

MAT 7003 : Mathematical Foundations

(for Software Engineering)

J Paul Gibson, A207

paul.gibson@it-sudparis.eu

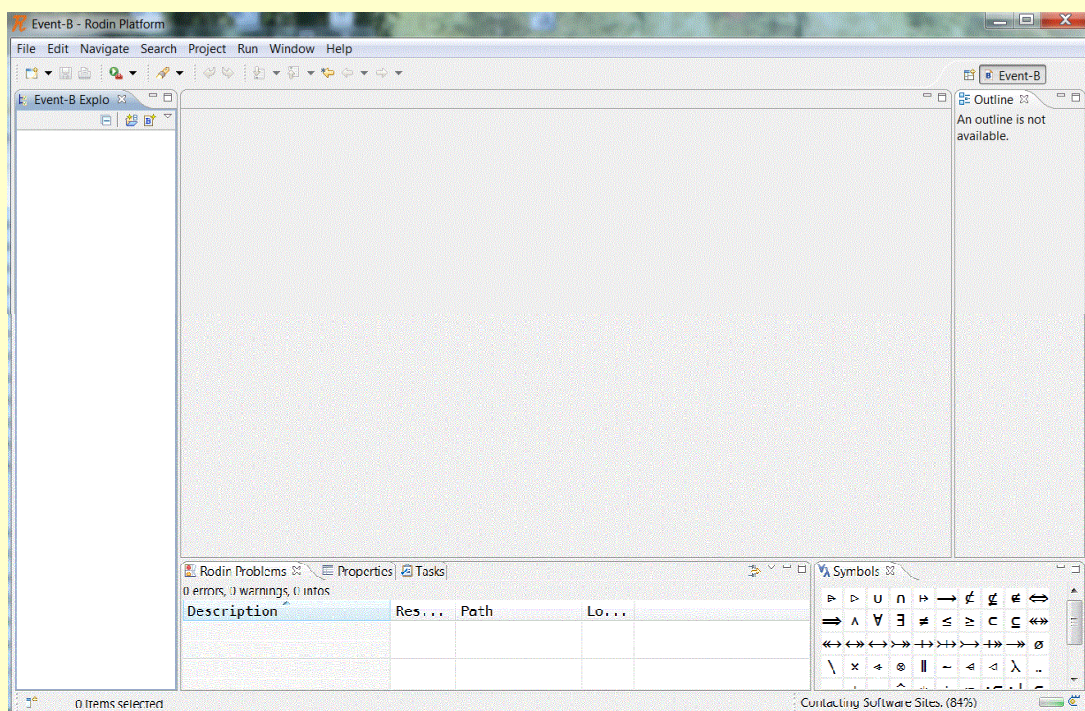
<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/>

RODIN

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/L1-RODIN.pdf>

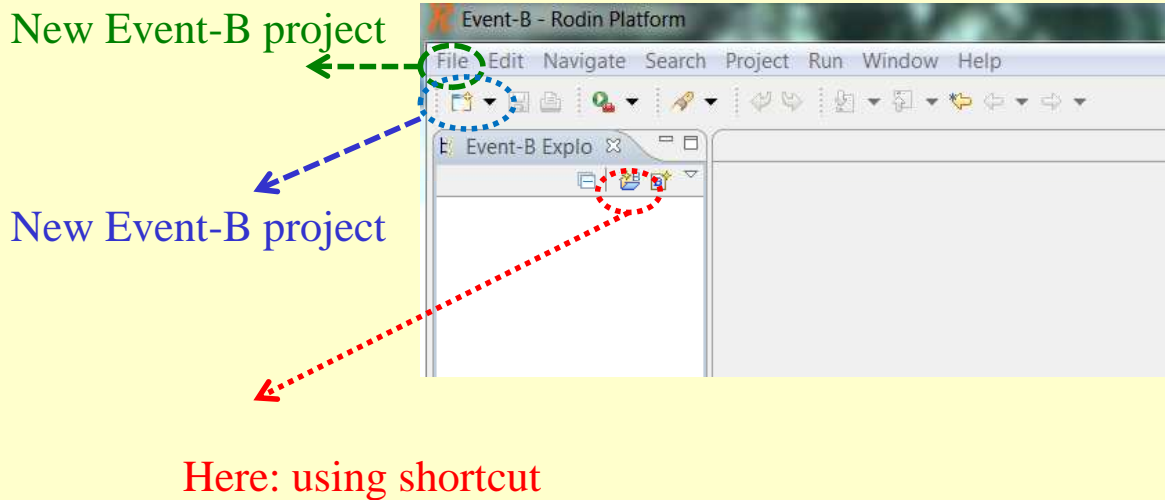
A CLEAN WORKSPACE

After installing RODIN and checking for updates you should have a clean workspace, which looks something like this:

