2. Proofs of correctness.

1-7. Prove that for all $c, y, z \in \mathbb{N}$ where $c \geq 2$, it follows that $S_z : yz = \text{multiply}(y, z)$.

Proof. [1]Note that by def. of division algorithm, $z = c\lfloor z/c \rfloor + (z \bmod c) \iff (z \bmod c) = z - c\lfloor z/c \rfloor$. Suppose $z = 1$ and $c, y \in \mathbb{Z}$ where $c \geq 2$. Observe that

$$\begin{aligned}
\text{multiply}(cy, \lfloor 1/c \rfloor) + y(1 \bmod c) &= \text{multiply}(cy, 0) + y(1 \bmod c) && (c > 1 \implies \lfloor 1/c \rfloor = 0)\\
&= 0 + y(1 \bmod c) && \text{(Base case)}\\
&= y(1 - c\lfloor 1/c \rfloor) = y(1) && (1).
\end{aligned}$$

Thus S_1. Now suppose S_m for all $m, z \in \mathbb{N}$ such that $m \leq z$. We will now show $S_m \implies S_{z+1}$.

$$\begin{aligned}
\text{multiply}(cy, \lfloor (z+1)/c \rfloor) + y((z+1) \bmod c) &= cy(\lfloor (z+1)/c \rfloor) + y((z+1) \bmod c) && \text{(Inductive hypothesis)}\\
&= cy\left(\frac{z + 1 - ((z+1) \bmod c)}{c}\right) + y((z+1) \bmod c) && (1)\\
&= y(z+1) - y((z+1) \bmod c) + y((z+1) \bmod c)\\
&= y(z+1).
\end{aligned}$$

Thus S_{z+1}. It follows by induction that S_z for all $c, y, z \in \mathbb{N}$ where $c \geq 2$. ■

1-8. Let A be a list where $A_{i \in [0,n]}$ for some $n \in \mathbb{N}$. Prove that $\text{horner}(A, x) = A_n x^n + A_{n-1}x^{n-1} + ... + A_1 x + A_0$.

Proof. Suppose A is a list where $A_{i \in [0,n]}$ for some $n \in \mathbb{N}$. Observe that

$$\begin{aligned}
\text{horner}(A, x) &= (...(((A_n)x + A_{n-1})x + A_{n-2})x + ... + A_1)x + A_0\\
&= (...((A_n x^2 + A_{n-1}x + A_{n-2})x + A_{n-3})x + ... + A_1)x + A_0\\
&= (A_n x^{n-1} + A_{n-1}x^{n-2} + ... + A_2 x + A_1)x + A_0 && \text{(Expanding)}\\
&= A_n x^n + A_{n-1}x^{n-1} + ... + A_1 x + A_0. && \blacksquare
\end{aligned}$$

1-9. Prove that for all $n \in \mathbb{N}$, $S_n : \text{bubblesort}(A : \text{list}[1, n]) = A'$ such that $A'[1] \leq A'[2] \leq ... \leq A'[n]$.

Proof. Suppose $n = 1$. Then $A = (A[1]) = A'$, thus S_1. Now suppose S_i for some $i, k \in \mathbb{N}$ where $i \leq k$. We will now show $S_i \implies S_{k+1}$. Let $i = k + 1$. Observe that the inner loop swaps the maximum $A[j]$ for $j \in [1, k+1]$ with $A[k+1]$. We assumed S_i for $i \leq k$, thus $A'[k+1] = \max(A[1], A[2], ..., A[k+1])$ and $A'[k] = \max(A[1], A[2], ..., A[k])$. Thus $A'[k] \leq A'[k+1]$ which implies S_{k+1}. It follows by induction that S_n for all $n \in \mathbb{N}$. ■