Department of Computing

Phometa — a visualised proof assistant that build a formal system and prove its theorems using derivation trees

Author:
Gun Pinyo

Supervisor:
Dr. Krysia Broda

Second Marker:
Prof. Alessio R. Lomuscio

May 29, 2016

Submitted in part of fulfilment of the requirements
for the master of engineering

Abstract

Manually drawing a derivation tree usually takes many iterations to be completed due to its layout (its width grows exponentially to its height) and variables being rewrite (by unification when derivation rule is applied). Even when the tree is completed, there are nothing to guarantee that the tree is error free.

Therefore, I decided to create *Phometa* which is a proof assistant that allows user to create a formal system and prove its theorems using derivation trees. Fundamentally, phometa consists of three kinds of node which are *Grammar* (Backus-Naur Form), *Rule* (derivation rule), and *Theorem* (derivation tree).

It can be used as educational platform for students to learn curtain formal systems provided in standard library. Alternatively, it also can be used as experimental sandbox where user implements their own formal system and try to reason about it.

Phometa is a web application so components such as terms and derivation trees can be render nicely in web browser and users can interact with these components directly by clicking button or pressing keyboard shortcut. Visualisation also allows Phometa to have curtain features that text-based proof assistants couldn't have, for example, nested underlines can be used to group terms instead of brackets, input method of terms can be controlled in such a way that ill-from terms couldn't be created, and so on.

As the result of this project, Phometa has been designed and been implemented in such a way that it is powerful enough to completely replace derivation-tree's manually-drawing, and easy enough to be used by anyone. Its standard library also include famous formal systems such as *Simple Arithmetic*, *Propositional Logic*, and *Typed Lambda Calculus*. This shows that Phometa is generic enough to handle most of formal systems out there.

Acknowledgements

First and most importantly, I would like to thank my supervisor, Dr Krysia Broda, for her constant dedication to supporting me on both project skill and mental advise.

I also would like to thank my second marker, Prof. Alessio R. Lomuscio, for his invaluable advice on interim report.

I also would like to thank many of Imperial's computing students, for their feedback on my project.

I also would like to thank Evan Czaplicki and the rest of Elm community, for their ambition and effort to develop Elm — a wonderful front-end functional reactive language that Phometa is built on top of.

And finally, I also would like to thank my parents for their unconditional love and continuous support on everything since I was born.

Contents

Chapter 1

Introduction

1.1 Motivation

Proofs are very important to all kinds of Mathematics because they ensure the correctness of theorems. However, it is hard to verify the correctness of a proof itself especially for a complex proof. To tackle this problem, we can prove a theorem on a *proof assistant*, aka *interactive theorem prover*, which provides a rigorous method to construct a proof such that an invalid proof will never occur. Therefore if we manage to complete a proof, it is guaranteed that the proof is valid.

There are many powerful and famous proof assistants such as Coq[9], Agda[4], and Isabelle[3] which are suitable for extreme use case of complex proofs. Nevertheless, they have a steep learning curve and have specific meta-theory behind it, for example, Coq has Calculus of Inductive Construction (CIC), Agda has Unified Theory of Dependent Types[12][11] which are quite hard for newcomers. To solve this problem they should start with something easier than these and come back again later.

One of the easiest starting point to learn about formal proof is to use derivation trees where validity of a term is derived from a derivation rule together with validity of zero or more terms depending on the rule. These prerequisite terms can be proven similarly to the main term. The proving process will happen recursively, this lead to tree-like structure of the final proof, this is why it is called "derivation tree".

The naive way to construct such a derivation tree is to draw it on a paper, however, this has many disadvantages such as

- The width of a derivation tree usually grow exponentially to its height — hard to arrange the layout on a paper.
- We don't know that how much space that each branch requires — need to recreate the tree for many iterations.

- Variables might need to be rewritten by other terms as a result of internal unification when applying a rule — again, need to recreate the tree for many iterations.
- When a derivation tree is completed, there is nothing to guarantee that it doesn't have any errors — conflict with the ambition to use proof assistant at the first place.

So I decided to create a proof assistants called *Phometa* to solve this derivation-tree manually-drawing problem. To be precise, Phometa is proof assistant that allows user to create a formal system and prove theorems using derivation trees.

Phometa fundamentally consists of three kinds[1] of node as the following

- *Grammar* (or Backus-Naur Form) — How to construct a well-form term.
  For example, a simple arithmetic expression can be constructed by a number *or* two expressions adding together *or* two expressions multiply together.
- *Rule* (or derivation rule) — A reason that can be used to prove validity of terms. For example, $(u + v) = (x + y)$ is valid if $u = x$ and $v = y$.
- *Theorem* (or derivation tree) — An evidence (proof) showing that a particular term is valid. For example,

  $((3 + 4) \times 5) = ((4 + 3) \times 5)$ is valid by rule ADD-INTRO and

  $(3 + 4) = (4 + 3)$ is valid by rule ADD-COMM

  $5 = 5$ is valid by rule EQ-REFL

A formal system will be represented by a set of grammars and rules. Validity of terms will be represented by theorems (derivation trees).

In term of usage, users can Phometa by either

- Learn one of many existing formal systems provided in Phometa's standard library and try to proof some theorem regarding to that formal system.
- Create their own formal system or extend an existing formal system, then do some experiments about it.

In order to make Phometa easy to use, it is designed to be web-based application. Users will interact with Phometa mainly by clicking buttons and pressing keyboard-shortcut. This has advantages over traditional proof assistant because it is easier to read, ill-from terms never occur, and guarantee that the entire system is always in consistent state.

[1]There exists the fourth kind of node which are comment node but I don't include it there since it is not relevant to the fundamental concept.

1.2 Objectives

- To make a construction of derivation tree become more systematic. Hence, users become more productive and have less chance to make an error.
- To encourage users to create their own formal systems and reason about it.
- To show that most of formal systems have a similar meta-structure which can be implemented using common framework.
- To show advantages of visualised proof assistant over traditional one.

1.3 Achievement

- Finished designing Phometa specification in such a way to keep it simple yet be able to produce a complex proof.
- Finished implementing Phometa. All of basic functionality is working.
- Encoded several formal systems such as Simple Arithmetic, Propositional Logic, and Typed Lambda Calculus as standard library in Phometa.
- Wrote a tutorial for newcomers to use Phometa (chapters 3, 4, 5, and 6).

Chapter 2

Related Work

There are many proof assistants available out there, each of them rely on slightly different meta-theory. We can separate proof assistants into 2 categories as the following

2.1 Text-Base Proof Assistants

Text-base proof assistants are similar to programming language where user writes everything in text-files and compile it, if the compilation is successful, then the proofs are correct. User can freely manipulate these text-files, hence, easier to write a complex proof. In addition, most of proof assistants have a plug-in to mainstream text editor, so user can use their favourite text editor with full performance.

There are several mainstream text-base proof assistants that worth mentioning

2.1.1 Coq

Coq[9] is one the most famous proof assistants. It is based on the Calculus of Inductive Constructions (CIC)[1] developed by Thierry Coquand[5].

Coq has customisable tactics which are commands that transform goal into smaller-sub goal (if any), this makes proving process become faster compared to other proof assistants. In contrast, tactics reduce readability, reader might need to replay each tactic step by step in order to understand a proof completely.

Coq is very mature, it has been developed since 1984. Hence, it is reliable and has lots of libraries supported.

[1] **CIC is itself is developed alongside Coq.**.

In term of editor, most people use Proof General[6] which is a plugin on Emacs[2]. Nevertheless, Coq has its own editor called CoqIde[10] that newcomers can use without learning Emacs.

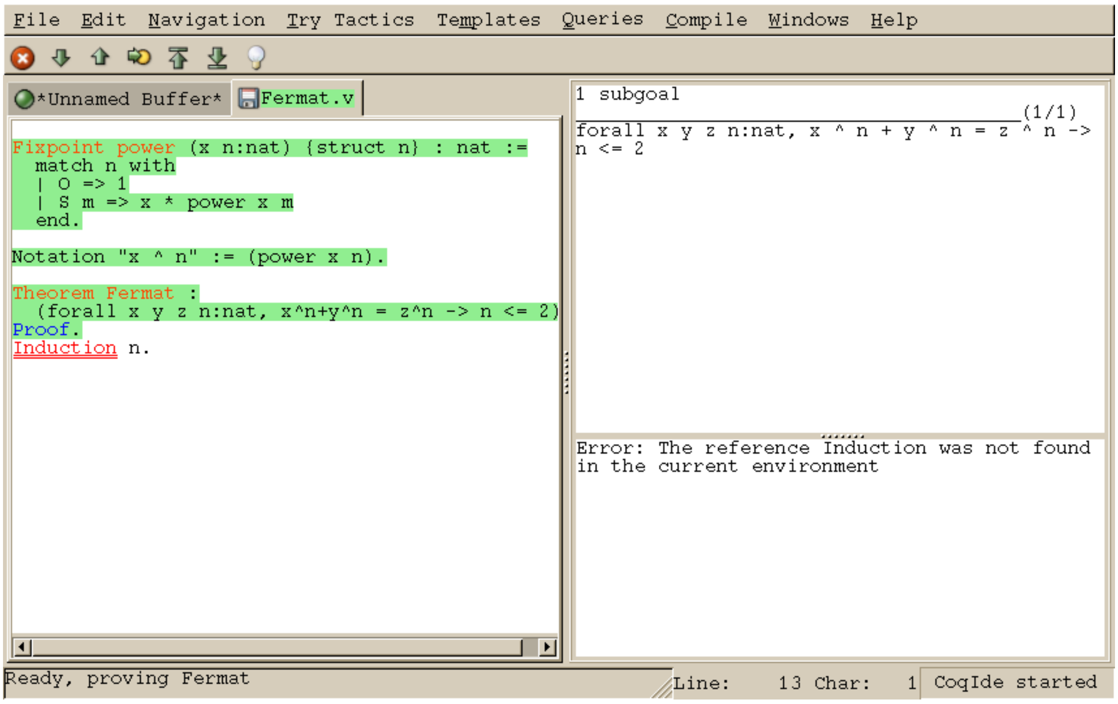


Figure 2.1: Screenshot of Coq (using CoqIde) — The left pane is file content and Upper right pane is the current goal which is changed depending on where the cursor point on file content.

2.1.2 Agda

Adga[4] is (dependently typed) functional programming which can be seen as a proof assistant as well. It is based on Unified Theory of Dependent Types[12][11] similar to Martin Lof Type Theory.

Its proving technique is relies on Curry-Howard correspondence which state that there is duality between computer programs and mathematical proofs[13], for example function corresponded to implication, product type corresponded to logical implication.

Agda is suitable for reasoning about functional programs because we can write a program and prove that curtain properties of a function hold using the same language. This is feasible since a proof is just a function due to Curry-Howard correspondence.

[2]Proof General also other proof assistants such as Isabelle and PhoX

Agda has less steep learning curve compared other proof assistants such as Coq. This is because user doesn't need to learn about proving system since it is the same as programming. In contrast, it doesn't have fancy tactic system so proving process is slower.

In term of popularity, it is less popular than Coq, however, some project such as Homotopy Type Theory[7][8] use Agda as alternative experiments to Coq.

In term of editor, Agda as its own plugin for Emacs which is very nice but user need to be familiar to Emacs before using it. There is no alternative plugin to other editor.

```
open import Data.Nat

ex₁ : ℕ
ex₁ = 1 + 3

open import Relation.Binary.PropositionalEquality

ex₂ : 3 + 5 ≡ 2 * 4
ex₂ = refl

open import Algebra
import Data.Nat.Properties as Nat
private
  module CS = CommutativeSemiring Nat.commutativeSemiring

ex₃ : ∀ m n → m * n ≡ n * m
ex₃ m n = CS.*-comm m n

open ≡-Reasoning
open import Data.Product

ex₄ : ∀ m n → m * (n + 0) ≡ n * m
ex₄ m n = begin
  m * (n + 0)  ≡⟨ cong (_*_ m) (proj₂ CS.+-identity n) ⟩
  m * n        ≡⟨ CS.*-comm m n ⟩
  n * m        ∎

open Nat.SemiringSolver

ex₅ : ∀ m n → m * (n + 0) ≡ n * m
ex₅ = solve 2 (λ m n → m :* (n :+ con 0)  :=  n :* m) refl
```

Figure 2.2: Screenshot of Agda — Credit: an example in Agda standard library, removing comment out to save space.

2.1.3 Isabelle

Isabelle[3] is generic proof assistant.

talk about isabelle readability

2.1.4 Lean

Lean**lean-offical-website** is a relatively new theorem prover[3]

[3]The Lean project was launched by Leonardo de Moura at Microsoft Research in 2013

2.2 Visualised Proof Assistant

TODO:

2.2.1 Logitext

http://logitext.mit.edu/tutorial

2.2.2 Panda

https://www.irit.fr/panda/

2.2.3 Pandora

http://www.doc.ic.ac.uk/pandora/newpandora/

2.2.4 PeaCoq

http://goto.ucsd.edu/peacoq/

2.2.5 Why3

http://why3.lri.fr/

Chapter 3

Background

In this chapter, we will go thought some required materials needed for later chapters. These can be linked together by an example of Simple Arithmetic explained below.

3.1 Formal System

A formal system is any well-defined system of abstract thought based on mathematical model[14]. Each formal system has a formal language composed of primitive symbols[1] acted by certain formation[2].

Informally, is an abstract system that has precise structures and can be reasoned about. For example, numbers (base 10) and their arithmetic (using $+$ and $\times$) could form a formal system. This is because every term (e.g. 5, $(3+1)$, (3×4)) has explicit structure and we can argue something like "*does* 12 *equal to* (3×4)" or "*for any integers a and b, $(a+b)$ is equal to $(b+a)$*".

3.2 Backus-Naur Form

Backus-Naur Form (BNF) is a way to construct a term, for example, grammars of formal system above can be defined as the following

[1] Phometa will assume that primitive symbols are any Unicode character.

```
<Digit>   ::= '0' | '1' | '2' | '3' | '4' | '5' | '6' | '7' | '8' | '9'

<Number> ::= <Digit> | <Number> <Digit>

<Expr>    ::= <Number>
            | '('<Expr> '+' <Expr>')'
            | '('<Expr> '×' <Expr>')'

<Equation> ::= <Expr> '=' <Expr>
```

Figure 3.1: Backus-Naur Form of Simple Arithmetic

- A term of `<Digit>` can be either 0 or 1 or 2 or . . . or 9 and nothing else.