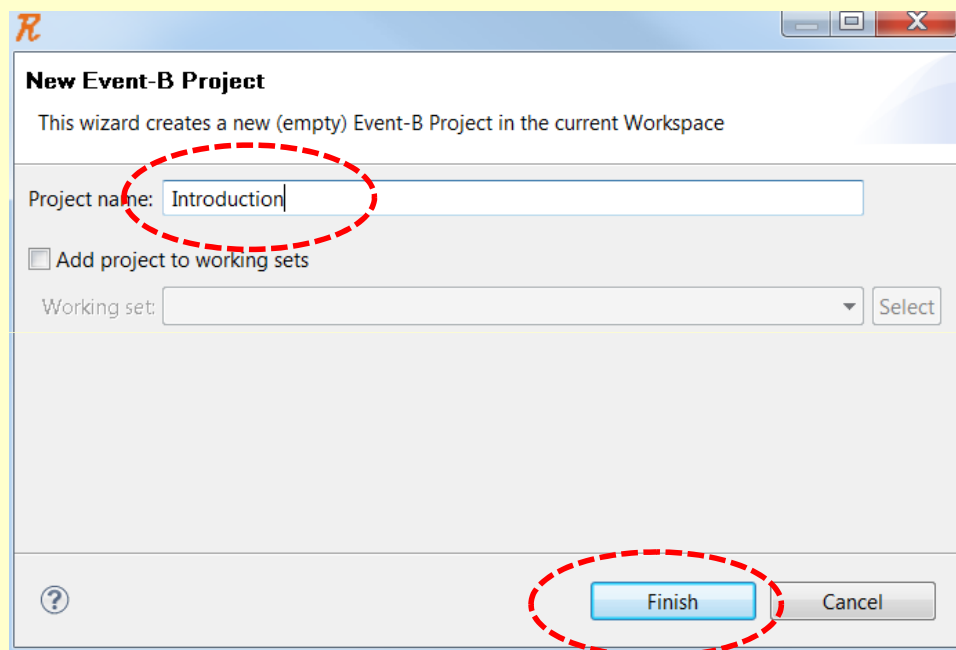


A NEW PROJECT

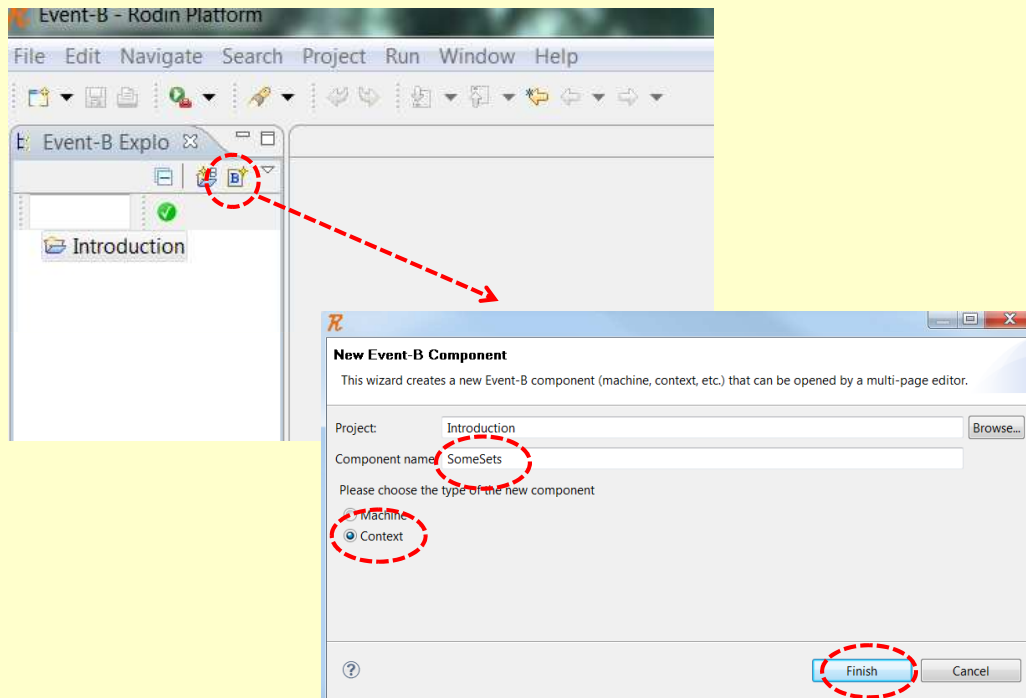
Now we wish to create a new project; and there are multiple ways of doing this (as there always is in RODIN):



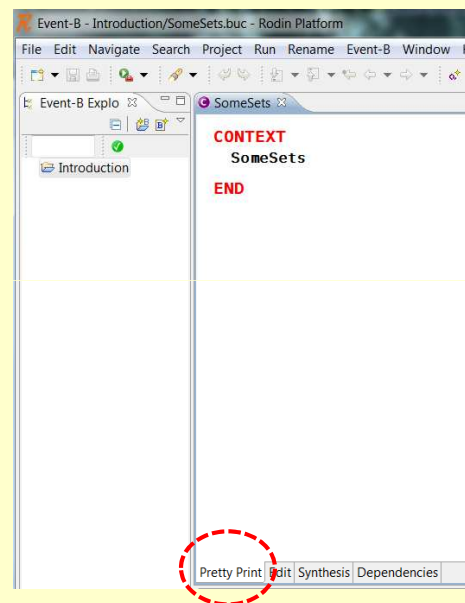
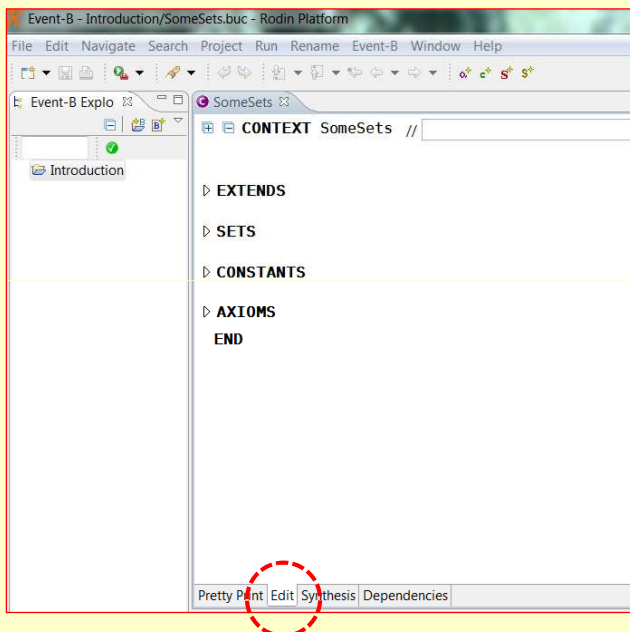
Give the Project a Name (like « Introduction »)



