

# impl TopKMeasure for ZeroConcentratedDivergence

Michael Shoemate

August 20, 2025

## 1 Hoare Triple

### Precondition

#### Compiler-verified

- Method `noisy_top_k` *Types consistent with pseudocode.*
- Method `privacy_map` *Types consistent with pseudocode.*

#### Caller-verified

- Method `noisy_top_k`
  - `x` elements are non-null.
  - `scale` is finite and non-negative.
- Method `privacy_map`
  - `d_in` is non-null and positive.
  - `scale` is non-null and positive.

### Pseudocode

```
1 class ZeroConcentratedDivergence(TopKMeasure):
2     @staticmethod
3     def noisy_top_k(x: list[TIA], scale: f64, k: usize, negate: bool) -> list[usize]:
4         return gumbel_top_k(x, scale, k, negate)
5
6     @staticmethod
7     def privacy_map(d_in: f64, scale: f64) -> f64:
8         return d_in.inf_div(scale).inf_powi(ibig(2)).inf_div(8.0)
```

### Postcondition

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

#### 1. Method `noisy_top_k`:

- Returns the index of the top element  $z_i$ , where each  $z_i \sim \text{DISTRIBUTION}(\text{shift} = y_i, \text{scale} = \text{scale})$ , and each  $y_i = -x_i$  if `negate`, else  $y_i = x_i$ ,  $k$  times with removal.
- Errors are data-independent, except for exhaustion of entropy.

#### 2. 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 $f(x) = \text{noisy\_top\_k}(x, k = 1, \text{scale} = \text{scale})$ .

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

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

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

*Proof of postcondition: `noisy_top_k`.* The preconditions of `gumbel_noisy_max` are met, therefore by the postcondition of `gumbel_top_k`, the postcondition of `noisy_top_k` is satisfied.  $\square$

*Proof of postcondition: `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 zCDP 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.