Teaching logic using ProofWeb

Cezary Kaliszyk, Freek Wiedijk
Radboud University Nijmegen
cek@cs.ru.nl

July 11, 2009

Outline

Motivation: teaching logic with the computer

logic course for math/computer science students:

- propositional logic
- predicate logic
- predicate logic with equality

Motivation: teaching logic with the computer

logic course for math/computer science students:

propositional logic
predicate logic
predicate logic with equality

practising natural deduction proofs

- **on paper**
- **with the computer**

Motivation: teaching logic with the computer

logic course for math/computer science students :

propositional logic
predicate logic
predicate logic with equality

practising natural deduction proofs

- **on paper**
  students does not learn to be precise
- **with the computer**

Motivation: teaching logic with the computer

logic course for math/computer science students :

propositional logic
predicate logic
predicate logic with equality

practising natural deduction proofs

- **on paper**
  students does not learn to be precise
- **with the computer**
  student does not learn to do it all himself

Motivation: teaching logic with the computer

logic course for math/computer science students :

propositional logic
predicate logic
predicate logic with equality

practising natural deduction proofs

- **on paper**
  students does not learn to be precise
- **with the computer**
  student does not learn to do it all himself

both necessary: complement each other

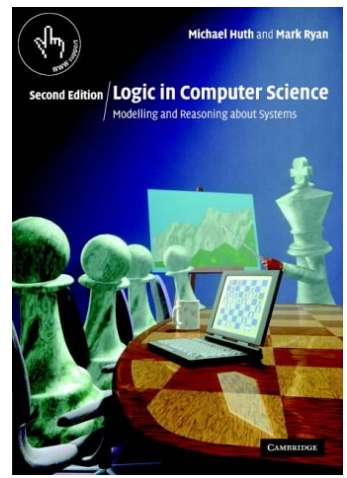
Web interface for proof assistants

- No installation for a user (not even browser plug-in)
- Responsive, fast interaction
- Resembles and behaves like a local interface
- Multiple proof assistants (like ProofGeneral)
  - Updated on the server, with extensions
- Secure environment

Outline

ProofWeb features

- built on top of serious proof system: Coq
  - students work with an industrial strength system
  - proofs look exactly like in a traditional textbook
    compatible with: Huth & Ryan, Login in Computer Science



- web-based
  - students don't need to install anything
  - students can access their work from anywhere
  - teacher has at all times full info on student's work