Now add a **Context** component to our project (in order to do some mathematics)



We have different **views** on our models (contexts and machines)



Now for a simple property about sets applied to « people »:

```
CONTEXT
  SomeSets

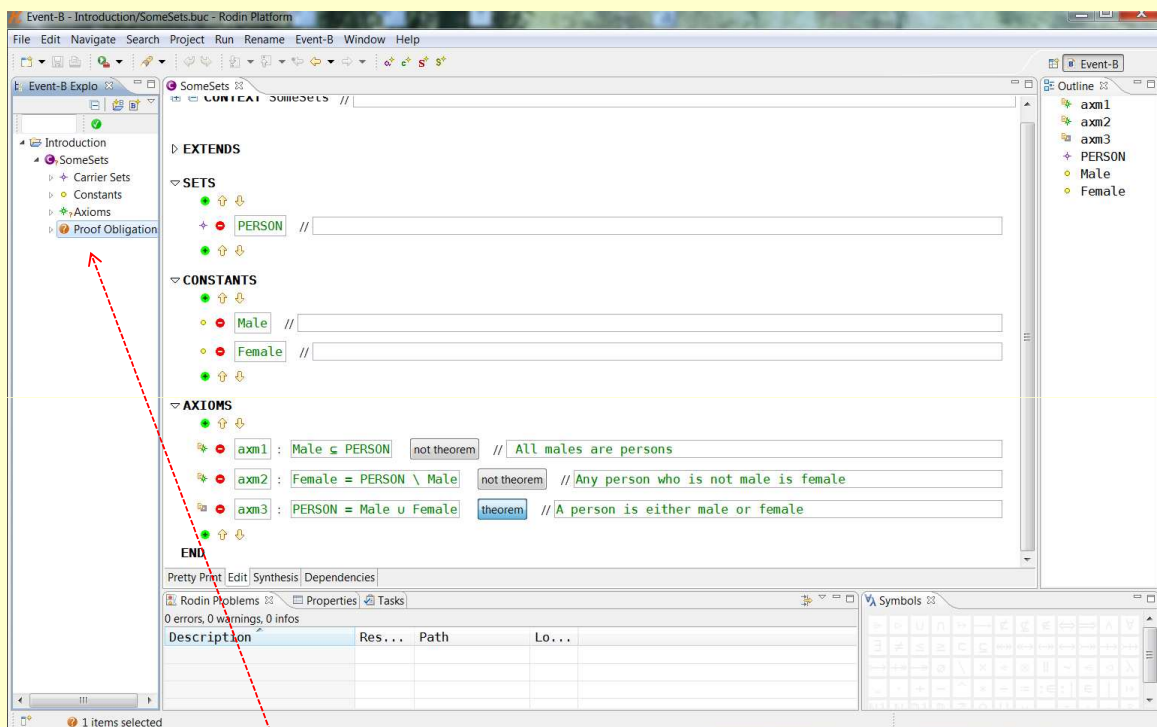
SETS
  PERSON

CONSTANTS
  Male
  Female

AXIOMS
  axm1 : Male  $\subseteq$  PERSON // All males are persons
  axm2 : Female = PERSON \ Male // Any person who is not male is female
  axm3 : PERSON = Male  $\cup$  Female // A person is either male or female

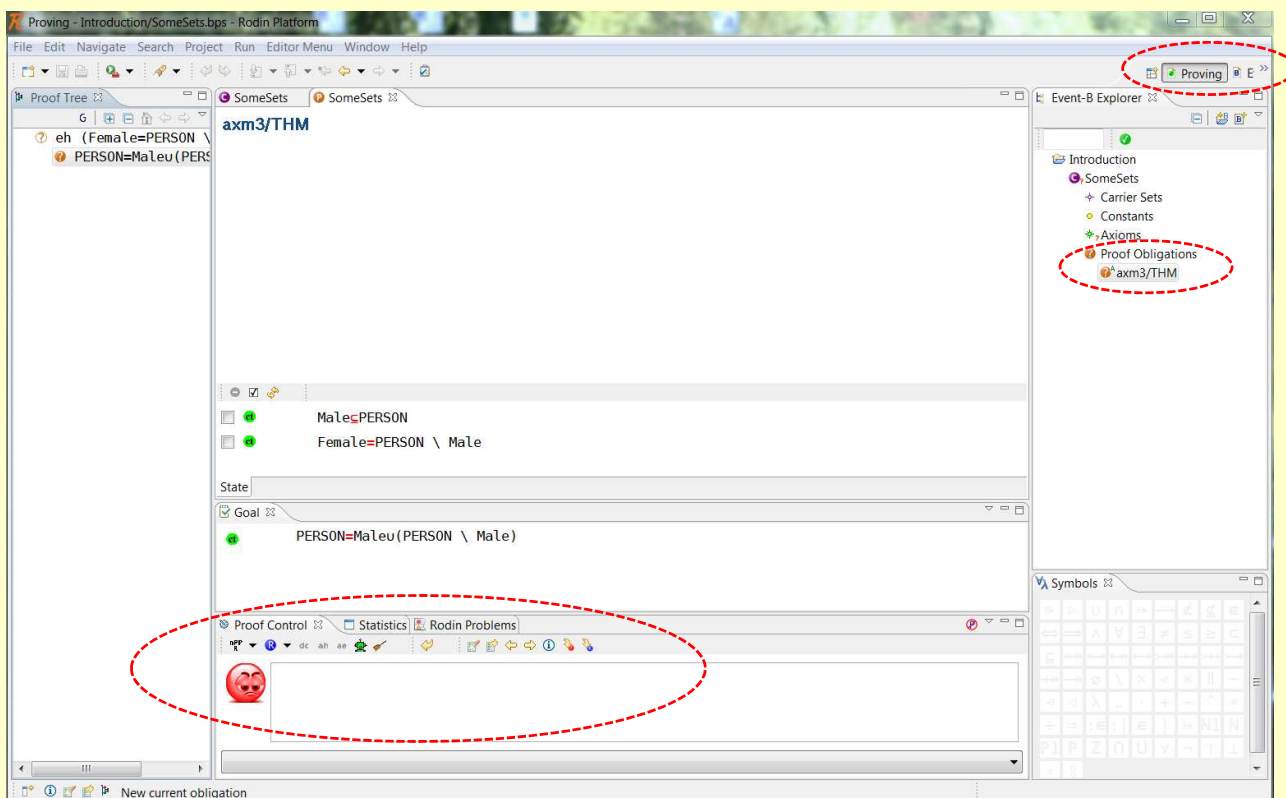
END
```