2 is `<Digit>` (3^{rd} choice)

Figure 3.2: This diagram explains that why 2 is a term of `<Digit>`

- A term of `<Number>` can be either
  - `<Digit>`
  - another `<Number>` concatenate with `<Digit>`

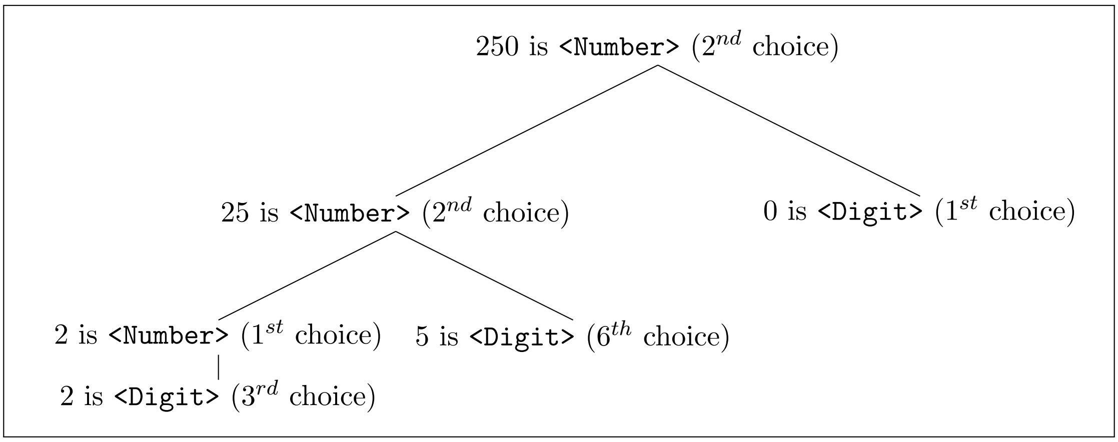


Figure 3.3: This diagram explains that why 250 is a term of `<Number>`

- A term of <Expr> can be either
  - <Number>
  - other two <Expr>s concatenate using '(' '+' ')'
  - other two <Expr>s concatenate using '(' '×' ')'

  Please note that we need brackets around '+' and '×' to avoid ambiguity. If we don't have these brackets, $3 + 4 + 5$ could be interpreted as either $(3 + 4) + 5$ or $3 + (4 + 5)$ which is not precise. Moreover, $12 + 0 \times 6$ will be interpreted as $12 + (0 \times 6)$ due to priority of $\times$ over $+$ and it is impossible to encode some thing like $(12 + 0) \times 6$.

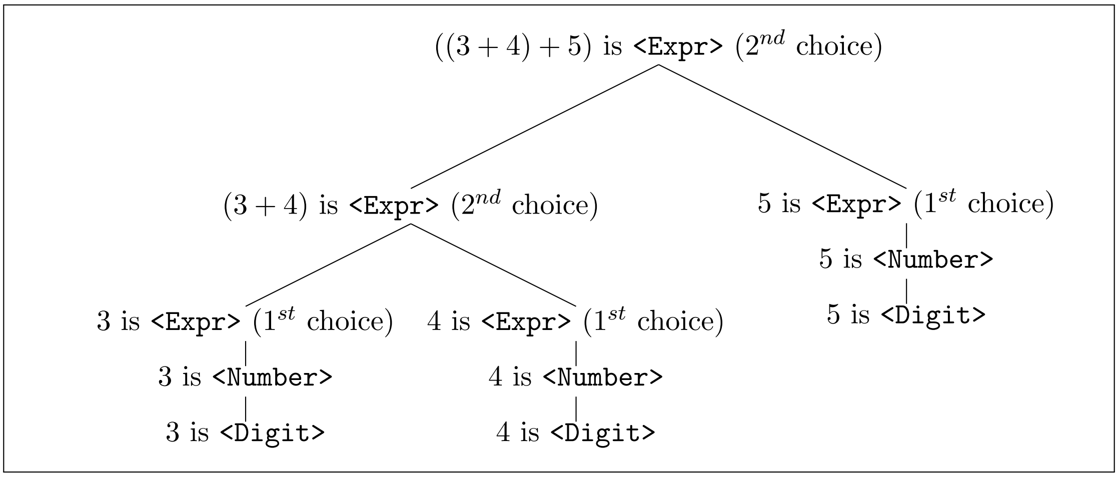


Figure 3.4: This diagram explains that why $((3 + 4) + 5)$ is a term of <Expr>

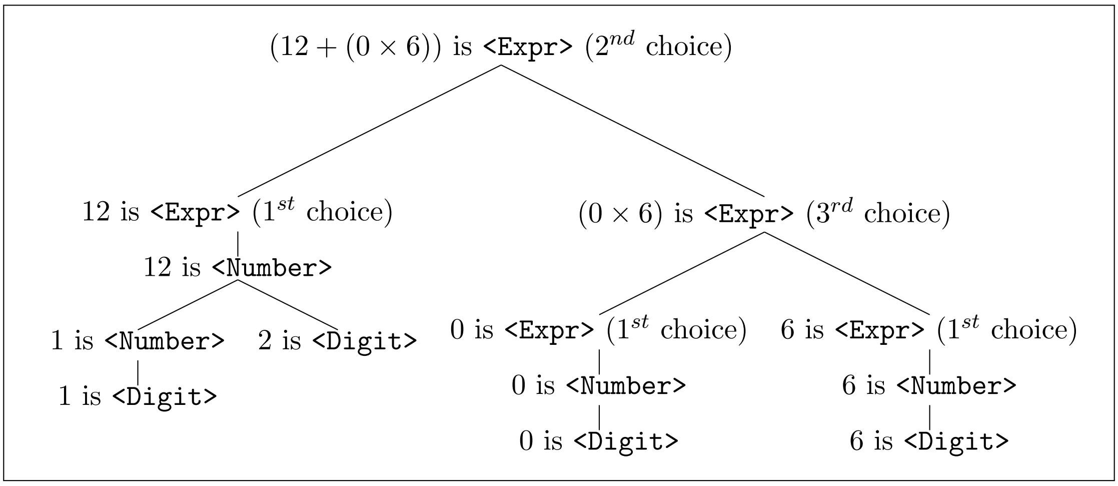


Figure 3.5: This diagram explains that why $(12 + (0 \times 6))$ is a term of <Expr>

- A term of <Equation> can be only two <Expr>s concatenate using ‘=’

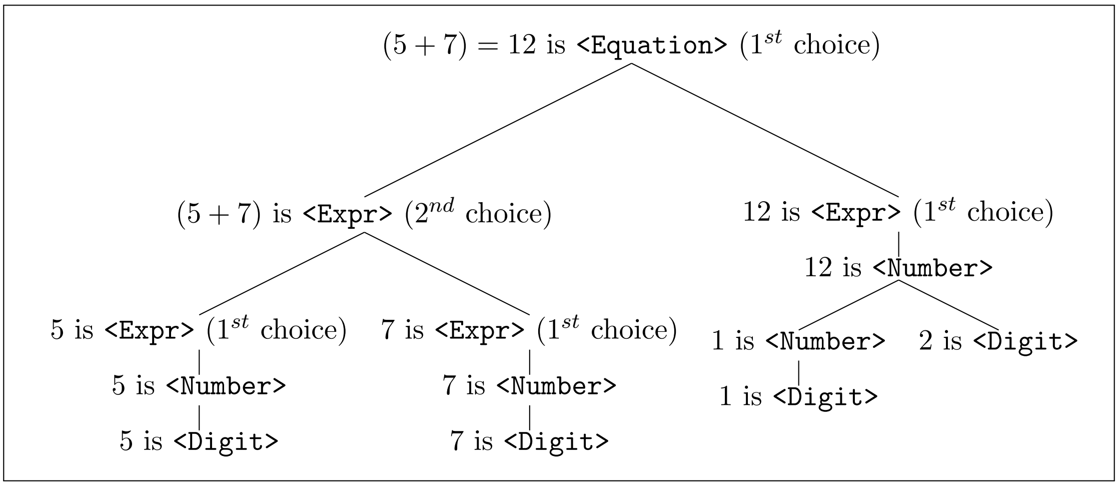


Figure 3.6: This diagram explains that why $(5 + 7) = 12$ is a term of <Equation>

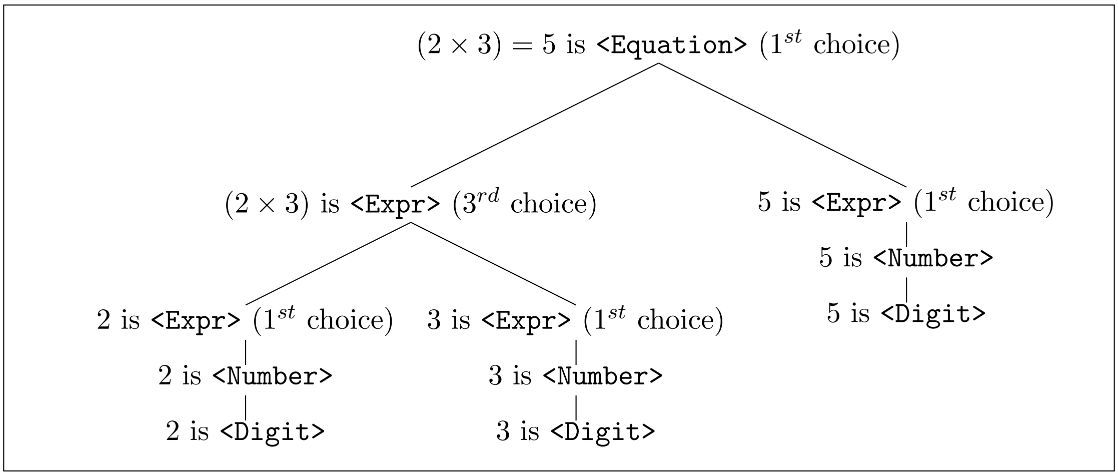


Figure 3.7: This diagram explains that why $(2 \times 3) = 5$ is a term of <Equation>. Please note that this construction is purely syntactic so wrong equation is acceptable.

3.3 Meta Variables and Pattern Matching

Meta variables are arbitrary sub-terms embedded inside root term. For example, an <Expr> $(x + y)$ represents two arbitrary <Expr> joined by ‘+’.

But if we have an `<Equation>` $(x + 7) = 12$, shouldn't x be an unknown variable that needed to be solve rather than being arbitrary `<Expr>`? Well, x still represents arbitrary `<Expr>` but in order make this equation hold, x must be 5. Hence "*variable needed to be solve*" is just spacial form of "*variable as arbitrary term*".

Meta variables help us to represents statement in more general manner. For example, "*the same expressions plus together is the same as 2 times that expression*" could be represented by $(x + x) = (2 \times x)$ rather than $(0 + 0) = (2 \times 0)$ and $(1 + 1) = (2 \times 1)$ and $(2 + 2) = (2 \times 2)$ and so on.

But if we know that $(x+x) = (2\times x)$, how could we derive its instance e.g. $(1+1) = (2\times 1)$ or even $(y \times z) + (y \times z) = (2 \times (y \times z))$? The solution for this is to use *Pattern Matching* which is algorithm that try to substitute pattern's meta variables into more specific form, in order to make pattern identical to target, for example

- $(x + x) = (2 \times x)$ is pattern matchable with $(1 + 1) = (2 \times 1)$ by substitute x with1
- $(x + x) = (2 \times x)$ is pattern matchable with $(y \times z) + (y \times z) = (2 \times (y \times z))$ by substitute x with $(y \times z)$
- $(x + x) = (2 \times x)$ is *not* pattern matchable with $(1 + 1) = 2$, if we try to substitute x with 1 we would get $(1 + 1) = (2 \times 1)$ which is not identical to $(1 + 1) = 2$
- $(1 + 1) = (2 \times 1)$ is *not* pattern matchable with $(x + x) = (2 \times x)$, because pattern $(1 + 1) = (2 \times 1)$ doesn't have any meta variable and it is not identical to $(x + x) = (2 \times x)$. This show that pattern matching doesn't generally holds in opposite direction
- $(x + x) = (2 \times x)$ is pattern matchable to itself by substitute x with x

If pattern matching is successful then the target is instance of the pattern.

3.4 Derivation of Formal Systems

So far, we construct any term based on Backus-Naur Form, this doesn't prevent invalid term, for example, $(2 \times 3) = 5$ is perfectly a term of `<Equation>`. Thus, we need some mechanism to verify a term i.e. *prove* that the particular term holds. One way to deal with this is to use derivation system, first, we have a set of derivation rules that has format as the following

$$\textsc{rule-name}\ \frac{Premise_1 \qquad Premise_2 \qquad Premise_3 \qquad \ldots \qquad Premise_n}{Conclusion}$$

Figure 3.8: Structure of derivation rule.

This say that if we know that $Premise_1$ and $Premise_2$ and $Premise_3$ and ... and $Premise_n$ hold then $Conclusion$ holds. In another word, if we want to prove $Conclusion$ then we can use this derivation rule then proof its premises.

Derivation rules of current example formal system could be shown as the following

$$\textsc{eq-refl}\ \frac{}{x = x} \qquad \textsc{eq-symm}\ \frac{y = x}{x = y} \qquad \textsc{eq-tran}\ \frac{x = z \qquad z = y}{x = y}$$

$$\textsc{add-intro}\ \frac{u = x \qquad v = y}{(u + v) = (x + y)} \qquad \textsc{mult-intro}\ \frac{u = x \qquad v = y}{(u \times v) = (x \times y)}$$

$$\textsc{add-assoc}\ \frac{}{((x + y) + z) = (x + (y + z))} \qquad \textsc{mult-assoc}\ \frac{}{((x \times y) \times z) = (x \times (y \times z))}$$

$$\textsc{add-comm}\ \frac{}{(x + y) = (y + x)} \qquad \textsc{mult-comm}\ \frac{}{(x \times y) = (y \times x)}$$

$$\textsc{dist-left}\ \frac{}{(x \times (y + z)) = ((x \times y) + (x \times z))} \qquad \textsc{dist-right}\ \frac{}{((x + y) \times z) = ((x \times z) + (y \times z))}$$

Figure 3.9: Derivation rules of Simple Arithmetic (not exhaustive, due to limited space).

In order to use a derivation rule, first the conclusion of the rule is pattern match against current goal, if it is pattern matchable then meta variables in premises are substituted respect to the pattern matching (if some meta variables of premises doesn't exist in substitution list then we are free to substitute by anything). These substituted premises will become next goals that we need to prove.

For example if we want to prove $((3+4)*5) = ((4+3)*5)$ we could use rule MULT-INTRO to prove it since $(u \times v) = (x \times y)$ is pattern matchable with $((3+4)*5) = ((4+3)*5)$ by substitute u with $(3+4)$, v with 5, x with $(4+3)$, and y with 5. Then premises $u = x$ and $v = y$ are substituted and become $(3+4) = (4+3)$ and $5 = 5$ respectively. Therefore, $((3+4)*5) = ((4+3)*5)$ can be proven by MULT-INTRO and produce another two sub-goals which are $(3+4) = (4+3)$ and $5 = 5$. This can be shown as instance of MULT-INTRO as the following

$$\dfrac{(3+4) = (4+3) \qquad 5 = 5}{((3+4)*5) = ((4+3)*5)}\ \textsc{add-intro}$$

Figure 3.10: Example of instance of derivation rule.

