Event-B Course

6. (cont'd) Mathematics with the Rodin Platform

Jean-Raymond Abrial

September-October-November 2011

- Some important mathematical concepts in Computer Science

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
    - Well-founded sets and relations

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
    - Well-founded sets and relations
    - Fixpoint

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
  - Well-founded sets and relations
  - Fixpoint
  - Transitive closure

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
    - Well-founded sets and relations
    - Fixpoint
    - Transitive closure
    - Graph

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
    - Well-founded sets and relations
    - Fixpoint
    - Transitive closure
    - Graph
    - Tree

Outline: Some Mathematical Studies

- Some important mathematical concepts in Computer Science
  - Well-founded sets and relations
  - Fixpoint
  - Transitive closure
  - Graph
  - Tree
- Conclusion

1. Well-founded sets and relations

Motivation for Well-founded Sets and Relations

Motivation for Well-founded Sets and Relations

- This mathematical structure formalizes the notion of reachability

Motivation for Well-founded Sets and Relations

- This mathematical structure formalizes the notion of reachability

- A discrete transition process, which:

- This mathematical structure formalizes the notion of reachability

- A discrete transition process, which:

    - either terminates

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

Motivation for Well-founded Sets and Relations

- This mathematical structure formalizes the notion of reachability

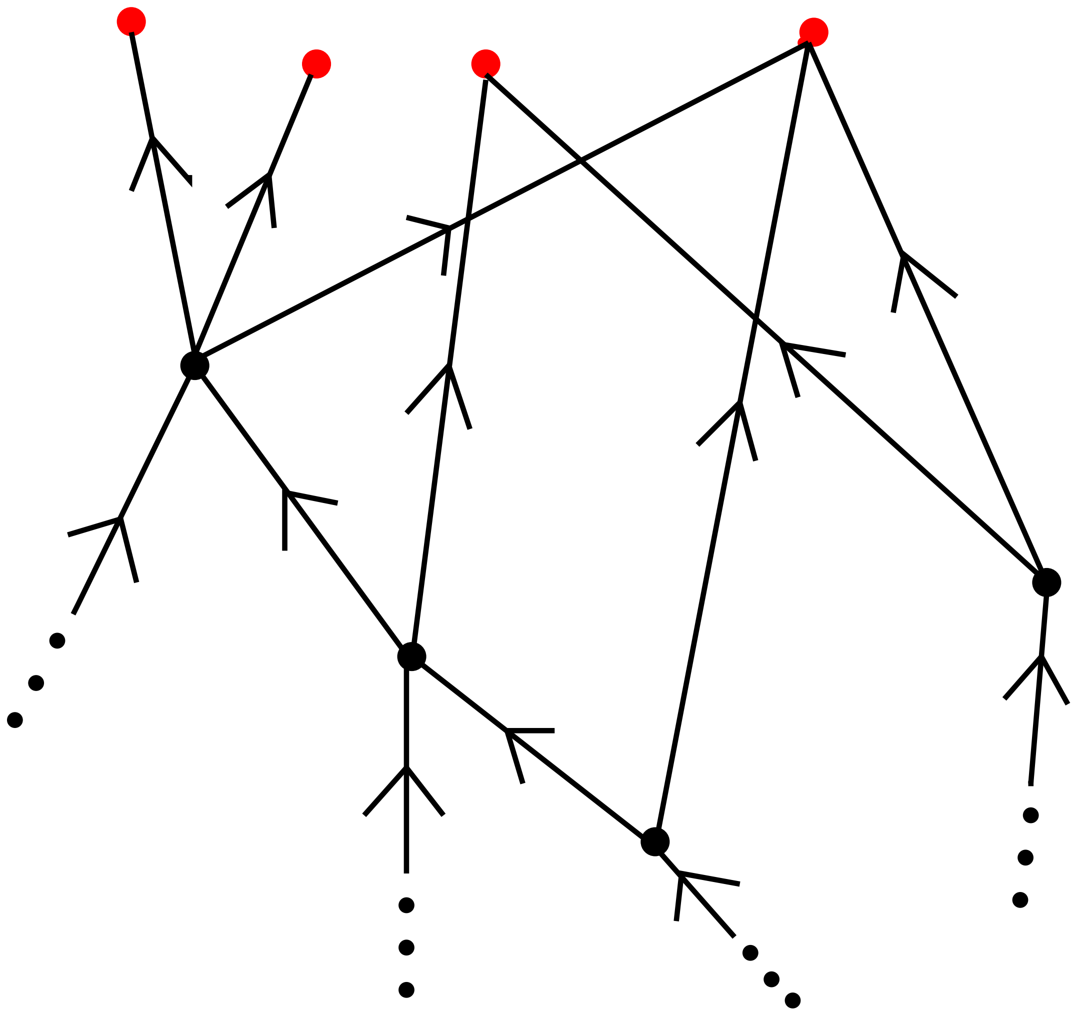
- A discrete transition process, which:

    - either terminates

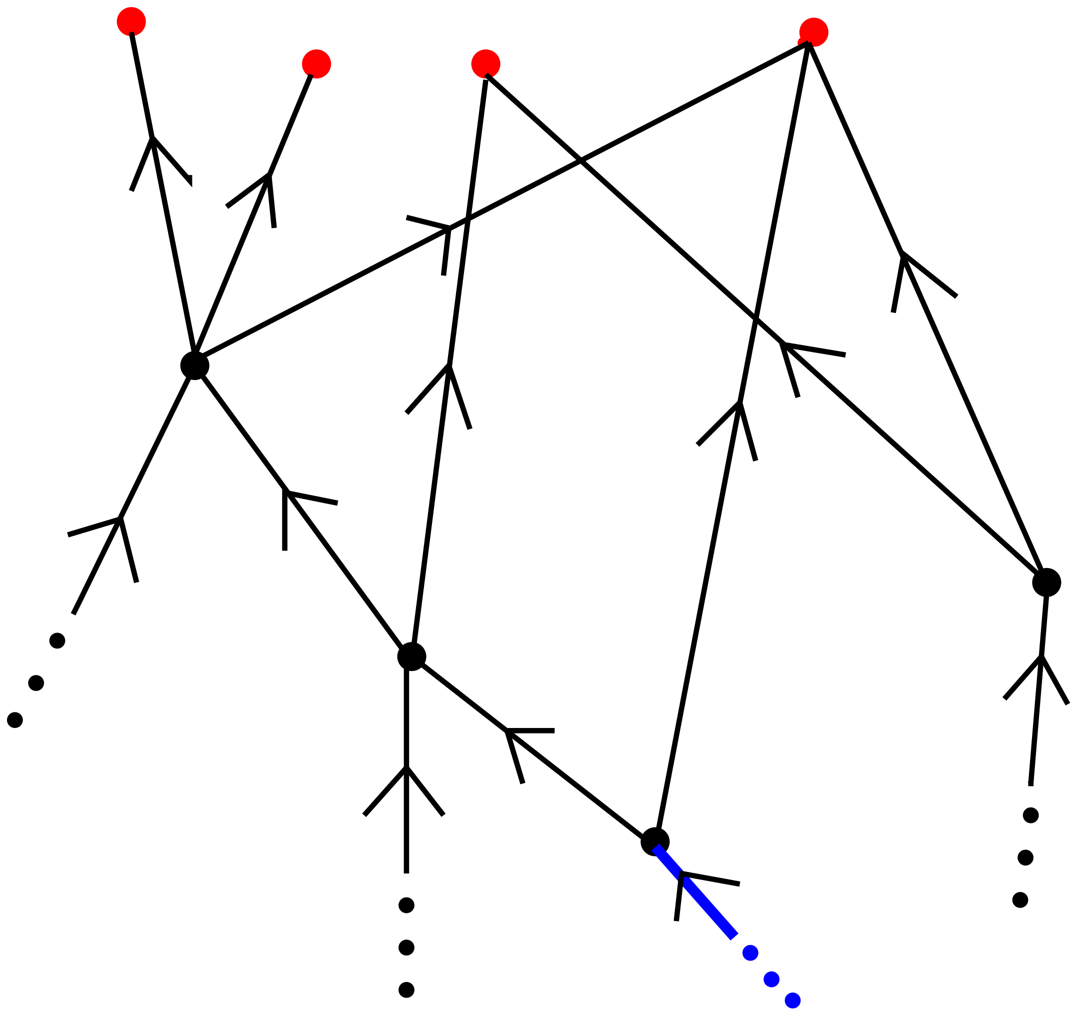
    - or eventually reaches certain states