Use the editor view to specify the required properties about these sets

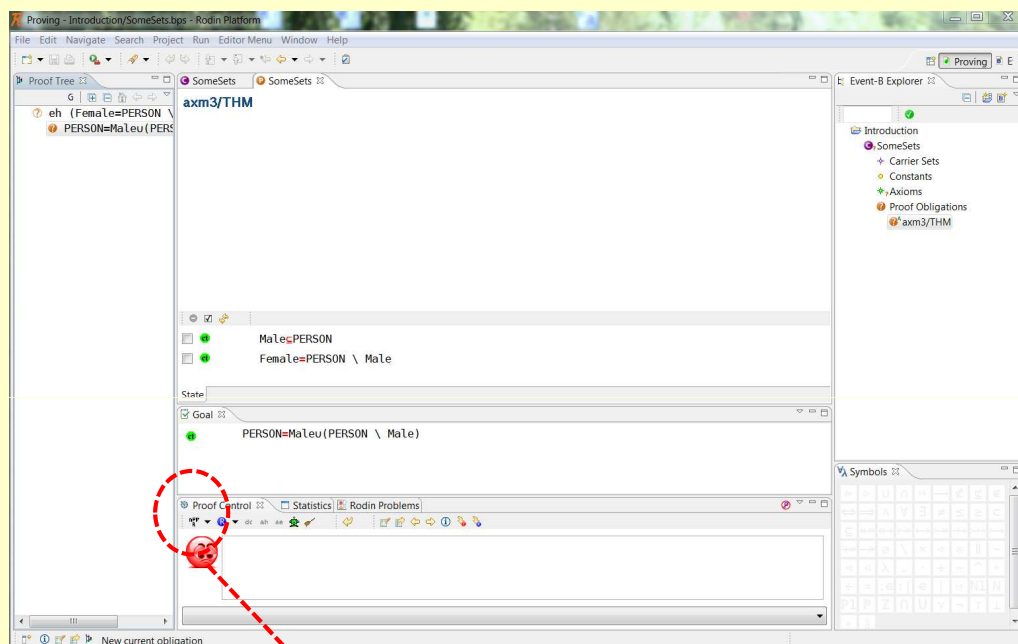


We have a new **Proof Obligation** that has appeared automatically

We can open the Proving perspective to try to prove axm3

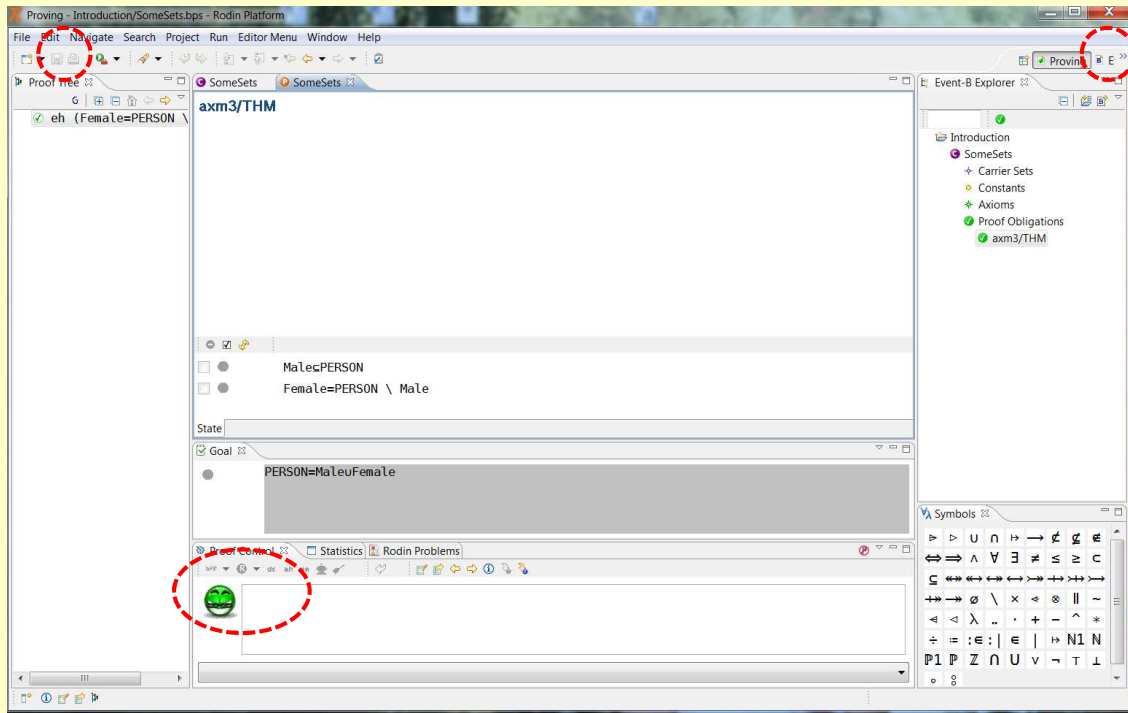


