Maynooth University
National University of Ireland Maynooth

Differential Privacy and Opacity for Positive Linear Systems and Observers

A dissertation submitted for the degree of
Doctor of Philosophy

By:

Aisling McGlinchey

Under the supervision of:

Dr. Oliver Mason

Mathematics and Statistics Department
Maynooth University
National University of Ireland Maynooth
Ollscoil na hÉireann, Má Nuad

August 2020

For Emmet, my parents, my family and friends

Contents

Declaration

I hereby declare that I have produced this manuscript without the prohibited assistance of any third parties and without making use of aids other than those specified.

The thesis work was conducted from October 2015 to April 2020 under the supervision of Dr. Oliver Mason in Department of Mathematics and Statistics, Maynooth University. This work was supported by the Science Foundation Ireland, and the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero – the Science Foundation Ireland Research Centre for Software, grant *[13/RC/2094]*.

Maynooth, Ireland,

April 2020

Acknowledgement

First and foremost, I want to express my sincere thanks and appreciation to my supervisor, Dr. Oliver Mason, for his constant support, encouragement and advice throughout the last few years. I have been fortunate to have a supervisor who is extremely helpful and has made this an enjoyable and positive experience.

I was very lucky to have the opportunity to work in both the Mathematics and Statistics department and the Hamilton Institute here at Maynooth University. Completing this work was made easier by the support and friendship provided by the members of staff in both the Mathematics and Statistics department, and the Hamilton Institute. I am indebted to them for their help. A special mention to Dr. Ciarán Mac an Bhaird and Dr. Ann O'Shea, for making sure I was okay at different times.

To my fellow Maths Support Centre and departmental tutors, I would like to thank you for providing an enjoyable and relaxed working atmosphere. When I needed a break from work, you were for the chats and a laugh.

I would like to gratefully acknowledge the financial support from the Science Foundation Ireland (Grant no. 13/RC/2094), and the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero – the Science Foundation Ireland Research Centre for Software (www.lero.ie).

I would also like to thank my examiners, Dr. Begona Canto and Dr. David Malone, for their careful reading of my thesis, and their insightful comments.

On a more personal level, I would like to thank my Mum and Dad, and my siblings Laurena, Colm, and Eamonn for their support, encouragement, and always believing in me throughout the years. I must express my heartfelt

gratitude to Emmet, for your love and support, and continue to put up with me over the years. You have helped me to keep some of my sanity.

I want to mention some of the people whose friendships helped me through these years. To Emma Berry, who convinced me to do this PhD in the first place and who was always there if I needed someone to "talk maths at" when I found myself lost and confused. Thanks to the MUMS Social Club, for the laughs at cook Tuesday, the pub quizzes and the zoom quizzes during lockdown.

Abstract

Positive systems are important for application such as transportation, population dynamics and epidemiology. These systems can sometimes make use of sensitive personal information, which leads to the challenge of publishing this information in a way that guarantees individuals' privacy, while keeping the data usable. In this thesis, we focus on the problem of applying privacy constraints to positive linear systems and observers via differential privacy and opacity.

After reviewing relevant notation and background, we first tackle the problem of building a differentially private mechanism that preserves positivity. We consider two methods of constructing these mechanisms: *post-processing* and *restriction*. We present explicit formulae for the bias and the mean square error of the mechanisms constructed. We derive two results showing that bias is unavoidable for both approaches. For post-processing with a ramp function, we determine the optimal such function that minimises the worst case bias. We also prove the existence of an optimal post-processing function for mean square error.

Throughout this thesis, a major focus is on the positive linear observer problem. Specifically, we derive bounds for both the l_1 and l_2 sensitivity of Luenberger observers. We also show how these bounds can be used to quantify the noise required to achieve differential privacy via the Laplace or Gaussian mechanism. We then study the optimisation problem of minimising these bounds for positive linear observers and provide methods for computing an optimal solution for different classes of systems. In particular, we derive theoretical results describing optimal observers, in the l_1 sensitivity sense, for compartmental systems with a single output and a subclass of multi-output compartmental systems. We also consider the trade-off between the l_1 sensi-

tivity bound of a positive linear observer and the rate at which it converges to the true system state.

Finally, we present preliminary results on initial state opacity for positive linear systems. In particular, we consider the problem of initial state opacity when the secret and non-secret states are defined by convex cones in R^n_+. Farkas' Lemma is used to derive a result characterising opacity in this case.

CHAPTER 1

Introduction

In this chapter, we discuss the motivations behind the work of this thesis and provide an overview of the material presented in the following chapters.

1.1 Motivation

Within the area of Systems and Control Theory, there has been a significant amount of interest in the class of Positive Systems over the past 3 decades [42, 66, 63]. A positive system is one where the state and output variables take only nonnegative values when the initial state and inputs to the system are nonnegative. These systems are important for applications such as population dynamics, transportation networks, epidemiology, and information propagation. An important subclass of positive systems is formed by compartmental systems which are used to model the flow of material or people between compartments; these can be used to model the movement of people in a smart building or a transport system for example [62, 105]. Positive and compartmental systems have been studied in continuous and discrete time [104, 106].

The theory of positive linear time-invariant (LTI) systems is now well developed [42]. Many fundamental results have been established about system properties such as stability, controllability, observability, and realizability for positive systems. The results on these properties for positive systems are often different to those from general systems because of the positivity con-

straint on the system variables. For example, far stronger stability properties can be established using the Perron-Frobenius theory of nonnegative matrices [83, 50]. On the other hand, questions such as controllability can be more involved as the inputs are constrained for positive systems. Recent work has focused on extending the basic theory for LTI systems to classes of nonlinear systems, switched systems, descriptor systems [107, 29], and systems subject to time-delay [50, 82]. Nonetheless, some of the core questions for positive LTI systems such as those related to minimal realizations [15], or positive dynamic observer design [7, 106] are not entirely resolved and still attract the attention of researchers.

Many of the applications that give rise to positive systems involve the use of personal data. For example, transport networks or smart buildings rely on location data for individuals [102]. In the recent past, there has been a lot of concern over questions of personal privacy where data of this nature is being used. High-profile privacy breaches such as the Netflix prize dataset [86], the AOL breach [2], and Massachusetts health records [100] have motivated the development of formal mechanisms for privacy protection. Building on earlier work in fields such as *statistical disclosure control* [60], there has been a lot of activity in the development and analysis of formal privacy frameworks such as k-anonymity, l-diversity, and differential privacy. The last of these is now probably the main mathematical framework used for privacy. As modern control systems often use personal data, we need to add privacy protection to the design of such systems. In particular, there has been interest in developing control methods that satisfy privacy constraints. Differentially private versions of consensus algorithms, routing algorithms, Kalman filtering, and observer design have recently been developed [40, 51, 98, 37, 99]. In the light of the remarks made at the beginning of this paragraph, it seems natural to consider differentially private versions of some of the main problems in the theory of positive systems. This observation is the central motivating theme of this thesis.

Positive systems, positive observers, and privacy

One of the most studied questions in the theory of positive systems is the positive observer problem [52, 10, 7]. Classical Luenberger observers [79] are not appropriate for positive systems as they can generate negative values for

the state estimate. This has driven many researchers to consider the question of how to design dynamic observers for positive systems that respect the positivity property. For applications such as smart buildings or syndromic surveillance, the output measurements used to estimate the system state may be sensitive or personal. One way to address privacy concerns is to add noise to the state estimate (observer output). If this is done appropriately, then the mapping from the measured output to the state estimate will be differentially private [68]. In order to determine the variance required, it is necessary to compute or estimate a parameter associated with the observer system known as the sensitivity. In general, calculating system sensitivity is not easy. A lot of our work concerns novel problems related to positive observer design that come from the need to estimate and optimise sensitivity. An important issue here is to make sure that the perturbed/noisy signals still take nonnegative values.

While the majority of this thesis is concerned with differential privacy and positive systems, *opacity* is an alternative framework for questions of privacy. Opacity was introduced for Discrete Event Systems but has now been studied for linear systems also. The idea of opacity is that someone looking in from the outside cannot easily distinguish a 'secret' system evolution from a 'non-secret' one. To date, nothing seems to have been done on the question of opacity for positive systems. We briefly consider this question in Chapter 8.

Key questions

At a high level, the main questions considered in the thesis are the following.

1. How can we construct differentially private mechanisms which take only nonnegative values? This is needed to apply the mechanism to positive systems.

2. How much noise do we need to add to a positive observer to make it differentially private? For this we need to estimate the sensitivity of the observer.

3. Can we determine positive observers that are optimal? Here we want to find an observer that minimises the sensitivity estimate above.

4. How can opacity be applied to positive linear systems?

1.2 Overview

The structure of this thesis is as follows:

- In Chapter 2, we give an outline of notation and background on positive systems, positive observers, differential privacy and opacity.
- In Chapter 3, we show how to construct a positive ε differentially private mechanism via post-processing and restriction. The main focus is on the bias and the mean square error of the nonnegative Laplace mechanisms. We calculate the bias and mean square error of both approaches (using a simple ramp function for post-processing). We establish that bias is inevitable and show how to achieve a lower bias with alternative ramp functions. We also prove the existence of a square-integrable post-processing function that minimises the worst case mean square error for the Laplace mechanism.
- In Chapter 4, we show how to apply the derived nonnegative mechanisms from Chapter 3 to control systems. We then calculate an upper bound of the l_1 sensitivity for a positive Luenberger observer and present initial results and methods on the problem of minimising this bound for a positive linear observer.
- In Chapter 5, we derive expressions for a positive observer that will minimise the l_1 sensitivity bound of a compartmental system, for single-output and classes of multiple-output systems. We also examine the trade-off between the l_1 sensitivity bound of a positive linear observer and the rate of convergence to the true system state. Finally, we investigate the sensitivity for a more general positive observer construction.
- In Chapter 6, we derive an upper for the l_2 sensitivity of a Luenberger observer. This is used to achieve relaxed (ε, δ) differential privacy via the Gaussian mechanism. We also establish steps for an algorithm to minimise this bound for a positive observer for a multiple-output system.
- In Chapter 7, we consider initial state opacity for positive linear systems. For this, we consider the problem when the secret and non-secret states are defined by convex cones in R^n_+.

- Concluding remarks and a discussion of possible future work are given in Chapter 8.

1.3 Outputs

The following papers have been published/submitted contributing to the work in this thesis.

1. McGlinchey, A. and Mason, O. Differential privacy and the l_1 sensitivity of positive linear observers, *IFAC Papers – Online, (IFAC World Congress)*, 50 (2017), 3111 – 3116.

2. McGlinchey, A. and Mason, O. Bounding the l_2 sensitivity for positive linear observers, in *European Control Conference*, 2018.

3. McGlinchey, A. and Mason, O. Some Novel Aspects of the Positive Linear Observer Problem: Differential Privacy and Optimal l_1 Sensitivity. *Journal of Franklin Institute*, Submitted July 2020.

4. McGlinchey, A. and Mason, O. On the Bias and Mean Square Error of Differentially Private Mechanisms for Positive Real-valued Data. *Foundations of Data Science*, Submitted August 2020.

CHAPTER 2

Background

In this chapter, we introduce some standard notation that is used throughout the thesis, and discuss relevant results from the literature in the areas of Positive Systems Theory, Di erential Privacy, and Opacity. Particular attention is given to the positive linear observer problem.

2.1 Introduction

As mentioned in Chapter 1, the positive observer design problem has been widely studied in the theory of positive systems. A simple Luenberger observer for a positive LTI system will typically generate negative state estimates. Imposing the requirement that all signals in the observer are nonnegative makes the question of positive observer design more complicated. While much work has been done on positive observer design, it is only very recently that privacy has been considered in connection with problems in control theory. In particular, the paper [67] is the first to have considered differentially private observers for general, not necessarily positive systems. Adding differential privacy as a requirement for an observer gives rise to several novel problems and directions for research; these shall play a central role in this thesis.

Throughout the thesis, we are concerned with problems arising from the combination of positive systems theory with privacy considerations. Hence, the material in the thesis draws on background from some diverse fields and, to set the scene for the remainder of the thesis, in this chapter we will present a variety of relevant definitions and results. In particular, we review well-known

results on positive linear systems and nonnegative matrices before discussing the most relevant prior work on the positive observer problem. As differential privacy is a central concern throughout, we devote a number of sections to this. We first describe its initial formulation for a static database [38], before considering more recent work extending it to control systems and observers [33].

For discrete event systems, the concept of opacity [61] has been widely used for privacy protection. In the last few years a version of opacity for linear systems has been developed. This gives an alternative approach to privacy protection to that of differential privacy and we will briefly consider its use for positive systems in Chapter 7. For this reason, we also include a brief discussion on opacity in this chapter.

2.2 Background on nonnegative matrices and positive systems

Our primary focus in this thesis is on formal definitions of privacy applied to positive systems [66, 63, 42]. For the most part, we will be concerned with positive linear systems in discrete time. Before describing relevant results from the literature on positive linear systems, we first recall some standard terminology and notation from linear algebra that will be used when we discuss positive linear systems. Most of the results discussed here are well known, and further details can be found in the standard references [59, 58, 17, 16, 12, 94, 42] and elsewhere in the literature on linear algebra and positive systems.

2.2.1 Notation and preliminaries on matrices and graphs

We denote the set of integers by Z. We use R^n to denote the vector space of n-tuples of real numbers. For vectors x, y R^n: $x \geq y$ means that $x_i \geq y_i$ for $1 \leq i \leq n$; $x > y$ means that $x \geq y$, $x = y$; x y means that $x_i > y_i$ for $1 \leq i \leq n$. We use R^n_+ to denote the nonnegative orthant

$$\mathsf{R}^n_+ := \{x \quad \mathsf{R}^n \mid x \geq 0\}.$$

We use $\mathsf{R}^{n \times m}$ to denote the space of $n \times m$ matrices with real entries. We say a matrix A $\mathsf{R}^{n \times m}$ is strictly greater (or greater) than B $\mathsf{R}^{n \times m}$, and

denote this by $A \quad B$ (or $A \geq B$), if for all $1 \leq i \leq n$ and $1 \leq j \leq m$, $a_{ij} > b_{ij}$ ($a_{ij} \geq b_{ij}$). $\sigma(A)$ denotes the spectrum of $A \quad \mathbb{R}^{n \times n}$, the set of all eigenvalues of A. $\rho(A) = \max\{|\lambda| : \lambda \quad \sigma(A)\}$ denotes the spectral radius of A and $\mu(A) = \max\{\mathrm{Re}(\lambda) : \lambda \quad \sigma(A)\}$, the maximal real part of eigenvalues of A, denote the spectral abscissa of A.

$\mathbb{R}_+^{n \times n}$ is the cone of $n \times n$ matrices with nonnegative entries. We say A is a positive matrix, $A \quad 0$, if for $1 \leq i \leq n$ and $1 \leq j \leq m$, $a_{ij} > 0$, and A is a nonnegative matrix, $A \geq 0$, if for $1 \leq i \leq n$ and $1 \leq j \leq m$, $a_{ij} \geq 0$.

Metzler matrices play a key role in the theory of positive linear systems in continuous time [42] and we now recall their definition.

Definition 2.2.1. A matrix $A \quad \mathbb{R}^{n \times n}$ is a Metzler matrix if its off-diagonal elements are nonnegative, formally $a_{ij} \geq 0, \quad i = j$ and $A = N - \alpha I$ for $N \geq 0$.

Many strong results in the theory of nonnegative matrices concern the class of irreducible matrices [59], defined as follows.

Definition 2.2.2. A matrix $A \quad \mathbb{R}_+^{n \times n}$ is reducible if there exists a permutation matrix $P \quad \mathbb{R}^{n \times n}$ such that

$$P^T A P = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$$

with B and D square matrices. A is said to be irreducible if A is not reducible.

Given a nonnegative matrix $A \quad \mathbb{R}_+^{n \times n}$, the directed graph, or digraph, of A, $D(A)$ is defined in the standard fashion. $D(A)$ consists of the vertices $V = \{1, \ldots, n\}$ and there is an edge (i, j) from vertex i to vertex j if and only if $a_{ij} > 0$. It is well known that the matrix $A \quad \mathbb{R}_+^{n \times n}$ is irreducible if and only if $D(A)$ is strongly connected [13]; the digraph ($D(A)$ is strongly connected if there exists a directed path from i to j for every pair (i, j) of vertices in $D(A)$. Another equivalent condition for A to be irreducible is $(I + A)^{n-1} \quad 0$. The following concept of primitivity is stronger than irreducibility.

Definition 2.2.3. A nonnegative matrix $A \quad \mathbb{R}_+^{n \times n}$ is primitive if $A^k \quad 0$ for some positive integer k.

Some of the results we describe later on the positive observer problem involve the *index of primitivity* of a nonnegative matrix.

