Doing Mathematics with the Rodin Platform
Using the “Theory” Plug-in

Jean-Raymond Abrial

July 2014

Introduction: Z, B and Event-B

- 1980: Z

- 1996 : B

- 2010: Event-B

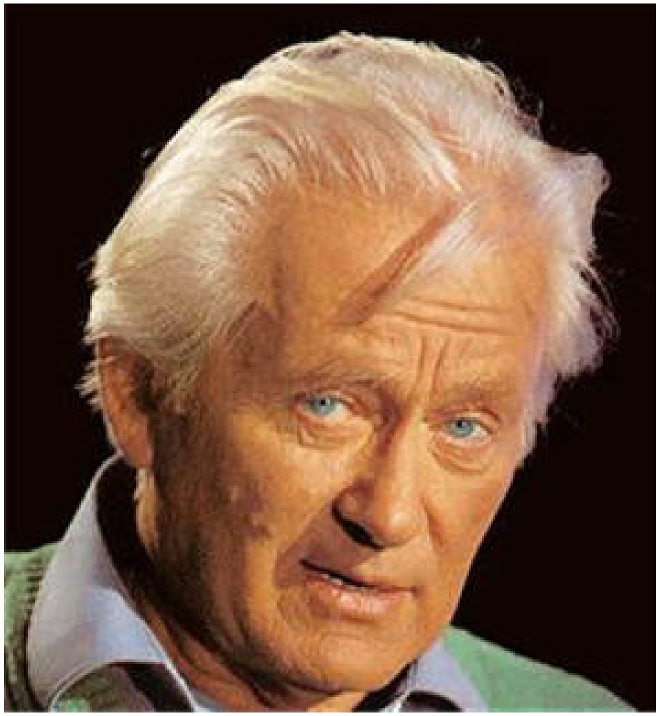
Introduction: the Mathematical Language

- In all 3 cases, the mathematical language is that of typed set theory

- In all 3 cases, the used language is limited (not easily extensible)

- The (free) tool for Event-B is called the Rodin Platform (RP)

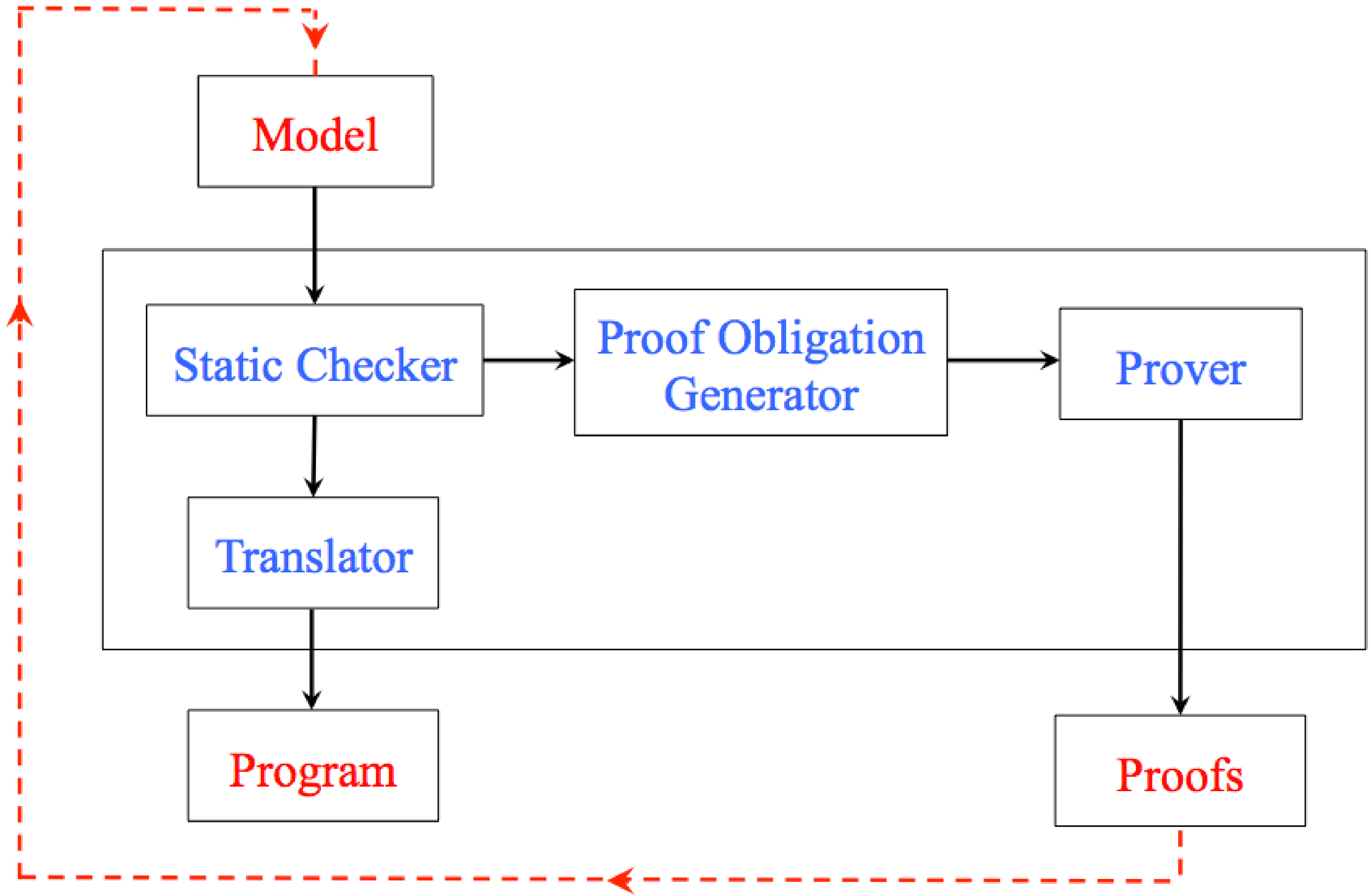
George Charpak (French Nobel Prize Winner in Physics)



- George Charpak, are you a theoretician?

