CompositionMeasure for MaxDivergence

Michael Shoemate

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

Proves soundness of the implementation of `CompositionMeasure` for `MaxDivergence` in `mod.rs` at commit f5bb719 (outdated[1]).

1 Hoare Triple

Precondition

Compiler-Verified

Types matching pseudocode.

Caller-Verified

None

Pseudocode

```
class CompositionMeasure(MaxDivergence):
    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:
        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 $\sum_i \texttt{d\_mids}_i \leq \texttt{compose(d\_mids)}$.

Adaptivity	Sequential	Concurrent
Non-Adaptive	Theorem 1[DMNS06]	Theorem 1.8[VW21]
Adaptive	Theorem 1[DMNS06]	Theorem 1.8[VW21]
Fully-Adaptive	None	None

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

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

□

References

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 265–284, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[VW21] Salil Vadhan and Tianhao Wang. Concurrent composition of differential privacy, 2021.