- comes with a manual explaining the system

- comes with a set of graded exercises

Coq

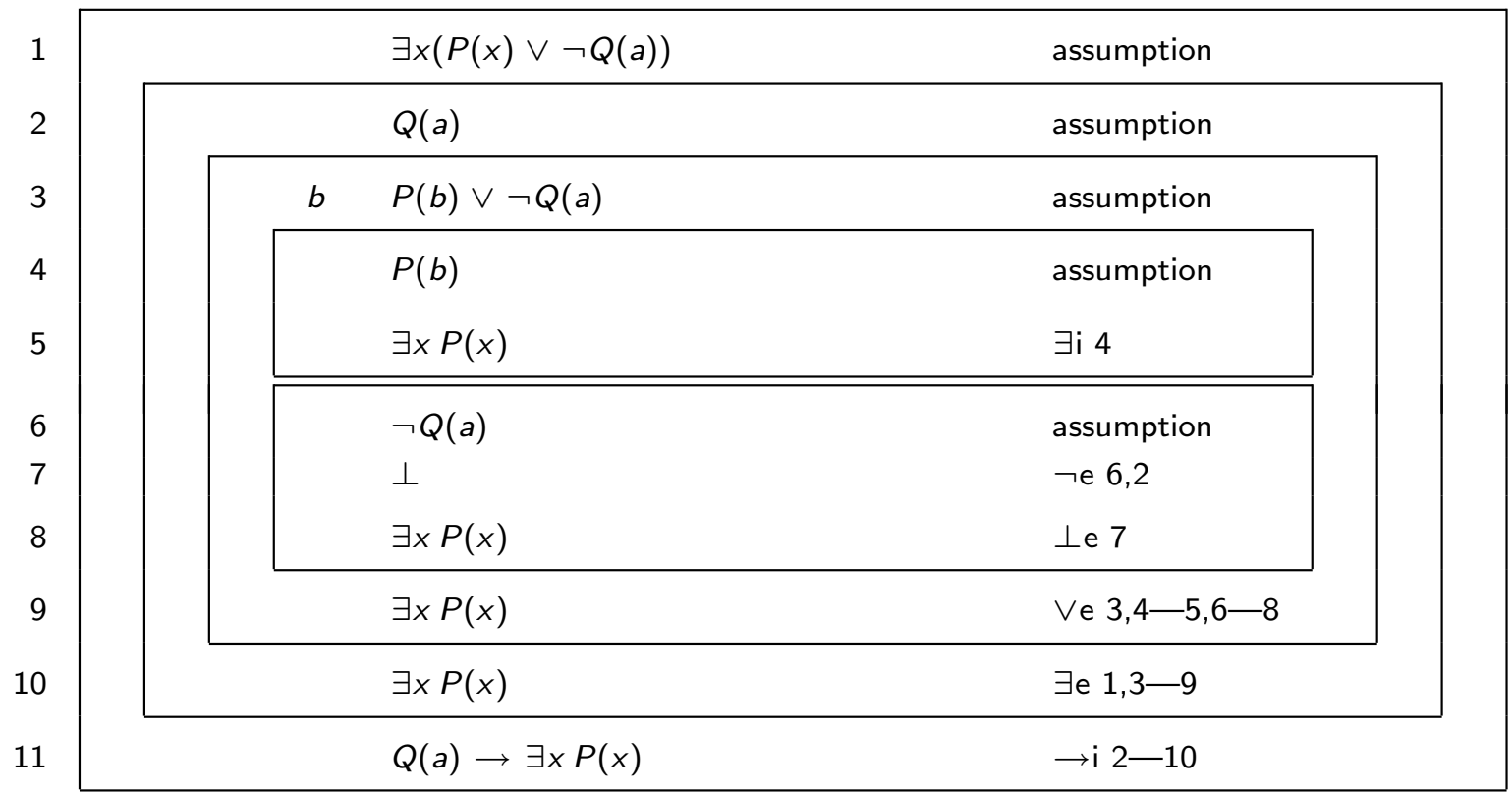
proof assistant based on constructive logic
developed at INRIA, France
1984 until today

used for impressive proofs :

- four color theorem, Georges Gonthier
- verified C compiler, Xavier Leroy

power of Coq also makes ProofWeb attractive for education

natural deduction (Fitch style)



natural deduction (Fitch style)

1	H1:	∃x, (P x ∨ ¬Q a)	assumption
2	H2:	Q a	assumption
	b		
3	H3:	P b ∨ ¬Q a	assumption
4	H4:	P b	assumption
5		∃x, P x	∃i 4
6	H5:	¬Q a	assumption
7		⊥	¬e 6,2
8		∃x, P x	⊥e 7
9		∃x, P x	∨e 3,4-5,6-8
10		∃x, P x	∃e 1,3-9
11		Q a ⟶ ∃x, P x	⟶i 2-10
12		∃x, (P x ∨ ¬Q a) ⟶ Q a ⟶ ∃x, P x	⟶i 1-11

1		$\exists x(P(x) \vee \neg Q(a))$	assumption
2		$Q(a)$	assumption
3	b	$P(b) \vee \neg Q(a)$	assumption
4		$P(b)$	assumption
5		$\exists x\, P(x)$	∃i 4
6		$\neg Q(a)$	assumption
7		$\bot$	¬e 6,2
8		$\exists x\, P(x)$	⊥e 7
9		$\exists x\, P(x)$	∨e 3,4—5,6—8
10		$\exists x\, P(x)$	∃e 1,3—9
11		$Q(a) \rightarrow \exists x\, P(x)$	→i 2—10

natural deduction (Gentzen style)

$$\dfrac{\dfrac{[\exists x(P(x) \vee \neg Q(a))]^{\mathtt{H1}} \qquad \dfrac{[P(b) \vee \neg Q(a)]^{\mathtt{H3}} \qquad \dfrac{[P(b)]^{\mathtt{H4}}}{\exists x\, P(x)}\,\exists\mathtt{i} \qquad \dfrac{\dfrac{[\neg Q(a)]^{\mathtt{H5}} \qquad [Q(a)]^{\mathtt{H2}}}{\bot}\,\neg\mathtt{e}}{\exists x\, P(x)}\,\bot\mathtt{e}}{\exists x\, P(x)}\,\vee\mathtt{e}\ [\mathtt{H4},\mathtt{H5}]}{\exists x\, P(x)}\,\exists\mathtt{e}\ [\mathtt{H3}]}{Q(a) \to \exists x\, P(x)}\,\to\mathtt{i}\ [\mathtt{H2}]}{\exists x(P(x) \vee \neg Q(a)) \to Q(a) \to \exists x\, P(x)}\,\to\mathtt{i}\ [\mathtt{H1}]$$

