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soundness of the implementation of CompositionMeasure for ZeroConcentratedDivergence in mod.rs at commit f5bb719 (outdated[1]).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

```python
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.

Definition 1.2 (Definition of `ZeroConcentratedDivergence`)**.** For any two distributions Y, Y' and any non-negative d, Y, Y' are d-close under the zero-concentrated divergence measure if, for every possible choice of $\alpha \in (1, \infty)$,

[1] See new changes with `git diff f5bb719..4850993 rust/src/combinators/sequential_composition/mod.rs`

$$D_\alpha(Y, Y') = \frac{1}{1-\alpha}\mathbb{E}_{x\sim Y'}\left[\ln\left(\frac{\Pr[Y=x]}{\Pr[Y'=x]}\right)^\alpha\right] \leq d \cdot \alpha. \tag{1}$$

Lemma 1.3. 1. $\mathcal{F}(\rho_1, \rho_2, \dots; \rho) = \mathbb{I}(\sum_i \rho_i \leq \rho)$ is a valid ρ-zCDP IM-filter.

2. $\mathcal{G}(\rho_1, \dots, \rho_k) = \sum_{i=1}^k \rho_i$ is a valid ρ-zCDP IM-privacy loss accumulator.

Proof. For any fixed choice of $\alpha > 1$, we have that $\mathcal{F}(\rho_1, \rho_2, \dots; \rho) = \mathbb{I}(\sum_i \epsilon_i/\alpha/ \leq \epsilon/\alpha)$, by 1.2, which by Theorem 1.22[VW21] is a valid (α, ϵ)-RDP IM-filter.

Similarly, for any fixed choice of $\alpha > 1$, we have that $\mathcal{G}(\rho_1, \dots, \rho_k) = \sum_i \epsilon_i/\alpha \leq \epsilon/\alpha$, by 1.2, which by Theorem 1.22[VW21] is a valid (α, ϵ)-RDP IM-privacy loss accumulator. □

Proof. By the postcondition of `InfAdd` we have that $\sum_i$ `d_mids`$_i \leq$ `compose(d_mids)`.

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]	1.3

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.

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