Matita V0.5.9 User Manual (rev. 0.5.9)

COLLABORATORS

	TITLE : Matita V0.5.9 User Manual (rev. 0.5.9)	

ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Andrea Asperti, Claudio Sacerdoti Coen, Ferruccio Guidi, Enrico Tassi, and Stefano Zacchiroli	December 23, 2014	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME
0.5.9	12/07/2006		

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Features

Matita is an interactive theorem prover (or proof assistant) with the following characteristics:

- It is based on a variant of the Calculus of (Co)Inductive Constructions (CIC). CIC is also the logic of the Coq proof assistant.
- It adopts a procedural proof language, but it has a new set of small step tacticals that improve proof structuring and debugging.
- It has a stand-alone graphical user interface (GUI) inspired by CtCoq/Proof General. The GUI is implemented according to the state of the art. In particular:
  - It is based and fully integrated with Gtk/Gnome.
  - An on-line help can be browsed via the Gnome documentation browser.
  - Mathematical formulae are rendered in two dimensional notation via MathML and Unicode.
- It integrates advanced browsing and searching procedures.
- It allows the use of the typical ambiguous mathematical notation by means of a disambiguating parser.
- It is compatible with the library of Coq (definitions and proof objects).

1.2 Matita vs Coq

The system shares a common look&feel with the Coq proof assistant and its graphical user interface. The two systems have the same logic, very close proof languages and similar sets of tactics. Moreover, Matita is compatible with the library of Coq. From the user point of view the main lacking features with respect to Coq are:

- proof extraction;
- an extensible language of tactics;
- automatic implicit arguments;
- several ad-hoc decision procedures;
- several rarely used variants for most of the tactics;
- sections and local variables. To maintain compatibility with the library of Coq, theorems defined inside sections are abstracted by name over the section variables; their instances are explicitly applied to actual arguments by means of explicit named substitutions.

Still from the user point of view, the main differences with respect to Coq are:

- the language of tacticals that allows execution of partial tactical application;
- the unification of the concept of metavariable and existential variable;
- terms with subterms that cannot be inferred are always allowed as arguments of tactics or other commands;
- ambiguous terms are disambiguated by direct interaction with the user;
- theorems and definitions in the library are always accessible without needing to require/include them; right now, only notation needs to be included to become active, but we plan to remove this limitation.

Chapter 2

Installation

Matita is a quite complex piece of software, we thus recommend you to either install al precompiled version or use the LiveCD. If you are running Debian GNU/Linux (or one of its derivatives like Ubuntu), you can install matita typing

```
aptitude install matita matita-standard-library
```

If you are running MacOSX or Windows, give the LiveCD a try before trying to compile Matita from its sources.

2.1 Using the LiveCD

In the following, we will assume you have installed virtualbox for your platform and downloaded the .iso image of the LiveCD

2.1.1 Creating the virtual machine

Click on the New button, a wizard will popup, you should ask to its questions as follows

1. The name should be something like Matita, but can be any meaningful string.
2. The OS type should be Debian
3. The base memory size can be 256 mega bytes, but you may want to increase it if you are going to work with huge formalizations.
4. The boot hard disk should be no hard disk. It may complain that this choice is not common, but it is right, since you will run a LiveCD you do not need to emulate an hard drive.

Now that you are done with the creation of the virtual machine, you need to insert the LiveCD in the virtual cd reader unit.

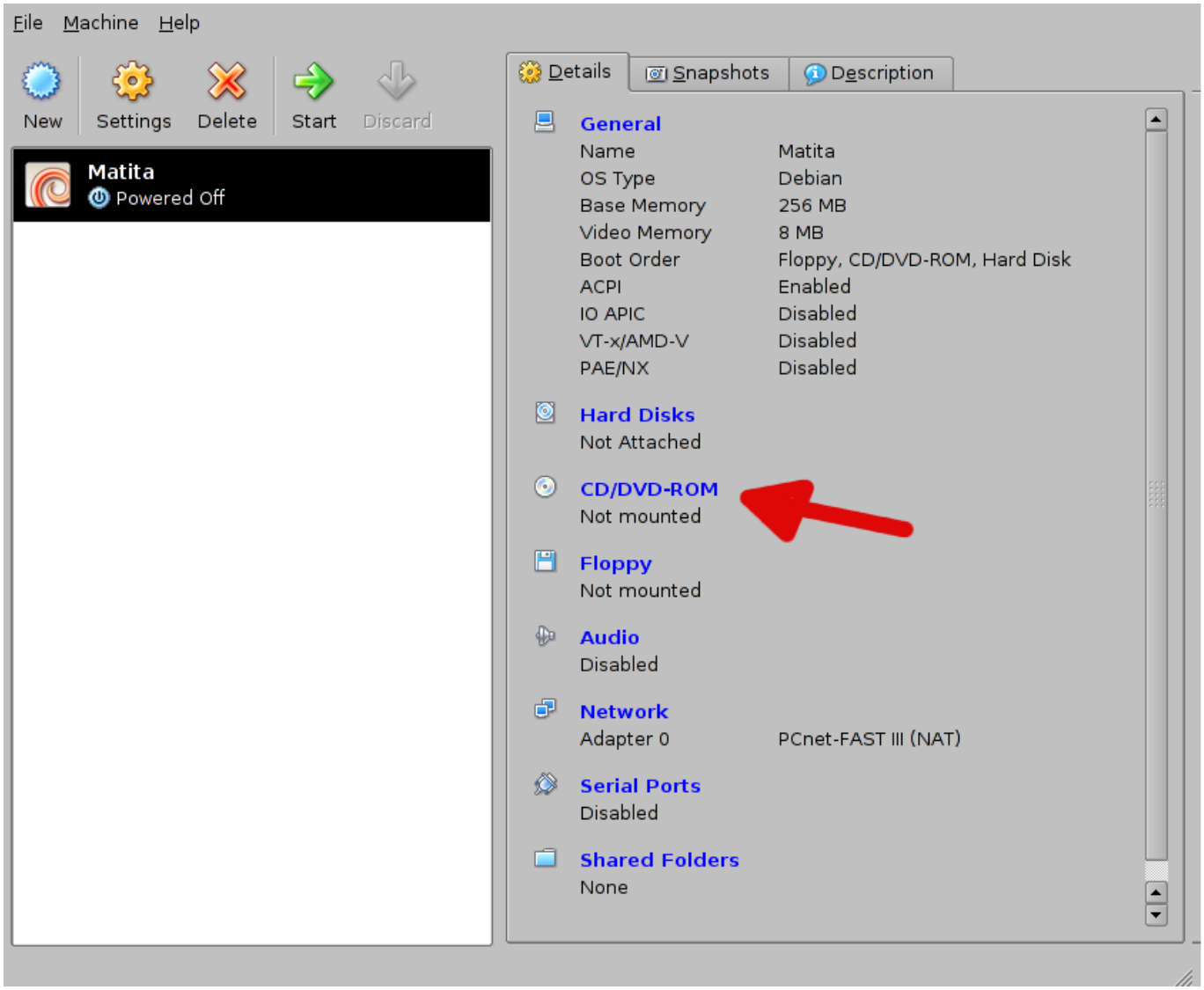

Figure 2.1: The brand new virtual machine

Click on CD/DVD-ROM (that should display something like: Not mouted). Then click on mount CD/DVD drive and select the ISO image option. The combo-box should display no available image, you need to add the ISO image you downloaded from the Matita website clicking on the button near the combo-box. to start the virtual machine.

