Hoare-Kalkül

Zuweisungsaxiom (ZWA)

{P}	S	{Q}
{a+2=5}	a=a+2	{a=5}
{false=false}	b=false	{b=false}

Zuweisungsaxiom (ZWA)

{P}	S	{Q}
{11=5+3+3} = {true}	a=5	{11=a+3+3}
{11=a+3+3}	b=3	{11=a+b+3}
{11=a+b+3}	c=a+b	{11=c+3}
{11=c+3}	d=3	{11=c+d}
{11=c+d}	e=c+d	{11=e}

Kompositions- oder Sequenzregel

$$\frac{\{P\}S\{R\},\{R\}T\{Q\}}{\{P\}S;T\{Q\}}$$

{P}	S	{Q}
{11=5+3+3} = {true}	a=5; b=3; c=a+b;	{11=c+3}
{11=c+3}	d=3; e=c+d;	{e=11}

Da wir keinen Parallelenbefehle haben kürzen wir das noch weiter ab, da jedes {P} definitv das {Q} von davor ist

$$\{11=5+3+3\}=\{true\}$$
$$a=5;$$
$$b=3;$$
$$c=a+b;$$
$$\{11=c+3\}$$
$$d=3;$$
$$e=c+d;$$
$$\{e=11\}$$

Konsequenzregel(KSR)

{P}	S	{Q}
{true}	x=0	{x>=0} anstatt {x=0}
{y=2}	x=y-1	{x<=1} anstatt {x=1}

Abschwächen der Folgerungen ist immer erlaubt!

Hoare - Negation

```
neg(a)

{true}

b=true;

if (a) {

 b = false;

} else {

 b = true;

}
{a!=b}
```

Auswahlregel

Regel

$$\frac{\{P \wedge B\}\, S\, \{Q\},\ \{P \wedge \neg B\}\, T\, \{Q\}}{\{P\}\ \mathit{if}\ B\ \mathit{then}\ S\ \mathit{else}\ T\ \{Q\}}$$

Bedeutet

$$\left.\begin{array}{l} \{P \wedge B\} \\ S \\ \{Q\} \\ \\ \{P \wedge \neg B\} \\ T \\ \{Q\} \end{array}\right\} \text{folgt} \quad \begin{array}{l} \{P\} \\ \text{if}\,(B)\,\{ \\ \qquad \{S\} \\ \}\ \text{else}\ \{ \\ \qquad \{T\} \\ \} \\ \{Q\} \end{array}$$

Hoare - Negation

```
neg(a)

{true}

b=true;
                                        P=? Wollen wir suchen!
if (a) {                                B = a!=b
 {a = true}
 b = false;                             S = b=false;
 {a!=b}
} else {
 {a=false}
 b = true;                              T=b=true;
 {a!=b}
}
{a!=b}                                  Q = {a!=b}
```

Hoare - Negation

```
neg(a)

{true}

b=true;

if (a) {
 {a = true & a!=false} ZWA
 b = false;
 {a!=b}
} else {
 {a = false & a!=true} ZWA
 b = true;
 {a!=b}
}
{a!=b}
```

Hoare - Negation

neg(a)

{true}

b=true;

if (a) {

{a = true & a!=false} = {a = true} KSR

b = false;

{a!=b}

} else {

{a = false & a!=true} = {a = false} KSR

b = true;

{a!=b}

}

{a!=b}

Hoare - Negation

neg(a)

{true}

b=true;

{a=true ˇ a = false} Auswahlregel oder If-Regel

if (a) {

{a = true & a!=false} = {a = true}

b = false;

{a!=b}

} else {

{a = false & a!=true} = {a = false}

b = true;

{a!=b}

}

{a!=b}

Hoare - Negation

neg(a)

{true}

b=true;

{a=true ˇ a = false} = {true} KSR

if (a) {

{a = true & a!=false} = {a = true}

b = false;

{a!=b}

} else {

{a = false & a!=true} = {a = false}

b = true;

{a!=b}

}

{a!=b}

Hoare - Negation

neg(a)

{true} ZWA

```
b=true;
{true}
if (a) {
 {a = true & a!=false} =  {a = true}
 b = false;
 {a!=b}
} else {
{a = false & a!=true} =  {a = false}
 b = true;
 {a!=b}
}
{a!=b}
```

Hoare - Min

```
min(a,b)
{true}
res=0;

if(a<=b){

    res=a;

} else {

    res=b;

}
```