No, I am not, but I know the theory,

and my tool is the mirror of the theory


Model
Static Checker
Proof Obligation Generator
Prover
Translator
Program
Proofs

Introduction: The "Theory" Plugin

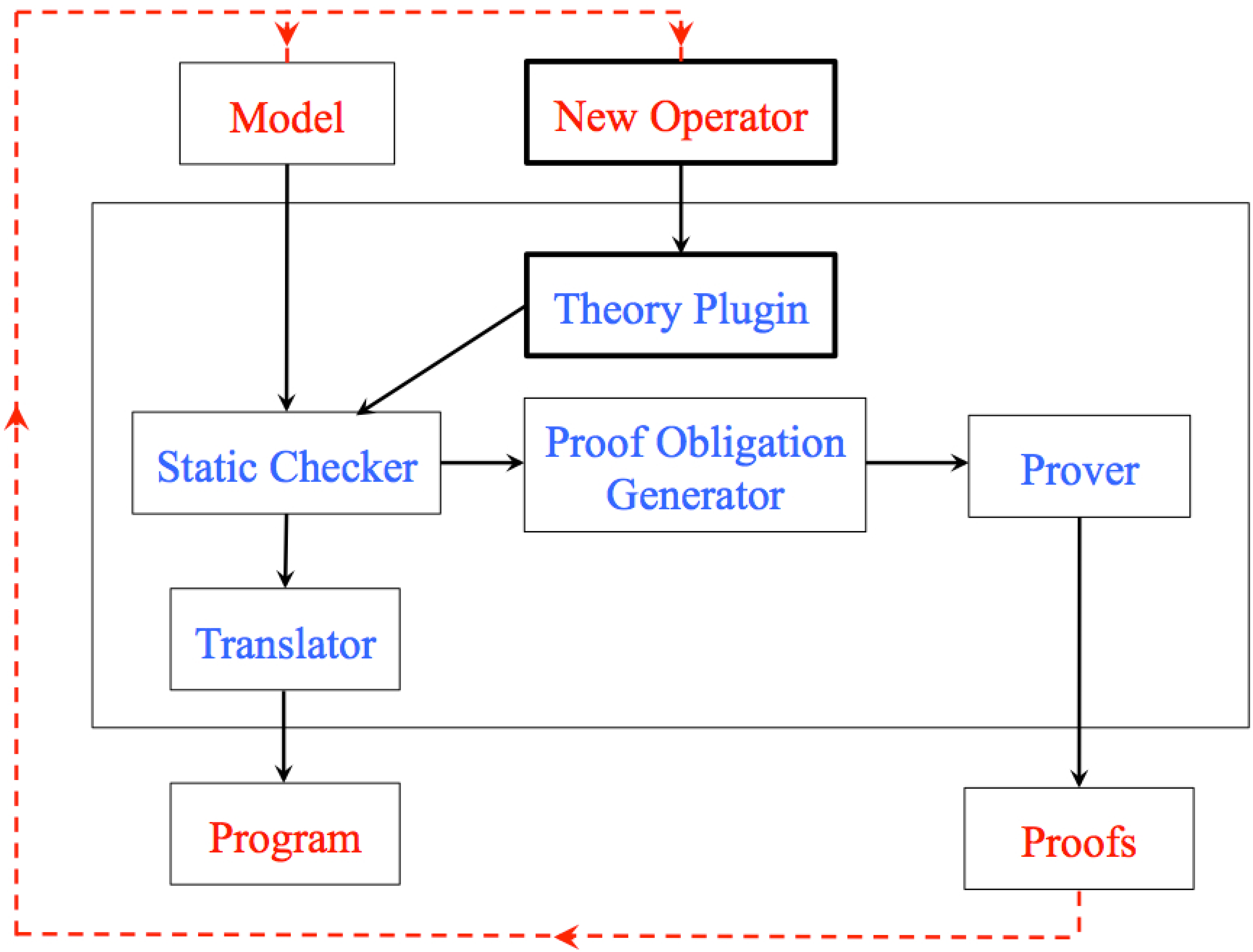
- As mentioned, the mathematical language was so far limited

- But recently, we develop a way to extend the set language of RP

- This is done by the, so called, Theory Plugin

- In this talk, I will present this plugin (with several demos)

The Rodin Platform with the "Theory" Plugin



Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science:

  1. Fixpoint
  2. Transitive closure
  3. Well-foundedness

Definition of the Fixpoint of a Set Function

- We are given a set function f

$$f \in \mathbb{P}(S) \to \mathbb{P}(S)$$

- We would like to construct a subset $\mathsf{fix}(f)$ of S such that:

$$\mathsf{fix}(f) = f(\mathsf{fix}(f))$$

- Proposal:

$$\boxed{\mathsf{fix}(f) \ \widehat{=} \ \mathrm{inter}(\{s \mid f(s) \subseteq s\})}$$

- fix(f) is a lower bound of the set $\{s \mid f(s) \subseteq s\}$

$$\forall s \cdot f(s) \subseteq s \Rightarrow \text{fix}(f) \subseteq s$$

- fix(f) is the greatest lower bound of the set $\{s \mid f(s) \subseteq s\}$

$$\forall v \cdot (\forall s \cdot f(s) \subseteq s \Rightarrow v \subseteq s) \Rightarrow v \subseteq \text{fix}(f)$$

Transforming the Lemmas into Inference Rules

$$\forall s \cdot f(s) \subseteq s \;\Rightarrow\; \mathsf{fix}(f) \subseteq s$$

$$\frac{f(s) \subseteq s}{\mathsf{fix}(f) \subseteq s}$$

$$\forall v \cdot (\forall s \cdot f(s) \subseteq s \;\Rightarrow\; v \subseteq s) \;\Rightarrow\; v \subseteq \mathsf{fix}(f)$$

$$\frac{\forall s \cdot f(s) \subseteq s \;\Rightarrow\; v \subseteq s}{v \subseteq \mathsf{fix}(f)}$$

The Main Result (Knaster-Tarski Theorem)

- Additional needed constraint: f is monotone

$$\forall a, b \cdot a \subseteq b \;\Rightarrow\; f(a) \subseteq f(b)$$
$$\Rightarrow$$
$$\text{fix}(f) = f(\text{fix}(f))$$

