Exercise 1: Associativity (10 points)

Definition (1 pt)

Give the definition of associativity. What does it mean for an operator `f` to be associative?

Answer

$$\forall x, y, z \ : \ f(x, f(y, z)) = f(f(x, y), z)$$

Associativity and commutativity (1 pt)

Give an example operator that is associative but that is *not* commutative.

Answer

Some possible answers are: Matrix multiplication, String/list concatenation,

$$f(x, y) = x$$

An associative operator (8 pt)

Given two types `A` and `B`, and two *associative* operators `f` and `g` with the following signatures: `f: (A, A) => A`, `g: (B, B) => B`

Define a third operator `h` with the following signature: `h: ((A, B), (A, B)) => (A, B)` such that `h` is associative. (1 pt)

Then, prove that `h` is indeed associative. (7 pt)

Be **very precise** in your proof. At each step, specify which axiom, hypothesis, or previous result you use.

Answer

We define h as:

$$h((x_1, x_2), (y_1, y_2)) = (f(x_1, y_1), g(x_2, y_2))$$

We know that

$$\forall x, y, z \ : \ f(x, f(y, z)) = f(f(x, y), z)$$

$$\forall x, y, z \ : \ g(x, g(y, z)) = g(g(x, y), z)$$

We have to prove that

$$\forall x, y, z \ : \ h(x, h(y, z)) \stackrel{?}{=} h(h(x, y), z)$$

Replacing x by (x_1, x_2), and similarly for y and z:

$$\forall x_1, x_2, y_1, y_2, z_1, z_2 \;:\; h((x_1, x_2), h((y_1, y_2), (z_1, z_2))) \stackrel{?}{=} h(h((x_1, x_2), (y_1, y_2)), (z_1, z_2))$$

From here on, I will assume implicitly the $\forall$ quantification.

Replacing h by its definition, in the inner invocation, on both sides, yields:

$$h((x_1, x_2), (f(y_1, z_1), g(y_2, z_2))) \stackrel{?}{=} h((f(x_1, y_1), g(x_2, y_2)), (z_1, z_2))$$

Replacing h by its definition a second time, on both sides, yields:

$$(f(x_1, f(y_1, z_1)), g(x_2, g(y_2, z_2))) \stackrel{?}{=} (f(f(x_1, y_1), z_1), g(g(x_2, y_2), z_2))$$

Separating the equality of tuples into equality of their members:

$$f(x_1, f(y_1, z_1)) \stackrel{?}{=} f(f(x_1, y_1), z_1)$$
$$g(x_2, g(y_2, z_2)) \stackrel{?}{=} g(g(x_2, y_2), z_2)$$

Which is true because of f and g are associative.

QED