$\{(a<=b \wedge res = a) \vee (a>b \wedge res = b)\}$

Hoare - Min

min(a,b)

{true}

res=0;

{P} P=? Wollen wir suchen

if(a<=b){ B = a<=b

res=a; S = res=a;

} else {

res=b; T=res=b;

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)} Q = {(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

{ a<=b}

res=a;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

} else {

{a>b}

res=b;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

{a<=b ^ ((a<=b ^ a = a) ˇ (a>b ^ a = b)) ZWA}

res=a;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

} else {

{a>b ^ ((a<=b ^ b = a) ˇ (a>b ^ b = b))}

res=b;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

{a<=b ^ ((a<=b ^ a = a)~~˘ (a>b ^ a = b)~~)} KSR, weil a>b verträgt sich nicht mit B

res=a;

{(a<=b ^ res = a) ˘ (a>b ^ res = b)}

} else {

{a>b ^ (~~(a<=b ^ b = a) ˘~~ (a>b ^ b = b))} KSR, weil a<=b verträgt sich nicht mit nicht B

res=b;

{(a<=b ^ res = a) ˘ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˘ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

{a<=b ^ ((a<=b ^ a = a)~~ ˇ (a>b ^ a = b)~~)} = {a<=b ~~ ^ a<=b~~ ^ a = a} KSR, doppelte Bedingung

res=a;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

} else {

{a>b ^ (~~(a<=b ^ b = a) ˇ~~ (a>b ^ b = b))} = {a>b ~~ ^ a>b~~ ^ b = b} KSR, doppelte Bedingung

res=b;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

KSR B^true=B

{a<=b ^ ((a<=b ^ a = a)~~ ˇ (a>b ^ a = b)~~)} = {a<=b ~~^ a<=b~~ ^ a = a} = {a<=b ~~^ a = a~~}

res=a;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

} else {

{a>b ^ (~~(a<=b ^ b = a) ˇ~~ (a>b ^ b = b))} = {a>b ~~^ a>b~~ ^ b = b} = {a>b ~~^ b = b~~}

KSR B^true=B

res=b;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

if(a<=b){

{a<=b ^ ((a<=b ^ a = a)~~ ˇ (a>b ^ a = b)~~)} = {a<=b ~~ ^ a<=b~~ ^ a = a} = {a<=b ~~ ^ a = a~~} = {a<=b}

res=a;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

} else {

{a>b ^ (~~(a<=b ^ b = a) ˇ~~ (a>b ^ b = b))} = {a>b ~~ ^ a>b~~ ^ b = b} = {a>b ~~ ^ b = b~~} = {a>b}

res=b;

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

}

{(a<=b ^ res = a) ˇ (a>b ^ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

{a<=b ˇ a>b}

if(a<=b){

{a<=b}

res=a;

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

} else {

{a>b}

res=b;

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

}

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

Hoare - Min

min(a,b)

{true}

res=0;

{a<=b ˇ a>b} = {true} KSR

if(a<=b){

{a<=b}

res=a;

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

} else {

{a>b}

res=b;

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

}

{(a<=b ˆ res = a) ˇ (a>b ˆ res = b)}

Hoare - Multiplikation

```
mul(a,b)

res=0;

n=b;

while(n>0){

   res=res+a;

   n=n-1;

}

{res=a*b}
```

Hoare - Multiplikation

mul(a,b)	
res=0;	
n=b;	
while(n>0){	
res=res+a;	
n=n-1;	
}	
{res=a*b}	

Iterationsregel

Regel

$$\frac{\{I \wedge B\}\, S\, \{I\}}{\{I\}\, B\, do\, S\, done\, \{I \wedge \neg B\}}$$

Bedeutet

$\{I\}$ ← Dann

$While(B)\{$

$\{I \wedge B\}$

S

$\{I\}$

Wenn

$\}$ ← Dann

$\{I \wedge \neg B\}$

Hoare - Multiplikation

Code	a		b		a		n		res
while(n>0){	5	*	3	=	5	*	2	+	5
res=res+a;	5	*	3	=	5	*	1	+	10
n=n-1;	5	*	3	=	5	*	0	+	15
}									

I = a*b = a*n+res

Hoare - Multiplikation

```
mul(a,b)

res=0;

n=b;

while(n>0){

   res=res+a;

   n=n-1;

}

{res=a*b}
```