Definition 2.2.4. For a matrix $A \quad \mathbb{R}_+^{n\times n}$, the least k such that $A^k \quad 0$ is the index of primitivity of A.

In the study of positive linear systems, and particularly their stability properties, the next classical result plays a key role. The first version of this celebrated result was proved for positive matrices while later work developed extensions to irreducible and primitive matrices.

Theorem 2.2.1 (Perron-Frobenius [59, 94, 12])**.** *Let $A \quad \mathbb{R}_+^{n\times n}$ be irreducible and nonnegative and suppose that $n \geq 2$. Then:*

a) $\rho(A) > 0$*;*

b) $\rho(A)$ *is an algebraically simple eigenvalue of* A*;*

c) there is a unique vector $x \quad \mathbb{R}^n$ with $x \quad 0$ such that $Ax = \rho(A)x$ and $x_1 + \ldots + x_n = 1$;

d) there is a unique vector $y \quad \mathbb{R}^n$ with $y \quad 0$ such that $y^T A = \rho(A)y^T$ and $y_1 + \ldots + y_n = 1$.

It is a standard result [59] in Perron-Frobenius theory that a primitive matrix has only one nonzero eigenvalue of maximum modulus.

Induced matrix norms

Later in the thesis, we shall make use of induced matrix norms when discussing sensitivity in the setting of differential privacy. First recall that given a norm $\cdot$ on $\mathbb{R}^n$, the associated *induced matrix norm* of A in $\mathbb{R}^{n\times n}$ is given by

$$A = \sup_{x \ \mathbb{R}^n, x=0} \frac{Ax}{x} = \max_{x \ =1} Ax \ . \tag{2.1}$$

The next result (see [59] for a proof) characterises the induced matrix norm associated with the usual l_1 and l_2 norms on $\mathbb{R}^n$.

Lemma 2.2.2. *The l_1 induced norm (the maximum column sum matrix norm) of a matrix A $\mathbb{R}^{n\times n}$ is given by*

$$A_1 = \max_{1\le j\le n} \sum_{i=1}^{n} |a_{ij}| \tag{2.2}$$

The l_2 induced norm (spectral norm) of a matrix A $\mathbb{R}^{n\times n}$ is given by

$$A_2 = \sqrt{\rho(A^T A)} \tag{2.3}$$

which is the largest singular value of A.

2.2.2 Positive linear systems in continuous and discrete time

Consider a linear time-invariant (LTI) system [91, 64]:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned} \tag{2.4}$$

in the discrete time case or

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned} \tag{2.5}$$

in continuous time. Here the state x $\mathbb{R}^n$, the input u $\mathbb{R}^m$, and the output y $\mathbb{R}^p$ and A $\mathbb{R}^{n\times n}$, B $\mathbb{R}^{n\times m}$, C $\mathbb{R}^{p\times n}$, D $\mathbb{R}^{p\times m}$.

Definition 2.2.5. An LTI system (2.4) or (2.5) is a positive LTI system [66, 42] if for every nonnegative initial state and for every nonnegative input its state and output are nonnegative for all times.

Positive LTI systems will be a significant concern throughout this thesis. Given their practical importance in applications such as epidemiology [30, 105], it is not surprising that positive systems have attracted a significant amount of attention in the research literature over the years. For general background on positive systems and their applications, consult the references [42, 66, 63].

A characterisation of discrete-time positive LTI systems is as follows [42].

Proposition 2.2.3. *The discrete-time LTI system (2.4) is positive if and only if*

$$A \quad \mathsf{R}_+^{n\times n},\ B \quad \mathsf{R}_+^{n\times m},\ C \quad \mathsf{R}_+^{p\times n},\ D \quad \mathsf{R}_+^{p\times m}.$$

A corresponding characterisation of continuous-time positive LTI systems is as follows [42].

Proposition 2.2.4. *The continuous-time LTI system (2.5) is positive if and only if*

$$B \quad \mathsf{R}_+^{n\times m},\ C \quad \mathsf{R}_+^{p\times n},\ D \quad \mathsf{R}_+^{p\times m}, \text{ and } A \text{ is a Metzler matrix.}$$

Throughout this work, we are mainly concerned with discrete-time LTI systems. Also, many of the results to follow concern systems without inputs. Such an LTI system takes the simpler form:

$$\begin{aligned} x(t+1) &= Ax(t) \\ y(t) &= Cx(t). \end{aligned} \tag{2.6}$$

2.2.3 Stability and positive linear systems

Stability theory is a major topic in Systems and Control Theory and a lot of the literature on positive systems has been dedicated to determining conditions for stability of various classes of positive systems. The autonomous LTI system

$$x(t+1) = Ax(t), \quad x(0) = x_0 \tag{2.7}$$

is *stable* if for every $\epsilon > 0$ there is some $\delta > 0$ such that $\|x_0\| < \delta$ implies $\|x(t)\| < \epsilon$ for all $t \geq 0$. If in addition, $x(t) \to 0$ as $t \to \infty$ for any initial condition x_0, we say that the system is (globally) asymptotically stable. For a general discrete time LTI system (2.7), it is well known that asymptotic stability is equivalent to $\rho(A) < 1$. Matrices with this property are referred to as *Schur*. Stability is directly relevant to our later discussion on the positive observer problem as the design of a positive linear observer requires the construction of an observer gain matrix such that the resulting error dynamics are given by an asymptotically stable system.

The following result characterising the stability of an autonomous positive LTI system (2.6) is well known; see for instance [5, 42].

Theorem 2.2.5. *Let $A \geq 0$ be given. Then the following statements are equivalent:*

1. *A is Schur;*
2. *the system (2.7) is asymptotically stable for every initial condition x_0 R^n;*
3. *the system (2.7) is asymptotically stable for every non-negative initial condition x_0 R^n_+;*
4. *there exists v 0 such that Av v;*
5. *there exists w 0 such that $A^T w$ w.*

Analogous results hold for continuous time systems. While stability theory is not the focus of this thesis, many researchers are still actively working on stability questions for positive systems [28, 20, 35]; moreover, stability is closely related to the problem of observer design, which is a major topic of our work.

Using the vector w in the 5th point above, we can define a *linear copositive Lyapunov function* $V(x) = w^T x$ for the system. Copositive Lyapunov functions for various classes of positive systems have been worked on by many authors. Their application to stability and stabilizability of positive switched systems has been investigated in numerous papers: for a sample of such work see, for instance [83, 65, 45, 20, 35]. It is worth noting here that much work has been done extending conditions such as those in Theorem 2.2.5 to positive systems subject to time-delay [50, 78, 77, 82] and classes of nonlinear positive systems [21, 1, 34, 22, 43]. Much of the work on extending stability results to nonlinear positive systems makes use of the theory of monotone or order-preserving systems [96]. Another interesting direction in which the basic theory has been extended is to the class of so-called positive descriptor systems [29, 107].

Influence graph of a discrete-time system

Now, we introduce the notion of *influence graph* for a discrete-time dynamic system. Similarly to how it is described in [42] for a single input/single output

system ($p = 1$, $m = 1$), the influence graph of a system (2.4) is a graph G with $n + 2$ nodes $0, 1, 2, \ldots, n + 1$. Nodes (0) and $(n + 1)$ are associated with the input u and output y of the system and the remaining nodes $(i = 1, 2, \ldots, n)$ are associated with the state variables x_i. The edges of the graph point out the direct interactions among the input, state, and output variables. If G has an edge $(0, j), j = 1, 2, \ldots, n$, this means the input $u(t)$ influences $x_j(t + 1)$. If there is an edges (i, j), for $i, j = 1, 2, \ldots, n$ in the graph G, then the state variable $x_j(t + 1)$ depends on $x_i(t)$. Lastly, an edge $(i, n + 1)$ indicates direct influence of $x_i(t)$ on $y(t)$.

The influence graph can be described by the matrices of the system. For the matrix A, if $a_{ij} > 0$ where i, j $\{1, 2, \ldots, n\}$ then there exists an edge (i, j) in the graph G. If $b_j > 0$, for j $\{1, 2, \ldots, n\}$, then there is an edge $(0, j)$ in the graph G. Similarly, if $c_i > 0$, for i $\{1, 2, \ldots, n\}$, then there is an edge $(i, n + 1)$ in the graph G.

2.3 Positive linear observers

In this section, we will give background on the general observer problem and then discuss the observer problem for positive linear systems, in more detail. The observer problem is to synthesise a dynamic system, called the *observer*, using the output of a linear system as an input, such that difference between the state of the linear system and the output of the observer converges to zero asymptotically. The idea for an observer for a dynamic system was introduced by Luenberger in [79, 80] and later developed in [81].

The classical problem of designing an observer of Luenberger form [79, 81] for (2.6), consists of constructing a matrix L $\mathbb{R}^{n \times p}$ such that the solution $\hat{x}(\cdot)$ given by

$$\begin{aligned} \hat{x}(t + 1) &= A\hat{x}(t) + L(y(t) - C\hat{x}(t)) \\ &= (A - LC)\hat{x}(t) + Ly(t) \end{aligned} \tag{2.8}$$

satisfies $\hat{x}(t) - x(t) \to 0$ as $t \to \infty$, where x is the solution of (2.6). In the absence of additional constraints, the problem, whose solution is classical, is to construct a matrix L such that $A - LC$ is Schur-stable [97].

In this thesis, we will be dealing mainly with Luenberger type observers for a linear system and versions of these for positive systems. The *positive observer*

problem is to construct an observer that ensures nonnegativity of the estimates of the nonegative states. However, the classical Luenberger observer can lead to negative estimates, so it is not adequate for estimating the states of systems that are inherently nonnegative. For a Luenberger observer to be positive we need to find an L such that all signals in the observer system are nonnegative. We now recall the original formulation of this problem in linear algebraic terms.

Problem 2.3.1. *Given* $A \quad \mathsf{R}_+^{n\times n}$, $C \quad \mathsf{R}_+^{p\times n}$, *find* $L \quad \mathsf{R}_+^{n\times p}$ *such that the following are satisfied*

1. $A - LC \quad \mathsf{R}_+^{n\times n}$, *and;*
2. $\sigma(A - LC) \quad \{\lambda \quad \mathsf{C} \mid |\lambda| < 1\}$.

There is now a large literature on positive observers. We shall discuss some of the most relevant references to our work in some detail later; in particular, the results in [106, 52, 10, 7] will play an important role. Additional results can be found in [95, 26, 108, 36]. In [26], the use of positive observers for general linear time varying systems, for both continuous and discrete time, is considered. This is based on stable internally positive representations of linear systems and this observer is used to develop interval observers and controllers for systems with uncertainties. In [36], a method to design a positive observer using generalised polar coordinates in the positive orthant is proposed. This observer's gain is tuned to maximise the contraction rate of the error as measured by the Hilbert projective matrix. In [108], the authors design a positive observer for a discrete time positive system with missing data in the output. Recently, in [76] a specific form of positive linear observer in discrete time was considered and sufficient conditions for its existence were derived. These were expressed as feasibility conditions for a linear program. The basic technique was then extended to systems with time-delay.

Observers for nonlinear systems and nonlinear positive systems have also been studied [87, 23, 110]

The classical observer design problem is related to certain key properties such as observability and detectability. We will now recall the definition of observability for a general LTI system [91, 31].

Definition 2.3.1. The time-invariant linear state equation (2.4) with $t_0 = 0$ is called *observable* if there is a finite positive integer t_f such that any initial state $x(0) = x_0$ is uniquely determined by the corresponding zero-input response sequence $y(t)$, $t = 0, \ldots, t_f - 1$.

For a discrete-time linear positive system of the from (2.4), with system matrices (A, C) define the obsverability matrix as

$$\text{obsm}(A, C) = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}$$

Theorem 2.3.1. *[91] The time-invariant linear state equation (2.4) is observable if and only if*

$$rank(obsm(A, C)) = n.$$

Detectability is a related condition to obsverability, and we will describe a version for positive systems in the next two section 2.3.1 an 2.3.2.

2.3.1 Canonical forms and positive observability

In control theory, observability and detectability are closely related to the properties of controllability and reachability. We note that these latter properties have been considered for positive systems by various authors. A survey of results on reachability and controllability for positive systems can be found in [27] while, in [103], graph-theoretic methods were used to characterise these properties for discrete-time positive systems. Related results, which characterise controllability, reachability and essential reachability in terms of the digraph associated with the system matrix can be found in [24]. It is also worth noting the work of [32] which describes simplified, graph theoretic, necessary and sufficient conditions for reachability.

Our focus later is on observer design and we now discuss results on positive observability from [52] in more detail as this paper directly concerns the positive linear observer problem.

In [52], the authors extend the classical definition of observability to the case of a positive linear system and provide a characterisation of positive observability. In addition, they give extra constraints that need to be satisfied in order for an observer of Luenberger form to exist for a positive linear system. They describe in detail how the decomposition of a positive system into irreducible subsystems depends on an underlying influence graph, as described in Section 2.2.3, associated with the system. This decomposition is then used to define the observable canonical form for a positive linear system with respect to an equivalence relation defined by permutations of the state and output sets.

The definition of observability for a positive system is identical to those for a general system from [91]. A time-invariant discrete-time linear positive system is observable if and only if

$$\text{rank}(\text{obsm}(A, C)) = n.$$

Within [52], the authors detail a canonical form with respect to a permutation of the state and output sets. For a system (2.6), the matrix A and matrix C are transformed to the form,

$$A = \begin{pmatrix} \bar{A}_{1,1} & 0 \\ & A_{k_2+1,k_2+1} \end{pmatrix}, C = \begin{pmatrix} \bar{C}_1 & 0 \end{pmatrix}$$

where $\bar{A}_{1,1}$ and $\bar{C}_1$ are block diagonal matrices. The permutation is done in a way such that block matrices satisfy $\text{rank}(\text{obsm}((A_{i,i}, C_i))) = n_i$, where $A_{i,i}$ $\mathsf{R}^{n_i \times n_i}$ for $i = 1, \ldots, k_1$, i.e. they are observable and $\text{rank}(\text{obsm}((A_{i,i}, C_i))) < n_i$, for $i = k_1 + 1, \ldots, k_2$. When a system is in this canonical form, we can easily see whether it is observable or detectable.

In [52], a positive linear system is said to be *detectable* if when the system matrices are in canonical form, then $\sigma(A_{i,i})$ $\{\lambda$ $\mathsf{C} \mid |\lambda| < 1\}$ for $i = k_1 + 1, \ldots, k_2 + 1$. This is consistent with the definition of detectability for a general system.

In [52], the authors give details of certain cases where there does exist a stable linear positive observer for a discrete-time linear positive system. For instance, if the system matrix A is irreducible and the index of imprimitivity of A is the same as the size of A, where the index of imprimitivity of A is defined as the value k Z_+ if A has exactly k different eigenvalues of modulus the maximal

eigenvalue and rank(obsm$(A, C)) = n$, then there exists a matrix L satisfying the conditions in Problem 2.3.1 to form a stable linear positive observer. We should also note here that it is shown that a stable linear positive observer for a discrete-time linear positive system may not exist.

The authors also give details of an algorithm for observer synthesis for a linear positive system if the system matrices A, C are in canonical form and (A, C) form an observerable pair.

2.3.2 Observers for compartmental systems

A compartmental system is a special type of positive system that arises in applications in areas such as transport, physiology, and hydrology. The reference [62] contains a substantial amount of background material on the properties of compartmental systems. We shall later be interested in designing differentially private observers for compartmental systems in discrete time. We now recall the main results of a paper by Van den Hof [106] concerning observer design for compartmental systems. As our interest is in discrete time systems throughout, we only discuss the results for discrete time observers here. [106] contains many result on continuous time systems also.

A compartmental system is a system consisting of a finite number of subsystems, which are called compartments, and the system models the transfer or flow of material between compartments. The variable $q_i(t)$ is the amount of material in the ith compartment at time t. $G_{ij}(t)$ denotes the amount transferred from the jth compartment to the ith in the time interval $t \to t + 1$.

One practical example of this arises in public transport with people moving from one train to another; similarly, within a building we may be modeling the number of people moving between different areas of the building. It is assumed that G_{ij} has a simple, time-invariant linear dependence on q_j: formally this means that $G_{ij} = g_{ij} q_j(t)$ for some fixed g_{ij} R_+.

Motivated by the above system class, a matrix G is said to be compartmental if it satisfies the following conditions:

1. $g_{ij} \geq 0$ for all $1 \leq i, j \leq n$
2. $\sum_{i=1}^{n} g_{ij} \leq 1$ for all $1 \leq j \leq n$

If $G \in \mathbb{R}_+^{n\times n}$ is a compartmental matrix and $L \in \mathbb{R}_+^{n\times p}$, $C \in \mathbb{R}_+^{p\times n}$ are such that $G - LC \in \mathbb{R}_+^{n\times n}$, then $G - LC$ is also a compartmental matrix.