- is formalized by means of well-founded traces

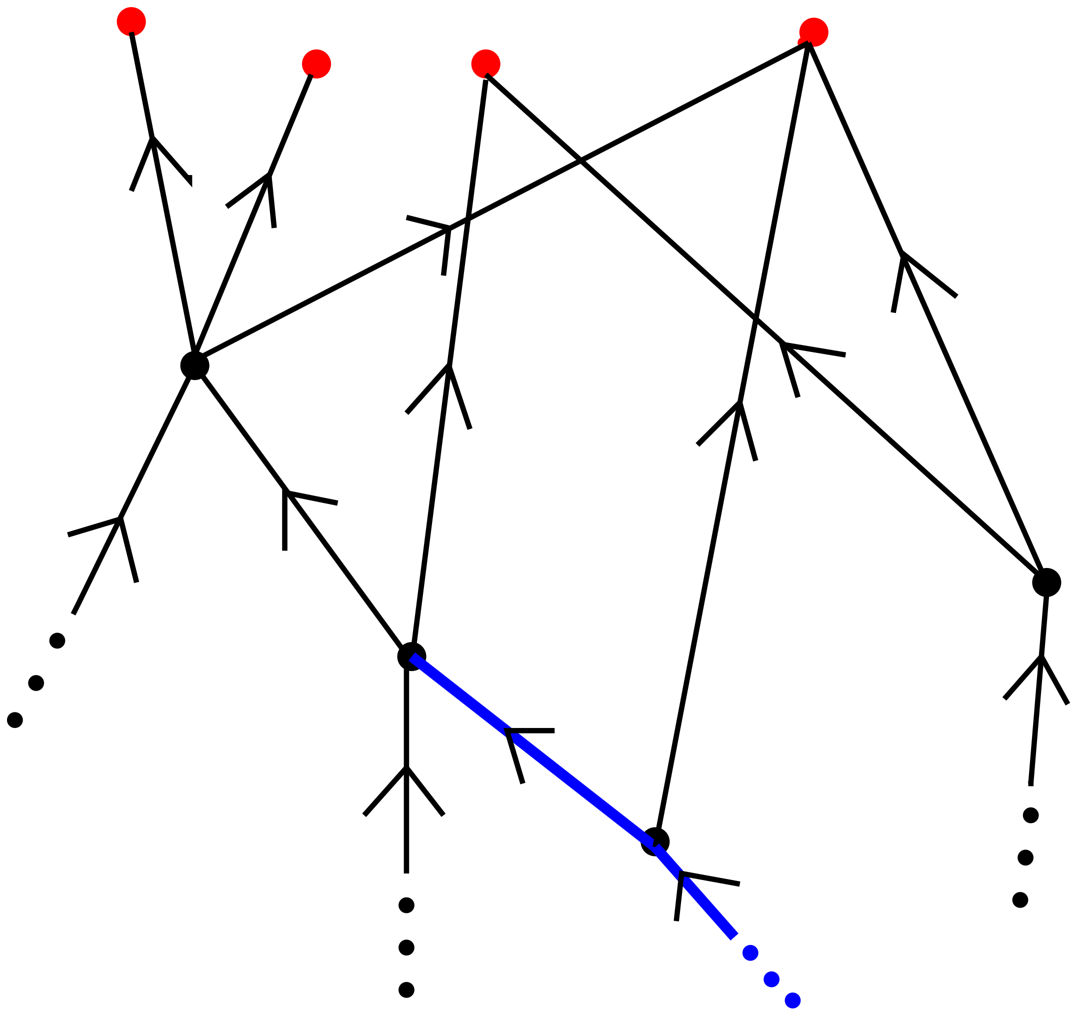
A Well-founded Relation



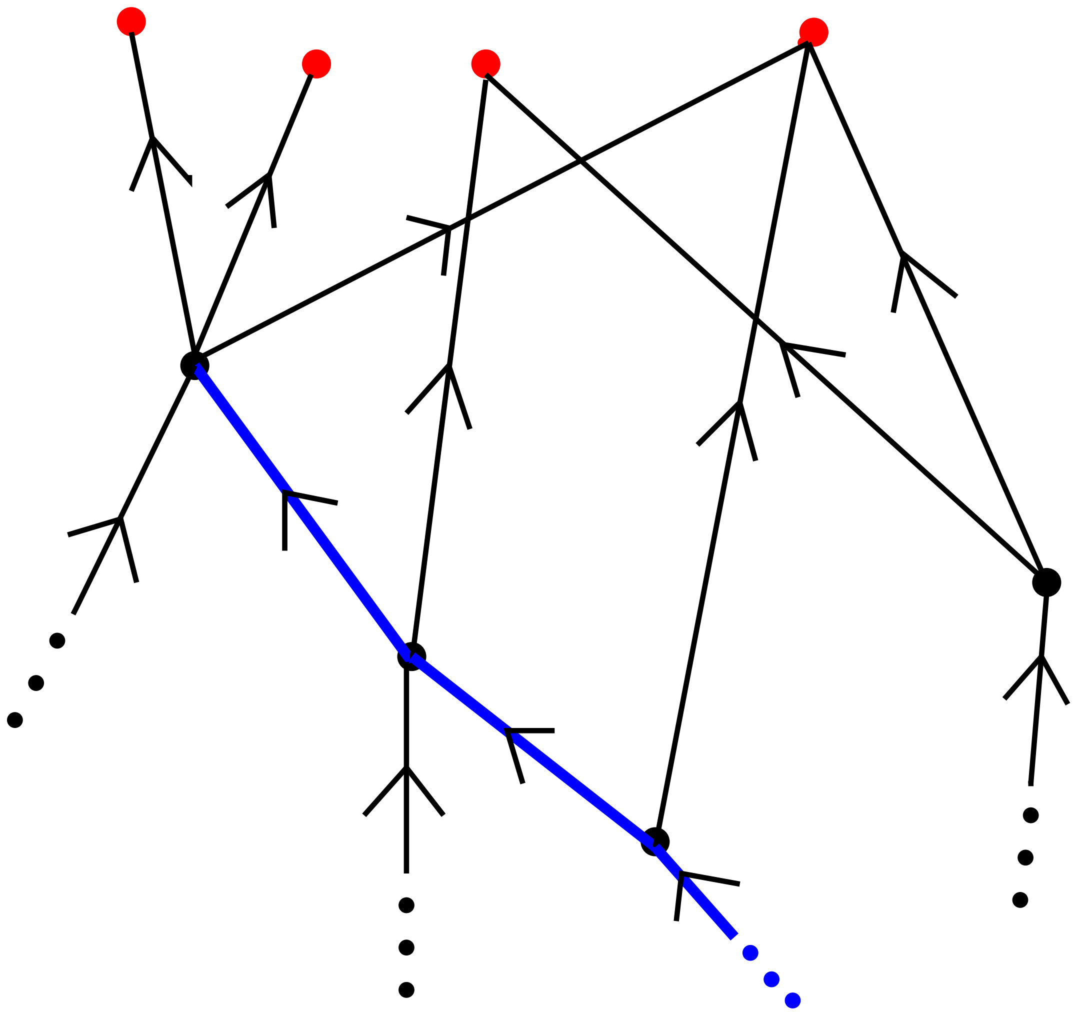
A Well-founded Relation



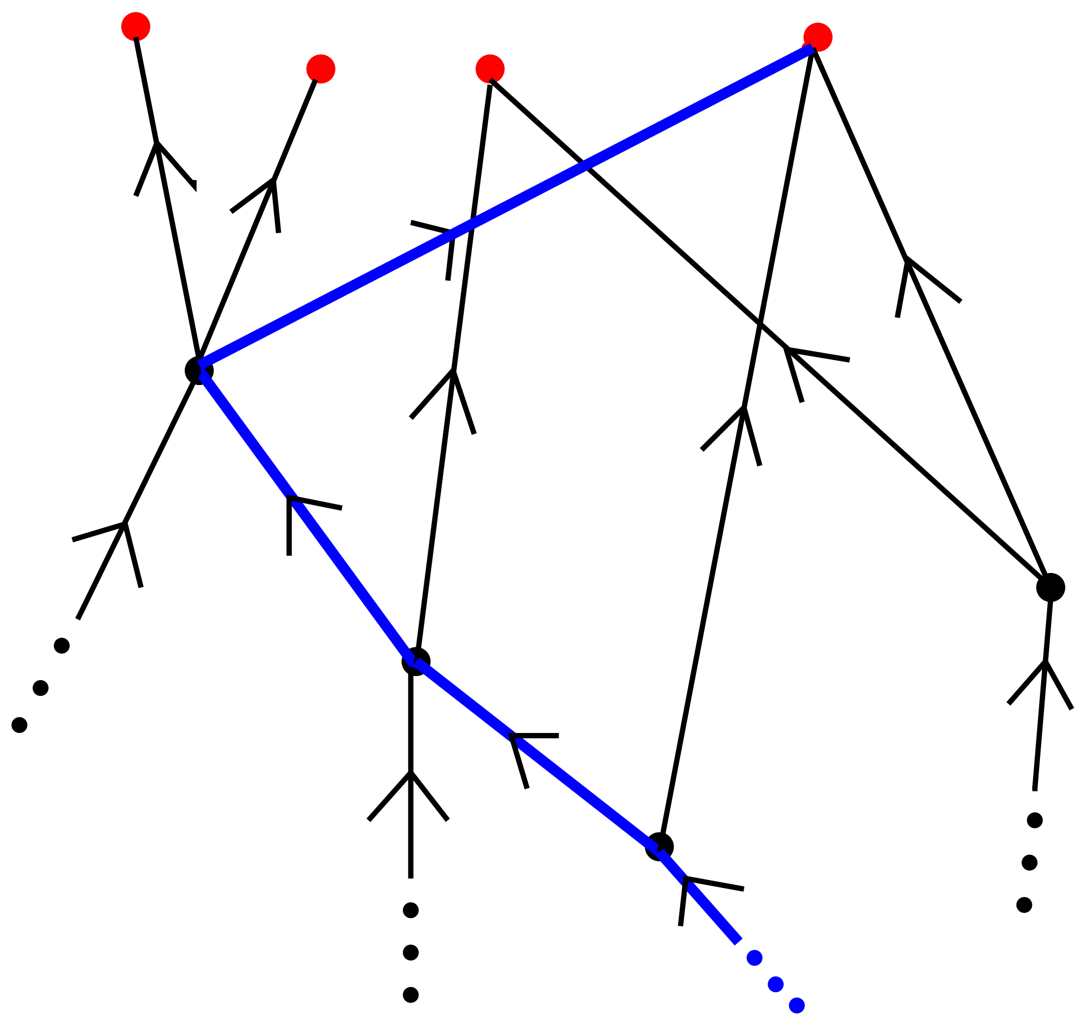
A Well-founded Relation



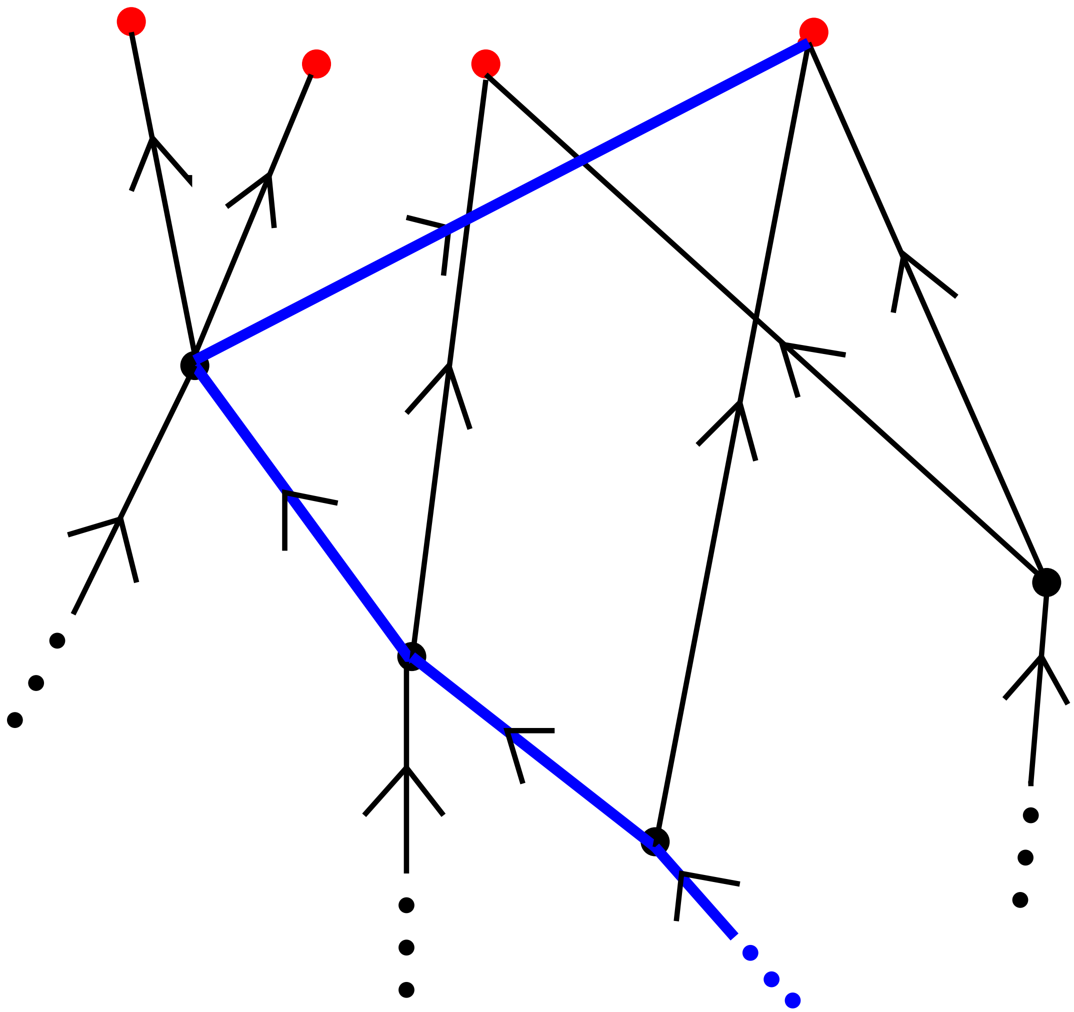