- DEMO

Naive Approach at the Irreflexive Transitive Closure r^+

- We are given a binary relation $\boldsymbol{r}$ built on a set $\boldsymbol{S}$:

$$\boldsymbol{r} \in \mathbb{P}(\boldsymbol{S} \times \boldsymbol{S})$$

- The irreflexive transitive closure $\boldsymbol{r}^+$ of r is "defined" as follows:

$$\boldsymbol{r}^+ \;=\; \boldsymbol{r} \cup \boldsymbol{r}^2 \cup \ldots \cup \boldsymbol{r}^n \cup \ldots$$

Naive Approach at the Irreflexive Transitive Closure r^+

$$r^+ \;=\; r \cup r^2 \cup \ldots \cup r^n \cup \ldots$$

- Let us compose r^+ with r

$$\begin{aligned} r^+ \,;\, r &= (r \;\cup\; r^2 \;\cup\; r^3 \;\cup\; \ldots \;\cup\; r^n \;\cup\; \ldots) \,;\, r \\ &= (r \,;\, r) \;\cup\; (r^2 \,;\, r) \;\cup\; \ldots \;\cup\; (r^n \,;\, r) \;\cup\; \ldots \\ &= r^2 \;\cup\; r^3 \;\cup\; \ldots \;\cup\; r^{n+1} \;\cup\; \ldots \end{aligned}$$

Hence we have a fixpoint equation

$$r^+ \;=\; r \cup (r^+ \,;\, r)$$

Mathematical Definition of Irreflexive Transitive Closure r^+

$$\boldsymbol{r}^+ \;=\; \boldsymbol{r} \cup (\boldsymbol{r}^+ \,;\, \boldsymbol{r})$$

- $\boldsymbol{r}^+$ can thus be defined to be the fixpoint of a function

$$\boxed{\boldsymbol{r}^+ \;\widehat{=}\; \mathsf{fix}(\boldsymbol{\lambda s} \cdot \boldsymbol{s} \in \mathbb{P}(\boldsymbol{S} \times \boldsymbol{S}) \,|\, \boldsymbol{r} \cup (\boldsymbol{s} \,;\, \boldsymbol{r}))}$$

- Notice that this function is monotone

Main Results of Irreflexive Transitive Closure r^+

$$r \subseteq r^+$$

$$\forall s \cdot \begin{array}{l} r \subseteq s \\ s \,;\, r \subseteq s \\ \Rightarrow \\ r^+ \subseteq s \end{array}$$

