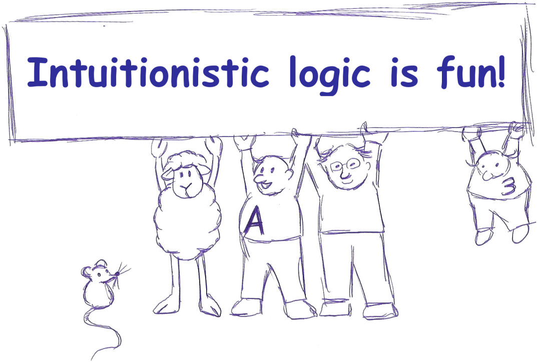
not the stronger statement

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

Applications

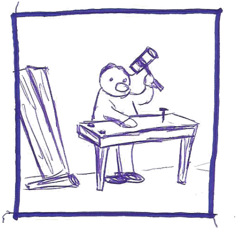
Intuitionistic logic …

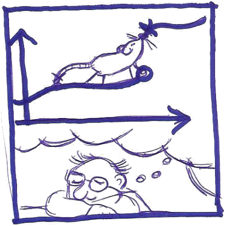
- can guide to more elegant proofs,
- is good for the mental hygiene, and
- allows to make finer distictions.



Applications

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





Here is a basic example for extracting algorithms from proofs. Consider the statement

> *"There are infinitely many prime numbers."* or somewhat more explicitly, *"For any finite list $p_1, \ldots, p_n$ of prime numbers, there exists an additional prime number q not on that list."*

The standard proof, attributed to Euclid, goes like this:

> *Consider the number $N := p_1 \cdots p_n + 1$. Since $N \geq 2$, there exists some prime factor q of N. (If N is itself prime, we can take $q := N$.) This prime is not equal to any p_i, since the numbers p_i don't divide N whereas q does.*

The algorithm for constructing q can be directly read off from the proof. Different proofs result in different algorithms; in particular, there exist (more complex) proofs whose algorithms produce better (smaller) witnesses.

See the wonderful book *Applied Proof Theory: Proof Interpretations and their Use in Mathematics* by Kohlenbach for details. Already its introduction is a very worthwhile reading.

Tangentially, observe that the stated constructive version of Euclid's proof is less prone to misunderstandings than its well-known counterpart which uses proof by contradiction:

> *Assume that there are only a finite number of primes, $p_1, \ldots, p_n$. Then consider $N := p_1 \cdots p_n + 1$. This number is either prime or composite. Since no prime number divides N (by assumption the only primes are the p_i and these don't divide N), it cannot be composite. Therefore N is prime. Since N doesn't equal any of the p_i, this is a contradiction.*

From this proof one might think that for primes $p_1, \ldots, p_n$ the number $N := p_1 \cdots p_n + 1$ is always prime. But this only holds in a counterfactual world where there are only finitely many primes. In fact, the number

$$N := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$$

is composite. A shorter example is

$$N := 2 \cdot 7 + 1 = 3 \cdot 5.$$

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.

Toposes are certain kinds of categories, thought of as *mathematical universes*. The usual topos in which we do mathematics in is the category of sets and maps between sets, but there are many others:

- In the *effective topos*, any map is computable.
- In the *sheaf topos* of a topological space X the objects and morphisms depend on our position in X.

A metatheorem states that *intuitionistically provable statements hold in any topos*. This greatly expands the scope of an intuitionistic theorem.

A side project of mine is to recognize the basic concepts and statements of algebraic geometry as topos-theoretic interpretations of simple concepts and statements of ordinary first-year linear algebra. See `https://github.com/iblech/internal-methods` for expository notes on this topic (directed at geometers).

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 $\iff$ $A^{\Box}$ intuitionistically.

The gray $\neg\neg$'s can be omitted: One can prove by structural induction that translating with those double negations yields logically equivalent formulas as translating without those.

The blue $\neg\neg$'s in contrast are crucial.

One could say that the only difference between intuitionistic logic and classical logic is in the meaning of disjunction and existential quantification.

Note that $\bot^\Box \equiv \neg\neg\bot \Leftrightarrow \bot$.

Corollary. Peano arithmetic and Heyting arithmetic are equiconsistent. (Recall that Heyting arithmetic is the same as Peano arithmetic, only with intuitionistic instead of classical logic.)

Proof. It is clear that inconsistency of Heyting arithmetic implies inconsistency of Peano arithmetic.

For the converse direction, write Ax for the axioms of Peano arithmetic, thought of as a single formula by conjuction. If Peano arithmetic proves $\bot$, that is if $\mathrm{Ax} \Rightarrow \bot$ classically, then by the theorem $\mathrm{Ax}^\Box \Rightarrow \bot^\Box$ intuitionistically. By inspection $\mathrm{Ax} \Rightarrow \mathrm{Ax}^\Box$ intuitionistically. Therefore $\mathrm{Ax} \Rightarrow \bot$ 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 intuitionistically $\iff$ we can defend A in any dialog.

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

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

Curry–Howard correspondence

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

Note that different, but logically equivalent versions of the double-negation translation yield different variants of the CPS transformation (call by name, call by value, …).

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
- 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
- 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