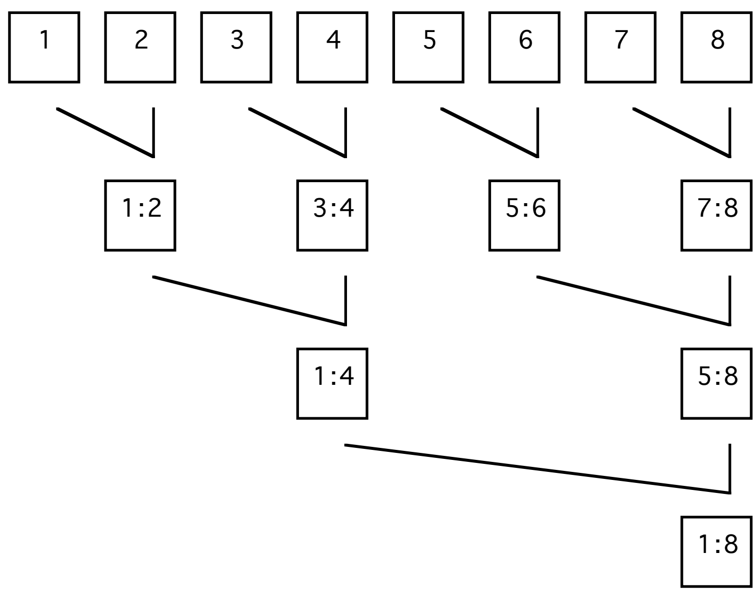
4. Sample Proofs (ch. 3)

Synchronous array summation

- Problem specification
  - Given an array A of size N (some power of 2) compute in logN steps the sum of all its array entries
- Basic idea
  - Sum pair wise (odd-even positions) and place the results in the even position
  - Treat the even positions as a new array and apply the procedure again



- The program

```
Program  Summation
   declare   j : integer
             x : array[1..N] of integer
   initially j,x = 1,A
   assign
   s1     ⟨ ∥ k : 1≤k≤N ∧ k mod (2j) = 0 :: x[k] := x[k] +x[k-j] ⟩
       ∥
   s2     j := 2j  if j<N
end
```

- Helpful definitions

```
pow2(k) ≡ ⟨ ∃ p : p≥0 :: k = 2^p ⟩
sum(i,u) ≡ ⟨ + k : i<k≤u :: A[k] ⟩
node(k,i) ≡ 1≤k≤N ∧ k mod i = 0
-- the nodes of interest to us in phase i = 1, 2, 4, 8
```

- Proof obligations

1. (Sum Completion)

   Initial → Post

   where

   Initial ≡ pow2(N) ∧ j=1 ∧ x=A
   Post ≡ j=N ∧ x[N]=sum(0,N)

2. (Sum Stability)

   stable Post

   Proof: When j=N none of the assignments alter the state.

- Sum Completion proof

2.1 (Phase Invariants)

```
(I1)   inv. pow2(N)
(I2)   inv. pow2(j)
(I3)   inv. 1≤j≤N
(I4)   inv. 〈 ∀ i : node(i,j) :: x[i] = sum(i-j,i) 〉
```

Proof:

```
- initially they all hold
- I1 follows from the assumption that N is constant
- I2 follows from the fact that j is only doubled
- I3 requires to show
    {I1 ∧ I2 ∧ I3 ∧ j<N} j:=2*j {I3}
    pow2(N) ∧ pow2(j) ∧ j≤N ∧ j<N ⇒ 2*j≤N
- I4 requires to show
    {I1 ∧ I2 ∧ I3 ∧ I4} s1 ‖ s2 {I4}
    I1 ∧ I2 ∧ I3 ∧ I4
        ⇒ 〈 ∀ i : node(i,2*j) :: x[i] + x[i-j] = sum(i-2*j,i) 〉
```

2.2 (Sum Completion)

- We select the well-founded metric N/j (goes from N to 1)
- We show that it is well-founded due to I3 above
- We need to show that it decreases (i.e., j increases)

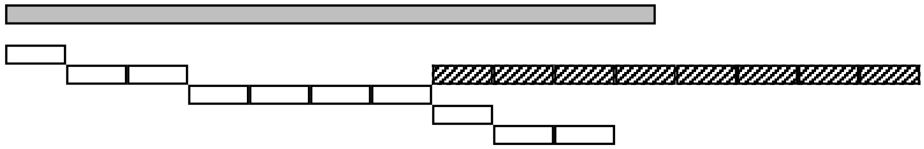
```
    j<N ∧ j=k → j>k
which can be proved from
    j<N ∧ j=k ensures j>k
since the program has one statement which doubles j when j<N
```

Integer division (pg 54)

- Problem specification
  - Given two strictly positive integers M and N
  - Write a program which satisfies the following properties
    (x is the quotient and y is the remainder)

```
true → FP
FP ⇒ (x * N + y = M) ∧ N>y≥0
```

- Basic idea
  - Remove one or more multiples of N from M until no longer possible



- The program

```
Program  Division
    declare    x,y,z,k : integer
    initially x,y,z,k = 0,M,N,1
    assign
    s1      z,k := 2*z, 2*k  if y≥2*z
                 ~ N, 1      if y<2*z
    s2 []   x,y := x+k, y-z  if y≥z
end
```

