Constructing Verification Conditions

Note Title 09/10/2007

$\{0 \leqslant M\}$

$k, y, z := M, 1, X$

$\{$ Invariant: $0 \leqslant k \wedge yxz^k = X^M$

Bound function: k $\}$

do $0 < k \rightarrow$

if even.k $\rightarrow$ **skip**

$\square$ odd.k $\rightarrow$ $k, y := k-1, yxz$

fi

; $k, z := k \div 2, z^2$

od

$\{y = X^M\}$

```
if  even.k →
                    skip
□   odd.k →
                    k,y := k-1, yxz
fi
```