TwoRavens

Visualization of Uncertainty Introduced by Differential Privacy

Jessica Bu

Wellesley College

Privacy Tools for Sharing Research Data

A National Science Foundation Secure and Trustworthy Cyberspace Project

with additional support from the Sloan Foundation and Google, Inc.

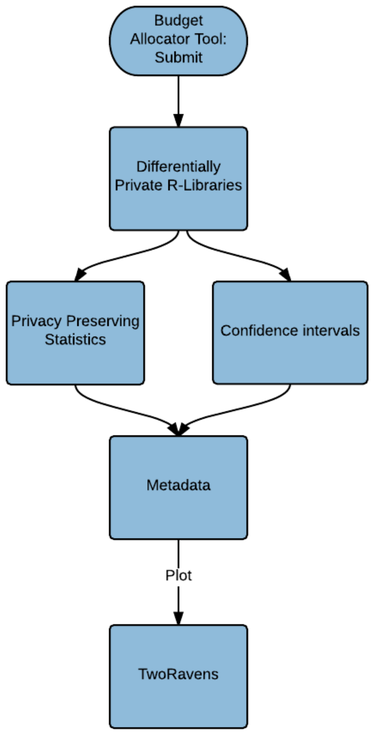
INTRODUCTION

The idea behind differential privacy, a method of anonymization, is to ensure that results derived from a database look the same whether or not it contains a given individual's data. It works by adding precisely constructed random noise to the data such that statistical results do not reveal any individual-level information, while remaining useful to researchers. As a result, however, a certain degree of uncertainty is introduced into the results.

OBJECTIVE

My objective was to communicate the uncertainty introduced by differentially private mechanisms in the graphical data exploration tool TwoRavens, which integrates with the statistical software package Zelig and the data repository Dataverse. Visualizing uncertainty in TwoRavens allows users to be aware of and understand the utility of the perturbed results.

METHOD



METHOD

Budget Allocator Tool:

Data depositors and analysts use the budget allocator tool to select the statistics they would like to calculate, and to distribute a global privacy budget across these statistics.

Private Zelig:

Privacy preserving statistics

Differentially private versions of the statistical summaries selected by the depositor are drawn from an R library of differentially private mechanisms.

statistic.release
Input:
eps – epsilon privacy parameter
data – vector of data
remainder of arguments dependent on type of statistic
Output:
A list of two variables: release and params.
release – privacy preserving statistic
params – list of the parameters that were passed into the release function (eps, del, etc.), in addition to n (the number of elements in the data), but excluding data

Confidence intervals

Confidence intervals for each statistic are also calculated. These confidence intervals describe the uncertainty associated with a privacy preserving version of the true sample value, and are defined as the range that captures some defined fraction, commonly 95 percent, of the probability distribution of the underlying value. That is, if we drew 100 differentially private releases for a sample answer and constructed 95% confidence intervals for each release, we would expect 95% of them to contain the true sample answer.

statistic.getCI
Input:
release – the privacy preserving statistic released by the release function
params – the parameters outputted by the release function
alpha – maximum failure probability (default: alpha=0.05)
Output:
A list of pairs of upper and lower confidence limits.

Metadata:

The values of the privacy preserving statistics and confidence intervals are stored in a metadata file.

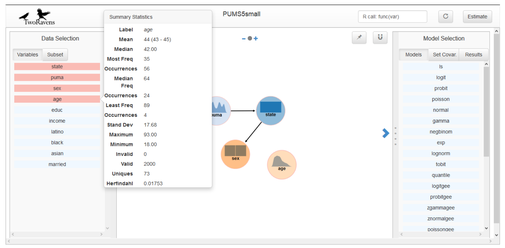
TwoRavens:

TwoRavens accesses the metadata file and displays the confidence intervals according to the type of statistic.

RESULTS

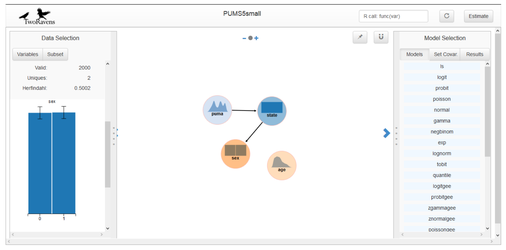
Means:

Confidence intervals for means are appended as numerical values.



Histograms:

Confidence intervals for histograms are displayed as error bars.

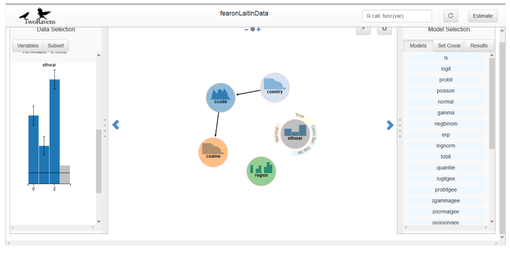


Stability based histograms:

The stability based algorithm excludes any bins whose counts fall below the threshold from the resulting perturbed histogram.

The threshold value of stability based histograms is displayed to allow users to understand that the non-zero bins near the threshold could have likely been set to zero instead.

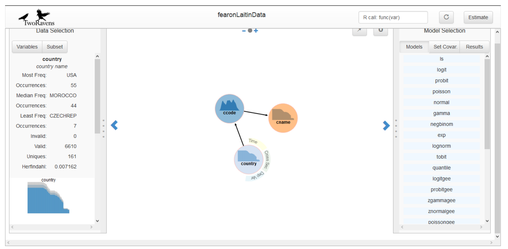
An approximation of the sum of the excluded bins is also shown through an extra bin appended to the end of the histogram.



RESULTS

Dense histograms:

In order to avoid visual clutter, confidence intervals in histograms containing a large number of bins are displayed differently.



Density graphs:

Confidence intervals at each point on the density graph are represented by the area between the uppermost and lowest curves.

CONCLUSIONS & FUTURE WORK

We accomplished our goal of communicating the noise for differentially private releases. Future work includes writing getCI functions for other types of releases as they become available, creating a smaller scale version of differentially private graphs for the pebbles inTwoRavens, allowing data uploaders to preview the uncertainty in their data, and testing the usability.

REFERENCES

Honaker J, D'Orazio V. **Statistical Modeling by Gesture: A graphical, browser-based statistical interface for data repositories**.
Extended Proceedings of ACM Hypertext 2014 [Internet]. 2014.

PI: Salil Vadhan Mentor: James Honaker
Harvard REU Summer Program 2015
Jessica Bu jbu2@wellesley.edu

CRCS Center for Research on Computation and Society at Harvard School of Engineering and Applied Sciences

BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

The Institute for Quantitative Social Science at Harvard University

DATA PRIVACY LAB