Compositional methods of Program Verification

Mykola (Nikolaj) S. Nikitchenko

Taras Shevchenko National University of Kyiv

Introduction

- From formal program models (algebras) to program logics and then to program verification
- Floyd-Hoare logic
- Validity of Floyd-Hoare logic

EL syntax: "mathematical" notation

prg::= begin *c* end

c::= *x*:=*a* | *c*1 ; *c*2| if *b* then *c*1 else *c*2 |while *b* do *c* |
begin *c* end | skip

a::= *n* | *x* | *a*1 + *a*2 | *a*1 – *a*2 | *a*1 * *a*2 | (*a*)

b::=*a*1= *a*2 |*a*1>*a*2 | *b*1∨*b*2 |¬*b* | (*b*),

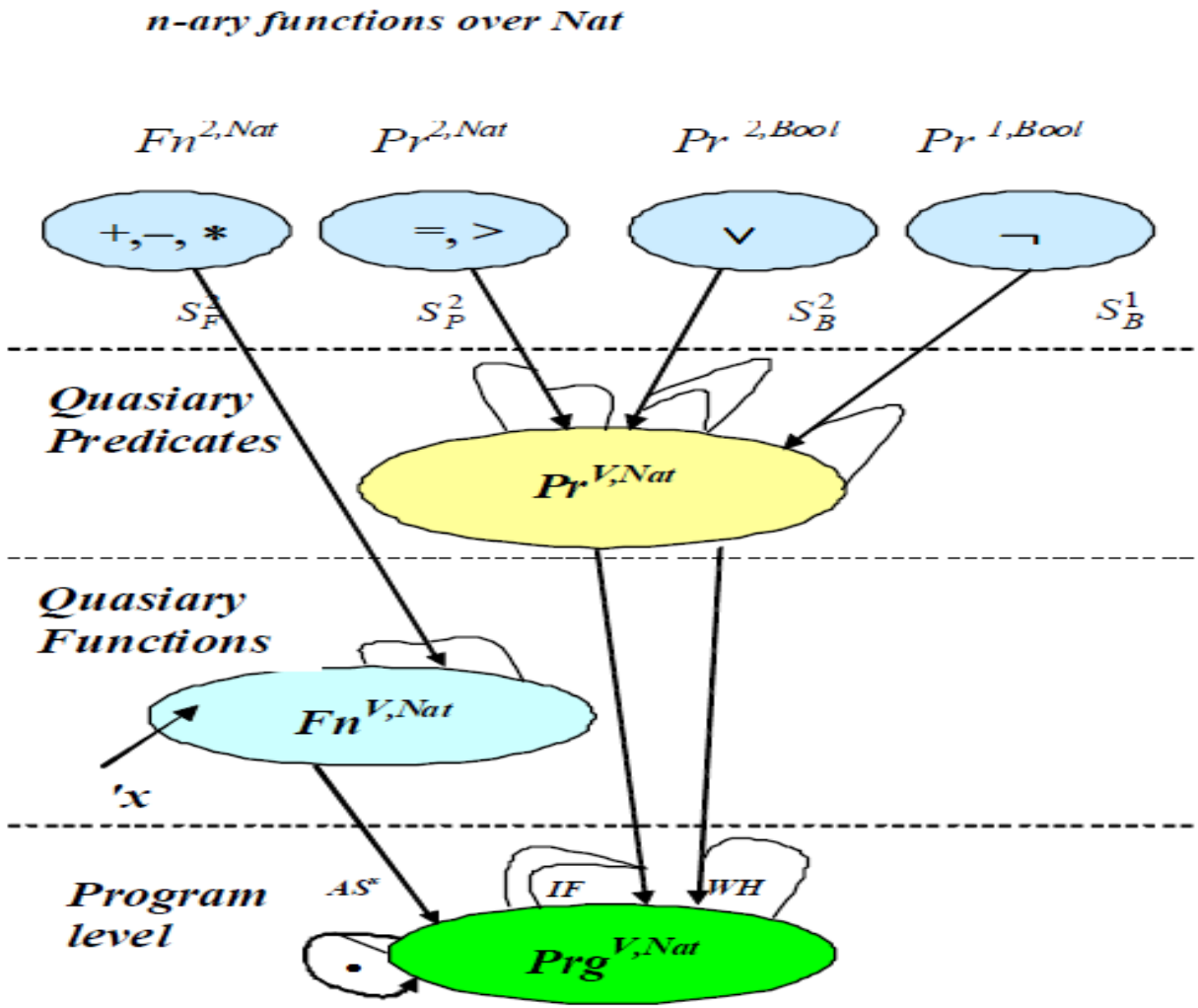
where:

- *n* ranges over natural numbers *Nat*={0, 1, 2, …},
- *x* ranges over variables (names) *V*={*M*, *N*, …},
- *a* ranges over arithmetic expressions *Aexpr*,
- *b* ranges over Boolean expressions *Bexpr*,
- *c* ranges over commands (statements) (programs) *Cmn*,
- *prg* ranges over programs *Prg*.

