Inductively defined subsets

Given a set of axioms and rules over a set U, the subset of U **inductively defined** by the axioms and rules consists of all and only the elements $u \in U$ for which there is a derivation with conclusion u.

finite (labelled) tree with u at root, axioms at leaves and each vertex the conclusion of a rule whose hypotheses are the children of the vertex

Rule Induction

Theorem. The subset $I \subseteq U$ inductively defined by a collection of axioms and rules is closed under them and is the least such subset: if $S \subseteq U$ is also closed under the axioms and rules, then $I \subseteq S$.

Given axioms and rules for inductively defining a subset of a set U, we say that a subset $S \subseteq U$ is **closed under the axioms and rules** if

- for every axiom $\dfrac{}{a}$, it is the case that $a \in S$
- for every rule $\dfrac{h_1 \; h_2 \; \cdots \; h_n}{c}$, if $h_1, h_2, \ldots, h_n \in S$, then $c \in S$.

E.g. for the axiom & rules

$$\frac{}{\varepsilon} \qquad \frac{u}{aub} \qquad \frac{u}{bua} \qquad \frac{u \quad v}{uv}$$

(all $u, v \in \{a,b\}^*$)

the subset

$$\{u \in \{a,b\}^* \mid \#_a(u) = \#_b(u)\}$$

number of 'a's in the string u

E.g. for the axiom & rules

$$\frac{}{\varepsilon} \qquad \frac{u}{aub} \qquad \frac{u}{bua} \qquad \frac{u \quad v}{uv}$$

(all $u, v \in \{a,b\}^*$)

the subset

$$\{u \in \{a,b\}^* \mid \#_a(u) = \#_b(u)\}$$

is closed under the axiom & rules.

(so is $\{u \in \{a,b\}^* \mid$ length of u is even $\}$)

N.B. for a given set $\mathcal{R}$ of axioms & rules

$$\boxed{\left\{ u \in \mathcal{U} \;\middle|\; \begin{array}{l} \forall S \subseteq \mathcal{U}. \\ (S \text{ closed under } \mathcal{R}) \Rightarrow u \in S \end{array} \right\}}$$

is closed under $\mathcal{R}$ (why?)
and so is the smallest such (with respect to subset inclusion, $\subseteq$).

Theorem. The subset $I \subseteq U$ inductively defined by a collection of axioms and rules is closed under them and is the least such subset: if $S \subseteq U$ is also closed under the axioms and rules, then $I \subseteq S$.

"the least subset closed under the axioms & rules"

is sometimes taken as the definition of

"inductively defined subset"

Proof of the Theorem [Page 21 of notes]

- I is closed under each axiom $\overline{\;a\;}$

'cos a is a derivation witnessing $a \in I$

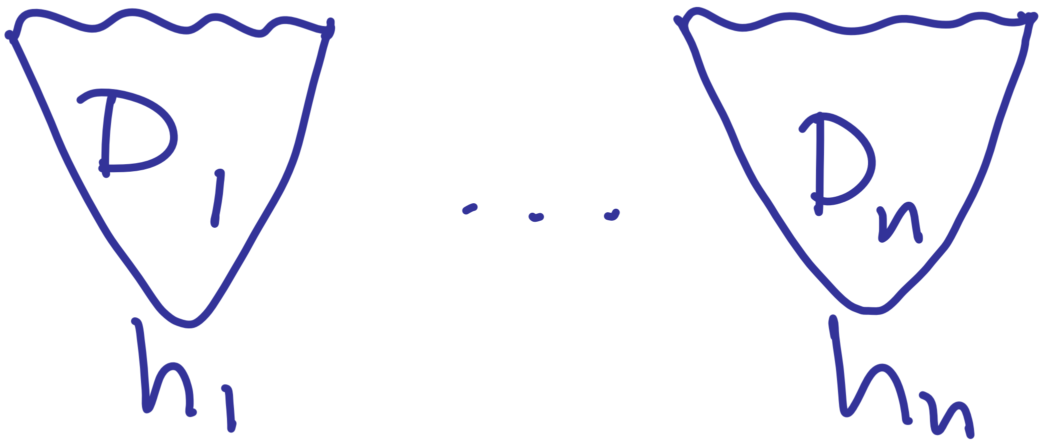
tree with root = leaf = a

Proof of the Theorem

- I is closed under each rule

$$\frac{h_1 \quad \cdots \quad h_n}{C}, \text{ 'cos if } h_1 \in I \;\&\; \cdots \;\&\; h_n \in I$$

