Chapter 38 : Fast Exponentiation.

Consider the following problem. Given X : Int ; N : Nat . Construct a program to establish the following postcondition.

Post: $r = X^N$

We strengthen to get

Post' : $r = X^n \wedge n = N$

Invariants.

P0 : $r = X^n$
P1 : $0 \leq n \leq N$

Establish Invariants.

n, r := 0, 1

Guard.

$n \neq N$

vf.

N - n

Loop body.

(n, r := n+1, E).P0
= {text substitution}
$E = X^{n+1}$
= {Algebra}
$E = X * X^n$
= {P0}
$E = X * r$

Algorithm.

n, r := 0, 1 ;
Do $n \neq N$ —>

n, r := n+1, X * r

Od
$\{r = X^n \wedge n = N\}$

This algorithm is O(N) complexity.

Key Insight.

$X^n = (X*X)^{(n \text{ div } 2)} \quad \Leftarrow \quad even.n$

$X^n = X*X^{(n - 1)} \quad \Leftarrow \quad odd.n$

Now we consider the same problem once again but this time we strengthen in a different way.

Post'' : $r * X^n = X^N \wedge n = 0$

Invariants.

P0 : $r * X^n = X^N$
P1 : $0 \leq n \leq N$

Establish invariants.

n, r := N, 1

Guard.
$n \neq 0$

vf.
n

Loop body.

We observe

P0
= {definition}
$r * X^n = X^N$
= {case even.n}
$r * (X*X)^{(n \text{ div } 2)}$
= {WP. }
(n, X := n div 2, X * X).P0

We further observe

P0
= {definition}
$r * X^n = X^N$
= {case odd.n}
$r * X*X^{(n - 1)}$
= {WP. }
(n, r := n - 1, r * X).P0

Algorithm.

n, r := N, 1 ;
Do $n \neq 0$ —>

If even.n —> n, X := n div 2, X * X
[] odd.n —> n, r := n - 1, r * X
fi

Od
$\{r * X^n = X^N \wedge n = 0\}$

This algorithm has complexity O(Log(N)).