fn make_tulap

Yu-Ju Ku, Jordan Awan, Aishwarya Ramasethu, Michael Shoemate

November 20, 2024

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

Proves soundness of make_tulap. make_tulap accepts parameters input_domain and input_metric specifying the input metric space. This consists of the space of non-null floating-point numbers, where distance is computed via the absolute distance.

Additionally, the privacy parameters epsilon (of type float) and delta are fixed the privacy loss. The measurement assumes (but does not require) that input data (arg) follows the Binomial Distribution, and returns a sample from the Tulap distribution centered at arg.

1 Hoare Triple

Preconditions

Compiler-verified

- Argument input_domain is of type AtomDomain<f64>.
- Argument input_metric is of type AbsoluteDistance<f64>.
- Argument epsilon is of type float
- Argument delta is of type float

Human-verified

None

Pseudocode

```python
def make_tulap(
    input_domain: AtomDomain[float],
    input_metric: AbsoluteDistance[float],
    epsilon: float,
    delta: float,
):
    assert not input_domain.nullable(), "input data must be non-null"
    assert epsilon >= 0 and delta >= 0, "epsilon and delta must not be negative"
    assert delta <= 1, "delta must not exceed 1"

    def function(arg: float) -> float:  #
        # inverse transform sampling of Tulap
        arg = arg or 0.0  # for robustness against NaN inputs
        tulap = TulapRV(shift=arg, epsilon=epsilon, delta=delta)
        return tulap.sample().value()
    def privacy_map(d_in: float) -> float:  #
        assert 0 <= d_in <= 1
        if d_in == 0:
            return (0.0, 0.0)
        return epsilon, delta

    return Measurement(
        input_domain,
        function,
        input_metric,
        output_measure=dp.fixed_smoothed_max_divergence(),
        privacy_map=privacy_map,
    )
```

Postcondition

Theorem 1.1. For every setting of the input parameters (`input_domain`, `input_metric`, `epsilon`, `delta`) to `make_tulap` such that the given preconditions hold, `make_tulap` raises an exception (at compile time or run time) or returns a valid measurement. A valid measurement has the following property:

1. (Privacy guarantee). For every pair of elements x, x' in `input_domain` and for every pair (`d_in`, `d_out`), where `d_in` has the associated type for `input_metric` and `d_out` has the associated type for `output_measure`, if x, x' are `d_in`-close under `input_metric`, `privacy_map(d_in)` does not raise an exception, and `privacy_map(d_in)` $\leq$ `d_out`, then `function`(x), `function`(x') are `d_out`-close under `output_measure`.

2 Proof

Proof. **(Privacy guarantee.)**

`PartialSample.value`, hereafter referred to as just `value` (a function) can only fail when the pseudorandom byte generator used in its implementation fails due to lack of system entropy. This is usually related to the computer's physical environment and not the dataset. The rest of this proof is conditioned on the assumption that `value` does not raise an exception.

A canonical noise distribution (CND) (Awan and Vadhan 2023), captures whether a real-valued distribution is perfectly tailored to satisfy . We formalize this in Definition 1 (Awan and Vadhan 2023)". The definition uses T which is the tradeoff function of *type*1 and *type*2 errors between two distributions. A larger T would mean it is harder to distiguish between two distributions.

Definition 1. *Awan and Vadhan 2023, Definition 3.1*
Let f be a symmetric nontrivial tradeoff function. A continuous distribution function F is a canonical noise distribution *(CND) for f if*

(1) for every statistic $S : X^n \to \mathbb{R}$ with sensitivity $\Delta > 0$, and $N \sim F(\cdot)$, the mechanism $S(X) + \Delta N$ satisfies f-DP. Equivalently, for every $m \in [0, 1]$, $T(F(\cdot), F(\cdot - m)) \geq f$,

(2) $f(\alpha) = T(F(\cdot), F(\cdot - 1))(\alpha)$ for all $\alpha \in (0, 1)$,

(3) $T(F(\cdot), F(\cdot - 1))(\alpha) = F(F^{-1}(1 - \alpha) - 1)$ for all $\alpha \in (0, 1)$,

(4) $F(x) = 1 - F(-x)$ for all $x \in \mathbb{R}$; that is, F is the cdf of a random variable which is symmetric about zero.

Definition 2. *Awan and Vadhan 2023, Definition 3.7*
Let f be a symmetric nontrivial tradeoff function, and let $c \in [0, 1/2)$ be the unique fixed point of f: $f(c) = c$.