then there are derivations



Proof of the Theorem

- I is closed under each rule

$$\frac{h_1 \quad \cdots\cdots \quad h_n}{c}$$

'cos if $h_1 \in I$ & $\cdots$ & $h_n \in I$

then there are derivations

$$\frac{\begin{matrix} D_1 \\ h_1 \end{matrix} \qquad \cdots \qquad \begin{matrix} D_n \\ h_n \end{matrix}}{c}$$

is a derivation witnessing that $c \in I$

Proof of the Theorem

So I is closed under the axioms & rules.

Finally, need to show for any $S \subseteq \mathcal{U}$

$$\boxed{S \text{ closed under axioms \& rules implies } I \subseteq S}$$

Proof of the Theorem

Suppose S closed under axioms & rules.

For each $n \in \mathbb{N} = \{0, 1, 2, \dots\}$, let

$\boxed{P(n) = \text{"all derivations of height } n \text{ have their conclusion in } S\text{"}}$

To see $I \subseteq S$, suffices to show

$\forall n \in \mathbb{N}.\ P(n)$

Prove this by Mathematical Induction

Proof of the Theorem

$\boxed{P(n) = \text{"all derivations of height } n \text{ have their conclusion in } S\text{"}}$

$$\forall n \in \mathbb{N}.\ P(n)$$

- Base case $P(0)$ — trivial ✓

Proof of the Theorem

$\boxed{P(n) = \text{"all derivations of height } n \text{ have their conclusion in } S\text{"}}$

$$\forall n \in \mathbb{N}.\ P(n)$$

- Base case $P(0)$ — trivial
- Induction step $P(n) \Rightarrow P(n+1)$

Proof of the Theorem

$P(n)$ = "all derivations of height n have their conclusion in S"

- Induction step $P(n) \Rightarrow P(n+1)$

Suppose $P(n)$ & D is a derivation of heigh $n+1$, with conclusion c say. So D looks like

$$\dfrac{\begin{matrix} D_1 & & D_m \\ c_1 & \cdots & c_m \end{matrix}}{c}$$

this is one of the rules (or an axiom, if $m=0$)

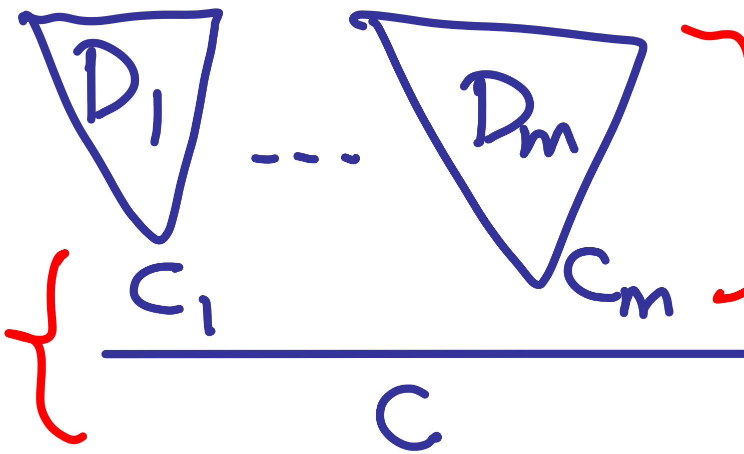
Proof of the Theorem

$P(n)$ = "all derivations of height n have their conclusion in S"

- Induction step $P(n) \Rightarrow P(n+1)$

Suppose $P(n)$ & D is a derivation of height $n+1$, with conclusion c say.

