impl TopKMeasure for MaxDivergence

Tudor Cebere Michael Shoemate

October 8, 2025

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

This document proves soundness of `TopKMeasure` for `MaxDivergence` in `mod.rs` at commit e62b0aa2 (outdated[1]).

1 Hoare Triple

Precondition

Compiler-verified

- Associated Const `REPLACEMENT = false`
- Method `privacy_map`
  Types consistent with pseudocode.

Caller-verified

- Method `privacy_map`
  - `d_in` is non-null and positive.
  - `scale` is non-null and positive.

Pseudocode

```
# MaxDivergence
REPLACEMENT = False

def privacy_map(d_in: f64, scale: f64) -> f64:
    return d_in.inf_div(scale)
```

Postcondition

Theorem 1.1. The implementation is consistent with the associated items in the `TopKMeasure` trait.

1. Method `privacy_map`: For any x, x' where $d_{\text{in}} \geq d_{\text{Range}}(x, x')$, return $d_{\text{out}} \geq D_{\text{self}}(f(x), f(x'))$, where $f(x) = \text{noisy\_top\_k}(x = x, k = 1, \text{scale} = \text{scale}, \text{replacement} = \text{Self :: REPLACEMENT})$.

Proof. Since `Self::REPLACEMENT` is false, then by the postcondition of `noisy_top_k`, `noisy_top_k` returns a sample from $\mathcal{M}_{PF}$. In the case that scores are not monotonic, by [1] Theorem 1, $\mathcal{M}_{PF}$ satisfies ϵ-DP, because the range distance is equal to $2 \cdot \Delta$. Otherwise in the case that scores are monotonic, by [1] Remark 1, $\mathcal{M}_{PF}$ satisfies $\epsilon/2$-DP, but the range distance is equal to Δ, thus satisfying ϵ-DP. □

[1] See new changes with `git diff e62b0aa2..f81c577 rust/src/measurements/noisy_top_k/mod.rs`

References

[1] Ryan McKenna and Daniel Sheldon. Permute-and-flip: A new mechanism for differentially private selection, 2020.