In [106], the main problem considered is the following: given $G \in \mathbb{R}_+^{n\times n}$ and $C \in \mathbb{R}_+^{p\times n}$ determine conditions for the existence of $L \in \mathbb{R}_+^{n\times p}$, $L = 0$ such that

1. $G - LC \in \mathbb{R}_+^{n\times n}$ is a compartmental matrix;
2. $\sigma(G - LC) \subset \{\lambda \in \mathbb{C} \mid |\lambda| < 1\}$.

These requirements are the same as those in [52], except with the addition of $G - LC \in \mathbb{R}_+^{n\times n}$ having to be a compartmental matrix.

The following definitions are taken straight from the paper [106] and are needed for theorems stated later.

Definition 2.3.2. Consider an n-compartmental system. A trap is a compartment or a set of compartments from which there are no transfers or flows to the environment nor to compartments that are not in that set. A trap is said to be simple if it does not strictly contain a trap.

Definition 2.3.3. Let $G \in \mathbb{R}_+^{n\times n}$ be a compartmental matrix and $C \in \mathbb{R}_+^{p\times n}$. The matrix pair (G, C) is said to be positively modifiable if there exists a $L \in \mathbb{R}_+^{n\times p}$ such that $LC = 0$ and $G - LC$ is a compartmental matrix.

Definition 2.3.4. The matrix pair (G, C) is said to be positively detectable if there exists a $L \in \mathbb{R}_+^{n\times p}$ such that $LC = 0$ and $G - LC$ is an asymptotically stable compartmental matrix.

These definitions imply that if (G, C) is positively modifiable then $\sigma(G - LC) \subset \{\lambda \in C : |\lambda| \leq 1\}$ and if (G, C) is positively detectable then $\sigma(G - LC) \subset \{\lambda \in C : |\lambda| < 1\}$.

This definition for detectability is stronger than the definition of detectability from [52]. This definition implies there exists a positive observer, whereas that in [52] does not necessarily imply the existence of a positive observer.

One of the results in [106] characterises positive modifiability in terms of the entries of G, C. Formally the following is shown:

Proposition 2.3.2. *Let* $G \in \mathbb{R}_+^{n\times n}$ *be a compartmental matrix and* $C \in \mathbb{R}_+^{p\times n}$. *(*$G$, C*) is positively modifiable if and only if there exists* $1 \leq i \leq n$ *and* $1 \leq r \leq k$ *such that the* r*th row of* C *is nonzero and for all* $1 \leq j \leq n$ *with* $c_{rj} > 0$, *also* $g_{ij} > 0$.

Using this theorem, the author has outlined the details of an algorithm to construct L such that $LC = 0$ and $G - LC$ is compartmental.

The main theorem (Theorem 4.12) in [106] characterises the relation between positive modifiability and positive detectability. If a system contains no traps then (G, C) is positively detectable if and only if (G, C) is positively modifiable.

If the system contains one or more traps, then G can be transformed into a block triangular form by permutation similarity where G_{ii} denotes the blocks on the diagonal. Then (G, C) is positively detectable if and only if (G_{ii}, C_i) is positively modifiable for all indices i corresponding to traps.

[106] then gives details of an algorithm to construct a positive linear observer by checking for modifiability of (G_{ii}, C_i) and then using the previous algorithm to construct L such that it satisfies the conditions above.

2.3.3 A relaxation of the conditions for positive linear observers

The authors of [7] note that the initial formulation of Problem 2.3.1 provides only sufficient, and not necessary, conditions for the existence of positive linear observers. The proposed numerical method in [7] is based on linear programming and follows a previous approach for the regulation problem in [3], which is further developed in [6]. Preliminary results for the observer problem for positive systems were presented in [5] for discrete-time and in [4] for continuous-time systems.

The following theorem from [7] gives necessary and sufficient conditions for the existence of a positive linear observer.

Lemma 2.3.3. *There exists a positive observer of the system* (2.6) *if and only there exists* L *with* $LC \geq 0$, $A - LC \geq 0$ *and* $A - LC$ *is a Schur matrix.*

In [52] and [106], L is required to be a nonnegative matrix but in [7] it is shown that it necessary and sufficient that LC is nonnegative for the existence of a positive linear observer. Therefore L is not necessarily nonnegative, except for $p = 1$.

The next theorem from [7] gives a computational approach for constructing a positive observer.

Theorem 2.3.4. *The following statements are equivalent:*

1. *There exists a positive observer for the system (2.6) of the form of (2.8).*
2. *There exists a matrix L $\mathbb{R}^{n\times p}$ such that $LC \geq 0$, $A - LC \geq 0$ and $A - LC$ is a Schur matrix.*
3. *The following LP problem is feasible:*

$$\begin{cases} (A^T - I)\lambda - C^T \sum_{i=1}^{n} z_i < 0 \\ \lambda > 0 \\ c_i^T z_j \geq 0 \text{ for } i, j = 1, ..., n, \\ a_{ij}\lambda_j - c_i^T z_j \geq 0 \end{cases} \tag{2.9}$$

where $A = [a_{ij}]$, $C = [c_1...c_n]$, $\lambda = [\lambda_1...\lambda_n]^T$ and z_i $\mathbb{R}^p$.

The proof of this result given in [7] makes use of Theorem 2.2.5 and Lemma 2.3.3.

Finally, it is also shown in [7] that for a controlled discrete linear system:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t), \\ y(t) &= Cx(t) \end{aligned} \tag{2.10}$$

that a positive observer of the form

$$\hat{x}(t+1) = (A - LC)\hat{x}(t) + Bu(t) + Ly(t) \tag{2.11}$$

cannot asymptotically stabilise System (2.10), when an observer feedback law $u(t) = K\hat{x}(t)$ is utilised. They prove the following result.

Theorem 2.3.5. *Assume that the matrix A is not Schur. Then, there does not exist a positive observer of the form (2.11) for system (2.10), such that the observer feedback law $u(t) = K\hat{x}(t)$ is asymptotically stabilising.*

2.3.4 Positive linear observers, coordinate transformations and the realization problem

2.3.4.1 Coordinate transformations and the Sylvester equation

In [10], an alternative approach to the construction of positive linear observers is considered. Here, the authors make use of the extra flexibility provided by allowing coordinate transformations to obtain potentially less conservative results and broaden the class of systems admitting such observers. Essentially, they suitably adapt the approach to constructing classical observers using the Sylvester equation; details on this matrix equation can be found in [31, 64] and elsewhere.

The focus of [10] is on continuous time positive systems

$$\begin{aligned} \dot{x} &= Ax \\ y &= Cx, \end{aligned} \tag{2.12}$$

with the matrix C nonnegative and A Metzler. An observer of the following form is considered:

$$\dot{\hat{z}} = F\hat{z} + Gy \tag{2.13}$$

$$\hat{x} = T^{-1}\hat{z}. \tag{2.14}$$

To obtain a positive observer where $\hat{x}$ estimates the state x, it is required that F is Metzler and Hurwitz, $G \quad \mathsf{R}_+^{n\times p}$, and $T \quad \mathsf{R}^{n\times n}$ is *inverse-positive*. The existence of an observer of the form (2.13) is equivalent to the existence of solutions F, G, T to the Sylvester equation

$$TA - FT = GC \tag{2.15}$$

where A is Metzler and Hurwitz, G is nonnegative, and T is inverse-positive. The authors describe a heuristic numerical procedure that can be used to search for such a solution which is based on first choosing matrices F, G and then checking whether the solution T obtained is nonnegative.

The general problem of theoretically characterising when solutions exist is a challenging one. In order to simplify the analysis, the authors of [9] first restrict attention to low dimensional systems under the assumption that the matrix F has distinct real, negative eigenvalues and that $\sigma(F) \cap \sigma(A)$ is empty.

Under these conditions, for 2-dimensional systems, it is shown that a necessary condition for the existence of a positive linear observer of the form (2.13) is that the matrix A has a negative, real eigenvalue. This same condition is shown to be necessary for the existence of an observer with T a Z-matrix for the case of 3-dimensional systems. Necessary and sufficient conditions for the 2-dimensional case are also given. These require the observability of (A, C), and the existence of a simple negative eigenvalue of A that satisfies inequalities defined by the system matrices.

It is worth noting that the relation of the system class covered in [10] and that covered by the results of [5] is not straightforward. An example illustrates this in the paper for a system for which no Luenberger observer exists, but an observer of the form (2.13) does exist. This example has a single output and hence no observer would exist for it following the construction of [5].

The work of [9] is significantly developed and expanded in [10]. First, the case of a single measured output, $p = 1$, is considered. The existence of a positive linear observer of the form (2.13) with F diagonal and satisfying $\sigma(F) \cap \sigma(A) =$ implies that A has at least $n - 1$ distinct negative real eigenvalues. This naturally extends the result of [9] for 2-dimensional systems. A separate, related, necessary condition is also given for the more general case where no restriction is imposed on either the structure of F or its spectrum. For this case, the existence of a positive linear observer implies that A has at most 1 nonnegative real eigenvalue. The following sufficient condition is also proven.

Theorem 2.3.6. *Consider the system (2.12) where* C $\mathsf{R}_+^{1\times n}$, *A is irreducible, and the pair (A, C) is observable. Suppose that $\sigma(A) = \{\lambda_1, \ldots, \lambda_n\}$ where*

- λ_i R *for* $1 \leq i \leq n$;
- $\lambda_1 > \lambda_2 > \cdots > \lambda_n$;
- $0 > \lambda_2$.

Then there exists a positive linear observer of the form (2.13) for (2.12).

Positive Realisations and Positive Observer

A further relaxation of the problem of positive linear observer design is also introduced in [10]. The key idea is to make the dimension of the observer system a design parameter; by contrast, the dimension of the observer (2.13) is required to equal that of the original system (2.12). With this relaxation, the authors make use of results on the positive realisation problem (see [15] for an introduction to this important problem) to provide conditions for the existence of a positive observer of the form

$$\begin{aligned} \dot{\hat{z}} &= F\hat{z} + Gy \\ \hat{x} &= H\hat{z}, \end{aligned} \tag{2.16}$$

where $F \quad \mathbb{R}_+^{N\times N}$, $G \quad \mathbb{R}_+^{N\times p}$, and $H \quad \mathbb{R}_+^{n\times N}$. Allowing the possibility that $N > n$ gives greater flexibility and may lead to less conservative conditions for a positive linear observer. In fact, it is shown that the following conditions are sufficient for the existence of a positive linear observer of the form (2.16).

- The pair (A, C) is detectable.
- There exists a matrix L such that $A - LC$ is Hurwitz (and thus defines a linear observer for (2.12)).
- The matrix transfer function $G(s) = (sI - A - LC)^{-1}L$ has a positive realisation.

The core idea behind the previous result is that the observer (2.16) is a positive realisation of the transfer function $G(s)$. Using this approach, the following extension of Theorem 2.3.6 is proven.

Theorem 2.3.7. *Consider the system (2.12) where $C \quad \mathbb{R}_+^{1\times n}$, A is irreducible, and the pair (A, C) is detectable. Let $\mu(A)$ denote the spectral abscissa of A. If all eigenvalues λ of A apart from $\mu(A)$ satisfy $Re(\lambda) < 0$, there exists a positive observer of the form (2.16) for (2.12).*

Compartmental Systems

A natural generalization of (continuous-time) compartmental systems is also considered in [9, 10]. Here the matrix A is assumed to satisfy

$$0 \quad \sigma(A) \quad \{0\} \quad \{z \quad \mathbb{C} : \mathrm{Re}(z) < 0\}. \tag{2.17}$$

The transformation matrices T considered are given by the product of a positive definite diagonal matrix and a permutation matrix. With this assumption, extending the work of [106], it is shown that for reducible matrices A, a necessary condition for the existence of a positive linear observer of the form (2.13) is that the multiplicity of the zero eigenvalue of A cannot exceed the dimension of the output space p. This condition, together with a number of structural requirements on the system matrices, is shown to be necessary and sufficient.

2.3.5 Variations on the Observer Problem

While we do not analyse these here, *interval* or *bounded observers* are another popular and useful way to estimate the state of a positive linear system [84, 41, 48] or more general systems. An interval observer involves two systems, giving two estimates, $\hat{x}_{lower}$ and $\hat{x}_{upper}$, that are designed in such a way that the real state will always be between these two estimates.

The authors in [7] highlight that an important use of positive observers is to provide bounds on the observed states when they are adequately initialised. It can also be used to take into account the uncertainties that affect the system parameters. If the initial state of the observed system is bounded: $0 \leq x_1 \leq x_0 \leq x_2$, the evolution of the real state $x(t)$ will always be between the estimated states $\hat{x}_{lower}$ and $\hat{x}_{upper}$, where $\hat{x}_{lower}$ has the initial value x_1 and $\hat{x}_{upper}$ has the initial condition x_2. The interval observers $\hat{x}_{upper}$ and $\hat{x}_{lower}$ are constructed in a similar way to a classical observer (2.8). So if we know that the initial state is bounded between two positive values, the two observer states will be nonnegative and converge to the observed state asymptotically. Further results on interval observers can be found in [41, 84, 48], while the reference [76] uses a particular form of positive observer to derive sufficient conditions for an interval observer to exist.

Finally, we note that the problem of observer design has also been considered for control systems over the max-plus algebra, which is used in applications such as scheduling and timetable design [55]. Results on the design of observers for max-plus systems can be found in [53] and later in [54].

2.4 Privacy and control systems

Modern cyber-physical systems in domains such as transport, public health and logistics often require the transmission and processing of sensitive or personal data. Hence, it is crucial to incorporate privacy into the development of such systems that protect user privacy while delivering near optimal performance in order to maintain public confidence in their adoption.

A vast amount of privacy models have been developed over the years, many of which are described in [47]. One such privacy model for tabular databases is k-anonymity [101]. In a k-anonymous table, the record of each individual is indistinguishable from at least $k - 1$ other records. l-diversity is an enhancement on k-anonymity, where it introduces diversity within the k-anonymity class.

In this thesis we will be concentrating on two different types of privacy models, differential privacy and opacity. In the section, we will outline the details and results needed for the work done later in the thesis.

2.4.1 Differential Privacy (DP)

Differential Privacy was first introduced in the Computer Science literature by C. Dwork in [38]. It was initially developed for static, real-valued databases. It is used for privately answering queries to a database. The overall aim of DP is to allow inference on a population level but make it difficult to get information on any individual in the database.

We now recall some formal definitions and results on differential privacy. $(\Omega, \mathcal{F}, \mathsf{P})$ denotes a probability space where $\mathcal{F}$ is a σ-algebra of subsets of Ω and P is a probability measure on Ω.

Given a set D (representing the possible datasets of interest), a static database is represented as a vector d in D^n. The space D^n is equipped with a symmetric, reflexive (but not transitive) adjacency relation . In early papers, d, d D^n were said to be adjacent, d d, if their Hamming distance is equal to one, i.e. if the databases differ in one entry. In later formulations, the adjacency depends on the database and on what may need to be kept private [40].

A **query** is a mapping $Q : D^n \to \mathsf{R}^n$. Given a query Q, a *mechanism* is a collection of random variables $\{X_{Q,d} : d \quad D^n\}$ where $X_{Q,d} : \Omega \to \mathsf{R}^n$ is a

random variable for each $d \quad D^n$. In a slight abuse of notation, we shall often simply refer to the mechanism $X_{Q,d}$.

Definition 2.4.1. Given $\varepsilon > 0$, the mechanism $X_{Q,d}$ is ε-differentially private if

$$\mathsf{P}(X_{Q,d} \quad A) \leq e^{\varepsilon}\mathsf{P}(X_{Q,d} \quad A) \tag{2.18}$$

for all $d \quad d$ in D^n and all Borel sets $A \quad \mathsf{R}^n$.

The idea is that an adversary would be unable to learn a particular person's information from an answer to a query, as the answers from two similar databases are statistically similar.

The concept of relaxed differential privacy is defined by including a second parameter $0 \leq \delta \leq 1$.

Definition 2.4.2. Given $\varepsilon > 0$, $0 \leq \delta \leq 1$, a mechanism $X_{Q,d}$ is (ε, δ) differentially private if

$$\mathsf{P}(X_{Q,d} \quad A) \leq e^{\varepsilon}\mathsf{P}(X_{Q,d} \quad A) + \delta \tag{2.19}$$

for all $d \quad d$ in D^n and all Borel sets $A \quad \mathsf{R}^n$.

To achieve differential privacy, we usually add an appropriate amount of noise to output of the query on the database. To do this, we first we need to calculate the sensitivity of the query:

Definition 2.4.3. Let $q \geq 1$. The l_q-sensitivity of a query Q with respect to an adjacency relation is defined by:

$$\Delta_q(Q) = \sup_{d \ d} \ Q(d) - Q(d\,)_{\ q} \tag{2.20}$$

$.\ _q$ is the usual q-norm on R^n and we are interested in the sensitivity for the cases $q = 1$ and $q = 2$.