A Well-founded Relation



A Well-founded Relation

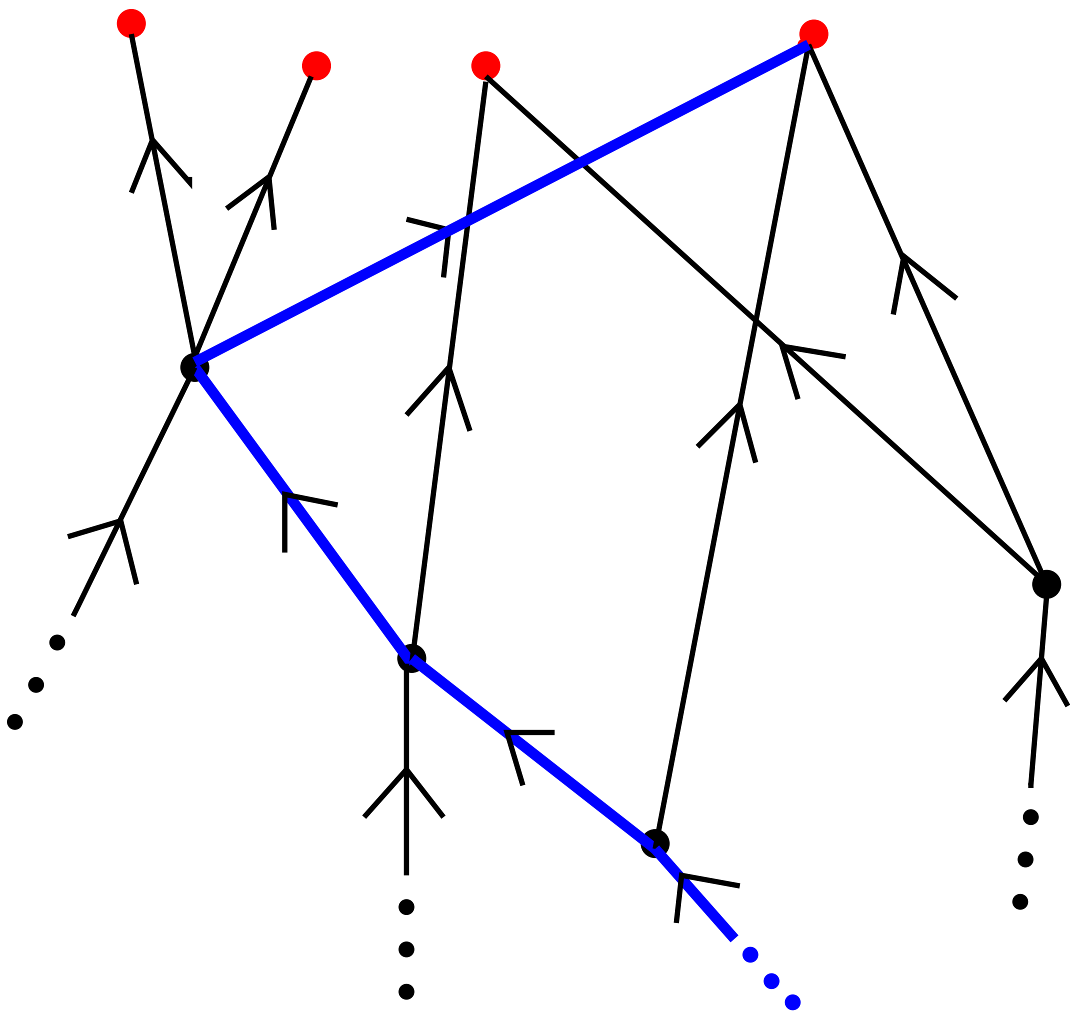


A Well-founded Relation



- From any point in the graph

A Well-founded Relation



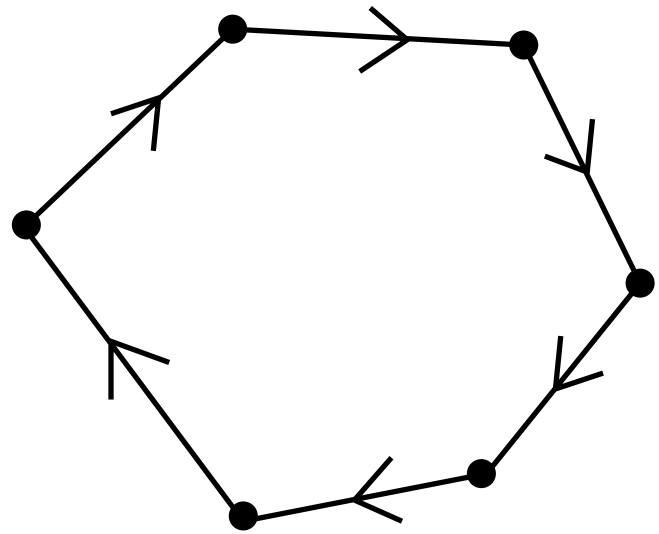
- From any point in the graph
- You always reach a red point after a FINITE travel