Example 1: GCD

```
begin
   while ¬(M=N) do
                  if M>N then
                                 M:=M–N
                  else
                                 N:=N–M
end
```

Program algebra with *n*-ary functions



GCD semantics

The term for EL program GCD:

$$WH(\, S^1_B\,(\neg, S^2_P\ \ (=, 'M, 'N)),$$

$$IF(\ \ S^2_P\,(>,'M,'N),$$

$$AS^M(\, S^2_F\,(-, 'M, 'N)),$$

$$AS^M(\, S^2_F\,(-, 'N, 'M))))).$$

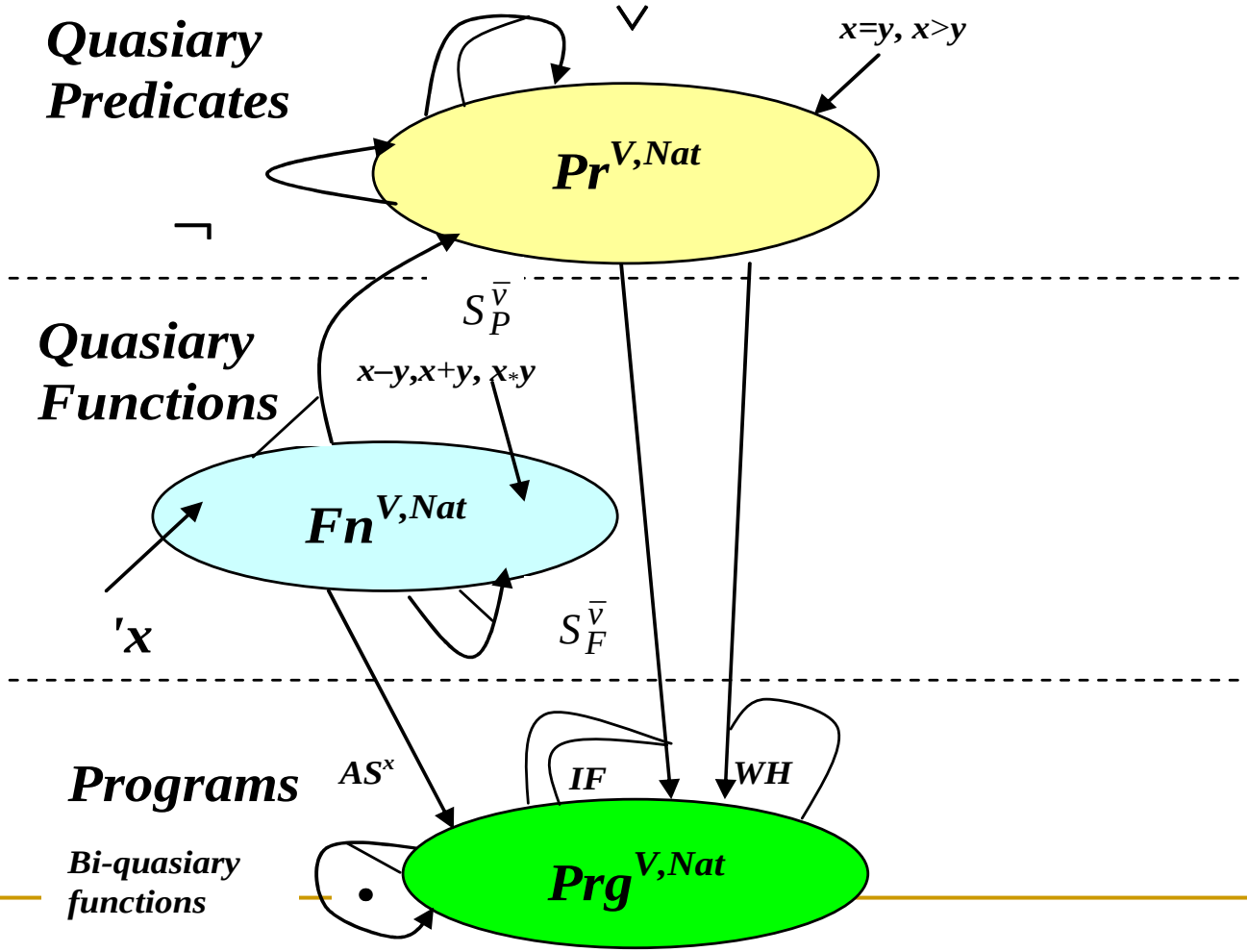
The second phase of program algebra development

to make the algebra simpler

- exclude the classes of *n*-ary functions and predicates,
- concentrate on logical symbols that are interpreted as compositions over nominative carriers

$$Fn^{V,Nat}, Pr^{V,Nat}, Prg^{V,Nat}.$$

Program algebra over nominative mapping (with constants)



GCD

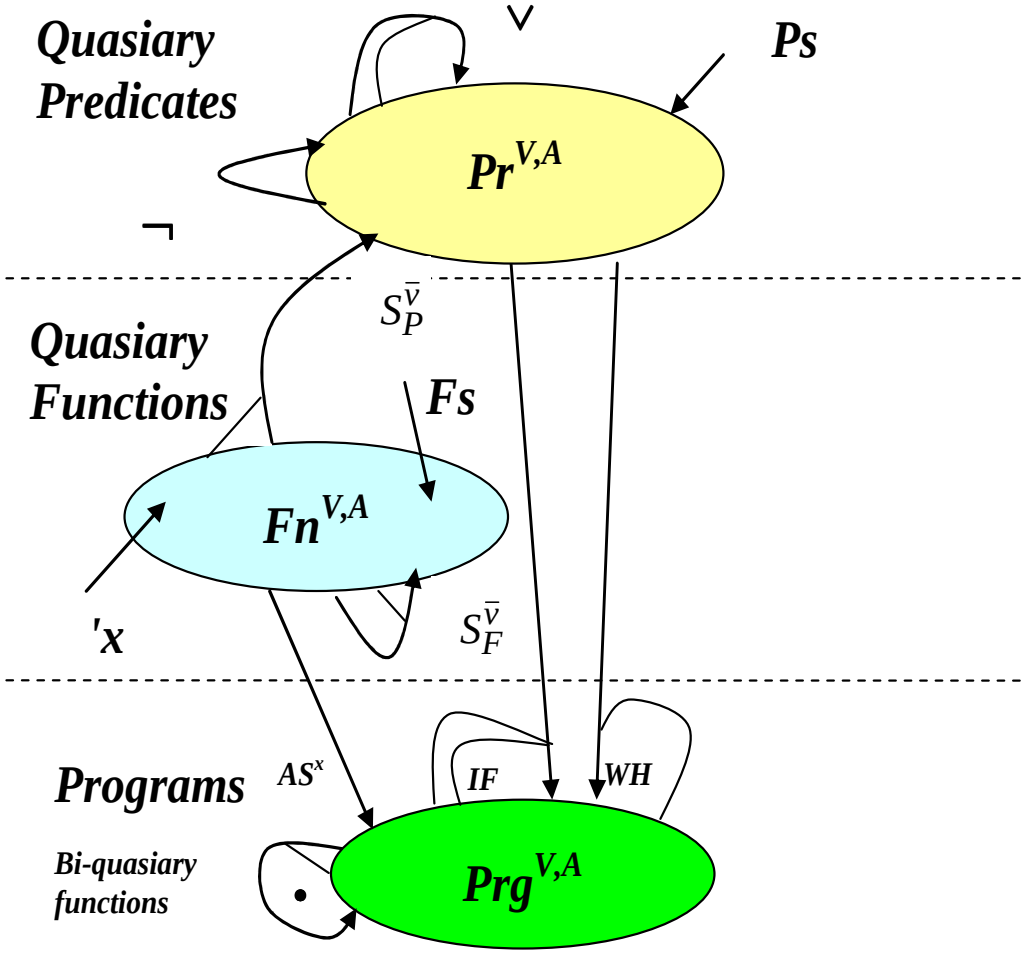
"Sugared" term:

$$WH\,(\ \neg\,(\boldsymbol{M}{=}\boldsymbol{N}),\ IF(\boldsymbol{M}{>}\boldsymbol{N},\ AS^{M}(\boldsymbol{M}{-}\boldsymbol{N})),\ AS^{M}(\boldsymbol{N}{-}\boldsymbol{M}))).$$

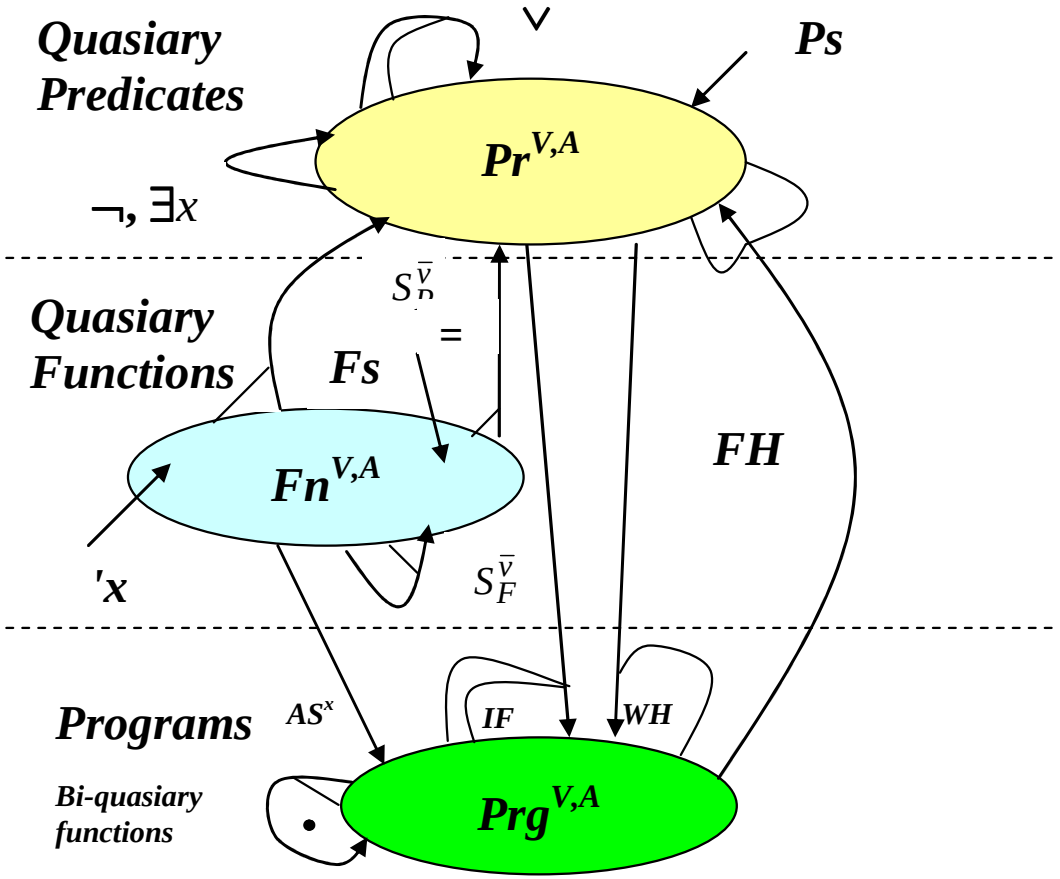
cf. Term in APn

$$WH(S^{1}_{B}(\neg, S^{2}_{P}(=, 'M, 'N)),\ IF(\ S^{2}_{P}(>,'M,'N),\ AS^{M}(S^{2}_{F}(-, 'M, 'N)),\ AS^{M}(S^{2}_{F}(-, 'N, 'M)))).$$

Class of Program Algebras



Composition-Nominative Program Algebra of Floyd-Hoare type



Partial correctness: example 1 (1/2)

$STR^{M,N} =$

$WH(S^1_B(\neg, S^2_P(=,'M,'N)),$

$IF(S^2_P(>,'M,'N), AS^M(S^2_F(-,'M,'N)), AS^N(S^2_F(-,'N,'M))))$

Theorem 1 (partial correctness of $STR^{M,N}$).
Let a state st be such that $'M(st)=m$, $'N(st)=n$ (natural numbers $m, n>0$).
If $STR^{M,N}(st)\downarrow=str$, then $'M(str)='N(str)=gcd(m, n)$.