$$r^+ \,;\, r \subseteq r^+$$

$$r^+ \,;\, r^+ \subseteq r^+$$

$$\forall b \cdot r[b] \subseteq b \Rightarrow r^+[b] \subseteq b$$

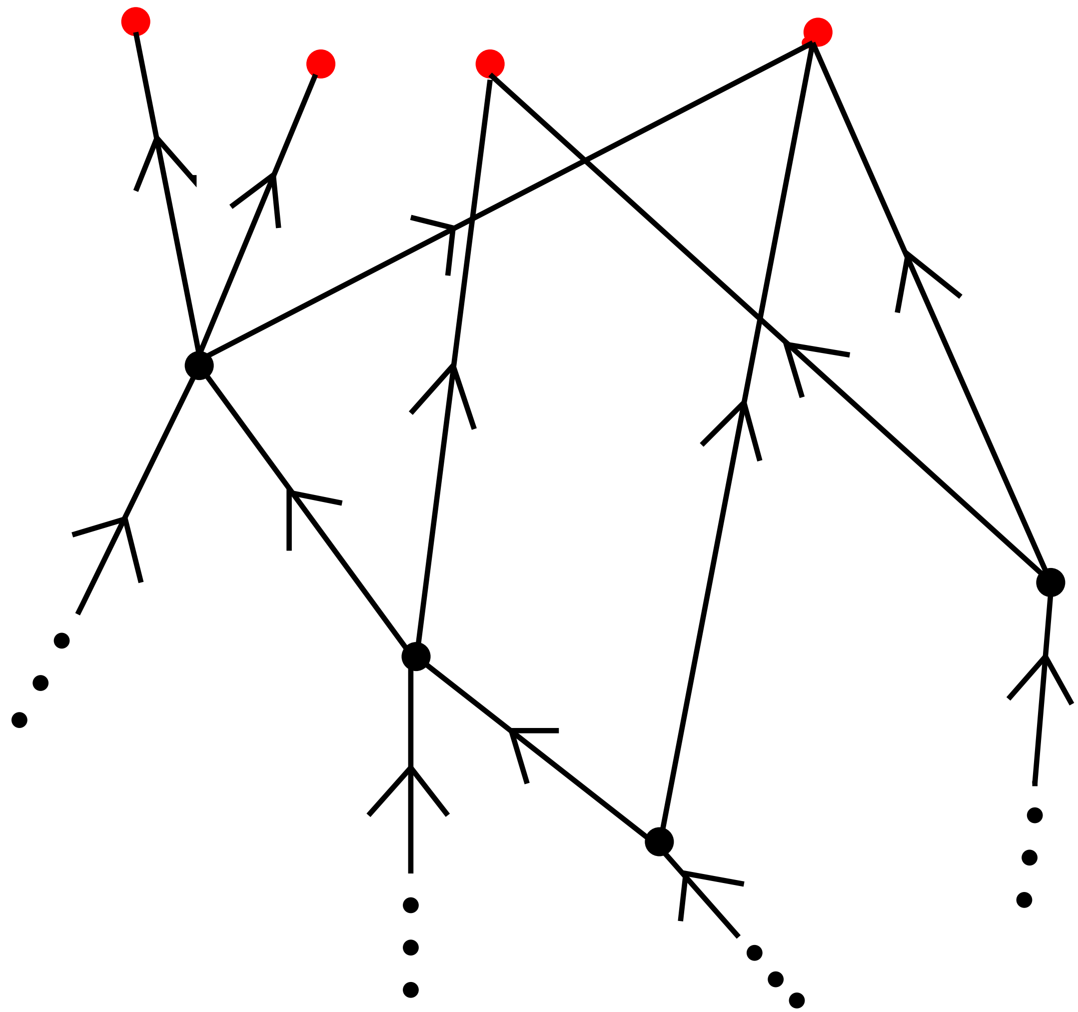
$$r^+ = r \cup (r \,;\, r^+)$$

$$r^+ = r \cup (r^+ \,;\, r)$$

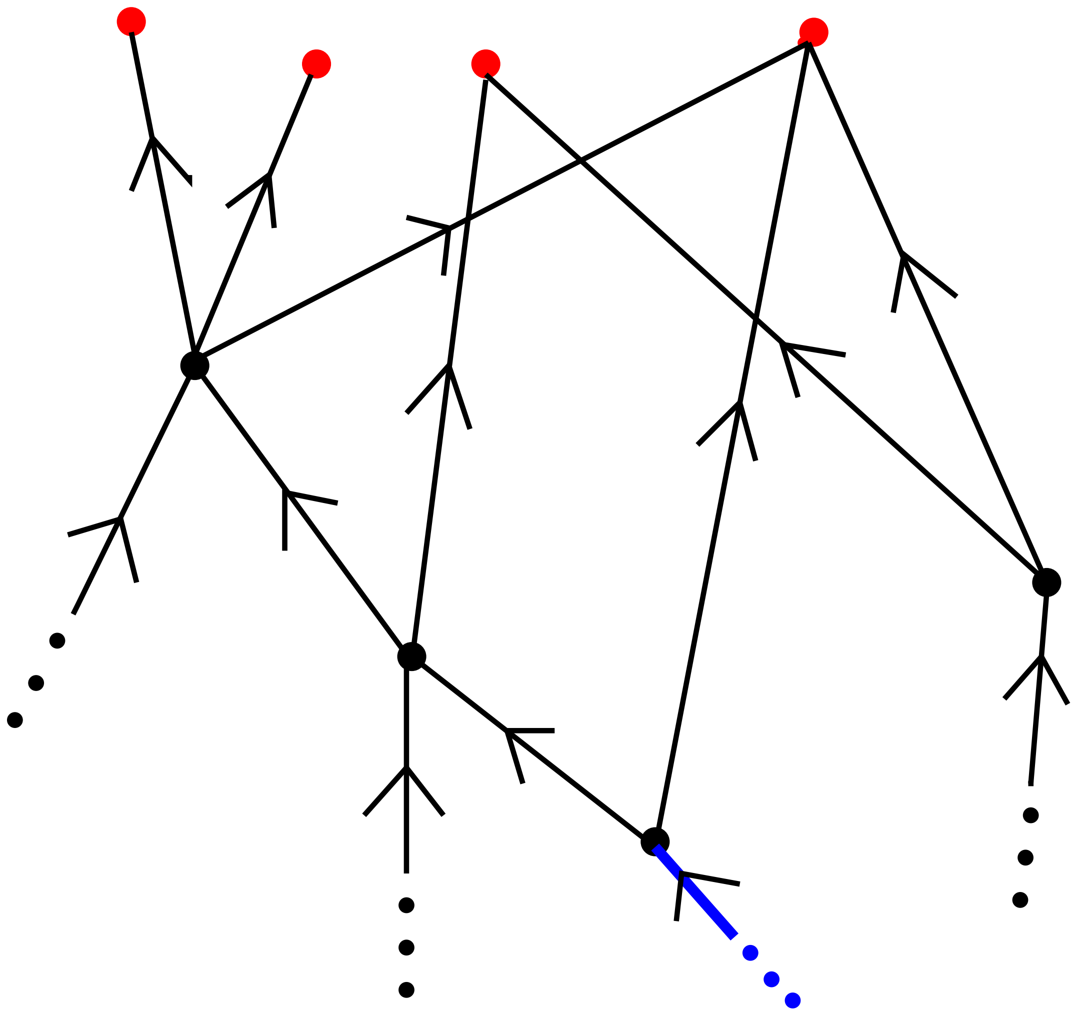
