

Technical University of Denmark



## NaDeA: A Natural Deduction Assistant with a Formalization in Isabelle

Villadsen, Jørgen; Jensen, Alexander Birch; Schlichtkrull, Anders

*Published in:*

Proceedings of the Fourth International Conference on Tools for Teaching Logic (TTL 2015)

*Publication date:*

2015

*Document Version*

Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

*Citation (APA):*

Villadsen, J., Jensen, A. B., & Schlichtkrull, A. (2015). NaDeA: A Natural Deduction Assistant with a Formalization in Isabelle. In Proceedings of the Fourth International Conference on Tools for Teaching Logic (TTL 2015) (pp. 253-262)

## DTU Library

Technical Information Center of Denmark

---

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# NaDeA: A Natural Deduction Assistant with a Formalization in Isabelle

Jørgen Villadsen, Alexander Birch Jensen, and  
Anders Schlichtkrull

DTU Compute - Department of Applied Mathematics and Computer Science,  
Technical University of Denmark, Richard Petersens Plads, Building 324, DK-2800  
Kongens Lyngby, Denmark  
jovi@dtu.dk

---

## Abstract

We present a new software tool for teaching logic based on natural deduction. Its proof system is formalized in the proof assistant Isabelle such that its definition is very precise. Soundness of the formalization has been proved in Isabelle. The tool is open source software developed in TypeScript / JavaScript and can thus be used directly in a browser without any further installation. Although developed for undergraduate computer science students who are used to study and program concrete computer code in a programming language we consider the approach relevant for a broader audience and for other proof systems as well.

**1998 ACM Subject Classification** F.4.1 Mathematical Logic

**Keywords and phrases** Natural Deduction, Formalization, Isabelle Proof Assistant, First-Order Logic, Higher-Order Logic

## 1 Introduction

In this paper we present the NaDeA software tool. First, we provide the motivation and a short description. We then present the natural deduction system as it is done in a popular textbook [15] and as is it done in NaDeA by looking at its formalization in Isabelle. This illustrates the differences between the two approaches. We also present the semantics of first-order logic as formalized in Isabelle, which was used to prove the proof system of NaDeA sound. Thereafter we explain how NaDeA is used to construct a natural deduction proof. Lastly, we compare NaDeA to other natural deduction assistants and consider how NaDeA could be improved.

### 1.1 Motivation

We have been teaching a bachelor logic course — with logic programming — for a decade using a textbook with emphasis on tableaux and resolution [1]. We have started to use the proof assistant Isabelle [2] and refutation proofs are less preferable here. The proof system of natural deduction [3, 4, 5, 15] with the introduction and elimination rules as well as a discharge mechanism seems more suitable. The natural deduction proof system is widely known, used and studied among logicians throughout the world. However, our experience shows that many of our undergraduate computer science students struggle to understand the most difficult aspects.

This also goes for other proof systems. The formal language of logic can be hard to teach our students because they do not have a strong theoretical mathematical background. Instead, most of the students have a good understanding of concrete computer code in a programming language. The syntax used in Isabelle is in many ways similar to a programming



© Jørgen Villadsen, Alexander Birch Jensen & Anders Schlichtkrull;  
licensed under Creative Commons License CC-BY  
4th International Conference on Tools for Teaching Logic.  
Editors: M. Antonia Huertas, João Marcos, María Manzano, Sophie Pinchinat,  
François Schwarzentruber; pp. 253–262



Université de Rennes 1

LIPICIS Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)



language, and therefore a clear and explicit formalization of first-order logic and a proof system may help the students in understanding important details. Formalizations of model theory and proof theory of first-order logic are rare, for example [6, 7, 11].

## 1.2 The Tool

We present the natural deduction assistant NaDeA with a formalization in the proof assistant Isabelle of its proof system. It can be used directly in a browser without any further installation and is available here:

<http://nadea.compute.dtu.dk/>

NaDeA is open source software developed in TypeScript / JavaScript and stored on GitHub. The formalization of its proof system in Isabelle is available here:

<http://logic-tools.github.io/>

Once NaDeA is loaded in the browser — about 250 KB with the jQuery Core library — no internet connection is required. Therefore NaDeA can also be stored locally.