To produce a differentially private mechanism we often use the following random variables defined using the Laplace distribution and Gaussian distribution. A Laplace random variable with mean $q \quad \mathsf{R}$ and scale parameter $b > 0$ is a real-valued random variable X with probability density function (pdf)

$$f(x) = \frac{1}{2b}\exp\left(\frac{-|x - q|}{b}\right) \tag{2.21}$$

and its variance is $2b^2$. The Q-function defined as

$$Q(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{u^2}{2})du.$$

Now for $\epsilon > 0$, $0 \leq \delta \leq 0.5$, let $K = Q^{-1}(\delta)$ and define $\kappa_{\delta,\epsilon} = \frac{1}{2\epsilon}(K + \sqrt{K^2 + 2\epsilon})$.

A differentially private mechanism for a database can be defined by

$$X_{Q,d} = Q(d) + w, \tag{2.22}$$

where w is defined as either a Laplace distribution or Gaussian distribution.

1. If w_i, $1 \leq i \leq n$, are iid Laplace random variables with mean zero and scale parameter $b \geq \frac{\Delta_1(Q)}{\varepsilon}$, then (2.22) is ε-differentially private.
2. If w is a white Gaussian noise such that the covarianvce matrix of w is $\sigma^2 I_n$ with $\sigma \geq \kappa_{\delta,\varepsilon}\Delta_2(Q)$, then (2.22) is (ε, δ)-differentially private.

Much of our work will rely on Laplace and Gaussian mechanisms throughout this thesis. However, the exponential mechanism is another popular mechanism. This mechanism is not restricted to queries that are numeric and is a more general mechanism [85, 39].

2.4.2 DP for control systems

Since DP was first developed for static databases, it has been extended in various ways. For our work, we rely heavily on the results in [69, 70] and most recently in [72]. Here, following [69] we review the formulation of differential privacy for a dynamic system. We consider the situation where the private participants contribute the input signals that drive a dynamic system, and the output signals of the system correspond to query outputs.

We consider a system as a causal mapping $G : U \to Y$ between an input space U and an output space Y. U will consist of sequences $u(t)$, t $\mathbb{Z}_+$, where $u(t)$ $\mathbb{R}^m$ for all t; Y consists of sequences $y(t)$, t $\mathbb{Z}_+$ where $y(t)$ $\mathbb{R}^p$ for all t.

The signals in the space U may contain personal information. We assume that a binary adjacency relation, u u , is defined on U. The precise definition of

will depend on context and reflects changes in input signals that differentially private mechanisms should render difficult to detect.

Given a system, $G : U \to Y$ and an adjacency relation on U, a *mechanism* is a set of measurable mappings $Y^{(u)} : \Omega \to Y$, indexed by $u \in U$.

To make a system differentially private, random noise can be added to the output, but this can cause the loss of information. Hence, we wish to calculate as precisely as possible the amount of noise needed to make a mechanism differentially private. To know how much noise to add we must calculate the sensitivity of the system.

Definition 2.4.1. The l_q sensitivity $\Delta_q(G)$ of a system G with respect to an adjacency relation is defined as

$$\Delta_q(G) := \sup_{u \sim u} \|G(u) - G(u')\|_q. \tag{2.23}$$

$\|\cdot\|_q$ on Y is defined by $\|y\|_q = \left(\sum_{k=0}^{\infty} \|y(k)\|_q^q\right)^{1/q}$, where $\|y(k)\|_q$ is the usual l_q norm defined on $\mathbb{R}^m$ for $q = 1, 2$. This definition is a natural extension of the sensitivity for a database defined in (2.20).

To produce a differentially private signal the mechanism in Theorem 2.4.1 from [69] can be used, following definition of the Laplace distribution and Gaussian distribution above in Section 2.4.1.

Theorem 2.4.1. *Let a system G, with m inputs and p outputs and an adjacency relation be given. The mechanism $Y^{(u)} = G(u) + w$, where all $w_{i,k}$, $k \in \mathbb{N}$, $1 \leq i \leq p$, are independent Laplace random variables with mean zero and scale parameter $b \geq \frac{\Delta_1(G)}{\varepsilon}$ is ε-differentially private. If w is instead a white Gaussian noise such that the covarianvce matrix of each sample w_k is $\sigma^2 I_n$ with $\sigma \geq \kappa_{\delta,\varepsilon}\Delta_2(G)$, then the mechanism is (ε, δ)-differentially private.*

These mechanisms are called the Laplace and the Gaussian mechanisms. Typically, the l_2-sensitivity is smaller than its l_1 counterpart, that leads to adding less noise depending on $\delta > 0$ which is one reason for using a Gaussian mechanism.

2.4.3 DP observers

The above results can also be applied to observers of a dynamic system. Here, the observer acts as a substitute for the query in a data set. For a system of the form (2.6) the measurement y that is used to form the observer $\hat{x}$ of the form (2.8) may contain sensitive or private information such as an individual's location, salary, etc. Therefore, when releasing the observer signal, privacy prevention needs to be taken into account. One method of achieving this is to add noise to make the observer differentially private.

Work by Jerome Le Ny in the paper [67] and later expanded on in [68] has heavily movitivated work in this thesis. In this section, we will describe how to apply differential privacy to an observer of a system.

The following definition of adjacency from [67], will be used most often in this thesis.

Let $K > 0$ and $0 \leq \alpha < 1$ be given. Then two sequences y, y are adjacent, $y \quad y$ if

$$t_0 \geq 0 \, s.t. \begin{cases} y(t) = y\,(t), & t < t_0 \\ y(t) - y\,(t)\ _q \leq K\alpha^{t-t_0}, & t \geq t_0 \end{cases} \tag{2.24}$$

where $q = 1$ or $q = 2$. This adjacency definition corresponds to a change in signals due to a small number of people at time t_0. The initial magnitude of the change is K and it decays geometrically at a rate of α.

As noted in [72], input and output perturbations can be applied to the observer to make it differentially private. An input perturbation mechanism can be obtained by adding noise directly to the input y. This method may be preferred when there is a low privacy level requirement or because sensitive information is made private before sending to a third party. The disadvantage of input perturbation is that an unnecessarily large amount of noise may be added which may lead to poor performance of the observer.

For an output perturbation mechanism, a noise signal proportional to the sensitivity of the system is added to the output. This is the method used in [68] and the method we will use throughout this thesis. Adding noise to the output does not impact stability or bias analysis of the observer so we need

to design an observer that has both a good tracking performance for the state trajectory and low sensitivity.

In [68], a differentially private observer for a nonlinear system is designed by using contraction analysis. Contraction theory is used to bound the sensitivity of the system and to compute the noise level needed to ensure privacy.

In [68], the author illustrates the methodology by giving two examples involving the analysis of dynamic data using sensitive information. One of these examples is a syndromic surveillance system that monitors health related data for early detection of epidemic outbreaks. For this example, the measurement y used to form the observer is non-medical data such as searches on a search engine or posts on social media. Using the correlation between this and the proportion of people infected can support early detection of an epidemic outbreak. People may wish to keep information posted online private as it can contain sensitive information.

The syndromic surveillance system is a positive system as it involves the measurement of variables such as a proportion of the population. This is not taken into account when adding Gaussian noise to the observer as it can cause the signal to be negative. This fact is the motivation of much of the work in this thesis.

2.4.4 Other DP applications and Kalman Filter

The choice of adjacency relation depends on the system and the privacy needs of the users. For example, in [72] a system $G : U \to Y$ where the input has n signals, one per participant is studied. Let $u = (u_1, \ldots, u_n)$, with u_i $\mathbb{R}^m$. An adjacency relation can be defined on U by u u if and only if u and u differ by one component signal and this deviation is bounded. Formally, for a fixed set of nonnegative numbers $b = (b_1, \ldots, b_n)$, we define

$$u \quad u \text{ iff for some } i, \quad u_i - u_{i\ r_i} \leq b_i, \quad \text{and } u_j = u_j \text{ for all } j = i \tag{2.25}$$

In [72] the authors produce simple mechanisms with two differentially private versions of G. The first uses input perturbation, which perturbs each input u_i by adding white Gaussian noise and then passing it through the system G.

The second, output perturbation, is done by adding one source of noise to the output of G. Both of these methods produce a different mean square error which depends on the system G and the number of participants, n.

Kalman Filter

In the papers [70, 72] the authors also discuss differentially private Kalman filtering. With Kalman filtering it is assumed that the dynamics of the processes of the individual signals are publicly known. For this we consider a set of n linear systems,

$$x_{i,t+1} = A_i x_{i,t} + b_i w_{i,t},\ t \geq 0,\ 1 \leq i \leq n, \tag{2.26}$$

where w_i is a standard zero-mean Gaussian white noise process with covariance $\mathsf{E}[w_{i,t} w_{i,t}] = \delta_{t-t}$, and the initial condition $x_{i,0}$ is a Gaussian random variable with mean $\bar{x}_{i,0}$. It is assumed that this is independent of the noise w_i. Each system i, for $1 \leq i \leq n$, sends measurements

$$y_{i,t} = c_i x_{i,t} = D_i w_{i,t} \tag{2.27}$$

to a data aggregator.

The data aggregator then wants to release a signal that estimates a linear combination of the individual states and asymptotically minimises the mean squared error. That is, we are looking to construct an estimator $\hat{z}$ of x from the measurement signals y_i. without privacy constraints, the solution is $\hat{z}_t = \sum_{i=1}^{n} L_i \hat{x}_{i,t}$ for given matrices L_i and $\hat{x}_{i,t}$ comes from the steady-state Kalman filter estimating the state of the system i from y_i.

The adjacency relation used in [70, 72] says that two adjacent state trajectories differ by the values of a signal participant, say i. Similar to the method in [69] and in the beginning of [72], we can add noise to different signals to achieve differential privacy. If the participants did not trust the data aggregator, then an input noise injection mechanism can be used. For this, the white Gaussian noise is added directly by the participants to the transmitted signal y_i. Next, they detail the method of output noise injection mechanism, where the white-Gaussian noise is added to the estimate $\hat{z}$ to guarantee (ε, δ) differential privacy.

Within the papers [70, 72], the authors describe filter redesign for stable systems and unstable systems that will guarantee differential privacy concerning

the adjacency relation. A practical example is detailed of a traffic monitoring system, where the state represents a vehicle's position and velocity on a straight road. The measurement y_i is GPS measurements from the vehicles.

2.5 Opacity and linear systems

While differential privacy has emerged as the dominant framework for incorporating privacy protections into control design for continuous-state systems, the related concept of *opacity* has attracted far more attention in the Discrete Event Systems (DES) community.

In the paper [74], the author considers the relationship between opacity and various other system theoretic concepts for discrete event systems (DES) modelled using finite state automata. In particular, they define two types of opacity: strong and weak opacity. By properly specifying the languages and observation mapping, the authors show that three properties of DES; observation, diagnosability, and detectability can be reformulated as opacity.

Formally, they model a DES by an automaton $G = (\Sigma, X, \delta, x_0, X_m)$, where Σ is the set of events, X is the state space, δ is the transition function, x_0 is the initial state and X_m X is the set of so-called marked states. The partially defined function $\delta : X \times \Sigma \to X$ determines the system dynamics where $\delta(x, \sigma) = y$ if the execution of σ Σ from state x takes the system to state y. If the execution of σ for x X is defined then we write $\delta(x, \sigma)!$. The language generated by G is defined by $L(G) = \{s \quad \Sigma \ : \delta(x_0, s)!\}$; thus $L(G)$ contains all possible strings that can be generated by the system. More generally, a langauge is a subset of Σ . In the study of opacity for DES, the notion of an observation map that characterises those events that are visible to an outside agent or observer is key. This is a mapping $\theta : \Sigma \to \Sigma$, where if the event s happens the agent can only see the events in $\theta(s)$. For a language L Σ we define $\theta(L) = \{t \quad \Sigma \ ; \ s \quad L, t = \theta(s)\}$ and its inverse image is given by, $\theta^{-1}(L) = \{t \quad \Sigma \ ; \theta(t) \quad L\}$.

With the above notation we now recall the definitions of opacity for a DES as follows:

Definition 2.5.1. Given two languages L_1, L_2 $L(G)$, L_1 is strongly opaque

with respect to L_2 and the observation map θ if

$$L_1 \quad \theta^{-1}(\theta(L_2)).$$

L_1 is weakly opaque with respect to L_2 and θ if

$$L_1 \cap \theta^{-1}(\theta(L_2)) = \quad .$$

With the above notations and definitions, the author of [74] characterises the properties of anonymity and secrecy as special cases of opacity and relates it to detectability.

For detectability, let $\Sigma^{>N}$ denote the set of strings in Σ that have length greater then N. Then for any state $x \quad X$ let $L_x = \{s \quad L(G) : \delta(x_0, s) = x\}$, $L_{\ x} = \{s \quad L(G) : \delta(x_0, s) = x\}$, and $L_x^{>N} = L_x \cap \Sigma^{>N}$. With this notation we can define strong detectability as follows.

Definition 2.5.2. A DES G is strongly detectable with respect to the observation map θ if there exists a positive integer N such that for all $x \quad X$,

$$s \quad L_x^{>N}, \quad s \quad \Sigma \ , \theta(s) = \theta(s\ ) \ = \quad s \ / \ L_{\ x}.$$

The main idea is that if the string s is long enough and the corresponding execution terminates in the state x, then every string s that looks like s with respect to θ gives an execution that leads to the state x. The following theorem is shown in [74].

Theorem 2.5.1. *A DES G is strongly detectable with respect to θ if and only if there exist a positive integer N such that for all $x \quad X$, $L_x^{>N}$ is not opaque with respect to $L_{\ x}$ and θ.*

State-based opacity

The state-based approach for opacity of DES was first introduced in [25, 92]. It relates to the intruder's ability to infer the system is or has been in some secret state or set of states. Different opacity properties have been defined depending on the nature of the secret sets. In [61], the authors give details on these different opacity properties.

A system is *current-state opaque (CSO)*, if the intruder can never infer whether the current state of the system in a secret state or not from the observation.

A system is *initial-state opaque (ISO)*, if the observer is never sure whether the system's initial state was a secret state or not.

Initial-and-final-state opacity (IFO), is an extension of ISO and CSO that requires the initial and final state to be hidden from the intruder.

K-step opacity is a more general property where it keeps secret the fact that the system was in a secret state a number of steps ago. This can be extended to *infinite-step opacity*.

2.5.1 Opacity for Linear Systems

In the paper [89], the authors describe a notion of state based opacity for a linear time invariant system as opposed to the language based opacity considered in [74]. The familiar definition of the observability problem aims to determine the initial state $x(0)$, given all the output and control history. However, in [89], the adversary only has access to a snapshot of the system and must determine the initial state. It is assumed that the adversary makes one observation at some time k. In [74], the observation of the entire secret trajectory must coincide with the non-secret trajectory, but in [89] only the secret and non-secret outputs at time k need to coincide. We now describe this work more formally.

Consider the discrete-time LTI system

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ x(0) &= x_0 \quad X_0 \\ y(t) &= Cx(t) \end{aligned} \tag{2.28}$$

where x R^n, u R^m, y R^p and A, B, C are real matrices of appropriate dimensions. Let X_s, X_{ns} X_0, where s corresponds to secret initial states and ns corresponds to non-secret initial states. Let K be a set of positive integers corresponding to the times the adversary will observe the system.

Now, we will define what it means for X_s to be strongly/weakly K initial state opaque (ISO) with respects to X_{ns} [89].

Definition 2.5.3. For (2.28), given X_s, X_{ns} X_0 and K, X_s is strongly K-ISO with respect to X_{ns} if for all k K, for all $x_s(0)$ X_s and every admissible control sequence $u_s(0), \ldots, u_s(k)$, there exists an $x_{ns}(0)$ X_{ns} and an admissible control sequence $u_{ns}(0), \ldots, u_{ns}(k)$ such that $y_s(k) = y_{ns}(k)$.

Definition 2.5.4. X_s is weakly K-ISO with respect to X_{ns} if for all k K, there exists $x_s(0)$ X_s, an admissible control sequence $u_s(0), \ldots, u_s(k)$, $x_{ns}(0)$ X_{ns} and an admissible control sequence $u_{ns}(0), \ldots, u_{ns}(k)$ such that $y_s(k) = y_{ns}(k)$.

Let $X_s(k)$ and $X_{ns}(k)$ denote the sets of reachable states in k steps, starting from X_s and X_{ns}. In [89], results are given that characterise the properties of X_s being strongly/weakly k-ISO with respect to X_{ns}, in terms of how the sets $X_s(k)$ and $X_{ns}(k)$ relate to each other with respect to the action of the observation map C from (2.28). The authors also present theorems describing how the weak/strong properties of k-ISO behave with respect to unions and intersections of secret and non-secret subsets of X_0.

Some of the results in [89] are framed in terms of the concept of output-controllability which we now define.

