CompositionMeasure for Approximate<MaxDivergence>

Michael Shoemate

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

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` in `mod.rs` at commit f5bb719 (outdated[1]).

1 Hoare Triple

Precondition

Compiler-Verified

Types matching pseudocode.

Caller-Verified

None

Pseudocode

```
class CompositionMeasure(ApproximateMaxDivergence):
    def composability(  #
        self, adaptivity: Adaptivity
    ) -> Composability:
        if matches(adaptivity, Adaptivity.FullyAdaptive):
            raise "fully-adaptive composition is not currently supported for max-divergence"
        return Composability.Concurrent

    def compose(self, d_mids: Vec[Self_Distance]) -> Self_Distance:
        eps_g, del_g = 0.0, 0.0
        for eps_i, del_i in d_mids:
            eps_g = eps_g.inf_add(eps_i)
            del_g = del_g.inf_add(del_i)
        return eps_g, del_g
```

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 $\sum_i \texttt{d\_mids}_i \leq \texttt{compose(d\_mids)}$, where the summation is applied independently to epsilons and deltas, and the comparison applies to both the global epsilon and global delta.

[1] See new changes with `git diff f5bb719..d7a6cc0 rust/src/combinators/sequential_composition/mod.rs`

Adaptivity	Sequential	Concurrent
Non-Adaptive	Theorem 1[DKM+06]	Theorem 1.3[VZ23]
Adaptive	Theorem 1[DKM+06]	Theorem 1.3[VZ23]
Fully-Adaptive	Lemma 3.5[RRUV21]	Theorem 1.3[VZ23]

The reference for fully adaptive sequential composition is specifically for the version of the paper prior to correction (v1, not v2). The correction is not necessary for the privacy proof when odometers are defined in terms of a truncated view.

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

□

References

[DKM+06] Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, and Moni Naor. Our data, ourselves: Privacy via distributed noise generation. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, pages 486–503, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[RRUV21] Ryan Rogers, Aaron Roth, Jonathan Ullman, and Salil Vadhan. Privacy odometers and filters: Pay-as-you-go composition, 2021.

[VZ23] Salil Vadhan and Wanrong Zhang. Concurrent composition theorems for differential privacy. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC '23, page 507–519. ACM, June 2023.