

fn make_int_to_bigint

Michael Shoemate

This proof resides in “**contrib**” because it has not completed the vetting process.

Proves soundness of the implementation of `make_int_to_bigint` in `mod.rs` at commit `f5bb719` (outdated¹).

1 Hoare Triple

Precondition

Compiler-Verified

- Generic T implements trait `SaturatingCast<IBig>`

User-Verified

None

Pseudocode

```
1 def make_int_to_bigint(  
2   input_space: tuple[VectorDomain[AtomDomain[T]], LpDistance[P, QI]],  
3 ) -> Transformation[  
4   VectorDomain[AtomDomain[T]],  
5   VectorDomain[AtomDomain[IBig]],  
6   LpDistance[P, QI],  
7   LpDistance[P, RBig],  
8 ]:  
9   input_domain, input_metric = input_space  
10  def stability_map(d_in):  
11      try:  
12          return RBig.try_from(d_in)  
13      except:  
14          raise f"d_in ({d_in}) must be finite"  
15  
16  return Transformation.new(  
17      input_domain,  
18      VectorDomain(  
19          element_domain=AtomDomain.default(IBig),  
20          size=input_domain.size,  
21      ),  
22      Function.new(lambda x: [IBig.from_(x_i) for x_i in x]),  
23      input_metric,  
24      LpDistance.default(),  
25      StabilityMap.new_fallible(stability_map),  
26  )
```

¹See new changes with `git diff f5bb719..d5ac0b48 rust/src/measurements/noise/nature/integer/mod.rs`

Postcondition

Theorem 1.1.

Theorem 1.2. For every setting of the input parameters (T) to `make_int_to_bigint` such that the given preconditions hold, `make_int_to_bigint` raises an exception (at compile time or run time) or returns a valid transformation. A valid transformation has the following properties:

1. (Appropriate output domain). For every element x in `input_domain`, `function(x)` is in `output_domain` or raises a data-independent runtime exception.
2. (Stability guarantee). For every pair of elements x, x' in `input_domain` and for every pair (d_in, d_out) , where d_in has the associated type for `input_metric` and d_out has the associated type for `output_metric`, if x, x' are d_in -close under `input_metric`, `stability_map(d_in)` does not raise an exception, and `stability_map(d_in) ≤ d_out`, then `function(x), function(x')` are d_out -close under `output_metric`.

Proof. By the definition of the function on line ??, and since `IBig.from` is infallible, the function is infallible, meaning that the function cannot raise data-dependent errors. The function also always returns a vector of `IBigs`, of the same length as the input, meaning the output of the function is always a member of the output domain, as defined on line ??. Finally, the function is 1-stable, because the real values of the numbers remain un-changed, meaning the distance between adjacent inputs always remains the same, satisfying the stability property. \square