This shouldnt be so hard for a prover to Prove automatically

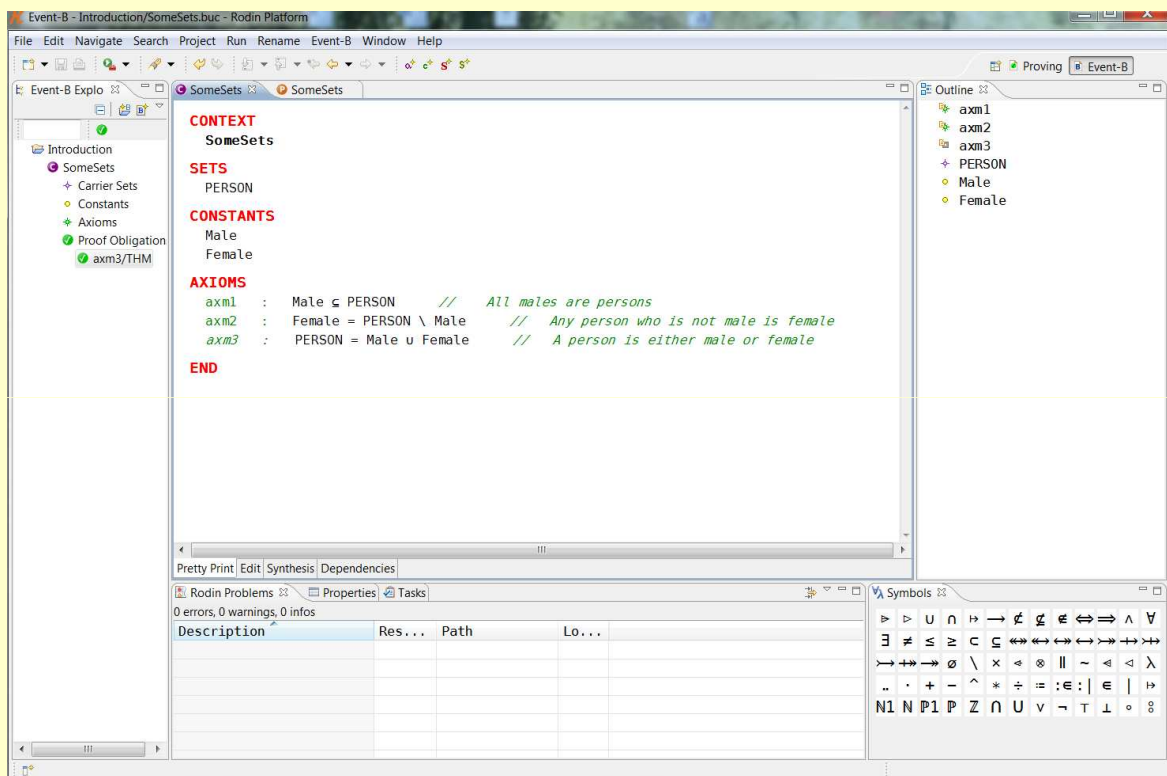


Launch nPP (with all hypotheses)

Now we save the proof and return to the Event-B context



You have proven your first property about a context



Let's add some more sets to our context.