For the remaining, we could prove $(3+4) = (4+3)$ using ADD-COMM because $(x+y) = (y+x)$ is pattern matchable with $(3+4) = (4+3)$, ADD-COMM doesn't have any premises hence there are no further sub-goal. For $5 = 5$ we could use EQ-REFL, this also deosn't produce further sub-goal so the entire proof is complete. We can the write the entire proof using *derivation tree* as the following

$$\dfrac{\dfrac{}{(3+4) = (4+3)}\ \textsc{add-comm} \qquad \dfrac{}{5 = 5}\ \textsc{eq-refl}}{((3+4)*5) = ((4+3)*5)}\ \textsc{add-intro}$$

Figure 3.11: Example of derivation tree.

Some rules in figure 3.9 don't have any premises. This is necessary, otherwise, applying rule always generate further sub goals and never terminate. These rules can be seen as *axiom* which is a term that valid by assumption i.e. so need to prove such a term.

For better understanding about derivation system, here is a more complex derivation tree which prove $(((w \times x) + (w \times y)) \times z) = (w \times ((x \times z) + (y \times z)))$. Reader is encouraged to explore that why this derivation tree is correct.

$$\dfrac{}{((w \times (x+y)) \times z) = (w \times ((x+y) \times z))}\ \textsc{mult-assoc}$$

$$\dfrac{\vdots \qquad \dfrac{\dfrac{}{w = w}\ \textsc{eq-refl} \qquad \dfrac{}{((x+y) \times z) = ((x \times z) + (y \times z))}\ \textsc{dist-right}}{(w \times ((x+y) \times z)) = (w \times ((x \times z) + (y \times z)))}\ \textsc{mult-intro}}{((w \times (x+y)) \times z) = (w \times ((x \times z) + (y \times z)))}\ \textsc{eq-tran}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(w \times (x+y)) = ((w \times x) + (w \times y))}\ \textsc{dist-left}}{((w \times x) + (w \times y)) = (w \times (x+y))}\ \textsc{eq-symm} \qquad \dfrac{}{z = z}\ \textsc{eq-refl}}{(((w \times x) + (w \times y)) \times z) = ((w \times (x+y)) \times z)}\ \textsc{mult-intro} \qquad \vdots}{(((w \times x) + (w \times y)) \times z) = (w \times ((x \times z) + (y \times z)))}\ \textsc{eq-tran}$$

Figure 3.12: Example of more complex derivation tree.

Chapter 4

Example Formal System — Simple Arithmetic

As in background chapter, Simple Arithmetic is used as example to explain basic concept of formal systems and its derivations. In order to make the transition goes smoother, this chapter aims to encode Simple Arithmetic and explain basic features and usability of *Phometa* at the same time. Please note that this is just a faction of actual arithmetic modified to make it easier to understand, so it is not as powerful as the actual one.

4.1 First time with Phometa

You can download complied version of Phometa at

`https://github.com/gunpinyo/phometa/raw/master/build/phometa.tar.gz`

Once you unzip this file, you can start Phometa server by execute

```
./phometa-server.py 8080
```

where `8080` is port number, you can change this to another port number if you like. Please note that Python is required for this server.

Then open your favourite web-browser[1] and enter

```
http://localhost:8080/phometa.html
```

The program will look like this

[1]but Google Chrome is recommended

Figure 4.1: Screenshot of Phometa when you open it from web-browser.

Phometa has a repository which consists of packages and modules that store formal systems and its proofs. The left pane of figure 4.1 shows global structure of a repository. The current repository has one package named "Standard Library" which consists of three modules named "Propositional Logic", "Simple Arithmetic", and "Typed Lambda Calculus".

Module in Phometa are analogous to text file. It consists of nodes that could depend on one another. There are four types of node which are *Comment*, *Grammar* (Backus-Naur Form), *Rule* (Derivation Rule), and *Theorem* (Derivation Tree). If you click at a module on the repository pane e.g. "Simple Arithmetic", you will see the whole content of the module appear on the centre pane. Alternatively, you can click on each node on the repository pane directly to focus on particular node.

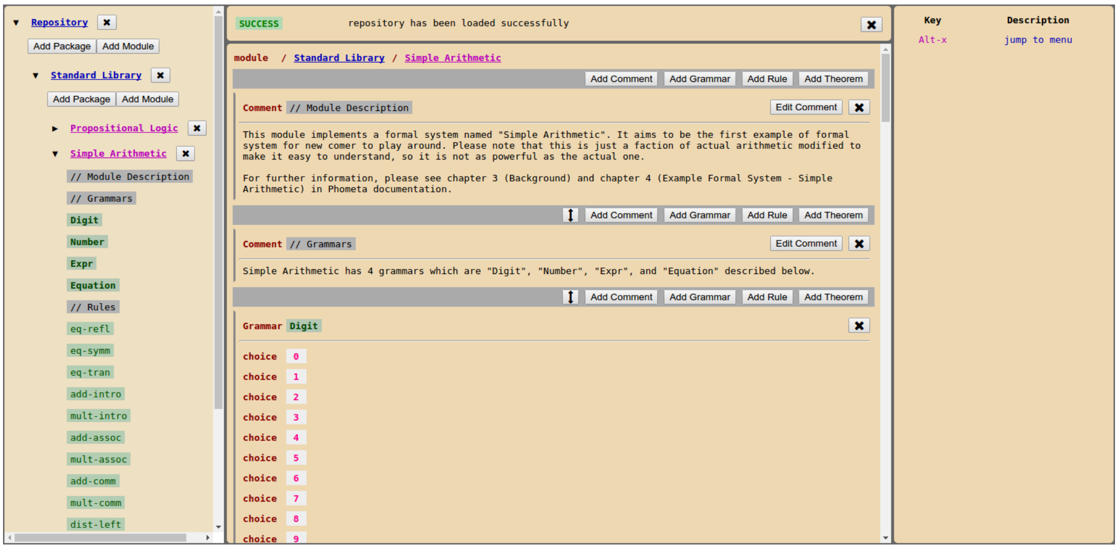


Figure 4.2: Screenshot of Phometa when you click "Simple Arithmetic" module.

In order to improve productivity, Phometa has several key-bindings specific to curtain state of program. Fortunately, user don't need to remember any of this since the right pane (i.e. keymap pane) shows every possible key-binding with its description on current state. This also allow new-comer to explore new features during using it

4.2 Grammars

The Backus-Naur Form of Simple Arithmetic in figure 3.1 could be transformed in to this four following grammars

```
Grammar Digit

choice  0
choice  1
choice  2
choice  3
choice  4
choice  5
choice  6
choice  7
choice  8
choice  9

Grammar Number

choice  Digit
choice  Number Digit

Grammar Expr

metavar_regex  [a-z][0-9]*
choice  Number
choice  Expr + Expr
choice  Expr × Expr

Grammar Equation

choice  Expr = Expr
```

Figure 4.3: Grammars of Simple Arithmetic

We take advantage of visualisation by replacing brackets with underlines, this should improve readability because reader can see a whole term in a compact way but still able check how they are bounded when needed, for example,

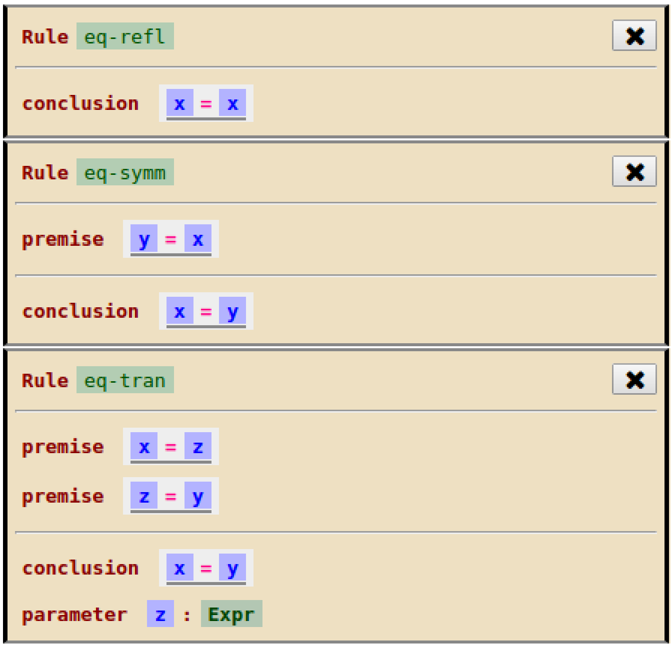
- `<Number>` 250 is transformed to `Number` `2 5 0`
- `<Expr>` $(0 + (12 \times 6))$ is transformed to `Expr` `1 2 + 0 × 6`
- `<Equation>` $(5 + 7) = 12$ is transformed to `Equation` `5 + 7 = 1 2`

These underline patterns coincide with diagram in figures 3.2, 3.3, 3.5, and 3.6 respectively.

`metavar_regex` is used to control the name meta variables of each grammar. If this property is omitted, the corresponding grammar cannot instantiate meta variables. For example, `Expr` can instantiate meta variables with the name comply to regular expression `/[a-z][0-9]*/` (e.g. `a`, `b`, ..., `z`, `a1`, `a2`, ...), whereas `Digit` , `Number` , and `Equation` couldn't instantiate any meta variables, however, it could have meta variables as sub-term e.g. `Equation` `x + x = 2 × x`.

4.3 Rules

The derivation rules of Simple Arithmetic in figure 3.9 can be transformed as the following



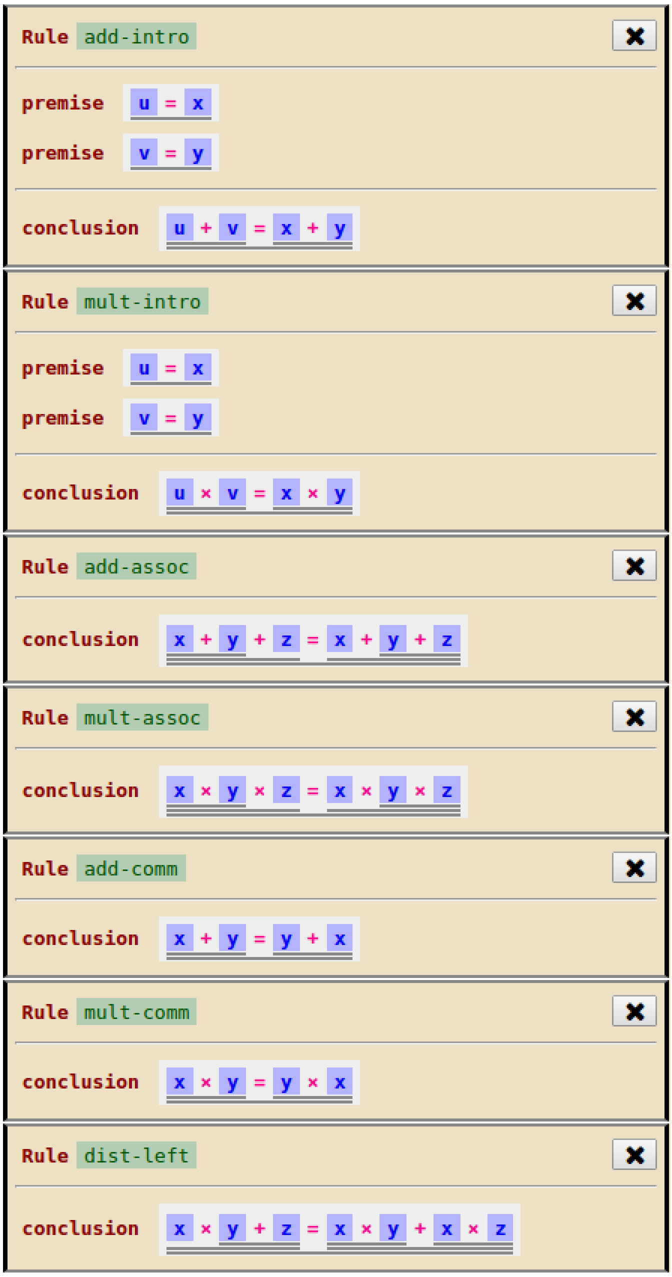


Figure 4.4: Rules of Simple Arithmetic

Most of rules here are self explain but in rule `eq-tran` , there is an additional property named `parameter` (s) which is a meta veritable that appear in premises but not in conclusion, hence user need to give a term when the rule is applied. Please note that `parameter` is automatic i.e. when user define they own rule, it will change automatically depending on premises and conclusion dist-right is not defined here but it will be defined as *lemma* in the next section.

4.4 Theorems and Lemmas

The first example of derivation tree (figure 3.11) could be transformed to theorem

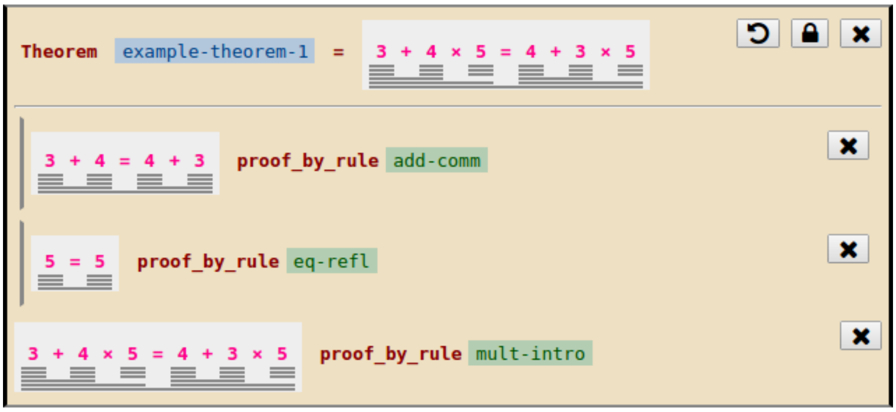
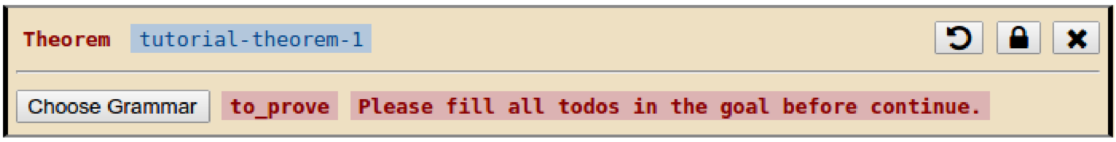


Figure 4.5: A theorem that show that $(3 + 4) \times 5 = (4 + 3) \times 5$.

You can see that the theorem still preserve tree-like structure but the width doesn't grow exponentially like derivation.

