Axiomatic Semantics

Principles of Programming Languages

Fatma Başak Aydemir

basak.aydemir@boun.edu.tr

Axiomatic Semantics

- Developed as a formal method to prove the correctness of programs
- Given some constraints,a program is claimed to compute an output
- So, beginning from this constraint, we analyze the program statement by statement using logic, and we arrive at a description of the output. If this is the same as the output then we prove that the program is correct.
- Later, it is used to derive the semantics of programming languages
- Based on predicate logic

Axiomatic Semantics

{P}
S1
S2
S3
.
.
.
Sn
{Q}

- **assertion** A logical expression
- **precondition** An assertion which indicates the input constraints
- **postcondition** n assertion which indicates the constraints after the program is executedx

Rules for Language Constructs

Axiom

An assertion that is assumed to be true.

Example: Assignment Statement

$\{P\}X = E\{Q\}$ Then, the axiom for $X = E$ is $P = Q_{x \to E}$, meaning P is equal to Q where every occurence of X is replaced by E.

Rules for Language Constructs

Inference Rule

$$\frac{A_1, \qquad A_2, \qquad \ldots \qquad A_n}{B}$$

Example: if statement

```
{P}  if  B  then  S1  else  S2  {Q}
```

$$\frac{\{P \text{ and } B\} S1 \{Q\}, \qquad \{P \text{ and } (\text{ not } B)\} S2 \{Q\}}{\{P\} \text{if B then S1 else S2} \{Q\}}$$

Assignment Statement

- Statement $X = E$
- Axiom $P = Q_{x \to E}$
- Axiomatic semantics $\{Q_{x \to E}\} X = E \{Q\}$
- Inference rule version $\dfrac{X = E}{\{P(E)\} X = E \{P(X)\}}$

Example: Assignment Statement

$a = b/2 - 1\{a < 10\}$

Example: Assignment Statement

$a = b/2 - 1\{a < 10\}$
$b/2 - 1 < 10 \implies b < 22$

Example: Assignment Statement

$a = b/2 - 1\{a < 10\}$
$b/2 - 1 < 10 \implies b < 22$
What about $b < 10$?

Example: Assignment Statement

$a = b/2 - 1\{a < 10\}$
$b/2 - 1 < 10 \implies b < 22$
What about $b < 10$?
We are looking for the least restrictive (weakest) precondition

Example: Assignment Statement

$x = x + y - 3\{x > 10\}$

Example: Assignment Statement

$x = x + y - 3\{x > 10\}$
$x + y - 3 > 10 \implies y > 13 - x$

Example: Assignment Statement

$x = x + y - 3\{x > 10\}$
$x + y - 3 > 10 \implies y > 13 - x$
Semantics: $\{y > 13 - x\}x = x + y - 3\{x > 10\}$

Example: Assignment Statement

$x = x + 1\{y < 10\}$

Example: Assignment Statement

$x = x + 1\{y < 10\}$
P is $\{y < 10\}$

If Statement

- Statement: if B then S1 else S2
- Inference Rule: $\dfrac{\{P \text{ and } B\}S1\{Q\}, \qquad \{P \text{ and } (\text{ not } B)\}S2\{Q\}}{\{P\}\text{if B then S1 else S2}\{Q\}}$
- Axiomatic semantics: P if B then S1 else S2 Q

Example: if statement

```
if (x>0) then y=y-1 else y=y+1 {y>0}
```

For the then part

Example: if statement

```
if (x>0) then y=y-1 else y=y+1 {y>0}
```

For the then part
$y = y - 1\{y > 0\} \implies$ P is $\{y > 1\}$
For the else part

Example: if statement

```
if (x>0) then y=y-1 else y=y+1 {y>0}
```

For the then part
$y = y - 1\{y > 0\} \implies$ P is $\{y > 1\}$
For the else part
$y = y + 1\{y > 0\} \implies$ P is $\{y > -1\}$

Example: if statement

```
if (x>0) then y=y-1 else y=y+1 {y>0}
```

For the then part
$y = y - 1\{y > 0\} \implies$ P is $\{y > 1\}$
For the else part
$y = y + 1\{y > 0\} \implies$ P is $\{y > -1\}$
Since $\{y > 1\}$ implies $\{y > -1\}$, $\{y > 1\} \implies \{y > -1\}$, we take $\{y > 1\}$ as P.