We define $F_f : \mathbb{R} \to \mathbb{R}$ as

$$F_f(x) = \begin{cases} f(1 - F_f(x+1)) & x < -1/2 \\ c(1/2 - x) + (1-c)(x+1/2) & -1/2 \leq x \leq 1/2 \\ 1 - f(F_f(x-1)) & x > 1/2. \end{cases}$$

In Definition 2 (Awan and Vadhan 2023), the fact that there is a unique fixed point follows from the fact that f is convex and decreasing f-DP (Dong, Roth, and Su 2022), and so intersects the line $y = \alpha$ at a unique value. Note that in Definition 2 (Awan and Vadhan 2023), the cumulative distribution function (CDF) corresponds to a uniform random variable on the interval $[-1/2, 1/2]$. However, due to the recursive nature of F_f and the fact that f is generally non-linear, the Canonical Noise Distribution (CND) from Definition 2 (Awan and Vadhan 2023) need not be uniformly distributed on any other intervals.

Theorem 1 (Awan and Vadhan 2023) below states that for any nontrivial tradeoff function, this construction yields a CND, which can be constructed as in Definition 2 (Awan and Vadhan 2023). This CND can be used to add perfectly calibrated noise to a statistic to achieve f-DP (Dong, Roth, and Su 2022, Proposition 2.2).

Theorem 1. Awan and Vadhan 2023, Theorem 3.9
Let f be a symmetric nontrivial tradeoff function and let F_f be as in Definition 2 (Awan and Vadhan 2023). Then, as stated in (Awan and Vadhan 2023, Theorem 3.9), F_f is a canonical noise distribution for f.

In Definition 2 (Awan and Vadhan 2023), we explained the cdf of the CND we made. This explanation helps us understand the distribution's features, but when it comes to sampling, the quantile function is key. In Proposition 1 (Awan and Vadhan 2023) provides a recursive formula for the CND's quantile function, as described in Definition 1 (Awan and Vadhan 2023), and show that we can finish it in just a few steps.

Proposition 1. *Awan and Vadhan 2023, Proposition F.6*
Let f be a symmetric nontrivial tradeoff function and let F_f be as in Definition 2. Then the quantile function $F_f^{-1} : (0,1) \to \mathbb{R}$ for F_f can be expressed as

$$F_f^{-1}(u) = \begin{cases} F_f^{-1}(1 - f(u)) - 1 & u < c \\ \frac{u - 1/2}{1 - 2c} & c \leq u \leq 1 - c \\ F_f^{-1}(f(1-u)) + 1 & u > 1 - c, \end{cases}$$

where c is the unique fixed point of f. Furthermore, for any $u \in (0,1)$, the expression $Q_f(u)$ takes a finite number of recursive steps to evaluate. Thus, if $U \sim U(0,1)$, then $F_f^{-1}(U) \sim F_f$.

According to Corollary 3.10 in Awan and Vadhan 2023, the distribution Tulap$(0, b, q)$, where $b = \exp(-\epsilon)$ and $q = \frac{2\delta b}{1 - b + 2\delta b}$ is a CND for $f_{\epsilon,\delta}$-DP, which agrees with the construction of Definition 2 (Awan and Vadhan 2023).

From the definition, it is easy to verify that the cdf of a Tulap random variable agrees with F_f on $[-1/2, 1/2]$. Tulap cdf also satisfies the recurrence relation of Definition 2 (Awan and Vadhan 2023). Note that the cdf of Tulap$(0, b, 0)$ is

$$F_{N_0}(x) = \begin{cases} \frac{b^{-[x]}}{1+b}(b + \{x - [x] + 1/2\}(1-b)) & x \leq 0 \\ 1 - \frac{b^{[x]}}{1+b}(b + \{[x] - x + 1/2\}(1-b)) & x > 0, \end{cases}$$

where $[x]$ is the nearest integer function. The cdf of Tulap$(0, b, q)$ is

$$F_N(x) = \begin{cases} 0 & F_{N_0}(x) < q/2 \\ \frac{F_{N_0}(x) - q/2}{1-q} & q/2 \leq F_{N_0}(x) \leq 1 - q/2 \\ 1 & F_{N_0}(x) > 1 - q/2. \end{cases}$$

By inspection, the fixed point of $f_{\epsilon,\delta}$ is $c = \frac{1-\delta}{1+e^{\epsilon}}$. It is easy to verify that $F_N(x) = c(1/2-x)+(1-c)(x+1/2)$ for $x \in (-1/2, 1/2)$. We then have that F_N satisfies the recurrence relation in Definition 2 (Awan and Vadhan 2023). We conclude that $F_N = F_f$ and that F_N is a CND for N. Therefore, The distribution Tulap$(0, b, q)$ satisfies (ϵ, δ)-DP. □

References

Awan, Jordan and Salil Vadhan (2023). "Canonical Noise Distributions and Private Hypothesis Tests". In: *The Annals of Statistics* 51.2, pp. 547–572.

Dong, Jinshuo, Aaron Roth, and Weijie J. Su (2022). "Gaussian Differential Privacy". In: *Journal of the Royal Statistical Society Series B: Statistical Methodology* 84.1, pp. 3–37. ISSN: 1369-7412.