6.977: Reasoning about sequential programs **CSAIL, MIT**
carroll@csail.mit.edu, 32-G708, x87110 **20/ix/07**

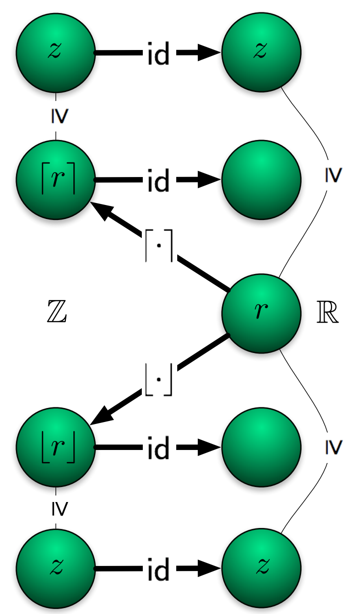
Notes for Lecture 2

Ceilings and floors as Galois connections

Program

All variables are integers.

$\{N \geq 0 \wedge D \geq 1\}$
$n, d := N, D;$
do $d \neq 0 \rightarrow$
  $x\colon [\, \lfloor n/d \rfloor \leq x \leq \lceil n/d \rceil \,];$ // Choose x so that $\lfloor n/d \rfloor \leq x \leq \lceil n/d \rceil$.
  $n, d := n{-}x, d{-}1;$
od
$\{N$ has been "evenly divided" into D pieces of $x\}$



Conjecture

$$d\lfloor N/D \rfloor \;\leq\; n \;\leq d\lceil N/D \rceil \quad \text{is invariant,}$$

whence every assignment to x satisfies $\lfloor N/D \rfloor \leq x \leq \lceil N/D \rceil$.

Proof

Working backwards, we have

$d\lfloor N/D \rfloor \;\leq\; n \;\leq\; d\lceil N/D \rceil$

through $wp.(n, d := n{-}x, d{-}1)$ gives

$(d{-}1)\lfloor N/D \rfloor \;\leq\; n{-}x \;\leq\; (d{-}1)\lceil N/D \rceil$

$\equiv \quad x + (d{-}1)\lfloor N/D \rfloor \;\leq\; n \;\leq\; x + (d{-}1)\lceil N/D \rceil$

through $wp.(x\colon [\, \lfloor n/d \rfloor \leq x \leq \lceil n/d \rceil \,])$ gives

$\lceil n/d \rceil + (d{-}1)\lfloor N/D \rfloor \;\leq\; n \;\leq \lfloor n/d \rfloor + (d{-}1)\lceil N/D \rceil$

$\equiv \quad n/d + (d{-}1)\lfloor N/D \rfloor \;\leq\; n \;\leq\; n/d + (d{-}1)\lceil N/D \rceil$ "Galois property"

$\equiv \quad (d{-}1)\lfloor N/D \rfloor \;\leq\; (d{-}1)n/d \;\leq\; (d{-}1)\lceil N/D \rceil$

$\Leftarrow \quad \lfloor N/D \rfloor \;\leq\; n/d \;\leq\; \lceil N/D \rceil$ "$d \geq 1$ from loop guard [1]"

$\equiv \quad \mathsf{true}$. "Galois property"

[1] Requires extra "housekeeping" invariant $d \geq 0$.