We display the natural deduction proofs in two different formats. We present the proof in an explicit code format that is equivalent to the Isabelle syntax, but with a few syntactic differences to make it easier to understand for someone trying to learn Isabelle. In this format, we present the proof in a style very similar to that of Fitch’s diagram proofs. We avoid the seemingly popular Gentzen’s tree style to focus less on a visually pleasing graphical representation that is presumably much more challenging to implement.

We find that the following requirements constitute the key ideals for any natural deduction assistant. It should be:

- Easy to use.
- Clear and explicit in every detail of the proof.
- Based on a formalization that can be proved at least sound, but preferably also complete.

Based on this, we saw an opportunity to develop NaDeA which offers help for new users, but also serves to present an approach that is relevant to the advanced users.

In a paper considering the tools developed for teaching logic over the last decade [14, p. 137], the following is said about assistants (not proof assistants like Isabelle but tools for learning/teaching logic):

Assistants are characterized by a higher degree of interactivity with the user. They provide menus and dialogues to the user for interaction purposes. This kind of tool gives the students the feeling that they are being helped in building the solution. They provide error messages and hints in the guidance to the construction of the answer. Many of them usually offer construction of solution in natural deduction proofs. [...] They are usually free licensed and of open access.

We think that this characterization in many ways fits NaDeA. While NaDeA might not bring something new to the table in the form of delicate graphical features, we emphasize the fact that it has some rather unique features such as a formalization of its proof system in Isabelle.

## 2 Natural Deduction in a Textbook

We consider natural deduction as presented in a popular textbook on logic in computer science [15]. First, we take a look substitution, which is central to the treatment of quantifiers in natural deduction.

### 2.1 On Substitution

The following definition for substitution is used in [15, p. 105 top]:

Given a variable  $x$ , a term  $t$  and a formula  $\phi$  we define  $\phi[t/x]$  to be the formula obtained by replacing each free occurrence of variable  $x$  in  $\phi$  with  $t$ .

The usual side conditions that come with rules using this substitution seem to be omitted. In [15, p. 106 top], we are shortly after given the following definition of what it means that ' $t$  must be free for  $x$  in  $\phi$ ':

Given a term  $t$ , a variable  $x$  and a formula  $\phi$ , we say that  $t$  is free for  $x$  in  $\phi$  if no free  $x$  leaf in  $\phi$  occurs in the scope of  $\forall y$  or  $\exists y$  for any variable  $y$  occurring in  $t$ .

The following quote [15, p. 106 bottom] from the same book emphasizes how it seems more preferable, due to the high level of complexity, to avoid the details of these important side conditions:

It might be helpful to compare ' $t$  is free for  $x$  in  $\phi$ ' with a precondition of calling a procedure for substitution. If you are asked to compute  $\phi[t/x]$  in your exercises or exams, then that is what you should do; but any reasonable implementation of substitution used in a theorem prover would have to check whether  $t$  is free for  $x$  in  $\phi$  and, if not, rename some variables with fresh ones to avoid the undesirable capture of variables.

We find that this way of presenting natural deduction proof systems leaves out some important notions that the students ought to learn. In our formalization such notions and their complications become easier to explain because all side conditions of the rules are very explicitly stated. We see it as one of the major advantages of presenting this formalization to students.

### 2.2 Natural Deduction Rules

We now present the natural deduction rules as described in the literature, again using [15]. The first 9 are rules for classical propositional logic and the last 4 are for first-order logic. Intuitionistic logic can be obtained by omitting the rule *PBC* (proof by contradiction, called "Boole" later) and adding the  $\perp$ -elimination rule (also known as the rule of explosion) [16]. The rules are as follows:

$$\begin{array}{c}
 \boxed{\begin{array}{c} \neg\phi \\ \vdots \\ \perp \end{array}} \\
 \hline
 \phi
 \end{array}
 \text{ PBC}
 \qquad
 \frac{\phi \quad \phi \rightarrow \psi}{\psi} \rightarrow E
 \qquad
 \frac{\boxed{\begin{array}{c} \phi \\ \vdots \\ \psi \end{array}}}{\phi \rightarrow \psi} \rightarrow I$$
  

