fn make_base_tulap

Yu-Ju Ku, Jordan Awan

August 21, 2023

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

Proves soundness of make_base_tulap in

`make_base_tulap` accepts a parameter `m` of type `float`, which is a rational number, a parameter `b` of type `float`, which is greater than 0 and less than 1, and a parameter `q` of type `float`, which is greater than or equal to 0 and less than 1. The function on the resulting measurement takes in float data points that follow Binomial Distribution `arg` and returns the probability `prob`, or the complement `!arg` with probability $1 - \texttt{prob}$.

PR History

- Pull Request #

1 Hoare Triple

Preconditions

- Variable `b` must be of type `float`
- Variable `scale` must be of type `float`
- Type `float` must have trait SampleDiscreteLaplaceZ2k

Pseudocode

```
def make_base_tulap(b: float, scale: float):
    input_domain = AllDomain(float)
    input_metric = AbsoluteDistance(float)
    output_measure = SmoothedMaxDivergence(float)

    def privacy_map(d_in: float) -> float:
        if d_in == 0 or d_out > scale:  # check that delta <= scale
            return 0
        else:
            return d_out

    def qCND(u, f, c):          # CND quantile function for f
        if u < c:
            return qCND(1 - f(u), f, c) - 1
        elif c <= u <= 1-c: # the linear function
            return (u - 1/2)/(1 - 2*c)
        else:
            return qCND(f(1-u),f ,c) + 1
```

```
    def function(epsilon: float, delta: float) -> float:

        # inverse transform sampling of Tulap
        prob = b
        unif = sample_standard_uniform(prob)
        c = (1 - delta) / (1 + exp(epsilon))
        f = max(0, 1 - delta - exp(epsilon) * unif, exp(-epsilon) * (1 - delta - unif))
        samples = qCND(unif, f, c)
        return samples

    return Measurement(input_domain, function, input_metric, output_measure, privacy_map)
```

Postcondition

For every setting of the input parameters `(prob, m, b, q, QO)` to `make_base_tulap` such that the given preconditions hold, `make_base_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 u, v 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 u, v are `d_in`-close under `input_metric` and `privacy_map`(`d_in`) $\leq$ `d_out`, then `function`(u), `function`(v) are `d_out`-close under `output_measure`.

2 Proof

Proof.

1. **(Domain-metric compatibility.)** For `make_base_tulap`, this corresponds to showing `AllDomain(bool)` is compatible with `DiscreteMetric`. This follows directly from the definition of `DiscreteMetric`.

2. **(Privacy guarantee.)**

   > **Note 1** (Proof relies on correctness of Discrete Laplace sampler and Uniform sampler)**.** The following proof makes use of the following lemmas that asserts the correctness of the Discrete Laplace sampler and Uniform sampler function.
   >
   > **Lemma 2.1.** If system entropy is insufficient, `sample_discrete_laplace_Z2k` raises an error. Otherwise, `sample_discrete_laplace_Z2k(shift, scale, k)`, the Discrete Laplace sampler function used in `make_base_tulap`, returns sample from the discrete laplace distribution on $\mathbb{Z} \cdot 2^k$.
   >
   > **Lemma 2.2.** If system entropy is insufficient, `sample_standard_uniform` raises an error. Otherwise, `sample_standard_uniform(constant_time)`, the Uniform sampler function used in `make_base_tulap`, returns sample drawn from Uniform[0,1).

   `sample_discrete_laplace_Z2k` and `sample_standard_uniform` can only fail when the OpenSSL 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 `sample_discrete_laplace_Z2k` and `sample_standard_uniform` does not raise an exception.
   The concept canonical noise distribution (CND)(Awan and Vadhan 2023), which captures whether a

real-valued distribution is perfectly tailored to satisfy f-DP(Dong, Roth, and Su 2022). We formalize this in Definition 1(Awan and Vadhan 2023).

Definition 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 $S : X^n \to$ 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 $x \in$; that is, F is the cdf of a random variable which is symmetric about zero.

Definition 2. *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, 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).

Theorem 1. Let f be a symmetric nontrivial tradeoff function and let F_f be as in Definition 2 (Awan and Vadhan 2023). Then 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. *Let f be a symmetric nontrivial tradeoff function and let F_f be as in Definition* **??**. *Then the quantile function $F_f^{-1} : (0, 1) \to$ 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 citeawan2023canonical, the distribution Tulap$(0, b, q)$, where $b = \exp(-)$ and $q = \frac{2b}{1-b+2b}$ is a CND for f,-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$(0, b, q)$ is privacy guaranteed.

□

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.