$$(r^{-1})^+ = (r^+)^{-1}$$

- DEMO

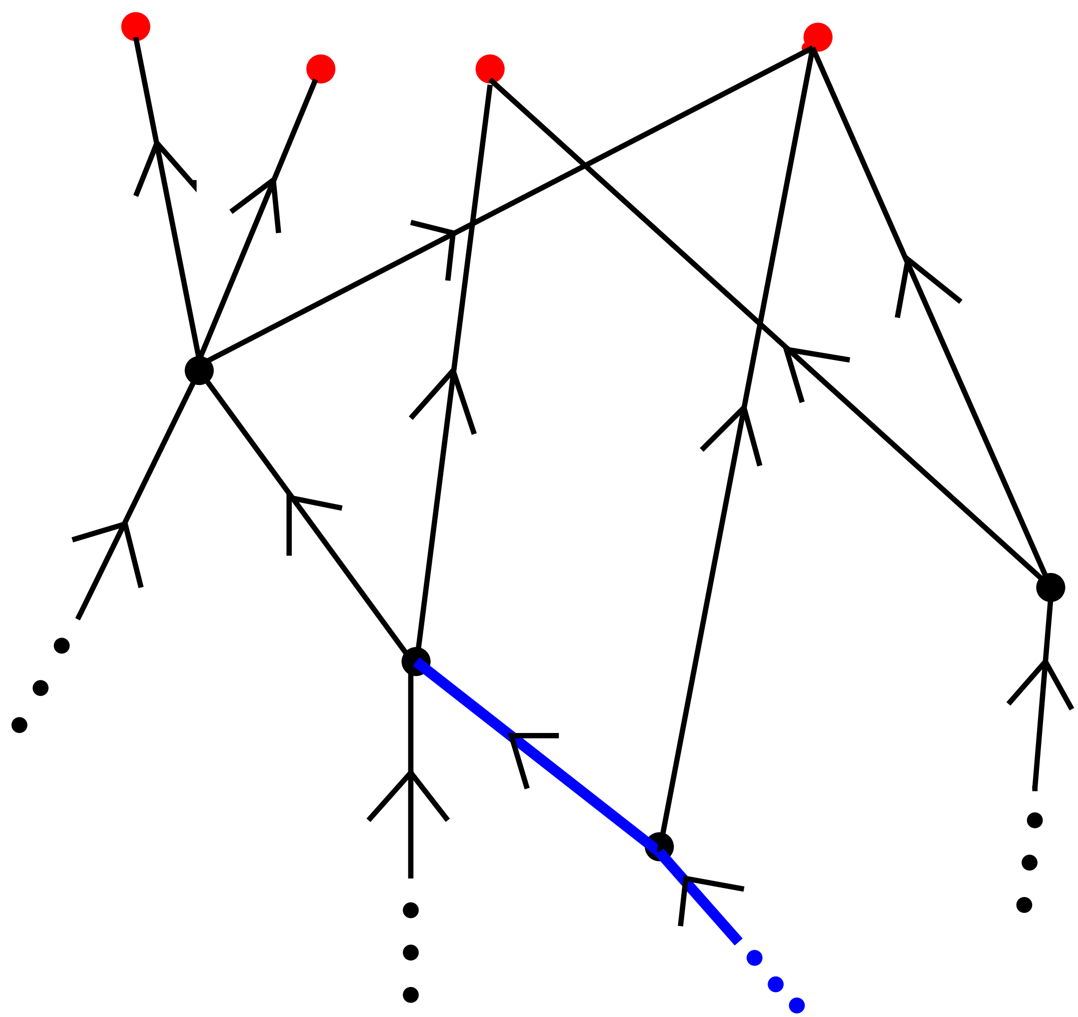
A Well-founded Relation



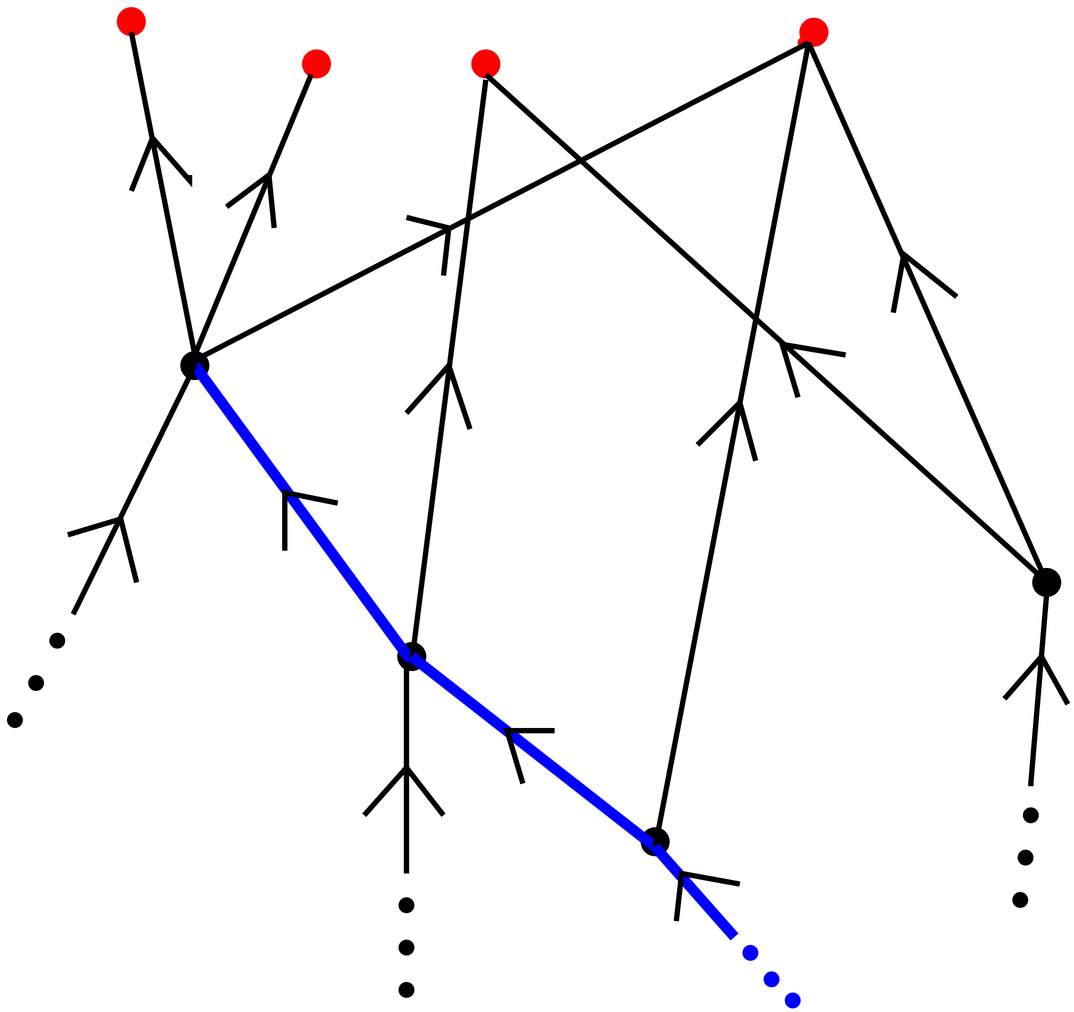
A Well-founded Relation



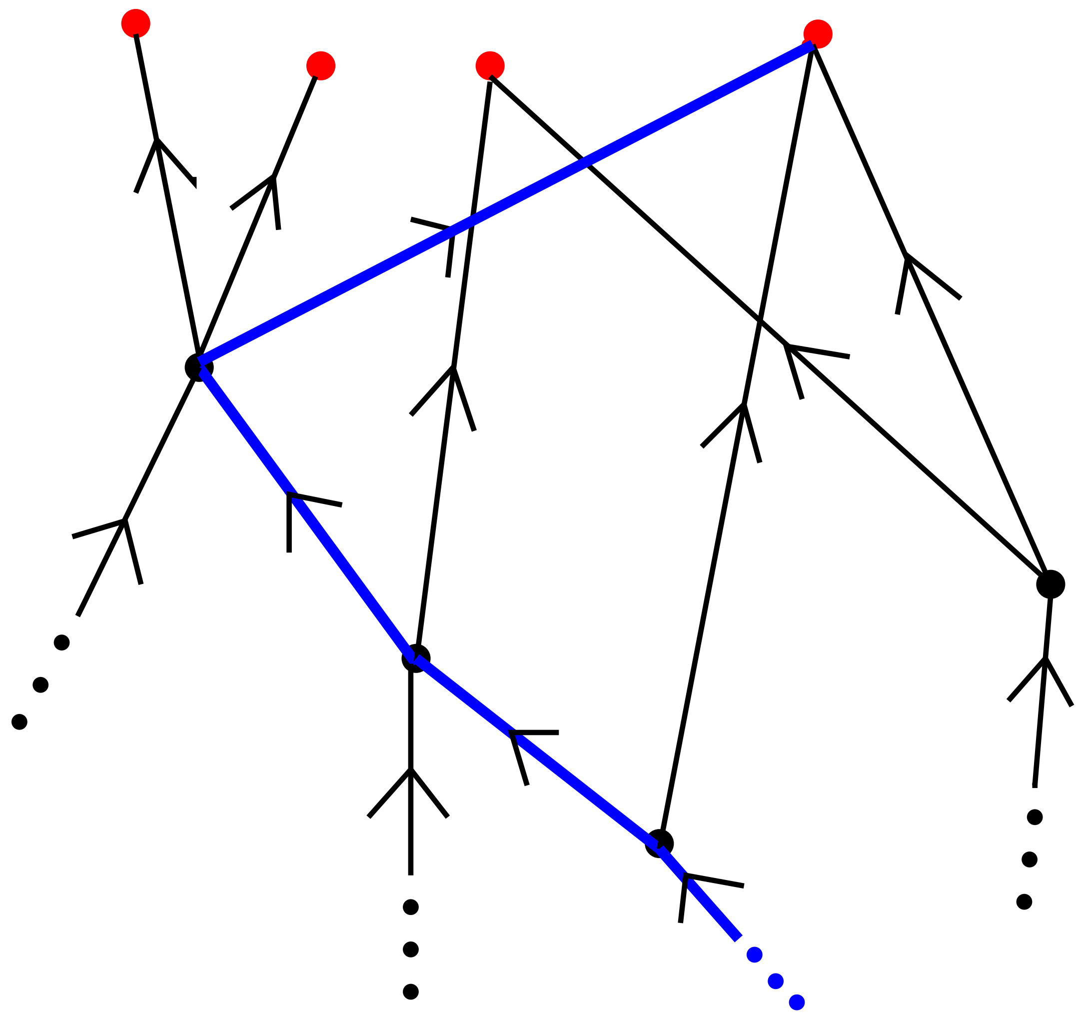
A Well-founded Relation