Imagine that we wish to build a context that models family relations

The types of concepts that we need are:

- Mother,
- Father,
- Parent,
- Child,
- Brother,
- Sister,
- Sibling,
- Ancestor,
- Descendant

TO DO: See how many of these you can model using just sets

Parents – the set of people who are mothers or fathers is pretty easy, eg:

CONTEXT

SomeSets

SETS

PERSON

CONSTANTS

Male

Female

Mothers

Fathers

Parents

AXIOMS

```
axm1 : Male  $\subseteq$  PERSON // All males are persons
axm2 : Female = PERSON \ Male // Any person who is not male is female
axm3 : PERSON = Male  $\cup$  Female // A person is either male or female
axm4 : Mothers  $\subseteq$  Female
axm5 : Fathers  $\subseteq$  Male
axm6 : Parents = Mothers  $\cup$  Fathers
```

END

But, it is not clear how to model the other concepts (if it is indeed possible) without introducing relations between sets

RELATIONS

If a set A is given explicitly, it is immaterial in which order the elements of A are listed, e.g. the set $\{x, y\}$ is the same as the set $\{y, x\}$. In many instances, however, one would like, and, indeed, needs, to have some **order** in the appearance of the elements.

We need to capture the notion of **ordering** using Set syntax and semantics.

RELATIONS

Definition Let A be a set:

1. A is called a **singleton** if $A = \{x\}$ for some x , i.e. if A has exactly one element.
2. A is called an **unordered pair**, if $A = \{x, y\}$ for some x, y , if A has exactly two elements.
3. A is called an **ordered pair** if $A = \{\{x\}, \{x, y\}\}$ for some x, y .

We shall usually *abbreviate* the right hand expression by

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$$

RELATIONS

The decisive property of **ordered pairs** is that two ordered pairs are equal if the respective components are the same.

Theorem Let $\langle a, b \rangle$ and $\langle c, d \rangle$ be ordered pairs.

Then $\langle a, b \rangle = \langle c, d \rangle$ **if and only if** $a = c$ and $b = d$.

Remark. The expression “if and only if” means that

1. If $\langle a, b \rangle = \langle c, d \rangle$, then $a = c$ and $b = d$.
2. If $a = c$ and $b = d$, then $\langle a, b \rangle = \langle c, d \rangle$

So, we have to prove two directions, namely 1. and 2.

Usually, “if and only if” is abbreviated as simply “**iff**”.

QUESTION: Can you prove this?

RELATIONS

Definition The **Cartesian (or cross-) product** $A \times B$ of two sets is defined as:

$$A \times B = \{ \langle a, b \rangle : a \in A, b \in B \}$$

This definition can be generalised to more than 2 sets (but we wont do this at the moment)

QUESTION:

- Is it possible that $A \times B = B \times A$?
- If A has n elements and B has m elements, how many elements does $A \times B$ have?

RELATIONS

Definition

Any subset of $A \times B$ is called a relation between A and B

Any subset of $A \times A$ is called a **relation on A**

Since a relation R on A is a subset of $A \times A$, it is an element of the powerset of $A \times A$, i.e. $R \subseteq \mathcal{P}(A \times A)$.

If R is a relation on A and $\langle x, y \rangle \in R$, then we also write:

- xRy , read as “ x is in R -relation to y ”, or simply
- x is in relation to y , if R is understood.

RELATIONS: pictorial representations

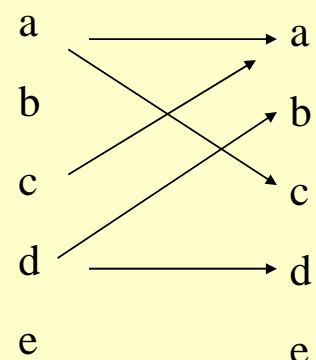
For small sets we can use a pictorial representation of relation R on A

Sketch two copies of A and, if xRy then draw an arrow from the x in the left sketch to the y in the right sketch.

Example,

Let $A = \{a, b, c, d, e\}$, and

$R = \{\langle a, a \rangle, \langle a, c \rangle, \langle c, a \rangle, \langle d, b \rangle, \langle d, d \rangle\}$



RELATIONS: definitions

Definition. Let R be a relation on A . Then,

$\text{dom}R = \{x \in A : \text{There exists some } y \in A \text{ such that } \langle x, y \rangle \in R\}$.
 $\text{dom}R$ is called the **domain** of R .

$\text{ran}R = \{y \in A : \text{There exists some } x \in A \text{ such that } \langle x, y \rangle \in R\}$
is called the **range** of R .

Finally, $\text{fld}R = \text{dom}R \cup \text{ran}R$ is called the field of R .

Note:

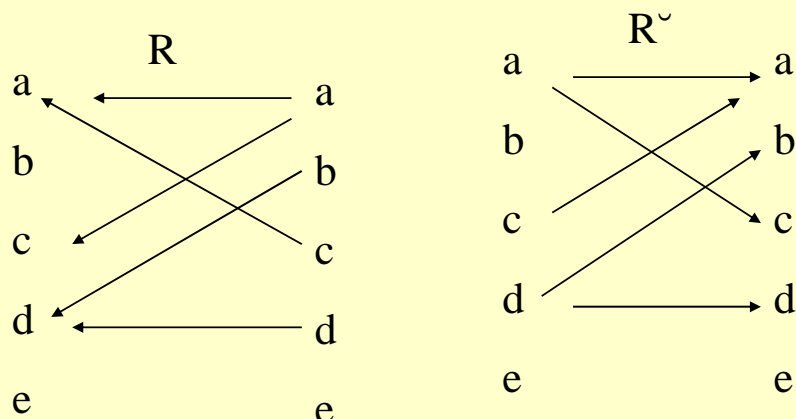
- $\text{dom}R$, $\text{ran}R$, and $\text{fld}R$ are all subsets of A .
- Sometimes they are written dom , ran and fld (when R is implicit in context of use)

RELATIONS: definitions

Definition. Let R be a relation on A . Then,

$R^\smile = \{\langle y, x \rangle : \langle x, y \rangle \in R\}$ is called the **converse** of R .