- Sample execution

x	y	z	k		
	(M)	(N)			
0	17	5	1		
		10	2	y≥2*z	17≥2*5
2	7			y≥z	17≥10
		5	1	y<2*z	7<10
3	2			FP	17=3*5+2

- The proof

1. Compute FP

$$\begin{aligned} FP \equiv\ & (y \geq 2z \Rightarrow z,k = 2z, 2k) \wedge (y<2z \Rightarrow z,k = N,1) \wedge \\ & (y \geq z \Rightarrow x,y = x+k, y-z) \\ \equiv\ & \{\text{using } p \Rightarrow q \equiv \neg p \vee q\} \\ & (y<2z \vee (z=2z \wedge k=2k)) \wedge (y \geq 2z \vee (z=N \wedge k=1)) \wedge \\ & (y<z \vee (x=x+k \wedge y=y-z)) \end{aligned}$$

2. Show $FP \Rightarrow x * N + y = M \wedge N>y\geq 0$

2.1 Find invariant I such that

$$(FP \wedge I) \Rightarrow (x * N + y = M \wedge N>y\geq 0)$$

$I \equiv y\geq 0 \wedge k\geq 1 \wedge z=N*k \wedge (x*N + y = M)$

$$\begin{aligned} I \wedge FP \equiv\ & y\geq 0 \wedge k\geq 1 \wedge z=N*k \wedge x*N + y = M \wedge \\ & (\underline{y<2z} \vee (z=2z \wedge \mathbf{k=2k})) \wedge (\underline{y\geq 2z} \vee (z=N \wedge k=1)) \wedge \\ & (y<z \vee (\mathbf{x=x+k} \wedge y=y-z)) \\ \equiv\ & \{\text{bold expressions are false due to } k\geq 1\text{, underlined are contradictions}) \\ & y\geq 0 \wedge k\geq 1 \wedge z=N*k \wedge x*N + y = M \wedge \\ & (y<2z) \wedge (z=N \wedge k=1) \wedge (y<z) \\ \Rightarrow\ & \{\text{simplification using } k=1 \text{ and } z=N) \\ & N>y\geq 0 \wedge x*N + y = M \end{aligned}$$

2.2 Prove {I} s {I} for statements s1 and s2

```
s1  {I ∧ y≥2z}    z,k := 2z, 2k    {I}
    {I ∧ y<2z}    z,k := N, 1      {I}

s2  {I ∧ y≥z}     x,y := x+k, y-z  {I}
```

```
e.g., proved by
   y≥0 ∧ k≥1 ∧ z=N*k ∧ x*N + y = M ∧ y≥z
   ⇒
   y-z≥0 ∧ k≥1 ∧ z=N*k ∧ (x+k)*N + y-z = M
```

3. Show that true → I ∧ FP

   3.1 Actually, due to I, it is enough to prove true → N>y≥0

   - We introduce a well-founded metric
     (a decreasing function bounded from below)
   - Let's consider (y,z) and the lexicographical order <
   - (y,z) starts as (M,N) and remains positive, actually reaches (remainder, N), and tends to decrease—except for occasional increases in z

   3.2 We must consider three possible situations

```
y≥z       -- y can decrease by s2
y<z ∧ z>N -- z decreases to N
y<z ∧ z≤N -- fixed point is reached (need not consider it)
```

thus we must prove
$(y,z)=(m,n) \wedge y\geq z \rightarrow y<m$ *eventually remainder is established*
$(y,z)=(m,n) \wedge y<z \wedge z>N \rightarrow y=m \wedge z<n$ *z drops once remainder is established*

which by applying the disjunction rule results in
$(y,z)=(m,n) \wedge (y\geq z \vee z>N) \rightarrow (y,z) < (m,n)$

by applying the induction rule, the LHS must eventually become false thus we have
$\neg(y\geq z \vee z>N) \equiv y<z \wedge z\leq N$

3.3 Prove (skipped)
$(y,z)=(m,n) \wedge y<z \wedge z>N \rightarrow y=m \wedge z<n$

3.4 Prove
$(y,z)=(m,n) \wedge y\geq z \rightarrow y<m$

```
we observe that
```
$y=m \wedge y\geq z$ **ensures** $y<m$

```
that is
   {(y,z)=(m,n) ∧ y≥z} x,y := x+k, y-z  if y≥z {y<m}
   and
```
$y=m \wedge y\geq z$ **unless** $y<m$

which can be proven by using the assignment axiom for

a) statement s1 part 1 (guard in bold)
   $y\geq z \wedge y=m \wedge (\mathbf{y\geq 2z}) \Rightarrow (y\geq 2z \wedge y=m) \vee y<m$
b) statement s1 part 2 (guard in bold) using the fact that z≥N
   $y\geq z \wedge y=m \wedge (\mathbf{y<2z}) \Rightarrow (y\geq N \wedge y=m) \vee y<m$
c) statement s2 (guard in bold)
   $y\geq z \wedge y=m \wedge (\mathbf{y\geq z}) \Rightarrow (y-z\geq z \wedge y-z=m) \vee y-z<m$