Next, I will show you that how was the theorem above constructed. Once we click module "Simple Arithmetic" on the repository pane, we will see the whole context similar to figure 4.2, you will also see that there are adding panel intersperse among each node

Now, click "Add Theorem", the button will change to input box where you can specify theorem name. Type "tutorial-theorem-1", can you will get empty theorem as the following



The first thing that we can do is to construct the goal that will be proven. On the picture above you will see button labelled "Choose Grammar" which is, in fact, a term that doesn't know its grammar. We can specify grammar by click the button, which in-tern, will change to input box. Now the keymap pane will look like this

Key	Description
Alt-1	Digit
Alt-2	Number
Alt-3	Expr
Alt-4	Equation
Alt-u	search unicode
Alt-x	jump to menu
↑	quit root term

The keymap pane told us that there are 4 grammars available, we can either press `Alt-1..4` or click on the row in keymap pane directly to select grammar. Alternatively, you can search a grammars by type faction on it is input box e.g. "eq"

Key	Description
Return	Equation
Alt-1	Equation
Alt-u	search unicode
Alt-x	jump to menu
↑	quit root term

Now, it is only `Equation` available because it is the only one that has "eq" as (case-insensitively) sub-string. And since it is the only one, you can select it by press `Return` , even though in this case we don't have too many options but still benefit from it in auto complete favour. Please note that this input box support multiple matching separated by space e.g. "eq ti" still match `Equation` because both of "eq" and "ti" are sub-string of it.

Once you select a grammar, the box will change to green colour and waiting for a term of that grammar. In this case, we select `Equation` since it has just one choice and doesn't have meta variable or literal[2] so Phometa automatically click such a choice and the theorem will look like this

Theorem tutorial-theorem-1

Expr = Expr to_prove Please fill all todos in the goal before continue.

You may notice that the goal term as grey background rather than white as before. This indicate that the term is still modifiable.

Next, we will continue on the `Expr` term on the left hand side of "=". When the cursor is in it, the keymap will look like this

[2]literal is similar to meta-variable but only match to itself, will be explained in later chapter

Key	Description
Return	create metavar or literal
Alt-1	Number
Alt-2	Expr + Expr
Alt-3	Expr × Expr
Alt-r	reset root term
Alt-u	search unicode
Alt-x	jump to menu
←	jump to prev todo
↑	jump to parent term
→	jump to next todo

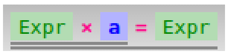
Again, there are 3 choice available which can be selected similar manner when we select grammar. At the this stage you might wonder how to type "×" since it is unicode character. Well, we can go to unicode mode by press `Alt-u` as keymap pane suggest. Then keymap pane will look like this

Key	Description
Alt-1	mathexclam !
Alt-2	mathoctothorpe #
Alt-3	mathdollar $
Alt-4	mathpercent %
Alt-5	mathampersand &
Alt-6	lparen (
Alt-7	rparen)
Alt-8	mathplus +
Alt-9	mathcomma ,
Alt-r	reset root term
Alt-x	jump to menu
Alt-[	prev choices
Alt-]	next choices
Escape	quit searching unicode
←	jump to prev todo
↑	jump to parent term
→	jump to next todo

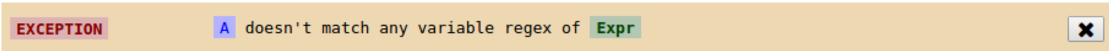
This allow us to search unicode character by using its LaTeX's math-mode name. Now type "times" in the input box, you should see "×" appear on keymap. Once you select it, the unicode mode disappear and put "×" in the input box, which in-tern, filter other choices out so you can hit `Return` for multiplication. The goal will transform to

Expr × Expr = Expr

Next we will focus middle `Expr` . If we type string and hit `Return` here it will assume that we enter meta variable or literal (to avoid conflict auto complete similar to choose grammar is disabled here). E.g. if we type "a" and press enter it will become like this

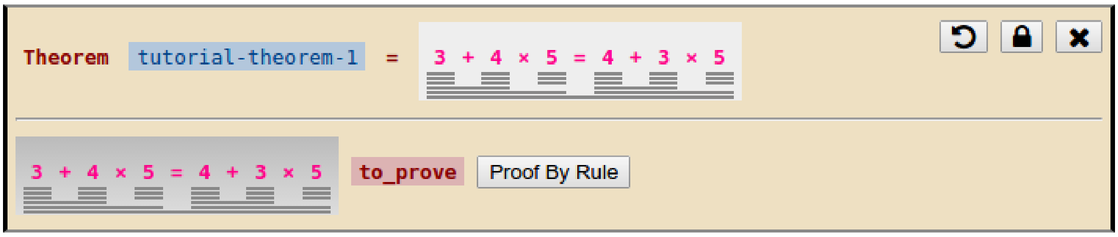


If we enter the name that that doesn't comply to regular expression, it will do nothing and prompt error message above main pane as the following

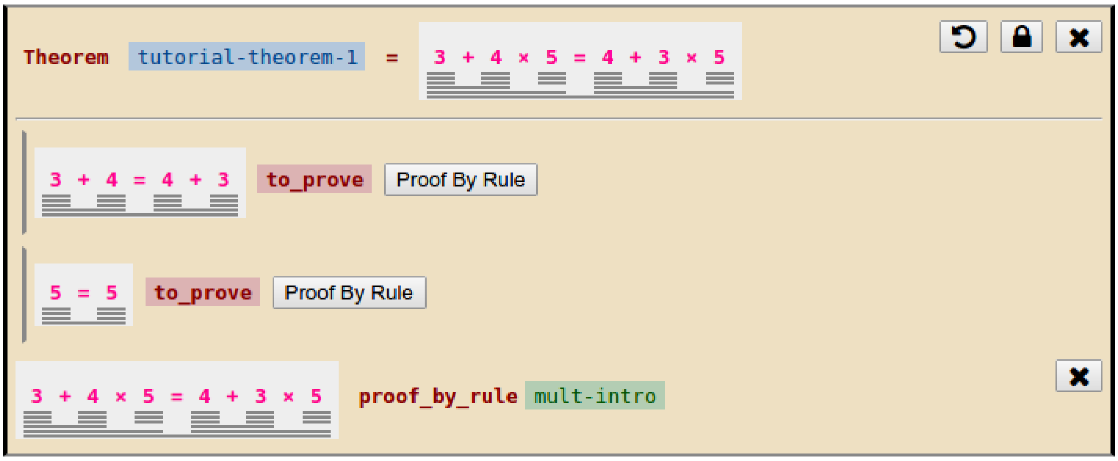


By the way, the goal here doesn't involve any meta variable. We can reset any sub-term (e.g. in this case `a`) by pressing `Alt-t` . Ultimately, you can reset the whole term by pressing `Alt-r` . In addition, you can jump to parent term by pressing `UP` , this is particularly useful when combine with `Alt-t` i.e. you can reset parent term only by keystrokes rather than clicking. You also be able to jump to previous todo or next todo by pressing `LEFT` or `RIGHT` respectively.

By recursively fill the the goal, eventually it will become like this



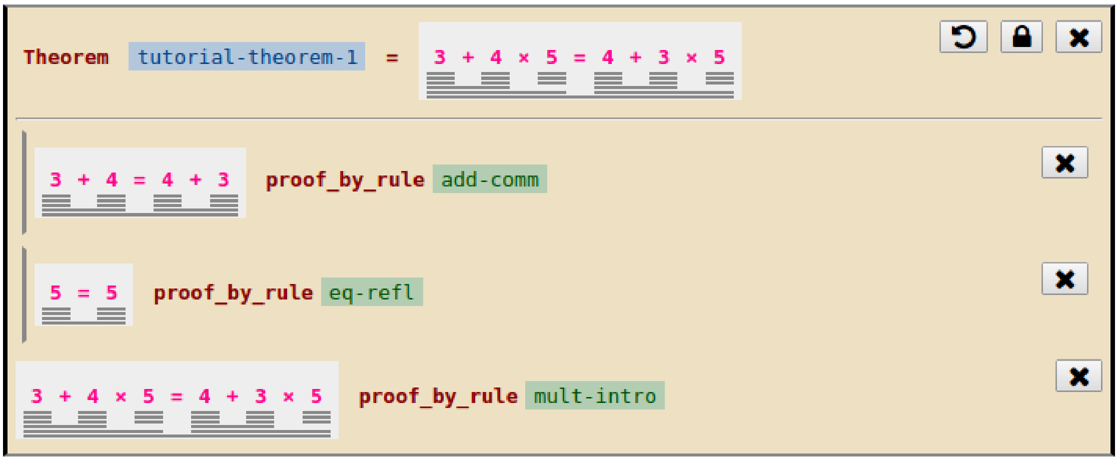
Since the goal is complete, it is ready to be proven. You can select a rule by clicking "Proof By Rule" and select `mult-intro` similar manner to choose grammar. Then the theorem will look like this



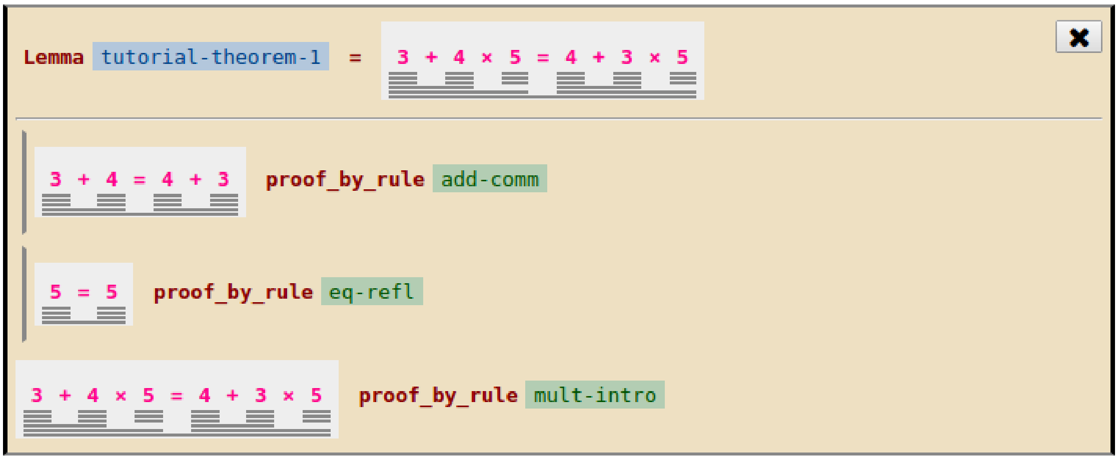
Once the rule is applied, it will generate further sub-goals.

Please notice that the goal background changes to white colour as we can longer modify the goal. However if you made a mistake and want to go back, you can click close button on the bottom right corner of current proof (or press `Alt-t`) to reset current proof then you can modify it again. Ultimately, you can click reset button on the top right corner of the theorem (or press `Alt-r`) to reset entire theorem.

Two remaining sub-goals that have been generated can be proven similar to the process above i.e. select rule `add-comm` for first sub goal and `eq-refl` for second one.



Once the theorem is complete, you can claim validity of the goal. More over you can convert it to lemma that can be used in later theorem by clicking lock button on top-right corner of theorem



Because other theorem can use this lemma so it is no longer modifiable, as you can see that close button of each sub-proof and reset button of the main theorem are gone.

Similarly, we can can create lemma `dist-right` as the following

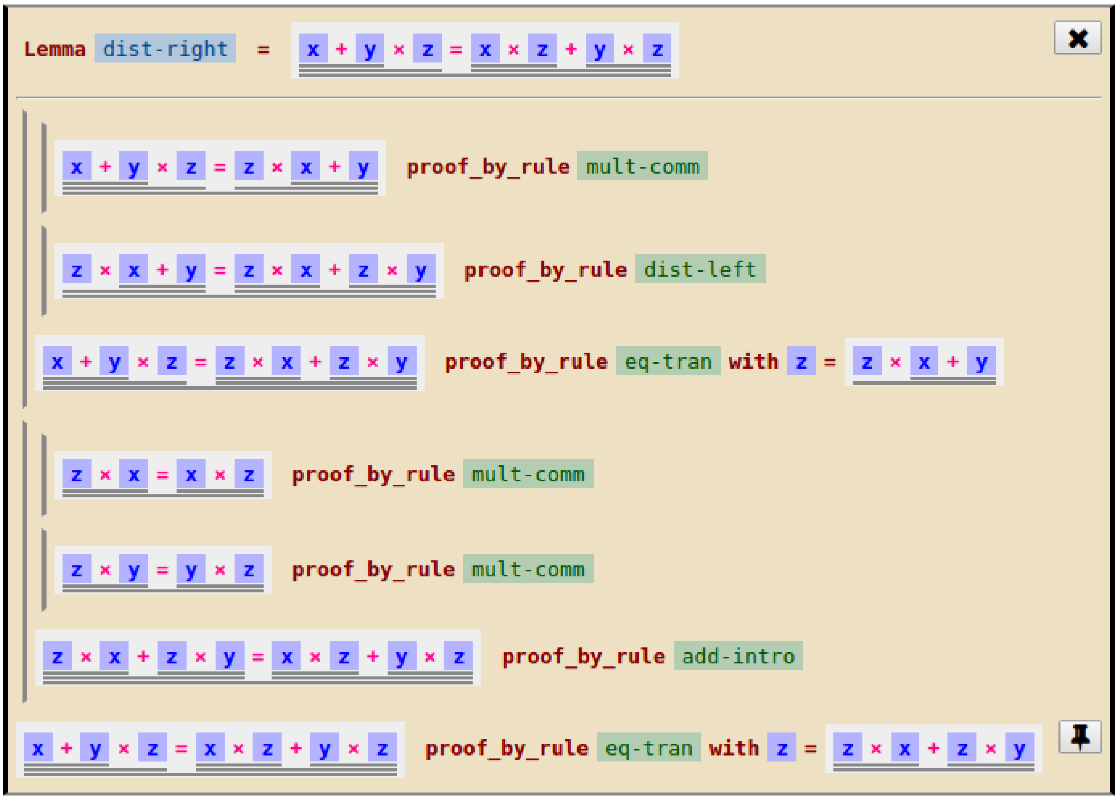


Figure 4.6: An example of lemma obtained by lock a theorem.

It is a good practice to create lots of small lemmas rather than a big theorem. This is because it is easier to read and you can use a lemma multiple time i.e. no need to duplicate sub-proof.