Proof (general schema without details).
Induction on k: the number of loop iterations (denoted $\downarrow^k$).
Induction statement:

$$STR^{M,N}(st)\downarrow^k=str \Rightarrow 'M(str)='N(str)=gcd(m, n).$$

Partial correctness: example 1 (2/2)

Base of induction (k=0).

In this case $S^1_B(\neg, S^2_P(=,'M,'N))(st)=F$. From this follows that $m=n=gcd(m, n)$.

Step of induction (*for* k+1). Let $STR^{M,N}(st)\downarrow^{k+1}=str$.

From this follows that $S^1_B(\neg, S^2_P(=,'M,'N))(st)=T$. Hence, $m\neq n$.

Let $IF(S^2_P(>,'M,'N), AS^M(S^2_F(-,'M,'N)), AS^N(S^2_F(-,'N,'M)))(st)=st'$.

Evaluating both cases of conditional operator we obtain:

$AS^M(S^2_F(-,'M,'N))(st)= st\nabla[M\rightarrow m-n]$ $(m>n)$

$AS^N(S^2_F(-,'N,'M))(st)= st\nabla[N\rightarrow n-m]$ $(n>m)$.

Since $gcd(m-n\ n)= gcd(m, n)$ for $m>n$ and $gcd(m-n, n)= gcd(m, n-m)$ for $n>m$ (recall the theory of natural numbers) we have that $gcd('M(st'), 'N(st'))=gcd(m, n)$.

By inductive hypothesis $'M(str)= 'N(str)= gcd('M(st'), 'N(st'))=gcd(m, n)$.

Total correctness: example 1

Termination of the program is based on the fact that $n+m$
is decreasing for each loop execution
until these numbers become equal
(details of this proof are omitted).

So, the following statement is valid:

Theorem 2. $STR^{M,N}$ is totally correct.

Floyd-Hoare Logic

Let A be a program algebra (with total predicates),

LP be the language of this algebra.

Assertions (formulas) of Floyd-Hoare logics: $\{P\}fs\{Q\}$,

- P is precondition
- Q is postcondition
- fs is program term

Formula $\{P\}\ fs\ \{Q\}$ is partially correct w.r.t. A

(is denoted $A \models \{P\}fs\{Q\}$*)*, if for any st such that

$$P_A(st)=T,\ fs_A(st)\downarrow=st' \Rightarrow Q_A(st')\downarrow= T.$$

In the sequel index A is omitted.

Examples of assertions

- $\{M>0 \wedge N>0\}\ AS^{M}(M–N)\ \{M=N\}$

- $\{M>0 \wedge N>0\}$

  $WH(M\neq N,\ IF(M>N,\ AS^{M}(M–N),\ AS^{N}(N–M)))$

  $\{M=N\}$

Floyd-Hoare rules for program algebra with total predicates

Inference rule	Rule #
$\{S^{\lfloor x \rfloor}(P, fa)\}\ AS^{x}(fa)\ \{P\}$	*Ax_AS*
$\{P\} id \{P\}$	*Ax_id*
$\dfrac{\{P\} f \{Q\}, \{Q\} g \{R\}}{\{P\}\ f \bullet g\ \{R\}}$	*Ax_SEQ*
$\dfrac{\{fb \wedge P\} f \{Q\}, \{\neg fb \wedge P\} g \{Q\}}{\{P\} IF(fb, f, g) \{Q\}}$	*Ax_IF*
$\dfrac{\{fb \wedge P\}\ fs \{P\}}{\{P\} WH(fb, fs) \{\neg fb \wedge P\}}$	*Ax_WH*
$\dfrac{\{P'\}\ fs \{Q'\}}{\{P\}\ fs \{Q\}}$, if $P \Rightarrow P'$, $Q' \Rightarrow Q$	*Ax_CONS*

Example: $GCD^{M,N}$ (1/6)

Two "logical" variables X and Y are introduced.
They do not change their meanings.

States are of the form $[X\mapsto x,\ Y\mapsto y,\ M\mapsto m,\ N\mapsto n]$
(x, y, m, n – natural numbers).

In the initial state $x=m$, $y=n$.

Correctness statement $gcd(X,Y)=gcd(M,N)$.

Example: $GCD^{M,N}$ (2 /6)

Then we make "sugaring" of the term:

$M–N =_{def} S^2_{\bar{P}}(–,'M,'N)$, $\quad N–M =_{def} S^2_{\bar{P}}(–,'N,'M)$,

$M>N =_{def} S^2_{\bar{P}}(>,'M,'N)$, $\quad \neg(M=N) =_{def} S^1_B(\neg, S^2_{\bar{P}}(=,'M,'N))$.

Thus, instead of

$WH(S^1_B(\neg, S^2_{\bar{P}}(=,'M,'N)), IF(S^2_{\bar{P}}(>,'M,'N),$

$AS^M(S^2_{\bar{F}}(–,'M,'N)), AS^N(S^2_{\bar{F}}(–,'N,'M))))$

we get

$WH(\neg(M=N), IF(M>N, AS^M(M–N), AS^N(N–M)))$

Example: $GCD^{M,N}$ (3 /6)

Let

- $P =_{def} gcd(X,Y)=gcd(M,N)$.
- $P1 =_{def} S^{[M]}(P, M–N)$.
- $P2 =_{def} S^{[N]}(P, N–M)$.

Then by *Ax_AS* we have that $\vdash \{S^{[M]}(P, M–N)\}\ AS^{M}(M–N)\{P\}$.

By *Ax_CONS* we have $\vdash \{(M>N) \wedge S^{[M]}(P, M–N)\}\ AS^{M}(M–N)\{P\}$.

Here we need to prove $(M>N) \wedge S^{[M]}(P, M–N) \Rightarrow S^{[M]}(P, M–N)$.