$B = n>0$

Hoare - Multiplikation

mul(a,b)	
res=0;	
n=b;	
{I}	{a*b = a*n+res}
while(n>0){	
{I ^ B}	{a*b = a*n+res ^ n>0}
res=res+a;	
n=n-1;	
{I}	
}	
{I ^ !B}	
{res=a*b}	

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res} ?!
while(n>0){
{a*b = a*n+res ^ n>0}
   res=res+a;
   n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0}  ?!
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res} ?!
while(n>0){
{a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res} ZWA
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0}  ?!
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res} ?!
while(n>0){
{a*b=a*n+res^n>0}={a*b=a*(n-1)+res+a^n>0} ZWA
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} ?!
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res}?!
while(n>0){
{a*b=a*n+res^n>0}={a*b=a*(n-1)+res+a^n>0}={a*b=a*(n-1)+a+res^n>0}=
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} ?!
{res=a*b}
```

Hoare - Multiplikation

mul(a,b)
res=0;
n=b;
{a*b = a*n+res}?!
while(n>0){
{a*b=a*n+res^n>0}={a*b=a*(n-1)+res+a^n>0}={a*b=a*(n-1)+a+res^n>0}={a*b=a*n+res^ n>0}
res=res+a;
{a*b = a*(n-1)+res}
n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} ?!
{res=a*b}

Hoare - Multiplikation

mul(a,b)
res=0;
n=b;
{a*b = a*n+res} !
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
res=res+a;
{a*b = a*(n-1)+res}
n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} !
{res=a*b}

!
Iterationsregel

!
Iterationsregel

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0} KSR
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} KSR
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} = {a*b = res} KSR
{res=a*b}
```

!

Hoare - Multiplikation

```
mul(a,b)
res=0;
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} = {a*b = res}
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
res=0;
{a*b = a*b+res} ZWA
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} = {a*b = res}
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
{a*b = a*b+0} ZWA
res=0;
{a*b = a*b+res}
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} = {a*b = res}
{res=a*b}
```

Hoare - Multiplikation

```
mul(a,b)
{a*b = a*b+0} = {a*b = a*b} KSR
res=0;
{a*b = a*b+res}
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
  res=res+a;
{a*b = a*(n-1)+res}
  n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0}  = {a*b = a*0+res} = {a*b = res}
{res=a*b}
```

Hoare - Multiplikation

mul(a,b)
{a*b = a*b+0} = {a*b = a*b} = {true} KSR
res=0;
{a*b = a*b+res}
n=b;
{a*b = a*n+res}
while(n>0){
{a*b = a*(n-1)+res+a ^ n>0} = {a*b = a*(n-1)+a+res ^ n>0} = {a*b = a*n+res ^ n>0}
res=res+a;
{a*b = a*(n-1)+res}
n=n-1;
{a*b = a*n+res}
}
{a*b = a*n+res ^ n<=0} = {a*b = a*n+res ^ n<=0} = {a*b = a*0+res} = {a*b = res}
{res=a*b}

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;

while(n>0){

   res=res*a;

   n=n-1;

}

{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;

while(n>0){

   res=res*a;

   n=n-1;
}

{res = a^b}
```

	a		n		res		a		b
while(n>0){	2	^	3	*	1	=	2	^	3
res=res*a;	2	^	2	*	2	=	2	^	3
n=n-1;	2	^	1	*	4	=	2	^	3
}	2	^	0	*	8	=	2	^	3

I = a^n*res=a^b

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;

while(n>0){

   res=res*a;

   n=n-1;

}

{res = a^b}
```

B = n > 0

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{I}
while(n>0){
{I ^ B}
   res=res*a;

   n=n-1;
{I}
}
{I ^ !B}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^n*res=a^b ^ n>0}
   res=res*a;

   n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^n*res=a^b ^ n>0}
  res=res*a;
 {a^(n-1)*res=a^b}  ZWA
  n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^n*res=a^b ^ n>0} = {a^(n-1)*res*a=a^b ^ n>0} ZWA
   res=res*a;
 {a^(n-1)*res=a^b}
   n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^n*res=a^b ^ n>0} = {a^(n-1)*res*a=a^b ^ n>0}= {a^(n-1)*a*res=a^b ^ n>0} KSR
   res=res*a;
 {a^(n-1)*res=a^b}
   n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^n*res=a^b^n>0}={a^(n-1)*res*a=a^b^n>0}={a^(n-1)*a*res=a^b^n>0}={a^n*res=a^b^n>0}
  res=res*a;
 {a^(n-1)*res=a^b}
  n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

KSR

!

