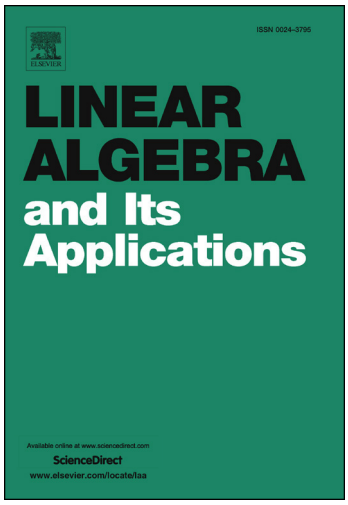

Extreme points of the local differential privacy polytope

Naoise Holohan, Douglas J. Leith, Oliver Mason

PII: S0024-3795(17)30487-1
DOI: http://dx.doi.org/10.1016/j.laa.2017.08.011
Reference: LAA 14293

To appear in: *Linear Algebra and its Applications*

Received date: 10 May 2016
Accepted date: 11 August 2017

Please cite this article in press as: N. Holohan et al., Extreme points of the local differential privacy polytope, *Linear Algebra Appl.* (2017), http://dx.doi.org/10.1016/j.laa.2017.08.011

Extreme Points of the Local Differential Privacy Polytope

Naoise Holohan[a], Douglas J. Leith[a], Oliver Mason[b,*]

[a]*School of Computer Science and Statistics, Trinity College Dublin, Ireland*
[b]*Dept. of Mathematics and Statistics/Hamilton Institute, Maynooth University, Co. Kildare, Ireland & Lero, the Irish Software Research Centre*

Abstract

We study the convex polytope of $n \times n$ stochastic matrices that define locally ϵ-differentially private mechanisms. We first present invariance properties of the polytope and results reducing the number of constraints needed to define it. Our main results concern the extreme points of the polytope. In particular, we completely characterise these for matrices with 1, 2 or n non-zero columns.

Keywords: Data Privacy, Stochastic Matrices, Matrix Polyopes, Differential Privacy.
2010 MSC: 68R01, 68R05, 60C05

1. Introduction

Data privacy has been of interest to researchers in computer science [1], statistics, cryptography [8] and law [6] for decades. The recent emergence of 'Big Data', while offering significant potential benefits to business and society, poses very real risks to personal privacy; this naturally has led to increased interest in questions pertaining to data privacy. The concept of *Differential Privacy*, introduced by C. Dwork in 2006 [12], has emerged as a popular theoretical paradigm in privacy research within the computer science community and has been applied to various different types of data and queries [11].

We are interested in the geometry of matrix polytopes arising in the study of differential privacy for categorical or finite-valued datasets. More formally, we consider databases $\mathbf{d} \in D^N$ where the set D is finite and can, without loss of generality, be taken to be $\{1, \ldots, n\}$. Each entry in $\mathbf{d}$, d_i, corresponds to data contributed by an individual; the base set D describes all the values that data entries can take.

The problem we consider is motivated by the construction of differentially private sanitisations, where we are interested in releasing a private, sanitised

*Corresponding author. Tel.: +353 (0)1 7083672; fax: +353 5(0)1 7083913; email: oliver.mason@nuim.ie