natural deduction (Gentzen style)

$$\dfrac{\dfrac{[\exists x,\ (P\ x \lor \neg Q\ a)]^{H1} \qquad \dfrac{\dfrac{[P\ b \lor \neg Q\ a]^{H3} \qquad \dfrac{[P\ b]^{H4}}{\exists x,\ P\ x}\exists i \qquad \dfrac{\dfrac{[\neg Q\ a]^{H5} \quad [Q\ a]^{H2}}{\bot}\neg e}{\exists x,\ P\ x}\bot e}{\exists x,\ P\ x}\lor e\,[H4,H5]}{\exists x,\ P\ x}\exists e\,[H3]}{Q\ a \to \exists x,\ P\ x}\to i\,[H2]}{\exists x,\ (P\ x \lor \neg Q\ a) \to Q\ a \to \exists x,\ P\ x}\to i\,[H1]$$

$$\dfrac{\dfrac{[\exists x(P(x) \lor \neg Q(a))]^{H1} \qquad \dfrac{\dfrac{[P(b) \lor \neg Q(a)]^{H3} \qquad \dfrac{[P(b)]^{H4}}{\exists x\,P(x)}\exists i \qquad \dfrac{\dfrac{[\neg Q(a)]^{H5} \quad [Q(a)]^{H2}}{\bot}\neg e}{\exists x\,P(x)}\bot e}{\exists x\,P(x)}\lor e\,[H4,H5]}{\exists x\,P(x)}\exists e\,[H3]}{Q(a) \to \exists x\,P(x)}\to i\,[H2]}{\exists x(P(x) \lor \neg Q(a)) \to Q(a) \to \exists x\,P(x)}\to i\,[H1]$$

user input

```
Require Import ProofWeb.

Variable P Q : D -> Prop.
Variable a : D.

Theorem example : exi x, (P(x) \/  Q(a)) -> Q(a) -> exi x, P(x).
Proof.




Qed.
```

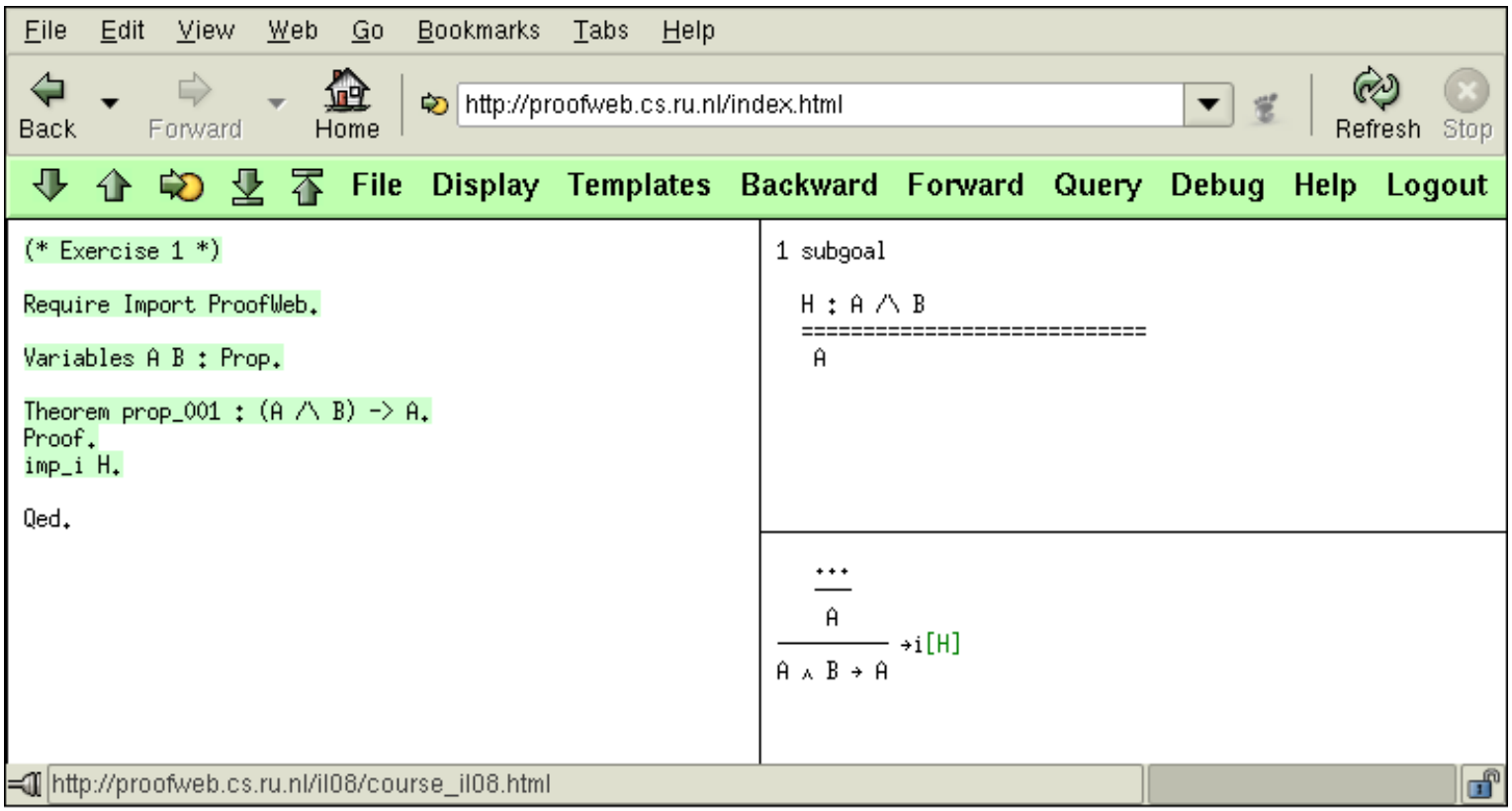
user input

```
Require Import ProofWeb.

Variable P Q : D -> Prop.
Variable a : D.

Theorem example : exi x, (P(x) \/  Q(a)) -> Q(a) -> exi x, P(x).
Proof.
imp_i H1.
imp_i H2.
f_exi_e H1 b H3.
f_dis_e H3 H4 H5.
f_exi_i H4.
fls_e.
f_neg_e H5 H2.
Qed.
```