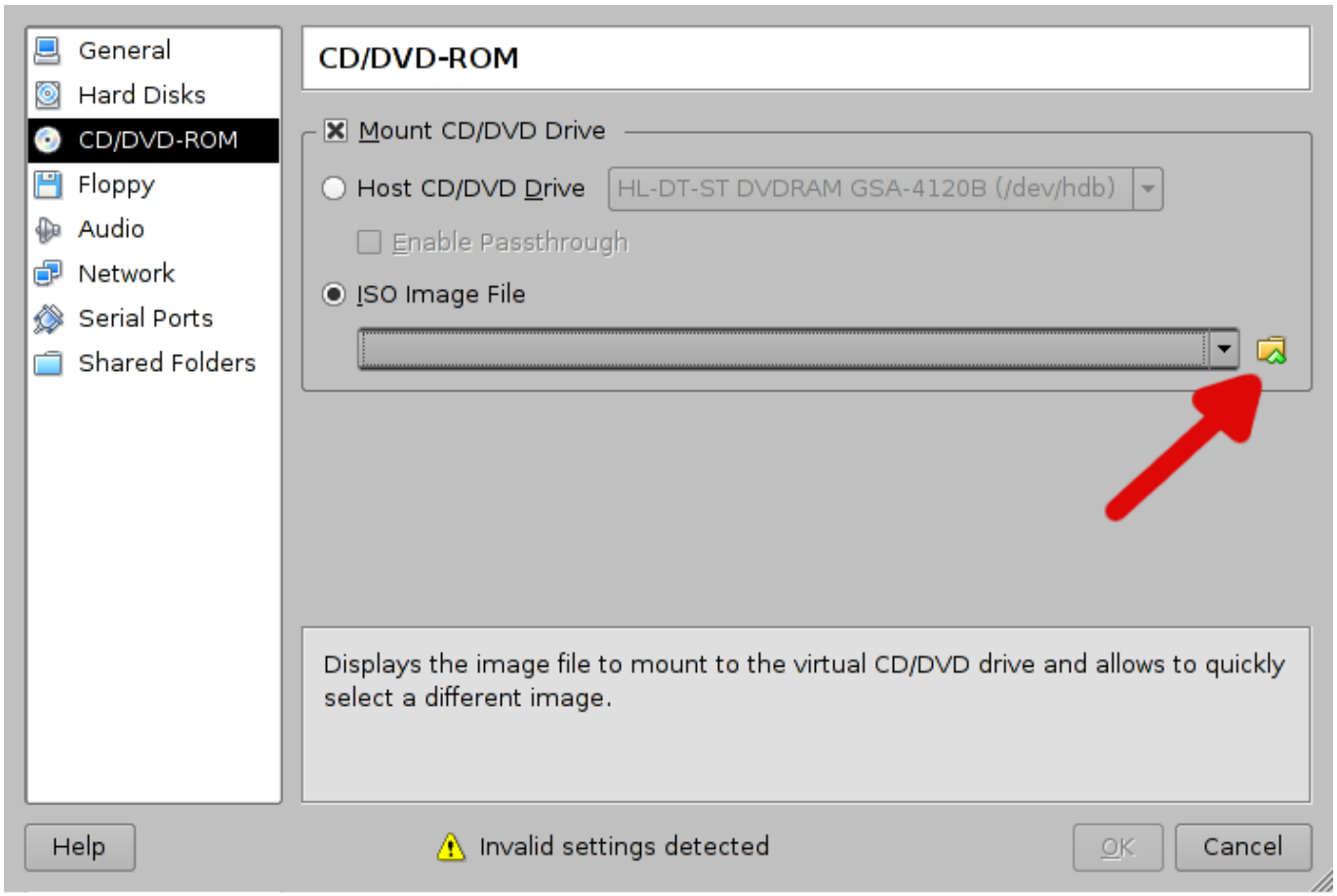

Figure 2.2: Mounting an ISO image

In the newely opened window click the Add button

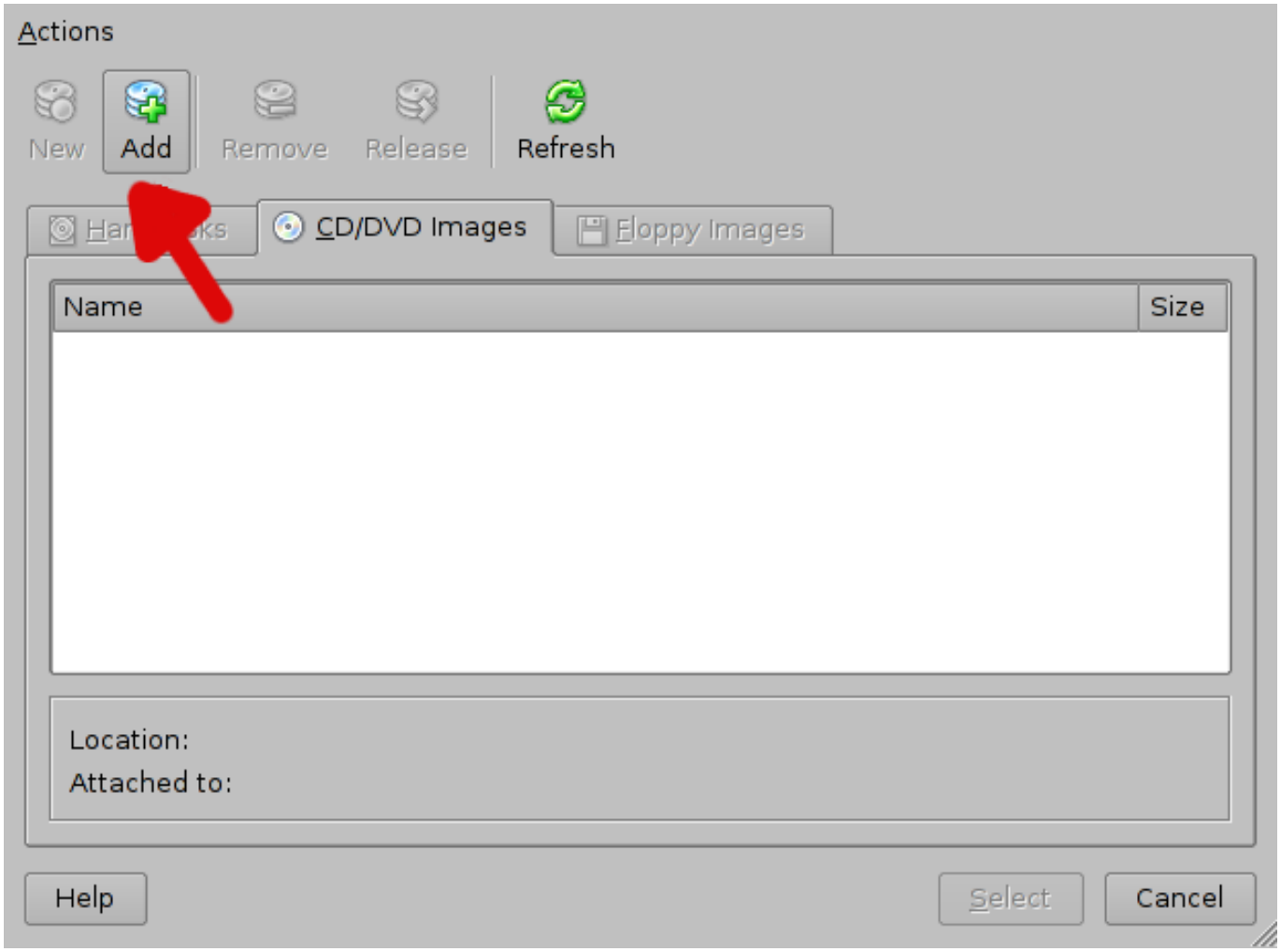

Figure 2.3: Choosing the ISO image

A new windows will pop-up: choose the file you downloaded (usually matita-version.iso) and click open.

Figure 2.4: Choosing the ISO image

Now select the new entry you just added as the CD image you want to insert in the virtual CD drive. You are now ready to start the virtual machine.

2.1.2 Sharing files with the real PC

The virtual machine Matita will run on, has its own file system, that is completely separated from the one of your real PC (thus your files are not available in the emulated environment) and moreover it is a non-presistent file system (thus you data is lost every time you turn off the virtual machine).

Virtualbox allows you to share a real folder (beloging to your real PC) with the emulated computer. Since this folder is persistent, you are encouraged to put your work there, so that it is not lost when the virtual machine is powered off.

The first step to set up a shared folder is to click on the shared folder configuration entry of the virtual machine.

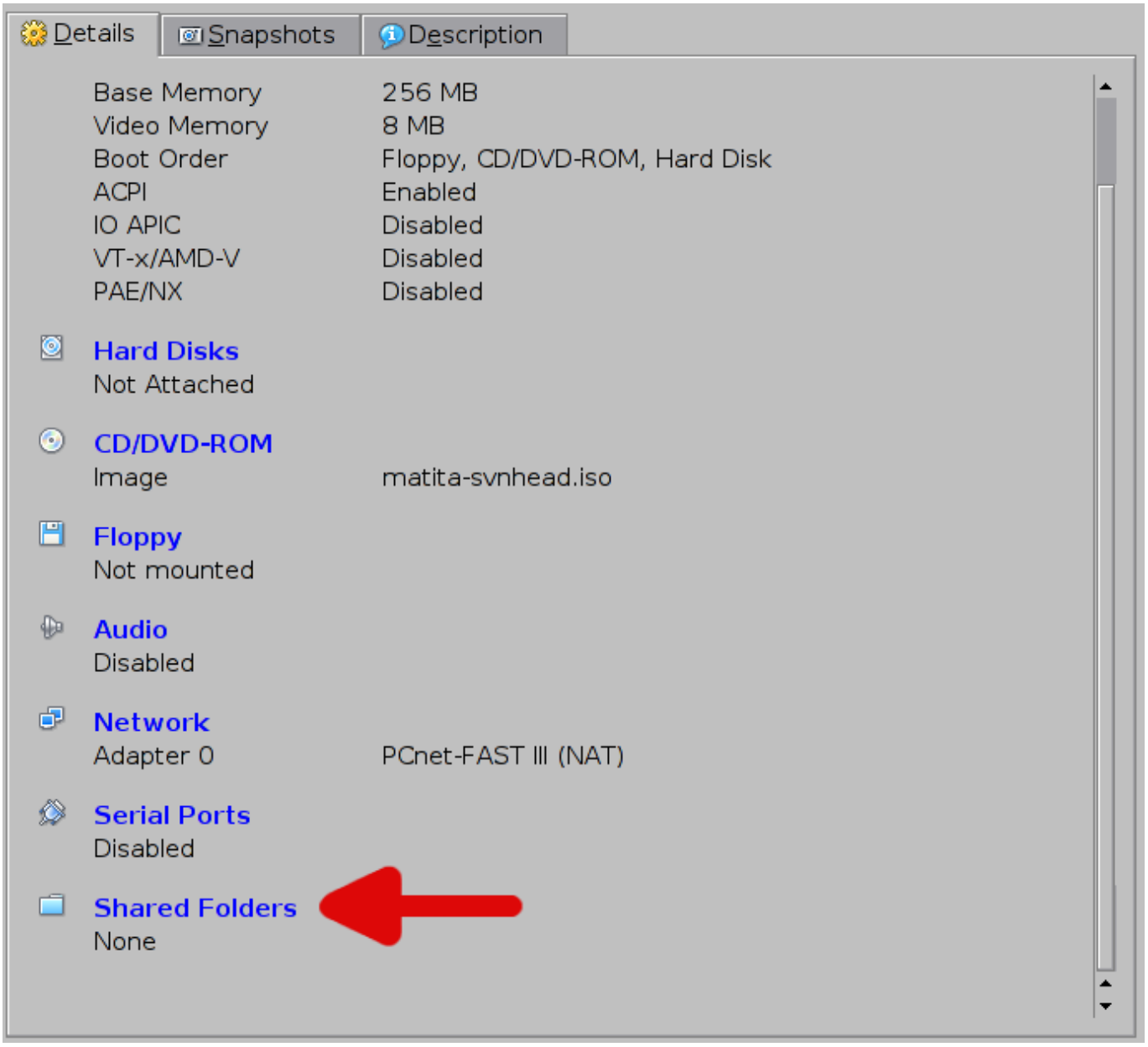

Figure 2.5: Set up a shared folder

Then you shuld add a shared folder clicking on the plus icon on the right

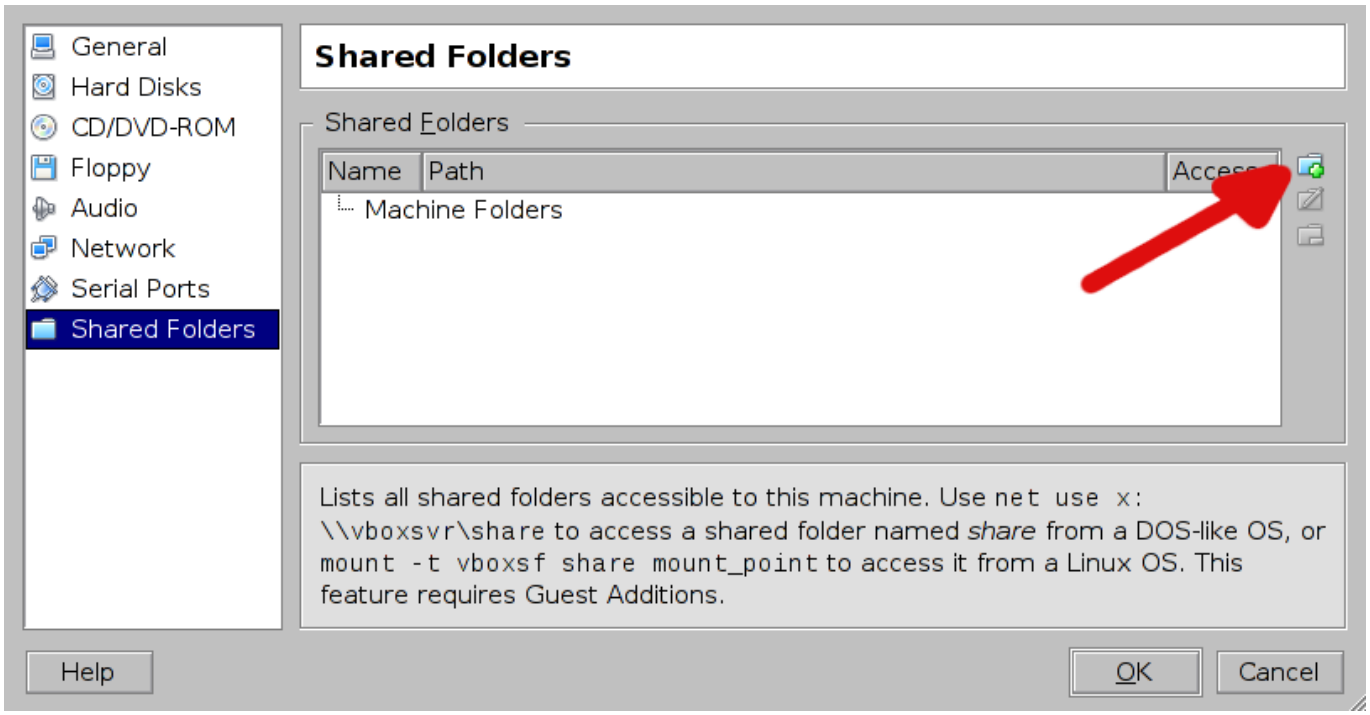

Figure 2.6: Choosing the folder to share

Then you have to specify the real PC folder you want to share and name it. A reasonable folder to share is /home on a standard Unix system, while /Users on MaxOSX. The name you give to the share is important, you should remember it.

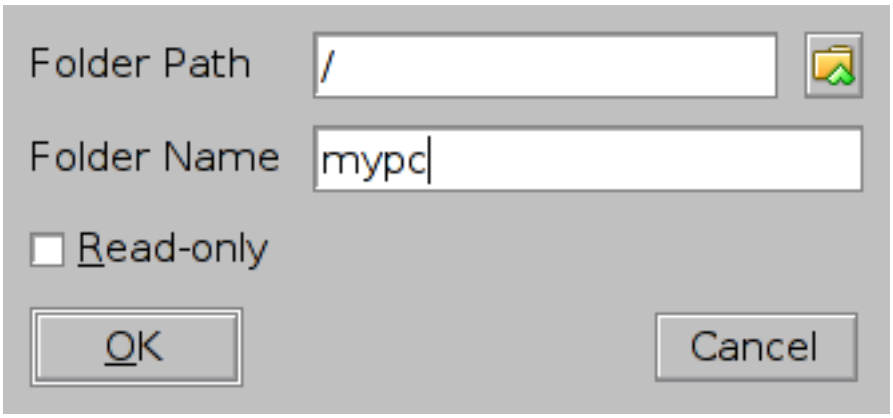

Figure 2.7: Naming the shared folder

Once your virtual machine is up and running, you can mount (that meand have access to) the shared folder by clicking on the Mount VirtualBox share icon, and typing the name of the share.