To prove this we use “semantic” reasoning. It means that we prove validity of the above formula.

Example: $GCD^{M,N}$ (4 /6)

Then again by *Ax_CONS* using
$(M>N)\wedge P \Rightarrow (M>N)\wedge\{S^{[M]}(P, M-N)\}$
we obtain $\vdash \{(M>N)\wedge P\}\ AS^{M}(M-N)\{P\}$.

Similarly, we obtain $\vdash \{\neg(M>N)\wedge P\}\ AS^{N}(N-M)\{P\}$.

By *Ax_IF* we get
$\vdash \{P\}\ IF(M>N, AS^{M}(M-N), AS^{N}(N-M))\ \{P\}$.

By *Ax_CONS* we get
$\vdash \{(\neg(M=N))\wedge P\}\ IF(M>N, AS^{M}(M-N), AS^{N}(N-M))\ \{P\}$.

Example: $GCD^{M,N}$ (5 /6)

By Ax_WH we get

$\{P\}\ WH(\neg(M=N),\ IF(M>N,\ AS^{M}(M-N),\ AS^{N}(N-M)))\ \{P\wedge\neg\ (\neg(M=N))\}.$

Proving $(X=M\wedge Y=N) \Rightarrow P$ and

$P\wedge\neg\ (\neg(M=N)) \Rightarrow (M=N)\ \wedge gcd(X,Y)=M$

and using Ax_CONS we get

$\vdash\{(X=M\wedge Y=N)\}\ WH(\neg(M=N),$

$IF(M>N,\ AS^{M}(M-N),\ AS^{N}(N-M)))\ \{(M=N)\ \wedge gcd(X,Y)=M\}.$

Example: $GCD^{M,N}$ (6 /6)

$$\frac{\{S^{[M]}(P, M-N)\}\ AS^{M}(M-N)\{P\}}{} \qquad \frac{\{S^{[N]}(P, N-M)\}\ AS^{N}(N-M)\{P\}}{} \qquad Ax\_AS$$

$$\frac{\{(M>N) \wedge S^{[M]}(P, M-N)\}\ AS^{M}(M-N)\{P\}}{} \qquad \frac{\{\neg(M>N) \wedge S^{[N]}(P, N-M)\}\ AS^{N}(N-M)\{P\}}{} \qquad Ax\_CONS$$

$$\frac{\{(M>N) \wedge P\}\ AS^{M}(M-N)\{P\}}{} \qquad \frac{\{\neg(M>N) \wedge P\}\ AS^{M}(N-M)\{P\}}{} \qquad Ax\_CONS$$

$$\frac{\{P\}\ IF(M>N, AS^{M}(M-N), AS^{N}(N-M))\ \{P\}}{} \qquad Ax\_IF$$

$$\frac{\{(\neg(M=N)) \wedge P\}\ IF(M>N, AS^{M}(M-N), AS^{N}(N-M))\{P\}}{} \qquad Ax\_CONS$$

$$\frac{\{P\}\ WH(\neg(M=N), IF(M>N, AS^{M}(M-N), AS^{N}(N-M)))\ \{P \wedge \neg(\neg(M=N))\}}{} \qquad Ax\_WH$$

$$\frac{\{(X=M \wedge Y=N)\}\ WH(\neg(M=N), IF(M>N, AS^{M}(M-N), AS^{N}(N-M)))\ \{(M=N) \wedge gcd(X,Y)=M\}}{} \qquad Ax\_CONS$$

Validity of Floyd-Hoare Logic (1/7)

Theorem (validity of Floyd-Hoare logic):

$$\vdash \{P1\}\, fs\, \{P2\} \Rightarrow \models \{P1\}\, fs\, \{P2\}\ .$$

Proof. Induction of the shape of a derivation tree.

Base of induction.

1. $fs = AS^{x}(fa)$. hence $\{P1\}\, fs\, \{P2\}$ is $\{S^{[x]}(P, fa)\}\, AS^{x}(fa)\, \{P\}$.

Let $st \in State$ and $S^{[x]}(P, fa)(st)\downarrow = true$, $AS^{x}(fa)\ (st)\downarrow = st'$, and $P(st')\downarrow$.

We should prove that $P(st')\downarrow = true$. Since $fa(st)$ is defined

then $S^{[x]}(P, fa)(st)\downarrow = P(st\nabla[x \rightarrow fa(st)]) = true$,

due to the second condition

$st' = As^{x}(fa)\ (st) = st\nabla[x \rightarrow fa(st)]$, so, $P(st')\downarrow = true$.

2. $fs = id$. Then $\{P1\}\, fs\, \{P2\}$ is $\{P\} id \{P\}$.

Validity of Floyd-Hoare Logic (2/7)

Step of induction.

All cases of derivation steps of $\{P1\}\ fs\ \{P2\}$ must be considered.

1. $\{P1\}\ fs\ \{P2\}$ has the form $\{P\}f \bullet g\{R\}$ $\{P\}f \bullet g\{R\}$

and was derived by the rule $\dfrac{\{P\}f\{Q\}, \{Q\}g\{R\}}{\{P\}f \bullet g\{R\}}$.

Let $P(st)\downarrow = true$, $f \bullet g(st)\downarrow = st'$, and $R(st')\downarrow$.

A state st'' exists such that $f(st)\downarrow = st''$, $g(st'')\downarrow = st'$.

By induction hypothesis, $\models \{P\}fs\{Q\}$.

It means that $Q(st'')\downarrow = true$. Then, by induction hypothesis, $\models \{Q\}fs\{R\}$.

Thus, $R(st')\downarrow = true$.

