Rodin User and Developer Worksop

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

Jean-Raymond Abrial

June 2014

# Outline: Some Mathematical Studies



- Some important mathematical concepts (in Computer Science):

1. Well-foundedness
2. Fixpoint
3. Transitive closure
4. Computation
5. Real Numbers
6. Some theorems (time permiting)

# Purpose of this Presentation



- We want to do some mathematical studies of these fields

- Showing some generic proofs done with the “Theory” plug-in

# 1. Well-foundedness

# Motivation for Well-founded Sets and Relations

- This mathematical structure formalizes the notion of reachability

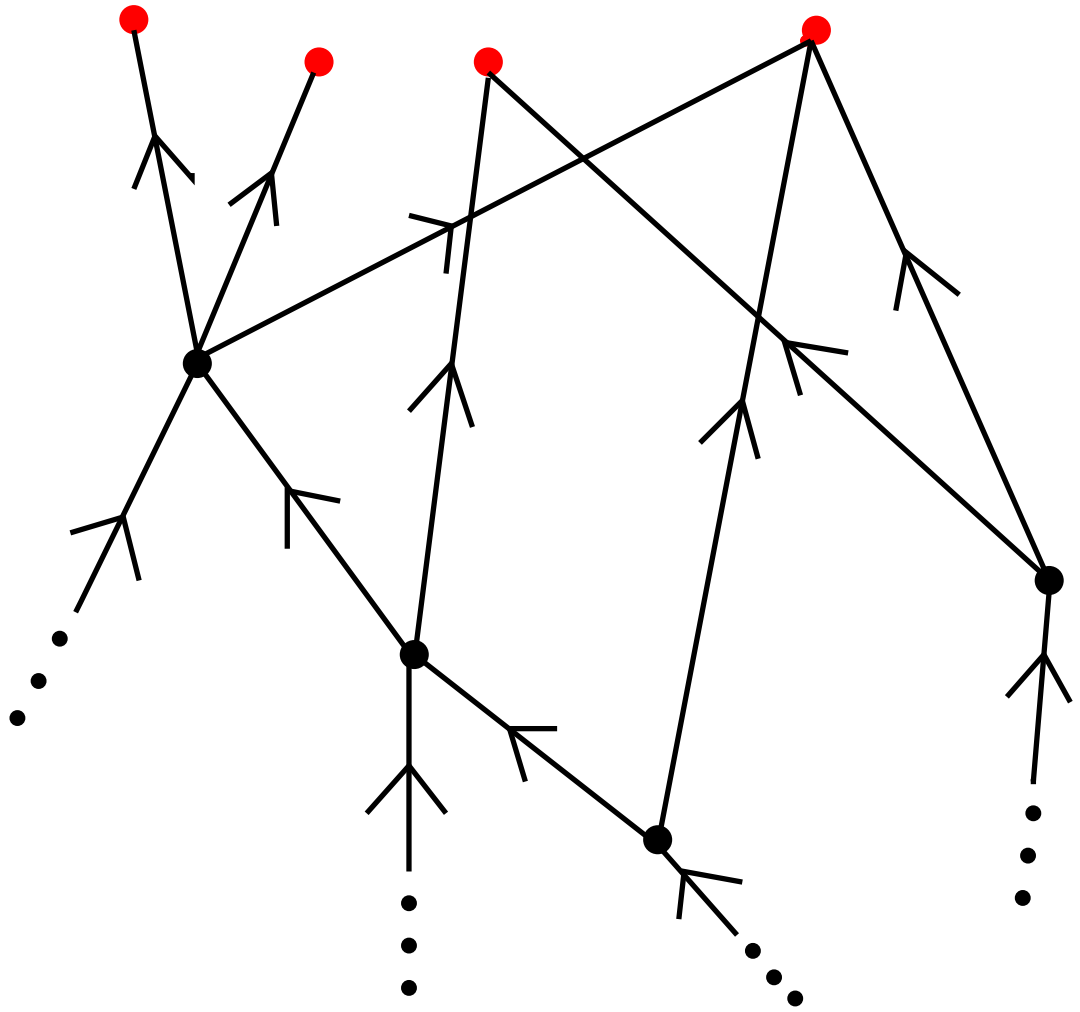
- A discrete transition process, which:

    - either terminates
    - or eventually reaches certain states

- is formalized by means of well-founded traces

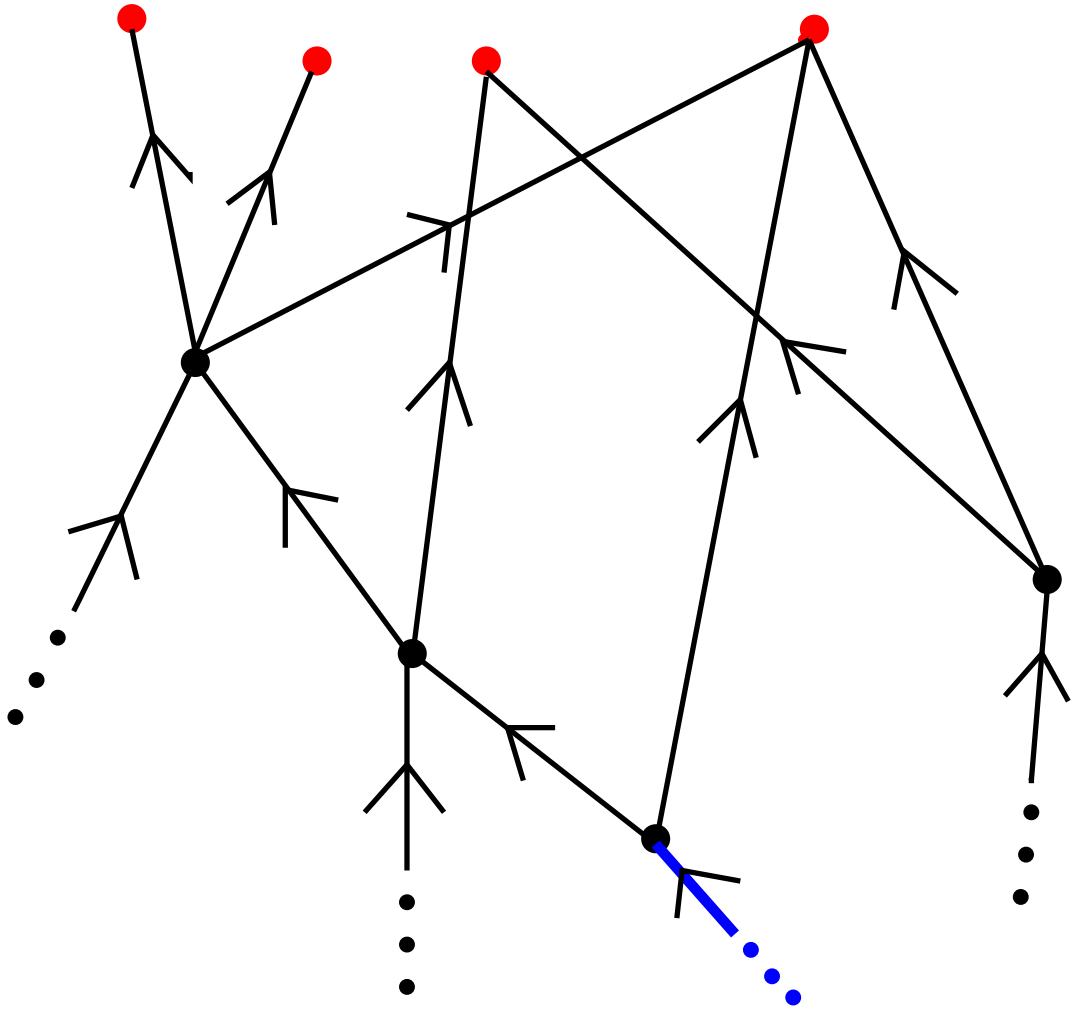
# A Well-founded Relation





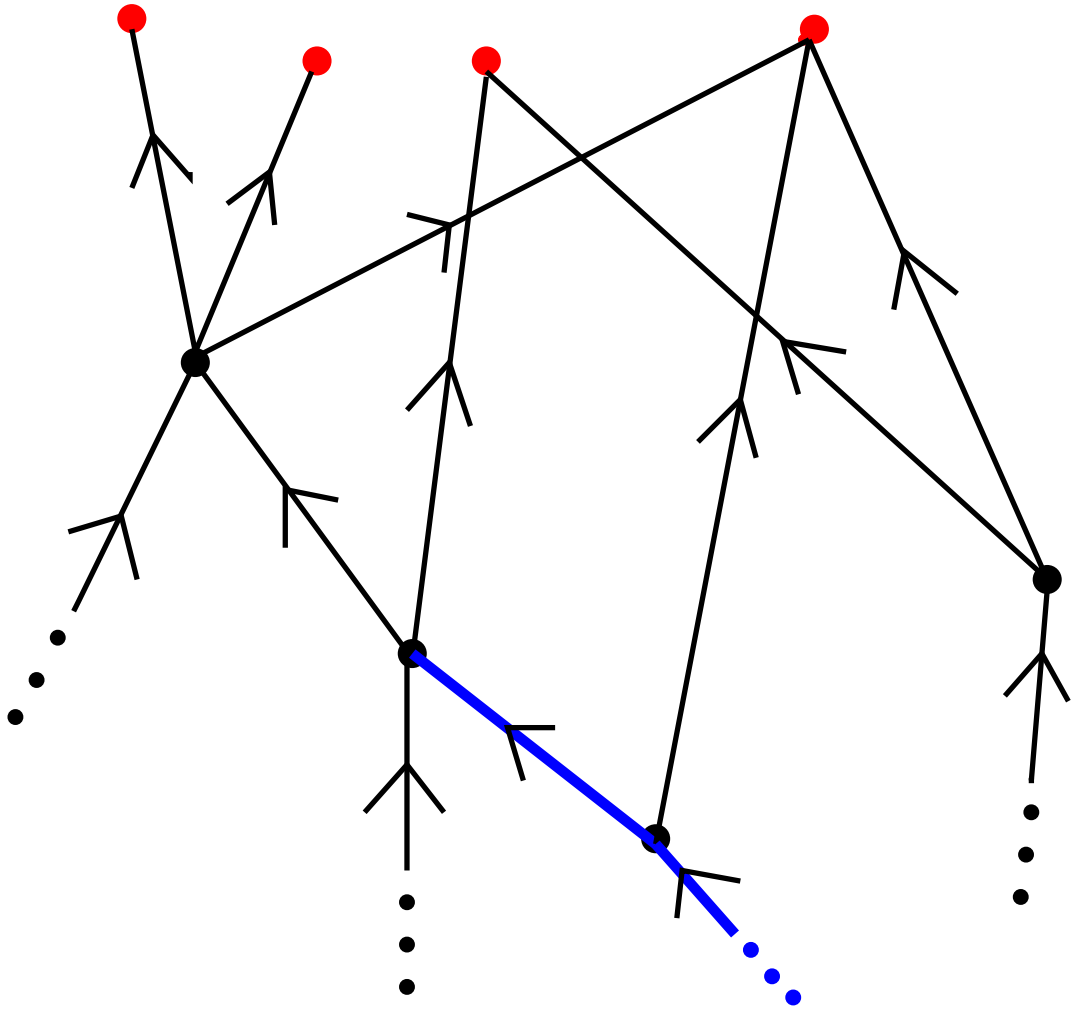
# A Well-founded Relation





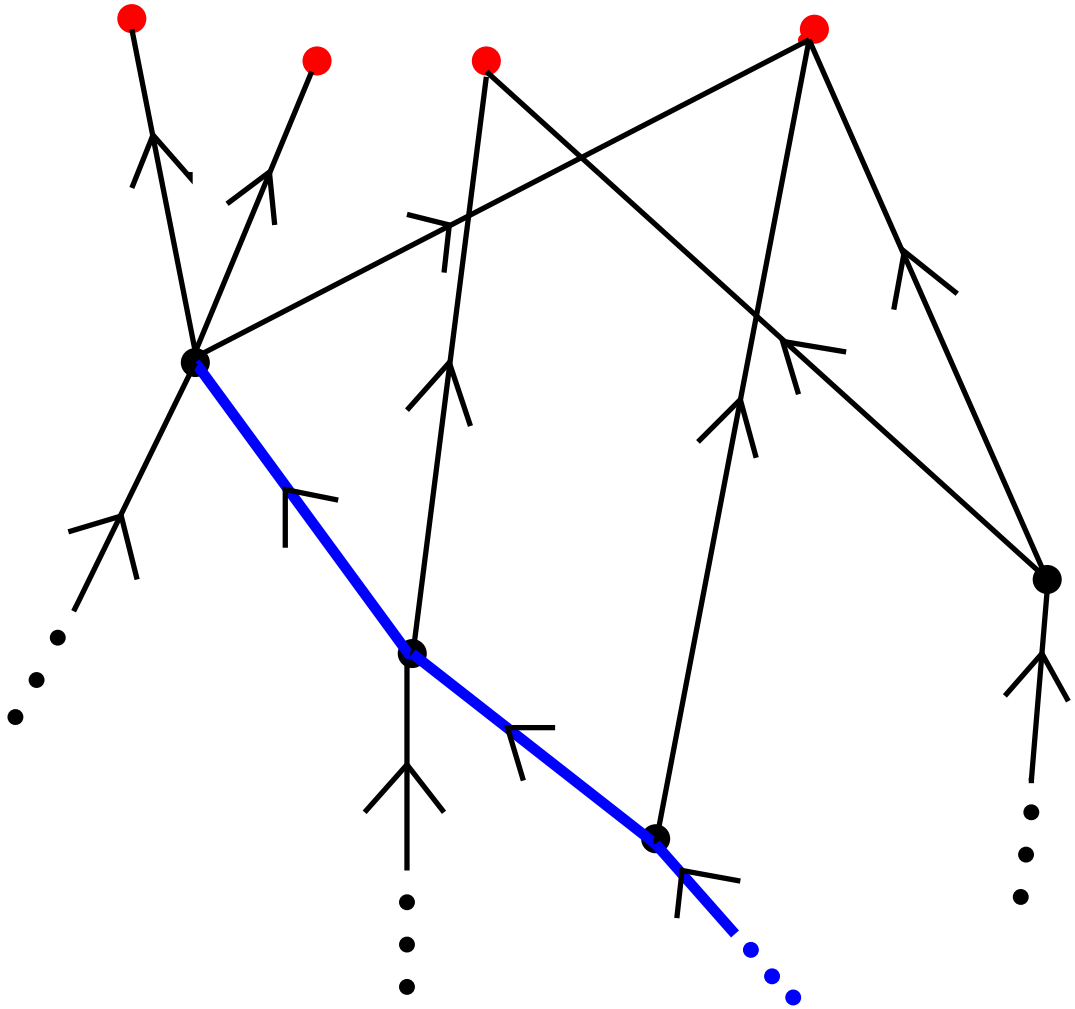