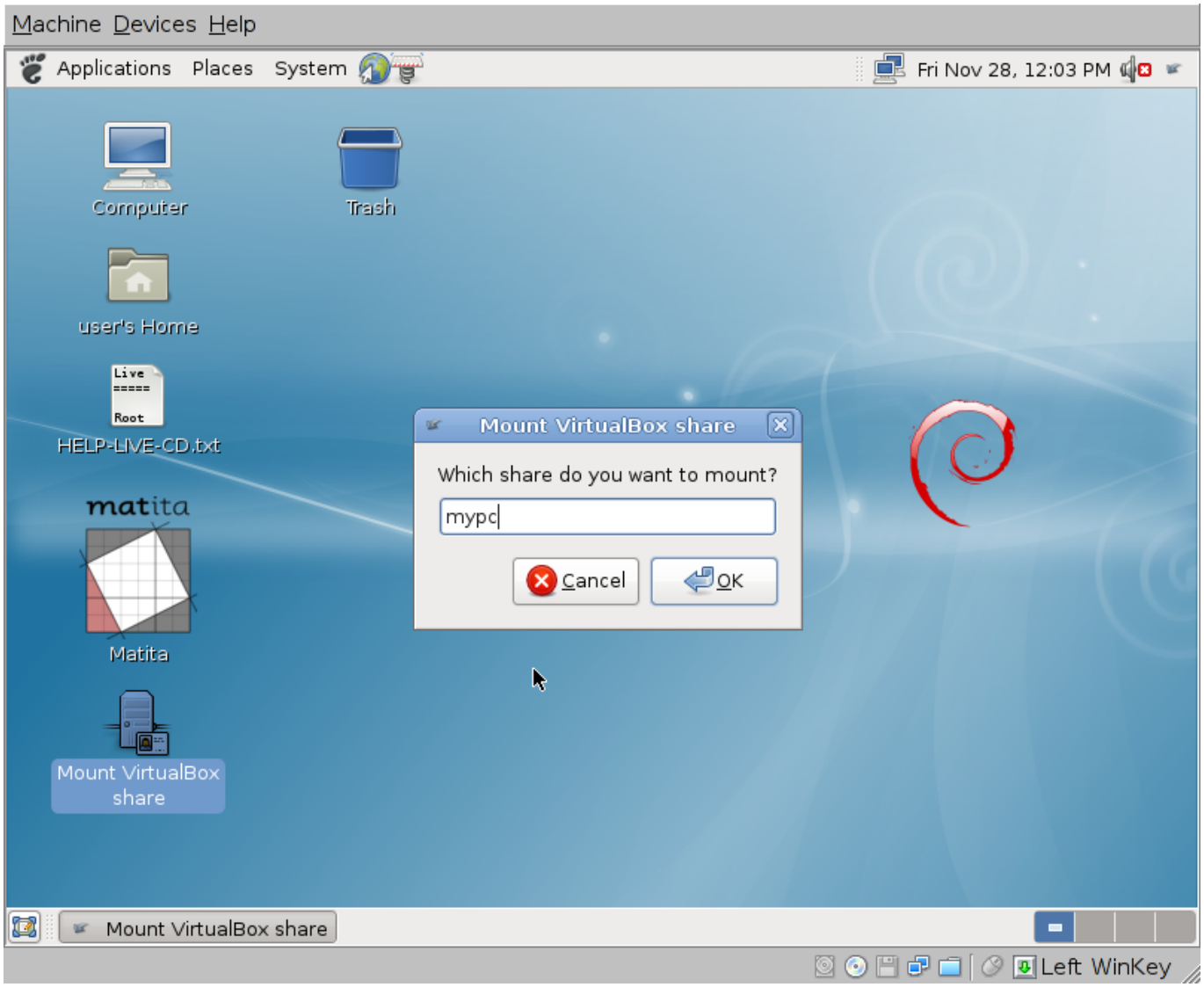

Figure 2.8: Using it from the virtual machine

A window will then pop-up, and its content will be the the content of the real PC folder.

2.2 Installing from sources

Install Matita from the sources is hard, you have been warned!

2.2.1 Getting the source code

You can get the Matita source code in two ways:

1. go to the download page and get the latest released source tarball;
2. get the development sources from our SVN repository. You will need the components/ and matita/ directories from the `trunk/helm/software/` directory, plus the `configure` and `Makefile*` stuff from the same directory.

   In this case you will need to run **autoconf** before proceding with the building instructions below.

2.2.2 Requirements

In order to build Matita from sources you will need some tools and libraries. They are listed below.

Note for Debian (and derivatives) users
If you are running a Debian GNU/Linux distribution, or any of its derivative like Ubuntu, you can use APT to install all the required tools and libraries since they are all part of the Debian archive.
apt-get install ocaml ocaml-findlib libgdome2-ocaml-dev liblablgtk2-ocaml-dev liblablgtkmathview-ocaml-dev liblablgtksourceview-ocaml-dev libsqlite3-ocaml-dev libocamlnet-ocaml-dev libzip-ocaml-dev libhttp-ocaml-dev ocaml-ulex08 libexpat-ocaml-dev libmysql-ocaml-dev camlp5
An official debian package is going to be added to the archive too.

REQUIRED TOOLS AND LIBRARIES

OCaml the Objective Caml compiler, version 3.09 or above

Findlib OCaml package manager, version 1.1.1 or above

OCaml Expat OCaml bindings for the expat library

GMetaDOM OCaml bindings for the Gdome 2 library

OCaml HTTP OCaml library to write HTTP daemons (and clients)

LablGTK OCaml bindings for the GTK+ library , version 2.6.0 or above

GtkMathView , LablGtkMathView GTK+ widget to render MathML documents and its OCaml bindings

GtkSourceView , LablGtkSourceView extension for the GTK+ text widget (adding the typical features of source code editors) and its OCaml bindings

MySQL , OCaml MySQL SQL database and OCaml bindings for its client-side library
The SQL database itself is not strictly needed to run Matita, but the client libraries are.

Sqlite , OCaml Sqlite3 Sqlite database and OCaml bindings

Ocamlnet collection of OCaml libraries to deal with application-level Internet protocols and conventions

ulex Unicode lexer generator for OCaml

CamlZip OCaml library to access `.gz` files

2.2.3 (optional) MySQL setup

To fully exploit Matita indexing and search capabilities on a huge metadata set you may need a working MySQL database. Detalied instructions on how to do it can be found in the MySQL documentation. Here you can find a quick howto.

In order to create a database you need administrator permissions on your MySQL installation, usually the root account has them. Once you have the permissions, a new database can be created executing **`mysqladmin create matita`** (*matita* is the default database name, you can change it using the `db.user` key of the configuration file).

Then you need to grant the necessary access permissions to the database user of Matita, typing **`echo "grant all privileges on matita.* to helm;" | mysql matita`** should do the trick (*helm* is the default user name used by Matita to access the database, you can change it using the `db.user` key of the configuration file).

Note
This way you create a database named *matita* on which anyone claiming to be the *helm* user can do everything (like adding dummy data or destroying the contained one). It is strongly suggested to apply more fine grained permissions, how to do it is out of the scope of this manual.

2.2.4 Compiling and installing

Once you get the source code the installations steps should be quite familiar.

First of all you need to configure the build process executing **`./configure`**. This will check that all needed tools and library are installed and prepare the sources for compilation and installation.

Quite a few (optional) arguments may be passed to the configure command line to change build time parameters. They are listed below, together with their default values:

CONFIGURE COMMAND LINE ARGUMENTS

**`--with-runtime-dir=`*`dir`* (*Default:* `/usr/local/matita`) Runtime base directory where all Matita stuff (executables, configuration files, standard library, ...) will be installed

**`--with-dbhost=`*`host`* (*Default:* localhost) Default SQL server hostname. Will be used while building the standard library during the installation and to create the default Matita configuration. May be changed later in configuration file.

`--enable-debug` (*Default:* disabled) Enable debugging code. Not for the casual user.

Then you will manage the build and install process using make as usual. Below are reported the targets you have to invoke in sequence to build and install:

MAKE TARGETS

`world` builds components needed by Matita and Matita itself (in bytecode or native code depending on the availability of the OCaml native code compiler)

`install` installs Matita related tools, standard library and the needed runtime stuff in the proper places on the filesystem.

As a part of the installation process the Matita standard library will be compiled, thus testing that the just built matitac compiler works properly.

For this step you will need a working SQL database (for indexing the standard library while you are compiling it). See Database setup for instructions on how to set it up.

2.3 Configuring Matita

The configuration file is divided in four sections. The user and matita ones are self explicative and does not need user intervention. Here we report a sample snippet for these two sections. The remaining db and getter sections will be explained in details later.

```
<section name="user">
  <key name="home">$(HOME)</key>
  <key name="name">$(USER)</key>
</section>
<section name="matita">
  <key name="basedir">$(user.home)/.matita</key>
  <key name="rt_base_dir">/usr/share/matita/</key>
  <key name="owner">$(user.name)</key>
</section>
```

Matita needs to store/fetch data and metadata. Data is essentially composed of XML files, metadata is a set of tuples for a relational model. Data and metadata can produced by the user or be already available. Both kind of data/metadata can be local and/or remote.

The db section tells Matita where to store and retrieve metadata, while the getter section describes where XML files have to be found. The following picture describes the suggested configuration. Dashed arrows are determined by the configuration file.

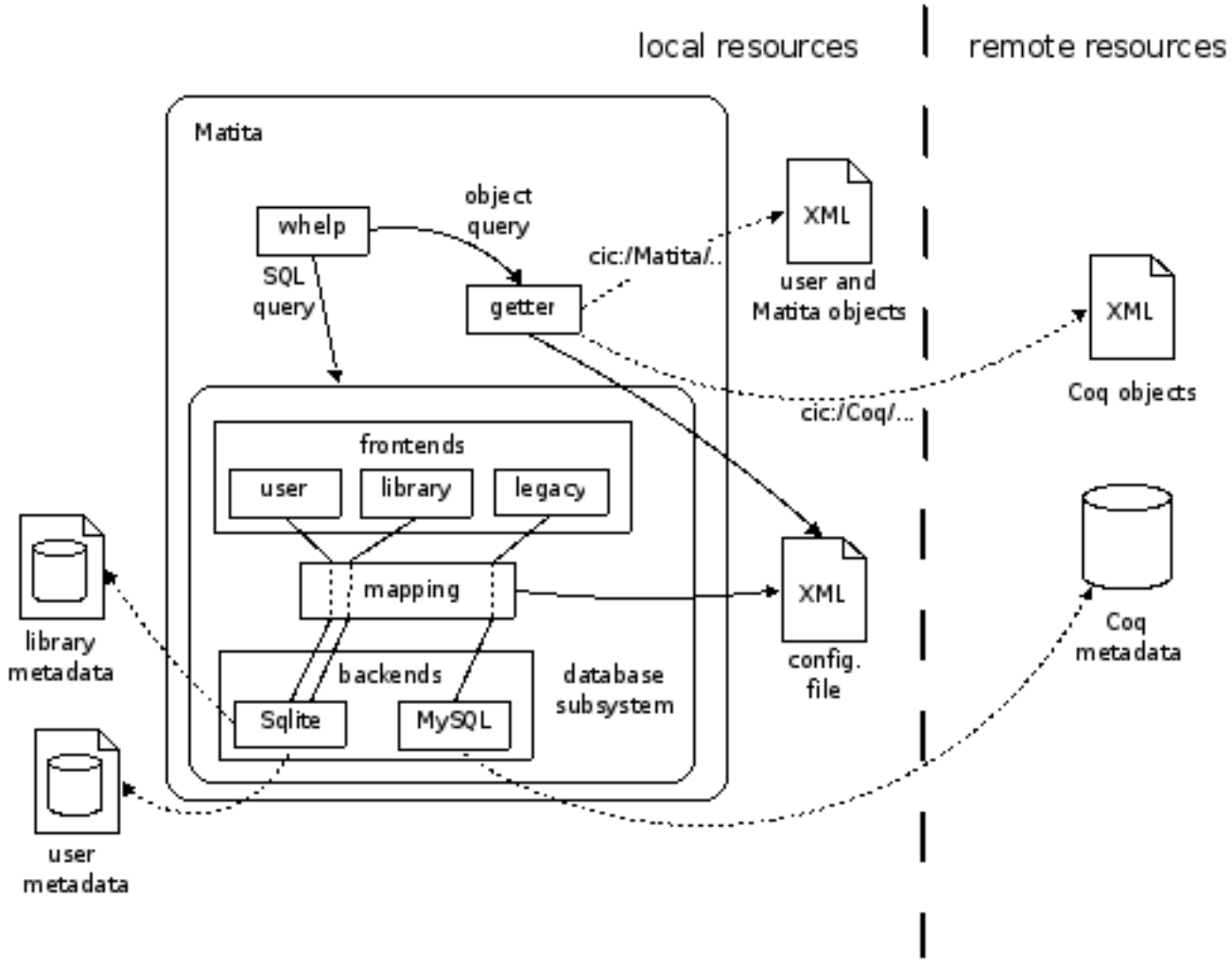

Figure 2.9: Configuring the Databases

The getter

Consider the following snippet and the URI **cic:/matita/foo/bar.con**. If Matita is asked to read that object it will resolve the object trough the getter. Since the first two entries are equally specific (longest match rule applies) first the path **file://$(matita.rt_base_dir)/xml/standard-library/foo/bar.con** and then **file://$(user.home)/.ma** are inspected.

```
<section name="getter">
  <key name="cache_dir">$(user.home)/.matita/getter/cache</key>
  <key name="prefix">
    cic:/matita/
    file://$(matita.rt_base_dir)/xml/standard-library/
    ro
  </key>
  <key name="prefix">
    cic:/matita/
    file://$(user.home)/.matita/xml/matita/
  </key>
  <key name="prefix">
    cic:/Coq/
    http://mowgli.cs.unibo.it/xml/
    legacy
```

```
    </key>
  </section>
```

if the same URI has to be written, the former prefix is skipped since it is marked as readonly (**ro**). Objects resolved using the third prefix are readonly too, and are retrieved using the network. There is no limit to the number of prefixes the user can define. The distinction between prefixes marked as readonly and legacy is that, legacy ones are really read only, while the ones marked with **ro** are considered for writing when Matita is started in system mode (used to publish user developments in the library space).