4.5 More complex theorem

To gain more familiarly on theorem, here is more complex theorem corresponded the second example of derivation tree on figure 3.12

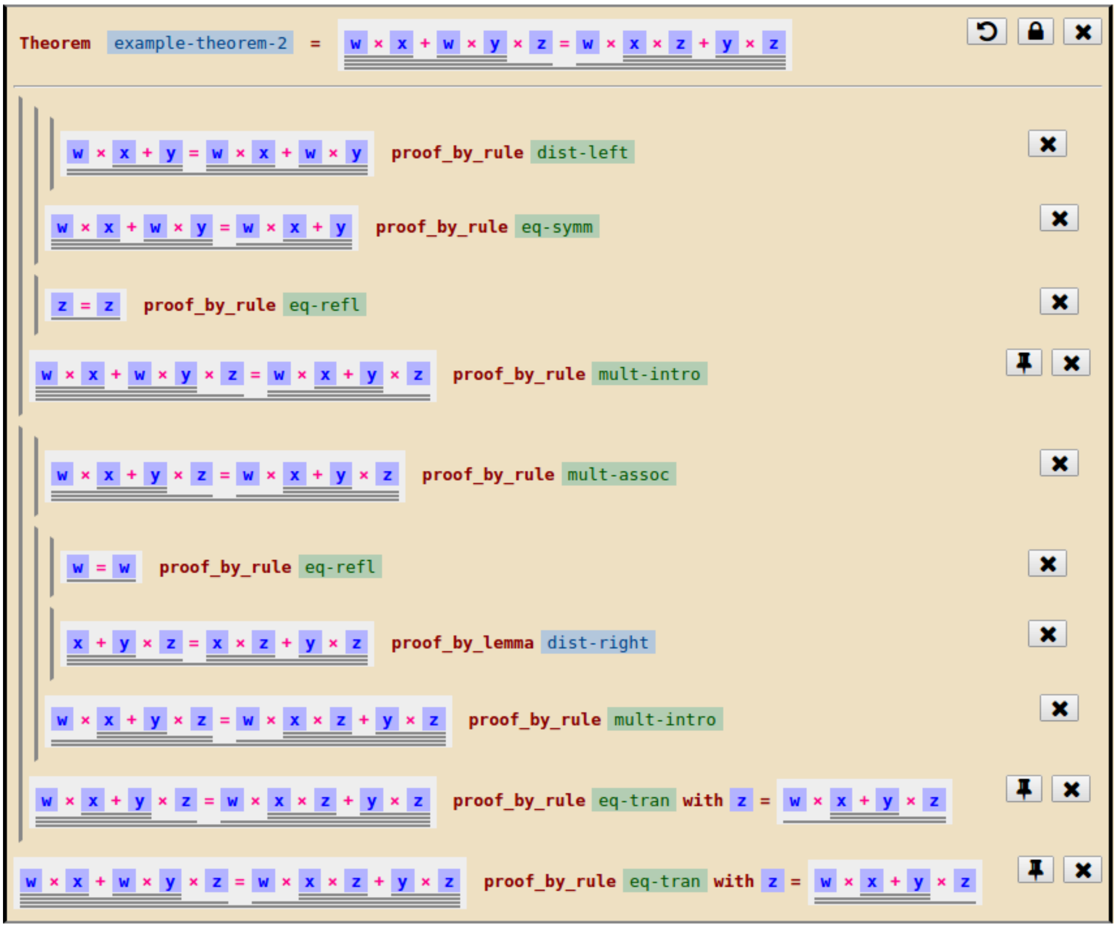
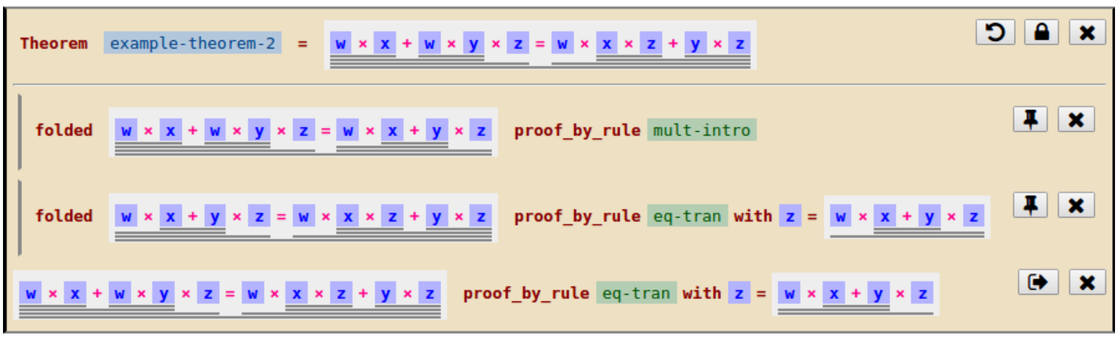


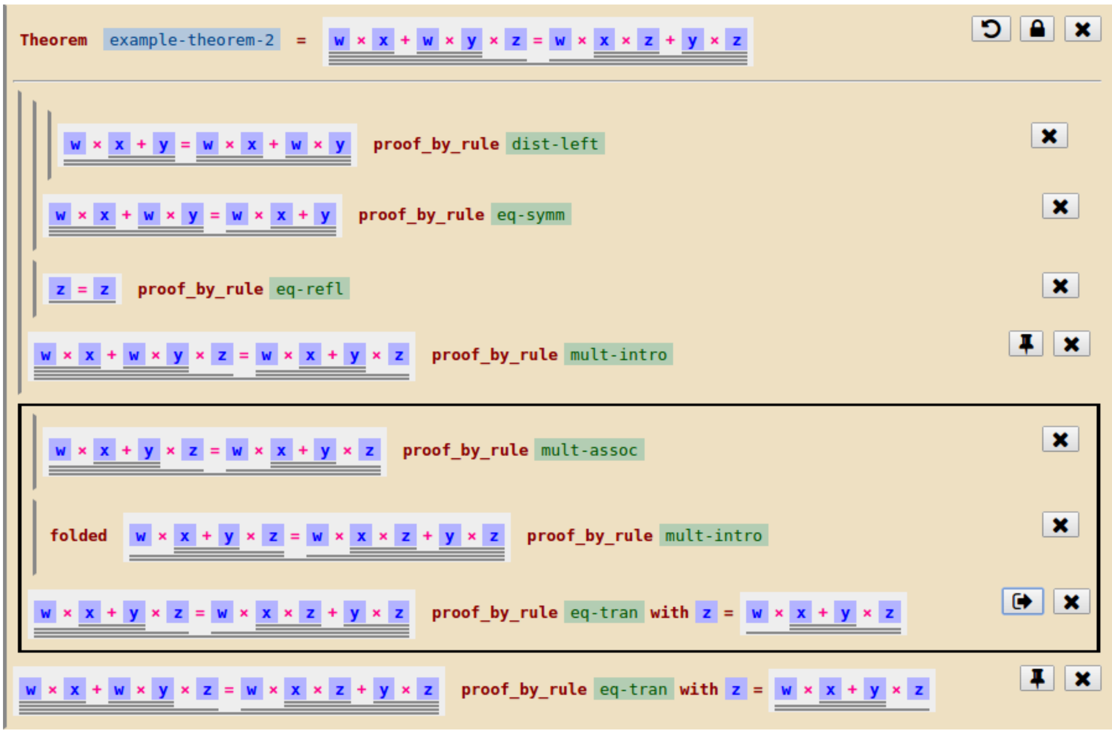
Figure 4.7: The second example theorem of Simple Arithmetic.

Sub-proofs become more complex and premises of main proof are far away which is harder to read, to avoid this kind of problem, we introduce a focus button that will fold sub-proof of corresponding proof. For example, if we click focus button on the main proof it will look like this



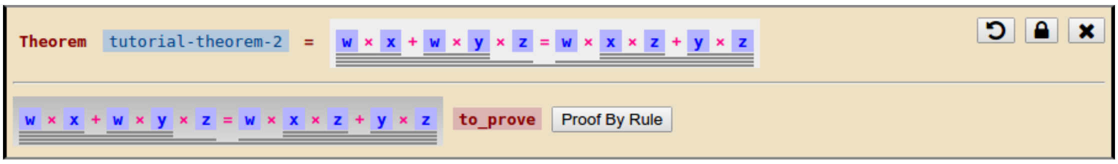
Two sub-proofs of the main theorem are folded, this allow us to read rule instance of `eq-tran` easily. You can unfolded sub-proofs by clicking unfocus button at the same position that focus button was there before. And the theorem will look the same as figure 4.7 again.

When you read some proof in Phometa, it is a good idea to click focus on the main proof first so you can read the main rule instance easily. Once you understand main proof you can read one of sub proof by clicking focus button that correspond to that sub-proof. If you click focus button on the first sub-proof it will look like this

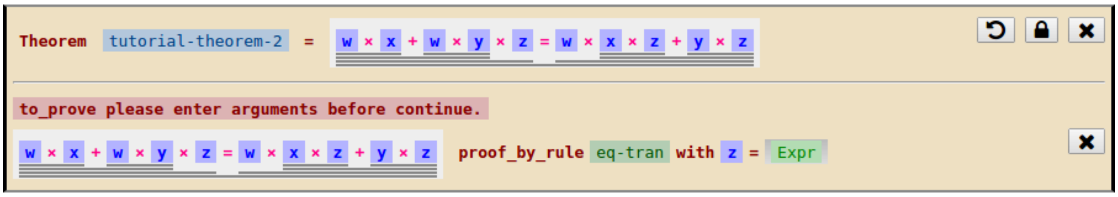


This process automatically unfold the previous one before folding sub-proof of this proof again. Please note that some of deeper proofs might not have focus button at all, this is because its sub-proofs cannot reduce further than original one.

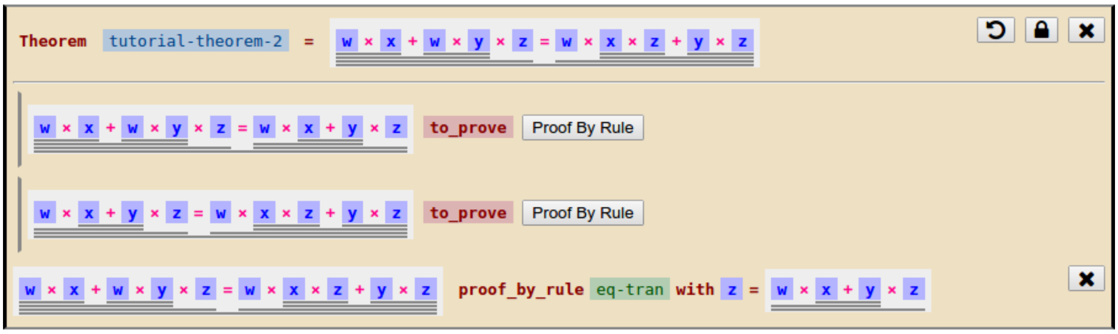
The next thing that I will show are how to use rule parameters and lemma. This can be illustrated by recreate this theorem again. First create create a theorem `tutorial-theorem-2` using the same goal as above theorem.



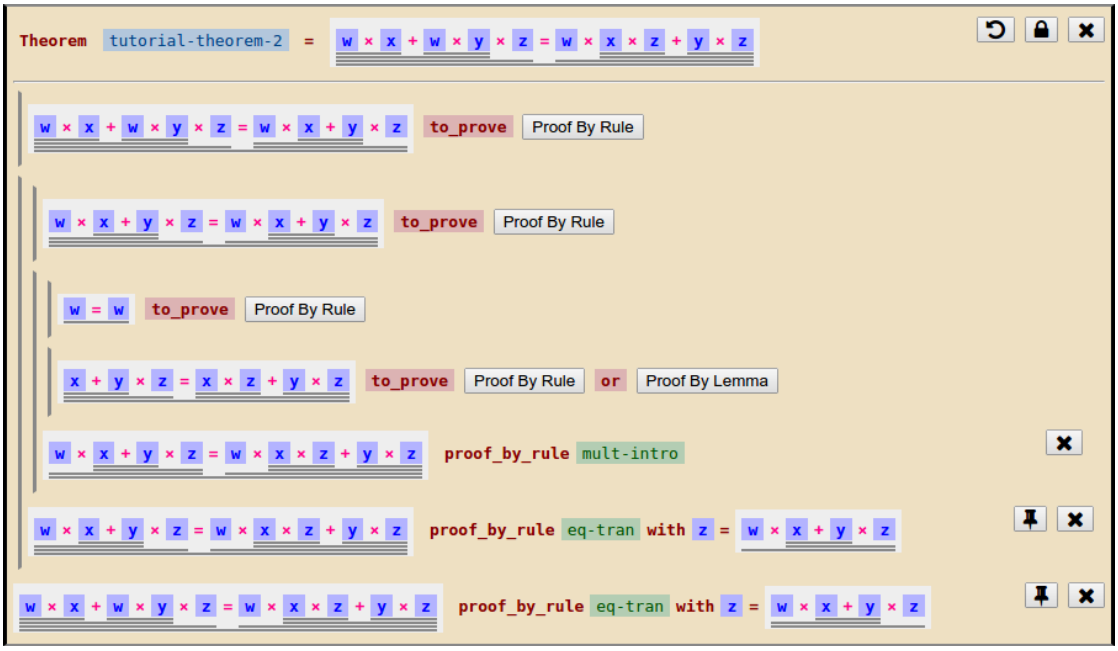
Then apply rule `eq-tran` to this goal



The rule applying process is not complete because `eq-tran` contains `z` which appear in premises but not in conclusion (i.e. `z` is parameter) so Phometa ask us to fill the term that we want to use. In this case we want `w × x + y × z` so put it there



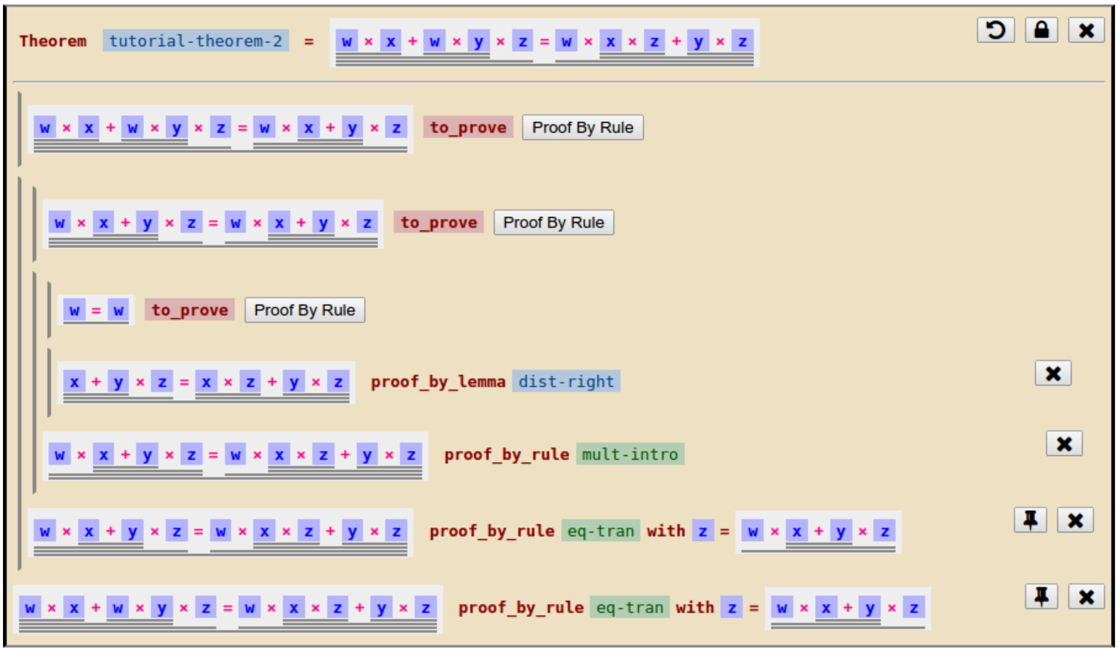
Now, let focus on the second sub-goal, we can apply `eq-tran` again but with `z` = `w × x + y × z`. Then, apply `mult-intro` in the second its sub-goal.



