## Seminar Objectives

- correctness

## Theoretical aspects

- Floyd's method to demonstrate program correctness
- Partial correctness
- Termination of a program
- References: [Frentiu] chapter 1,2 , [Morgan]

Floyd's method to demonstrate program correctness

- Partial correctness
    - Cutting points are chosen inside the algorithm
        - 1 point at the beginning of the algorithm and 1 point at the end;
        - At least 1 point for each *while* statement.
    - For each cutting point an assertion (invariant predicate) is chosen.
        - Entry point - ϕ(X);
        - Ending point – ψ(X,Z);
    - Construction of the verification conditions
        - Path from i to j = $\alpha$ ;
        - $P_i$ *and* $P_j$ - assertions in *i* and *j*;
        - $R_\alpha(X,Y)$ - predicate that gives the condition for path $\alpha$ ;
        - $r_\alpha(X,Y)$ - function that gives the transformations of the variables *Y* from path $\alpha$ ;
        - $\forall X \forall Y (P_i(X,Y) \wedge R_\alpha(X,Y) \to P_j(X, r_\alpha(X, Y)))$.
    - *Theorem:* If all the verification conditions are true then P is partial correct.
- Termination of a program
    - Well-ordered set – partial ordered and doesn't have an infinite decreasing sequence.
    - To demonstrate that some termination conditions hold: passing from one cutting point to another the values of some functions in the well-ordered set decrease
    - In point *i* a function is chosen $u_i : D_X \times D_Y \to M$ and the termination condition on $\alpha$ is:

$$\forall X \forall Y (\varphi(X) \wedge R_\alpha(X,Y) \to (u_i(X,Y) > u_j(X, r_\alpha(X,Y)))).$$

- If partial correctness was demonstrated then the termination condition can be:

$$\forall X \forall Y (P_i(X,Y) \wedge R_\alpha(X,Y) \to (u_i(X,Y) > u_j(X, r_\alpha(X,Y)))).$$

- *Theorem:* If all the termination conditions hold then the program P terminates/ends.

[Frentiu] M. Frentiu, Verificarea si validarea sistemelor soft, Presa Universitara Clujeana, 2010

[Morgan] C. Morgan, Programming from specification, Prentice Hall International, 1998

## Assignment

Demonstrate using Floyd's method partial correctness and termination for the following subalgorithm:

- Search
- cmmdc