The db

The database subsystem has three fron ends: library, user and legacy. The latter is the only optional one. Every query is done on every frontend, making the duplicate free union of the results. The user front end kepps metadata produced by the user, and is thus heavily accessed in read/write mode, while the library and legacy fron ends are read only. Every front end can be connected to backend, the storage actually. Consider the following snippet.

```
<section name="db">
  <key name="metadata">mysql://mowgli.cs.unibo.it matita helm none legacy</key>
  <key name="metadata">file://$(matita.rt_base_dir) metadata.db helm helm library</key>
  <key name="metadata">file://$(matita.basedir) user.db helm helm user</key>
</section>
```

Here the usr database is a file (thus locally accessed trough the Sqlite library) placed in the user's home directory. The library one is placed in the Matita runtime directory. The legacy fron end is connected to a remote MySQL based storage. Every metadata key takes a path to the storage, the name of the database, the user name, a password (or **none**) and the name of the front end to which it is attached.

Chapter 3

Getting started

If you are already familiar with the Calculus of (Co)Inductive Constructions (CIC) and with interactive theorem provers with procedural proof languages (expecially Coq), getting started with Matita is relatively easy. You just need to learn how to type Unicode symbols, how to browse and search the library and how to author a proof script.

3.1 How to type Unicode symbols

Unicode characters can be typed in several ways:

- Using the "Ctrl+Shift+Unicode code" standard Gnome shortcut. E.g. Ctrl+Shift+3a9 generates "Ω".
- Typing the ligature "\name" where "name" is a standard Unicode or LaTeX name for the character or an ASCII art resembling the shape of the character. Pressing "Alt+L" or Space or Enter just after the last character of the name converts the ligature to the Unicode symbol. E.g. "\Delta" followed by Alt+L generates "Δ", while pressing Alt-L after "=>" generates "⇒"
- Typing a symbol and rotating trough its equivalence class with Alt-L. E.g. pressing Alt-L after an "l" generates a "λ", while pressing Alt-L after an "→" once generates "⇉" and pressing Alt-L again generates "⇒".

The comprehensive list of symbols names or shortcuts and their equivalence classes is available clicking on the "TeX/UTF-8 table" item of the "View" menu.

There is a memory mechanism related to equivalence classes that remembers your last choice, making it the default one. For example, if you use "_" to generate "⎻" (that is the third choice, after "⎽" and "⎼"), the next time you type Alt-L after "_" you immediately get "⎻".

3.2 Browsing and searching

The CIC browser is used to browse and search the library. You can open a new CIC browser selecting "New Cic Browser" from the "View" menu of Matita, or by pressing "F3". The CIC browser is similar to a traditional Web browser.

3.2.1 Browsing the library

To browse the library, type in the location bar the absolute URI of the theorem, definition or library fragment you are interested in. "cic:/" is the root of the library. Contributions developed in Matita are under "cic:/matita"; all the others are part of the library of Coq.

Following the hyperlinks it is possible to navigate in the Web of mathematical notions. Proof are rendered in pseudo-natural language and mathematical notation is used for formulae. For now, mathematical notation must be included in the current script to be activated, but we plan to remove this limitation.

3.2.2 Looking at a proof under development

A proof under development is not yet part of the library. The special URI "about:proof" can be used to browse the proof currently under development, if there is one. The "home" button of the CIC browser sets the location bar to "about:proof".

3.2.3 Searching the library

The query bar of the CIC browser can be used to search the library of Matita for theorems or definitions that match certain criteria. The criteria is given by typing a term in the query bar and selecting an action in the drop down menu right of it.

3.2.3.1 Searching by name

TODO

3.2.3.2 List of lemmas that can be applied

TODO

3.2.3.3 Searching by exact match

TODO

3.2.3.4 List of elimination principles for a given type

TODO

3.2.3.5 Searching by instantiation

TODO

3.3 Authoring

3.3.1 How to compile a script

Scripts are compiled to base URIs. Base URIs are of the form "cic:/matita/path" and are given once for all for a set of scripts using the "root" file.

A "root" file has to be placed in the root of a script set, for example, consider the following files and directories, and assume you keep files in "list" separated from files in "sort" (for example the former directory may contain functions and proofs about lists, while latter sorting algorithms for lists):

```
list/
  list.ma (* depending just on the standard library *)
  utils/
    swap.ma (* including list.ma *)
sort/
  qsort.ma (* including utils/swap.ma *)
```

To be able to compile properly the contents of "list" a file called root has to be placed in it. The file should be like the following snippet.

```
baseuri=cic:/matita/mydatastructures
```

This file tells Matita that objects generated by "list.ma" have to be placed in "cic:/matita/mydatastructures/list" while objects generated by "swap.ma" have to be placed in "cic:/matita/mydatastructures/utils/swap".

Once you created the root file, you must generate a depend file. Enter the "list" directory (the root of yuor file set) and type "matitadep". Remember to regenerate the depend file every time you alter the dependencies of your files (for example including other scripts). You can now compile you files typing "matitac".

To compile the "sort" directory, create a root file in "sort/" like the following one and then run "matitadep".

```
baseuri=cic:/matita/myalgorithms
include_paths=../list
```

The include_paths field can declare a list of paths separated by space. Please omit any "/" from the end of base URIs or paths.

3.3.2 The authoring interface

TODO

Chapter 4

Syntax

To describe syntax in this manual we use the following conventions:

1. Non terminal symbols are emphasized and have a link to their definition. E.g.: *term*
2. Terminal symbols are in bold. E.g.: **theorem**
3. Optional sequences of elements are put in square brackets. E.g.: [**in** *term*]
4. Alternatives are put in square brakets and they are separated by vertical bars. E.g.: [**<|>**]
5. Repetitions of a sequence of elements are given by putting the sequence in square brackets, that are followed by three dots. The empty sequence is a valid repetition. E.g.: [**and** *term*]...
6. Characters belonging to a set of characters are given by listing the set elements in square brackets. Hyphens are used to specify ranges of characters in the set. E.g.: [**a-zA-Z0-9_-**]

4.1 Terms & co.

4.1.1 Lexical conventions

qstring	::=	**"**⟨⟨*any sequence of characters excluded "*⟩⟩**"**

Table 4.1: qstring

id	::=	⟨⟨*any sequence of letters, underscores or valid XML digits prefixed by a latin letter ([a-zA-Z]) and post-fixed by a possible empty sequence of decorators ([?``])*⟩⟩

Table 4.2: id

nat	::=	⟨⟨*any sequence of valid XML digits*⟩⟩

Table 4.3: nat

char	::=	[**a-zA-Z0-9_-**]

Table 4.4: char

uri-step	::=	*char*[*char*]...

Table 4.5: uri-step

uri	::=	[**cic:/**|**theory:/**]*uri-step*[**/***uri-step*]....*id*[**.***id*]... [**#xpointer(***nat***/***nat*[**/***nat*]...)]

Table 4.6: uri

csymbol	::=	**'***id*

Table 4.7: csymbol

symbol	::=	⟨⟨**None of the above**⟩⟩

Table 4.8: symbol

term	::=	*sterm*	simple or delimited term
	|	*term term*	application
	|	λ*args***.***term*	λ-abstraction
	|	Π*args***.***term*	dependent product meant to define a datatype
	|	$\forall$*args***.***term*	dependent product meant to define a proposition
	|	*term* $\rightarrow$ *term*	non-dependent product (logical implication or function space)
	|	**let** [*id*|(*id***:** *term*)] $\stackrel{def}{=}$ *term* **in** *term*	local definition
	|	**let** [**co**]**rec** *rec_def* [**and** *rec_def*]... **in** *term*	(co)recursive definitions
	|	...	user provided notation
rec_def	::=	*id* [*id*|_|(*id*[**,***id*]... **:***term***)**]... [**on** *id*] [**:** *term*] $\stackrel{def}{=}$ *term*]	

Table 4.9: Terms

sterm	::=	(*term*)	
	|	*id*[**\subst[** *id***:=***term* [**;***id***:=***term*]...]]	identifier with optional explicit named substitution
	|	*uri*	a qualified reference
	|	**Prop**	the impredicative sort of propositions
	|	**Set**	the impredicate sort of datatypes
	|	**CProp**	one fixed predicative sort of constructive propositions
	|	**Type**	one predicative sort of datatypes
	|	**?**	implicit argument
	|	**?n** [[[_|*term*]...]]	metavariable
	|	**match** *term* [**in** *id*] [**return** *term*] **with** [*match_branch*[|*match_branch*]...]	case analysis
	|	(*term***:***term*)	cast
	|	...	user provided notation at precedence 90

Table 4.10: Simple terms

args	::=	_[**:** *term*]	ignored argument
	|	(_[**:** *term*])	ignored argument
	|	*id*[**,***id*]... [**:** *term*]	
	|	(*id*[**,***id*]... [**:** *term*])	
args2	::=	*id*	
	|	(*id*[**,***id*]... **:** *term*)	

Table 4.11: Arguments

match_branch	::=	*match_pattern* ⇒ *term*	
match_pattern	::=	*id*	0-ary constructor
	|	(*id id* [*id*]...)	n-ary constructor (binds the n arguments)
	|	*id id* [*id*]...	n-ary constructor (binds the n arguments)
	|	_	any remaining constructor (ignoring its arguments)

Table 4.12: Pattern matching

4.1.2 Terms

4.2 Definitions and declarations

4.2.1 axiom *id*: *term*

```
axiom H: P
```

H is declared as an axiom that states **P**

4.2.2 definition *id*[: *term*] [$\stackrel{def}{=}$ *term*]

```
definition f:  T ≝ t
```

f is defined as **t**; **T** is its type. An error is raised if the type of **t** is not convertible to **T**.

T is inferred from **t** if omitted.

t can be omitted only if **T** is given. In this case Matita enters in interactive mode and **f** must be defined by means of tactics.

Notice that the command is equivalent to **theorem f: T** $\stackrel{def}{=}$ **t**.

4.2.3 letrec *TODO*

TODO

4.2.4 [inductive|coinductive] *id* [*args2*]... : *term* $\stackrel{def}{=}$ [|] [*id*:*term*] [| *id*:*term*]... [with *id* : *term* $\stackrel{def}{=}$ [|] [*id*:*term*] [| *id*:*term*]...]...

```
inductive i x y z:  S ≝ k1:T1 | ...  | kn:Tn with i' :  S' ≝ k1':T1' | ...  | km':Tm'
```

Declares a family of two mutually inductive types **i** and **i'** whose types are **S** and **S'**, which must be convertible to sorts.

The constructors **ki** of type **Ti** and **ki'** of type **Ti'** are also simultaneously declared. The declared types **i** and **i'** may occur in the types of the constructors, but only in strongly positive positions according to the rules of the calculus.

The whole family is parameterized over the arguments **x,y,z**.

If the keyword **coinductive** is used, the declared types are considered mutually coinductive.

Elimination principles for the record are automatically generated by Matita, if allowed by the typing rules of the calculus according to the sort **S**. If generated, they are named **i_ind**, **i_rec** and **i_rect** according to the sort of their induction predicate.

4.2.5 record *id* [*args2*]... : *term* $\stackrel{def}{=}${[*id* [:|:>] *term*] [;*id* [:|:>] *term*]...}

```
record id x y z:  S ≝ { f1:  T1; ...; fn:Tn }
```

Declares a new record family **id** parameterized over **x,y,z**.

S is the type of the record and it must be convertible to a sort.

Each field **fi** is declared by giving its type **Ti**. A record without any field is admitted.

Elimination principles for the record are automatically generated by Matita, if allowed by the typing rules of the calculus according to the sort **S**. If generated, they are named **i_ind**, **i_rec** and **i_rect** according to the sort of their induction predicate.

For each field **fi** a record projection **fi** is also automatically generated if projection is allowed by the typing rules of the calculus according to the sort **S**, the type **T1** and the definability of depending record projections.