# A Well-founded Relation





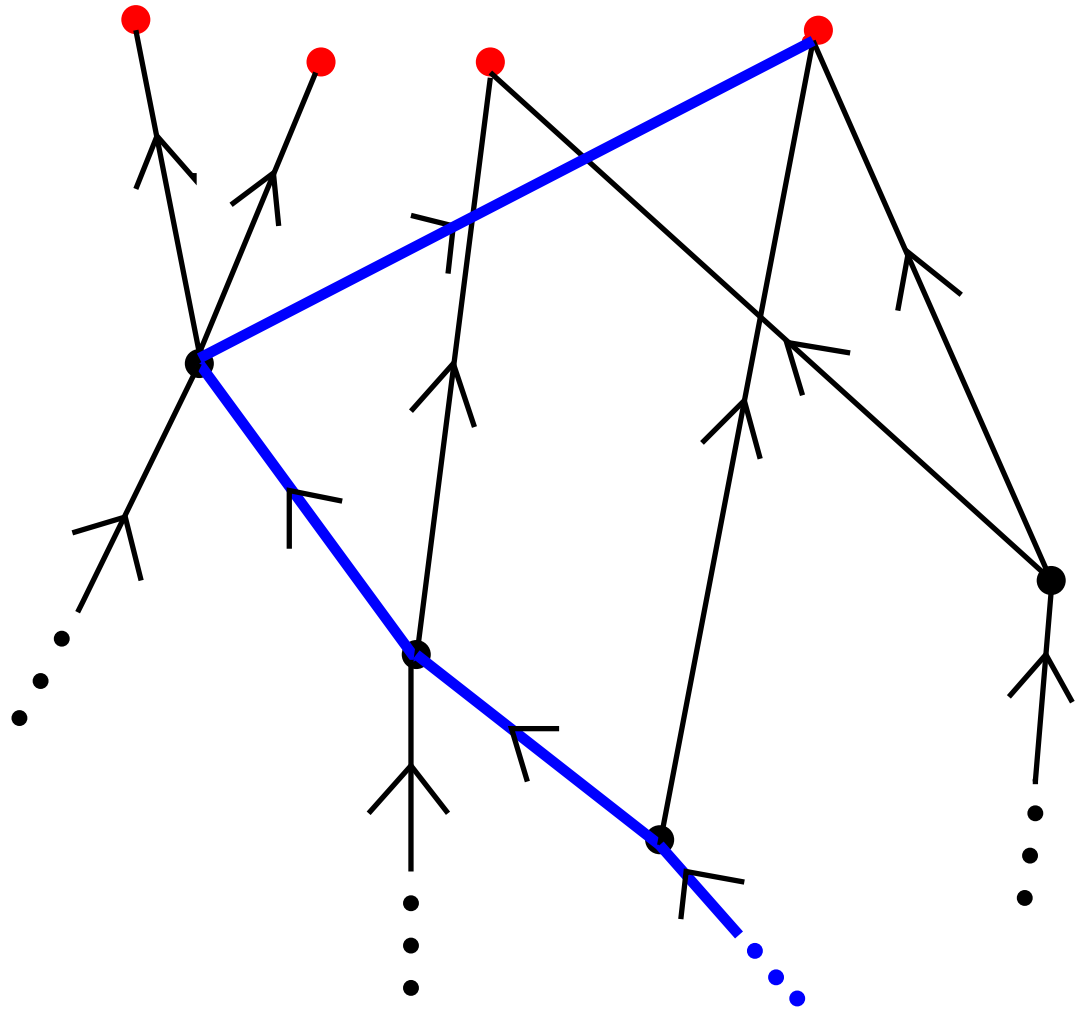
# A Well-founded Relation





# A Well-founded Relation



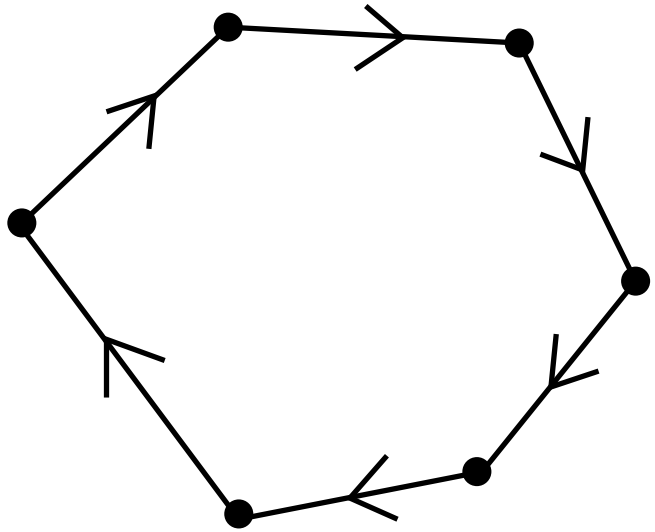


- From any point in the graph

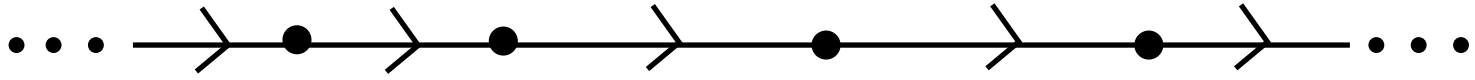
- You always reach a red point after a FINITE travel