$$\frac{\phi \vee \psi \quad \boxed{\begin{array}{c} \phi \\ \vdots \\ \chi \end{array}} \quad \boxed{\begin{array}{c} \psi \\ \vdots \\ \chi \end{array}}}{\chi} \vee E
 \qquad
 \frac{\phi}{\phi \vee \psi} \vee I_1
 \qquad
 \frac{\psi}{\phi \vee \psi} \vee I_2$$

$$\begin{array}{c}
\frac{\phi \wedge \psi}{\phi} \wedge E_1 \qquad \frac{\phi \wedge \psi}{\psi} \wedge E_2 \qquad \frac{\phi \quad \psi}{\phi \wedge \psi} \wedge I \\
\\
\frac{\exists x \phi \quad \boxed{\begin{array}{c} x_0 \quad \phi[x_0/x] \\ \vdots \\ \chi \end{array}}}{\chi} \exists E \qquad \frac{\phi[t/x]}{\exists x \phi} \exists I \\
\\
\frac{\forall x \phi}{\phi[t/x]} \forall E \qquad \frac{\boxed{\begin{array}{c} x_0 \\ \vdots \\ \phi[x_0/x] \end{array}}}{\forall x \phi} \forall I
\end{array}$$

Side conditions to rules for quantifiers:

$\exists E$ :  $x_0$  cannot occur outside its box (and therefore not in  $\chi$ ).

$\exists I$ :  $t$  must be free for  $x$  in  $\phi$ .

$\forall E$ :  $t$  must be free for  $x$  in  $\phi$ .

$\forall I$ :  $x_0$  is a new variable which does not occur outside its box.

In addition there is a special copy rule [15, p. 20]:

A final rule is required in order to allow us to conclude a box with a formula which has already appeared earlier in the proof. [...] The rule ‘copy’ allows us to repeat something that we know already. We need to do this in this example, because the rule  $\rightarrow I$  requires that we end the inner box with  $p$ . The copy rule entitles us to copy formulas that appeared before, unless they depend on temporary assumptions whose box has already been closed. Though a little inelegant, this additional rule is a small price to pay for the freedom of being able to use premises, or any other ‘visible’ formulas, more than once.

The copy rule is not needed in our formalization due to the way it manages assumptions.

As it can be seen, there are no rules for truth, negation or biimplication, but the following equivalences can be used:

$$\begin{array}{l}
\top \equiv \perp \rightarrow \perp \\
\neg A \equiv A \rightarrow \perp \\
A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)
\end{array}$$

The symbols  $A$  and  $B$  are arbitrary formulas.

### 3 Natural Deduction in NaDeA

One of the unique features of NaDeA is that it comes with a formalization in Isabelle of its proof system.

### 3.1 Syntax for Terms and Formulas

The terms and formulas of the first-order logic language are defined as the data types `term` and `formula` (later abbreviated `tm` and `fm`, respectively). The type `identifier` represents predicate and function symbols (later abbreviated `id`).

`identifier` := string

`term` := Var nat | Fun identifier [term, ..., term]

`formula` := Falsity | Pre identifier [term, ..., term] | Imp formula formula |

Dis formula formula | Con formula formula | Exi formula | Uni formula

Truth, negation and biimplication are abbreviations. In the syntax of our formalization, we refer to variables by use of the de Bruijn indices. That is, instead of identifying a variable by use of a name, usually  $x, y, z$  etc., each variable has an index that determines its scope. The use of de Bruijn indices instead of named variables allows for a simple definition of substitution. Furthermore, it also serves the purpose of teaching the students about de Bruijn indices. Note that we are not advocating that de Bruijn indices replace the standard treatment of variables in general. It arguably makes complex formulas harder to read, but the pedagogical advance is that the notion of scope is exercised.

### 3.2 Natural Deduction Rules

Provability in NaDeA is defined inductively as follows:

$$\begin{array}{c}
 \frac{\text{member } p \ a}{\text{OK } p \ a} \text{ Assume} \qquad \frac{\text{OK Falsity } ((\text{Imp } p \ \text{Falsity}) \ \# \ a)}{\text{OK } p \ a} \text{ Boole} \\
 \\
 \frac{\text{OK } (\text{Imp } p \ q) \ a \quad \text{OK } p \ a}{\text{OK } q \ a} \text{ Imp\_E} \qquad \frac{\text{OK } q \ (p \ \# \ a)}{\text{OK } (\text{Imp } p \ q) \ a} \text{ Imp\_I} \\
 \\
 \frac{\text{OK } (\text{Dis } p \ q) \ a \quad \text{OK } r \ (p \ \# \ a) \quad \text{OK } r \ (q \ \# \ a)}{\text{OK } r \ a} \text{ Dis\_E} \\
 \\
 \frac{\text{OK } p \ a}{\text{OK } (\text{Dis } p \ q) \ a} \text{ Dis\_I1} \qquad \frac{\text{OK } q \ a}{\text{OK } (\text{Dis } p \ q) \ a} \text{ Dis\_I2} \\
 \\
 \frac{\text{OK } (\text{Con } p \ q) \ a}{\text{OK } p \ a} \text{ Con\_E1} \qquad \frac{\text{OK } (\text{Con } p \ q) \ a}{\text{OK } q \ a} \text{ Con\_E2} \qquad \frac{\text{OK } p \ a \quad \text{OK } q \ a}{\text{OK } (\text{Con } p \ q) \ a} \text{ Con\_I} \\
 \\
 \frac{\text{OK } (\text{Exi } p) \ a \quad \text{OK } q \ ((\text{sub } 0 \ (\text{Fun } c \ [])) \ p) \ \# \ a \quad \text{news } c \ (p \ \# \ q \ \# \ a)}{\text{OK } q \ a} \text{ Exi\_E} \\
 \\
 \frac{\text{OK } (\text{sub } 0 \ t \ p) \ a}{\text{OK } (\text{Exi } p) \ a} \text{ Exi\_I} \\
 \\
 \frac{\text{OK } (\text{Uni } p)}{\text{OK } (\text{sub } 0 \ t \ p) \ a} \text{ Uni\_E} \qquad \frac{\text{OK } (\text{sub } 0 \ (\text{Fun } c \ [])) \ p \ a \quad \text{news } c \ (p \ \# \ a)}{\text{OK } (\text{Uni } p) \ a} \text{ Uni\_I}
 \end{array}$$

$\text{OK } p \ a$  means that the formula  $p$  follows from the list of assumptions  $a$  and member  $p \ a$  means that  $p$  is a member of  $a$ . The operator  $\#$  is between the head and the tail of a list.  $\text{news } c \ l$  checks if the identifier  $c$  does not occur in the any of the formulas in the list  $l$  and  $\text{sub } n \ t \ p$  returns the formula  $p$  where the term  $t$  has been substituted for the variable with the de Bruijn index  $n$ . Instead of writing  $\text{OK } p \ a$  we could also use the syntax  $a \vdash p$ , even in Isabelle, but we prefer a more programming-like approach. In the types we use  $\Rightarrow$  for function spaces. The definitions of member, news and sub are as follow:

```

member :: fm  $\Rightarrow$  fm list  $\Rightarrow$  bool
member p [] = False
member p (q # a) = (if p = q then True else member p a)

new_term :: id  $\Rightarrow$  tm  $\Rightarrow$  bool
new_term c (Var v) = True
new_term c (Fun i l) = (if i = c then False else new_list c l)

new_list :: id  $\Rightarrow$  tm list  $\Rightarrow$  bool
new_list c [] = True
new_list c (t # l) = (if new_term c t then new_list c l else False)

new :: id  $\Rightarrow$  fm  $\Rightarrow$  bool
new c Falsity = True
new c (Pre i l) = new_list c l
new c (Imp p q) = (if new c p then new c q else False)
new c (Dis p q) = (if new c p then new c q else False)
new c (Con p q) = (if new c p then new c q else False)
new c (Exi p) = new c p
new c (Uni p) = new c p

news :: id  $\Rightarrow$  fm list  $\Rightarrow$  bool
news c [] = True
news c (p # a) = (if new c p then news c a else False)

inc_term :: tm  $\Rightarrow$  tm
inc_term (Var v) = Var (v + 1)
inc_term (Fun i l) = Fun i (inc_list l)

inc_list :: tm list  $\Rightarrow$  tm list
inc_list [] = []
inc_list (t # l) = inc_term t # inc_list l

sub_term :: nat  $\Rightarrow$  tm  $\Rightarrow$  tm  $\Rightarrow$  tm
sub_term n s (Var v) = (if v = n then s else if v > n then Var (v - 1) else Var v)
sub_term n s (Fun i l) = Fun i (sub_list n s l)

sub_list :: nat  $\Rightarrow$  tm  $\Rightarrow$  tm list  $\Rightarrow$  tm list
sub_list n s [] = []
sub_list n s (t # l) = sub_term n s t # sub_list n s l

sub :: nat  $\Rightarrow$  tm  $\Rightarrow$  fm  $\Rightarrow$  fm
sub n s Falsity = Falsity
sub n s (Pre i l) = Pre i (sub_list n s l)
sub n s (Imp p q) = Imp (sub n s p) (sub n s q)
sub n s (Dis p q) = Dis (sub n s p) (sub n s q)
sub n s (Con p q) = Con (sub n s p) (sub n s q)
sub n s (Exi p) = Exi (sub (n + 1) (inc_term s) p)
sub n s (Uni p) = Uni (sub (n + 1) (inc_term s) p)