Validity of Floyd-Hoare Logic (3/7)

2. $\{P1\}\ fs\ \{P2\}$ has the form $\{P\}IF(fb, f, g)\{Q\}$

and was derived by the rule

$$\frac{\{fb \wedge P\}f\{Q\}, \{\neg fb \wedge P\}g\{Q\}}{\{P\}IF(fb, f, g)\{Q\}}.$$

Let st be such that $P(st)\downarrow = true$, $IF(fb, f, g)(st)\downarrow = st'$, and $Q(st')\downarrow$.

Since $IF(fb, f, g)(st)$ is defined follows that $fb(st)$ is defined.

There are two cases: $fb(st)\downarrow = true$ or $f(st)\downarrow = false$.

For the first case $f(st)\downarrow = st'$. By induction hypothesis

$\models \{fb \wedge P\}f\{Q\}$ and $\models \{\neg fb \wedge P\}g\{Q\}$.

Validity of Floyd-Hoare Logic (4/7)

Since $P(st)\downarrow=true$ and $fb(st)\downarrow=true$, we have $fb \wedge P(st)\downarrow=true$.

Also we have $f(st)\downarrow=st'$. It means $Q(st')\downarrow=true$.

Thus $\{P\}IF(fb, f, g)\{Q\}$ is valid.

Similarly the second case is considered.

Validity of Floyd-Hoare Logic (5/7)

3. $\{P1\}\ fs\ \{P2\}$ has the form $\{P\}WH(fb, fs)\{\neg b \wedge P\}$

and was derived by the rule $\dfrac{\{b \wedge P\}\, fs\, \{P\}}{\{P\}WH(fb, fs)\{\neg b \wedge P\}}$.

Let st be such that $P(st)\downarrow = true$, $WH(fb, fs)(st)\downarrow = st'$, and $P(st')\downarrow$.

Since $WH(fb, fs)(st)$ is defined then: $st_0 = st$, $st_1 = fs(st_0)$,

$st_2 = fs(st_1)$, …, $st_n = fs(st_{n-1})$, and $fb(st_0) = true$, $fb(st_1) = true$, …, $fb(st_{n-1}) = true$, $fb(st_n) = false$, $st_n = st'$.

Two cases: $n=0$ and $n>0$.

Validity of Floyd-Hoare Logic (6/7)

1) $fb(st)\downarrow=false$, $WH(fb, fs)(st)\downarrow=st$, therefore $(\neg b \wedge P)(st)\downarrow=true$.

Thus, $\{P\}WH(fb, fs)\{\neg b \wedge P\}$ is valid.

2) $fb(st)\downarrow=true$, $fs(st_0)\downarrow=st_1$. By induction hypothesis $\{b \wedge P\}\, fs\{P\}$

is valid, therefore $P(st_1)\downarrow=true$. Then we use induction by n and prove that

$P(st_1)\downarrow=true, \ldots, P(st_n)\downarrow=true$.

Thus, $(\neg b \wedge P)(st_n)\downarrow=(\neg b \wedge P)(st')\downarrow=true$ and $\{P\}WH(fb, fs)\{\neg b \wedge P\}$ is valid.

Validity of Floyd-Hoare Logic (7/7)

4. $\{P1\}\ fs\ \{P2\}$ has the form $\{P\}\,fs\,\{Q\}$ and was derived by *Ax_CONS*

of the form $\dfrac{\{P'\}\,fs\,\{Q'\}}{\{P\}\,fs\,\{Q\}}$, if $P \Rightarrow P'$, $Q' \Rightarrow Q$

Let st be such that $P(st)\downarrow = true$, $fs(st)\downarrow = st'$, and $Q(st')\downarrow$.

Since $P \Rightarrow P'$ we have that $P'(st)\downarrow = true$. By induction hypothesis,

$\{P'\}\,fs\,\{Q'\}$ is valid, therefore $Q'(st')\downarrow = true$.

Since $Q' \Rightarrow Q$ we have $Q(st')\downarrow = true$. Thus, $\{P\}\,fs\,\{Q\}$ is valid.

Example 2 (1/12)

Example 2:

Problem: evaluate $r = 1^2+2^2+\ldots+n^2$.

We write program with variables *R*, *N*, *I*:

```
begin
     R:=0;
     I:=0;
     while I<N do
               begin
                    I:=I+1;
                    R:=R+I*I
               end
end
```

Example 2 (2/12)

Important note. To simplify notation we will use "sugared" terms. It means that all "traditional" arithmetical and Boolean expressions are considered as terms of (semantic) program algebra. Thus, such expressions represent quasiary functions and predicates. If required, such terms may be rewritten using n-ary functions and predicates and superpositions into n-are mappings. Thus, the sugared term for our program is as follows:

$$AS^R(\overline{0}) \bullet AS^I(\overline{0}) \bullet WH(I<N.\, AS^I(I+1) \bullet AS^R(R+I*I))$$

Example 2 (3/12)

We chose as a loop invariant the following predicate:

$$P =_{def} ((R = 1^2 + 2^2 + \ldots + I^2) \& (I \leq N))$$

Later we prove that it is indeed a loop invariant.

This invariant is considered as a quasiary predicate!
Thus, it should be evaluated on a state to obtain a Boolean value as result.
On a state $st = [N \rightarrow n, R \rightarrow r, I \rightarrow i]$ this predicate is evaluated in the following way:

$$P(st) = ((R = 1^2 + 2^2 + \ldots + I^2) \& (I \leq N))\ (st) = ((r = 1^2 + 2^2 + \ldots + i^2) \& (i \leq n)).$$

Example 2 (4/12)

Important note. Here notation is simplified and we denote by the same signs (&, ∨, ¬) both compositions of quasiary predicates and functions with Boolean values. For example, in the expression $((R=1^2+2^2+\ldots+I^2)\&(I\leq N))$ the sign & is considered as composition of quasiary predicates, but in the expression $((r=1^2+2^2+\ldots+i^2)\&(i\leq n))$ this sign denotes a Boolean function. The same concerns the equality sign =, but additionally this sign is also used as meta-equality in term transformations.