So D looks like



height n

this is one of the rules (or an axiom, if $m=0$)

Proof of the Theorem

$P(n) =$ "all derivations of height n have their conclusion in S"

- Induction step $P(n) \Rightarrow P(n+1)$

Suppose $P(n)$ & D is a derivation of heigh $n+1$, with conclusion c say.
So D looks like

$$\dfrac{\overset{\in S}{c_1} \qquad\qquad \overset{\in S}{c_m}}{c} \quad \Big\} \text{ height } n$$

Proof of the Theorem

$P(n) =$ "all derivations of height n have their conclusion in S"

- Induction step $P(n) \Rightarrow P(n+1)$

Suppose $P(n)$ & D is a derivation of heigh $n+1$, with conclusion c say.
So D looks like

this is one of the rules under which S is closed,

$$\frac{\overset{\in S}{c_1} \qquad \qquad \overset{\in S}{c_m}}{c}\quad \text{height } n$$

so $c \in S$

Proof of the Theorem

$P(n)$ = "all derivations of height n have their conclusion in S"

- Induction step $P(n) \Rightarrow P(n+1)$

Suppose $P(n)$ & D

heigh $n+1$, with conclusion c

... we have proved $P(n+1)$. ✓

Rule Induction

Theorem. The subset $I \subseteq U$ inductively defined by a collection of axioms and rules is closed under them and is the least such subset: if $S \subseteq U$ is also closed under the axioms and rules, then $I \subseteq S$.

We use the theorem as method of proof: given a property $P(u)$ of elements of U, to prove $\forall u \in I.\, P(u)$ it suffices to show

- **base cases:** $P(a)$ holds for each axiom $\dfrac{}{a}$
- **induction steps:** $P(h_1) \,\&\, P(h_2) \,\&\, \cdots \,\&\, P(h_n) \Rightarrow P(c)$ holds for each rule $\dfrac{h_1\ h_2\ \cdots\ h_n}{c}$

(To see this, apply the theorem with $S = \{u \in U \mid P(u)\}$.)

Example using rule induction

Let I be the subset of $\{a, b\}^*$ inductively defined by the axioms and rules on Slide 15.

$$\frac{}{\varepsilon} \qquad \frac{u}{aub} \qquad \frac{u}{bua} \qquad \frac{u \quad v}{uv}$$

Associated Rule Induction:

$$\begin{aligned}
& P(\varepsilon) \\
& \& \ \forall u \in I.\ P(u) \Rightarrow P(aub) \\
& \& \ \forall u \in I.\ P(u) \Rightarrow P(bua) \\
& \& \ \forall u, v \in I.\ P(u) \,\&\, P(v) \Rightarrow P(uv) \\
\Rightarrow\ & \forall u \in I.\ P(u)
\end{aligned}$$

Example using rule induction

Let I be the subset of $\{a,b\}^*$ inductively defined by the axioms and rules on Slide 15.

For $u \in \{a,b\}^*$, let $P(u)$ be the property

u contains the same number of a and b symbols

We can prove $\forall u \in I.\, P(u)$ by rule induction:

- **base case:** $P(\varepsilon)$ is true (the number of as and bs is zero!)
- **induction steps:** if $P(u)$ and $P(v)$ hold, then clearly so do $P(aub)$, $P(bua)$ and $P(uv)$.

(It's not so easy to show $\forall u \in \{a,b\}^*.\, P(u) \Rightarrow u \in I$ – rule induction for I is not much help for that.)

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,{}^{0} \qquad \frac{u}{au}\,{}^{1} \qquad \frac{u \quad v}{buv}\,{}^{2}}$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\quad \frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2 \quad}$$

In this case Rule Induction says:

if (0) $P(a)$

& (1) $\forall u \in I.\ P(u) \Rightarrow P(au)$

& (2) $\forall u,v \in I.\ P(u)\ \&\ P(v) \Rightarrow P(buv)$

then $\forall u \in I.\ P(u)$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,{}^{0} \qquad \frac{u}{au}\,{}^{1} \qquad \frac{u \quad v}{buv}\,{}^{2}}$$

Want to show

$$u \in I \Rightarrow \#_a(u) > \#_b(u)$$

number of 'a's in the string u

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\quad \frac{}{a}\,{}^{0} \qquad \frac{u}{au}\,{}^{1} \qquad \frac{u \quad v}{buv}\,{}^{2} \quad}$$

Want to show

$$u \in I \Rightarrow \#_a(u) > \#_b(u)$$

Do so by Rule Induction, with property $P(u) = \#_a(u) > \#_b(u)$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(0) $P(a)$ holds $(1 > 0)$

