循环不变量的证明

循环不变量的证明方法：

1. 证明在初始情况下，循环不变量成立；

2. 假设在某次循环开始前，循环不变量成立；证明，在执行循环体后循环不变量仍然成立。

int f (int x, int y)

//@requires y >= 0;

//@ensures \result == POW(x,y);

{

int r = 1;

int b = x; /\* base \*/

int e = y; /\* exponent \*/

while (e > 0)

//@loop\_invariant e >= 0;

//@loop\_invariant r \* POW(b,e) == POW(x,y);

{

if (e % 2 == 1) r = b \* r;

b = b \* b;

e = e / 2;

}

//@assert e == 0;

return r;

}

证明r \* be == xy为循环不变量

证：1. 初始状态下：

∵ r = 1， b = x， e = y

∴ r \* be = 1 \* xy = xy。循环不变量成立。

2. 假设，在循环前循环不变量成立，即：

r \* be = xy

分两种情况讨论在执行循环体后r、b和e的变化，用r1、b1和e1表示变化后的r、b和e：

(1) e为偶数，设e = 2k (k是整数)，则：

r1 = r，b1 = b \* b = b2， e1 = e / 2 = k

那么，r1 \* b1e1 = r \* (b2)k

= r \* b2k

= r \* be

= xy (根据假设)

循环不变量成立。

(2) e为奇数，设e = 2k+1(k是整数)，则：

r1 = r\*b，b1 = b\*b = b2，e1 = e/2 = (2k+1)/2 = k(整数除)

那么，r1 \* b1e1 = r \* b \* (b2)k

= r \* b \* b2k

= r \* b2k+1

= r \* be

= xy (根据假设)

循环不变量成立。

综合(1)和(2)，在执行循环体后，循环不变量仍然成立。