A Well-founded Relation



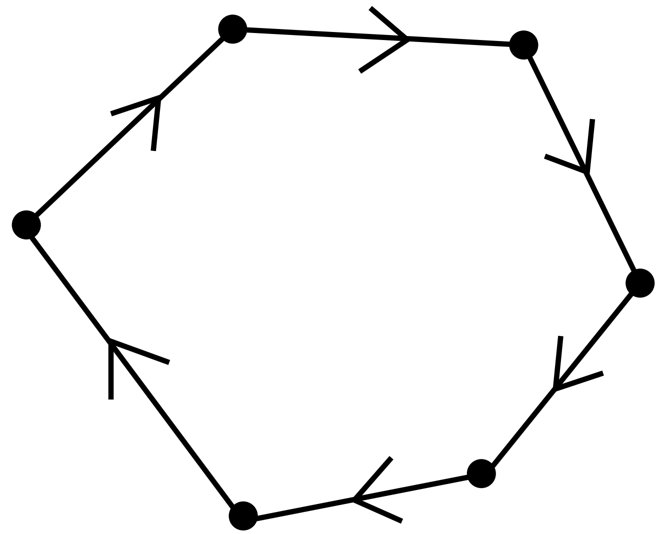
A Well-founded Relation



- From any point in the graph
- You always reach a red point after a FINITE TRAVEL

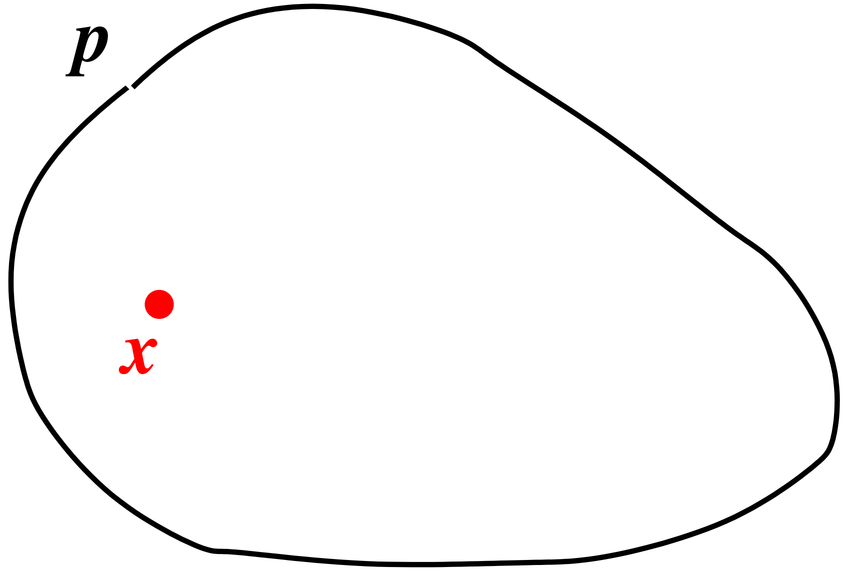
Relations that are not Well-founded: no Red Points