# Relations which are not Well-founded: no Red Points

- A cycle

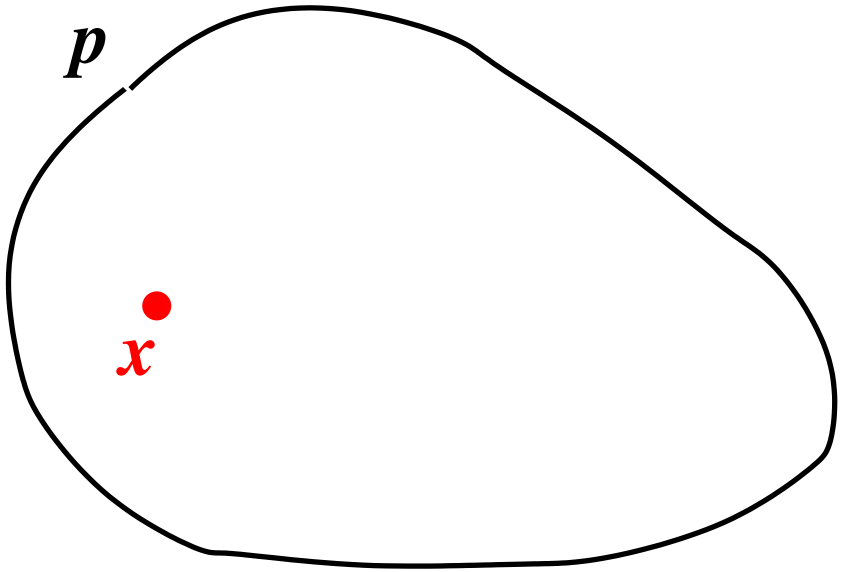


- An infinite chain



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



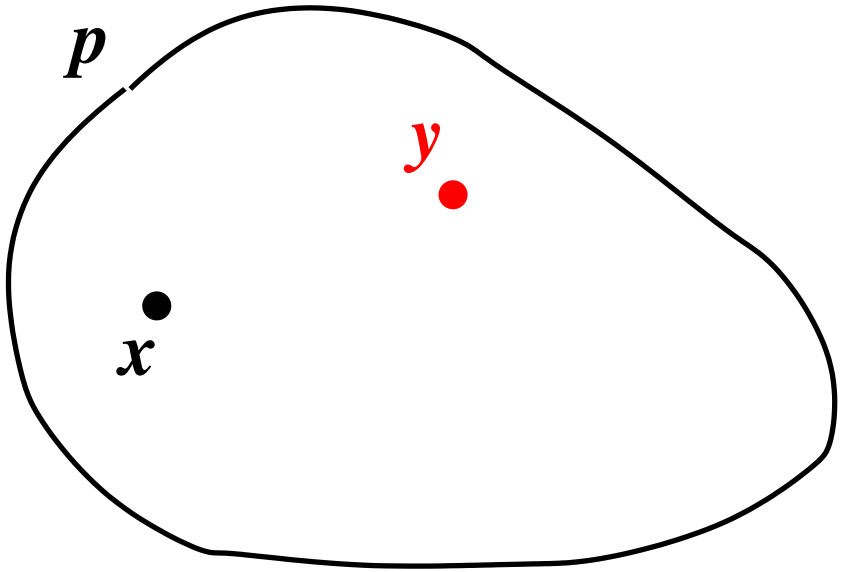



For all $x$ in $p$

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

# Set $p$ Containing a Cycle or an Infinite Chain



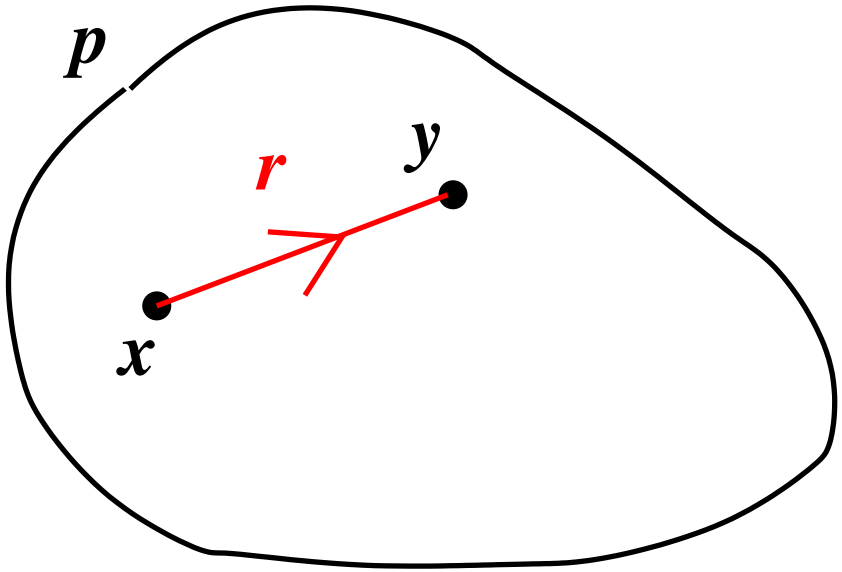



For all $x$ in $p$ there exists a $y$ in $p$

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

# Set $p$ Containing a Cycle or an Infinite Chain

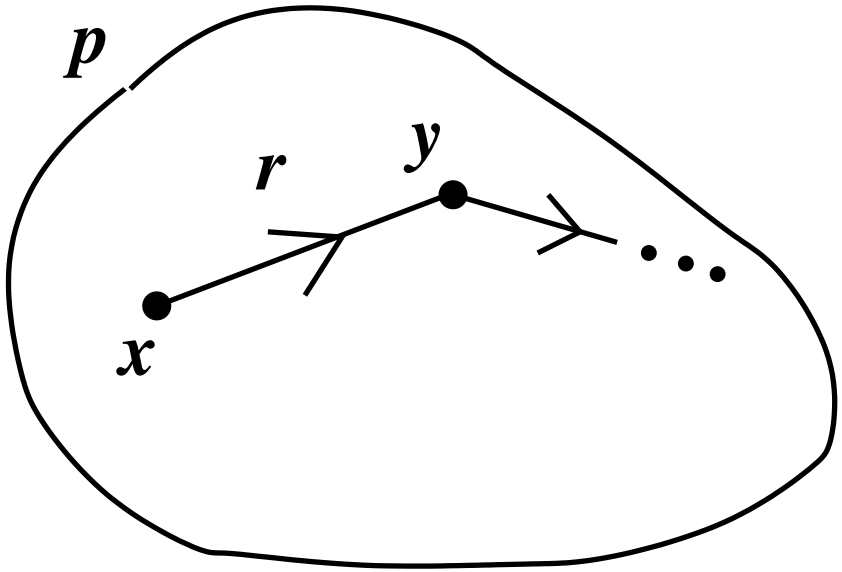





For all $x$ in $p$ there exists a $y$ in $p$ related to $x$ by relation $r$

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

# 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 $r$

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

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

# Definition of a Well-founded Relation

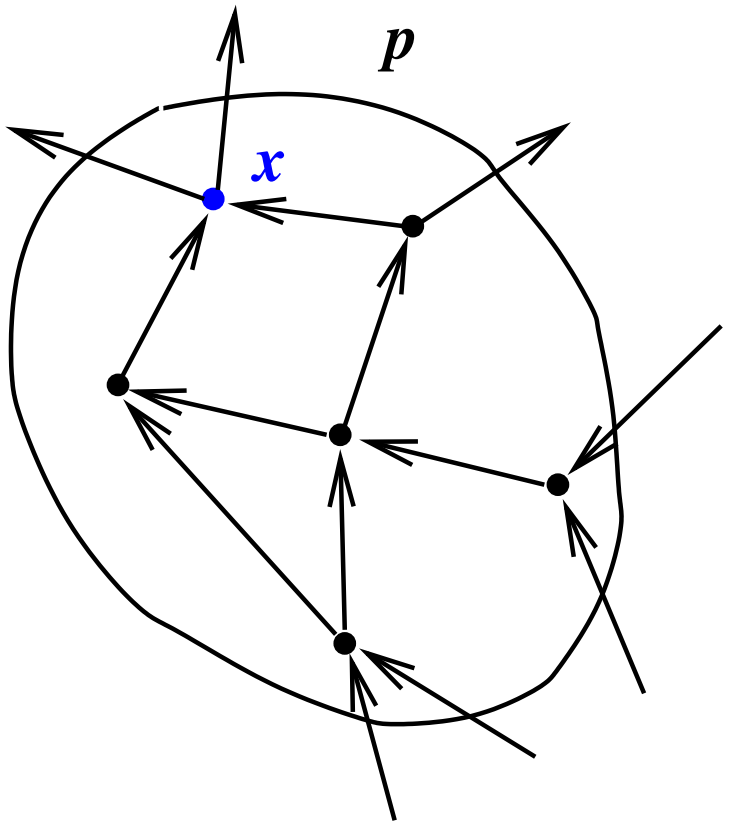
- A well-founded relation does not contain such a set $p$ . . .

- . . . unless it is the empty set

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

# Another Definition

- Every non-empty subset $p$ has at least one $r$-maximal element $x$




- That is, $x$ is NOT related to another point in $p$

# Another Definition

- For every non-empty subset $p$ then
  -
  -

$$\forall p \cdot \quad p \neq \varnothing \Rightarrow$$

# Another Definition

- For every non-empty subset $p$ then
  - there exists a point $x$ of $p$ such that
  -

$$\forall p \cdot \quad p \neq \varnothing \Rightarrow \exists x \cdot x \in p \ \wedge$$

# Another Definition

- For every non-empty subset $p$ then
  - there exists a point $x$ of $p$ such that
  - forall $z$ in $p$,

$$\forall p \cdot \quad p \neq \varnothing \Rightarrow \exists x \cdot x \in p \ \wedge \ (\forall z \cdot z \in p \ \Rightarrow$$

# Another Definition

- For every non-empty subset $p$ then
  - there exists a point $x$ of $p$ such that
  - forall $z$ in $p$, $x$ is NOT related to $z$

$$\forall p \cdot \quad p \neq \varnothing \Rightarrow \exists x \cdot x \in p \ \wedge \ (\forall z \cdot z \in p \ \Rightarrow \ x \mapsto z \notin r)$$

# Another Definition

- For every non-empty subset $p$ then
  - there exists a point $x$ of $p$ such that
  - forall $z$ in $p$, $x$ is NOT related to $z$

$$wf(r) \;\Leftrightarrow\; \forall p \cdot p \neq \varnothing \;\Rightarrow\; \exists x \cdot x \in p \;\wedge\; (\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r)$$

- Can we explain this?

# Manual Proof

$$p \neq \varnothing \;\Rightarrow\; \exists x \cdot x \in p \;\wedge\; (\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r)$$

$\Leftrightarrow$ contraposition

$$\neg\,(\exists x \cdot x \in p \;\wedge\; (\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r)) \;\Rightarrow\; p = \varnothing$$

$\Leftrightarrow$ de Morgan

$$(\forall x \cdot x \in p \;\Rightarrow\; \neg\,(\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r)) \;\Rightarrow\; p = \varnothing$$

$\Leftrightarrow$ de Morgan

$$(\forall x \cdot x \in p \;\Rightarrow\; (\exists z \cdot z \in p \;\wedge\; x \mapsto z \in r)) \;\Rightarrow\; p = \varnothing$$

$\Leftrightarrow$ set theory

$$p \subseteq r^{-1}[p] \;\Rightarrow\; p = \varnothing$$

# Induction Principle: for Proving Properties of w.f. Sets

# Induction Principle: for Proving Properties of w.f. Sets

If for any $x$

then

$\forall x \cdot$
$\Rightarrow$

# Induction Principle: for Proving Properties of w.f. Sets

If for any $x$

if under the assumption that $Q(y)$ holds for all $y$ s.t. $x \mapsto y \in r$ then

then

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow Q(y)) \Rightarrow$$
$$\Rightarrow$$

# Induction Principle: for Proving Properties of w.f. Sets

If for any $x$

if under the assumption that $Q(y)$ holds for all $y$ s.t. $x \mapsto y \in r$ then

you can prove a property $Q(x)$

then

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow Q(y)) \Rightarrow Q(x)$$

$\Rightarrow$

# Induction Principle: for Proving Properties of w.f. Sets

If for any $x$

if under the assumption that $Q(y)$ holds for all $y$ s.t. $x \mapsto y \in r$ then

you can prove a property $Q(x)$

then

$Q(z)$ holds for all $z$ in S

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \;\Rightarrow\; Q(y)) \;\Rightarrow\; Q(x)$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \;\Rightarrow\; Q(z)$$