Relations which are not Well-founded: no Red Points

- A cycle

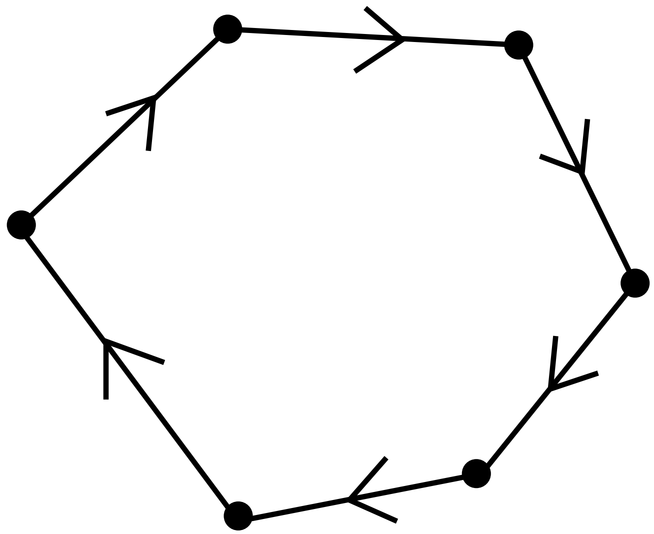
Relations which are not Well-founded: no Red Points

- A cycle



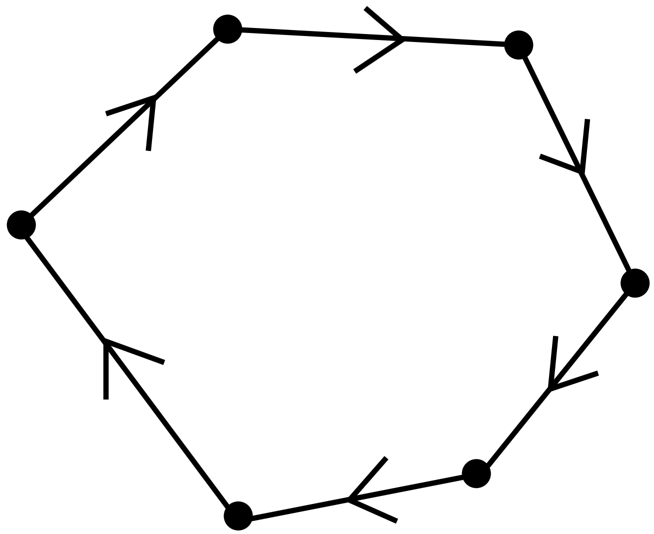
Relations which are not Well-founded: no Red Points