Example 2 (5/12)

Now we start derivation.

By *Ax_AS* we have that

$$\vdash \{S^{[R]}(P, R+I*I)\}\ AS^{R}(R+I*I)\{P\}.$$

We use *Ax_AS* once more and obtain

$$\vdash \{\ S^{[I]}\ (S^{[R]}(P, R+I*I), I+1)\}\ AS^{I}(I+1)\{S^{[R]}(P, R+I*I)\}$$

By *Ax_SEQ* we get

$$\vdash \{\ S^{[I]}\ (S^{[R]}(P, R+I*I), I+1)\}\ \ AS^{I}(I+1) \bullet AS^{R}(R+I*I)\ \{\ P\}$$

To use *Ax_CONS* we have to prove the following implication:

$$(I<N)\&\ P \Rightarrow S^{[I]}\ (S^{[R]}(P, R+I*I), I+1)$$

Example 2 (6/12)

To prove it we use *semantic reasoning*.

This means that we demonstrate validity of this implication in then following way:

on each state $st=[N\rightarrow n, R\rightarrow r, I\rightarrow i]$ such that $(I<N)\& P(st)=T$

we should show that $S^{[I]}(S^{[R]}(P, R+I*I), I+1)(st)=T$.

To do this, we evaluate

$((I<N)\& P)(st)= ((I<N)\& P)([N\rightarrow n, R\rightarrow r, I\rightarrow i])=$

$=(i<n)\& (r=1^2+2^2+\ldots+i^2)\&(i\leq n)=$

$=(i<n)\& (r=1^2+2^2+\ldots+i^2)=$

$=T$

Example 2 (7/12)

Then we evaluate

$(S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1))(st) =$

$=S^{[R]}(P,\ R+I*I)(st\nabla[I\rightarrow(I+1)(st)])=$

$=P((st\nabla[I\rightarrow(I+1)(st)])\ \nabla[R\rightarrow(R+I*I)(\ st\nabla[I\rightarrow(I+1)(st)])])=$

$= P((st\nabla[I\rightarrow(i+1)])\ \nabla[R\rightarrow(R+I*I)(\ st\nabla[I\rightarrow(i+1)])=$

$= P([N\rightarrow n,\ R\rightarrow r,\ I\rightarrow i+1])\ \nabla[R\rightarrow(R+I*I)([N\rightarrow n,\ R\rightarrow r,\ I\rightarrow i+1])])=$

$= P([N\rightarrow n,\ R\rightarrow r,\ I\rightarrow i+1])\ \nabla[R\rightarrow(\ r+(i+1)*\ (i+1))])=$

$= P([N\rightarrow n,\ I\rightarrow i+1,\ R\rightarrow(\ r+(i+1)*\ (i+1))])=$

$= ((\ r+(i+1)^2)=1^2+2^2+\ldots+i^2+(i+1)^2)\ \&(i+1\leq n)$

Example 2 (8/12)

This evaluates to T because we know that
$(i<n)\&\ (r=1^2+2^2+\ldots+i^2)=T$.
Thus, our implication is proved and we can use *Ax_CONS* to obtain

$$\vdash\{\ (I<N)\&\ P\}\ \ AS^I(I+1)\bullet AS^R(R+I*I)\ \{\ P\}$$

By *Ax_WH* we get

$$\vdash\{P\}\ WH(I<N,\ AS^I(I+1)\bullet AS^R(R+I*I))\ \{\ (\neg(I<N))\&\ P\}$$

Example 2 (9/12)

By Ax_AS we have

$\vdash\{S^{[I]}(P,\ \overline{0})\}\ AS^{I}(\overline{0})\{P\}$

Again by Ax_AS we have

$\vdash\{S^{[R]}(S^{[I]}(P,\ \overline{0}),\ \overline{0})\}\ AS^{R}(\overline{0})\{S^{[I]}(P,\ \overline{0})\}$

By Ax_SEQ we get

$\vdash\{S^{[R]}(S^{[I]}(P,\ \overline{0}),\ \overline{0})\}AS^{R}(\overline{0})\bullet AS^{I}(\overline{0})\{P\}$

By Ax_SEQ we get

$\vdash\{S^{[R]}(S^{[I]}(P,\overline{0}),\overline{0})\}AS^{R}(\overline{0})\bullet AS^{I}(\overline{0})\bullet WH(I<N,\ AS^{I}(I+1)\bullet AS^{R}(R+I*I))\{\neg(I<N)\ \&P\}$

Let us prove that

$(0\le N)\Rightarrow S^{[R]}(S^{[I]}(P,\ \overline{0}),\ \overline{0})$

We will use again semantic reasoning.

Consider arbitrary state $stin=[N\rightarrow n]$. Let

$(0\le N)(stin)=T$. It means that $0\le n$.

Example 2 (10/12)

Evaluate

$$S^{[R]}(S^{[I]}(P,\ \overline{0}),\ \overline{0})(stin) = S^{[I]}(P,\ \overline{0})(stin\ \nabla[\ R \rightarrow \overline{0}\ (stin)]) =$$

$$= S^{[I]}(P,\ \overline{0})(stin\ \nabla[\ R \rightarrow 0]) = S^{[I]}(P,\ \overline{0})([\ N \rightarrow n,\ R \rightarrow 0]) =$$

$$= P([\ N \rightarrow n,\ R \rightarrow 0]\ \nabla[\ I \rightarrow \overline{0}\ ([\ N \rightarrow n,\ R \rightarrow 0])) =$$

$$= P([\ N \rightarrow n,\ R \rightarrow 0,\ I \rightarrow 0]) = ((0 = 0)\&(\ 0 \leq n))$$

The last expression evaluates to T, thus, implication is valid.