If the type of a field is declared with **:>**, the corresponding record projection becomes an implicit coercion. This is just syntactic sugar and it has the same effect of declaring the record projection as a coercion later on.

4.3 Proofs

4.3.1 theorem *id*[: *term*] [$\stackrel{def}{=}$ *term*]

`theorem f: P` $\stackrel{def}{=}$ `p`

Proves a new theorem **f** whose thesis is **P**.

If **p** is provided, it must be a proof term for **P**. Otherwise an interactive proof is started.

P can be omitted only if the proof is not interactive.

Proving a theorem already proved in the library is an error. To provide an alternative name and proof for the same theorem, use **variant f: P** $\stackrel{def}{=}$ **p**.

A warning is raised if the name of the theorem cannot be obtained by mangling the name of the constants in its thesis.

Notice that the command is equivalent to **definition f: T** $\stackrel{def}{=}$ **t**.

4.3.2 variant *id*: *term* $\stackrel{def}{=}$ *term*

`variant f: T` $\stackrel{def}{=}$ `t`

Same as **theorem f: T** $\stackrel{def}{=}$ **t**, but it does not complain if the theorem has already been proved. To be used to give an alternative name or proof to a theorem.

4.3.3 lemma *id*[: *term*] [$\stackrel{def}{=}$ *term*]

`lemma f: T` $\stackrel{def}{=}$ `t`

Same as **theorem f: T** $\stackrel{def}{=}$ **t**

4.3.4 fact *id*[: *term*] [$\stackrel{def}{=}$ *term*]

`fact f: T` $\stackrel{def}{=}$ `t`

Same as **theorem f: T** $\stackrel{def}{=}$ **t**

4.3.5 remark *id*[: *term*] [$\stackrel{def}{=}$ *term*]

`remark f: T` $\stackrel{def}{=}$ `t`

Same as **theorem f: T** $\stackrel{def}{=}$ **t**

4.4 Tactic arguments

This section documents the syntax of some recurring arguments for tactics.

4.4.1 intros-spec

The natural number is the number of new hypotheses to be introduced. The list of identifiers gives the name for the first hypotheses.

intros-spec	::=	[*nat*] [([*id*]...)]	

Table 4.13: intros-spec

4.4.2 pattern

pattern	::=	**in** [*id*[**:** *path*]]... [⊢ *path*]]	simple pattern
	|	**in match** *path* [**in** [*id*[**:** *path*]]... [⊢ *path*]]	full pattern

Table 4.14: pattern

path	::=	⟨⟨*any* sterm *without occurrences of* ***Set***, ***Prop***, ***CProp***, ***Type***, id, uri *and user provided notation; however,* **%** *is now an additional production for* sterm⟩⟩

Table 4.15: path

A *path* locates zero or more subterms of a given term by mimicking the term structure up to:

1. Occurrences of the subterms to locate that are represented by **%**.
2. Subterms without any occurrence of subterms to locate that can be represented by **?**.

Warning: the format for a path for a **match** ... **with** expression is restricted to: **match** *path* **with** [_ ⇒ *path* | ... | _ ⇒ *path*] Its semantics is the following: the n-th "_ ⇒ *path*" branch is matched against the n-th constructor of the inductive data type. The head λ-abstractions of *path* are matched against the corresponding constructor arguments.

For instance, the path `∀_,_:?.(? ? % ?)→(? ? ? %)` locates at once the subterms `x+y` and `x*y` in the term `∀x,y:nat.x+y=1→0=x*y` (where the notation `A=B` hides the term `(eq T A B)` for some type `T`).

A *simple pattern* extends paths to locate subterms in a whole sequent. In particular, the pattern `in H: p K: q ⊢ r` locates at once all the subterms located by the pattern `r` in the conclusion of the sequent and by the patterns `p` and `q` in the hypotheses `H` and `K` of the sequent.

If no list of hypotheses is provided in a simple pattern, no subterm is selected in the hypothesis. If the `⊢ p` part of the pattern is not provided, no subterm will be matched in the conclusion if at least one hypothesis is provided; otherwise the whole conclusion is selected.

Finally, a *full pattern* is interpreted in three steps. In the first step the `match T in` part is ignored and a set *S* of subterms is located as for the case of simple patterns. In the second step the term `T` is parsed and interpreted in the context of each subterm $s \in S$. In the last term for each $s \in S$ the interpreted term `T` computed in the previous step is looked for. The final set of subterms located by the full pattern is the set of occurrences of the interpreted `T` in the subterms *s*.

A full pattern can always be replaced by a simple pattern, often at the cost of increased verbosity or decreased readability.

Example: the pattern `⊢ in match x+y in ∀_,_:?.(? ? % ?)` locates only the first occurrence of `x+y` in the sequent `x,y: nat ⊢ ∀z,w:nat. (x+y) * (z+w) = z * (x+y) + w * (x+y)`. The corresponding simple pattern is `⊢ ∀_,_:?.(? ? (? % ?) ?)`.

Every tactic that acts on subterms of the selected sequents have a pattern argument for uniformity. To automatically generate a simple pattern:

1. Select in the current goal the subterms to pass to the tactic by using the mouse. In order to perform a multiple selection of subterms, hold the Ctrl key while selecting every subterm after the first one.
2. From the contextual menu select "Copy".
3. From the "Edit" or the contextual menu select "Paste as pattern"

4.4.3 reduction-kind

Reduction kinds are normalization functions that transform a term to a convertible but simpler one. Each reduction kind can be used both as a tactic argument and as a stand-alone tactic.

reduction-kind	::=	**normalize**	Computes the $\beta\delta\iota\zeta$-normal form
	|	**simplify**	Computes a form supposed to be simpler
	|	**unfold** [*sterm*]	δ-reduces the constant or variable if specified, or that in head position
	|	**whd**	Computes the $\beta\delta\iota\zeta$-weak-head normal form

Table 4.16: reduction-kind

4.4.4 auto-params

auto_params	::=	[*simple_auto_param*]... [**by** *term* [,*term*]...]

Table 4.17: auto-params

simple_auto_param	::=	**depth=*nat***	Give a bound to the depth of the search tree
	|	**width=*nat***	The maximal width of the search tree
	|	**library**	Search everywhere (not only in included files)
	|	**type**	Try to close also goals of sort Type, otherwise only goals living in sort Prop are attacked.
	|	**paramodulation**	Try to close the goal performing unit-equality paramodulation
	|	**size=*nat***	The maximal number of nodes in the proof
	|	**timeout=*nat***	Timeout in seconds

Table 4.18: simple-auto-param

4.4.5 justification

justification	::=	**using** *term*	Proof term manually provided
	|	*auto_params*	Call automation

Table 4.19: justification

Chapter 5

Extending the syntax

Introduction: *TODO*

5.1 notation

`notation usage "presentation" associativity with precedence p for content`

Synopsis: **notation** [*usage*] "*notation_lhs*" [*associativity*] **with precedence** *nat* **for** *notation_rhs*

Action: Declares a mapping between the presentation AST **presentation** and the content AST **content**. The declared presentation AST fragment **presentation** is at precedence level **p**. The precedence level is used to determine where parentheses must be inserted. In particular, the content AST fragment **content** is actually a pattern, since it contains placeholders (variables) for sub-ASTs. Every placeholder for a term is given an expected precedence level. Parentheses must be inserted around sub-ASTs having a precedence level strictly smaller than the expected one.

If **presentation** describes a binary infix operator and if no precedence level is explicitly given for the operator arguments, an **associativity** declaration can be given to automatically choose the right level for the operands. Otherwise, no **associativity** can be given.

If **direction** is omitted, the mapping is bi-directional and is used both during parsing and pretty-printing of terms. If **direction** is **>**, the mapping is used only during parsing; if it is **<**, it is used only during pretty-printing. Thus it is possible to use simple notations to type for writing the term, and nicer ones for rendering it.

Notation arguments:

usage	::=	**<**	Only for pretty-printing
	|	**>**	Only for parsing

Table 5.1: usage

associativity	::=	**left associative**	Left associative
	|	**right associative**	Right associative
	|	**non associative**	Non associative (default)

Table 5.2: associativity

5.2 interpretation

`interpretation "description" 'symbol` p_1 `...` p_n `= rhs`

notation_rhs	::=	*unparsed_ast*	*TODO*
	|	*unparsed_meta*	*TODO*

Table 5.3: notation_rhs

unparsed_ast	::=	@{*enriched_term*}	A content level AST (a term which is parsed, but not disambiguated).
	|	@*id*	@**id** is just an abbreviation for @**{id}**
	|	@*csymbol*	@**'symbol** is just an abbreviation for @**{'symbol}**

Table 5.4: unparsed_ast

enriched_term	::=	⟨⟨A term that may contain occurrences of *unparsed_meta*, even as variable names in binders, and occurrences of *csymbol*⟩⟩	*TODO*

Table 5.5: enriched_term

unparsed_meta	::=	**${***level2_meta***}**	*TODO*
	|	**$***id*	**$id** is just an abbreviation for **${id}**
	|	**$_**	**$_** is just an abbreviation for **${_}**

Table 5.6: unparsed_meta

level2_meta	::=	*unparsed_ast*	*TODO*
	|	**term** *nat id*	*TODO*
	|	**number** *id*	*TODO*
	|	**ident** *id*	*TODO*
	|	**fresh** *id*	*TODO*
	|	**anonymous**	*TODO*
	|	*id*	*TODO*
	|	**fold** [**left**|**right**] *level2_meta* **rec** *id level2_meta*	*TODO*
	|	**default** *level2_meta level2_meta*	*TODO*
	|	**if** *level2_meta* **then** *level2_meta* **else** *level2_meta*	*TODO*
	|	**fail**	*TODO*

Table 5.7: level2_meta

notation_lhs	::=	*layout* [*layout*]...

Table 5.8: notation_lhs

layout	::=	*layout* **\sub** *layout*	Subscript
	|	*layout* **\sup** *layout*	Superscript
	|	*layout* **\below** *layout*	
	|	*layout* **\above** *layout*	
	|	*layout* **\over** *layout*	
	|	*layout* **\atop** *layout*	
	|	*layout* **\frac** *layout*	Fraction
	|	**\infrule** *layout layout layout*	Inference rule (premises, conclusion, rule name)
	|	**\sqrt** *layout*	Square root
	|	**\root** *layout* **\of** *layout*	Generalized root
	|	**hbox** (*layout* [*layout*]...)	Horizontal box
	|	**vbox** (*layout* [*layout*]...)	Vertical box
	|	**hvbox** (*layout* [*layout*]...)	Horizontal and vertical box
	|	**hovbox** (*layout* [*layout*]...)	Horizontal or vertical box
	|	**break**	Breakable space
	|	(*layout* [*layout*]...)	Group
	|	*id*	Placeholder for a term with no explicit precedence
	|	**term** *nat id*	Placeholder for a term with explicit expected precedence
	|	**number** *id*	Placeholder for a natural number
	|	**ident** *id*	Placeholder for an identifier
	|	*literal*	Literal
	|	**opt** *layout*	Optional layout (it can be omitted for parsing)
	|	**list0** *layout* [**sep** *literal*]	List of layouts separated by **sep** (default: any blank)
	|	**list1** *layout* [**sep** *literal*]	Non empty list of layouts separated by **sep** (default: any blank)
	|	**mstyle** *id* value (*layout*)	Style attributes like color #ff0000
	|	**mpadded** *id* value (*layout*)	padding attributes like width -150%
	|	**maction** (*layout*) [(*layout*) ...]	Alternative notations (output only)

Table 5.9: layout

literal	::=	*symbol*	Unicode symbol
	|	*nat*	Natural number (a constant)
	|	**'***id***'**	New keyword for the lexer

Table 5.10: literal

Synopsis: **interpretation** *qstring csymbol* [*interpretation_argument*]... **=** *interpretation_rhs*

Action: It declares a bi-directional mapping **{...}** between the content-level AST **'symbol** $\mathbf{t_1}$ **...** $\mathbf{t_n}$ and the semantic term **rhs[{**$\mathbf{t_1}$**}/**$\mathbf{p_1}$**;...;{**$\mathbf{t_n}$**}/**$\mathbf{p_n}$**]** (the simultaneous substitution in **rhs** of the interpretation **{...}** of every content-level actual argument $\mathbf{t_i}$ for its corresponding formal parameter $\mathbf{p_i}$). The **description** must be a textual description of the meaning associated to **'symbol** by this interpretation, and is used by the user interface of Matita to provide feedback on the interpretation of ambiguous terms.

Interpretation arguments:

interpretation_argument	::=	[η.]... *id*	A formal parameter. If the name of the formal parameter is prefixed by n symbols "η", then the mapping performs (multiple) η-expansions to grant that the semantic actual parameter begins with at least n λ-abstractions.

