Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

{ $n \geq 0$ }

{ $q = x^n$ }

Schritte:

1. **Vor-, Nachbedingung**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

Schritte:

1. Vor-, Nachbedingung
2. **Schleifeninvariante**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \}$

$\{ INV \}$

solange i > 0 wiederhole

$\{ INV \wedge i > 0 \}$

$\{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. **Schleife mit INV**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \} \rightarrow \{ n = n \wedge n \geq 0 \wedge x = x \wedge 1 = 1 \}$

```
a := x; q := 1; i := n;
```

$\{ i = n \wedge i \geq 0 \wedge a = x \wedge q = 1 \} \rightarrow \{ INV \}$

```
solange i > 0 wiederhole
```

$\{ INV \wedge i > 0 \}$

$\{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. Schleife mit INV
4. **Initialisierung**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \} \rightarrow \{ n = n \wedge n \geq 0 \wedge x = x \wedge 1 = 1 \}$

```
a := x; q := 1; i := n;
```

$\{ i = n \wedge i \geq 0 \wedge a = x \wedge q = 1 \} \rightarrow \{ INV \}$

```
solange i > 0 wiederhole
```

$\{ INV \wedge i > 0 \}$

$\{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

falls i gerade: $x^n = q * (a^2)^{i/2}$

falls i ungerade: $x^n = q * a * (a^2)^{i/2}$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. Schleife mit INV
4. Initialisierung
5. **Idee für Schleifenrumpf**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

falls i gerade: $x^n = q * (a^2)^{i/2}$

falls i ungerade: $x^n = q * a * (a^2)^{i/2}$

Algorithmus:

$\{ n \geq 0 \} \rightarrow \{ n = n \wedge n \geq 0 \wedge x = x \wedge 1 = 1 \}$

```
a := x; q := 1; i := n;
```

$\{ i = n \wedge i \geq 0 \wedge a = x \wedge q = 1 \} \rightarrow \{ INV \}$

```
solange i > 0 wiederhole
```

$\{ INV \wedge i > 0 \}$

```
falls i ungerade:
```

$\{ INV \wedge i > 0 \wedge i \text{ ungerade} \} \rightarrow$

$\{ x^n = q * a * (a^2)^{i/2} \wedge i > 0 \}$ `q := q * a;` $\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

leere Alternative für i gerade:

$\{ INV \wedge i > 0 \wedge i \text{ gerade} \} \rightarrow \{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

$\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

$\{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. Schleife mit INV
4. Initialisierung
5. Idee für Schleifenrumpf
6. **Alternative**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \} \rightarrow \{ n = n \wedge n \geq 0 \wedge x = x \wedge 1 = 1 \}$

```
a := x; q := 1; i := n;
```

$\{ i = n \wedge i \geq 0 \wedge a = x \wedge q = 1 \} \rightarrow \{ INV \}$

```
solange i > 0 wiederhole
```

$\{ INV \wedge i > 0 \}$

falls i ungerade: $\{ INV \wedge i > 0 \wedge i \text{ ungerade} \} \rightarrow$

$\{ x^n = q * a * (a^2)^{i/2} \wedge i > 0 \}$ `q := q * a;` $\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

leere Alternative für i gerade:

$\{ INV \wedge i > 0 \wedge i \text{ gerade} \} \rightarrow \{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

$\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

```
a := a * a;
```

$\{ x^n = q * a^{i/2} \wedge i > 0 \} \rightarrow \{ x^n = q * a^{i/2} \wedge i/2 \geq 0 \}$

```
i := i / 2
```

$\{ x^n = q * a^i \wedge i \geq 0 \} \leftrightarrow \{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

falls i gerade: $x^n = q * (a^2)^{i/2}$

falls i ungerade: $x^n = q * a * (a^2)^{i/2}$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. Schleife mit INV
4. Initialisierung
5. Idee für Schleifenrumpf
6. Alternative
7. **Schleife komplett**

Schrittweise Konstruktion und Verifikation

Vorbedingung: $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$

Nachbedingung: $q = x^n$

Algorithmus:

$\{ n \geq 0 \} \rightarrow \{ n = n \wedge n \geq 0 \wedge x = x \wedge 1 = 1 \}$

```
a := x; q := 1; i := n;
```

$\{ i = n \wedge i \geq 0 \wedge a = x \wedge q = 1 \} \rightarrow \{ INV \}$

```
solange i > 0 wiederhole
```

$\{ INV \wedge i > 0 \}$

```
falls i ungerade:
```
$\{ INV \wedge i > 0 \wedge i \text{ ungerade} \} \rightarrow$

$\{ x^n = q * a * (a^2)^{i/2} \wedge i > 0 \}$ `q := q * a;` $\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

leere Alternative für i gerade:

$\{ INV \wedge i > 0 \wedge i \text{ gerade} \} \rightarrow \{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

$\{ x^n = q * (a^2)^{i/2} \wedge i > 0 \}$

```
a := a * a;
```

$\{ x^n = q * a^{i/2} \wedge i > 0 \} \rightarrow \{ x^n = q * a^{i/2} \wedge i/2 \geq 0 \}$

```
i := i / 2
```

$\{ x^n = q * a^i \wedge i \geq 0 \} \leftrightarrow \{ INV \}$

$\{ INV \wedge i \leq 0 \} \rightarrow \{ q = x^n \}$

Terminierung der Schleife: i fällt monoton und $i \geq 0$ ist invariant.

Konstruktionsidee:

Invariante INV: $x^n = q * a^i \wedge i \geq 0$

Zielbedingung: $i \leq 0$

falls i gerade: $x^n = q * (a^2)^{i/2}$

falls i ungerade: $x^n = q * a * (a^2)^{i/2}$

Schritte:

1. Vor-, Nachbedingung
2. Schleifeninvariante
3. Schleife mit INV
4. Initialisierung
5. Idee für Schleifenrumpf
6. Alternative
7. Schleife komplett
8. **Terminierung**