Hoare - Potenzieren

pow(a,b)
{b>=0}
res = 1;
n = b;
{a^n*res=a^b}
while(n>0){
{a^(n-1)*res*a=a^b ˆ n>0} = {a^(n-1)*a*res=a^b ˆ n>0} = {a^n*res=a^b ˆ n>0}
res=res*a;
{a^(n-1)*res=a^b}
n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ˆ n<=0}
{res = a^b}

Iterationsregel!

Iterationsregel!

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;

n = b;
{a^n*res=a^b}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0} = {a^(n-1)*a*res=a^b ^ n>0} = {a^n*res=a^b ^ n>0}
  res=res*a;
 {a^(n-1)*res=a^b}
  n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{b>=0}
res = 1;
{a^b*res=a^b} ZWA
n = b;
{a^n*res=a^b}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0} = {a^(n-1)*a*res=a^b ^ n>0} = {a^n*res=a^b ^ n>0}
  res=res*a;
 {a^(n-1)*res=a^b}
  n=n-1;
{a^n*res=a^b}
}
{a^n*res=a^b ^ n<=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{a^b*1=a^b ^ b>=0} ZWA + KSR
res = 1;
{a^b*res=a^b ^ b>=0}
n = b;
{a^n*res=a^b ^ b>=0 ^ n>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^ n>=0}
  res=res*a;
 {a^(n-1)*res=a^b ^ b>=0 ^ n>=0}
  n=n-1;
{a^n*res=a^b ^ b>=0 ^ n>=0}
}
{a^n*res=a^b ^ n<=0 ^ b>=0 ^ n>=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{a^b*1=a^b ^ b>=0} = {a^b=a^b^ b>=0}  KSR
res = 1;
{a^b*res=a^b ^ b>=0}
n = b;
{a^n*res=a^b ^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^  n>=0}
   res=res*a;
 {a^(n-1)*res=a^b^ b>=0}
   n=n-1;
{a^n*res=a^b^ b>=0}
}
{a^n*res=a^b ^ n<=0^ b>=0}
{res = a^b}
```

Hoare - Potenzieren

```
pow(a,b)
{a^b*1=a^b^ b>=0} = {a^b=a^b^ b>=0} = {b>=0} KSR
res = 1;
{a^b*res=a^b^ b>=0}
n = b;
{a^n*res=a^b^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^  n>=0}
  res=res*a;
 {a^(n-1)*res=a^b^ b>=0}
  n=n-1;
{a^n*res=a^b^ b>=0}
}
{a^n*res=a^b ^ n<=0^ b>=0}
{res = a^b}
```

Hoare - Potenzieren

pow(a,b)
{a^b*1=a^b^ b>=0} = {a^b=a^b^ b>=0} = {b>=0}
res = 1;
{a^b*res=a^b^ b>=0}
n = b;
{a^n*res=a^b^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^ n>=0}
res=res*a;
{a^(n-1)*res=a^b^ b>=0}
n=n-1;
{a^n*res=a^b^ b>=0}
}
{a^n*res=a^b ^ n<=0^ b>=0}={a^n*res=a^b ^ n=0} KSR
{res = a^b}

Hoare - Potenzieren