We obtain the converse R^\smile of R if we turn around all the ordered pairs of R , ie if we have a pictorial representation of R , this means that all existing arrows are reversed.



RELATIONS: definitions

Definition: composition

Let R and S be relations on A ; then

$$R \circ S = \{ \langle x, z \rangle : \text{there is a } y \in A \text{ such that } xRy \text{ and } ySz \}.$$

The operation \circ is called the **composition** or the **relative product** of R and S .

RELATIONS:

Ordering relation example

let $A = \mathbb{N}$ and let R be the relation defined by $\langle x, y \rangle \in R$ iff $x \leq y$;
we note that \leq (or R) has the properties that for all $x, y, z \in \mathbb{N}$:

1. $x \leq x$,
2. If $x \leq y$ and $y \leq x$ then $x = y$,
3. If $x \leq y$ and $y \leq z$ then $x \leq z$,
4. $x \leq y$ or $y \leq x$, i.e. any two elements of \mathbb{N} are comparable with respect to \leq .

RELATIONS: ordering definitions

1. R is **reflexive** if $\langle x, x \rangle \in R$ for all $x \in A$.
2. R is **antisymmetric** if for all $x, y \in A$, $\langle x, y \rangle \in R$ and $\langle y, x \rangle \in R$ implies $x = y$.
3. R is **transitive** if for all $x, y, z \in A$, $\langle x, y \rangle \in R$ and $\langle y, z \rangle \in R$ implies $\langle x, z \rangle \in R$.
4. R is a **partial order** on A , if R is reflexive, antisymmetric, and transitive.

Sometimes we will call a partial order on A just an order on A , or an ordering of A .

5. R is a **linear order** on A if R is a partial order, and xRy or yRx for all $x, y \in A$, i.e. if any two elements of A are comparable with respect to R .

RELATIONS: ordering definitions

If R is an ordering relation on A , then we usually write \leq (or a similar symbol) for R , i.e.

$$x \leq y \text{ iff } xRy$$

If \leq is a **partial order** on A , then we call the pair $\langle A, \leq \rangle$ a **partially ordered set**, or just an **ordered set**.

Furthermore, if \leq is a linear order, then $\langle A, \leq \rangle$ is called a **linearly ordered set** or a **chain**.

PROBLEM:

Let $A = \{1, 2, \dots, 10\}$ and define the relation $\#$ on A by $x\#y$ iff x is a multiple of y . Show that $\#$ is a partial order on A and draw its diagram

RELATIONS: Equivalence Relations

Definition: A relation R on a set A is called **symmetric** if $\langle a, b \rangle \in R$ implies $\langle b, a \rangle \in R$ for all $a, b \in A$;

in other words, R is **symmetric** if $R = R^\smile$.

Definition R is called an **equivalence** relation if R is reflexive, transitive and symmetric

The importance of equivalence relations lies in the fact that they induce a grouping of the base set into subsets.

RELATIONS: Equivalence Relations

Definition: Let A be a non-empty set. A family P of non-empty subsets of A is called a **partition** of A , if every element of A is in exactly one element of P .

In other words,

1. For all $S, T \in P$ we have $S \cap T = \emptyset$,
2. The union of all elements of P is A .

The elements of the partition are called the **classes** of P . A **partition** of A is also called a **classification**.

If P is a partition of A , and if its classes are defined by certain properties, then each element of a specific class has the property which defines the class; in other words all the elements of a class are indistinguishable or equivalent with respect to the defining property of the class.

FUNCTIONS

Definition: A function is an ordered triple $\langle f, A, B \rangle$ such that:

1. A and B are sets, and $f \subseteq A \times B$,
2. For every $x \in A$ there is some $y \in B$ such that $\langle x, y \rangle \in f$
3. If $\langle x, y \rangle \in f$ and $\langle x, z \rangle \in f$, then $y = z$; in other words, the assignment is unique in the sense that an $x \in A$ is assigned at most one element of B .

A is called the **domain** of f , and B its **codomain**.

FUNCTIONS

Definition:

A **partial function** from X to Y is a function $f: X' \rightarrow Y$, where X' is a subset of X .

It generalizes the concept of a function by not forcing f to map every element of X to an element of Y (only some subset $X' \subseteq X$).

If $X' = X$, then f is called a total function and is equivalent to a function (as defined previously).

Partial functions are often used when the exact domain, X' , is not known .

FUNCTIONS

Notation:

It is customary to write the function $\langle f, A, B \rangle$ as

$$f : A \rightarrow B$$

Also, if $\langle x, y \rangle \in f$, then we will usually write

$$y = f(x)$$

and call y the **image** of x under f .

The set $\{y \in B : \text{There is an } x \in A \text{ such that } y = f(x)\}$ is called the **range** of f .

FUNCTIONS

If for a function $f : A \rightarrow B$ it is clear what A and B are, we sometimes call the function simply f , but we must keep in mind that a function is only properly defined if we also give a domain and a codomain!

Definition Let $f : A \rightarrow B$ be a function.