By *Ax_CONS* we get

$$\vdash \{(0 \leq N)\} AS^{R}(\overline{0}) \bullet AS^{I}(\overline{0}) \bullet WH(I < N,\ AS^{I}(I+1) \bullet AS^{R}(R + I*I)) \{\neg(I < N)\ \&P\}$$

Example 2 (11/12)

At last, we prove by semantic reasoning an implication

$\neg(I<N)\ \&P \Rightarrow R=1^2+2^2+\ldots+N^2$

Consider an arbitrary state $st=[N\rightarrow n, R\rightarrow r, I\rightarrow i]$.

Let $(\neg(I<N)\ \&P)(st)=T$. It means that

$(\neg(i<n)\ \&(r=1^2+2^2+\ldots+i^2)\&(i\leq n)=$

$=(i\geq n)\ \&(r=1^2+2^2+\ldots+i^2)\&(i\leq n)=$

$=((i=n)\ \&(r=1^2+2^2+\ldots+i^2))=(r=1^2+2^2+\ldots+n^2)=T$

From this follows that

$(R=1^2+2^2+\ldots+N^2)\ (st)=(r=1^2+2^2+\ldots+n^2)=T$

By *Ax_CONS* we get the final conclusion:

$\vdash\{(0\leq N)\}AS^R(\overline{0})\bullet AS^I(\overline{0})\bullet WH(I<N, AS^I(I+1)\bullet AS^R(R+I*I))\{R=1^2+2^2+\ldots+N^2\}$

Example 2 (12/12)

The derivation tree is as follows ($P=_{def}((R=1^2+2^2+\ldots+I^2)\&(I\leq N))$):

$$\frac{\{S^{[R]}(P,\ R+I*I)\}\ AS^R(R+I*I)\{P\}}{\{\ S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)\}\ AS^I(I+1)\{S^{[R]}(P,\ R+I*I)\}}\ Ax\_AS$$

$$\frac{\{\ S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)\}\ AS^I(I+1)\{S^{[R]}(P,\ R+I*I)\}}{\{\ S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)\}\ AS^I(I+1)\bullet AS^R(R+I*I)\ \{\ P\}}\ Ax\_AS$$

$$\frac{\{\ S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)\}\ AS^I(I+1)\bullet AS^R(R+I*I)\ \{\ P\}}{\{\ (I<N)\&\ P\}\ AS^I(I+1)\bullet AS^R(R+I*I)\ \{\ P\}}\ Ax\_SEQ$$

$$\frac{\{\ (I<N)\&\ P\}\ AS^I(I+1)\bullet AS^R(R+I*I)\ \{\ P\}}{\text{under implication } (I<N)\&\ P\Rightarrow S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)}\ Ax\_CONS$$

$$\frac{\text{under implication } (I<N)\&\ P\Rightarrow S^{[I]}\ (S^{[R]}(P,\ R+I*I),\ I+1)}{\{P\}\ WH(I<N,\ AS^I(I+1)\bullet AS^R(R+I*I))\ \{\ (\neg(I<N))\&\ P\}}\ Ax\_WH$$

$$\{S^{[I]}\ (P,\ \overline{0})\}\ AS^I(\overline{0})\{P\}\ Ax\_AS$$

$$\{S^{[R]}\ (S^{[I]}\ (P,\ \overline{0}),\ \overline{0})\}AS^R(\overline{0})\bullet AS^I(\overline{0})\{P\}\ Ax\_AS$$

$$\{S^{[R]}\ (S^{[I]}\ (P,\ \overline{0}),\ \overline{0})\}AS^R(\overline{0})\bullet AS^I(\overline{0})\bullet WH(I<N,\ AS^I(I+1)\bullet AS^R(R+I*I))\{\neg(I<N)\ \&P\}\ Ax\_SEQ$$

$$\{(0\leq N)\}AS^R(\overline{0})\bullet AS^I(\overline{0})\bullet WH(I<N,\ AS^I(I+1)\bullet AS^R(R+I*I))\{\neg(I<N)\ \&P\}\ Ax\_CONS$$

$$\frac{\text{under implication } (0\leq N)\Rightarrow S^{[R]}\ (S^{[I]}\ (P,\ \overline{0}),\ \overline{0})}{\vdash\{(0\leq N)\}AS^R(\overline{0})\bullet AS^I(\overline{0})\bullet WH(I<N,\ AS^I(I+1)\bullet AS^R(R+I*I))\{\ R=1^2+2^2+\ldots+N^2\}}\ Ax\_CONS$$

under implication $\neg(I<N)\ \&P\Rightarrow R=1^2+2^2+\ldots+N^2$

Syntax-oriented calculus

Inference rule	Rule #
$\{P[x \mapsto a]\}x:=a\{P\}$	*AS*
$\{P\}skip\{P\}$	*skip*
$\dfrac{\{P\}S1\{Q\}, \{Q\}S2\{R\}}{\{P\}S1; S2\{R\}}$	*SEQ*
$\dfrac{\{b \wedge P\}S1\{Q\}, \{\neg b \wedge P\}S2\{Q\}}{\{P\}\text{if b then } S1 \text{ else } S2\{Q\}}$	*IF*
$\dfrac{\{b \wedge P\}S\{P\}}{\{P\}\text{while b do } S\ \{\neg b \wedge P\}}$	*WH*
$\dfrac{\{P'\}S\{Q'\}}{\{P\}S\{Q\}}$, if $P \Rightarrow P', Q' \Rightarrow Q$	*CONS*

Generalizations of Floyd-Hoare logic

1. Complex data structures

2. Communicating processes

3. New compositions

4. Program termination and complete correctness

Conclusions

- **Compositional program models (algebras and logics) generalize traditional models**
- **They have a wider area of application**
- **Compositional program verification methods can be constructed based on program models and program logics**
- **Program verification tools can support verification**