```

### 3.3 Semantics for Terms and Formulas

To give meaning to formulas and to prove NaDeA sound we need a semantics of the first-order logic language. This semantics is defined in the formalization in Isabelle, and it is thus not part of the tool itself. We present the semantics below.  $e$  is the environment, i.e. a mapping of variables to elements.  $f$  maps function symbols to the maps they represent. These maps are from lists of elements of the universe to elements of the universe. Likewise,  $g$  maps predicate symbols to the maps they represent.  $'u$  is a type variable that represents the universe. It can be instantiated with any type. For instance, it can be instantiated with the natural numbers, the real number or strings.

```

semantics_term :: (nat => 'u) => (id => 'u list => 'u) => tm => 'u
semantics_term e f (Var v) = e v
semantics_term e f (Fun i l) = f i (semantics_list e f l)

semantics_list :: (nat => 'u) => (id => 'u list => 'u) => tm list => 'u list
semantics_list e f [] = []
semantics_list e f (t # l) = semantics_term e f t # semantics_list e f l

semantics :: (nat => 'u) => (id => 'u list => 'u) => (id => 'u list => bool) => fm => bool
semantics e f g Falsity = False
semantics e f g (Pre i l) = g i (semantics_list e f l)
semantics e f g (Imp p q) = (if semantics e f g p then semantics e f g q else True)
semantics e f g (Dis p q) = (if semantics e f g p then True else semantics e f g q)
semantics e f g (Con p q) = (if semantics e f g p then semantics e f g q else False)
semantics e f g (Exi p) = (? x. semantics (% n. if n = 0 then x else (n - 1)) f g p)
semantics e f g (Uni p) = (! x. semantics (% n. if n = 0 then x else (n - 1)) f g p)

```

Most of the cases of `semantics` should be self-explanatory, but the `Uni` case is complicated. The details are not important here, but in the case for `Uni` it uses the universal quantifier (`!`) of Isabelle's higher-order logic to consider all values of the universe. It also uses the lambda abstraction operator (`%`) to keep track of the indices of the variables. Likewise, the case for `Exi` uses the existential quantifier (`?`) of Isabelle's higher-order logic.

We have proved soundness of the formalization in Isabelle (shown here as a derived rule):

$$\frac{\text{OK } p \ []}{\text{semantics } e \ f \ g \ p} \text{ Soundness}$$

This result makes NaDeA interesting to a broader audience since it gives confidence in the formulas proved using the tool.

## 4 Construction of a Proof

We now describe the core features of NaDeA from the perspective of the user. That is, we uncover how to use NaDeA to conduct and edit a proof as well as how proofs are presented.

In order to start a proof, you have to start by specifying the goal formula, that is, the formula you wish to prove. To do so, you must enable editing mode by clicking the Edit button in the top menu bar. This will show the underlying proof code and you can build formulas by clicking the red  $\alpha$  symbol. Alternatively, you can load a number of tests by clicking the Load button.

At all times, once you have fully specified the conclusion of any given rule, you can continue the proof by selecting the next rule to apply. Again you can do this by clicking the



the red  $\boxtimes$  symbol. Furthermore, NaDeA allows for undoing and redoing editing steps with no limits.