Table 5.11: interpretation_argument

interpretation_rhs	::=	*uri*	A constant, specified by its URI
	|	*id*	A constant, specified by its name, or a bound variable. If the constant name is ambiguous, the one corresponding to the last implicitly or explicitly specified alias is used.
	|	**?**	An implicit parameter
	|	(*interpretation_rhs* [*interpretation_rhs*]...)	An application

Table 5.12: interpretation_rhs

Chapter 6

Tacticals

6.1 Interactive proofs and definitions

An interactive definition is started by giving a definition command omitting the definiens. An interactive proof is started by using one of the proof commands omitting an explicit proof term.

An interactive proof or definition can and must be terminated by a qed command when no more sequents are left to prove. Between the command that starts the interactive session and the qed command the user must provide a procedural proof script made of tactics structured by means of tacticals.

In the tradition of the LCF system, tacticals can be considered higher order tactics. Their syntax is structured and they are executed atomically. On the contrary, in Matita the syntax of several tacticals is destructured into a sequence of tokens and tactics in such a way that is is possible to stop execution after every single token or tactic. The original semantics is preserved: the execution of the whole sequence yields the result expected by the original LCF-like tactical.

6.2 The proof status

During an interactive proof, the proof status is made of the set of sequents to prove and the partial proof built so far.

The partial proof can be inspected on demand in the CIC browser. It will be shown in pseudo-natural language produced on the fly from the proof term.

The set of sequents to prove is shown in the notebook of the authoring interface, in the top-right corner of the main window of Matita. Each tab shows a different sequent, named with a question mark followed by a number. The current role of the sequent, according to the following description, is also shown in the tab tag.

1. **Selected sequents** (name in boldface, e.g. **?3**). The next tactic will be applied to every selected sequent, producing new selected sequents. Tacticals such as branching ("**[**") or "**focus**" can be used to change the set of selected sequents.
2. **Sibling sequents** (name prefixed by a vertical bar and their position, e.g. $|_3$?2). When the set of selected sequents has more than one element, the user can decide to focus in turn on each of them. The branching tactical ("**[**") selects the first sequent only, marking every previously selected sequent as a sibling sequent. Each sibling sequent is given a different position. The tactical "**2,3:**" can be used to select one or more sibling sequents, different from the one proposed, according to their position. Once the user starts to work on the selected sibling sequents it becomes impossible to select a new set of siblings until the ("|") tactical is used to end work on the current one.
3. **Automatically solved sibling sequents** (name strokethrough, e.g. $|_3$*?2*). Sometimes a tactic can close by side effects a sibling sequent the user has not selected yet. The sequent is left in the automatically solved status in order for the user to explicitly accept (using the "**skip**" tactical) the automatic instantiation in the proof script. This way the correspondence between the number of branches in the proof script and the number of sequents generated in the proof is preserved.

6.3 Tacticals

proof-script	::=	*proof-step* [*proof-step*]...

Table 6.1: proof script

Every proof step can be immediately executed.

proof-step	::=	*LCF-tactical*	The tactical is applied to each selected sequent. Each new sequent becomes a selected sequent.
	|	**.**	The first selected sequent becomes the only one selected. All the remaining previously selected sequents are proposed to the user one at a time when the next "**.**" is used.
	|	**;**	Nothing changes. Use this proof step as a separator in concrete syntax.
	|	**[**	Every selected sequent becomes a sibling sequent that constitute a branch in the proof. Moreover, the first sequent is also selected.
	|	**|**	Stop working on the current branch of the innermost branching proof. The sibling branches become the sibling sequents and the first one is also selected.
	|	*nat*[**,***nat*]. . . **:**	The sibling sequents specified by the user become the next selected sequents.
	|	***:**	Every sibling branch not considered yet in the innermost branching proof becomes a selected sequent.
	|	**skip**	Accept the automatically provided instantiation (not shown to the user) for the currently selected automatically closed sibling sequent.
	|	**]**	Stop analyzing branches for the innermost branching proof. Every sequent opened during the branching proof and not closed yet becomes a selected sequent.
	|	**focus** *nat* [*nat*]. . .	Selects the sequents specified by the user. The selected sequents must be completely closed (no new sequents left open) before doing an "**unfocus** that restores the current set of sibling branches.
	|	**unfocus**	Used to match the innermost "**focus**" tactical when all the sequents selected by it have been closed. Until "**unfocus**" is performed, it is not possible to progress in the rest of the proof.

LCF-tactical	::=	*tactic*	Applies the specified tactic.
	|	*LCF-tactical* **;** *LCF-tactical*	Applies the first tactical first and the second tactical to each sequent opened by the first one.
	|	*LCF-tactical* **[** [*LCF-tactical*] [| *LCF-tactical*]. . . **]**	Applies the first tactical first and each tactical in the list of tacticals to the corresponding sequent opened by the first one. The number of tacticals provided in the list must be equal to the number of sequents opened by the first tactical.
	|	**do** *nat LCF-tactical*	*TODO*
	|	**repeat** *LCF-tactical*	*TODO*
	|	**first [** [*LCF-tactical*] [| *LCF-tactical*]. . . **]**	*TODO*
	|	**try** *LCF-tactical*	*TODO*
	|	**solve [** [*LCF-tactical*] [| *LCF-tactical*]. . . **]**	*TODO*
	|	**(***LCF-tactical***)**	Used for grouping during parsing.

Table 6.3: tactics and LCF tacticals

Chapter 7

Tactics

7.1 Quick reference card

7.2 absurd

```
absurd P
```

Synopsis: **absurd** *sterm*

Pre-conditions: **P** must have type **Prop**.

Action: It closes the current sequent by eliminating an absurd term.

New sequents to prove: It opens two new sequents of conclusion **P** and ¬**P**.

7.3 apply

```
apply t
```

Synopsis: **apply** *sterm*

Pre-conditions: **t** must have type $\mathbf{T_1} \to \ldots \to \mathbf{T_n} \to \mathbf{G}$ where **G** can be unified with the conclusion of the current sequent.

Action: It closes the current sequent by applying **t** to **n** implicit arguments (that become new sequents).

New sequents to prove: It opens a new sequent for each premise $\mathbf{T_i}$ that is not instantiated by unification. $\mathbf{T_i}$ is the conclusion of the **i**-th new sequent to prove.

7.4 applyS

```
applyS t auto_params
```

Synopsis: **applyS** *sterm auto_params*

Pre-conditions: **t** must have type $\mathbf{T_1} \to \ldots \to \mathbf{T_n} \to \mathbf{G}$.

tactic	::=	absurd *sterm*
	|	apply *sterm*
	|	applyS *sterm auto_params*
	|	assumption
	|	auto *auto_params*. **autobatch** *auto_params*
	|	cases *term pattern* [([*id*]...)]
	|	change *pattern* **with** *sterm*
	|	clear *id* [*id*...]
	|	clearbody *id*
	|	compose [*nat*] *sterm* [**with** *sterm*] [*intros-spec*]
	|	constructor *nat*
	|	contradiction
	|	cut *sterm* [**as** *id*]
	|	decompose [**as** *id*...]
	|	demodulate *auto_params*
	|	destruct *sterm*
	|	elim *sterm pattern* [**using** *sterm*] *intros-spec*
	|	elimType *sterm* [**using** *sterm*] *intros-spec*
	|	exact *sterm*
	|	exists
	|	fail
	|	fold *reduction-kind sterm pattern*
	|	fourier
	|	fwd *id* [**as** *id* [*id*]...]
	|	generalize *pattern* [**as** *id*]
	|	id
	|	intro [*id*]
	|	intros *intros-spec*
	|	inversion *sterm*
	|	lapply [**linear**] [**depth=***nat*] *sterm* [**to** *sterm* [**,***sterm*...]] [**as** *id*]
	|	left
	|	letin *id* $\stackrel{def}{=}$ *sterm*
	|	normalize *pattern*
	|	reflexivity
	|	replace *pattern* **with** *sterm*
	|	rewrite [**<**|**>**] *sterm pattern*
	|	right
	|	ring
	|	simplify *pattern*
	|	split
	|	subst
	|	symmetry
	|	transitivity *sterm*
	|	unfold [*sterm*] *pattern*
	|	whd *pattern*

Table 7.1: tactics

Action: **applyS** is useful when **apply** fails because the current goal and the conclusion of the applied theorems are extensionally equivalent up to instantiation of metavariables, but cannot be unified. E.g. the goal is **P(n*O+m)** and the theorem to be applied proves ∀**m.P(m+O)**.

It tries to automatically rewrite the current goal using auto paramodulation to make it unifiable with **G**. Then it closes the current sequent by applying **t** to **n** implicit arguments (that become new sequents). The **auto_params** parameters are passed directly to **auto paramodulation**.

New sequents to prove: It opens a new sequent for each premise $\mathbf{T_i}$ that is not instantiated by unification. $\mathbf{T_i}$ is the conclusion of the **i**-th new sequent to prove.

7.5 assumption

`assumption`

Synopsis: **assumption**

Pre-conditions: There must exist an hypothesis whose type can be unified with the conclusion of the current sequent.

Action: It closes the current sequent exploiting an hypothesis.

New sequents to prove: None

7.6 auto

`auto params`

Synopsis: **auto** *auto_params*.

autobatch *auto_params*

Pre-conditions: None, but the tactic may fail finding a proof if every proof is in the search space that is pruned away. Pruning is controlled by the optional **params**. Moreover, only lemmas whose type signature is a subset of the signature of the current sequent are considered. The signature of a sequent is essentially the set of constats appearing in it.

Action: It closes the current sequent by repeated application of rewriting steps (unless **paramodulation** is omitted), hypothesis and lemmas in the library.

New sequents to prove: None

7.7 cases

`cases t pattern hyps`

Synopsis: **cases** *term pattern* [([*id*]...)]

Pre-conditions: **t** must inhabit an inductive type

Action: It proceed by cases on **t**. The new generated hypothesis in each branch are named according to **hyps**. The elimintation predicate is restricted by **pattern**. In particular, if some hypothesis is listed in **pattern**, the hypothesis is generalized and cleared before proceeding by cases on **t**. Currently, we only support patterns of the form $\mathbf{H_1}$ **...** $\mathbf{H_n} \vdash$ **%**. This limitation will be lifted in the future.

New sequents to prove: One new sequent for each constructor of the type of **t**. Each sequent has a new hypothesis for each argument of the constructor.

7.8 clear

```
clear H1 ... Hm
```

Synopsis: **clear** *id* [*id*...]

Pre-conditions: $\mathbf{H_1}$ **...** $\mathbf{H_m}$ must be hypotheses of the current sequent to prove.

Action: It hides the hypotheses $\mathbf{H_1}$ **...** $\mathbf{H_m}$ from the current sequent.

New sequents to prove: None

7.9 clearbody

```
clearbody H
```

Synopsis: **clearbody** *id*

Pre-conditions: **H** must be an hypothesis of the current sequent to prove.

Action: It hides the definiens of a definition in the current sequent context. Thus the definition becomes an hypothesis.

New sequents to prove: None.

7.10 compose

```
compose n t1 with t2 hyps
```

Synopsis: **compose** [*nat*] *sterm* [**with** *sterm*] [*intros-spec*]

Pre-conditions:

Action: Composes t1 with t2 in every possible way **n** times introducing generated terms as if **intros hyps** was issued.

If **t1:**$\forall$**x:A.B[x]** and **t2:**$\forall$**x,y:A.B[x]**$\rightarrow$**B[y]**$\rightarrow$**C[x,y]** it generates:

- λ**x,y:A.t2 x y (t1 x) :** $\forall$**x,y:A.B[y]**$\rightarrow$**C[x,y]**
- λ**x,y:A.**λ**H:B[x].t2 x y H (t1 y) :** $\forall$**x,y:A.B[x]**$\rightarrow$**C[x,y]**

If **t2** is omitted it composes **t1** with every hypothesis that can be introduced. **n** iterates the process.

New sequents to prove: The same, but with more hypothesis eventually introduced by the *intros-spec*.

7.11 change

```
change patt with t
```

Synopsis: **change** *pattern* **with** *sterm*

Pre-conditions: Each subterm matched by the pattern must be convertible with the term **t** disambiguated in the context of the matched subterm.

Action: It replaces the subterms of the current sequent matched by **patt** with the new term **t**. For each subterm matched by the pattern, **t** is disambiguated in the context of the subterm.

New sequents to prove: None.

7.12 constructor

`constructor n`

Synopsis: **constructor** *nat*

Pre-conditions: The conclusion of the current sequent must be an inductive type or the application of an inductive type with at least **n** constructors.

Action: It applies the **n**-th constructor of the inductive type of the conclusion of the current sequent.