# Induction Principle: for Proving Properties of w.f. Sets

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \;\Rightarrow\; Q(y)) \;\Rightarrow\; Q(x)$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \;\Rightarrow\; Q(z)$$

# Induction Principle: for Proving Properties of w.f. Sets

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \;\Rightarrow\; Q(y)) \;\Rightarrow\; Q(x)$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \;\Rightarrow\; Q(z)$$

- We replace the predicate $Q(\_)$ by the set $q$

# Induction Principle: for Proving Properties of w.f. Sets



$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow Q(y)) \Rightarrow Q(x)$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \Rightarrow Q(z)$$

- We replace the predicate $Q(\_)$ by the set $q$

$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow y \in q) \Rightarrow x \in q$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \Rightarrow z \in q$$

# Induction Principle: for Proving Properties of w.f. Sets



$$\forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow Q(y)) \Rightarrow Q(x)$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \Rightarrow Q(z)$$

- And now we quantify over $q$ (previous is 2nd order over $Q$)

$$\forall q \cdot \quad \forall x \cdot (\forall y \cdot x \mapsto y \in r \Rightarrow y \in q) \Rightarrow x \in q$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \Rightarrow z \in q$$

# Induction Principle: for Proving Properties of w.f. Sets

$$\forall q \cdot \quad \forall x \cdot (\forall y \cdot x \mapsto y \in r \;\Rightarrow\; y \in q) \;\Rightarrow\; x \in q$$
$$\Rightarrow$$
$$\forall z \cdot z \in S \;\Rightarrow\; z \in q$$

- The final touch:

$$\forall r \cdot wf(r) \;\Rightarrow\; (\forall q \cdot (\forall x \cdot r[\{x\}] \subseteq q \;\Rightarrow\; x \in q) \;\Rightarrow\; S \subseteq q)$$

- If $p$ is included in a well-founded relation $q$, then so is $p$

$$\forall p, q \cdot q \in S \leftrightarrow S \ \wedge \ wf(q) \ \wedge \ p \subseteq q \ \Rightarrow \ wf(p)$$

- Intuition: If $q$ has no cycle or infinite chain, then so is $p$

- We connect $S$ and $T$ by means of a relation $v$

$$v \in S \leftrightarrow T$$

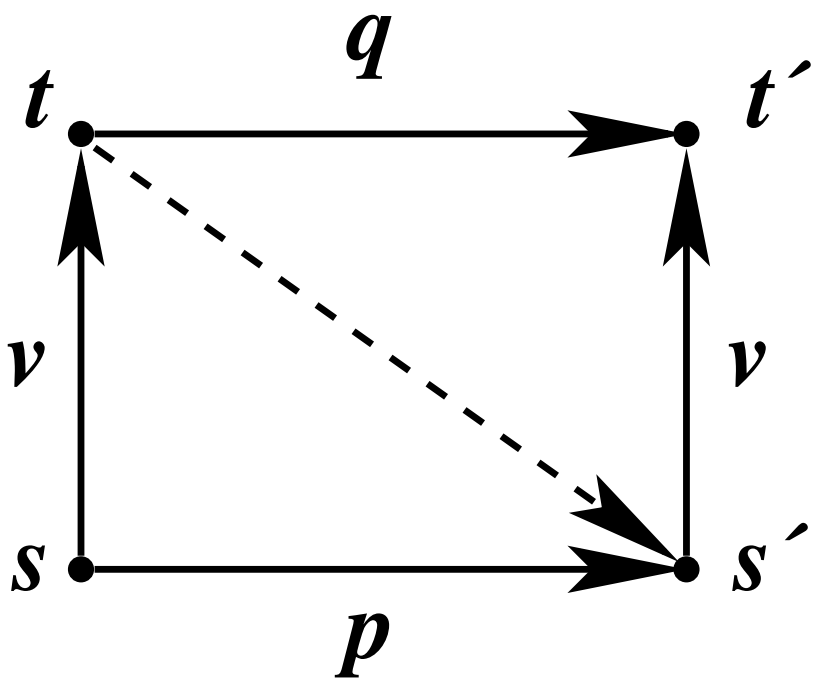
Some conditions ?

- Here is what we have to prove

$wf(q)$
Some conditions
$\Rightarrow$
$wf(p)$

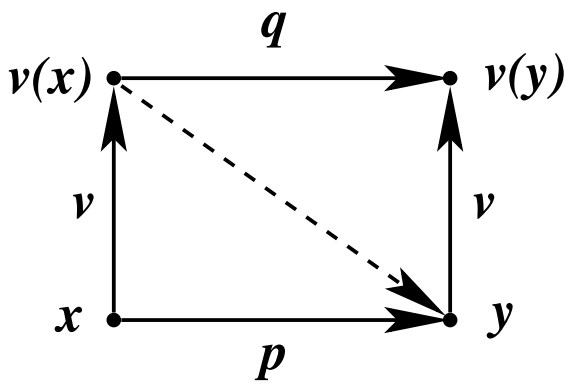
- Here is what one has to prove:

$$
\begin{array}{l}
p \in S \leftrightarrow S \\
q \in T \leftrightarrow T \\
wf(q) \\
v \in S \leftrightarrow T \\
\mathrm{dom}(v) = S \\
v^{-1} ; p \subseteq q ; v^{-1} \\
\Rightarrow \\
wf(p)
\end{array}
$$



# A Useful Lemma

- The relations $v$ is a total function: $v \in S \rightarrow T$




- Here is what we have to prove:

$$
\begin{array}{l}
p \in S \leftrightarrow S \\
q \in T \leftrightarrow T \\
v \in S \rightarrow T \\
\forall x, y \cdot x \mapsto y \in p \;\Rightarrow\; v(x) \mapsto v(y) \in q \\
\Rightarrow \\
v^{-1} ; p \;\subseteq\; q ; v^{-1}
\end{array}
$$

# A Given Well-founded Relation

- Here is what we would like to prove:

$$wf(\{x \mapsto y \mid x \in \mathbb{N} \ \wedge \ y \in \mathbb{N} \ \wedge \ y < x\})$$

# Putting the Previous Results Together

$$
\begin{array}{l}
r \in S \leftrightarrow S \\
v \in S \rightarrow \mathbb{N} \\
\forall x, y \cdot x \mapsto y \in r \;\Rightarrow\; v(y) < v(x) \\
\Rightarrow \\
wf(r)
\end{array}
$$

- This introduces the concept of variant

- DEMO

# 2. Fixpoint

# Motivation for Fixpoint

- This mathematical concept is used to formalize recursion

# Definition

- 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

$$\mathsf{fix}(f) \;\widehat{=}\; \mathbf{inter}(\{s \mid f(s) \subseteq s\})$$

# Two Useful Lemmas

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

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

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

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

# The Main Results (Knaster-Tarski)

- Additional needed constraint: $f$ is monotone

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

- $\text{fix}(f)$ is the least fixpoint

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

# Complement and Conjugate

- Given a set $k$ of type $\mathbb{P}(S)$, the complement, $\overline{k}$, of $k$ is as follows:

$$\overline{k} \;\widehat{=}\; S \setminus k$$

- Given a function $f$:

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

- Then, the conjugate, $\widetilde{f}$ , of $f$ is defined as follows:

$$\widetilde{f} \;\widehat{=}\; \lambda k \cdot k \subseteq s \mid \overline{h(\overline{k})}$$

- Properties:

$$\overline{\overline{k}} = k$$

$$\widetilde{\widetilde{f}} = f$$

# Greatest Fixpoint

- Given a function $f$:

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

- The set FIX($f$) is defined as follows:

$$\mathsf{FIX}(f) \;\widehat{=}\; \overline{\mathsf{fix}(\widetilde{f})}$$

- Therefore, we have

$$\mathsf{fix}(f) = \overline{\mathsf{FIX}(\widetilde{f})}$$

- The following can be proved:

$$\mathsf{FIX}(f) = \mathbf{union}(\{s \mid s \subseteq f(s)\})$$

$$\begin{array}{l} \forall a, b \cdot a \subseteq b \Rightarrow f(a) \subseteq f(b) \\ \Rightarrow \\ \mathsf{FIX}(f) = f(\mathsf{FIX}(f)) \end{array}$$

$$\forall t \cdot t = f(t) \Rightarrow t \subseteq \mathsf{FIX}(f)$$

- DEMO

- A very important theorem by Tarski (1955) and Montague (1955)