All proofs are conducted in backward-chaining mode. That is, you must start by specifying the formula that you wish to prove. You then apply the rules inductively until you reach a proof — if you can find one. The proof is finished by automatic application of the **Assume** rule once the conclusion of a rule is found in the list of assumptions.

To start over on a new proof, you can load the blank proof by using the Load button, or you can refresh the page. Please note that any unsaved work will then be gone.

In NaDeA we present any given natural deduction proof (or an attempt at one) in two different types of syntax. One syntax follows the rules as defined in section 3.2 and is closely related to the formalization in Isabelle, but with a redefined and more simple syntax in terms of learning. The proof is not built as most often seen in the literature about natural deduction. Usually, for each rule the premises are placed above its conclusion separated by a line. We instead follow the procedure of placing each premise of the rule on separate lines below its conclusion with an additional level of indentation.

## Natural Deduction Assistant

1	Imp_I	[] $P \wedge (P \rightarrow Q) \rightarrow Q$	
2	Imp_E	[ $P \wedge (P \rightarrow Q)$ ] $Q$	$\frac{\frac{}{p \wedge (p \rightarrow q)}}{p \rightarrow q} \quad (1) \quad \frac{\frac{}{p \wedge (p \rightarrow q)}}{p} \quad (1)}{p \wedge (p \rightarrow q) \rightarrow q} \quad (1)$
3	Con_E2	[ $P \wedge (P \rightarrow Q)$ ] $P \rightarrow Q$	
4	Assume	[ $P \wedge (P \rightarrow Q)$ ] $P \wedge (P \rightarrow Q)$	
5	Con_E1	[ $P \wedge (P \rightarrow Q)$ ] $P$	
6	Assume	[ $P \wedge (P \rightarrow Q)$ ] $P \wedge (P \rightarrow Q)$	

The above proof also can be written in terms of the OK syntax as follows:

1	OK (Imp (Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" []))) (Pre "Q" []) []	Imp_I
2	OK (Pre "Q" []) [(Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" []))]	Imp_E
3	OK (Imp (Pre "P" []) (Pre "Q" [])) [(Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" []))]	Con_E2
4	OK (Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" [])) [(Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" []))]	Assume
5	OK (Pre "P" []) [Con (Pre "P" []) (Imp (Pre "P" []) (Pre "Q" []))]	Con_E1
6	OK (Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" [])) [(Con (Pre "P" [])) (Imp (Pre "P" []) (Pre "Q" []))]	Assume

## 5 Related Work

Throughout the development of NaDeA we have considered some of the natural deduction assistants currently available. Several of the tools available share some common flaws. They can be hard to get started with, or depend on a specific platform. However, there are also many tools that each bring something useful and unique to the table. One of the most prominent is PANDA, described in [13]. PANDA includes a lot of graphical features that make it fast for the experienced user to conduct proofs, and it helps the beginners to tread safely. Another characteristic of PANDA is the possibility to edit proofs partially before combining them into a whole. It definitely serves well to reduce the confusion and complexity involved in conducting large proofs. However, we still believe that the way of presenting the proof

can be more explicit. In NaDeA, every detail is clearly stated as part of the proof code. In that sense, the students should become more aware of the side conditions to rules and how they work.

Another tool that deserves mention is ProofWeb [10] which is open source software for teaching natural deduction. It provides interaction between some proof assistants (Coq, Isabelle, Lego) and a web interface. The tool is highly advanced in its features and uses its own syntax. Also, it gives the user the possibility to display the proof in different formats. However, the advanced features come at the cost of being very complex for undergraduate students and require that you learn a new syntax. It serves as a great tool for anyone familiar with natural deduction that wants to conduct complex proofs that can be verified by the system. It may, on the other hand, prove less useful for teaching natural deduction to beginners since there is no easy way to get started. In NaDeA, you are free to apply any (applicable) rule to a given formula, and thus, beginners have the freedom to play around with the proof system in a safe way. Furthermore, the formalized soundness result for the proof system of NaDeA makes it relevant for a broader audience, since this gives confidence in that the formulas proved with the tool are actually valid.

## 6 Further Work

In NaDeA there is support for proofs in propositional logic as well as first-order logic. We would also like to extend to more complex logic languages, the most natural step being higher-order logic. This could be achieved using the CakeML approach [8]. Other branches of logic would also be interesting, and the possibilities are numerous. Apart from just extending the natural deduction proof system to support other types of logic, another option is to implement other proof systems as well.