- A cycle



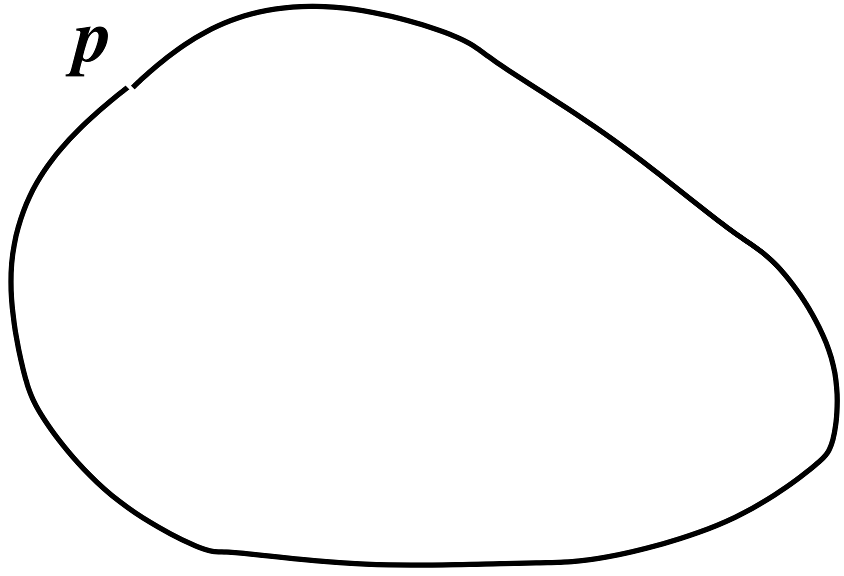
- An infinite chain

- A cycle

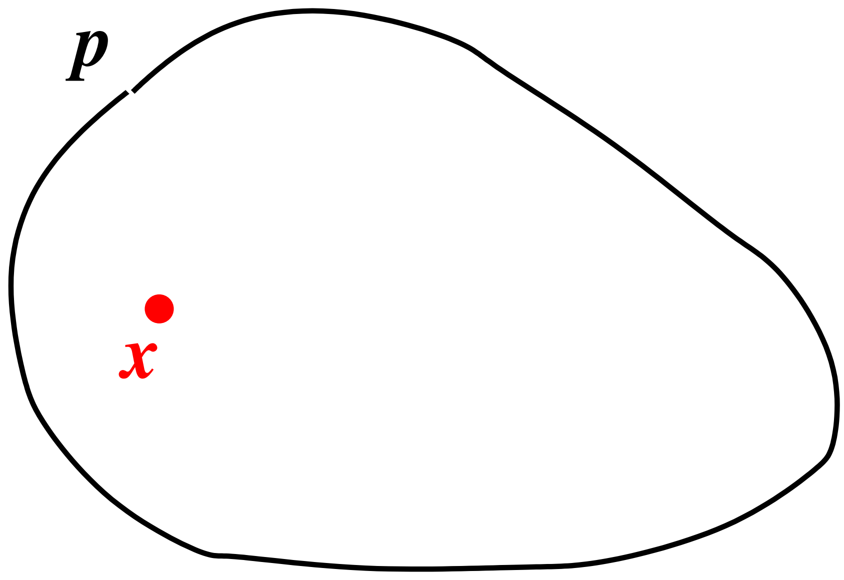


- An infinite chain

Set p Containing a Cycle or an Infinite Chain


p

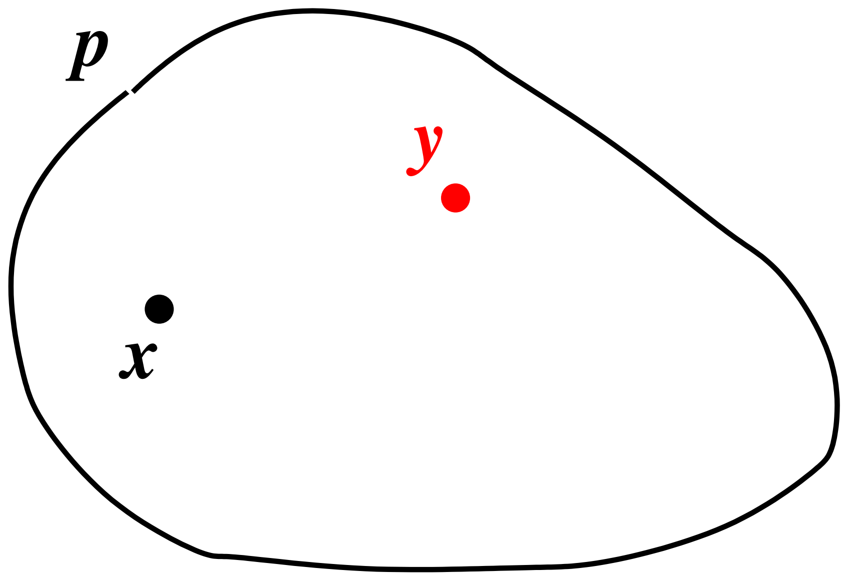
Set p Containing a Cycle or an Infinite Chain



For all x in p

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

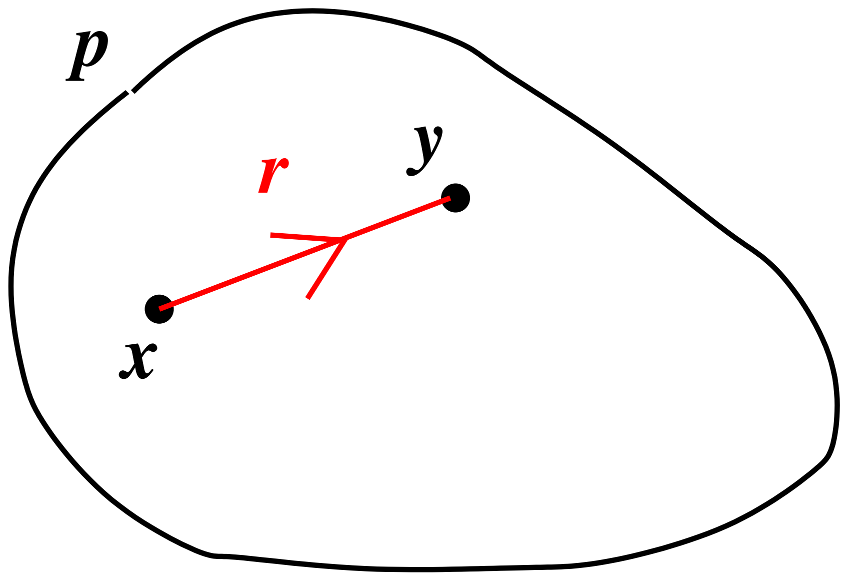
Set p Containing a Cycle or an Infinite Chain



For all x in p there exists a y in p

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

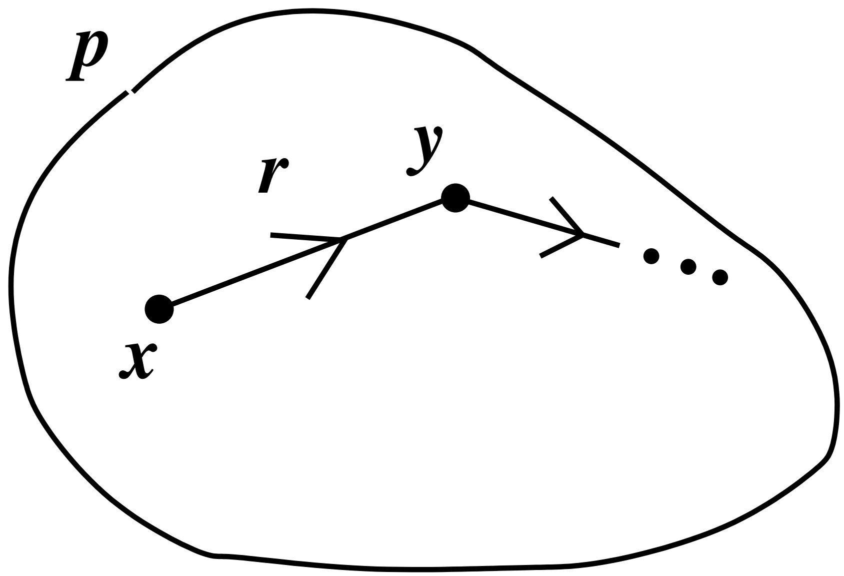
Set p Containing a Cycle or an Infinite Chain



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

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

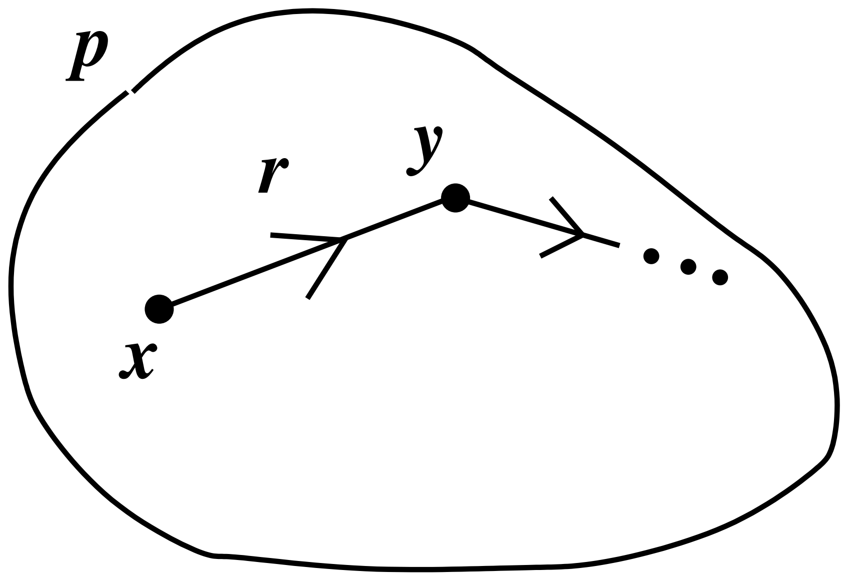
Set p Containing a Cycle or an Infinite Chain