You can see that there is a sub-goal that has button “Proof By Lemma”. This is because there is at least one lemma that is pattern matchable with that sub-goal. If you click “Proof By Lemma” button, the keymap will look like this

Key	Description
Return	dist-right
Alt-1	dist-right
Alt-l	lock as lemma
Alt-r	reset whole theorem
Alt-t	reset current proof
Alt-u	search unicode
Alt-x	jump to menu

In this case, there is one lemma which is `dist-right` that is pattern matchable to that sub-goal. You can hit `Return` to use this lemma and it will look like this



The remaining step is easy enough.

4.6 Exercises

- Create a theorem and proof each of the following
  - $w + x + y \times z = z \times y + x + w$
  - $u + v \times x + y = u \times x + u \times y + v \times x + v \times y$
  - $u + v \times x + y + z = u \times x + v \times x + u \times y + v \times y + u \times z + v \times z$
- Extend Simple Arithmetic to support
  - addition and multiplication identity.
  - addition and multiplication idempotent.
  - inequality.
- Create a theorem of your own choice and proof it.

Chapter 5

Example Formal System — Propositional Logic

Once you are familiar with some basic features and usability of *Phometa* from the last chapter. This chapter aims to show more advance features on another formal system named *Propositional Logic* which is the most well known logical system[1].

Logic, in general, works so well with traditional derivation system, hence there is spacial name called *Natural Deduction* which is a combination of any kind of Logic together with derivation system.

5.1 Grammars

As usual, the first thing that needed to be defined grammars. Propositional Logic has 4 grammars which are `Prop` , `Atom` , `Context` , and `Judgement` as its grammars.

`Prop` is a proposition, semantically, it is a term that can be evaluated to either true or false (given that there are no meta variables in the term). Grammars of `Prop` can be defined in Phometa as the following

[1] Logical system is a formal system together with semantics[14]

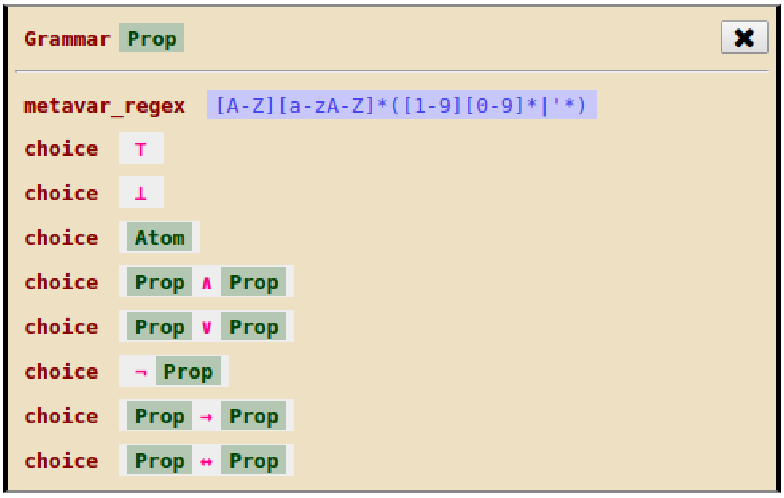


Figure 5.1: Definition of `Prop`

This grammar is equivalence to the following Backus Normal Form

```
<Prop> ::= ⊤ | ⊥ | <Atom>
         | <Prop> ∧ <Prop>
         | <Prop> ∨ <Prop>
         | ¬ <Prop>
         | <Prop> → <Prop>
         | <Prop> ↔ <Prop>
         | meta-variables comply with regex
           /[A-Z][a-zA-Z]*([1-9][0-9]*|'*)/
```

Figure 5.2: Backus-Naur Form correspond to `Prop`

On the 3^{rd} choice of `Prop` depends on `Atom` which represents primitive truth statement that cannot be broken down any further. It can be defined in Phometa as the following.

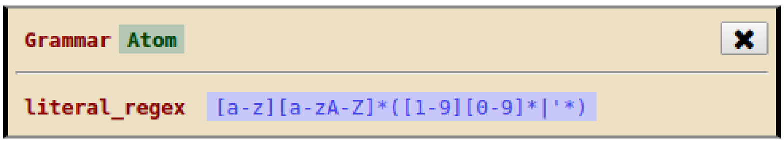


Figure 5.3: Definition of `Atom`

You can see that `literal_regex` appears inside `Atom` definition, this allows `Atom` be instantiated by literal which is similar to meta variable, the only different is that literal doesn't have ability to be substituted by arbitrary term like meta variable.

At this stage, you might wonder that why `Prop` needs both of meta variables and `Atom` . Well, meta variable will be used when referring to something general and `Atom` will used when referring to particular truth statement. For example, if we can prove that `A ∨ ¬ A` is valid, then terms such as `⊤ ∨ ¬ ⊤`, `⊤ → ⊥ ∨ ¬ ⊤ → ⊥`, `B ∨ ¬ B`, `rainning ∨ ¬ rainning`, and `B ∧ rainning ∨ ¬ B ∧ rainning` are also valid. However, if we can prove that `rainning ∨ ¬ rainning` is valid, we don't want to expose this proof to other terms since it might be proven from specific knowledge.

Now, we have enough ingredient to create a proper proposition, one might say that we can start proving it directly, however, most of proposition that we will dealing with only holds under certain assumptions, hence, a *judgement* should be in the form $A_1, A_2, ..., A_n \vdash B$ where $A_{1..n}$ are assumptions and B is conclusion.

To model a judgement in Phometa, first we need to model assumptions or in the other name, `Context` as the following

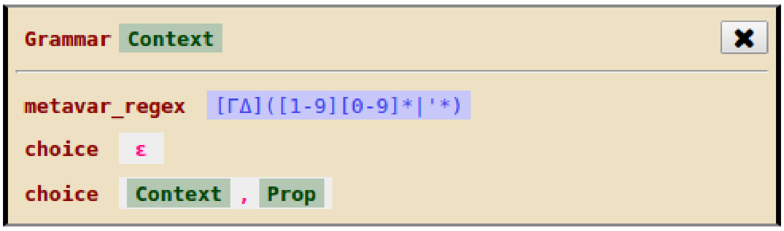


Figure 5.4: Definition of `Context`

So a term of `Context` can be either empty context or another context appended by a proposition. We can see a context as a list of proposition.

Now we are ready to define `Judgement` as the following

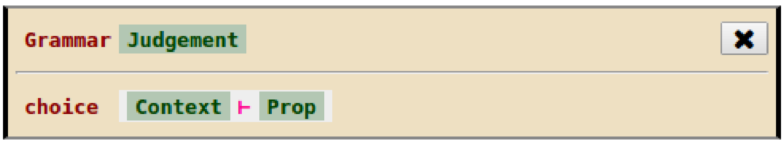


Figure 5.5: Definition of `Judgement`

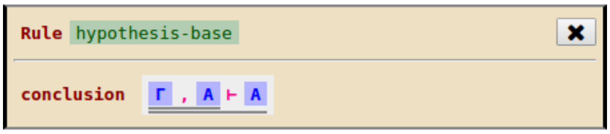
`Judgement` has a meaning of validity. For example, validity of `ε , p , q ∨ r ⊢ p ∧ q ∨ p ∧ r` means, assuming that `p` and `q ∨ r` hold then `p ∧ q ∨ p ∧ r` holds.

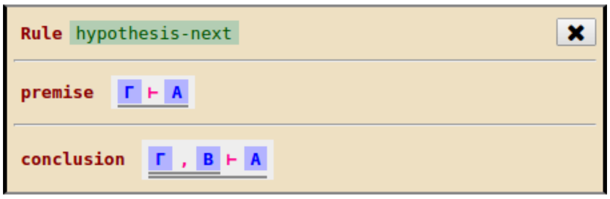
Please note that `Judgement` doesn't have field `metavar_regex` nor `literal_regex` so we can't accidentally use meta variable or literal for `Judgement` .

5.2 Hypothesis rules

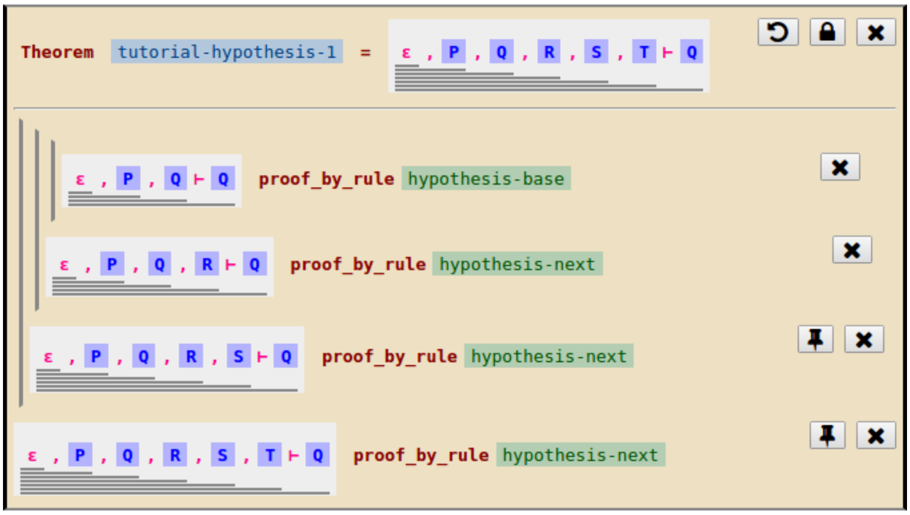
In order to prove any judgement, we want ability to state that for any proposition that is in assumptions, it can be conclusion i.e. $A_{1..n} \vdash A_i$ where $i \in 1..n$

This is achievable by `hypothesis-base` and `hypothesis-next` .





`hypothesis-base` matches the last assumption with the conclusion whereas `hypothesis-next` removes the last assumption and pass on to a premise, this can prove a judgement that has conclusion as assumption like this.



This is not efficient as we might need to call `hypothesis-next` $(n-1)$ times where n is the number of assumptions. To solve this problem, we introduce `hypothesis` that is more complex than ordinary derivation rule.

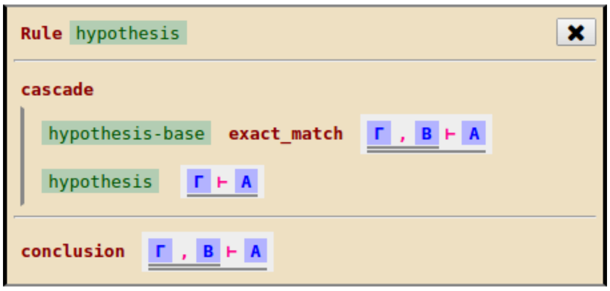
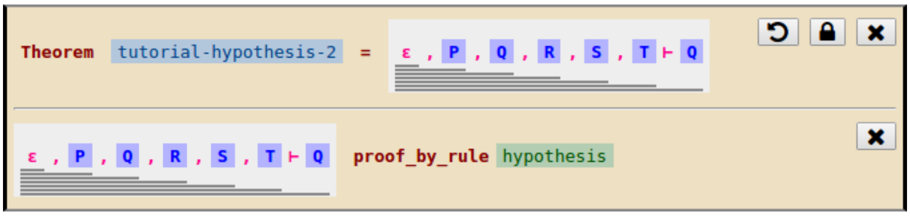


Figure 5.6: rule `Hypothesis`

`hypothesis` uses a cascade premise instead of direct premise. A cascade premise has several sub-rules calling-template that will be tried in order. In this case, `hypothesis` tries to apply `hypothesis-base` on its goal,

- If sub-rule is applicable, then use sub-goals generated from sub-rule as its sub-goals, in this case, `hypothesis-base` doesn't have any premises so this cascade premise has no further sub-goals.
- Otherwise, *cascades* down and tries to apply the next sub-rule which is `hypothesis` itself[2]. Again, if applicable, use sub-goals of sub-rule, otherwise, the main `hypothesis` rule fail as the cascade premise fail to match with any ofsub-rules.

`hypothesis` could solve the last theorem like this



To show the process, first `hypothesis` conclusion — Γ , B ⊢ A is pattern match against goal = ε , P , Q , R , S , T ⊢ Q, this results in A = Q, B = T, and Γ = ε , P , Q , R , S.

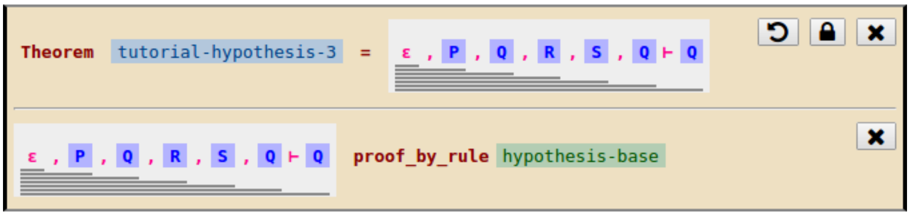
This cascade premise try to apply `hypothesis-base` with goal[3] = ε , P , Q , R , S , T ⊢ Q.

`hypothesis-base` , as sub-rule, let Γ , A ⊢ A pattern match against ε , P , Q , R , S , T ⊢ Q and get A = Q, A = T, and Γ = ε , P , Q , R , S. When a meta variable is matched

[2]Yes, it supports recursive call

[3]This is result from substitution to that sub-rule goal template. Coincidentally, it is the same as `hypothesis` conclusion

with two or more terms, those terms will be unified to make pattern match still possible. So `T` will be replaced by `Q` and this sub-rule will success. Here is the same result if `hypothesis-base` is applied directly on the theorem.



However, this is not what we want, to avoid this problem, we cat put flag `exact_match` to this sub-rule, this flag will prevent further unification. Now, `T` cannot unify with `Q` so this sub-rule fail. So, the cascade premise will move to second sub-rule and try to apply `hypothesis` with `ε , P , Q , R , S ⊢ Q`.

`hypothesis` , as sub-rule, let `Γ , B ⊢ A` pattern match against `ε , P , Q , R , S ⊢ Q`, the process is similar as before so I can tell directly that it will apply `hypothesis` as sub-sub-rule with goal = `ε , P , Q , R ⊢ Q`, which in tern, apply `hypothesis` as sub-sub-sub-rule with goal = `ε , P , Q ⊢ Q`.

Now, `hypothesis-base` with goal = `ε , P , Q ⊢ Q` will not fail again since the last assumption and the conclusion is exactly match, i.e. no further unification needed hence it will success and return no sub-goals as `hypothesis-base` doesn't have any. This success will propagate up to the top level and the entire will cascade success with no further sub-goals as shown in `tutorial-hypothesis-2` .

Please note that a cascade premise is just another type of a premise, sub-goals that are generated from sub-rule will replace the cascade premise itself, similar to how a sub-goal replaces direct premise. Thus, cascade premise can be used alongside with direct premises, for more information on cascade blocks please see specification chapter.

