

impl SelectionMeasure for RangeDivergence

Michael Shoemate

March 18, 2025

1 Hoare Triple

Precondition

Compiler-verified

- Associated Type RV
 - RV must implement trait `InverseCDF`.
- Method `random_variable` *Types consistent with pseudocode.*
- Method `privacy_map` *Types consistent with pseudocode.*

Caller-verified

- Associated Type RV (*no caller verified preconditions*)
- Method `random_variable`
 - `scale` is positive (*cannot be null due to `FBig` dtype*).
- Method `privacy_map`
 - `d_in` is non-null and non-negative.
 - `scale` is non-null and non-negative.

Pseudocode

```
1 class RangeDivergence(SelectionMeasure):
2     ONE_SHOT = True
3     RV = GumbelRV
4
5     @staticmethod
6     def random_variable(shift: FBig, scale: FBig) -> GumbelRV:
7         return GumbelRV(shift=shift, scale=scale)
8
9     @staticmethod
10    def privacy_map(d_in: f64, scale: f64, k: usize) -> f64:
11        if d_in < 0:
12            raise ValueError("input distance must be non-negative")
13
14        if scale.is_zero():
15            return f64.INFINITY
16
17        return d_in.inf_div(scale).inf_mul(f64.inf_cast(k))
```

Postcondition

Theorem 1.1. The implementation is consistent with all associated items in the **SelectionMeasure** trait.

1. Associated Type RV
2. Method `random_variable`
3. Method `privacy_map`

Definition 1.2. A random variable follows the Gumbel distribution if it has density

$$f(x) = \frac{1}{\beta} e^{-e^{-e^{-z}} - z} \quad (1)$$

where $z = \frac{x-\mu}{\beta}$, μ is the location parameter and β is the scale parameter.

Proof of valid associated type: RV. The associated type RV is defined as **GumbelRV**, which represents a random variable following the Gumbel distribution 1.2. The compiler verifies that **GumbelRV** implements the **InverseCDF** trait. \square

Proof of valid method: `random_variable`. By the precondition on `scale` being positive, `random_variable` returns a valid instance of **GumbelRV**. \square

Proof of valid method: `privacy_map`. By Lemma 4.2 of [2], $\mathcal{M}_{\text{Gumbel}}^k(x)$ is equal in distribution to the peeling exponential mechanism, which is the k-fold composition of the exponential mechanism. Proposition 2 of [1] shows that the exponential mechanism satisfies the RangeDivergence privacy guarantee. \square

References

- [1] Jinshuo Dong, David Durfee, and Ryan Rogers. Optimal differential privacy composition for exponential mechanisms and the cost of adaptivity. *CoRR*, abs/1909.13830, 2019.
- [2] David Durfee and Ryan Rogers. Practical differentially private top-k selection with pay-what-you-get composition. *CoRR*, abs/1905.04273, 2019.