

CompositionMeasure for RenyiDivergence

Michael Shoemate

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

Proves soundness of the implementation of **CompositionMeasure** for **RenyiDivergence** in **mod.rs** at **commit f5bb719** (outdated¹).

1 Hoare Triple

Precondition

Compiler-Verified

Types matching pseudocode.

Caller-Verified

None

Pseudocode

```
1 class CompositionMeasure(RenyiDivergence):
2     def composability( #
3         self, adaptivity: Adaptivity
4     ) -> Composability:
5         return Composability.Concurrent
6
7     def compose(self, d_mids: Vec[Self_Distance]) -> Self_Distance:
8         def curve(alpha: float) -> float: #
9             epsilons = [d_mid(alpha) for d_mid in d_mids]
10
11             d_out = 0.0
12             for d_mid in epsilons:
13                 d_out = d_out.inf_add(d_mid)
14             return d_out
15
16         return Function.new_fallible(curve)
```

Postcondition

Theorem 1.1. **composability** returns **Ok(out)** if the composition of a vector of privacy parameters **d_mids** is bounded above by **self.compose(d_mids)** under **adaptivity** **adaptivity** and **out-composability**. Otherwise returns an error.

Proof. The new curve constructed on line 8 composes all epsilon parameters at a given fixed **alpha**. By the postcondition of **InfAdd** we have that for any choice of **alpha**, $\sum_i d_mid_i(\alpha) \leq \text{compose}(d_mids)(\alpha)$.

¹See new changes with `git diff f5bb719..b4e9d3e rust/src/combinators/sequential_composition/mod.rs`

| Adaptivity | Sequential | Concurrent |
|----------------|----------------------|--------------------|
| Non-Adaptive | Proposition 1[Mir17] | Theorem 2[Lyu22] |
| Adaptive | - | - |
| Fully-Adaptive | Theorem 4.3[FZ22] | Theorem 1.22[VW21] |

This table is reflected in the implementation of `composability` on line 2.

□

References

- [FZ22] Vitaly Feldman and Tijana Zrnic. Individual privacy accounting via a renyi filter, 2022.
- [Lyu22] Xin Lyu. Composition theorems for interactive differential privacy, 2022.
- [Mir17] Ilya Mironov. Rényi differential privacy. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, page 263–275. IEEE, August 2017.
- [VW21] Salil Vadhan and Tianhao Wang. Concurrent composition of differential privacy, 2021.