- Let $r$ be a well-founded relation on $S$: $r \in S \leftrightarrow S$

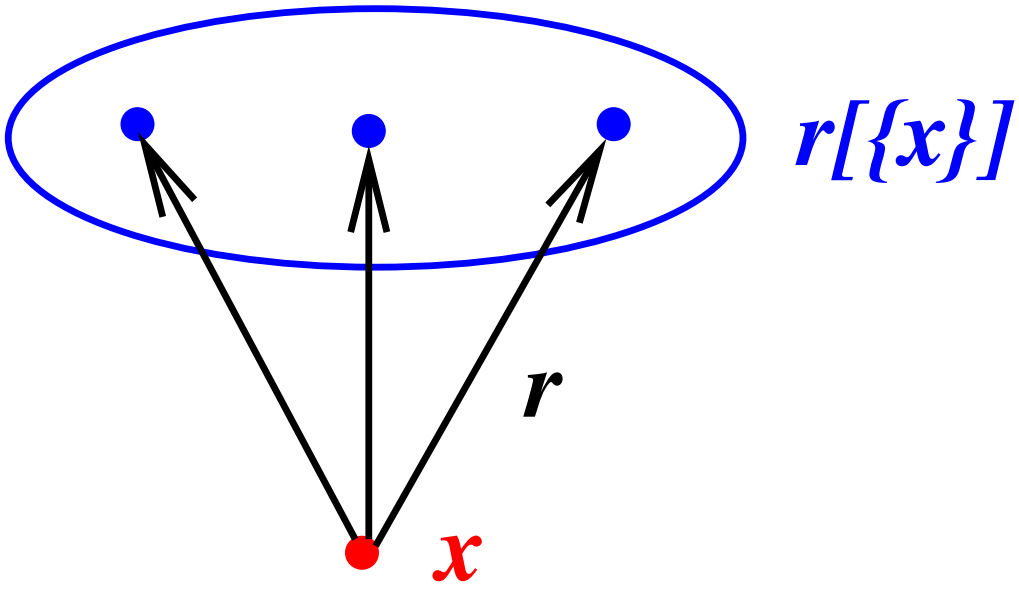
  Let $g$ be a a function such that: $g \in (S \nrightarrow T) \rightarrow T$

  There is a unique total function $f$: $f \in S \rightarrow T$

  such that we have:

$$\forall x \cdot x \in S \Rightarrow f(x) = g(r[\{x\}] \lhd f)$$

$$\forall x \cdot x \in S \Rightarrow f(x) = g(r[\{x\}] \lhd f)$$




- The value of the function $f$ at $x$ depends on its values on $r[\{x\}]$

- More on this is skipped

# 3. Transitive Closure

# Motivation for Transitive Closure

- Transition system achievement

# Naive Approach at the Irreflexive Transitive Closure $r^+$

- We are given a relation $r$ built on a set $S$:

$$r \in S \leftrightarrow S$$

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

$$r^+ \quad \widehat{=} \quad r \cup r^2 \cup \ldots \cup r^n \cup \ldots$$

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

- Let us compose $r^+$ with $r$

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

Hence we have . . . a fixpoint equation

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

- $r^+$ and $r^*$ are thus fixpoints of some functions

$$r^+ \;\widehat{=}\; fix(\lambda s \cdot s \in S \leftrightarrow S \mid r \cup (s ; r))$$

$$r^* \;\widehat{=}\; fix(\lambda s \cdot s \in S \leftrightarrow S \mid \mathrm{id} \cup (s ; r))$$

- Notice that these functions are monotone

# Main Results (similar results for $r^*$, except for wf)



$$r \subseteq r^+$$

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

$$\forall s \cdot \; r \subseteq s \;\; s ; r \subseteq s \;\Rightarrow\; r^+ \subseteq s$$

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

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

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

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

$$\mathsf{wf}(r) \Rightarrow \mathsf{wf}(r^+)$$

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

- DEMO

# 4. Computation

# The Forward Approach

- The forward relation

$$r \subseteq A \times A$$

- The pre-condition set

$$p \subseteq A$$

- The constraint

$$\overline{p} \times A \subseteq r$$

- The backward set transformer:

$$\boldsymbol{F} \in \mathbb{P}(\boldsymbol{A}) \rightarrow \mathbb{P}(\boldsymbol{A})$$

- The constraint: conjunctivity property

$$\boldsymbol{F}(\boldsymbol{q1} \cap \boldsymbol{q2}) \;=\; \boldsymbol{F}(\boldsymbol{q1}) \cap \boldsymbol{F}(\boldsymbol{q2})$$

- Monotonicity: this is a consequence of conjunctivity

$$\boldsymbol{q1} \subseteq \boldsymbol{q2} \;\Rightarrow\; \boldsymbol{F}(\boldsymbol{q1}) \subseteq \boldsymbol{F}(\boldsymbol{q2})$$

# From Forward Approach $(r, p)$ to Backward Approach $(F)$

- We want to derive $\boldsymbol{F}$ from $\boldsymbol{r}$ and $\boldsymbol{p}$.

$$\boldsymbol{F(q) \;=\; p \;\cap\; \overline{r^{-1}[\overline{q}]}}$$

- The constraint $\boldsymbol{F(q1 \cap q2) = F(q1) \cap F(q2)}$ is easy to prove

# From Backward Approach ($F$) to Forward Approach ($r, p$)

- We want to derive $r$ and $p$ from $F$.

$$p = F(A)$$

$$r = \{x \mapsto x' \mid x \notin F(\overline{\{x'\}})\}$$

- The constraint $\overline{p} \times A \subseteq r$ is easy to prove

# Computation Combinators. Some Examples

| | |
|---|---|
| sequencing | $S1; S2$ |
| choice | $S1 \sqcap S2$ |
| parallelism | $S1 \mid\mid S2$ |
| guarding | $G \Longrightarrow S$ |
| pre-conditioning | $P \mid S$ |
| ... | ... |

# Computation Combinators. Some Examples (cont'd)

- Forward and backward interpretation can be given for each of them.

- Corresponding constraints can be proved for each of them.

# Iteration: the While Loop

- Iteration usually studied under the form of a while loop:

$$\textbf{while}\ \ G\ \ \textbf{do}\ \ S\ \ \textbf{end}$$

- The unfolding of the while loop yields:

$$\textbf{while}\ \ G\ \ \textbf{do}\ \ S\ \ \textbf{end} \quad = \quad \begin{array}{l} \textbf{if}\ \ G\ \ \textbf{then} \\ \quad S; \textbf{while}\ \ G\ \ \textbf{do}\ \ S\ \ \textbf{end} \\ \textbf{else} \\ \quad \textbf{skip} \\ \textbf{end} \end{array}$$

- We do not formalize iteration with the while loop: too complicated!

# The Abstract Iteration Combinator

- We use the following abstract iteration combinator, $S^{\triangledown}$.

- here is the unfolding of the abstract iteration:

$$S^{\triangledown} = \textbf{skip} \sqcap (S ; S^{\triangledown})$$

- The while loop can then be defined with various combinators:

$$\textbf{while}\ G\ \textbf{do}\ S\ \textbf{end} \ \widehat{=}\ (G \Longrightarrow S)^{\triangledown} ; (\neg G \Longrightarrow \textbf{skip})$$

# Backward Approach to Abstract Iteration

- Given a set transformer $G$, let $p \mid G$ be the set transformer where:

$$(p \mid G)(k) \;\widehat{=}\; p \cap G(k)$$

- Translating abstract iteration to the backward set transformer yields:

$$F^{\triangledown}(q) \;=\; q \cap F(F^{\triangledown}(q))$$

- Then we have a fixpoint:

$$F^{\triangledown}(q) \;=\; (q \mid F)(F^{\triangledown}(q))$$

# Backward Approach to Abstract Iteration (cont'd)

- We defined $F^{\triangledown}(q)$ as the least fixpoint of the set function $q \mid F$:

$$F^{\triangledown}(q) \quad \widehat{=} \quad \mathbf{fix}(q \mid F)$$

- We also define the greatest fixpoint:

$$F^{\triangle}(q) \quad \widehat{=} \quad \mathbf{FIX}(q \mid F)$$

- Here is the provable relationship between these two combinators:

$$F^{\triangledown} \quad = \quad \mathbf{fix}(F) \mid F^{\triangle}$$

- We can prove the conjunctivity of these combinators

# Forward Approach to Iteration: the Pre-condition Set

- We have $p^{\triangledown} = F^{\triangledown}(A) = \mathbf{fix}(A \mid F)$, thus:

$$\boxed{p^{\triangledown} = \mathbf{fix}(F)}$$

- By taking the complement, we obtain

$$\boxed{\overline{p^{\triangledown}} \;=\; \overline{p} \;\cup\; r^{-1}[\overline{p^{\triangledown}}]}$$