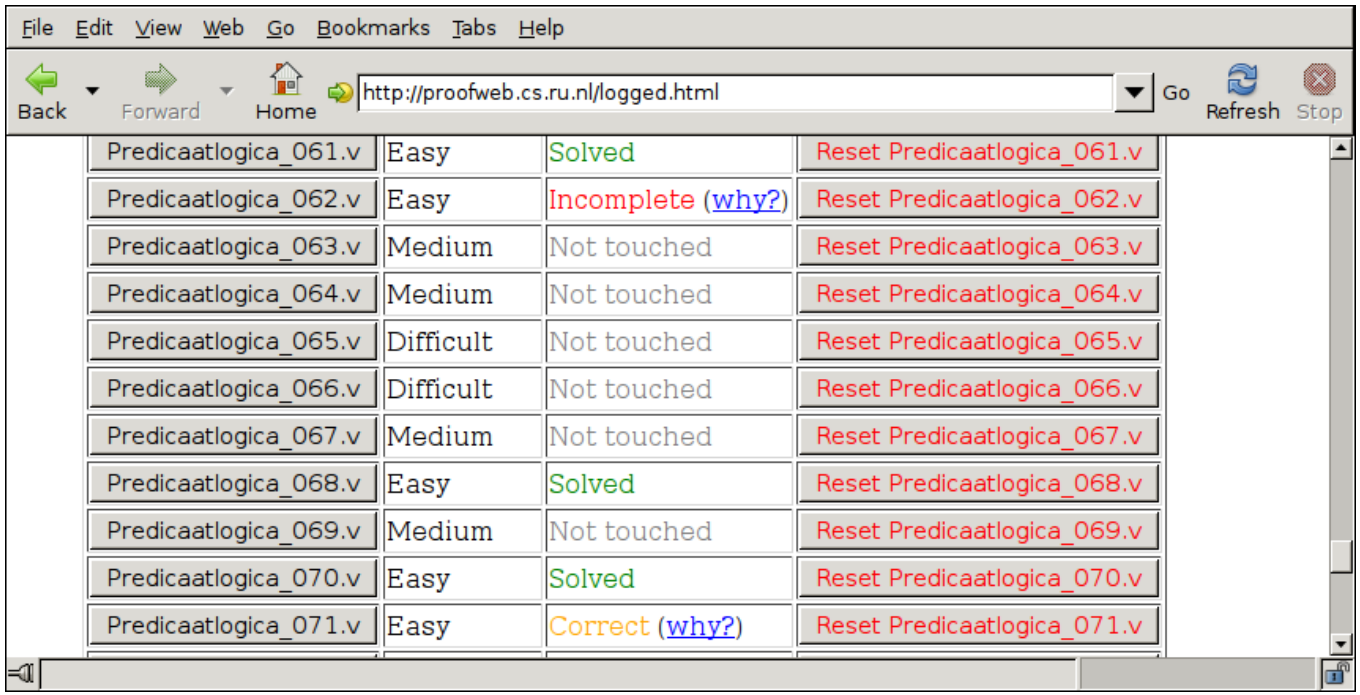
Working with ProofWeb



exercise colors

possibilities for an exercise :

- Not touched
- Incomplete
- Correct
- Solved



trying ProofWeb

three possibilities :

`http://proofweb.cs.ru.nl/`

1. **guest access** (no registration needed)
2. **host course in Nijmegen** (free)