5.3 Main Rules

Now, Propositional Logic is ready for new rules as the following,

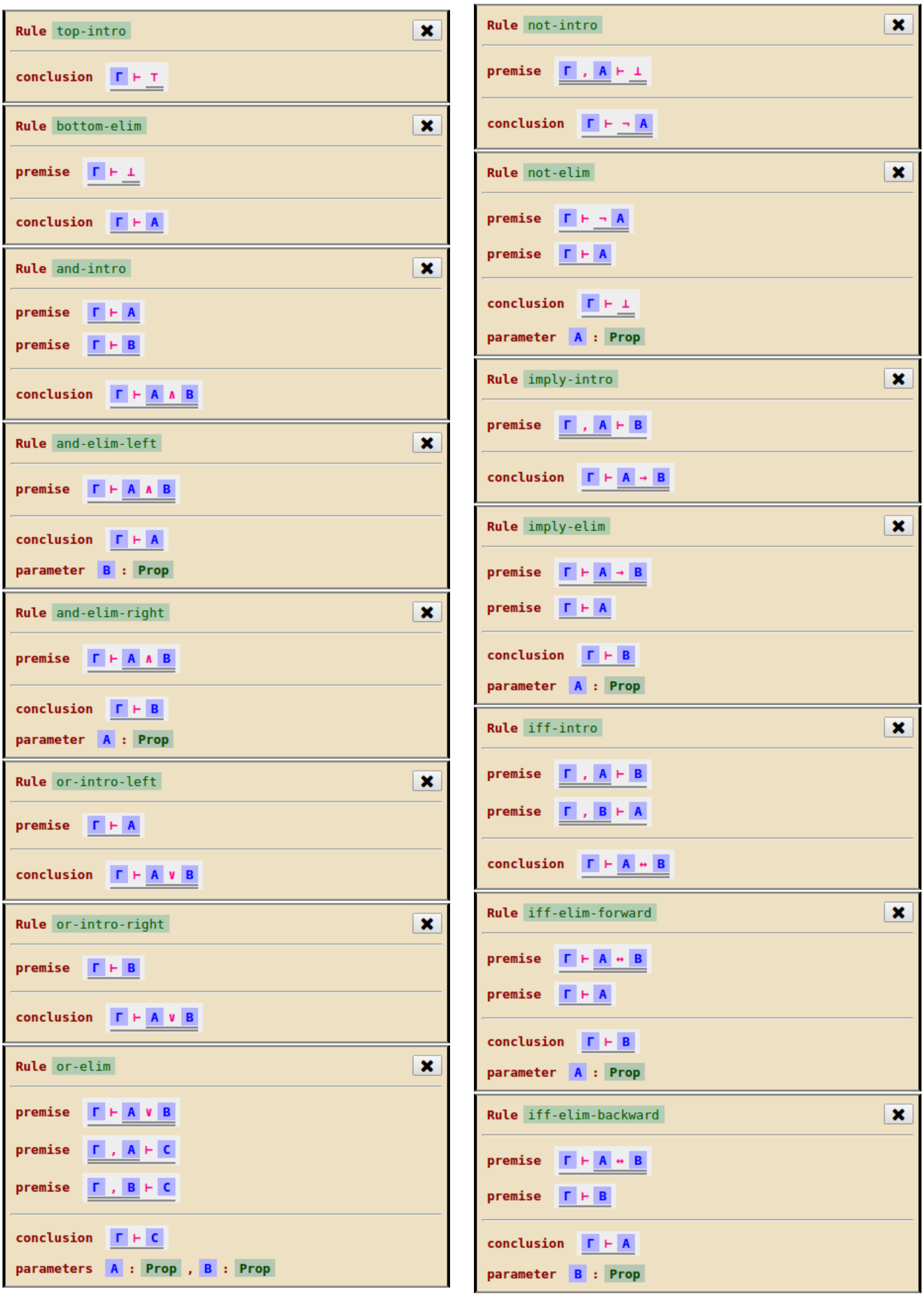
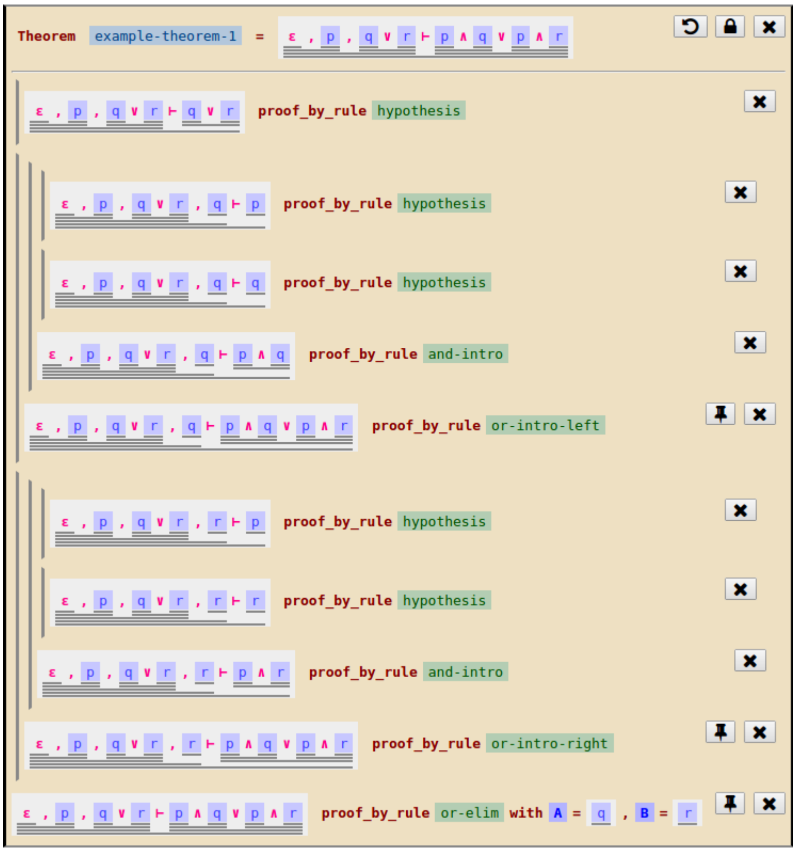
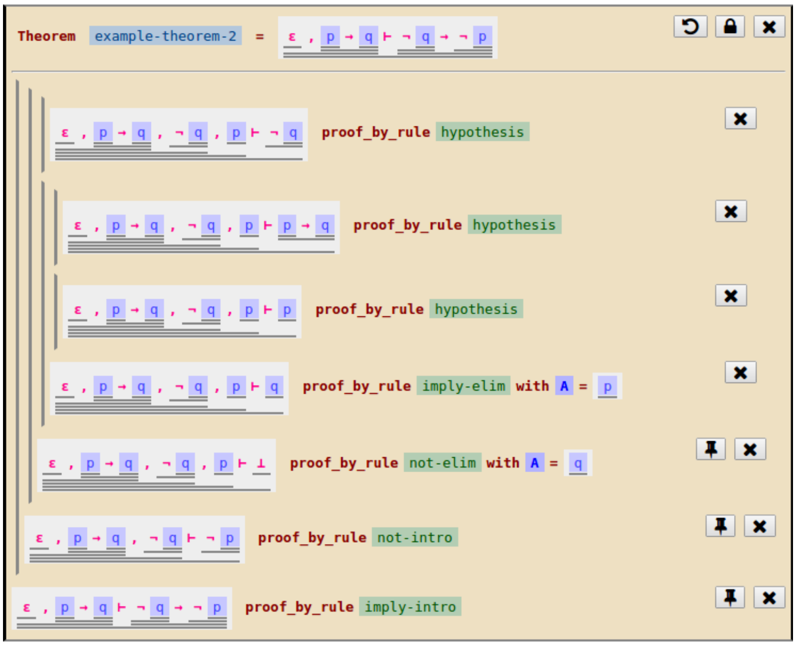


Figure 5.7: Main Rules for Propositional Logic

For example, these rules can be used together with `hypothesis` as the following

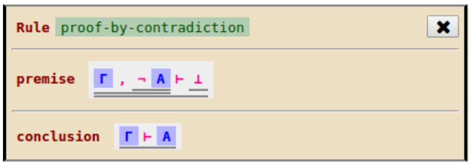




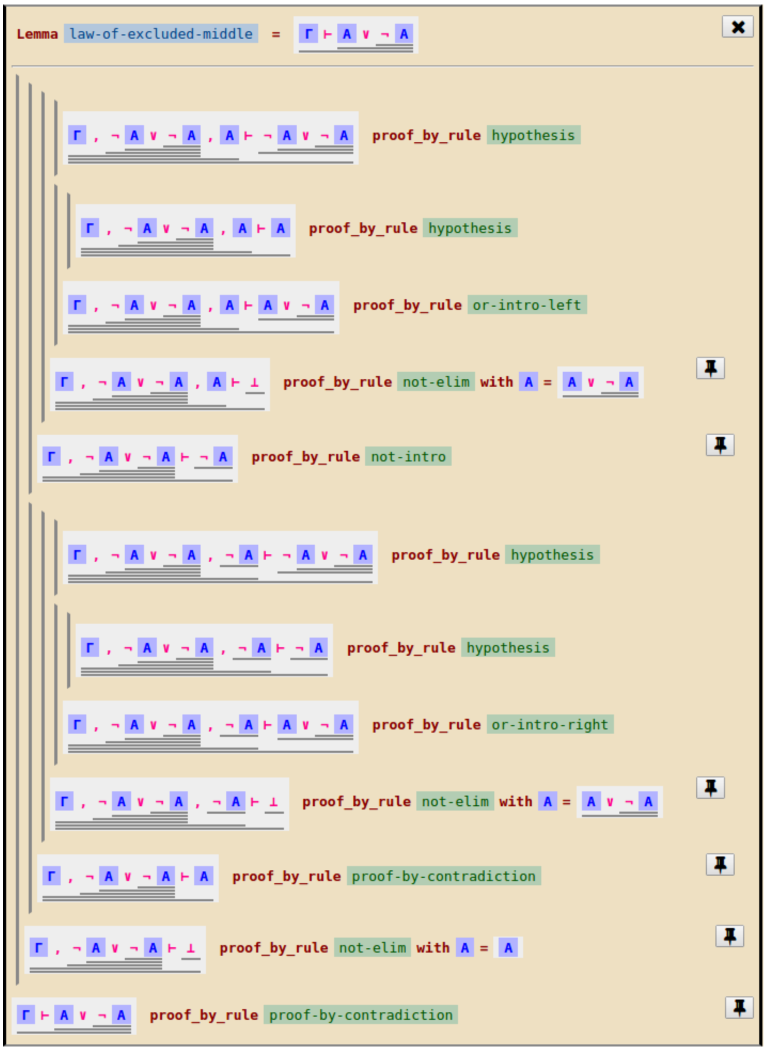
5.4 Classical Logic

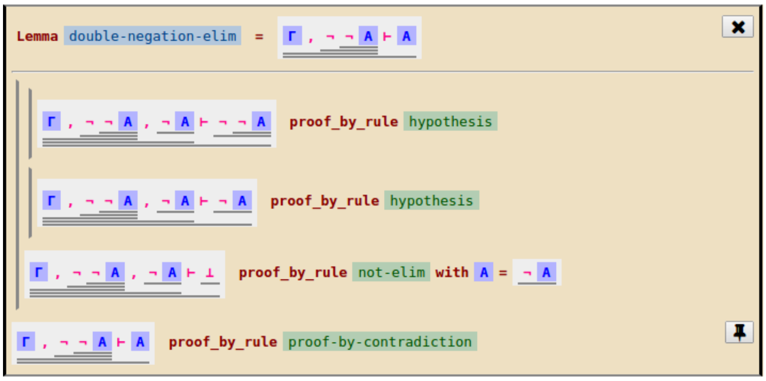
The rules so far create Intuitionistic Logic i.e. it doesn't assume that each proposition must be either true or false. Hence, cannot prove some thing like $A \lor \neg A$.

We can introduce rule `proof-by-contradiction` , which is equivalent to axiom `law-of-exclude-middle` or `double-negation-elim` , to make Intuitionistic Logic become Classical one.

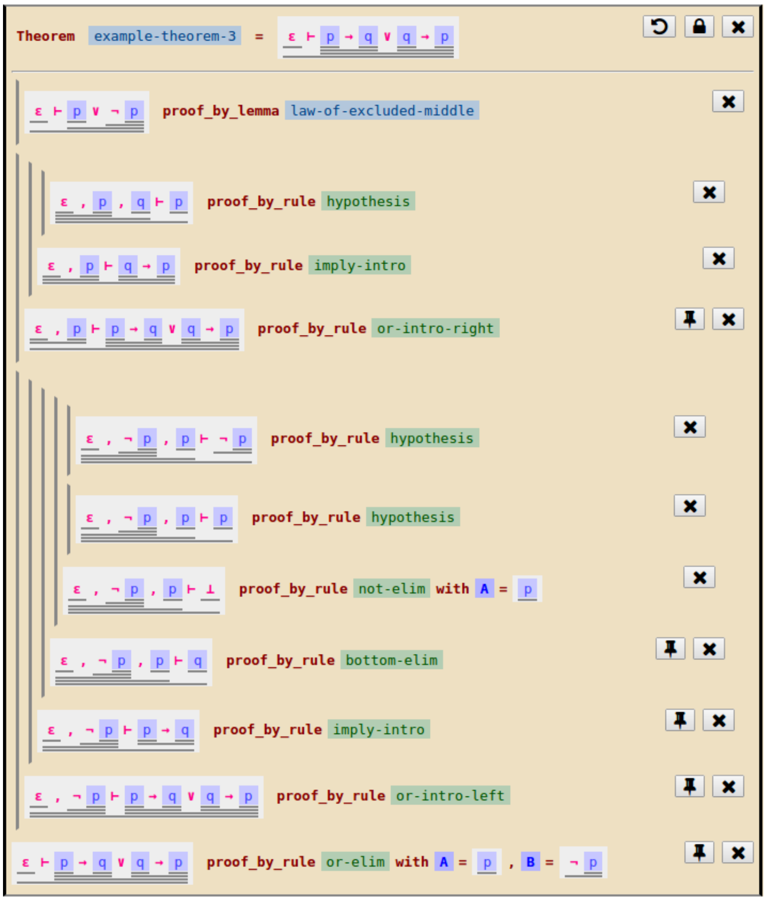


And now we can prove `law-of-exclude-middle` and `double-negation-elim` as lemmas.





For example, this example only holds only under Classical Logic.



5.5 Validity of Proposition

Although we prove validity of `Judgement` to show that a curtain proposition holds under curtain assumptions. But `Prop` it self has meaning of validity as well, that is, a proposition holds without any assumptions. Hence, we could introduce a rule to prove stand alone `Prop` like this.