(1) If $P(u)$, then $\#_a(au) = 1 + \#_a(u)$

$$> \#_a(u)$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(0) $P(a)$ holds $(1 > 0)$

(1) If $P(u)$, then $\#_a(au) = 1 + \#_a(u)$

$$> \#_a(u)$$
$$> \#_b(u)$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,{}^{0} \qquad \frac{u}{au}\,{}^{1} \qquad \frac{u \quad v}{buv}\,{}^{2}}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(0) $P(a)$ holds $(1 > 0)$

(1) If $P(u)$, then $\#_a(au) = 1 + \#_a(u)$

$> \#_a(u)$

$> \#_b(u) = \#_b(au)$

so $P(au)$ holds as well.

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(2) Suppose $P(u)$ & $P(v)$ hold. Then

$$\#_a(buv) = \#_a(u) + \#_a(v)$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(2) Suppose $P(u)$ & $P(v)$ hold. Then

$$\#_a(buv) = \#_a(u) + \#_a(v)$$
$$\geq (\#_b(u)+1) + (\#_b(v)+1)$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(2) Suppose $P(u)$ & $P(v)$ hold. Then

$$\begin{aligned}\#_a(buv) &= \#_a(u) + \#_a(v) \\ &\geq \#_b(u) + \#_b(v) + 2 \\ &> \#_b(u) + \#_b(v) + 1\end{aligned}$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(2) Suppose $P(u)$ & $P(v)$ hold. Then

$$\begin{aligned}\#_a(buv) &= \#_a(u) + \#_a(v) \\ &> \#_b(u) + \#_b(v) + 1 \\ &= \#_b(buv)\end{aligned}$$

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\quad \frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2 \quad}$$

$$P(u) = \#_a(u) > \#_b(u)$$

(2) Suppose $P(u)$ & $P(v)$ hold. Then

$$\begin{aligned} \#_a(buv) &= \#_a(u) + \#_a(v) \\ &> \#_b(u) + \#_b(v) + 1 \\ &= \#_b(buv) \end{aligned}$$

so $P(buv)$ holds.

Example [CST 2009, Paper 2, Question 5]

$I \subseteq \{a,b\}^*$ inductively defined by

$$\boxed{\frac{}{a}\,0 \qquad \frac{u}{au}\,1 \qquad \frac{u \quad v}{buv}\,2}$$

$$P(u) = \#_a(u) > \#_b(u)$$

N.B. although we have

$$\forall u \in I.\ P(u)$$

don't have $\forall u \in \{a,b\}^*.\ P(u) \Rightarrow u \in I$

E.g. $P(aab)$, but $aab \notin I$ [WHY?]

Deciding membership of an inductively defined subset can be hard!

E.g. . . .

Collatz Conjecture

$$f(n) = \begin{cases} 1 & \text{if } n = 0, 1 \\ f(n/2) & \text{if } n > 1, n \text{ even} \\ f(3n+1) & \text{if } n > 1, n \text{ odd} \end{cases}$$

Does this define a total function $f : \mathbb{N} \to \mathbb{N}$? (nobody knows)

(If it does, then f is necessarily the constantly 1 function $n \mapsto 1$.)

Collatz Conjecture

$$f(n) = \begin{cases} 1 & \text{if } n = 0, 1 \\ f(n/2) & \text{if } n > 1, n \text{ even} \\ f(3n+1) & \text{if } n > 1, n \text{ odd} \end{cases}$$

Does this define a <u>total</u> function $f : \mathbb{N} \to \mathbb{N}$? (nobody knows)

Can reformulate as a problem about inductively defined subsets...

Collatz Conjecture

$$f(n) = \begin{cases} 1 & \text{if } n = 0, 1 \\ f(n/2) & \text{if } n > 1, n \text{ even} \\ f(3n+1) & \text{if } n > 1, n \text{ odd} \end{cases}$$

Is the subset $I \subseteq \mathbb{N}$ inductively defined by:

$$\boxed{\frac{}{0} \qquad \frac{}{1} \qquad \frac{k}{2k} \qquad \frac{6k+4}{2k+1} \qquad (k \geq 1)}$$

equal to the whole of $\mathbb{N}$?