fn make_fully_adaptive_composition

Michael Shoemate

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

Proves soundness of `fn make_fully_adaptive_composition`.

1 Hoare Triple

Precondition

Compiler-verified

- Argument `input_domain` of type `DI`.
- Argument `input_metric` of type `MI`.
- Argument `output_measure` of type `MO`.
- Generic `DI` implements `Domain`.
- Generic `MI` implements `Metric`.
- Generic `MO` implements `CompositionMeasure`.
- `(DI, MI)` implements `MetricSpace`.

Caller-verified

None

Pseudocode

```
def make_fully_adaptive_composition(
    input_domain: DI,
    input_metric: MI,
    output_measure: MO,
) -> Odometer[DI, MI, MO, Measurement[DI, MI, MO, TO], TO]:

    # check if fully adaptive composition is supported
    output_measure.composability(Adaptivity.FullyAdaptive)

    def function(
        arg: DI_Carrier,
    ) -> OdometerQueryable[Measurement[DI, MI, MO, TO], TO, MO_Distance]:
        return new_fully_adaptive_composition_queryable(
            input_domain, input_metric, output_measure, arg
        )

    return Odometer.new(
        input_domain, input_metric, output_measure, Function.new_fallible(function)
    )
```

Postcondition

Theorem 1.1. For every setting of the input parameters `(input_domain, input_metric, output_measure, DI, MI, MO, TO)` to `make_fully_adaptive_composition` such that the given preconditions hold, `make_fully_adaptive_com` raises an error (at compile time or run time) or returns a valid odometer. A valid odometer has the following properties:

1. (Data-independent runtime errors). For every pair of members x and x' in `input_domain`, `invoke`(x) and `invoke`(x') either both return the same error or neither return an error.

2. (Valid odometer queryable). For every member x in `input_domain`, where `function`(x) does not raise an error, `function`(x) returns a valid odometer queryable.

Proof of data-independent errors. Errors are data-independent by the the postcondition of `new_sequential_odometer_query`

□

Proof of valid odometer queryable. Under the assumption that the input data is a member of the input domain, the precondition of `new_fully_adaptive_composition_queryable` is met, so by its postcondition the return is a valid odometer queryable. □