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

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

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

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

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

Definition of a Well-founded Relation

Definition of a Well-founded Relation

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

Definition of a Well-founded Relation

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

- . . . unless it is the empty set

Definition of a Well-founded Relation

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

- ... unless it is the empty set

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

Definition of a Well-founded Relation

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

- . . . unless it is the empty set

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

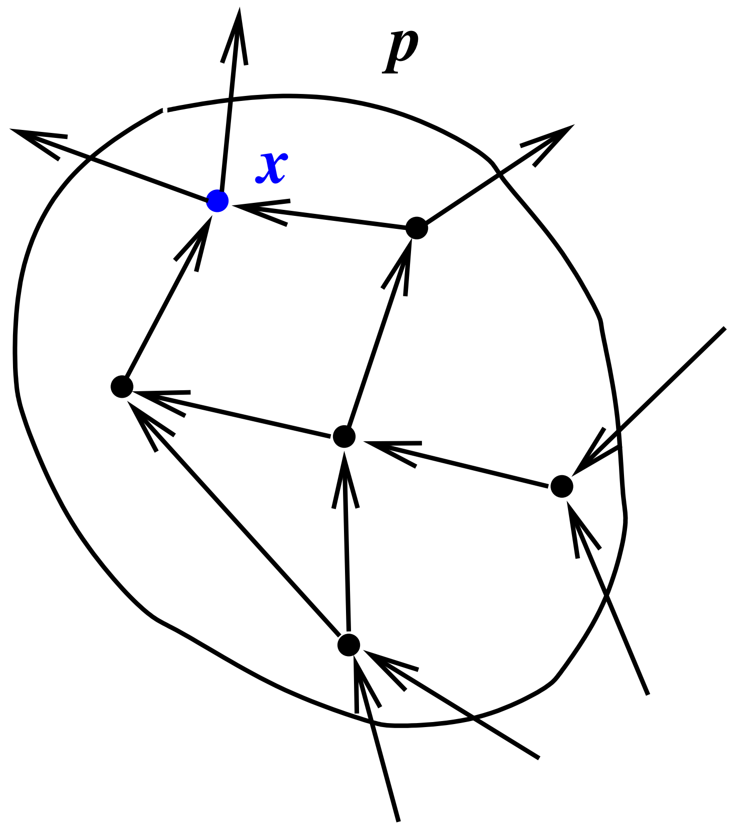
Another Definition

Another Definition

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

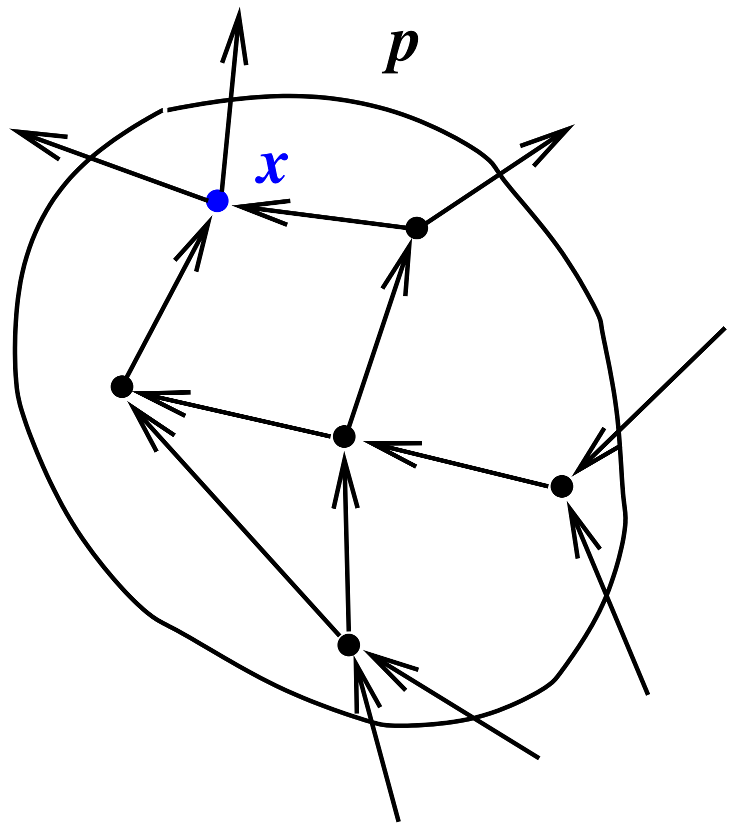
Another Definition

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



Another Definition

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



- Thus, forall z in p, x is NOT related to z

- For every non-empty subset p then
  -
  -

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

Another Definition

- For every non-empty subset $\boldsymbol{p}$ then

  - there exists a point $\boldsymbol{x}$ of $\boldsymbol{p}$ such that

  -

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

Another Definition

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

$$
\begin{array}{ll}
\forall \boldsymbol{p} \cdot & \boldsymbol{p} \neq \varnothing \\
& \Rightarrow \\
& \exists \boldsymbol{x} \cdot \boldsymbol{x} \in \boldsymbol{p} \;\wedge\; (\forall \boldsymbol{z} \cdot \boldsymbol{z} \in \boldsymbol{p} \;\Rightarrow
\end{array}
$$

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

$$
\begin{array}{ll}
\forall p \cdot & p \neq \varnothing \\
& \Rightarrow \\
& \exists x \cdot x \in p \ \land \ (\forall z \cdot z \in p \ \Rightarrow \ x \mapsto z \notin r)
\end{array}
$$

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

$$\begin{array}{ll}\forall p \cdot & p \neq \varnothing \\ & \Rightarrow \\ & \exists x \cdot x \in p \;\wedge\; (\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r)\end{array}$$

- Can we prove it with the Rodin Platform?

- 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

$$\begin{array}{ll} \forall p \cdot & p \neq \varnothing \\ & \Rightarrow \\ & \exists x \cdot x \in p \;\wedge\; (\forall z \cdot z \in p \;\Rightarrow\; x \mapsto z \notin r) \end{array}$$

- Can we prove it with the Rodin Platform?

- Can we explain what the computer has done?

Manual Proof

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

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

$\Leftrightarrow$ contraposition

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

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

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

Manual Proof

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

$\Leftrightarrow$ contraposition

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

$\Leftrightarrow$ de Morgan

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

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

$\Leftrightarrow$ 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

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

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

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

$\Leftrightarrow$ 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

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

$\Leftrightarrow$ 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

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

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

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

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

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

- 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

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

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

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

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

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

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

- The final touch

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

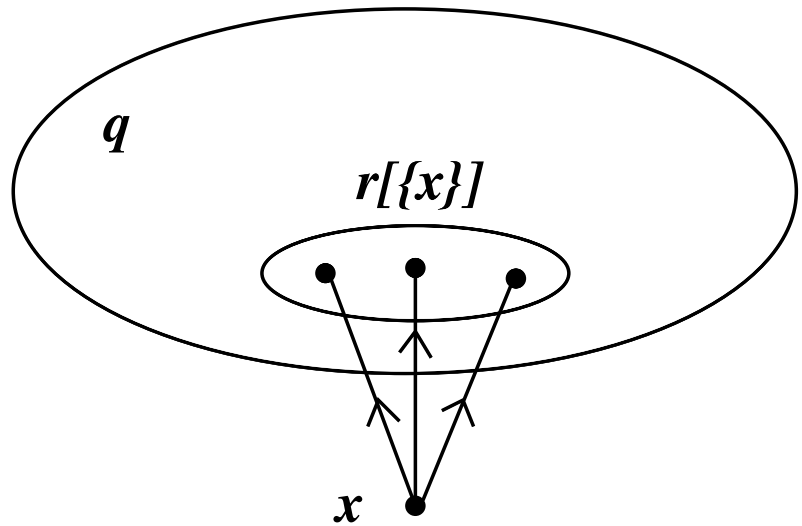
$$\forall q \cdot \quad \forall x \cdot (\forall y \cdot x \mapsto y \in r \;\Rightarrow\; y \in q) \;\Rightarrow\; x \in q \\ \Rightarrow \\ \forall z \cdot z \in S \;\Rightarrow\; z \in q$$