```
pow(a,b)
{a^b*1=a^b^ b>=0} = {a^b=a^b^ b>=0} = {b>=0}
res = 1;
{a^b*res=a^b^ b>=0}
n = b;
{a^n*res=a^b^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^  n>=0}
   res=res*a;
 {a^(n-1)*res=a^b^ b>=0}
   n=n-1;
{a^n*res=a^b^ b>=0}
}
                                                    KSR
{a^n*res=a^b ^ n<=0^ b>=0}={a^n*res=a^b ^ n=0}={a^0*res=a^b}
{res = a^b}
```

Hoare - Potenzieren

pow(a,b)
{a^b*1=a^b^ b>=0} = {a^b=a^b^ b>=0} = {b>=0}
res = 1;
{a^b*res=a^b^ b>=0}
n = b;
{a^n*res=a^b^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^ n>=0}
res=res*a;
{a^(n-1)*res=a^b^ b>=0}
n=n-1;
{a^n*res=a^b^ b>=0}
}
KSR {a^n*res=a^b ^ n<=0^ b>=0}={a^n*res=a^b ^ n=0}={a^0*res=a^b}={1*res=a^b}
{res = a^b}

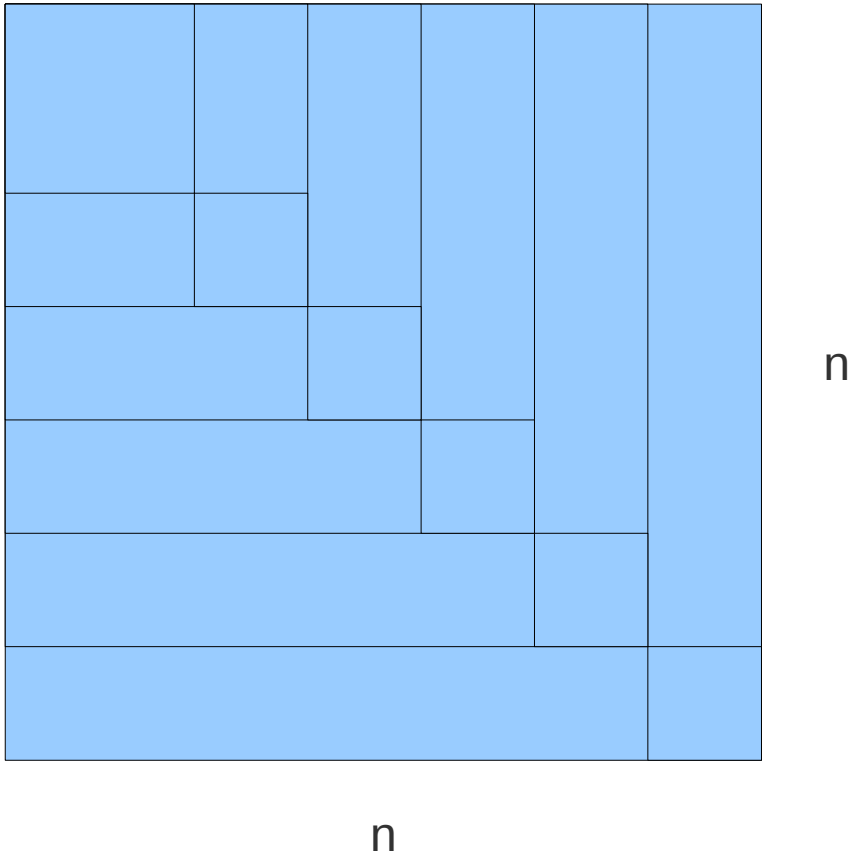
Hoare - Potenzieren

```
pow(a,b)
{a^b*1=a^b^ b>=0} = {a^b=a^b^ b>=0} = {b>=0}
res = 1;
{a^b*res=a^b^ b>=0}
n = b;
{a^n*res=a^b^ b>=0}
while(n>0){
{a^(n-1)*res*a=a^b ^ n>0}={a^(n-1)*a*res=a^b ^ n>0}={a^n*res=a^b ^ n>0 ^ b>=0 ^  n>=0}
   res=res*a;
 {a^(n-1)*res=a^b^ b>=0}
   n=n-1;
{a^n*res=a^b^ b>=0}
}
                                                                                    KSR
{a^n*res=a^b ^ n<=0^ b>=0}={a^n*res=a^b ^ n=0}={a^0*res=a^b}={1*res=a^b}={res=a^b}
{res = a^b}
```

Quadrieren

