Harvard Privacy Tools Project

Gaussian Mechanism Accuracy

April 23, 2020

Definition 1. Let z be the true value of the statistic and let X be the random variable the noisy release is drawn from. Let α be the statistical significance level, and let $Y = |X - z|$. Then, accuracy a for statistical significance level α is the a s.t.

$$\alpha = \Pr[Y > a].$$

Theorem 1. *The accuracy of an ϵ-differentially private release from the geometric mechanism on a function with sensitivity Δ_1, at statistical significance level α is*

$$a = \lceil \frac{\Delta_1}{\epsilon} \ln(1/\alpha) \rceil.$$

[BV17, GRS12]

Proof. This follows directly from the proof of accuracy for the Laplace mechanism, with the observation that the geometric mechanism is simply a discretization of the Laplace mechanism, hence the ceiling in the accuracy statement. □

0.1 A note on converting from accuracy to privacy

We offer the ability to convert from an accuracy guarantee to a privacy guarantee in our system. In the context of the geometric mechanism, it is not entirely clear what that conversion would mean, since for a set accuracy level a and significance level α, there are a range of possible values for ϵ. Since this range of ϵ depends on both a *and* α, rather than choosing the minimum or maximum over the range of ϵ's we instead use the original accuracy guarantee from the Laplace mechanism (i.e. the geometric mechanism's accuracy guarantee without the ceiling) to convert from statements about accuracy to statements about privacy:

$$\epsilon = \frac{\Delta_1}{a} \ln(1/\alpha).$$

One might argue that in general we shouldn't take the ceiling when determining the accuracy, since the additional information might be useful to an end-user. For example, if a user is attempting to determine how much budget to give a query, and they first ask

for accuracy for an ϵ that gives (without the ceiling) $a = 3.02$, they might determine to increase the amount of accuracy to get the accuracy guarantee to $a = 3$. If instead we take the ceiling, they would get back $a = 4$ and not know that a (theoretical) small change in ϵ would lead to a noticeable improvement in their accuracy guarantee.

References

[BV17] Victor Balcer and Salil Vadhan. Differential privacy on finite computers. *arXiv preprint arXiv:1709.05396*, 2017.

[GRS12] Arpita Ghosh, Tim Roughgarden, and Mukund Sundararajan. Universally utility-maximizing privacy mechanisms. *SIAM Journal on Computing*, 41(6):1673–1693, 2012.