- A cycle



- An infinite chain

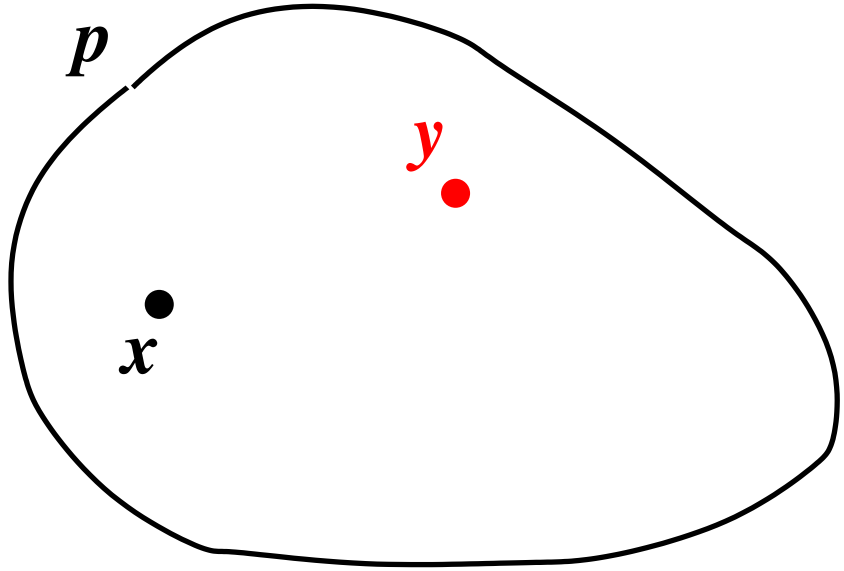
Non-empty Set p Containing a Cycle or an Infinite Chain



For all x in p

$$\forall x \cdot x \in p \;\Rightarrow$$

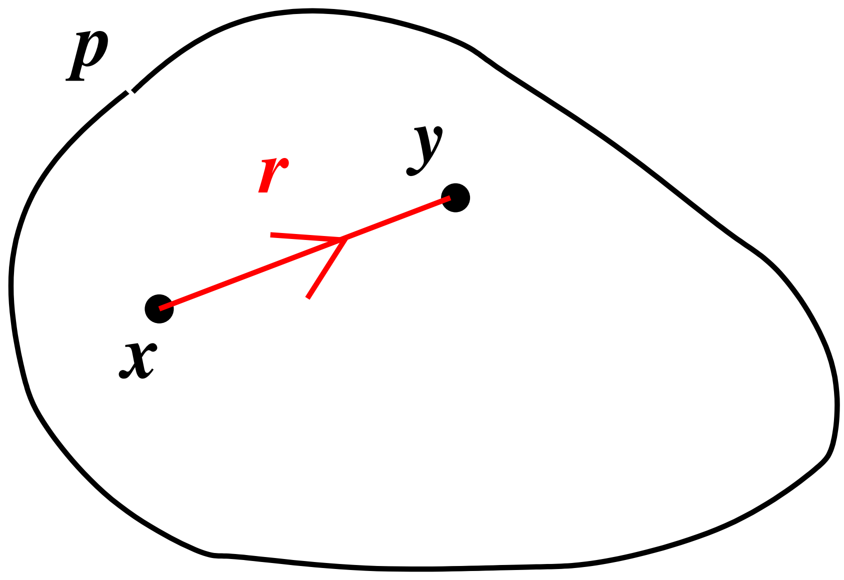
Non-empty Set p Containing a Cycle or an Infinite Chain



For all x in p there exists a y in p

$$\forall x \cdot x \in p \;\Rightarrow\; (\exists y \cdot y \in p \;\wedge$$

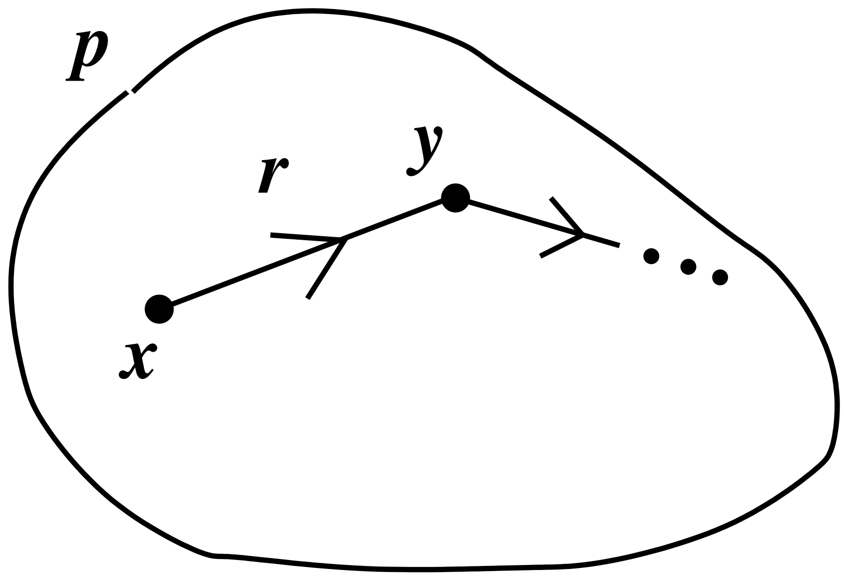
Non-empty Set p Containing a Cycle or an Infinite Chain



For all x in p there exists a y in p related to x by relation r

$$\forall x \cdot x \in p \;\Rightarrow\; (\exists y \cdot y \in p \;\land\; x \mapsto y \in r)$$

Non-empty Set p Containing a Cycle or an Infinite Chain



For all x in p there exists a y in p related to x by relation r

$$\forall x \cdot x \in p \;\Rightarrow\; (\exists y \cdot y \in p \;\wedge\; x \mapsto y \in r)$$

- That is:

$$p \subseteq r^{-1}[p]$$

Definition of a Well-founded Relation

- A well-founded relation does not contain such a set $\boldsymbol{p}$ . . .