- The final touch

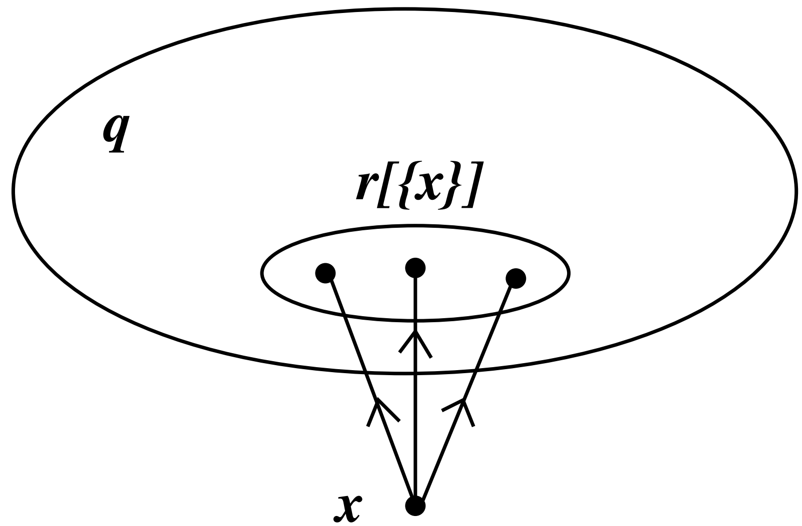
$$\forall q \cdot \quad \forall x \cdot r[\{x\}] \subseteq q \;\Rightarrow\; x \in q \\ \Rightarrow \\ S \subseteq q$$

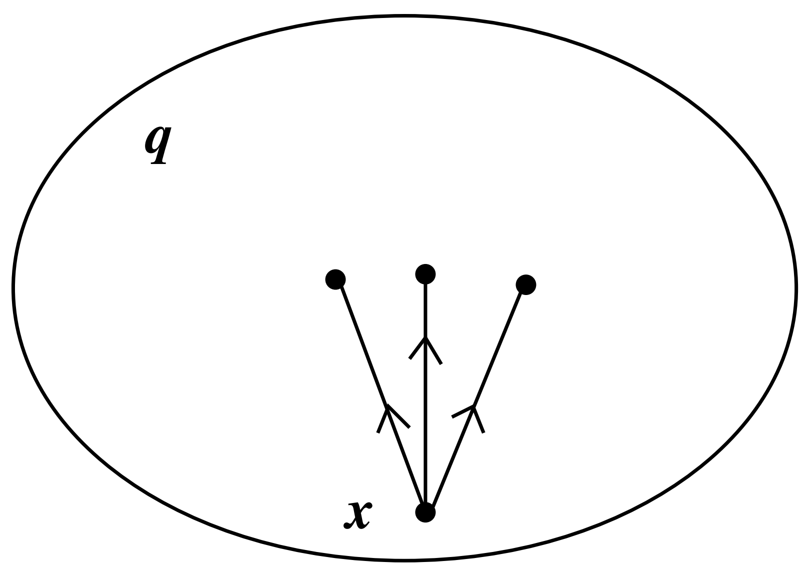
- Can we prove it with the Rodin Platform?

Induction Principle: Informal Explanation



Induction Principle: Informal Explanation





2. Fixpoint

Motivation for Fixpoint

- This mathematical concept is used to formalize recursion

Definition

- We are given a set function $\boldsymbol{f}$

$$\boldsymbol{f} \in \mathbb{P}(\boldsymbol{S}) \rightarrow \mathbb{P}(\boldsymbol{S})$$

Definition

- We are given a set function f

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

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

$$fix(f) = f(fix(f))$$

- We are given a set function f

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

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

$$fix(f) = f(fix(f))$$

- Proposal

$$fix(f) = \mathrm{inter}(\{s | f(s) \subseteq s\})$$

Two Useful Lemmas

Two Useful Lemmas

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

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

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

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

$$\forall s \cdot f(s) \subseteq s \Rightarrow fix(f) \subseteq s$$

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

Two Useful Lemmas

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

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

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

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

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

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

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

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

- Can we prove them with the Rodin Platform?

- Additional needed constraint: f is monotone

- Additional needed constraint: f is monotone

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

- Additional needed constraint: f is monotone

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

- $fix(f)$ is the least fixpoint

The Main Results (Knaster-Tarski)

- Additional needed constraint: f is monotone

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

- $fix(f)$ is the least fixpoint

$$\forall t \cdot t = f(t) \;\Rightarrow\; fix(f) \subseteq t$$

The Main Results (Knaster-Tarski)

- Additional needed constraint: f is monotone

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

- $fix(f)$ is the least fixpoint

$$\forall t \cdot t = f(t) \;\Rightarrow\; fix(f) \subseteq t$$

- Can we prove them with the Rodin Platform?

3. Transitive Closure

Motivation for Transitive Closure

- This mathematical concept formalizes the notion of a transition system achievement

Naive Approach at the Irreflexive Transitive Closure r^+

Naive Approach at the Irreflexive Transitive Closure r^+

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

$$\boldsymbol{r} \in \boldsymbol{S} \leftrightarrow \boldsymbol{S}$$

- 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:

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:

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

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

Naive Approach at the Irreflexive Transitive Closure r^+

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

- Let us compose $\boldsymbol{r^+}$ with $\boldsymbol{r}$

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

- Let us compose $\boldsymbol{r}^+$ with $\boldsymbol{r}$

$$\boldsymbol{r}^+ ; \boldsymbol{r} \;=\; (\boldsymbol{r} \;\cup\; \boldsymbol{r}^2 \;\cup\; \boldsymbol{r}^3 \;\cup\; \ldots \;\cup\; \boldsymbol{r}^n \;\cup\; \ldots) ; \boldsymbol{r}$$

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

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

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

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

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

- 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

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

- 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

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

- r^+ is thus a fixpoint of the function $f \in (S \leftrightarrow S) \rightarrow (S \leftrightarrow S)$ where

- r^+ is thus a fixpoint of the function $f \in (S \leftrightarrow S) \rightarrow (S \leftrightarrow S)$ where

$$\forall s \cdot s \in S \leftrightarrow S \;\Rightarrow\; f(s) = r \cup (s \,;\, r)$$

- r^+ is thus a fixpoint of the function $f \in (S \leftrightarrow S) \rightarrow (S \leftrightarrow S)$ where

$$\forall s \cdot s \in S \leftrightarrow S \;\Rightarrow\; f(s) = r \cup (s\,;r)$$

$$\boxed{r^+ \;=\; fix(f)}$$

- r^+ is thus a fixpoint of the function $f \in (S \leftrightarrow S) \rightarrow (S \leftrightarrow S)$ where

$$\forall s \cdot s \in S \leftrightarrow S \;\Rightarrow\; f(s) = r \cup (s \,;\, r)$$

$$\boxed{r^+ \;=\; fix(f)}$$

Exercise: Prove that the function f is indeed monotone

$$r \subseteq r^+$$

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

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

- Can we prove them with Rodin?

More Results

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

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

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

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

r is wf $\Rightarrow$ r^+ is wf

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

- Can we prove them with Rodin?