New sequents to prove: It opens a new sequent for each premise of the constructor that can not be inferred by unification. For more details, see the **apply** tactic.

7.13 contradiction

`contradiction`

Synopsis: **contradiction**

Pre-conditions: There must be in the current context an hypothesis of type **False**.

Action: It closes the current sequent by applying an hypothesis of type **False**.

New sequents to prove: None

7.14 cut

`cut P as H`

Synopsis: **cut** *sterm* [**as** *id*]

Pre-conditions: **P** must have type **Prop**.

Action: It closes the current sequent.

New sequents to prove: It opens two new sequents. The first one has an extra hypothesis **H:P**. If **H** is omitted, the name of the hypothesis is automatically generated. The second sequent has conclusion **P** and hypotheses the hypotheses of the current sequent to prove.

7.15 decompose

`decompose as` H_1 `...` H_m

Synopsis: **decompose** [**as** *id*...]

Pre-conditions: None.

Action: For each each premise **H** of type **T** in the current context where **T** is a non-recursive inductive type without right parameters and of sort Prop or CProp, the tactic runs **elim H as** H_1 **...** H_m , clears **H** and runs itself recursively on each new premise introduced by **elim** in the opened sequents.

New sequents to prove: The ones generated by all the **elim** tactics run.

7.16 demodulate

```
demodulate auto_params
```

Synopsis: **demodulate** *auto_params*

Pre-conditions: None.

Action: *TODO*

New sequents to prove: None.

7.17 destruct

```
destruct p
```

Synopsis: **destruct** *sterm*

Pre-conditions: **p** must have type $\mathbf{E_1 = E_2}$ where the two sides of the equality are possibly applied constructors of an inductive type.

Action: The tactic recursively compare the two sides of the equality looking for different constructors in corresponding position. If two of them are found, the tactic closes the current sequent by proving the absurdity of **p**. Otherwise it adds a new hypothesis for each leaf of the formula that states the equality of the subformulae in the corresponding positions on the two sides of the equality.

New sequents to prove: None.

7.18 elim

```
elim t pattern using th hyps
```

Synopsis: **elim** *sterm pattern* [**using** *sterm*] *intros-spec*

Pre-conditions: **t** must inhabit an inductive type and **th** must be an elimination principle for that inductive type. If **th** is omitted the appropriate standard elimination principle is chosen.

Action: It proceeds by cases on the values of **t**, according to the elimination principle **th**. The induction predicate is restricted by **pattern**. In particular, if some hypothesis is listed in **pattern**, the hypothesis is generalized and cleared before eliminating **t**

New sequents to prove: It opens one new sequent for each case. The names of the new hypotheses are picked by **hyps**, if provided. If hyps specifies also a number of hypotheses that is less than the number of new hypotheses for a new sequent, then the exceeding hypothesis will be kept as implications in the conclusion of the sequent.

7.19 elimType

```
elimType T using th hyps
```

Synopsis: **elimType** *sterm* [**using** *sterm*] *intros-spec*

Pre-conditions: **T** must be an inductive type.

Action: TODO (severely bugged now).

New sequents to prove: TODO

7.20 exact

`exact p`

Synopsis: **exact** *sterm*

Pre-conditions: The type of **p** must be convertible with the conclusion of the current sequent.

Action: It closes the current sequent using **p**.

New sequents to prove: None.

7.21 exists

`exists`

Synopsis: **exists**

Pre-conditions: The conclusion of the current sequent must be an inductive type or the application of an inductive type with at least one constructor.

Action: Equivalent to **constructor 1**.

New sequents to prove: It opens a new sequent for each premise of the first constructor of the inductive type that is the conclusion of the current sequent. For more details, see the **constructor** tactic.

7.22 fail

`fail`

Synopsis: **fail**

Pre-conditions: None.

Action: This tactic always fail.

New sequents to prove: N.A.

7.23 fold

`fold red t patt`

Synopsis: **fold** *reduction-kind sterm pattern*

Pre-conditions: The pattern must not specify the wanted term.

Action: First of all it locates all the subterms matched by **patt**. In the context of each matched subterm it disambiguates the term **t** and reduces it to its **red** normal form; then it replaces with **t** every occurrence of the normal form in the matched subterm.

New sequents to prove: None.

7.24 fourier

`fourier`

Synopsis: **fourier**

Pre-conditions: The conclusion of the current sequent must be a linear inequation over real numbers taken from standard library of Coq. Moreover the inequations in the hypotheses must imply the inequation in the conclusion of the current sequent.

Action: It closes the current sequent by applying the Fourier method.

New sequents to prove: None.

7.25 fwd

`fwd H as H0 ... Hn`

Synopsis: **fwd** *id* [**as** *id* [*id*]...]

Pre-conditions: The type of **H** must be the premise of a forward simplification theorem.

Action: This tactic is under development. It simplifies the current context by removing **H** using the following methods: forward application (by **lapply**) of a suitable simplification theorem, chosen automatically, of which the type of **H** is a premise, decomposition (by **decompose**), rewriting (by **rewrite**). **H_0 ... H_n** are passed to the tactics **fwd** invokes, as names for the premise they introduce.

New sequents to prove: The ones opened by the tactics **fwd** invokes.

7.26 generalize

`generalize patt as H`

Synopsis: **generalize** *pattern* [**as** *id*]

Pre-conditions: All the terms matched by **patt** must be convertible and close in the context of the current sequent.

Action: It closes the current sequent by applying a stronger lemma that is proved using the new generated sequent.

New sequents to prove: It opens a new sequent where the current sequent conclusion **G** is generalized to $\forall$**x.G{x/t}** where **{x/t}** is a notation for the replacement with **x** of all the occurrences of the term **t** matched by **patt**. If **patt** matches no subterm then **t** is defined as the **wanted** part of the pattern.

7.27 id

`id`

Synopsis: **id**

Pre-conditions: None.

Action: This identity tactic does nothing without failing.

New sequents to prove: None.

7.28 intro

`intro H`

Synopsis: **intro** [*id*]

Pre-conditions: The conclusion of the sequent to prove must be an implication or a universal quantification.

Action: It applies the right introduction rule for implication, closing the current sequent.

New sequents to prove: It opens a new sequent to prove adding to the hypothesis the antecedent of the implication and setting the conclusion to the consequent of the implicaiton. The name of the new hypothesis is **H** if provided; otherwise it is automatically generated.

7.29 intros

`intros hyps`

Synopsis: **intros** *intros-spec*

Pre-conditions: If **hyps** specifies a number of hypotheses to introduce, then the conclusion of the current sequent must be formed by at least that number of imbricated implications or universal quantifications.

Action: It applies several times the right introduction rule for implication, closing the current sequent.

New sequents to prove: It opens a new sequent to prove adding a number of new hypotheses equal to the number of new hypotheses requested. If the user does not request a precise number of new hypotheses, it adds as many hypotheses as possible. The name of each new hypothesis is either popped from the user provided list of names, or it is automatically generated when the list is (or becomes) empty.

7.30 inversion

`inversion t`

Synopsis: **inversion** *sterm*

Pre-conditions: The type of the term **t** must be an inductive type or the application of an inductive type.

Action: It proceeds by cases on **t** paying attention to the constraints imposed by the actual "right arguments" of the inductive type.

New sequents to prove: It opens one new sequent to prove for each case in the definition of the type of **t**. With respect to a simple elimination, each new sequent has additional hypotheses that states the equalities of the "right parameters" of the inductive type with terms originally present in the sequent to prove.

7.31 lapply

`lapply linear depth=d t to t1, ..., tn as H`

Synopsis: **lapply** [**linear**] [**depth=***nat*] *sterm* [**to** *sterm* [**,***sterm*...]] [**as** *id*]

Pre-conditions: **t** must have at least **d** independent premises and **n** must not be greater than **d**.

Action: Invokes **letin H** $\stackrel{def}{=}$ **(t ? ... ?)** with enough **?**'s to reach the **d**-th independent premise of **t** (**d** is maximum if unspecified). Then istantiates (by **apply**) with t_1, ..., t_n the **?**'s corresponding to the first **n** independent premises of **t**. Usually the other **?**'s preceding the **n**-th independent premise of **t** are istantiated as a consequence. If the **linear** flag is specified and if **t, t_1, ..., t_n** are (applications of) premises in the current context, they are **clear**ed.

New sequents to prove: The ones opened by the tactics **lapply** invokes.

7.32 left

`left`

Synopsis: **left**

Pre-conditions: The conclusion of the current sequent must be an inductive type or the application of an inductive type with at least one constructor.

Action: Equivalent to **constructor 1**.

New sequents to prove: It opens a new sequent for each premise of the first constructor of the inductive type that is the conclusion of the current sequent. For more details, see the **constructor** tactic.

7.33 letin

`letin x` $\stackrel{def}{=}$ `t`

Synopsis: **letin** *id* $\stackrel{def}{=}$ *sterm*

Pre-conditions: None.

Action: It adds to the context of the current sequent to prove a new definition **x** $\stackrel{def}{=}$ **t**.

New sequents to prove: None.

7.34 normalize

`normalize patt`

Synopsis: **normalize** *pattern*

Pre-conditions: None.

Action: It replaces all the terms matched by **patt** with their $\beta\delta\iota\zeta$-normal form.

New sequents to prove: None.

7.35 reflexivity

`reflexivity`

Synopsis: **reflexivity**

Pre-conditions: The conclusion of the current sequent must be **t=t** for some term **t**

Action: It closes the current sequent by reflexivity of equality.

New sequents to prove: None.

7.36 replace

`change patt with t`

Synopsis: **replace** *pattern* **with** *sterm*

Pre-conditions: None.

Action: It replaces the subterms of the current sequent matched by **patt** with the new term **t**. For each subterm matched by the pattern, **t** is disambiguated in the context of the subterm.

New sequents to prove: For each matched term **t'** it opens a new sequent to prove whose conclusion is **t'=t**.

7.37 rewrite

`rewrite dir p patt`

Synopsis: **rewrite** [**<**|**>**] *sterm pattern*

Pre-conditions: **p** must be the proof of an equality, possibly under some hypotheses.

Action: It looks in every term matched by **patt** for all the occurrences of the left hand side of the equality that **p** proves (resp. the right hand side if **dir** is **<**). Every occurence found is replaced with the opposite side of the equality.

New sequents to prove: It opens one new sequent for each hypothesis of the equality proved by **p** that is not closed by unification.

7.38 right

`right`

Synopsis: **right**

Pre-conditions: The conclusion of the current sequent must be an inductive type or the application of an inductive type with at least two constructors.

Action: Equivalent to **constructor 2**.

New sequents to prove: It opens a new sequent for each premise of the second constructor of the inductive type that is the conclusion of the current sequent. For more details, see the **constructor** tactic.

7.39 ring

`ring`

Synopsis: **ring**

Pre-conditions: The conclusion of the current sequent must be an equality over Coq's real numbers that can be proved using the ring properties of the real numbers only.

Action: It closes the current sequent veryfying the equality by means of computation (i.e. this is a reflexive tactic, implemented exploiting the "two level reasoning" technique).

New sequents to prove: None.

7.40 simplify

`simplify patt`

Synopsis: **simplify** *pattern*

Pre-conditions: None.

Action: It replaces all the terms matched by **patt** with other convertible terms that are supposed to be simpler.

New sequents to prove: None.

7.41 split

`split`

Synopsis: **split**

Pre-conditions: The conclusion of the current sequent must be an inductive type or the application of an inductive type with at least one constructor.

Action: Equivalent to **constructor 1**.

New sequents to prove: It opens a new sequent for each premise of the first constructor of the inductive type that is the conclusion of the current sequent. For more details, see the **constructor** tactic.

7.42 subst

`subst`

Synopsis: **subst**

Pre-conditions: None.

Action: For each premise of the form **H: x = t** or **H: t = x** where **x** is a local variable and **t** does not depend on **x**, the tactic rewrites **H** wherever **x** appears clearing **H** and **x** afterwards.

New sequents to prove: The one opened by the applied tactics.

7.43 symmetry

The tactic **symmetry**

`symmetry`

Synopsis: **symmetry**

Pre-conditions: The conclusion of the current proof must be an equality.

Action: It swaps the two sides of the equalityusing the symmetric property.

New sequents to prove: None.

7.44 transitivity

```
transitivity t
```

Synopsis: **transitivity** *sterm*

Pre-conditions: The conclusion of the current proof must be an equality.

Action: It closes the current sequent by transitivity of the equality.

New sequents to prove: It opens two new sequents **l=t** and **t=r** where **l** and **r** are the left and right hand side of the equality in the conclusion of the current sequent to prove.