Definition 2.5.5. A state x of (2.28) is output controllable on $[0, k]$ if there exists a control sequence $\{u(\cdot)\}$ that transfers the system from $x(0) = x$ to $y(k) = 0$.

The authors then determine conditions under which k-ISO is equivalent to output controllability. These conditions are outlined in the following theorem.

Theorem 2.5.2. *Let X_s be (strongly or weakly) k-ISO with respect to X_{ns}. Then there exists a state of (2.28) that is output controllable on $[0, k]$.*

In [88], the authors also define several notions of decentralized opacity in the presence of multiple adversaries. The definition of decentralized opacity is proposed for the presence or absence of collusion among the adversaries and the presence or absence of a coordinator that aggregates information based on the adversaries' observations.

The first case considered is that of *no coordinator, no collusion*, where the agents do not communicate with each, and there is no coordinator. The next

case is *with coordinator, no collusion*, where there is a coordinator, who polls the observations of each adversary and decides on co-opacity according to some rule. Here, the coordinator does not know the system model or observation maps and can not do any better with this knowledge. The last case is *no coordinator, with collusion*, where there is no coordinator, but the adversaries communicate with each other.

In the last section of the paper [88], the authors define a weaker form of opacity, ε-k-ISO. For this to hold the outputs from the secret and non-secret states differ, by a predefined amount, ε.

The results form [89] and [88] have been combined into a more recent journal paper [90] with the addition of extra results. The additional material considers the relationship between opacity and reach-set approximations. This line of work follows on from the conditions to establish k-ISO for sets of reachable states, $X(k)$, where $X(k)$ is the set of reachable states in k steps from a set of initial states X. The second novel section in [90] considers opacity for nonlinear systems. Here, the authors define k-ISO and conditions for k-ISO, which is similar to the definition and results for a linear system in [89].

2.6 Conclusions

In this chapter, we have discussed various definitions and results on positive linear systems and the positive linear observer problem. We also described two privacy concepts: differential privacy and opacity. Throughout this thesis, our major theme is the combination of positive systems with privacy concerns; specifically we study several design questions for a positive linear system that preserve that privacy of individuals who contribute data to the system. Some of the main topics we will consider in the following chapters are the following:

- the design of differentially private mechanisms that produce nonnegative outputs;
- bounds for the sensitivity of positive linear observers with a view to construct differentially private observers using Laplace and Gaussian distributions;
- optimisation problems related to the bounds mentioned above;

- the problem of opacity for positive linear systems.

CHAPTER 3

Differential Privacy and Positivity

In this chapter, our main focus is on the bias and the mean square error (MSE) of nonnegative Laplace mechanisms. We consider two methods of constructing these mechanisms: post-processing *and* restriction*. We present explicit formulae for the bias of restricted Laplace mechanisms and Laplace mechanisms obtained by post-processing with the standard ramp function, which sets negative values to zero. Post-processing with the ramp function always leads to lower bias than restriction. We briefly discuss multiplicative mechanisms for positive data that were proposed in [71] and show that, without extra restrictions, these mechanisms can lead to infinite bias. We then consider alternative post-processing functions and show that lower bias can be achieved by using translated ramp functions. We determine the optimal such function that minimises the worst case bias. A major contribution of this chapter is to show that bias is unavoidable for any post-processed nonnegative Laplace mechanism that has finite first and second moments. A corresponding result is also proven for restricted mechanisms, where the original base mechanism is not necessarily a Laplace mechanism. The final topic of the chapter is the mean square error (MSE) of post-processed and restricted Laplace mechanisms. We prove the existence of a square-integrable post-processing function that minimises the worst case MSE for the Laplace mechanism.*

3.1 Introduction

It has been said before [56] that the Laplace mechanism is the "workhorse of differential privacy". It is one of the most popular and widely used mechanisms for real-valued data [38]. Recently, various extensions and adaptations of this basic mechanism have been studied. In [99] a discrete Laplace mechanism was introduced for *individual differential privacy*. A shortcoming of the mechanism for some situations is that the Laplace distribution is unbounded, and the range of Laplace random variables is the real line, R. For contexts where data is bounded, in some interval $[l, u]$ R, this is not suitable. This has led researchers to consider ways of adapting the basic Laplace mechanism for such data [56, 76]. In [75] two approaches to this question were presented: *truncation* and *boundary inflated truncation*; the main focus was on ε (strict) differential privacy and the authors derived formulae for the bias introduced by both of these approaches as well as upper bounds for their mean square error (MSE). In [56], the use of truncation (referred to as bounding in [56]) for generating bounded mechanisms satisfying (ε, δ) differential privacy was studied and, using techniques from Fixed Point Theory, conditions for the bounded Laplace mechanism to be differentially private were derived.

Our interest in this chapter is in nonnegative, unbounded data arising from queries whose range is the half-line $[0, \infty)$. Boundary inflated truncation corresponds to post-processing [40] the Laplace mechanism with the ramp function. For this reason, we refer to mechanisms obtained using this method, and generalisations of it, as *post-processed* mechanisms. We refer to nonnegative mechanisms constructed by analogy with truncation as *restricted* mechanisms. Our objective in this chapter is to study in detail the bias of post-processed and restricted nonnegative mechanisms for ε differential privacy. Formulae corresponding to those in [75] are readily derived for mechanisms constructed by restriction or post-processing with the ramp function. It is natural to ask whether lower bias can be achieved by post-processing with alternative functions. We show that this is indeed possible simply by translating the ramp function and determine the *translated ramp function* that achieves minimal bias (in a sense made precise later). A second related question concerns whether or not bias is inevitable for mechanisms obtained using the constructions here. We show that this is indeed the case and present results on this question for both post-processed Laplace mechanisms, and general restricted

mechanisms.

To finish the chapter, we calculate the MSE of both the restricted mechanism and the post-processed mechanism with the simple ramp function. We also prove the existence of a square-integrable post-processing function that minimises the worst case mean square error for the Laplace mechanism.

3.2 Background and Notation

In this section, for the convenience of the reader, we fix the main notation and terminology that is used throughout the chapter. We also recall the main definitions and results related to differential privacy needed in the chapter. Our notation and formulation of differential privacy follows the general formalism outlined in the paper [57].

In Chapter 2, in Section 2.4.1, we give a detailed background on differential privacy for a database and queries defined on R^n, in this chapter we will be concerned with queries taking values in R.

Let a set D representing the possible datasets of interest be given which is equipped with a adjacency relation . We consider a real-valued **query** $Q : D \to \mathsf{R}$. Given a query Q, as is standard, a *mechanism* is a collection of random variables $\{X_{Q,d} : d \in D\}$ where $X_{Q,d} : \Omega \to \mathsf{R}$ is a real-valued random variable for each $d \in D$. In a slight abuse of notation, we shall often simply refer to the mechanism $X_{Q,d}$.

If Q has range $Q(D)$, an *output perturbation mechanism* is defined by specifying a family $\{Y_q : q \in Q(D)\}$ of random variables $Y_q : \Omega \to \mathsf{R}$. Given such a family, for $d \in D$, we set $X_{Q,d} = Y_{Q(d)}$. All of the mechanisms considered later in the chaper take this form.

Given $\varepsilon > 0$, the mechanism $X_{Q,d}$ is ε-differentially private if

$$\mathsf{P}(X_{Q,d} \in A) \leq e^{\varepsilon}\mathsf{P}(X_{Q,d'} \in A) \tag{3.1}$$

for all $d \sim d'$ in D and all Borel sets $A \subseteq \mathsf{R}$.

For real-valued queries, we have only one notion of sensitivity, defined using the absolute value. The **sensitivity** of the query $Q : D \to \mathsf{R}$ is given by:

$$\Delta(Q) := \sup\{|Q(d) - Q(d')| : d, d' \in D, d \sim d'\}.$$

Base and derived mechanisms

Throughout this chapter, $Q : D \to \mathsf{R}_+$ is a nonnegative valaued query with sensitivity Δ. We assume that a family of random variables $\{Y_q : q \quad \mathsf{R}_+\}$ is given where the range of each Y_q is R and $\mathsf{E}[Y_q] = q$; informally, q corresponds to the 'true' value of the query so we are assuming the base mechanism is unbiased. We refer to the associated mechanism $X_{Q,d} = Y_{Q(d)}$ as the *base mechanism*. We assume that the mechanism $X_{Q,d}$ is ε differentially private for some $\varepsilon > 0$.

The main focus of this chapter is to construct and analyse a *derived family* $\{\hat{Y}_q : q \quad \mathsf{R}_+\}$ of nonnegative-valued random variables where each $\hat{Y}_q$ has range R_+, such that the *derived mechanism* $\hat{X}_{Q,d} = \hat{Y}_{Q(d)}$ is differentially private and nonnegative.

The **bias** of $\hat{X}_{Q,d}$ is $\mathsf{E}[X_{Q,d}] - Q(d)$. The form of $X_{Q,d}$ and the nonnegativity of the query Q means that it is enough to consider $\mathsf{E}[Y_q] - q$ for $q \geq 0$.

A major focus of this chapter, is the *maximal absolute bias* of the family $\{\hat{Y}_q : q \geq 0\}$ of derived random variables.

Definition 3.2.1. The maximal absolute bias of $\{\hat{Y}_q : q \geq 0\}$ is given by

$$B := \sup\{|\mathsf{E}[\hat{Y}_q] - q| : q \quad \mathsf{R}_+\}. \tag{3.2}$$

Laplace mechanisms

For most of the chapter, the base mechanism will be the Laplace mechanism, constructed using a family of Laplace random variables, whose definition we now recall from Chapter 2.

A Laplace random variable with mean $q \quad \mathsf{R}$ and scale parameter $b > 0$ is a real-valued random variable X with probability density function (pdf) given by

$$f(x) = \frac{1}{2b}\exp\left(-\frac{|x - q|}{b}\right), \quad x \quad \mathsf{R}. \tag{3.3}$$

Throughout this chapter, we shall use L to denote a Laplace random variable with mean 0 and scale parameter b, where the scale parameter will be made clear in context. Clearly, a Laplace random variable L has range R.

The following result concerning the Laplace mechanism and differential privacy, is a particular case of Theorem 2.4.1 in Chapter 2.

Proposition 3.2.1. *Let $Q : D \to \mathsf{R}$ have sensitivity Δ and $\varepsilon > 0$ be given. The* Laplace mechanism *defined by $X_{Q,d} = Q(d) + L$ where $L : \Omega \to \mathsf{R}$ is a Laplace random variable with mean 0 and scale parameter $b \geq \frac{\Delta}{\varepsilon}$ is ε-differentially private.*

The Laplace mechanism is determined by the family of random variables $\{Y_q = q + L : q \quad Q(D)\}$. This notation (for the case where $Q(D) = [0, \infty)$) will be used frequently in the chapter.

3.3 Nonnegative derived mechanisms via post-processing and restriction

In this section, we describe the two approaches to constructing derived nonnegative mechanisms that shall be studied for the rest of the chapter. We first discuss the approaches for a general base mechanism before specialising to the case of the Laplace mechanism in the following sections.

Let $\varepsilon > 0$ be given and consider a family $\{Y_q : q \quad \mathsf{R}_+\}$ of real-valued random variables where the range of each Y_q is R. Assume that the base mechanism $X_{Q,d} = Y_{Q(d)}$ is ε differentially private.

3.3.1 Post-processing and restriction – general case

We now describe two general results that can be used to construct a derived mechanism $\hat{X}_{Q,d} = \hat{Y}_{Q(d)}$ which is nonnegative-valued and also differentially private.

Post-processing

The first technique is based on the following fundamental, and well-known, fact [40].

Proposition 3.3.1. *Let $X_{Q,d} : \Omega \to \mathsf{R}$ be an ε differentially private mechanism for the query $Q : D \to \mathsf{R}_+$. Let $\phi : \mathsf{R} \to \mathsf{R}_+$ be measurable. Then the mechanism $\hat{X}_{Q,d}$ given by $\hat{X}_{Q,d}(\omega) = \phi(X_{Q,d}(\omega))$ for $d \quad D$ is ε differentially private.*

Remark: The last result is also true in the more general case of relaxed (ε, δ) differential privacy [57, 40] and for queries Q and mappings ϕ taking values in an arbitrary measurable output set (as opposed to the real line R). For our purposes, the form stated in Proposition 3.3.1 is sufficient.

Restriction

Our second construction is inspired by the exponential mechanism of McSherry and Talwar [85]. It is essentially the same technique that was used in [75] to construct the boundary inflated truncation mechanism for bounded mechanisms. We include a brief proof here in the interests of completeness.

Proposition 3.3.2. *Let $X_{Q,d} : \Omega \to \mathsf{R}$ be an ε differentially private mechanism for the query $Q : D \to \mathsf{R}_+$. If the family of measurable mappings $\hat{X}_{Q,d} : \Omega \to \mathsf{R}_+$ for $d \quad D$ satisfies*

$$\mathsf{P}(\hat{X}_{Q,d} \quad A) = \frac{\mathsf{P}(X_{Q,d} \quad A)}{\mathsf{P}(X_{Q,d} \quad \mathsf{R}_+)} \tag{3.4}$$

for all $d \quad D$ and all measurable subsets $A \quad \mathsf{R}_+$, then $\hat{X}_{Q,d}$ is 2ε differentially private.

Proof: Let $d \quad d$ be given and let $A \quad E$ be measurable. Then as $X_{Q,d}$ is ε differentially private:

$$\mathsf{P}(X_{Q,d} \quad A) \leq e^{\varepsilon}\mathsf{P}(X_{Q,d} \quad A); \ \mathsf{P}(X_{Q,d} \quad \mathsf{R}_+) \leq e^{\varepsilon}\mathsf{P}(X_{Q,d} \quad \mathsf{R}_+). \tag{3.5}$$

Combining the two above inequalities we see that

$$\begin{aligned} \mathsf{P}(\hat{X}_{Q,d} \quad A) &= \frac{\mathsf{P}(X_{Q,d} \quad A)}{\mathsf{P}(X_{Q,d} \quad \mathsf{R}_+)} \\ &\leq \frac{e^{\varepsilon}\mathsf{P}(X_{Q,d} \quad A)}{e^{-\varepsilon}\mathsf{P}(X_{Q,d} \quad \mathsf{R}_+)} \\ &= e^{2\varepsilon}\mathsf{P}(\hat{X}_{Q,d} \quad A). \end{aligned}$$

□

Remarks:

(i) For the rest of the chapter, mechanisms constructed using Proposition 3.3.1 shall be referred to as *post-processed mechanisms* and those constructed using Proposition 3.3.2 shall be called *restricted mechanisms*.

(ii) Versions of both Proposition 3.3.1 and Proposition 3.3.2 for the construction of mechanisms taking values in some bounded interval $[l, u]$ can be found in the recent papers [56, 75].

3.3.2 Post-processing and restriction - Laplace mechanism

We now consider the particular case where the base mechanism is a Laplace mechanism. So, let $\varepsilon > 0$ be given and let L denote a Laplace random variable with mean 0 and scale parameter $b = \frac{\Delta}{\varepsilon}$. For q R_+, set $Y_q = q + L$ and $X_{Q,d} = Y_{Q(d)} = Q(d) + L$. It is straightforward to construct nonnegative derived mechanisms using Proposition 3.3.1 and Proposition 3.3.2. We deal with the simpler case of post-processing first.

Post-processing and differential privacy

By Proposition 3.2.1, the base mechanism $X_{Q,d}$ is ε differentially private. Now consider the derived mechanism $\hat{X}_{Q,d} = \tau(X_{Q,d})$ where $\tau : \mathsf{R} \to [0, \infty)$ is the *ramp function* given by:

$$\tau(x) = \begin{cases} x & \text{if } x \geq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{3.6}$$

As τ is continuous and hence measurable, it is immediate from Proposition 3.3.1 that $\hat{X}_{Q,d}$ is ε differentially private. Later we shall consider various questions related to more general choices of the post-processing function. Note that if we set $\hat{Y}_q = \tau(Y_q)$, then $\hat{X}_{Q,d} = \hat{Y}_{Q(d)}$.

Constructing nonnegative mechanisms via restriction

Proposition 3.3.2 shows that if a mechanism $\hat{X}_{Q,d}$ satisfies (3.4) then it will be 2ε differentially private. We now show how to implement a derived mechanism satisfying (3.4) given a base mechanism $X_{Q,d}$. This is of course an important consideration for practical applications.

Let $q \geq 0$ be given. We will describe how to construct a random variable, $L_q : \Omega \to [-q, \infty)$ satisfying

$$\mathsf{P}(L_q \quad A) = \frac{\mathsf{P}(L \quad A)}{\mathsf{P}(L \quad [-q, \infty))}, \tag{3.7}$$

for all measurable $A \quad [-q, \infty)$.

The first step is to calculate the cumulative distribution function (cdf) F_q of a random variable L_q satisfying (3.7).