4. Graph

- Used a lot in networking

- A graph is simply formalized as a binary relation r built on set S

$$r \in S \leftrightarrow S$$

$r = r^{-1}$	r is symmetric
$r \cap r^{-1} = \varnothing$	r is asymmetric
$r \cap r^{-1} \subseteq \mathrm{id}$	r is antisymmetric
$\mathrm{id} \subseteq r$	r is reflexive
$r \cap \mathrm{id} = \varnothing$	r is irreflexive
$r ; r \subseteq r$	r is transitive

$r = r^{-1}$	$\forall x, y \cdot x \in S \wedge y \in S \Rightarrow (x \mapsto y \in r \Leftrightarrow y \mapsto x \in r)$
$r \cap r^{-1} = \varnothing$	$\forall x, y \cdot x \mapsto y \in r \Rightarrow y \mapsto x \notin r$
$r \cap r^{-1} \subseteq \mathrm{id}$	$\forall x, y \cdot x \mapsto y \in r \wedge y \mapsto x \in r \Rightarrow x = y$
$\mathrm{id} \subseteq r$	$\forall x \cdot x \in S \Rightarrow x \mapsto x \in r$
$r \cap \mathrm{id} = \varnothing$	$\forall x, y \cdot x \mapsto y \in r \Rightarrow x \neq y$
$r ; r \subseteq r$	$\forall x, y, z \cdot x \mapsto y \in r \wedge y \mapsto z \in r \Rightarrow x \mapsto z \in r$

Set-theoretic statements are far more readable than predicate calculus statements

Formalizing Strong Connectivity

- A strongly connected graph $\boldsymbol{r}$ is one where:

every node can be reached from any other node

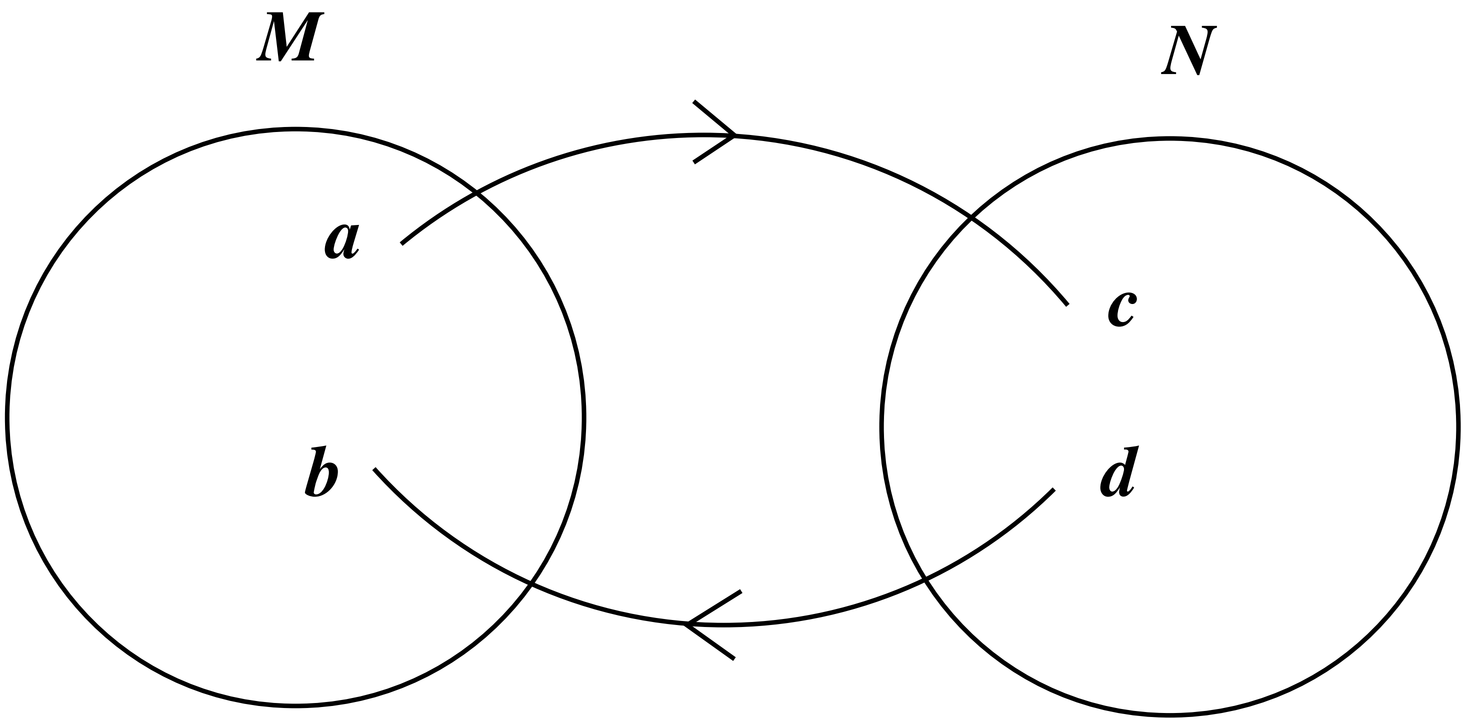
- Formal definition

$$\boldsymbol{r}^{\star} = \boldsymbol{S} \times \boldsymbol{S}$$

- Equivalent definition (more convenient for proofs)

$$\forall \boldsymbol{s} \cdot \boldsymbol{s} \neq \varnothing \;\land\; \boldsymbol{r}[\boldsymbol{s}] \subseteq \boldsymbol{s} \;\;\Rightarrow\;\; \boldsymbol{S} \subseteq \boldsymbol{s}$$

An Interesting Theorem about Strong Connectivity



Strongly connected graph g built on M

Strongly connected graph h built on N

The resulting graph on built on MVN is strongly connected

5. Tree

Motivation for Tree

- It is a very common data structure in Informatics

Special Case: a Tree

Special Case: a Tree

- A tree is a special case of well-founded relation

Special Case: a Tree

- A tree is a special case of well-founded relation

- We are given a special point t: the top of the tree

Special Case: a Tree

- A tree is a special case of well-founded relation

- We are given a special point t: the top of the tree

- The well-founded relation relation r becomes a total function f

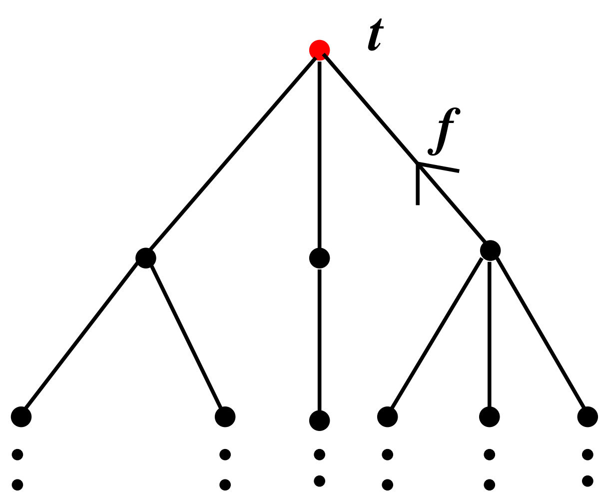
Special Case: a Tree

- A tree is a special case of well-founded relation

- We are given a special point t: the top of the tree

- The well-founded relation relation r becomes a total function f

$$f \in S \setminus \{t\} \to S$$



Special Case: a Tree

-Definition

$$f \in S \setminus \{t\} \rightarrow S$$

$$\forall z \cdot s \subseteq f^{-1}[s] \;\Rightarrow\; s = \varnothing$$

- The Induction Principle becomes

$$\begin{array}{ll} \forall q \cdot & t \in q \\ & (\forall x \cdot x \neq t \;\wedge\; f(x) \in q \;\Rightarrow\; x \in q) \\ & \Rightarrow \\ & \forall z \cdot z \in q \end{array}$$

Special Case: a Tree

- The Induction Principle becomes

$$
\begin{array}{ll}
\forall q \cdot & t \in q \\
& (\forall x \cdot x \neq t \;\wedge\; f(x) \in q \;\Rightarrow\; x \in q) \\
& \Rightarrow \\
& \forall z \cdot z \in q
\end{array}
$$

- Can we prove it with the Rodin Platform?

Conclusion

- The pros:

Conclusion

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

Conclusion

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

Conclusion

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

- The cons:

Conclusion

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

- The cons:
    - theorems cannot be reused easily

Conclusion

- 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

Conclusion

- 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:

Conclusion

- 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:
    - mathematical extensions