7.45 unfold

```
unfold t patt
```

Synopsis: **unfold** [*sterm*] *pattern*

Pre-conditions: None.

Action: It finds all the occurrences of **t** (possibly applied to arguments) in the subterms matched by **patt**. Then it δ-expands each occurrence, also performing β-reduction of the obtained term. If **t** is omitted it defaults to each subterm matched by **patt**.

New sequents to prove: None.

7.46 whd

```
whd patt
```

Synopsis: **whd** *pattern*

Pre-conditions: None.

Action: It replaces all the terms matched by **patt** with their $\beta\delta\iota\zeta$-weak-head normal form.

New sequents to prove: None.

Chapter 8

Declarative Tactics

8.1 Quick reference card

tactic	::=	assume *id* **:** *sterm*
	|	by induction hypothesis we know *term* (*id*)
	|	case *id* [(*id* **:** *term*)] . . .
	|	*justification* done
	|	*justification* **let** *id* **:** *term* **such that** *term* (*id*)
	|	[obtain *id* | **conclude** *term*] **=** *term*
	|	[*auto_params* | **using** *term* | **using once** *term* | **proof**] [**done**]
	|	suppose *term* (*id*) [**that is equivalent to** *term*]
	|	the thesis becomes *term*
	|	we need to prove *term* [(*id*)] [**or equivalently** *term*]
	|	we proceed by cases on *term* **to prove** *term*
	|	we proceed by induction on *term* **to prove** *term*
	|	*justification* we proved *term* (*id*)

Table 8.1: tactics

8.2 assume

```
assume x : t
```

Synopsis: **assume** *id* **:** *sterm*

Pre-conditions: The conclusion of the current proof must be ∀**x:T.P** or **T**→**P** where **T** is a data type (i.e. **T** has type **Set** or **Type**).

Action: It adds to the context of the current sequent to prove a new declaration **x : T** . The new conclusion becomes **P**.

New sequents to prove: None.

8.3 by induction hypothesis we know

```
by induction hypothesis we know t (id)
```

Synopsis: **by induction hypothesis we know** *term* **(** *id* **)**

Pre-condition: To be used in a proof by induction to state the inductive hypothesis.

Action: Introduces the inductive hypothesis.

New sequents to prove: None.

8.4 case

```
case id (id1:t1) ...  (idn:tn)
```

Synopsis: **case** *id* [**(** *id* **:** *term* **)**] . . .

Pre-condition: To be used in a proof by induction or by cases to start a new case

Action: Starts the new case **id** declaring the local parameters **(id1:t1) . . . (idn:tn)**

New sequents to prove: None

8.5 done

```
justification done
```

Synopsis: *justification* **done**

Pre-condition:

Action: It closes the current sequent given the justification.

New sequents to prove: None.

8.6 let such that

```
justification let x:t such that p (id)
```

Synopsis: *justification* **let** *id* **:** *term* **such that** *term* **(** *id* **)**

Pre-condition:

Action: It derives ∃**x:t.p** using the **justification** and then it introduces in the context **x** and the hypothesis **p** labelled with **id**.

New sequent to prove: None.

8.7 obtain

```
obtain H t1 = t2 justification
```

Synopsis: [**obtain** *id* | **conclude** *term*] **=** *term* [*auto_params* | **using** *term* | **using once** *term* | **proof**] [**done**]

Pre-condition: **conclude** can be used only if the current sequent is stating an equality. The left hand side must be omitted in an equality chain.

Action: Starts or continues an equality chain. If the chain starts with **obtain H** a new subproof named **H** is started.

New sequent to prove: If the chain starts with **obtain H** a nre sequent for **t2 = ?** is opened.

8.8 suppose

```
suppose t1 (x) that is equivalent to t2
```

Synopsis: **suppose** *term* (*id*) [**that is equivalent to** *term*]

Pre-condition: The conclusion of the current proof must be ∀**x:T.P** or **T**→**P** where **T** is a proposition (i.e. **T** has type **Prop** or **CProp**).

Action: It adds to the context of the current sequent to prove a new declaration **x : T** . The new conclusion becomes **P**.

New sequents to prove: None.

8.9 the thesis becomes

```
the thesis becomes t
```

Synopsis: **the thesis becomes** *term*

Pre-condition: The provided term **t** must be convertible with current sequent.

Action: It changes the current goal to the one provided.

New sequent to prove: None.

8.10 we need to prove

```
we need to prove t1 (id) or equivalently t2
```

Synopsis: **we need to prove** *term* [(*id*)] [**or equivalently** *term*]

Pre-condition:

Action: If **id** is provided, starts a subproof that once concluded will be named **id**. Otherwise states what needs to be proved. If **t2** is provided, the new goal is immediately changed to **t2** wich must be equivalent to **t1**.

New sequents to prove: The stated one if **id** is provided

8.11 we have

```
justification we have t1 (id1) and t2 (id2)
```

Synopsis: *justification* **we have** *term* (*id*) **and** *term* (*id*)

Pre-condition:

Action: It derives **t1**∧**t2** using the **justification** then it introduces in the context **t1** labelled with **id1** and **t2** labelled with **id2**.

New sequent to prove: None.

8.12 we proceed by cases on

```
we proceed by cases on t to prove th
```

Synopsis: **we proceed by cases on** *term* **to prove** *term*

Pre-condition: **t** must inhabitant of an inductive type and **th** must be the conclusion to be proved by cases.

Action: It proceeds by cases on **t**

New sequents to prove: It opens one new sequent for each constructor of the type of **t**.

8.13 we proceed by induction on

```
we proceed by induction on t to prove th
```

Synopsis: **we proceed by induction on** *term* **to prove** *term*

Pre-condition: **t** must inhabitant of an inductive type and **th** must be the conclusion to be proved by induction.

Action: It proceed by induction on **t**.

New sequents to prove: It opens one new sequent for each constructor of the type of **t**.

8.14 we proved

```
justification we proved t (id)
```

Synopsis: *justification* **we proved** *term* **(** *id* **)**

Pre-condition: **t**must have type **Prop**.

Action: It derives **t** using the justification and labels the conclusion with **id**.

New sequent to prove: None.

Chapter 9

Other commands

9.1 alias

```
alias id "s" = "def"
alias symbol "s" (instance n) = "def"
alias num (instance n) = "def"
```

Synopsis: **alias** [**id** *qstring* **=** *qstring* | **symbol** *qstring* [(**instance** *nat*)] **=** *qstring* | **num** [(**instance** *nat*)] **=** *qstring*]

Action: Used to give an hint to the disambiguating parser. When the parser is faced to the identifier (or symbol) **s** or to any number, it will prefer interpretations that "map **s** (or the number) to **def**". For identifiers, "def" is the URI of the interpretation. E.g.: **cic:/matita/nat/nat.ind#xpointer(1/1/1)** for the first constructor of the first inductive type defined in the block of inductive type(s) **cic:/matita/nat/nat.ind**. For symbols and numbers, "def" is the label used to mark the wanted interpretation.

When a symbol or a number occurs several times in the term to be parsed, it is possible to give an hint only for the instance **n**. When the instance is omitted, the hint is valid for every occurrence.

Hints are automatically inserted in the script by Matita every time the user is interactively asked a question to disambiguate a term. This way the user won't be posed the same question twice when the script will be executed again.

9.2 check

```
check t
```

Synopsis: **check** *term*

Action: Opens a CIC browser window that shows **t** together with its type. The command is immediately removed from the script.

9.3 eval

```
eval red on t
```

Synopsis: **eval** *reduction-kind* **on** *term*

Action: Opens a CIC browser window that shows the reduct of **t** together with its type.

9.4 prefer coercion

```
prefer coercion u
```

Synopsis: **prefer coercion** (*uri* | *term*)

Action: The already declared coercion **u** is preferred to other coercions with the same source and target.

9.5 coercion

```
coercion u with ariety saturation nocomposites
```

Synopsis: **coercion** (*uri* | *term* **with**) [*nat* [*nat*]] [**nocomposites**]

Action: Declares **u** as an implicit coercion. If the type of **u** is ∀**x1:T1. ...** ∀**x(n-1):T(n-1).Tn** the coercion target is **T(n - ariety)** while its source is **T(n - ariety - saturation - 1)**. Every time a term **x** of type source is used with expected type target, Matita automatically replaces **x** with **(u ? ... ? x ? ... ?)** to avoid a typing error. Note that the number of **?** added after **x** is saturation.

Implicit coercions are not displayed to the user: **(u ? ... ? x)** is rendered simply as **x**.

When a coercion **u** is declared from source **s** to target **t** and there is already a coercion **u'** of target **s** or source **t**, a composite implicit coercion is automatically computed by Matita unless **nocomposites** is specified.

9.6 default

```
default "s" u1 ... un
```

Synopsis: **default** *qstring uri* [*uri*]...

Action: It registers a cluster of related definitions and theorems to be used by tactics and the rendering engine. Some functionalities of Matita are not available when some clusters have not been registered. Overloading a cluster registration is possible: the last registration will be the default one, but the previous ones are still in effect.

s is an identifier of the cluster and $\mathbf{u_1}$ **...** $\mathbf{u_n}$ are the URIs of the definitions and theorems of the cluster. The number **n** of required URIs depends on the cluster. The following clusters are supported.

9.7 hint

```
hint
```

Synopsis: **hint**

Action: Displays a list of theorems that can be successfully applied to the current selected sequent. The command is removed from the script, but the window that displays the theorems allow to add to the script the application of the selected theorem.

9.8 include

```
include "s"
```

Synopsis: **include** *qstring*

Action: Every coercion, notation and interpretation that was active when the file **s** was compiled last time is made active. The same happens for declarations of default definitions and theorems and disambiguation hints (aliases). On the contrary, theorem and definitions declared in a file can be immediately used without including it.

The file **s** is automatically compiled if it is not compiled yet.

name	expected object for 1st URI	expected object for 2nd URI	expected object for 3rd URI	expected object for 4th URI	expected object for 5th URI
equality	an inductive type (say, of type **eq**) of type ∀A:Type.A → **Prop** with one family parameter and one constructor of type ∀x:A.eq A x	a theorem of type ∀A.∀x,y:A.eq A x y → eq A y x	a theorem of type ∀A.∀x,y,z:A.eq A x y → eq A y z → eq A x z	∀A.∀a.∀ P:A → **Prop**.P x → ∀y.eq A x y → P y	∀A.∀a.∀ P:A → **Prop**.P x → ∀y.eq A y x → P y
true	an inductive type of type **Prop** with only one constructor that has no arguments				
false	an inductive type of type **Prop** without constructors				
absurd	a theorem of type ∀A:Prop.∀B:Prop.A → Not A → B				

Table 9.1: clusters

9.9 include' "s"

Synopsis: **include'** *qstring*

Action: Not documented (*TODO*), do not use it.

9.10 whelp

```
whelp locate "s"
whelp hint t
whelp elim t
whelp match t
whelp instance t
```

Synopsis: **whelp** [**locate** *qstring* | **hint** *term* | **elim** *term* | **match** *term* | **instance** *term*]

Action: Performs the corresponding query, showing the result in the CIC browser. The command is removed from the script.

9.11 qed

```
qed
```

Synopsis: **qed**

Action: Saves and indexes the current interactive theorem or definition. In order to do this, the set of sequents still to be proved must be empty.

9.12 inline

`inline "s" params`

Synopsis: **inline** *qstring inline_params*

Action: Inlines a representation of the item **s**, which can be the URI of a HELM object. If an entire HELM directory (i.e. a base URI) or the path of a *.ma source file is provided, all the contained objects are represented in a row. If the inlined object has a proof, this proof is represented in several ways depending on the provided parameters.

9.12.1 inline-params

inline_params	::=	[*inline_param* [*inline_param*] . . .]

Table 9.2: inline-params

inline_param	::=	**axiom**	Try to give an axiom flavour (bodies are omitted even if present)
	|	**definition**	Try give a definition flavour
	|	**theorem**	Try give a theorem flavour
	|	**lemma**	Try give a lemma flavour
	|	**remark**	Try give a remark flavour
	|	**fact**	Try give a fact flavour
	|	**variant**	Try give a variant flavour (implies **plain**)
	|	**declarative**	Represent proofs using declarative tactics (this is the dafault and can be omitted)
	|	**procedural**	Represent proofs using procedural tactics
	|	**plain**	Represent proofs using plain proof terms
	|	**nodefaults**	Do not use the tactics depending on the default command (rewrite in the **procedural** mode)
	|	**level=*nat***	Set the level of the procedural proof representation (the default is the highest level) • Tactics used at level 1: exact • Additional tactics used at level 2: letin, cut, change, intros, apply, elim, cases, rewrite
	|	**depth=*nat***	*TODO*

Table 9.3: inline-param

Chapter 10

License