Because the NaDeA tool has a formalization in Isabelle of its proof system, we would like to provide features that allow for a direct integration with Isabelle. For instance, we would like to allow for proofs to be exported to an Isabelle format that could verify the correctness of the proofs. A formal verification of the implementation would require much effort, but perhaps it could be reimplemented on top of Isabelle (although probably not in TypeScript / JavaScript).

We would like to extend NaDeA with more features in order to help the user in conducting proofs and in understanding logic. For example, the tool could be extended with step-by-step execution of the auxiliary primitive recursive functions used in the side conditions of the natural deduction rules.

So far only a small group of computer science students have tested NaDeA, but it will be classroom tested with around 60 bachelor students in the next semester. Currently the tool has no support for student assignments and automatic feedback and/or grading. The tool could be extended such that the students are evaluated and perhaps given a score based on the proofs they conduct. It is not obvious how this could best be implemented. We hope to find the resources for the development of such features but already now we think that the tool has the potential to be one of the main ways to teach logic in mathematics and computer science.

**Acknowledgements** We would like to thank Stefan Berghofer for discussions about the formalization of natural deduction in Isabelle. We would also like to thank Andreas Halkjær From and Andreas Viktor Hess for comments on the paper.

---

**References**

---

- 1 Mordechai Ben-Ari. *Mathematical Logic for Computer Science*. Third Edition. Springer 2012.
- 2 Tobias Nipkow, Lawrence C. Paulson and Markus Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*. Lecture Notes in Computer Science 2283, Springer 2002.
- 3 Dag Prawitz. *Natural Deduction. A Proof-Theoretic Study*. Stockholm: Almqvist & Wiksell 1965.
- 4 Francis Jeffrey Pelletier. *A Brief History of Natural Deduction*. *History and Philosophy of Logic*, 1-31, 1999.
- 5 Melvin Fitting. *First-Order Logic and Automated Theorem Proving*. Second Edition Springer 1996.
- 6 John Harrison. *Formalizing Basic First Order Model Theory*. Lecture Notes in Computer Science 1497, 153–170, Springer 1998.
- 7 Stefan Berghofer. *First-Order Logic According to Fitting*. *Formal Proof Development*. Archive of Formal Proofs 2007.
- 8 Ramana Kumar, Rob Arthan, Magnus O. Myreen and Scott Owens. *HOL with Definitions: Semantics, Soundness, and a Verified Implementation*. Lecture Notes in Computer Science 8558, 308–324, Springer 2014.
- 9 Jørgen Villadsen, Anders Schlichtkrull and Andreas Viktor Hess. *Meta-Logical Reasoning in Higher-Order Logic*. Accepted at 29th International Symposium Logica, Hejnice Monastery, Czech Republic, 15-19 June 2015.
- 10 ProofWeb. Online <http://proofweb.cs.ru.nl/login.php> (ProofWeb is both a system for teaching logic and for using proof assistants through the web). Accessed April 2015.
- 11 Jasmin Christian Blanchette, Andrei Popescu and Dmitriy Traytel. *Unified Classical Logic Completeness - A Coinductive Pearl*. Lecture Notes in Computer Science 8562, 46–60, 2014.
- 12 Krysia Broda, Jiefei Ma, Gabrielle Sinnadurai and Alexander Summers. *Pandora: A Reasoning Toolbox Using Natural Deduction Style*. *Logic Journal of IGPL*, 15(4):293–304, 2007.
- 13 Olivier Gasquet, François Schwarzentruher and Martin Strecker. *Panda: A Proof Assistant in Natural Deduction for All. A Gentzen Style Proof Assistant for Undergraduate Students*. Lecture Notes in Computer Science 6680, 85–92. Springer 2011.
- 14 Antonia Huertas. *Ten Years of Computer-Based Tutors for Teaching Logic 2000-2010: Lessons learned*. Lecture Notes in Computer Science 6680, 131–140, Springer 2011.
- 15 Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and Reasoning About Systems*. Second Edition. Cambridge University Press 2004.
- 16 Jonathan P. Seldin. *Normalization and Excluded Middle. I*. *Studia Logica*, 48(2):193–217, 1989.