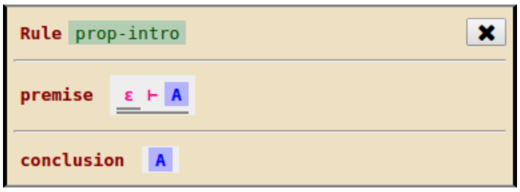
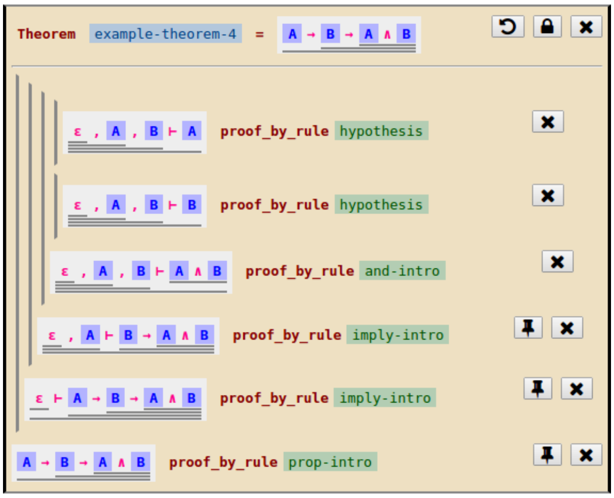


Figure 5.8: Rule that allow to prove `Prop` directly

For example, the following theorem shows that A → B → A ∧ B always holds no matter of what A or B will be



5.6 Context manipulation

Context in Propositional Logic is just a set of assumption so the order and duplication among assumptions shouldn't matter. The three rules below allow context to be manipulated during proving a theorem.

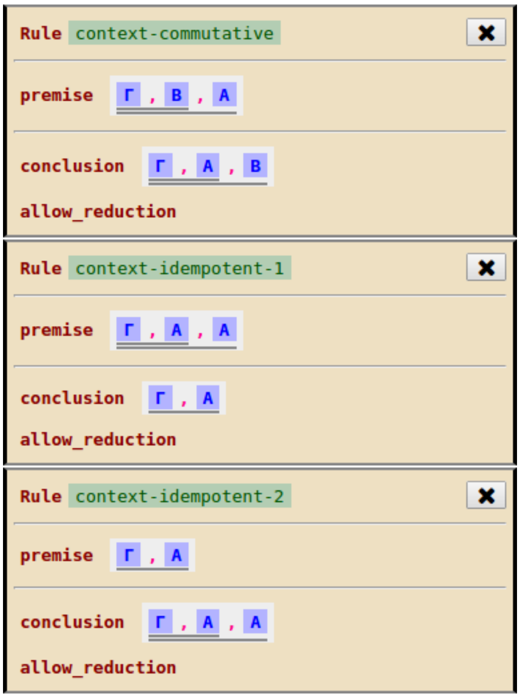


Figure 5.9: Rule for context manipulation

You can TODO:

5.7 How to build Grammars and Rules

So far we introduce grammars and rules out of the box, this allows user to prove a theorem which is the most important part directly. However, Phometa also have ability to create new grammars and rules as well.

To show how these can be built. I will recreate `Prop` for grammars and recreate `and-intro` and `hypothesis` for rules.

The first step, we need to press "Add Grammar" on one of adding panels in module "Propositional Logic", then enter the grammar name. I will use "TutorialProp" to avoid conflict with the real one.

5.8 Exercises

TODO:

Chapter 6

Example Formal System - Lambda Calculus

Since the last two chapters show most of features and usability of *Phometa* already so this chapter aims to show that Phometa is powerful enough as it can even encode more complex formal system like *typed lambda calculus*. Hence, it is clear that Phometa is suitable to encode most of formal system that user can think of.

6.1 Untyped Lambda Calculus

6.2 Simply-typed Lambda Calculus

TODO: don't forget to write about unification (type resolution)

Chapter 7

Specification

In this chapter, we will the full detail of phometa.

7.1 Overview

mainly talk about phometa UI structure, grids, and keymap pane

7.2 Repository

structure of repository

- add new sub-package or module inside a package (using package pane)
- load/save repository using textarea in home pane + also talk about stdlib
- add/swap nodes inside module
- dedicate view for each node (using package pane)

7.3 Node Comment

7.4 Node Grammar

7.5 Root Term

7.6 Input method of a term (TODO: modify this)

7.7 Node Rule

7.8 Node Theorem

Chapter 8

Implementation

This part we will talk about the implementation of phometa which is written in elm hosted at https://github.com/gunpinyo/phometa.

8.1 Decision on programming language

Elm[1] is a functional reactive programming language. It allows programmer to create web application by declaratively coding in Haskell-like language then compile the program to JavaScript. For more information, please see elm official website at elm-lang.org.

One of the most attractive feture of elm is its reactivity. This idea introduces a new data type called "signal" which is a data type that can change over time. For example, let c be a signal of integer defined as $a + b$ where a and b are other signal of integers. If $a = 2$ and $b = 3$, then surely $c = 5$. If later a is change to 4, then c will got automatically updated to 7.

Reactivity work very well with functional paradigm since all variables are immutable, so it is impossible for the program to be in inconsistent state in the sense that programmer forget to update value. In fact, this can lead to a good fit of model-controller-view (MCV) architecture.

Here are summery of reasons why I choose elm to implement phometa,

- Phometa is a web application, and elm is created to build something like this
- Phometa mainly dealing with declarative object, it is better to use funcation language to build it.
- Elm by its very nature, leads to MCV architecture which is good for application like phometa.

8.2 Model-Controller-View Architecture

also talk about phometa modules hierarchy as well

8.3 Modes and Keymap

how modes work and interact with keymap

8.4 Examples of code — Pattern Matching

provide a full explanation of this part of code it is very interesting and small enough to show some aspect of functional programming

8.5 Compilation to Javascript, Html, and Css

8.6 Backend communication, Load / Save repository

8.7 Testing / Continious Integration

Chapter 9

Evaluation

9.1 Users Feedback — discuss with friends

On the 25^{th} of May 2016, it was the first day of project fair where students can demonstrate their work to other students and get a feedback so I went there and discuss about our projects. At this stage, the implementation is finished with Simple Arithmetic and Propositional Logic included in the standard library.

I started showing my project by explaining about Phometa background and Simple Arithmetic using chapter 3 and 4 on this report. Then I asked them do to exercises on chapter 4 by having me as helper. All of them understood Phometa and was able to proof a theorem. Finally, I asked them to try Propositional Logic, some of them really interest but of them didn't want to.

From my observation, all of them were comfortable to proof by clicking options from keymap pane rather than using keyboard shortcut. They also forgot to use searching pattern to select options faster.

There were a few parts of user interface that were not trivial enough, they needed to ask me what to do next, this should be fine if user have time to read whole tutorial.

On the bright side, most of them said that they really like the way that underlines was use to group sub-term rather than brackets (although they needed some time to familiar with it), they also said that the proof is quite easy to read and it will benefit newcomer.

There were several improvements that they suggest. Some of suggestions were easy to change (e.g. theorems should state its goal on header as well) so I changed it already. Some of other suggestions were quite big (e.g. make it mobile friendly and have a proper server) which can be considered as future works. We also managed to find some bugs[1] that I never found before, this gave me an opportunity to fix it in time.

[1]These bug are related Html and CSS rendering i.e. they are not related to Phometa internal.

9.2 Users feedback — discuss with junior students

TODO: Wait until 1^{st} of May.

9.3 Professional Feedback

TODO: I am not sure should I exclude this section or not

9.4 Strengths

- Phometa specification itself is more powerful than traditional derivation system because it has extra features such as cascade premise and meta-level reduction. Thus, be able to support more formal systems than traditional one.
- It has less steep learning curve than mainstream proof assistants because the specification is small enough for user to learn in short time and all of component are diagram based which is easier to understand than sequence of characters.
- If a term can be construct, it is guaranteed to be well form. And if it is a goal of complete theorem (or lemma) it is definitely valid based on soundness on rules on that formal systems.
- The repository of phometa is always in consistent state. Phometa is quite caution when the repository is being modified, for example, theorem can apply only a rule or a lemma that has been locked i.e. it is impossible that its dependencies will be changed, another example is when a node is deleted, phometa will delete all of node that depend on it as well[2]. This is opposite to text-based proof assistants where user have full control over repository, if the repository is in inconsistent, the compiler will rise an error and user can fix it.
- Lemmas allow reuse of proofs so no need for duplication. User can select to do forward style proving (lots of small lemmas as steps of a proof) or backward style proving (a few big theorems).
- It supports unicode input method and doesn't have reserved words so formal system can be constructed in more mathematical friendly environment.
- It is web-application so it can run on any machine that support web browser. One might argue that it required Python for back-end but most of machine support Python out of the box anyway.

[2] Of course, it will ask for confirmation first whether user want delete all of these or not.

9.5 Limitation

- It is hard to extend a formal system at the moment because Phometa doesn't allow grammar to inherit choices from another grammar. If user want to extend a formal system, they need to create a new one from scratch. For example, first order logic cannot be built from an existing propositional logic. If user build grammars of first order logic from scratch, existing propositional logic rules cannot be extended to support first order logic anyway.

- Phometa doesn't support automation well i.e. when user construct a proof, they need to tell which rule or which lemma will be used explicitly. Guessing each step and automating the tree is possible, mainstream proof assistants such as Coq and Isabelle have done it, however, it requires lots of heuristics and cleaver tricks, this is unrealistic to implement due to project time frame but it is good consideration for future work.

- Each web-browser supports different set of keyboard shortcuts. It is very hard for Phometa to find such keystrokes that are not visible characters and not keyboard shortcuts of any web-browser. So I end-up using `Alt` combined with a visible character to create Phometa shortcut. This might have unwanted side effect but at least it work reasonably well with Google Chrome[3] under a condition that the window containing Phometa have only one tab, so it will not suffer from `Alt-1..9` are using for switch tab. However, this is not such a serious problem since user can always click a command in keymap pane directly.

- The entire repository must be loaded into Phometa when it starts. This impacts scalability where repository is large since JavaScript can run out of memory. This is not usually a problem of text-based proof assistants since it verify a theorems one by one and doesn't need to put everything in memory at once.

- Phometa required user to start a local server for individual use. It doesn't have a proper server where user can enter a link use it directly. To implement such a proper server, it requires user accounts and database to manage users repositories, although it is possible to implement but it seems to overkill method and doesn't match project objective, hence it has lower priority than other feature and hasn't been done.

- Directly modify `repository.json` before it is loaded into Phometa could result in undefined behaviour. This is because Phometa currently doesn't have mechanism to verify consistency of repository before it will be loaded. This shouldn't cause any problem if user only interact with repository via Phometa interface and not try to hack repository file directly.

[3] To be precise, Chromium web-browser.

Chapter 10

Conclusion

At the end of this project. Phometa has been designed and been implemented up to the level that is ready to use by anybody with a decent standard library and tutorial. This, in tern, satisfies all of objective stated in introduction chapter. In addition, I also believe that Phometa on this state is a potential replacement for derivation-tree's manually-drawing so people don't have to suffer from it tedious process and error prone anymore.

10.1 Lesson Learnt

Time management for research project is one of many thing that I have learnt during this project. I learnt that tasks are always take time twice or thrice longer than expectation so it is vital to spare plenty of time before the deadline. More importantly, I learnt that better idea of feature always come after we start to implement something. It is quite hard to decide whether Phometa should include some curtain feature or not. It is about a tread off between usefulness of the feature and the risk of the project being not finish in time. This kind of features usually came near the end of implementation where I knew exactly what Phometa should be. This is bad because if I accepted the feature, this would take sometime to implement and edit related part of this report, which in tern, would impact the entire schedule of the plan. So I usually take it as future work as described in next section.

I also learnt to believe in myself being capable to building something I dream of. Formal proof always be my favourite topic since I studied Logic in the first year. One day, I was drawing a derivation tree for a coursework, I had the idea of this project. At the first time it seemed too scary because it is about building a proof assistant from scratch, however after evaluated proof of concept, it turned out to be feasible. So I decide to start it and approached my supervisor.

Most importantly, I learnt many thing regarding to formal proof from this project which is relevant to the topic that I want to do for PhD (Dependent Type Theory). This gave me more familiarity and confident in that field. Oppositely, curiosity on the field motivated me to work on this project better since I know that this kind of knowledge gained during the project will be useful later for sure.

10.2 Future Works

Although Phometa designed and implement up to satisfactory level. There are still plenty of room for improvement as the followng

10.2.1 Make Grammars and Rules extensible

10.2.2 Make proving technique more autometics

10.2.3 Importation between Modules

10.2.4 Copy, Move, and Renaming on Packages and Modules

10.2.5 Export Grammars, Rules and Theorems to LaTeX

10.2.6 Repository Verification on Loading

10.2.7 Adding new Formal Systems to Standard Library

10.2.8 Make Messages become more informative

e.g. if pattern match when applying rule fails, it should tell why it falls

10.2.9 Implement a proper server for Phometa

10.2.10 Make Interface to be more mobile friendly

10.2.11 User preference

Bibliography

[1] Evan Czaplicki et al. *Elm offical website*. http://www.elm-lang.org. [Online; accessed 3-February-2016].

[2] Encyclopedia Britannica. *Formal system*. http://www.britannica.com/topic/formal-system. [Online; accessed 29-January-2016].

[3] University of Cambridge and Technische Universität München. *Isabelle offical website*. http://isabelle.in.tum.de/index.html. [Online; accessed 15-May-2016].

[4] Chalmers and Gothenburg University. *Agda offical website*. http://wiki.portal.chalmers.se/agda/pmwiki.php. [Online; accessed 29-January-2016].

[5] Thierry Coquand. *Thierry Coquand homepage*. http://www.cse.chalmers.se/~coquand. [Online; accessed 29-January-2016].

[6] University of Edinburgh. *Proof General offical website*. http://proofgeneral.inf.ed.ac.uk. [Online; accessed 18-May-2016].

[7] *Homotopy Type Theory Repository*. https://github.com/HoTT/HoTT. [Online; accessed 18-May-2016].

[8] *Homotopy Type Theory Repository — Agda alternative*. https://github.com/HoTT/HoTT-Agda. [Online; accessed 18-May-2016].

[9] Inria. *Coq offical website*. https://coq.inria.fr. [Online; accessed 29-January-2016].

[10] Inria. *CoqIde offical website*. https://coq.inria.fr/cocorico/CoqIde. [Online; accessed 18-May-2016].

[11] Zhaohui Luo. *Computation and Reasoning: A Type Theory for Computer Science*. New York, NY, USA: Oxford University Press, Inc., 1994. ISBN: 0-19-853835-9.

[12] Ulf Norell. “Towards a practical programming language based on dependent type theory”. PhD thesis. SE-412 96 Göteborg, Sweden: Department of Computer Science and Engineering, Chalmers University of Technology, Sept. 2007.

[13] Wikipedia. *Curry Howard correspondence*. https://en.wikipedia.org/wiki/Curry-Howard_correspondence. [Online; accessed 29-January-2016].

[14] Wikipedia. *Formal system*. https://en.wikipedia.org/wiki/Formal_system. [Online; accessed 29-January-2016].