Proposition 3.3.3. *Let $L : \Omega \to \mathbb{R}$ be a Laplace random variable with mean 0 and scale parameter $b > 0$ and let $q \geq 0$ be given. If $L_q : \Omega \to [-q, +\infty)$ satisfies (3.7), the cumulative distribution function F_q of L_q is given by:*

$$F_q(x) = \begin{cases} 1 - \frac{e^{\frac{-x}{b}}}{2 - e^{\frac{-q}{b}}} & x > 0 \\ \frac{e^{\frac{x}{b}} - e^{\frac{-q}{b}}}{2 - e^{\frac{-q}{b}}} & -q \leq x \leq 0 \\ 0 & x < -q \end{cases} . \tag{3.8}$$

Proof: For $x \geq -q$:

$$F_q(x) = \mathbb{P}(L_q \quad [-q, x]) = \frac{\int_{-q}^{x} e^{-\frac{|\xi|}{b}} d\xi}{\int_{-q}^{\infty} e^{-\frac{|\xi|}{b}} d\xi} \tag{3.9}$$

The integral $\int_{-q}^{\infty} e^{-\frac{|\xi|}{b}} d\xi$ can be readily calculated as:

$$\int_{-q}^{\infty} e^{-\frac{|\xi|}{b}} d\xi = b(2 - e^{-\frac{q}{b}})$$

For $\int_{-q}^{x} e^{-\frac{|\xi|}{b}} d\xi$ by considering the two cases, $x > 0$, $-q \leq x \leq 0$, a straightforward calculation then shows that $F_q(x)$ is given by (3.8). $\square$

Using the expression for F_q in (3.8), we can use a standard technique in Probability Theory to construct L_q satisfying (3.7). As $F_q : [-q, \infty) \to [0, 1)$ is a strictly increasing function, $F_q^{-1} : [0, 1) \to [-q, \infty)$ is well defined. Let $U : \Omega \to [0, 1]$ be a uniform random variable, and set

$$L_q(\omega) = F_q^{-1}(U(\omega)). \tag{3.10}$$

It is easy to see that L_q will have cdf given by F_q. For this, note that for $x \geq -q$:

$$\begin{aligned} \mathbb{P}(L_q(\omega) \leq x) &= \mathbb{P}(F_q^{-1}(U(\omega)) \leq x) \\ &= \mathbb{P}(U(\omega) \leq F_q(x)) \\ &= F_q(x). \end{aligned}$$

As F_q is monotonically increasing and $F_q(0) = \frac{1-e^{-\frac{q}{b}}}{2-e^{-\frac{q}{b}}}$, for x $[0,1)$:

$$F_q^{-1}(x) = \begin{cases} -b\ln[(1-x)(2-e^{-\frac{q}{b}})] & x > \frac{1-e^{-\frac{q}{b}}}{2-e^{-\frac{q}{b}}} \\ b\ln[(1-x)e^{-\frac{q}{b}} + 2x] & x \leq \frac{1-e^{-\frac{q}{b}}}{2-e^{-\frac{q}{b}}} \end{cases} \tag{3.11}$$

To generate noise from a random variable satisfying (3.7), we take the output u from a uniformly distributed random variable U on $[0,1]$, (which can be simulated using standard functions provided by packages such as MATLAB or Octave) and evaluate $F_q^{-1}(u)$.

Finally, set $\hat{Y}_q = q + L_q$ for all $q \geq 0$ and $\hat{X}_{Q,d} = \hat{Y}_{Q(d)}$. By construction, $\hat{Y}_q$ maps into $[0, \infty)$. Moreover, it is a straightforward application of Proposition 3.3.2 to see that the derived mechanism $\hat{X}_{Q,d}$ is 2ε differentially private.

Corollary 3.3.4. *Let $\varepsilon > 0$ and $Q : D \to \mathsf{R}_+$ be given. Further, let L be a Laplace random variable with mean 0 and scale parameter $b = \frac{\Delta(Q)}{\varepsilon}$ and for $q \geq 0$, let L_q satisfy (3.7). Then the mechanism defined by $\hat{X}_{Q,d} = \hat{Y}_{Q(d)}$ is 2ε differentially private.*

Proof: We know that $X_{Q,d} = Q(d) + \mathsf{L}$ is ε differentially private. Note that for any measurable A $[0, \infty)$:

$$\begin{aligned} \mathsf{P}(\hat{X}_{Q,d} \quad A) &= \mathsf{P}(L_{Q(d)} \quad A - Q(d)) \\ &= \frac{\mathsf{P}(L \quad A - Q(d))}{\mathsf{P}(L \quad [-Q(d), \infty))} \\ &= \frac{\mathsf{P}(X_{Q,d} \quad A)}{\mathsf{P}(X_{Q,d} \quad [0, \infty))}. \end{aligned}$$

It follows immediately from Proposition 3.3.2 that $\hat{X}_{Q,d}$ is 2ε differentially private as claimed. □

3.4 Bias for nonnegative derived Laplace mechanisms

As in the previous section, we assume that the base mechanism is a Laplace mechanism so that $\mathsf{E}[X_{Q,d}] = Q(d)$ and the mechanism is unbiased. The bias of the derived mechanism $\hat{X}_{Q,d}$ is given by $\mathsf{E}[\hat{X}_{Q,d}] - Q(d)$. In this subsection, we show that the post-processed Laplace mechanism $\hat{X}_{Q,d} = \tau(X_{Q,d})$ where

τ is given by (3.6), and the restricted Laplace mechanism both have positive bias. We also determine which of the approaches leads to a larger bias.

Post-processing and bias

As above, for $q \geq 0$, $Y_q = q + L$ is a Laplace random variable with mean q and scale parameter b. We now compute the expected value of $\hat{Y}_q = \tau(Y_q)$. The bias of the mechanism $\hat{X}_{Q,d}$ at $d \quad D$ is then equal to $\mathsf{E}[\hat{Y}_{Q(d)}] - Q(d)$.

The next result gives the expected value of the random variable Y_q for $q \geq 0$ and can be verified by direct calculation.

Proposition 3.4.1. *Let $Y_q : \Omega \to \mathsf{R}$ be a Laplace random variable with mean $q \geq 0$ and scale parameter b. Let $\hat{Y}_q = \tau(Y_q)$ where τ is given by (3.6). Then*

$$\mathsf{E}[\hat{Y}_q] = q + \frac{b}{2} \exp\left(\frac{-q}{b}\right).$$

Proof: The expectation of $\hat{Y}_q = \tau(Y_q)$ can be readily shown by direct calculation to be:

$$\begin{aligned} \mathsf{E}[\hat{Y}_q] &= \frac{1}{2b} \int_0^\infty x e^{\frac{-|x-q|}{b}} dx \\ &= q + \frac{b}{2} e^{-\frac{q}{b}}. \end{aligned}$$

□

Remark: It follows immediately from Proposition 3.4.1 that, for $b = \frac{\Delta}{\varepsilon}$ the bias of $\hat{Y}_q = \tau(Y_q)$ is $\frac{\Delta}{2\varepsilon} e^{-\frac{q\varepsilon}{\Delta}}$.

Restricted mechanisms and bias

In order to quantify the bias of restricted Laplace mechanisms, we first compute an expression for the expected value of the random variables $L_q : \Omega \to [-q, \infty)$ satisfying (3.7).

Lemma 3.4.2. *Let L be a Laplace random variable with mean 0 and scale parameter $b > 0$ and let $q \geq 0$ be given. If $L_q : \Omega \to [-q, +\infty)$ satisfies (3.7), then*

$$\mathsf{E}[L_q] = \frac{1}{2e^{\frac{q}{b}} - 1}(q + b).$$

Proof: We use the fact [46] that for a nonnegative random variable Y, with cumulative distribution function $F(\cdot)$,

$$\mathsf{E}[Y] = \int_0^\infty \mathsf{P}(Y > t)dt = \int_0^\infty (1 - F(t))dt.$$

While L_q is not nonnegative, the random variable $q + \mathsf{L}_q$ is. Let $F_+(t)$ denote the cumulative distribution function of $q + \mathsf{L}_q$. Then $F_+(t) = F_q(t - q)$ for $t \geq 0$. Hence, $\int_0^\infty (1 - F_+(t))dt = \int_{-q}^\infty (1 - F_q(\xi))d\xi$. Therefore, with some simple integration

$$\mathsf{E}[q + \mathsf{L}_q] \;=\; q + \frac{1}{2e^{\frac{q}{b}} - 1}\,(q + b)\,.$$

It now follows immediately that

$$\mathsf{E}[\mathsf{L}_q] = \frac{1}{2e^{\frac{q}{b}} - 1}(q + b).$$

□

Corollary 3.4.3. *Let L be a Laplace random variable with mean 0 and scale parameter $b = \frac{\Delta}{\varepsilon}$, let $q \geq 0$ be given, and let $\mathsf{L}_q : \Omega \to [-q, +\infty)$ satisfy (3.7). The bias of the restricted derived mechanism $\hat{Y}_q = q + L_q$ is given by*

$$\frac{q\varepsilon + \Delta}{2\varepsilon e^{\frac{q\varepsilon}{\Delta}} - \varepsilon}.$$

Proof: This follows immediately from Lemma 3.4.2.

3.4.1 Comparison of bias for post-processing and restriction

We wish to compare mechanisms with the same guaranteed level of differential privacy, as quantified by the parameter ε. With this in mind, for the post-processed mechanism, we take the scale parameter $b = \frac{\Delta}{\epsilon}$, while for the restricted Laplace mechanism, we should take $b = \frac{2\Delta}{\varepsilon}$.

Consider the ratio between $B_1 = \frac{\Delta}{2\varepsilon} \exp\left(\frac{-\varepsilon q}{\Delta}\right)$ (the bias of a post-processed mechanism) and $B_2 = \frac{1}{2\exp(\frac{\varepsilon q}{2\Delta}) - 1}(q + \frac{2\Delta}{\varepsilon})$ (the bias of the restricted mechanism). After some algebraic manipulation, we find that:

$$\frac{B_2}{B_1} = \frac{2\exp(\frac{\varepsilon q}{\Delta})}{2\exp(\frac{\varepsilon q}{2\Delta}) - 1}\left(\frac{\varepsilon q}{\Delta} + 2\right) > 2. \tag{3.12}$$

This simple calculation shows that post-processing leads to a bias that is always strictly less than that caused by restriction for the Laplace mechanism.

3.4.2 Positivity and Log-Laplace Random Variables

We now briefly describe a different approach taken in [71]; the authors considered the problem of how to release models of dynamic systems (described via transfer functions, for example) in a differentially private manner. In order to accurately reflect the stability properties of the models considered, such mechanisms need to preserve the sign of some important model parameters. The authors introduced a *multiplicative mechanism* based on the *log-Laplace* distribution that preserves positivity; they refer to this as a sign-preserving mechanism. This technique can prove useful provided we impose restrictions on the queries considered and on the adjacency relation on D. We now briefly describe how it would apply to the general nonnegative valued queries considered here, and we explain why it is not appropriate for this general context.

A key assumption is that $Q : D \to (0, \infty)$ is a positive valued query for which there is some $K > 0$ such that for all $d \quad d'$:

$$\frac{|Q(d) - Q(d')|}{\min\{Q(d), Q(d')\}} \leq K. \tag{3.13}$$

This then implies that the query $\log(Q) : D \to \mathsf{R}$ will have sensitivity bounded above by K. Hence the mechanism $X_{Q,d} = \log(Q(d)) + \mathsf{L}$ is ε differentially private where L is a Laplace random variable with mean 0 and $b = \frac{K}{\epsilon}$. As differential privacy is invariant under post-processing, it follows that the positive mechanism

$$\hat{X}_{Q,d} = e^{X_{Q,d}} = Q(d)e^{L}$$

is also ε differentially private.

While this technique can be used for queries satisfying (3.13) and was applied successfully to the problem of releasing dynamic models in a differentially private manner while preserving stability properties, there are several issues with its use for the more general setting considered here.

- From the form of (3.13) it is clear that the technique is unsuitable to queries which can take the value 0.
- Even when the query is strictly positive, the bound K may be significantly larger than the sensitivity of the query itself, meaning that a greater level of noise is required. In fact, it may not be possible to obtain a finite bound K. As a simple example, if we take $D = (0, 1]^n$ and

$Q : D \to (0, 1]$ to be the mean $Q(d) = \frac{\sum_{i=1}^{n} d_i}{n}$, then the sensitivity of Q is easily seen to be $\frac{1}{n}$. On the other hand, set $d = (\gamma, \gamma, \ldots, \gamma)$ and $d' = (1, \gamma, \gamma, \ldots, \gamma)$ and consider the standard adjacency relation given by $d \sim d'$ if for some i, $d_j = d'_j, j = i$. Then

$$\frac{|Q(d) - Q(d')|}{\min\{Q(d), Q(d')\}} = \frac{1 - \gamma}{\gamma n}.$$

Thus by choosing γ sufficiently small, we see that there is no finite K for which (3.13) will be satisfied in this case.

- Following on from the last point, the next result illustrates that even if the query Q satisfies (3.13) for some finite $K > 0$, the multiplicative mechanism will fail to have finite expectation unless K satisfies additional restrictions. This is clearly undesirable.

Proposition 3.4.4. *Let $K > 0$, $\varepsilon > 0$ be given and let $Q : D \to (0, \infty)$ be a query satisfying (3.13). Further, let $\hat{X}_{Q,d} = Q(d)e^{L}$ be the multiplicative mechanism with L a Laplace random variable with mean 0 and scale parameter $b = \frac{K}{\varepsilon}$. Then the expected value $\mathsf{E}[\hat{X}_{Q,d}] < \infty$ if and only if $K < \varepsilon$.*

Proof: If L is a Laplace random variable with mean 0 and scale parameter $b > 0$, then

$$\mathsf{E}[e^{L}] = \frac{1}{2b} \int_{-\infty}^{\infty} e^{x} e^{-\frac{|x|}{b}} dx.$$

The integral above is finite if and only if $b < 1$. The result follows immediately.

Remark: The previous result shows that even for queries satisfying (3.13), the multiplicative mechanism will have an infinite bias if $K > \varepsilon$. An identical calculation shows that $\hat{X}_{Q,d}$ will have finite variance if and only if $K < \frac{\varepsilon}{2}$. From a practical viewpoint, these simple observations mean that for a given query satisfying (3.13), it is only possible to design ε-differentially private mechanisms with finite mean and variance for values of $\varepsilon > 2K$. This is in marked contrast to mechanisms obtained by post-processing and restriction.

3.5 Optimising bias over translated ramp functions

Consider again a Laplace random variable L with mean 0 and scale parameter $b > 0$. Let $Y_q = q + L$ for $q \geq 0$. For $\alpha \geq 0$, consider the translated ramp

function $\tau_\alpha(x) = \tau(x - \alpha)$. For $q \geq 0$, the expected value of the post-processed random variable $\tau_\alpha(Y_q)$ is given by

$$\mathsf{E}[\tau_\alpha(Y_q)] = \frac{1}{2b}\int_\alpha^\infty (x - \alpha)e^{-\frac{|x-q|}{b}}dx.$$

For a fixed $q \geq 0$, set $G(\alpha) = \mathsf{E}[\tau_\alpha(Y_q)]$. From Proposition 3.4.1, we know that for $\alpha = 0$, corresponding to the standard ramp function, the expectation of $\tau(Y_q)$ is $G(0) = q + \frac{b}{2}\exp\left(\frac{-q}{b}\right)$. This also means that the maximal absolute bias of the family $\{\tau(Y_q) : q \geq 0\}$ is $\frac{b}{2}$. It is readily verified that the derivative of G with respect to α is given by $G'(\alpha) = -\frac{1}{2b}\int_\alpha^\infty e^{-\frac{|x-q|}{b}}dx < 0$. Thus for any fixed q, $G(\alpha)$ is a decreasing function of α. Moreover, for every q, the bias of $\tau(Y_q)$ is strictly positive, meaning that $G(0) > 0$. These observations suggest that it may be possible to reduce the bias of $\tau(Y_q)$ by instead considering $\tau_\alpha(Y_q)$ for $\alpha > 0$.

For $\alpha \geq 0$, let $B(\alpha)$ denote the maximal absolute bias (3.2) of the family $\{\tau_\alpha(Y_q) : q \geq 0\}$. In the following result, we determine the minimum value of $B(\alpha)$ over $\alpha \geq 0$.