1. If $A = B$ and $f(x) = x$ for all $x \in A$, the f is called the **identity** function on A , and it is denoted by id_A

FUNCTIONS

Definition Let $f : A \rightarrow B$ be a function.

If $A \subseteq B$ and $f(x) = x$ for all $x \in A$, then f is called the **inclusion** function from A to B , or, if no confusion can arise, simply the inclusion.

If $A = B$ and f is the inclusion, then f is in fact the identity on A .

FUNCTIONS

Definitions Let $f : A \rightarrow B$ be a function.

If $f(x) = x$ for some $x \in A$, then x is called a **fixed point** of f .

If $f(x) = b$ for all $x \in A$, then f is called a **constant function**.

If $g : C \rightarrow D$ is a function such that $A \subseteq C$, $B \subseteq D$, and $f \subseteq g$, then g is called an **extension** of f over C , and f is called the **restriction** of g to A .

FUNCTIONS

Definition

Let $f : A \rightarrow B$ and $g : C \rightarrow D$ be functions such that

$\text{ran } f \subseteq \text{dom } g$.

Then the function $g \circ f : A \rightarrow D$ defined by $(g \circ f)(x) = g(f(x))$ is called the **(functional) composition** of f and g .

Lemma Let $f : A \rightarrow B$, $g : B \rightarrow C$, $h : C \rightarrow D$ be functions. Then,
 $h \circ (g \circ f) = (h \circ g) \circ f$,

i.e. the composition of functions is associative

FUNCTIONS

Definitions Let $f : A \rightarrow B$

f is called **onto** or **surjective** if $\text{codom } f = \text{ran } f$. If f is surjective, we sometimes indicate this by writing

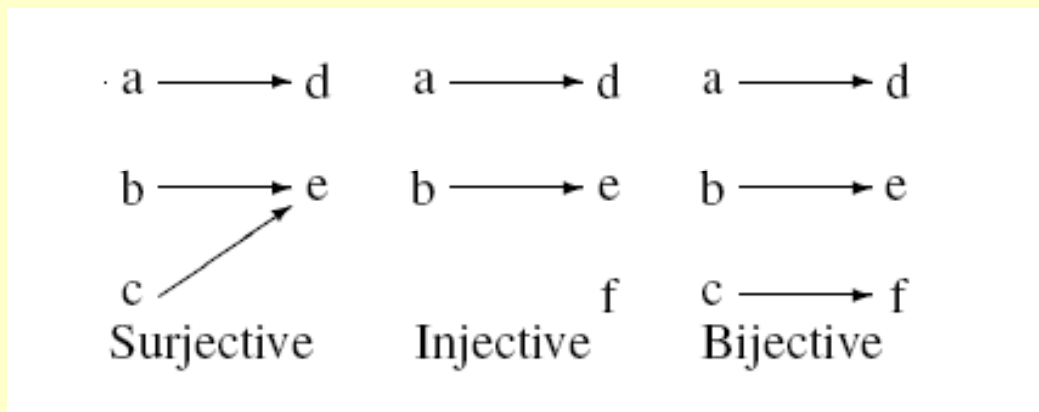
$$f : A \twoheadrightarrow B.$$

f is called **one-one** or **injective** if for all $x, y \in A$, $f(x) = f(y)$ implies $x = y$. If f is injective, we sometimes indicate this by writing

$$f : A \hookrightarrow B.$$

f is called **bijective** if f is onto and one-one

FUNCTIONS



QUESTION: Give an example of these types of function over the sets of *people*

FUNCTIONS

Definition Let $f : A \rightarrow B$ and $g : B \rightarrow A$ be functions;

g is called the inverse of f , if $g(f(x)) = x$ for all $x \in A$.

It is often written as: f^{-1}

In other words, g is an inverse of f , if and only if $g \circ f = id_A$

Theorem $f : A \rightarrow B$ has an inverse
if and only if
 f is injective

FUNCTIONS

Definition

Let $A = \{1, 2, 3, \dots, n\}$, and $f : A \rightarrow A$ be a bijective function; then f is called a **permutation** on n .

QUESTION: for a set with N elements then how many permutations exist?

CODING TASK: Write a program to generate all the permutations of a set of integers, and to count the number generated. Does your program verify your answer to the question, above?

Let us return to the family in RODIN to try and model the relationships

CONTEXT

SomeSets

SETS

PERSON

CONSTANTS

Male
Female
Mothers
Fathers
Parents
MotherOf
FatherOf
ParentOf

AXIOMS

```
axm1 : Male ⊆ PERSON // All males are persons
axm2 : Female = PERSON \ Male // Any person who is not male is female
axm3 : PERSON = Male ∪ Female // A person is either male or female
axm4 : Mothers ⊆ Female
axm5 : Fathers ⊆ Male
axm6 : Parents = Mothers ∪ Fathers
axm7 : MotherOf ∈ PERSON → Mothers // All persons have a single Mother
axm8 : FatherOf ∈ PERSON → Fathers // All persons have a single Father
axm9 : ParentOf = MotherOf ∪ FatherOf // Your parent is either:
// your mother or your father
```

END

TO DO (before next week):

Attempt to add new family relations to the axioms

Attempt to introduce new theorems

Can the prover discharge the proof obligations automatically?

A sample solution to this problem will be put on-line before the next session; but you should try it for yourselves.

The next 2 sessions are practical work with RODIN involving sets and relations. They will be taught by Jean-Luc Raffy (the director of the MSc SAI)