Let
\[ \text{exp} \equiv u := 1; \]
\[ \text{while } 1 < x \text{ do} \]
\[ (\text{div2}, \]
\[ \text{if } z = 1 \text{ then } u := u * y \text{ else skip;} \]
\[ y := y * y; \]
\[ y := y * u \]
where \text{div2} is some command such that

**Lemma.** For any \( \sigma \) with \( \sigma(x) > 0 \) and \( \sigma(y) = m \). Prove that

(a) If \( \langle w, \sigma \rangle \rightarrow \sigma' \) then \( \sigma'(y) \cdot \sigma'(u) = \sigma(u) \cdot m^n \).

(b) If \( \langle \text{exp}, \sigma \rangle \rightarrow \sigma' \) then \( \sigma'(y) = m^n \).

where
\[ w \equiv 1 < x \text{ do c} \]
\[ c \equiv \text{div2;} d; y := y * y \]
\[ d \equiv \text{if } z = 1 \text{ then } u := u * y \text{ else skip} \]

It follows that \( \sigma(x) > 1 \) and that
\[ \sigma'' = \sigma[y=0, z=1|x|] \] (1)

From the Lemma we know that
\[ \sigma_1 = \sigma[x=0, z=0|x|] \] (2)

where \( r \in [0, 1] \) and \( n = \sigma(x) = 2q + r \). We argue by cases on \( r \): 

\( r = 0 \): Then derivation \( B' \) must look as follows
\[ \langle z, \sigma_1 \rangle \rightarrow \sigma_1[z] = 0 \]
\[ \langle x, \sigma_1 \rangle \rightarrow 1 \]
\[ \langle z = 1, \sigma_1 \rangle \rightarrow 1 \]
\[ \langle \text{skip}, \sigma \rangle \rightarrow \sigma_2 \]
\[ \langle d, \sigma_1 \rangle \rightarrow \sigma_2 \]

hence \( \sigma_2 = \sigma_1 \). Using (1) and (2) we get
\[ \sigma'' = \sigma_1[y=m^n] = \sigma[x=0, z=0|x=0, y=m^n] \]

(note that \( \sigma_2[y] = \sigma(y) = \sigma(y) = m \). Since \( n = 2q > 1 \)
we know that \( \sigma''(x) = q > 0 \). Therefore we can apply

Assume that \( \sigma(x) > 0 \) and \( \langle w, \sigma \rangle \rightarrow \sigma' \). The proof proceeds by induction on the height of the derivation of \( \langle w, \sigma \rangle \rightarrow \sigma' \).

**Base Case:** \( \langle w, \sigma \rangle \rightarrow \sigma' \) was derived using
\[ \langle 1, \sigma \rangle \rightarrow true \]
\[ \langle x, \sigma \rangle \rightarrow \sigma(x) \]
\[ \langle z = 1, \sigma \rangle \rightarrow 1 \]
\[ \langle \text{skip}, \sigma \rangle \rightarrow \sigma_2 \]

Then \( \sigma' = \sigma \) and \( \sigma(x) \leq 1 \). Since \( \sigma(x) > 0 \) we get that \( \sigma(x) = 1 \) and hence
\[ \sigma'(y) \cdot \sigma'(u) = \sigma(u) \cdot \sigma(y) = \sigma(u) \cdot \sigma(y)^{q|x|} \]

**General Case:** The derivation of \( \langle w, \sigma \rangle \rightarrow \sigma' \) looks as follows:
\[ i \]
\[ B \]
\[ C \]
\[ \langle 1, \sigma \rangle \rightarrow true \]
\[ \langle c, \sigma \rangle \rightarrow \sigma'' \]
\[ \langle w, \sigma \rangle \rightarrow \sigma' \]

Using equations (1) and (2) we get
\[ \sigma'' = \sigma[x=0, z=0|x=m^n] = \sigma[x=0, z=0|x=m^n] \]

From \( n = 2q + 1 > 1 \) follows that \( 2q > 0 \) and \( \sigma''(x) = q > 0 \). Hence we can again use L.H to infer that
\[ \sigma'(y) \cdot \sigma'(u) = \sigma'(u) \cdot \sigma'(y)^{q|x|} \]
\[ = \sigma(u) \cdot m \cdot m^n = \sigma(u) \cdot m^{2q+1} = \sigma(u) \cdot m^n \]

Semantik och Principer f"or Programmeringspr"alken Tutorial 1

I.H. to a shorter derivation \( C \) and conclude that
\[ \sigma'(y) \cdot \sigma'(u) = \sigma'(u) \cdot \sigma'(y)^{q|x|} \]
\[ = \sigma(u) \cdot m \cdot m^n = \sigma(u) \cdot m^{2q+1} = \sigma(u) \cdot m^n \]

Exponentation

Semantik och Principer f"or Programmeringspr"alken Tutorial 1

L.H. to a shorter derivation \( C \) and conclude that
\[ \sigma'(y) \cdot \sigma'(u) = \sigma'(u) \cdot \sigma'(y)^{q|x|} \]
\[ = \sigma(u) \cdot m \cdot m^n = \sigma(u) \cdot m^{2q+1} = \sigma(u) \cdot m^n \]

(from (2), \( \sigma_1[u] = \sigma[u] \) and \( \sigma_1[y] = \sigma(y) = m \)). It follows that \( \sigma_2 = \sigma_1[x=0, z=0|x=m^n] \)

Using equations (1) and (2) we get
\[ \sigma'' = \sigma[x=0, z=0|x=m^n] = \sigma[x=0, z=0|x=m^n] \]

From \( n = 2q + 1 > 1 \) follows that \( 2q > 0 \) and
\[ \sigma''(x) = q > 0 \). Hence we can again use L.H to infer that
\[ \sigma'(y) \cdot \sigma'(u) = \sigma'(u) \cdot \sigma'(y)^{q|x|} \]
\[ = \sigma(u) \cdot m \cdot m^n = \sigma(u) \cdot m^{2q+1} = \sigma(u) \cdot m^n \]