3. download (open source) and **host course on your own system**

Outline

A future project: MathWiki

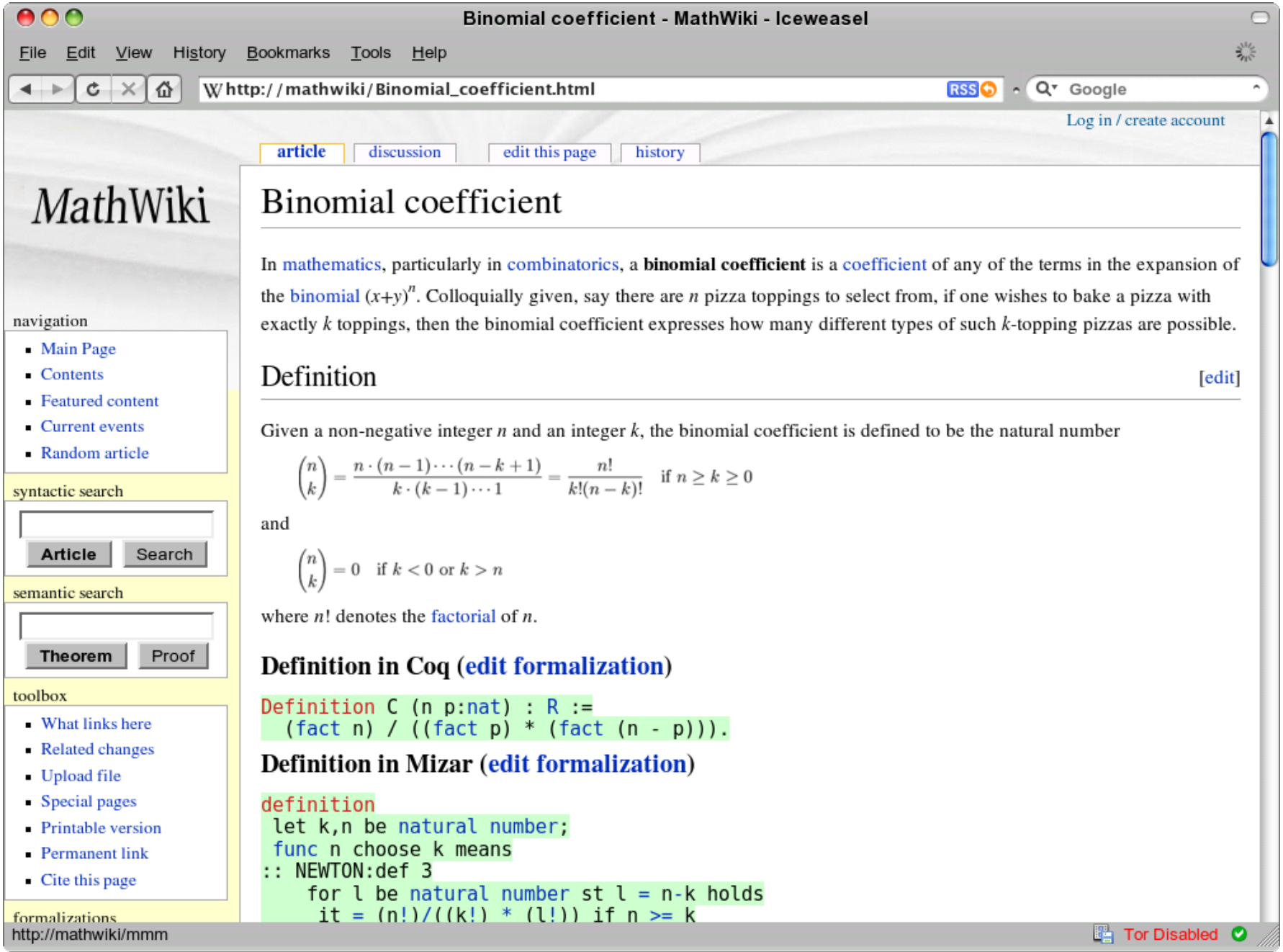
- 4 year project, 2009-2013
  - Post-doc and PhD student
- Combine an **encyclopedia** with a proof assistant environment
  - Semantically annotated high-level knowledge