- An interesting informal explanation of $\overline{p^{\triangledown}}$

- We can also prove that the relation $p^{\triangledown} \lhd r$ is well-founded

# Forward Approach to Iteration: the Relation

- We also derive it from the backward approach:

$$r^{\triangledown} = (\overline{\mathbf{fix}(F)} \times A) \cup r^*$$

- $r^{\triangledown}$ obeys the same fixpoint equation as $r^*$

- $r^{\triangledown}$ is the greatest fixpoint of the same function as for $r^*$

- DEMO

# 5. Real Numbers

# Axioms: Addition

1. Addition is associative: $x + (y + z) = (x + y) + z$

2. Addition is commutative: $x + y = y + x$

3. Addition has an identity: $x + 0 = x$

4. Addition has an inverse: $x + (-x) = 0$

# Axioms: Multiplication

5. Multiplication is associative: $x * (y * z) = (x * y) * z$

6. Multiplication is commutative: $x * y = y * x$

7. Multiplication has an identity: $x * 1 = x$

8. Additive and multiplicative identities are different: $0 \neq 1$

9. Distributivity of multiplication: $x * (y + z) = (x * y) + (x * z)$

10. Multiplication has an inverse: $x \neq 0 \;\Rightarrow\; x * \frac{1}{x} = 1$

# Axioms: Order

11. Reflexivity: $x \leq x$

12. Antisymmetry: $x \leq y \ \wedge \ y \leq x \ \Rightarrow \ x = y$

13. Transitivity: $x \leq y \ \wedge \ y \leq z \ \Rightarrow \ x \leq z$

14. Totality: $x \leq y \ \vee \ y \leq x$

15. Addition and order: $x \leq y \ \Rightarrow \ x + z \leq y + z$

16. Multiplication and order: $x \leq y \ \wedge \ 0 < z \ \Rightarrow \ x * z \leq y * z$

# Axioms: Completeness

17. Completeness: Every non empty subset of reals with an upper bound has a least upper bound:

$$
\begin{array}{l}
\forall A \cdot A \subseteq \mathbb{R} \\
\quad A \neq \varnothing \\
\quad \exists UB \cdot UB \in \mathbb{R} \ \wedge \ (\forall x \cdot x \in A \ \Rightarrow \ x \leq UB) \\
\Rightarrow \\
\quad \sup(A) \in \mathbb{R} \\
\quad \forall x \cdot x \in A \ \Rightarrow \ x \leq \sup(A) \\
\quad \forall v \cdot v \in \mathbb{R} \ \wedge \ (\forall x \cdot x \in A \ \Rightarrow \ x \leq v) \ \Rightarrow \ \sup(A) \leq v
\end{array}
$$

- $\mathbb{R}$ is a totally ordered complete field

$$0 * 0 = 0$$

Proof

$$0 * 0 = (0 * 0) + 0 = (0 * 0) + (0 * 1) = 0 * (0 + 1) = 0 * 1 = 0$$

$$0 * (-1) = 0$$

Proof

$$0 * (-1) = 0 * (-1) + 0 = 0 * (-1) + 0 * 1 = 0 * ((-1) + 1) = 0 * (1 + (-1)) = 0 * 0 = 0$$

$$0 < 1$$

Proof

$$1 < 0 \Leftrightarrow 0 < (-1) \Rightarrow 1 * (-1) < 0 * (-1) \Leftrightarrow -1 < 0 \Leftrightarrow 0 < 1 \Leftrightarrow \bot$$

$$1 = 0 \Leftrightarrow \bot$$

$$0 < 1$$

$$0 * x = 0$$

Proof

$0 * x > 0 \Rightarrow 0 * (0 * x) < 1 * (0 * x) \Leftrightarrow$
$(0 * 0) * x < 0 * x \Leftrightarrow 0 * x < 0 * x \Leftrightarrow \perp$

$0 * x < 0 \Rightarrow 0 < 0 * (-x) \Rightarrow 0 * (0 * (-x)) < 1 * (0 * (-x))$
$(0 * 0) * (-x) < 0 * (-x) \Leftrightarrow 0 * (-x) < 0 * (-x) \Leftrightarrow \perp$

$0 * x = 0$

# Natural Numbers as a Subset of the Reals

$$\mathbb{N} = \mathsf{fix}(\boldsymbol{\lambda s} \cdot \boldsymbol{s} \subseteq \mathbb{R} \mid \{\mathbf{0}\} \cup (\boldsymbol{\lambda x} \cdot \boldsymbol{x} \in \mathbb{R} \mid \boldsymbol{x} + \mathbf{1})[\boldsymbol{s}])$$

$$\mathbb{N} \subseteq \mathbb{R}$$

- Archimedean Property:

$$\forall \boldsymbol{x} \cdot \boldsymbol{x} \in \mathbb{R} \;\Rightarrow\; \exists \boldsymbol{n} \cdot \boldsymbol{n} \in \mathbb{N} \;\wedge\; \boldsymbol{n} > \boldsymbol{x}$$

The proof is by contradiction. Suppose $\mathbb{N}$ is bounded above. Since $\mathbb{N}$ is a non empty subset of $\mathbb{R}$, then by the completeness axiom it must follows that $\exists \boldsymbol{\alpha} \in \mathbb{R} : \boldsymbol{\alpha} = \sup\mathbb{N}$. Since $\boldsymbol{\alpha}$ is the least upper bound, $\boldsymbol{\alpha} - \mathbf{1}$ is not an upper bound and thus there exists $\boldsymbol{n0} \in \mathbb{N} : \boldsymbol{\alpha} - \mathbf{1} < \boldsymbol{n0}$. But then $\boldsymbol{n0} + \mathbf{1} \in \mathbb{N}$ and $\boldsymbol{\alpha} < \boldsymbol{n0} + \mathbf{1}$, contradicting that $\boldsymbol{\alpha}$ was an upper bound for $\mathbb{N}$.

# "$\epsilon$,$\delta$" Continuity at Point $c$ for Real Function $f$

$$
\begin{array}{l}
\forall\, f, c \cdot \; f \in \mathbb{R} \to \mathbb{R} \\
\qquad\quad c \in \mathbb{R} \\
\qquad\quad \text{continuous}(f, c) \\
\qquad \Rightarrow \\
\qquad\quad \forall \epsilon \cdot \; \epsilon > 0 \\
\qquad\qquad \Rightarrow \\
\qquad\qquad\quad \exists\, \delta \cdot \delta > 0 \;\wedge\; (\forall\, x \cdot x \in \,]c - \delta, c + \delta[ \;\Rightarrow\; f(x) \in \,]f(c) - \epsilon, f(c) + \epsilon[)
\end{array}
$$

# Intermediate Value Theorem

If $f$ is a continuous function then, given a real number $u$ in the open interval $]f(a), f(b)[$, there exists a real number $c$ in the open interval $]a, b[$ such that $f(c) = u$.

$$
\begin{array}{l}
\forall\, a, b, f, u \cdot f \in \mathbb{R} \to \mathbb{R} \\
\qquad \forall\, x \cdot x \in \mathbb{R} \;\Rightarrow\; \text{continuous}(f, x) \\
\qquad a \in \mathbb{R} \\
\qquad b \in \mathbb{R} \\
\qquad a < b \\
\qquad u \in\, ]f(a), f(b)[ \\
\qquad \Rightarrow \\
\qquad \exists\, c \cdot c \in\, ]a, b[ \;\wedge\; f(c) = u
\end{array}
$$

- Showing a proof from internet
- DEMO

# 6. Some Theorems:

## Zermelo Theorem, Cantor-Bernstein Theorem

# The Well-ordering Theorem (Zermelo 1904)



**Every set can be well-ordered**

# Refresher on Orders

- Partial order

- Well-order

- Transporting well-orders

# Partial Order $q$ on a set $S$

- Relation: $q \in S \leftrightarrow S$

- Reflexive: $\mathrm{id} \subseteq q$

- Transitive: $q ; q \subseteq q$

- Anti-symmetric: $q \cap q^{-1} \subseteq \mathrm{id}$

- Example: the set inclusion relation is a partial order

  Reflexivity: $A \subseteq A$

  Transitivity: $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

  Anti-symmetry: $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$

## Well-order $q$ on a set $S$

- Partial order: $q$ is a partial order on $S$

- Each non-empty subset $A$ of $S$ has a smallest element $x$:

$$\forall A \cdot A \subseteq S \ \wedge \ A \neq \varnothing \ \Rightarrow \ (\exists x \cdot x \in A \ \wedge \ A \subseteq q[\{x\}])$$

# Transporting a Well-order $q$ by Means of an Injection $f$

- We are given two sets $S$ and $T$

- We suppose that a relation $q$ is a well-order on $T$

- We are given a total injection $f$ from $S$ to $T$: $f \in S \rightarrowtail T$

- **Theorem 1**: $f ; q ; f^{-1}$ is a well-order on $S$

- Mind the polymorphism on $S$ and $T$.

