CompositionMeasure for ZeroConcentratedDivergence

Michael Shoemate

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

Proves soundness of the implementation of `CompositionMeasure` for `ZeroConcentratedDivergence` in `mod.rs` at commit f5bb719 (outdated[1]).

1 Hoare Triple

Precondition

Compiler-Verified

Types matching pseudocode.

Caller-Verified

None

Pseudocode

```
class CompositionMeasure(ZeroConcentratedDivergence):
    def composability(  #
        self, adaptivity: Adaptivity
    ) -> Composability:
        match adaptivity:
            case Adaptivity.FullyAdaptive:
                return Composability.Sequential
            case _:
                return Composability.Concurrent

    def compose(self, d_mids: Vec[Self_Distance]) -> Self_Distance:
        d_out = 0.0
        for d_mid in d_mids:
            d_out = d_out.inf_add(d_mid)
        return d_out
```

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. By the postcondition of `InfAdd` we have that $\sum_i \texttt{d\_mids}_i \leq \texttt{compose(d\_mids)}$.

[1] See new changes with `git diff f5bb719..991c3fb5 rust/src/combinators/sequential_composition/mod.rs`

Adaptivity	Sequential	Concurrent
Non-Adaptive	Lemma 1.7[BS16]	Corollary 1[Lyu22]
Adaptive	Lemma 1.7[BS16]	Corollary 1[Lyu22]
Fully-Adaptive	Remark 4.4[FZ22]	None

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

□

References

[BS16] Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds, 2016.

[FZ22] Vitaly Feldman and Tijana Zrnic. Individual privacy accounting via a renyi filter, 2022.

[Lyu22] Xin Lyu. Composition theorems for interactive differential privacy, 2022.