Theorem 3.5.1. *Let L be a Laplace random variable with mean 0 and scale parameter $b > 0$ and, for $q \geq 0$, let $Y_q = q + \mathsf{L}$. Let α be the unique solution of $\frac{b}{2}e^{-\frac{\alpha}{b}} - \alpha = 0$ in $[0, \infty)$. Then $\min\{B(\alpha) : \alpha \geq 0\} = \alpha$.*

Proof: Fix some $\alpha \geq 0$. It can be readily verified by direct calculation that the expectation of $\tau_\alpha(Y_q)$ is given by

$$\mathsf{E}[\tau_\alpha(Y_q)] = (q - \alpha) + \frac{b}{2}e^{\frac{\alpha-q}{b}}$$

for $q \geq \alpha$ and

$$\mathsf{E}[\tau_\alpha(Y_q)] = \frac{b}{2}e^{\frac{q-\alpha}{b}}$$

for $0 \leq q \leq \alpha$. It follows that the bias $\beta_\alpha(q) = \mathsf{E}[\tau_\alpha(Y_q)] - q$ is given by:

- $\beta_\alpha(q) = -\alpha + \frac{b}{2}e^{\frac{\alpha-q}{b}}$ for $q \geq \alpha$;
- $\beta_\alpha(q) = \frac{b}{2}e^{\frac{q-\alpha}{b}} - q$ for $0 \leq q \leq \alpha$.

It is clear that $\beta_\alpha(q)$ is a monotonically decreasing function of q for $q \geq \alpha$. Moreover, a simple calculation shows that for $0 \leq q \leq \alpha$, $\beta_\alpha(q) = \frac{1}{2}e^{\frac{q-\alpha}{b}} - 1$

which is negative for $0 \leq q \leq \alpha$. Thus $\beta_\alpha(q)$ is decreasing for all $\alpha \geq 0$ and moreover it is continuous. This implies that the maximum absolute bias of $\{\tau_\alpha(Y_q) : q \geq 0\}$ is either given by $|\beta_\alpha(0)| = \frac{b}{2}e^{-\frac{\alpha}{b}}$ or the limit $\lim_{q\to\infty} |\beta_\alpha(q)| = \alpha$. Formally,

$$B(\alpha) = \max\{\frac{b}{2}e^{-\frac{\alpha}{b}}, \alpha\}.$$

To complete the proof, let α^* be the unique solution of $\frac{b}{2}e^{-\frac{\alpha}{b}} - \alpha = 0$ in $[0, \infty)$. Then:

(i) $B(\alpha) = \frac{b}{2}e^{-\frac{\alpha}{b}}$ on $[0, \alpha^*]$;

(ii) $B(\alpha) = \alpha$ on $[\alpha^*, \infty)$.

Clearly $B(\alpha)$ is decreasing on $[0, \alpha^*]$ and increasing on $[\alpha^*, \infty)$. Hence the minimum value of $B(\alpha)$ on $[0, \infty)$ is given by $B(\alpha^*) = \alpha^*$ as claimed. □

Remark: As $\alpha^* > 0$, the maximal absolute bias of $\{\tau_{\alpha^*}(Y_q) : q \geq 0\}$, given by $\frac{b}{2}e^{-\frac{\alpha^*}{b}}$ is clearly less than $\frac{b}{2}$ corresponding to the standard ramp function.

3.6 Bias is inevitable for post-processing and restriction

Proposition 3.4.1 shows that if the base mechanism $X_{Q,d}$ is a Laplace mechanism, the nonnegative, post-processed mechanism corresponding to the ramp function τ has a strictly positive bias. Corollary 3.4.3 establishes the corresponding fact for a restricted Laplace mechanism. In this context, it is entirely natural to consider the following questions. Is it possible to construct an unbiased mechanism by post-processing a Laplace mechanism with some function other than τ? Does there exist an unbiased base mechanism given by a family of random variables $\{Y_q : q \geq 0\}$, such that the corresponding restricted mechanism $\hat{Y}_q$ is also unbiased? In this section, we shall show that the answer to both of these questions is negative under reasonable assumptions on both the post-processing function and the base mechanism for restriction.

3.6.1 Bias and post-processed Laplace mechanisms

We first consider the maximal absolute bias for post-processed Laplace mechanisms. Let the family $\{Y_q : q \geq 0\}$ consist of Laplace random variables with

scale parameter $b > 0$; each Y_q has the pdf

$$f_q(x) = \frac{1}{2b} e^{-\frac{|x-q|}{b}}.$$

Let $\phi : \mathsf{R} \to \mathsf{R}_+$ be a measurable function and define the derived family $\hat{Y}_{\phi,q}$ by $\hat{Y}_{\phi,q} = \phi(Y_q)$ for $q \geq 0$.

In order to ensure that each of the the derived random variables, $\hat{Y}_{\phi,q}$ $q \geq 0$, has finite first and second moments, we consider post-processing functions in the Hilbert space $V = L^2(e^{-\frac{|x|}{b}} dx)$:

$$V := \{\phi : \mathsf{R} \to \mathsf{R} : \int_{-\infty}^{\infty} |\phi(x)|^2 e^{-\frac{|x|}{b}} dx < \infty\}.$$

The cone of nonnegative valued functions ϕ in V is denoted by V_+.

It is straightforward to show that ϕ in V implies that $\int_{-\infty}^{\infty} |\phi(x)| e^{-\frac{|x|}{b}} dx < \infty$ also. In the following lemma we note that given $\phi \quad V_+$, the first and second moments of $\hat{Y}_{\phi,q}$ are finite for all $q \geq 0$.

Lemma 3.6.1. *Let $\phi \quad V_+$ be given. Then for any $q \geq 0$:*

$$\int_{-\infty}^{\infty} |\phi(x)| e^{-\frac{|x-q|}{b}} dx \quad < \quad \infty,$$
$$\int_{-\infty}^{\infty} |\phi(x)|^2 e^{-\frac{|x-q|}{b}} dx \quad < \quad \infty.$$

Proof: As $\phi \quad V$, we know that

$$\int_{-\infty}^{\infty} |\phi(x)|^p e^{-\frac{|x|}{b}} dx < \infty \tag{3.14}$$

for $p = 1, 2$. The result now follows from a simple application of the triangle inequality as

$$e^{-\frac{|x-q|}{b}} \leq e^{\frac{|q|}{b}} e^{-\frac{|x|}{b}}.$$

We now consider the mapping from V into R which takes a function ϕ to the maximal absolute bias given by (3.2). Formally, for $\phi \quad V$:

$$B(\phi) = \sup \left\{ \left| \int_{-\infty}^{\infty} \phi(x) f_q(x) dx - q \right| : q \quad \mathsf{R}_+ \right\}. \tag{3.15}$$

The following result establishes that $B(\phi) > 0$ for any $\phi \quad V_+$.

Proposition 3.6.2. *Let $\{Y_q = q + \mathsf{L} : q \geq 0\}$ be a family of Laplace random variables where L is Laplace with mean 0 and scale parameter $b > 0$. Let $\phi \quad V_+$ be given. Then $B(\phi) > 0$.*

Proof: Consider $q = 0$. Then as $\phi \quad V_+$ and $f_0(x) > 0$ for all x, it follows that

$$\int_{-\infty}^{\infty} \phi(x) f_0(x) dx > 0$$

unless $\phi = 0$ almost everywhere. If ϕ is not zero a.e., it follows immediately that

$$B(\phi) \geq \int_{-\infty}^{\infty} \phi(x) f_0(x) dx > 0.$$

On the other hand, if $\phi = 0$ a.e. then

$$\left| \int_{-\infty}^{\infty} \phi(x) f_q(x) dx - q \right| = q$$

for all $q \geq 0$ which means that $B(\phi) = \infty$ in this case. This completes the proof. □

Remark: Speaking informally, the previous result shows that bias is inevitable for any post-processed Laplace mechanism with finite first and second moments.

3.6.2 Bias and restricted mechanisms

We now consider the maximal absolute bias of general restricted mechanisms; we do not assume that the base mechanism is a Laplace mechanism here. Let a family of continuous real-valued random variables $\{Y_q : q \geq 0\}$ with associated pdfs f_q, $q \geq 0$ be given. We make the following assumptions for all $q \geq 0$:

$$\mathsf{E}[Y_q] = q \tag{3.16}$$

$$f_q(x) > 0 \quad x \quad \mathsf{R}. \tag{3.17}$$

Thus, we are assuming that the base mechanism is unbiased and has range given by R.

Let $\hat{Y}_q$ denote the restricted family of nonnegative random variables satisfying:

$$\mathsf{P}(\hat{Y}_q \quad A) = \frac{\mathsf{P}(Y_q \quad A)}{\mathsf{P}(Y_q \quad [0, \infty))} \tag{3.18}$$

for all measurable sets $A \quad \mathsf{R}_+$.

We will show that for $\hat{Y}_q$, the maximal bias given by (3.2) also satisfies $B > 0$. The proof of this makes use of the standard coupling technique from probability theory (see Section 4.12 of [49]) to construct a common space Ω_1 on which $\hat{Y}_q$ and a copy of Y_q can be defined for all $q \geq 0$.

Proposition 3.6.3. *Let a family of random variables $\{Y_q : q \geq 0\}$ satisfying (3.16), (3.17) and a restricted family $\hat{Y}_q$ satisfying (3.18) be given. Then the maximal absolute bias B given by (3.2) satisfies $B > 0$.*

Proof: For $q \geq 0$, let F_q denote the cumulative distribution function of Y_q and F_q^R the cdf of $\hat{Y}_q$. As $\hat{Y}_q$ takes values in $[0, \infty)$, $F_q^R(t) = 0$ for $t < 0$. Moreover, for $t \geq 0$:

$$\begin{aligned} F_q^R(t) &= \mathsf{P}(\hat{Y}_q \leq t) \\ &= \frac{\mathsf{P}(Y_q \quad [0,t])}{\mathsf{P}(Y_q \quad [0,\infty))} \\ &= \frac{F_q(t) - F_q(0)}{1 - F_q(0)}. \end{aligned}$$

We now show that $F_q^R(t) < F_q(t)$ for all $t \quad \mathsf{R}$. This is trivially true for $t < 0$. For $t \geq 0$,

$$\begin{aligned} F_q^R(t) &= \frac{F_q(t) - F_q(0)}{1 - F_q(0)} \\ &= \frac{F_q(t)(1 - F_q(0)) + F_q(0)(F_q(t) - 1)}{1 - F_q(0)} \\ &= F_q(t) + F_q(0)\frac{(F_q(t) - 1)}{1 - F_q(0)}. \end{aligned}$$

As $f_q(x) > 0$ for all x in R, it follows that $F_q(t) < 1$ for all $t \quad \mathsf{R}$ and $F_q(0) < 1$. This immediately implies that $F_q^R(t) < F_q(t)$ for $t \geq 0$ also. Therefore, the restricted mechanism $\hat{Y}_q$ stochastically dominates Y_q [49] for all $q \geq 0$. This means that we can construct a probability space $(\Omega_1, \mathsf{F}_1, \mathsf{P}_1)$ and random variables $\hat{Y}_q^1$, Y_q^1 for $q \geq 0$ such that

1. $\hat{Y}_q^1$ has the same distribution (cdf) as $\hat{Y}_q$ and Y_q^1 has the same distribution as Y_q for all $q \geq 0$;
2. $\hat{Y}_q^1(\omega) \geq Y_q^1(\omega)$ for all $q \geq 0$ and all $\omega \quad \Omega_1$.

The construction we employ here is standard; however we shall strengthen statement 2 slightly in order to prove that $\hat{Y}_q^1$ has strictly positive bias. We set $\Omega_1 = [0,1]$, F_1 to be the Borel subsets of $[0,1]$, and define P_1 to be the

Lebesgue measure on $[0,1]$. For $q \geq 0$, we define random variables $\hat{Y}_q^1$, Y_q^1 on Ω_1 by setting:

$$\begin{aligned} \hat{Y}_q^1(\omega) &= \inf\{t : F_q^R(t) > \omega\} \\ Y_q^1(\omega) &= \inf\{t : F_q(t) > \omega\}. \end{aligned}$$

As each of the cdfs, F_q^R, F_q for $q \geq 0$ is continuous and non-decreasing, it is not difficult to see that for $t \in \mathbb{R}$, $\hat{Y}_q^1(\omega) \leq t \Leftrightarrow \omega \leq F_q^R(t)$, and $Y_q^1(\omega) \leq t \Leftrightarrow \omega \leq F_q(t)$. These two facts imply that

$$\mathbb{P}(\hat{Y}_q^1 \leq t) = F_q^R(t); \mathbb{P}(Y_q^1 \leq t) = F_q(t).$$

It follows immediately that as $\hat{Y}_q^1$ has the same distribution as $\hat{Y}_q$, $\mathbb{E}[\hat{Y}_q^1] = \mathbb{E}[\hat{Y}_q]$. Similarly, $\mathbb{E}[Y_q^1] = \mathbb{E}[Y_q] = q$. Furthermore, as $F_q^R(t) < F_q(t)$ for all $t \in \mathbb{R}$, $\hat{Y}_q^1(\omega) \geq Y_q^1(\omega)$ for all $\omega \in [0,1]$. We next show that for every $q \geq 0$, there exists some subset S_q of $(0,1)$ of positive measure with the property that

$$\hat{Y}_q^1(\omega) > Y_q^1(\omega) \quad \omega \in S_q.$$

As $F_q(t) = \int_{-\infty}^t f_q(x)dx$ with $f_q(x) > 0$ for $x \in (-\infty, \infty)$ by assumption, it follows that we can choose $K > 0$ and $\alpha > 0$ such that $F_q(-K) = \alpha$. This immediately implies that $Y_q^1(\omega) \leq -K$ for $\omega \in (0, \alpha)$. Moreover, by construction $\hat{Y}_q^1(\omega) \geq 0$ for all $\omega \in (0,1)$ and hence taking $S_q = (0, \alpha)$, we have that

$$\hat{Y}_q^1(\omega) - Y_q^1(\omega) \geq K, \quad \omega \in S_q.$$

It now follows immediately that:

$$\begin{aligned} \mathbb{E}[\hat{Y}_q] &= \mathbb{E}[\hat{Y}_q^1] \\ &= \int_{\Omega_1} \hat{Y}_q^1(\omega) d\mathbb{P}_1(\omega) \\ &= \int_{S_q} \hat{Y}_q^1(\omega) d\mathbb{P}_1(\omega) + \int_{S_q^c} \hat{Y}_q^1(\omega) d\mathbb{P}_1(\omega) \\ &> \int_{S_q} Y_q^1(\omega) d\mathbb{P}_1(\omega) + \int_{S_q^c} Y_q^1(\omega) d\mathbb{P}_1(\omega) \\ &= \mathbb{E}[Y_q^1] = \mathbb{E}[Y_q]. \end{aligned}$$

Here $S_q^c = \Omega_1 \setminus S_q$. The argument above shows that, for any $q \geq 0$ $\mathbb{E}[\hat{Y}_q] > \mathbb{E}[Y_q] = q$ and hence the maximal absolute bias B satisfies:

$$B = \sup\{|\mathbb{E}\hat{Y}_q - q| : q \geq 0\} > 0.$$

This completes the proof. □

3.7 Mean square error (MSE) for nonnegative derived Laplace mechanisms

The privacy-accuracy trade-off is one of the most important questions in Differential Privacy. The results in previous sections address one aspect of this issue by considering the bias introduced by post-processing or restriction. We now consider a different accuracy measure: the *mean-square error* (MSE) of post-processed and restricted mechanisms.

The mean square error (MSE) of a random variable X as an estimator of q is

$$MSE(X) := \mathsf{E}[(X - q)^2].$$

A standard computation shows that

$$\begin{aligned} MSE(X) &= \mathsf{E}[X^2 - 2qX + q^2] \\ &= \mathsf{E}[X^2] - 2q\mathsf{E}[X] + q^2. \end{aligned} \tag{3.19}$$

3.7.1 MSE for post-processed and restricted Laplace mechanisms

$\{Y_q : q \geq 0\}$ is a family of Laplace random variables, $Y_q = q + \mathsf{L}$, where L has mean 0 and scale parameter $b = \frac{\Delta}{\varepsilon}$. $\hat{Y}_{\tau,q}$ denotes the post-processed family of random variables constructed with the function τ given by (3.6); we will use $\hat{Y}_q$ to denote the family of restricted random variables.

As we have already calculated both $\mathsf{E}[\hat{Y}_{\tau,q}]$ and $\mathsf{E}[\hat{Y}_q]$, it follows from (3.19) that to compute the corresponding MSEs it is enough to calculate $\mathsf{E}[(\hat{Y}_{\tau,q})^2]$ and $\mathsf{E}[(\hat{Y}_q)^2]$

We will use the following integrals which can be readily calculated:

$$\begin{aligned} \int_0^q x^2 e^{\frac{x}{b}} dx &= bq^2 e^{\frac{q}{b}} - 2b^2 q e^{\frac{q}{b}} + 2b^3(e^{\frac{q}{b}} - 1) \\ \int_q^\infty x^2 e^{-\frac{x}{b}} dx &= bq^2 e^{-\frac{q}{b}} + 2b^2 q e^{-\frac{q}{b}} + 2b^3 e^{-\frac{q}{b}}, \end{aligned} \tag{3.20}$$

where $b > 0$, $q \geq 0$.