- . . . unless it is the empty set

$$\boxed{\mathsf{wf}(\boldsymbol{r}) \;\widehat{=}\; \forall \boldsymbol{p} \cdot \boldsymbol{p} \subseteq \boldsymbol{r}^{-1}[\boldsymbol{p}] \;\Rightarrow\; \boldsymbol{p} = \varnothing}$$

- DEMO

- If a relation r is well-founded than so is r^+

$$\text{wf}(r) \;\vdash\; \text{wf}(r^+)$$

- That is:

$$\forall p \cdot p \subseteq r^{-1}[p] \;\Rightarrow\; p = \varnothing \;\vdash\; \forall p \cdot p \subseteq (r^+)^{-1}[p] \;\Rightarrow\; p = \varnothing$$

- That is:

$$\forall p \cdot p \subseteq r^{-1}[p] \;\Rightarrow\; p = \varnothing \,,\; p \subseteq (r^+)^{-1}[p] \;\vdash\; p = \varnothing$$

Informal Intuition(2)

$$\forall p \cdot p \subseteq r^{-1}[p] \;\Rightarrow\; p = \varnothing \;,\; p \subseteq (r^{+})^{-1}[p] \;\vdash\; p = \varnothing$$

- In order to prove $p = \varnothing$, it is sufficient to prove $(r^{+})^{-1}[p] = \varnothing$

- Therefore, we instantiate the quantified variable p with $(r^{+})^{-1}[p]$

- It remains now for us to prove:

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; (r^{+})^{-1}[p] \;\subseteq\; r^{-1}[(r^{+})^{-1}[p]]$$

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; (r^{+})^{-1}[p] \;\subseteq\; r^{-1}[(r^{+})^{-1}[p]]$$

- That is:

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; (r^{-1})^{+}[p] \;\subseteq\; \underline{r^{-1}[(r^{-1})^{+}[p]]}$$

- That is:

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; (r^{-1})^{+}[p] \;\subseteq\; \underline{((r^{-1})^{+}; r^{-1})[p]}$$

Informal Intuition(4)

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; \underline{(r^{-1})^{+}[p] \;\subseteq\; ((r^{-1})^{+}; r^{-1})[p]}$$

- But, we have $(r^{-1})^{+} = r^{-1} \cup ((r^{-1})^{+}; r^{-1})$

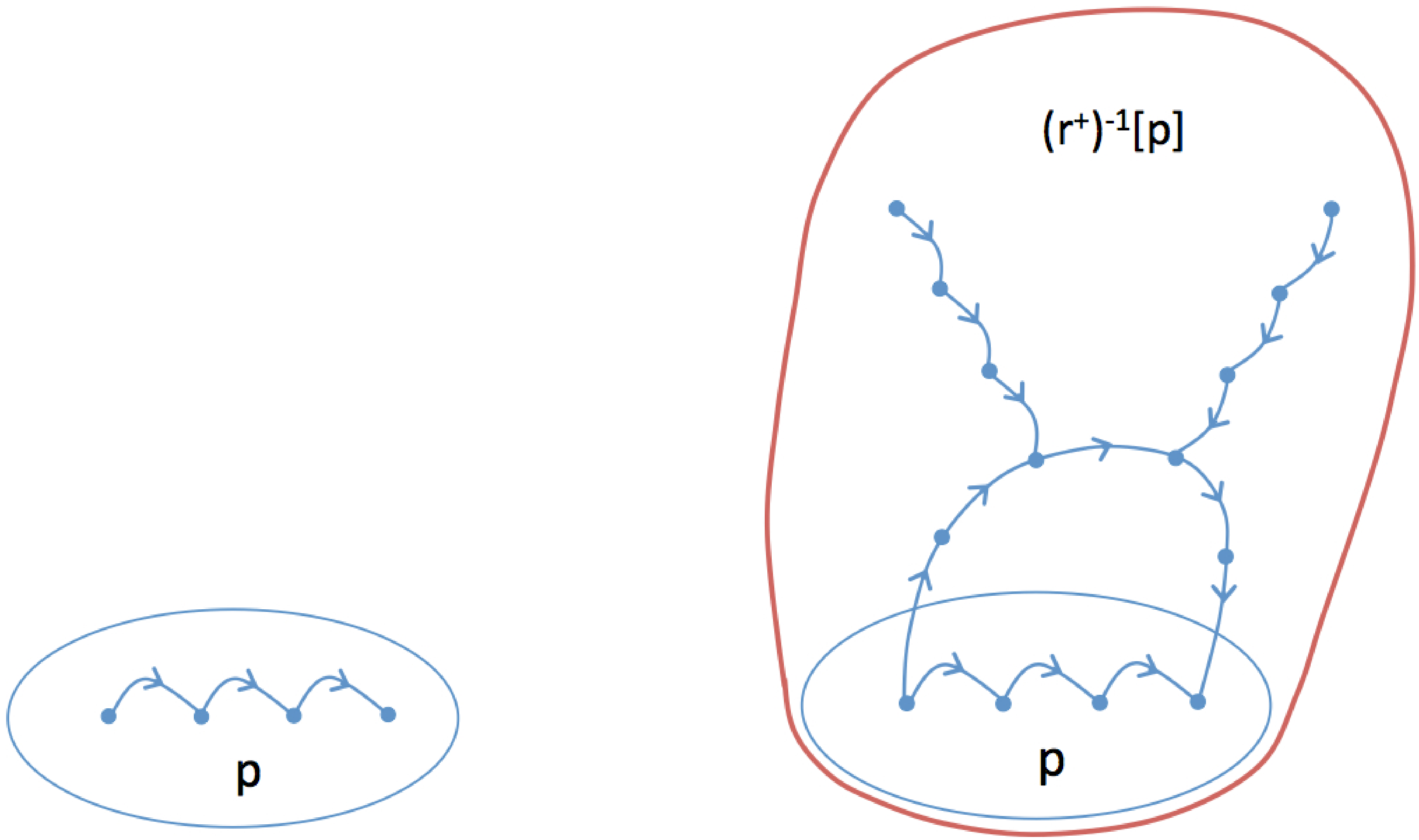
- Thus: $\underline{(r^{-1})^{+}[p] = r^{-1}[p] \cup ((r^{-1})^{+}; r^{-1})[p]}$

- But we also have:

$$p \subseteq (r^{+})^{-1}[p] \;\vdash\; r^{-1}[p] \;\subseteq\; ((r^{-1})^{+}; r^{-1})[p]$$

- Thus: $\underline{(r^{-1})^{+}[p] = ((r^{-1})^{+}; r^{-1})[p]}$ QED

Informal Intuition (5)



- DEMO

Conclusion (4 years ago)

- The pros:
  - all proofs done with the Rodin Platform
  - all proofs done "easily"

- The cons:
  - theorems cannot be reused easily
  - they have to be instantiated manually

- What next (the solution):
  - mathematical extensions: NOW WE HAVE IT