⌜Proof By Induction⌟

Example Problem

"free variables" $FV : \mathcal{A} \to P(Var)$

recursion
$$\begin{cases} FV(x) = \{x\} \\ FV(n) = \emptyset \\ FV(e_1 + e_2) = FV(e_1) \cup FV(e_2) \\ FV(e_1 - e_2) = FV(e_1) \cup FV(e_2) \\ FV(e_1 * e_2) = FV(e_1) \cup FV(e_2) \end{cases}$$

$State = Var \to \mathbb{Z}$

If $\forall x \in FV(e)$, $\sigma(x) = \sigma'(x)$
then $[\![e]\!]_{\mathcal{A}}(\sigma) = [\![e]\!]_{\mathcal{A}}(\sigma')$

↳ recursive definitions
there are infinitely many e

$P(e) = \forall \sigma, \sigma' \in State$
If $\forall x \in FV(e)$. $\sigma(x) = \sigma'(x)$
then $[\![e]\!]_{\mathcal{A}}(\sigma) = [\![e]\!]_{\mathcal{A}}(\sigma')$

Prove $\forall e \in \mathcal{A}$. $P(e)$ by induction.

(Var) Suppose e is $x \in Var$
Goal: $P(x) = \forall \sigma, \sigma' \in State$
If $\forall x \in FV(x)$. $\sigma(x) = \sigma'(x)$
then $[\![x]\!]_{\mathcal{A}}(\sigma) = [\![x]\!]_{\mathcal{A}}(\sigma')$

let $\sigma, \sigma' \in State$.
asm. $\forall x \in FV(x)$. $\sigma(x) = \sigma'(x)$
i.e $\sigma(x) = \sigma'(x)$
therefore. $[\![x]\!]_{\mathcal{A}}(\sigma) = \sigma(x)$
$= \sigma'(x) = [\![x]\!]_{\mathcal{A}}(\sigma')$

(Add) Goal: $P(e_1 + e_2)$
Assume Induction hypotheses $P(e_1)$ and $P(e_2)$

Expand
$\forall \sigma, \sigma' \in State$
If $\forall x \in FV(e_1 + e_2)$. $\sigma(x) = \sigma'(x)$
then $[\![e_1 + e_2]\!](\sigma) = [\![e_1 + e_2]\!](\sigma')$

Expand

let $\sigma, \sigma' \in State$
such that $\forall x \in FV(e_1 + e_2)$. $\sigma(x) = \sigma'(x)$.

Goal: $\underbrace{[\![e_1]\!](\sigma)} + \underbrace{[\![e_2]\!](\sigma)} = [\![e_1]\!](\sigma') + [\![e_2]\!](\sigma')$

Here we relate the goal to
the <u>induction hypotheses</u> $P(e_1)$ and $P(e_2)$
but we need that:
$\forall x \in FV(e_1)$. $\sigma(x) = \sigma'(x)$
and $\forall x \in FV(e_2)$. $\sigma(x) = \sigma'(x)$
for the hypotheses to apply

As $FV(e_1), FV(e_2) \subseteq FV(e_1 + e_2)$ by defn.
we have that
$\forall x \in FV(e_1)$. $\sigma(x) = \sigma'(x)$
and $\forall x \in FV(e_2)$. $\sigma(x) = \sigma'(x)$
as required

Therefore, the induction hypotheses tell
us that $[\![e_1]\!](\sigma) = [\![e_1]\!](\sigma')$
and $[\![e_2]\!](\sigma) = [\![e_2]\!](\sigma')$

Application of induction hypotheses

Thus $[\![e_1 + e_2]\!](\sigma) = [\![e_1 + e_2]\!](\sigma')$.

Numerical Induction

Proof by induction
$\forall n \in \mathbb{N}$. $P(n)$ ← Property.
(Base Case) $P(0)$
(Inductive Case) $P(n) \Rightarrow P(n+1)$ for all $n \in \mathbb{N}$.

$P(0)$ by base case
$P(1)$ because $P(0)$
and $P(n) \Rightarrow P(n+1)$
$\therefore P(1)$

$P(2)$ because $P(1)$
and $P(n) \Rightarrow P(n+1)$
$\therefore P(2)$

$\forall n$. $0 + \cdots + n = \frac{1}{2} \cdot n \cdot (n+1)$
By induction:
(Base) $0 + \cdots + 0 = \frac{1}{2} \cdot 0 \cdot (0+1)$ ← "Goal"
$\Leftrightarrow 0 = 0$
trivial

(Induction)
Supp. $0 + \cdots + n = \frac{1}{2} \cdot n \cdot (n+1)$ ← "Induction Hypothesis" $(P(n))$

Expand defn.
$\Leftrightarrow (0 + \cdots + n) + n + 1 = \frac{1}{2} \cdot n \cdot (n+1) + (n+1)$
$\Leftrightarrow 0 + \cdots + (n+1) = \frac{1}{2} \cdot n^2 + \frac{1}{2} n + n + 1$ ↳ simplification
$\Leftrightarrow 0 + \cdots + (n+1) = \frac{1}{2} \cdot (n+1)(n+2)$
$(P(n+1))$

Goal: $0 + \cdots + (n+1) = \frac{1}{2} \cdot (n+1)\{(n+1)+1\}$

Numbers as a Grammar

$\ulcorner N \to 0 \mid N + 1 \lrcorner$

"2" $= \underbrace{(0+1)}_{\text{"1"}} + 1$

Production Rules
⟷ Cases of an
Induction principle

$2 \in \mathbb{N}$.
because $1 \in \mathbb{N}$
because $0 \in \mathbb{N}$

$P(2)$
because $P(1)$
because $P(0)$

Structural induction

for Arithmetic Expressions:
$A \to x \mid n \mid A + A \mid A - A \mid A * A$

To prove $\forall e \in A$. $P(e)$

Induction Principle for Arithmetic Expressions:

(Var) $P(x)$ for all $x \in Var$
"base case"

(Literals) $P(n)$ for all $n \in \mathbb{Z}$
"base case"

(Add) $P(e_1 + e_2)$
assuming $\underbrace{P(e_1) \text{ and } P(e_2)}_{\text{Induction Hypothesis}}$
"Induction case"
sub-expressions / sub-trees

(Sub) $P(e_1 - e_2)$
assuming $\underbrace{P(e_1) \text{ and } P(e_2)}_{\text{Induction hypotheses}}$

(Mul) $P(e_1 * e_2)$
assuming $\underbrace{P(e_1) \text{ and } P(e_2)}_{\text{induction hypotheses}}$

$P(x + 1)$?
because $P(x)$ and $P(1)$
because (Var) and (Lited)