4/11 Program verification

4/13 Fri.
pm 12:00 ~ 1:00

$(A, \leq)$ poset.

$\forall a, b \in A \ \exists_1$ l.u.b. $\vee$ g.l.b. $\wedge$: lattice

$(A, \vee)$ $(A, \wedge)$ ... algebraic system.

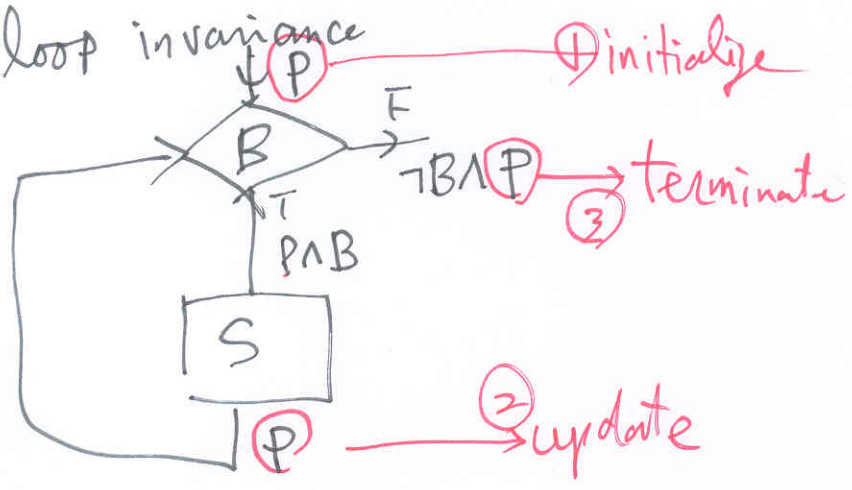
$(A, \oplus)$: alg. system
$\oplus : A \times A \to A$
$\forall a, b \in A$, $a \oplus b \in A$
closed

Ex) $(\mathbb{Z}, <)$ poset $\to$ $(\mathbb{Z}, \max)$ $(\mathbb{Z}, \min)$ alg. system
$(\mathbb{Z}^+, |)$ " $\to$ $(\mathbb{Z}^+, \gcd)$ $(\mathbb{Z}^+, \mathrm{lcm})$ "
$(2^S, \subseteq)$ " $\to$ $(2^S, \cup)$ $(2^S, \cap)$ "

Burble sort $O(n^2)$
Merge sort $O(n \log n)$

Program correctness

loop invariance



loop invariance
p.

~~for~~ $S := 0$, $i = 1$
do $i \leq 100$ do $\to$ $S := S + i$, $i := i + 1$ od

i: induced variable

$p = \left(\sum_{k=1}^{i} k = S \right)$ loop invariance

Pascal for i := 1 to 100 do ...
C for (i=1; i≤100; i++) ~

A discipline of Programming
E. D. Dijkstra
Prentice-Hall
(1972?)

3) Second example

set $A = \{x \in \bar{U} \mid p(x)\}$

$W := \emptyset$

repeate

$W := W \cup \{a\}$ $(a \in A ?)$

until no more

$(W = A)$ ← fixedpoint!

$W \subseteq A$ loop invariance

if $k<a$ do

$x := \eta(x+m);\ k{+}{+}$ X → do $k<a$ → $x := x+\eta;\ k{+}{+}$ od

od