```
quad(a)
{a>0}
y=0

z=0

while(y<=a){

  z=z+2y+1

  y=y+1

}

```

Idee des Quadrierens



In jedem Schritt,

müssen wir den Eckpunkt(1) + die 2 alten Kanten(erhöhen sich jeden Schritt um 1) hinzuadieren

Quadrieren

	y	z	a	
	0	0	3	
while(y<=a){	1	1	3	
	2	4	3	
z=z+2y+1	3	9	3	
y=y+1	$I = z=y^2 \wedge a > 0$			
	Wir haben durch ds letzte Mal dazu gelernt, dass es eleganter ist die Vorbedingung P mit in die Invariante zu ziehen (a>0)			
}	Leider werden wir feststellen, dass das nicht ausreicht, und wir zusäzlich y-1<=a brauchen, dazu später, also $I=z=y^2 \wedge a>0 \wedge y-1<=a$			

Quadrieren

quad(a)	
{a>0}	
y=0	
z=0	
{I}	
while(y<=a){	B=y<=a
{I∧B}	
z=z+2y+1	
y=y+1	
{I}	
}	
{I∧¬B}	

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a} ?!
while(y<=a){
{z=y²∧a>0∧y-1<=a∧y<=a}
z=z+2y+1
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}?!

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a} ?!
while(y<=a){
{z=y²∧a>0∧y<=a∧y<=a}
z=z+2y+1
{z=(y+1)²∧a>0∧y<=a} ZWA
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}?!

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a} ?!
while(y<=a){
{z=y²∧a>0∧y<=a}={z+2y+1=(y+1)^2∧a>0∧y<=a∧y<=a} ZWA
z=z+2y+1
{z=(y+1)²∧a>0∧y<=a}
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}?!

Quadrieren

quad(a)	
	$\{z+2y+1=(y+1)^2 \wedge a>0 \wedge y<=a\}$
	$\{z+2y+1=(y+1)^2 \wedge a>0 \wedge y<=a\}$
	$\{z+2y+1=(y+1)(y+1) \wedge a>0 \wedge y<=a\}$
	$\{z+2y+1=z+2y+1 \wedge a>0 \wedge y<=a\}$
	Dürfen wir also ersetzen, mit
	$\{z=y^2 \wedge a>0 \wedge y<=a\}$

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a} ?!
while(y<=a){
{z=y²∧a>0∧y<=a∧y-1<=a}={z=z+2y+1=(y+1)^2∧a>0∧y<=a∧y-1<=a}={z=y²∧a>0∧y<=a∧y<=a} KSR
z=z+2y+1
{z=(y+1)²∧a>0∧y<=a}
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}?!

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a} ?!
while(y<=a){
{z=y²∧a>0∧y<=a∧y-1<=a}={z=z+2y+1=(y+1)^2∧a>0∧y<=a∧y-1<=a}={z=y²∧a>0∧y<=a∧y<=a}={z=y²∧a>0∧y<=a} KSR
z=z+2y+1
{z=(y+1)²∧a>0∧y<=a}
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}?!

Quadrieren

quad(a)
{a>0}
y=0
z=0
{z=y²∧a>0∧y-1<=a}
while(y<=a){
{z=y²∧a>0∧y<=a}={z=y²∧a>0∧y<=a} ZWA
z=z+2y+1
{z=(y+1)²∧a>0∧y<=a}
y=y+1
{z=y²∧a>0∧y-1<=a}
}
{z=y²∧a>0∧y-1<=a∧¬B}

Iterationsregel

Iterationsregel

Quadrieren

quad(a)
$\{a>0\}$
$y=0$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
$z=z+2y+1$
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
$y=y+1$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}$
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$ ZWA
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}$ ZWA
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}$ KSR doppelte Bedingung
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}=\{a>0 \wedge -1<=a\}$ KSR $x \wedge true \Rightarrow x$
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
$z=z+2y+1$
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
$y=y+1$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}=\{a>0 \wedge -1<=a\}$ KSR mit a>0 korrekt
y=0
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
z=0
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge \neg B\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}=\{a>0 \wedge -1<=a\}$
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge y-1<=a \wedge y>a\}$

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}=\{a>0 \wedge -1<=a\}$
$y=0$
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
$z=0$
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge \mathbf{y-1<=a \wedge y>a}\}$ = $\{z=y^2 \wedge a>0 \wedge y=a\}$ KSR Eingrenzung von A

Quadrieren

quad(a)
$\{a>0\}=\{a>0 \wedge 0=0^2 \wedge a>0 \wedge -1<=a\}=\{a>0 \wedge 0=0^2 \wedge -1<=a\}=\{a>0 \wedge -1<=a\}$
y=0
$\{0=y^2 \wedge a>0 \wedge y-1<=a\}$
z=0
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
while(y<=a){
$\{z=y^2 \wedge a>0 \wedge y<=a\}=\{z=y^2 \wedge a>0 \wedge y<=a\}$ ZWA
z=z+2y+1
$\{z=(y+1)^2 \wedge a>0 \wedge y<=a\}$
y=y+1
$\{z=y^2 \wedge a>0 \wedge y-1<=a\}$
}
$\{z=y^2 \wedge a>0 \wedge \mathbf{y-1<=a \wedge y>a}\} = \{z=y^2 \wedge a>0 \wedge y=a\} = \{z=y^2 \wedge a>0 \wedge z=a^2\}$ KSR