Example: if statement

```
if (x>0) then y=y-1 else y=y+1 {y>0}
```

For the then part
$y = y - 1\{y > 0\} \implies$ P is $\{y > 1\}$
For the else part
$y = y + 1\{y > 0\} \implies$ P is $\{y > -1\}$
Since $\{y > 1\}$ implies $\{y > -1\}$, $\{y > 1\} \implies \{y > -1\}$, we take $\{y > 1\}$ as P.

```
{y>1} if (x>0) then y=y-1 else y=y+1 {y>0} {y>0}
```

Statement Sequence

$$y = 3x + 1; x = y + 3\{x < 10\}$$

Consequence Rule 1

$$\frac{\{P\}S\{Q\}, \qquad P^{'} \implies P}{\{P^{'}\}S\{Q\}}$$

Example

$$\{x > 0\}x = x + 1\{x > 1\}$$

Consequence Rule 2

$$\frac{\{P\}S\{Q\}, \qquad Q \implies Q^{'}}{\{P\}S\{Q^{'}\}}$$

Example

$$\{x > 0\}x = x + 1\{x > 1\}$$

while statement

$$\langle \text{stetement} \rangle \quad \rightarrow \quad \texttt{while}\langle \text{B} \rangle\texttt{do}\langle \text{S} \rangle\texttt{end}$$

while statement

$$\langle \text{stetement} \rangle \quad \rightarrow \quad \texttt{while}\langle \mathbf{B} \rangle \texttt{do} \langle \mathbf{S} \rangle \texttt{end}$$

- More complex

while statement

$$\langle \text{stetement} \rangle \quad \rightarrow \quad \texttt{while}\langle \mathbf{B} \rangle \texttt{do} \langle \mathbf{S} \rangle \texttt{end}$$

- More complex
- How many times do we execute S?

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times

white statement

$$\frac{\cdot}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

Idea:

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

Idea: use $\{P$ and (not $B)\}$ instead of Q, provided that
P and (not B) $\implies Q$ (consequence rule 2)

white statement

$$\frac{\cdot}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

Idea: use $\{P$ and (not $B)\}$ instead of Q, provided that
P and (not B) $\implies Q$ (consequence rule 2)

$$\frac{\{P\}\ \text{while} \ldots \{P\ \text{and (not}\ B)\},\qquad P\ \text{and (not}\ B) \implies Q}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

white statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

Consider the post condition

- B will be false after the loop terminates
- The loop can execute zero or more times
- If the loop does not execute at all, P will remain true after the loop

Idea: use $\{P \text{ and } (\text{not } B)\}$ instead of Q, provided that
$P \text{ and } (\text{not } B) \implies Q$ (consequence rule 2)

$$\frac{\{P\}\ \text{while} \ldots \{P \text{ and } (\text{not } B)\}, \qquad P \text{ and } (\text{not } B) \implies Q}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{Q\}}$$

If we find a P such that P and (not B) is satisfied and this implies Q, then after the loop Q must be satisfied

while statement

$$\frac{\cdot}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and (not}\ B)\}}$$

while statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and (not}\ B)\}}$$

Consider the following antecedent:

$$\frac{\{P\ \text{and}\ B\}S\{P\}}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and (not}\ B)\}}$$

while statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and}\ (\text{not}\ B)\}}$$

Consider the following antecedent:

$$\frac{\{P\ \text{and}\ B\}S\{P\}}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and}\ (\text{not}\ B)\}}$$

If we can find such a P that when P and B are true, after executing S, P remains true, then the consequent obviously will be satisfied.

while statement

$$\frac{.}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and (not}\ B)\}}$$

Consider the following antecedent:

$$\frac{\{P\ \text{and}\ B\}S\{P\}}{\{P\}\ \text{while}\ B\ \text{do}\ S\ \text{end}\ \{P\ \text{and (not}\ B)\}}$$

If we can find such a P that when P and B are true, after executing S, P remains true, then the consequent obviously will be satisfied.
P is called a *loop invariant* because it is true before and after the loop.

Find the P

We want to find a P such that

- $\{P \text{ and } B\}S\{P\}$

Find the P

We want to find a P such that

- $\{P \text{ and } B\}S\{P\}$
- P and (not B) $\implies Q$

Find the P

We want to find a P such that

- $\{P \text{ and } B\}S\{P\}$
- P and (not B) $\implies Q$
- $\{P\}B\{P\}$ When replacing Q with $\{P \text{ and } B\}$ we have assumed that when B is executed and found false, (the loop does not execute at all) P remains true. Execution of B does not invalidate P.