A future project: MathWiki

- 4 year project, 2009-2013
  - Post-doc and PhD student
- Combine an **encyclopedia** with a proof assistant environment
  - Semantically annotated high-level knowledge
- Web-based, interactive, collaborative environment
  - For multiple proof assistants

A future project: MathWiki

- 4 year project, 2009-2013
  - Post-doc and PhD student
- Combine an **encyclopedia** with a proof assistant environment
  - Semantically annotated high-level knowledge
- Web-based, interactive, collaborative environment
  - For multiple proof assistants
- Supports large joint formalisations in a distributed way
- *Search and retrieval*
  - informal and formal
  - high level and proof assistant specific


Binomial coefficient - MathWiki - Iceweasel
File Edit View History Bookmarks Tools Help
http://mathwiki/Binomial_coefficient.html
Google
Log in / create account
article discussion edit this page history
MathWiki
navigation
Main Page
Contents
Featured content
Current events
Random article
syntactic search
Article Search
semantic search
Theorem Proof
toolbox
What links here
Related changes
Upload file
Special pages
Printable version
Permanent link
Cite this page
formalizations
Binomial coefficient
In mathematics, particularly in combinatorics, a binomial coefficient is a coefficient of any of the terms in the expansion of the binomial $(x+y)^n$. Colloquially given, say there are n pizza toppings to select from, if one wishes to bake a pizza with exactly k toppings, then the binomial coefficient expresses how many different types of such k-topping pizzas are possible.
Definition [edit]
Given a non-negative integer n and an integer k, the binomial coefficient is defined to be the natural number
$$\binom{n}{k} = \frac{n\cdot(n-1)\cdots(n-k+1)}{k\cdot(k-1)\cdots 1} = \frac{n!}{k!(n-k)!} \quad \text{if } n \geq k \geq 0$$
and
$$\binom{n}{k} = 0 \quad \text{if } k < 0 \text{ or } k > n$$
where $n!$ denotes the factorial of n.
Definition in Coq (edit formalization)
Definition C (n p:nat) : R :=
(fact n) / ((fact p) * (fact (n - p))).
Definition in Mizar (edit formalization)
definition
let k,n be natural number;
func n choose k means
:: NEWTON:def 3
for l be natural number st l = n-k holds
it = (n!)/((k!) * (l!)) if n >= k
http://mathwiki/mmm
Tor Disabled

QED 15 years later?

- Success of the Wiki approach
  - Collaborative approach as a good way of developing bodies of shared knowledge
- *Semantic Web* technology can provide the presentation layer

QED 15 years later?

- Success of the Wiki approach
  - Collaborative approach as a good way of developing bodies of shared knowledge
- *Semantic Web* technology can provide the presentation layer
- Proof assistants provide mathematical semantics
  - Solid systems
  - Substantial formal developments
  - Coverage of a wide range of Proof Assistants:
    - initial proposed ones: Coq, Isabelle and Mizar
    - Type Theory, Higher Order Logic and Set Theory
    - classical and intuitionistic
    - de Bruijn style, LCF-style and batch-mode interaction

QED 15 years later?

- Success of the Wiki approach
  - Collaborative approach as a good way of developing bodies of shared knowledge
- *Semantic Web* technology can provide the presentation layer
- Proof assistants provide mathematical semantics
  - Solid systems
  - Substantial formal developments
  - Coverage of a wide range of Proof Assistants:
    - initial proposed ones: Coq, Isabelle and Mizar
    - Type Theory, Higher Order Logic and Set Theory
    - classical and intuitionistic
    - de Bruijn style, LCF-style and batch-mode interaction
- *Web 2.0*

Future plans

other proof display styles

other logics

- modal logics
- temporal logics
- logic in Dijkstra style

MathWiki