# Strategy for Proving that a Set $S$ can be Well-ordered

- We apply **Theorem 1**

- For this:

  (1) We construct a well-order $q$ on a certain set $T$

  (2) We construct a total injection $f$ from $S$ to $T$

- This is done by:

  (1) Using some **Assumptions** and **Definitions**

  (2) Later proving the **Assumptions**

- More on this is skipped

# The Theorem of Cantor Bernstein Schröder

- Given two sets $S$ and $T$

- We have a total injective function $f$ from $S$ to $T$: $f \in S \rightarrowtail T$

- We have a total injective function $g$ from $T$ to $S$: $g \in T \rightarrowtail S$

- Hence, there exists a bijection $h$ fom $S$ to $T$: $h \in S \rightarrowtail\!\!\!\!\twoheadrightarrow T$

# Cantor-Bernstein-Schröder Theorem (history)

1887 Dedekind proves the theorem but does not publish it.

1895 Cantor states the theorem in his first paper on set theory

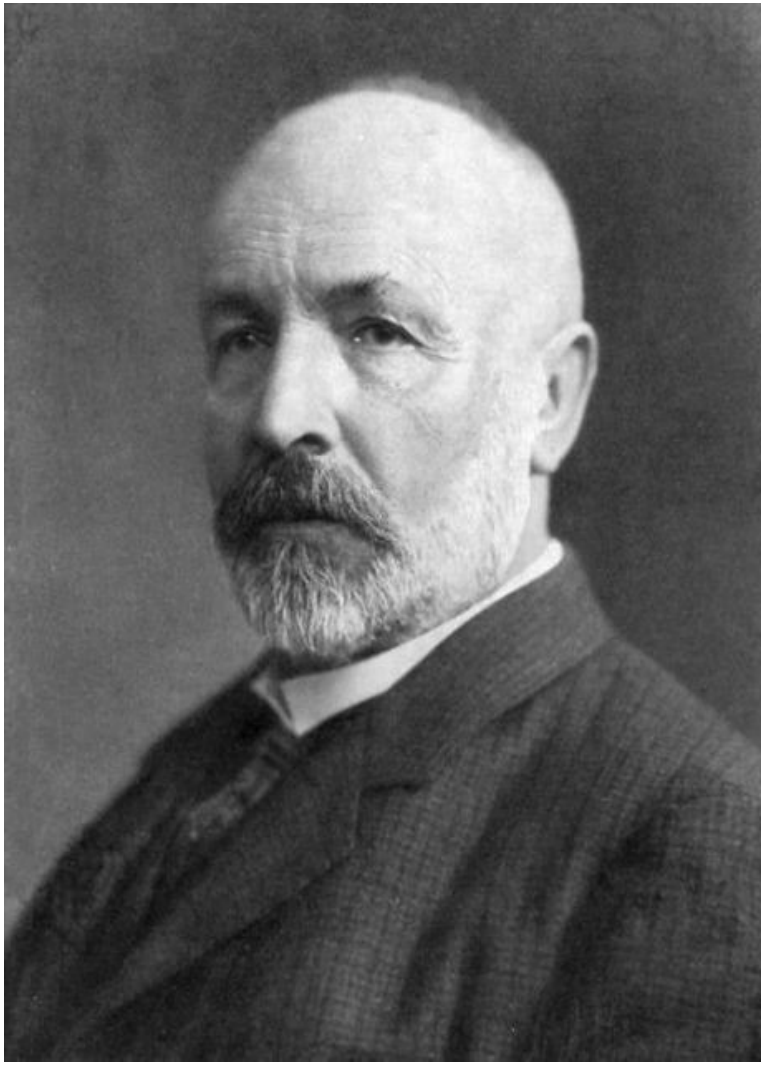
1896 Schröder announces a proof

1897 Bernstein, a student of Cantor, presents his proof.

1897 Dedekind independently proves it a second time.

# Dedekind and Cantor





# Schröder and Bernstein




## Proof Found on internet (1)

Assume without loss of generality that A and B are disjoint. For any a in A or b in B we can form a unique two-sided sequence of elements that are alternately in A and B, by repeatedly applying and to go right and and to go left (where defined).

For any particular a, this sequence may terminate to the left or not, at a point where or is not defined. Call such a sequence (and all its elements) an A-stopper, if it stops at an element of A, or a B-stopper if it stops at an element of B. Otherwise, call it doubly infinite if all the elements are distinct or cyclic if it repeats. See the picture for examples. By the fact that and are injective functions, each a in A and b

in B is in exactly one such sequence to within identity, (as if an element occurs in two sequences, all elements to the left and to the right must be the same in both, by definition). Therefore, the sequences form a partition of the (disjoint) union of A and B. Hence it suffices to produce a bijection between the elements of A and B in each of the sequences separately, as follows: For an A-stopper, the function is a bijection between its elements in A and its elements in B. For a B-stopper, the function is a bijection between its elements in B and its elements in A. For a doubly infinite sequence or a cyclic sequence, either or will do ( is used in the picture).

The proof below is from a 1994 paper by Peter G. Doyle and John Horton Conway.

We want to show that given injections f : A $\rightarrow$ B and g : B $\rightarrow$ A we can determine a one-to-one correspondence between A and B. We can and will assume that A and B are disjoint. Here's how it goes. We visualize the set A as a collection of blue dots, and the set B as a collection of red dots. We visualize the injection f as a collection of blue directed arcs connecting each element x $\in$ A to its image f(x) $\in$ B. Similarly, we visualize g as a collection of red directed arcs. If we put in both the blue and the red arcs, we get a directed graph where every vertex has one arc going out and at most one arc coming in.

Such a graph decomposes into a union of connected components, each of which is either a finite directed cycle, a doubly-infinite path, or a singly-infinite path. As you go along one of these paths or cycles, the vertices you encounter belong alternately to A and B. In the case of a cycle or a doubly-infinite path, the blue arcs define a one-to-one correspondence between the blue vertices of the component and the red vertices. In the case of a singly-infinite path, the blue edges will still determine a one-to-one correspondence between the blue and red vertices of the path if the path begins with a blue vertex, but not if the path begins with a red vertex. However in this latter case we can take the red edges instead. Thus we can pair up the vertices of A and B along each connected component, and the union of these correspondences determines a one-to-one correspondence between A and B.

# A Simple Proof

- Let $x \subseteq S$ and $y \subseteq T$ such that:

$$f[x] = \overline{y} \quad \text{that is} \quad y = \overline{f[x]}$$
$$g[y] = \overline{x} \quad \text{that is} \quad x = \overline{g[y]}$$

- We can prove the following (proved AUTOMATICALLY by Rodin):

$$(x \lhd f) \cup (y \lhd g)^{-1} \in S \rightarrowtail\!\!\!\!\!\rightarrow T$$

- By eliminating $y$, we obtain:

$$x = \overline{g[\overline{f[x]}]}$$

- We can then take $x$ as a fixpoint (notice the monotonicity)

$$x = \text{fix}(\lambda s \cdot s \subseteq S \mid \overline{g[\overline{f[s]}]})$$

- 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