Find the P

- Sometimes beginning from Q executing loop body may give us a pattern
- Sometimes we can analyze the loop body to find such an invarying assertion
- There is no method to systematically find a loop invariant

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$

Example

while y<>x **do y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$

Example

```
while y<>x do y=y+1 end {y=x}
```

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Example

`while y<>x do y=y+1 end {y=x}`

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$

So

`{y <= x}while y<>x do y=y+1 end {y=x}`

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Example

`while y<>x do y=y+1 end {y=x}`

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$

So

`{y <= x}while y<>x do y=y+1 end {y=x}`

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$
- P and (not B) $\implies Q$

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$
- P and (not B) $\implies Q$
  - $(y \leq x$ and $y = x) \implies y = x$

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$
- P and (not B) $\implies Q$
  - $(y \leq x$ and $y = x) \implies y = x$
  - $y = x \implies y = x$

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P$ and $B\}S\{P\}$
  - $\{y \leq x$ and $y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$
- P and (not B) $\implies Q$
  - $(y \leq x$ and $y = x) \implies y = x$
  - $y = x \implies y = x$
- $\{P\}B\{P\}$

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Example

while **y**<>x **do** **y**=**y**+1 end {**y**=x}

- If loop executes 0 times, P is $y = x$
- If loop executes 1 time, P is $y = x - 1$
- If loop executes 2 times, P is $y = x - 2$

Maybe, $y \leq x$ Let's check if this is a suitable P.

- $\{P \text{ and } B\}S\{P\}$
  - $\{y \leq x \text{ and } y <> x\}y = y + 1\{y \leq x\}$
  - $\{y < x\}y = y + 1\{y \leq x\}$
- P and (not B) $\implies Q$
  - $(y \leq x \text{ and } y = x) \implies y = x$
  - $y = x \implies y = x$
- $\{P\}B\{P\}$
  - This is true since B has not side effects

So

{**y** <= x}**while** **y**<>x **do** **y**=**y**+1 end {**y**=x}

Do not forget to show that the loop terminates!

Another Example

```
{B>=0}
function multiply(A,B)
    a=A
    b=B
    y=0
    while b>0 do
        y=y+a
        b=b-1
    end
{y=A*B}
```

Another Example

	y	a.b
Initially	0	AB
After 1 iteration	a	AB-a
After 2 iterations	2a	AB-2a

Another Example

	y	a.b
Initially	0	AB
After 1 iteration	a	AB-a
After 2 iterations	2a	AB-2a

What can be the pattern?

Another Example

	y	a.b
Initially	0	AB
After 1 iteration	a	AB-a
After 2 iterations	2a	AB-2a

What can be the pattern?
$y + ab = AB$ is always true!

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- P and (not B) $\implies Q$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- P and (not B) $\implies Q$
  - $y + ab = AB \text{ and } b \geq 0 \text{ and } b \leq 0 \implies y = AB$

Another Example

Check if this is valid

- $\{P \text{ and } B\} S \{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- P and (not B) $\implies Q$
  - $y + ab = AB \text{ and } b \geq 0 \text{ and } b \leq 0 \implies y = AB$
  - $y + ab = AB \text{ and } b = 0$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- P and (not B) $\implies Q$
  - $y + ab = AB \text{ and } b \geq 0 \text{ and } b \leq 0 \implies y = AB$
  - $y + ab = AB \text{ and } b = 0$
  - $y + ab = AB \implies y = AB$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- $P \text{ and (not } B) \implies Q$
  - $y + ab = AB \text{ and } b \geq 0 \text{ and } b \leq 0 \implies y = AB$
  - $y + ab = AB \text{ and } b = 0$
  - $y + ab = AB \implies y = AB$
- $\{P\}B\{P\}$

Another Example

Check if this is valid

- $\{P \text{ and } B\}S\{P\}$
  - $\{y + ab = AB \text{ and } b \geq 0 \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
  - $\{y + ab = AB \text{ and } b > 0\} \ldots \{y + ab = AB \text{ and } b \geq 0\}$
- P and (not B) $\implies Q$
  - $y + ab = AB \text{ and } b \geq 0 \text{ and } b \leq 0 \implies y = AB$
  - $y + ab = AB \text{ and } b = 0$
  - $y + ab = AB \implies y = AB$
- $\{P\}B\{P\}$
  - $b > 0$ has no side efffects

Let's compute the precondition

```
{B>=0}
function multiply(A,B)
    a=A
    b=B
    y=0
    while b>0 do
        y=y+a
        b=b-1
    end
{y=A*B}
```