Post-processed mechanism

We first consider the post-processed mechanism $\hat{Y}_{\tau,q} = \tau(Y_q)$ constructed using the standard ramp function τ. It can be checked by direct computation that for $x = 0$, the pdf of $\hat{Y}_{\tau,q}$ is given by

$$f_{\tau,q}(x) = \begin{cases} 0 & x < 0 \\ \frac{1}{2b} e^{\frac{x-q}{b}} & 0 < x < q \\ \frac{1}{2b} e^{\frac{-x+q}{b}} & x \geq q. \end{cases} \tag{3.21}$$

Using this, we can now calculate the MSE of the post-processed mechanism.

Proposition 3.7.1. *For $q \geq 0$, the mean square error of $\hat{Y}_{\tau,q} = \tau(Y_q)$ is given by:*

$$MSE(\hat{Y}_{\tau,q}) = b^2(2 - e^{-\frac{q}{b}}) - bqe^{-\frac{q}{b}}. \tag{3.22}$$

Proof: Using (3.21),

$$\mathsf{E}[(\hat{Y}_{\tau,q})^2] = \frac{e^{-\frac{q}{b}}}{2b} \int_0^q x^2 e^{\frac{x}{b}} dx + \frac{e^{\frac{q}{b}}}{2b} \int_q^\infty x^2 e^{-\frac{x}{b}} dx. \tag{3.23}$$

It is now straightforward to verify using the formulae in (3.20) that

$$\mathsf{E}[(\hat{Y}_{\tau,q})^2] = q^2 + b^2(2 - e^{-\frac{q}{b}}).$$

Combining this with the formula

$$\mathsf{E}[\hat{Y}_{\tau,q}] = q + \frac{b}{2} e^{-\frac{q}{b}},$$

the result follows immediately from (3.19). □

Restricted mechanisms

Now consider the restricted family, $\hat{Y}_q$ for $q \geq 0$, whose cumulative distribution function is given by

$$F_q^R(t) = \begin{cases} 0 & x \leq 0 \\ 1 - \frac{e^{\frac{-x+q}{b}}}{2 - e^{\frac{-q}{b}}} & x > q \\ \frac{e^{\frac{x-q}{b}} - e^{\frac{-q}{b}}}{2 - e^{\frac{-q}{b}}} & 0 \leq x \leq q \end{cases}.$$

Differentiating, we see that the pdf of $\hat{Y}_q$ is:

$$f_q^R(x) = \begin{cases} 0 & x \leq 0 \\ \frac{e^{\frac{-x+q}{b}}}{b(2-e^{\frac{-q}{b}})} & x > q \\ \frac{e^{\frac{x-q}{b}}}{b(2-e^{\frac{-q}{b}})} & 0 \leq x \leq q \end{cases}.$$

Proposition 3.7.2. *For $q \geq 0$, the mean square error of the restricted family $\hat{Y}_q$, is given by:*

$$MSE(\hat{Y}_q) = \frac{1}{2 - e^{-\frac{q}{b}}} \left(4b^2 - e^{-\frac{q}{b}}(2b^2 + 2bq + q^2)\right). \tag{3.24}$$

Proof: The calculation is essentially the same as that used in Proposition 3.7.1. First, use the formulae for the pdf $f_q^R(x)$ of Z_q^R to see that

$$\mathsf{E}[(\hat{Y}_q)^2] = \frac{e^{-\frac{q}{b}}}{b(2 - e^{-\frac{q}{b}})} \int_0^q x^2 e^{\frac{x}{b}} dx + \frac{e^{\frac{q}{b}}}{b(2 - e^{-\frac{q}{b}} \int_q^\infty x^2 e^{-\frac{x}{b}} dx.$$

It follows from (3.20) that

$$\mathsf{E}[(\hat{Y}_q)^2] = \frac{2}{2 - e^{-\frac{q}{b}}} \left(q^2 + b^2(2 - e^{-\frac{q}{b}})\right).$$

The result now follows from noting that

$$\mathsf{E}[\hat{Y}_q] = \frac{1}{2 - e^{-\frac{q}{b}}} \left(2q + be^{-\frac{q}{b}}\right).$$

□

Comparison of MSE for restricted and post-processed mechanisms

We saw in Section 3.4 that the bias of the restricted mechanism is always strictly greater than that of a post-processed mechanism with the same differential privacy parameter ε. To finish this section, we carry out the corresponding comparison for the MSE. To ensure ε differential privacy for both the post-processed mechanism and the restricted Laplace mechanism, if we use the scale parameter b for the post-processed mechanism, we should use $2b$ for the restricted Laplace mechanism.

Consider the ratio between

$$M_1 = b^2(2 - e^{-\frac{q}{b}}) - bqe^{-\frac{q}{b}}$$

(corresponding to $\hat{Y}_{\tau,q}$) and

$$M_2 = \frac{1}{2 - e^{-\frac{q}{2b}}} \left(16b^2 - e^{-\frac{q}{2b}}(8b^2 + 4bq + q^2)\right)$$

(corresponding to $\hat{Y}_q$). Note that

$$M_1 \leq b^2(2 - e^{-\frac{q}{b}}) \;=\; \frac{1}{M_1} \geq \frac{1}{b^2(2 - e^{-\frac{q}{b}})}$$

as $bqe^{-\frac{q}{b}} \leq 0$ for all $q \geq 0$.

Also note that

$$M_2 \geq \frac{1}{2 - e^{-\frac{q}{2b}}}(8b^2)$$

as $e^{-\frac{q}{2b}}(8b^2 + 4bq + q^2)$ is a decreasing function for all $q \geq 0$, and hence its maximum value occurs at $q = 0$. Therefore, it can be shown that

$$\frac{M_2}{M_1} \geq 8\left(\frac{1}{2 - e^{-\frac{q}{b}}}\right)\left(\frac{1}{2 - e^{-\frac{q}{2b}}}\right) \geq 2$$

as $\frac{1}{2-e^{-\frac{q}{2b}}} \geq \frac{1}{2}$ and $\frac{1}{2-e^{-\frac{q}{b}}} \geq \frac{1}{2}$ for all $q \geq 0$. This calculation shows that the MSE for post-processing is always strictly less than the MSE of the restricted Laplace mechanism.

3.8 Optimising the Mean Square Error

In this section, we consider the MSE of a post-processed Laplace mechanism. In particular, we introduce the *worst case MSE* as a function of the post-processing function ϕ, and analyse the problem of minimising this function over all nonnegative ϕ for which the associated mechanism has finite first and second moments. The main contribution of this section is to prove the existence of a minimising function ϕ for this problem. While we do not give a constructive result here, proving the existence of a minimising function is an important step in solving the optimisation problem.

For ϕ V_+, the MSE of the post-processed mechanism $\hat{Y}_{\phi,q} = \phi(Y_q)$ is given by:

$$\begin{aligned} MSE(\hat{Y}_{\phi,q}) &= \mathsf{E}[(\hat{Y}_{\phi,q} - q)^2] \\ &= \mathsf{E}[(\hat{Y}_{\phi,q} - \mathsf{E}[\hat{Y}_{\phi,q}] + \mathsf{E}[\hat{Y}_{\phi,q}] - q)^2] \\ &= V[\hat{Y}_{\phi,q}] + (\mathsf{E}[\hat{Y}_{\phi,q}] - q)^2, \end{aligned} \tag{3.25}$$

where $V[\hat{Y}_{\phi,q}]$ is the variance of $\hat{Y}_{\phi,q}$. We note the following simple observations.

- Lemma 3.6.1 implies that if $\phi \quad V$, then $\hat{Y}_{\phi,q} = \phi(Y_q)$ will have finite first and second moments for all $q \geq 0$. In particular, it follows from (3.25) that $MSE(\hat{Y}_{\phi,q}))$ will be finite for all $q \geq 0$.

- Proposition 3.6.2 implies that

$$\sup\{MSE(\hat{Y}_{\phi,q}) : q \geq 0\} > 0$$

  for any choice of the function ϕ. In this section, we are interested in the question of minimising this *worst case MSE* over $\phi \quad V_+$.

V is a real Hilbert space with inner product

$$\phi, \psi \ = \int_{-\infty}^{\infty} \phi(x)\psi(x)e^{-\frac{|x|}{b}}dx$$

and the associated norm

$$\psi \ = \left(\int_{-\infty}^{\infty} |\psi(x)|^2 e^{-\frac{|x|}{b}}dx\right)^{1/2}.$$

In particular, V is a reflexive Banach space.

We now define the *worst case MSE* function.

Definition 3.8.1. The worst case MSE is the function $F : V \to \mathbb{R}_+ \quad \{\infty\}$ given by

$$F(\phi) := \sup\{MSE(\phi(Y_q)) : q \geq 0\}. \tag{3.26}$$

For the remainder of this section, we will consider the problem of minimising the worse case MSE of a post-processed mechanism. Formally, we consider the following question.

Problem 3.8.1. *Minimise $F(\phi)$ subject to $\phi \quad V_+$.*

We will prove the existence of a minimising function $\hat{\phi}$ in V_+ such that

$$F(\hat{\phi}) = \inf\{F(\phi) : \phi \quad V_+\}.$$

As with all optimisation problems, proving the existence of a global minimiser is a crucial first step in the development of algorithms for determining a minimising function ϕ.

We first recall some standard definitions and technical facts from the theory of nonlinear optimisation; for background and additional details on these topics, the reader may consult [93].

Definition 3.8.2. A function $f : E \to \mathsf{R}$ on a Banach space E is *coercive* if $\lim_{n\to\infty} x_n = \infty$ implies $\limsup_{n\to\infty} f(x_n) = \infty$.

Definition 3.8.3. Let S be a non-empty subset of a Banach space E. The function $f : S \to \mathsf{R}$ is lower semicontinuous at $\bar{x} \in S$ if for all $\epsilon > 0$, there is some $\delta > 0$ such that $x \in S$, $\|x - \bar{x}\| < \delta$ implies $f(x) > f(\bar{x}) - \epsilon$.

In order to prove the existence of a minimising $\hat{\phi}$ in V_+ with $F(\hat{\phi}) \leq F(\phi)$ for all $\phi \in V_+$, we make use of the following rephrased version of Theorem 5.4.4 in [93].

Theorem 3.8.1. *Let E be a reflexive Banach space and let $S \subseteq E$ be a nonempty, convex, closed subset of E. If $f : S \to \mathsf{R}$ is a coercive, convex, lower-semicontinuous function on S then there exists some $\hat{x} \in S$ with $f(\hat{x}) \leq f(x)$ for all $x \in S$.*

We wish to apply this theorem to the function F given by (3.26) defined on the set V_+. First note that as V is a Hilbert space it is a reflexive Banach space [8].

For the remainder of this section, we use the notation $d\mu(x)$ ($d\mu_q(x)$) for the measure $e^{-\frac{|x|}{b}}dx$ ($e^{-\frac{|x-q|}{b}}dx$). We also use the more compact notation $\int_{\mathsf{R}} \phi d\mu$ for $\int_{-\infty}^{\infty} \phi(x)d\mu(x)$.

The first step in our proof is to prove that the cone V_+ is convex and closed. We include the proof here in the interests of completeness.

Lemma 3.8.2. *The set V_+ is convex and closed.*

Proof: For convexity, simply note that if $\phi_1(x) \geq 0$ and $\phi_2(x) \geq 0$ for almost all x and $0 < \alpha < 1$, then the set of x where $\alpha\phi_1(x) + (1 - \alpha)\phi_2(x) < 0$ is contained in the union

$$\{x : \phi_1(x) < 0\} \cup \{x : \phi_2(x) < 0\}$$

which has measure 0. This implies that $\alpha\phi_1(x)+(1-\alpha)\phi_2(x) \geq 0$ for almost all x. To see that V_+ is closed, we suppose that the sequence ϕ_n in V_+ converges to some ϕ in V. This means that $\int_{\mathsf{R}}(\phi_n - \phi)^2 d\mu$ tends to 0 as $n \to \infty$. If $\phi(x) < 0$ on a set of non-zero measure then for some n, the set $S_n = \{x :$

$\phi(x) < -\frac{1}{n}\}$ has non-zero measure. It is then simple to see that for all n, $\int_{\mathsf{R}}(\phi_n - \phi)^2 d\mu \geq \frac{1}{n^2}\mu(S_n) > 0$ which contradicts $\phi_n \to \phi$ as $n \to \infty$. $\square$

Our next lemma shows that F given by (3.26) is both convex and coercive.

Lemma 3.8.3. *The function $F : V \to \mathsf{R}$ defined by (3.26) is convex and coercive.*

Proof: It follows from standard results in convex analysis [93] that for a set $\{f_q : q \quad \mathsf{R}_+\}$ of convex functions, $f_q : V \to \mathsf{R}$, the function f given by $f(x) = \sup\{f_q(x) : q \quad \mathsf{R}_+\}$ is also convex. We shall show that for each $q \geq 0$, the function $\phi \to MSE(\phi(Y_q))$ is convex. The convexity of F will then follow.

Direct calculation shows that

$$MSE(\phi(Y_q)) = \mathsf{E}[\phi(Y_q)^2] - 2q\mathsf{E}[\phi(Y_q)] + q^2.$$

Clearly the function $\phi \to -2q\mathsf{E}[\phi(Y_q)] + q^2$ is affine and hence convex. Thus it is enough for us to verify that $H(\phi) = \mathsf{E}[\phi(Y_q)^2]$ is convex.

So let ϕ_1, ϕ_2 in V, $q \geq 0$, and $0 < \alpha < 1$ be given. Then, keeping in mind that $\alpha^2 < \alpha$ as $0 < \alpha < 1$,

$$\begin{aligned}
H(\alpha\phi_1 + (1-\alpha)\phi_2) &= \int_{\mathsf{R}} (\alpha\phi_1 + (1-\alpha)\phi_2)^2 d\mu_q \\
&= \int_{\mathsf{R}} (\phi_2 + \alpha(\phi_1 - \phi_2))^2 d\mu_q \\
&= \int_{\mathsf{R}} \phi_2^2 + \alpha^2(\phi_1 - \phi_2)^2 + 2\alpha\phi_2(\phi_1 - \phi_2) d\mu_q \\
&\leq \int_{\mathsf{R}} \phi_2^2 + \alpha(\phi_1 - \phi_2)^2 + 2\alpha\phi_2(\phi_1 - \phi_2) d\mu_q \\
&= \int_{\mathsf{R}} \alpha\phi_1^2 + (1-\alpha)\phi_2^2 d\mu_q \\
&= \alpha\mathsf{E}[\phi_1(Y_q)^2] + (1-\alpha)\mathsf{E}[\phi_2(Y_q)^2].
\end{aligned}$$

Thus H is indeed convex and hence so is MSE and the function F.

To show that F is coercive, suppose we have a sequence ϕ_n in V with $\lim_{n\to\infty} \quad \phi_n \quad = \infty$. Then, taking $q = 0$,

$$\begin{aligned}
MSE(\phi_n(Y_0)) &= \int_{-\infty}^{\infty} |\phi_n(x)|^2 d\mu(x) \\
&= \quad \phi_n(x) \quad ^2 \to \infty
\end{aligned}$$

as $n \to \infty$. This immediately implies that $F(\phi_n) \geq MSE(\phi_n(Y_0)) \to \infty$ as $n \to \infty$ and hence F is coercive as claimed. $\square$

The final fact that we need to establish is the lower-semicontinuity of F.

Lemma 3.8.4. *The function $F : V \to \mathbb{R}$ given by (3.26) is lower semicontinuous on V_+.*

Proof: First note that for each $q \geq 0$, $MSE(\phi(Y_q)) = \|\phi - q\|_q^2$ where $\|\cdot\|_q$ denotes the norm in the Hilbert space $L^2(d\mu_q)$. Moreover, it is an exercise in the triangle inequality to show that for any such q, $\|\phi\|_q^2 \leq e^{\frac{q}{b}} \|\phi\|^2$ where $\|\cdot\|$ denotes the norm in V. It follows that if a sequence ϕ_n converges to ϕ in V, then it also converges to ϕ in $L^2(d\mu_q)$. The continuity of the norm on a Hilbert space [8] immediately implies that $MSE(\phi_n(Y_q))$ converges to $MSE(\phi(Y_q))$. This shows that $\phi \to MSE(\phi(Y_q))$ is continuous on V for each $q \geq 0$.

To show that F is lower semicontinuous on V_+, let $\bar{\phi}$ in V_+ and $\epsilon > 0$ be given. We need to show that there is some $\delta > 0$ such that $F(\phi) > F(\bar{\phi})$ for $\phi \quad V_+$ with $\|\phi - \bar{\phi}\| < \delta$. As $F(\bar{\phi}) = \sup\{MSE(\bar{\phi}(Y_q)) : q \geq 0\}$ there is some $q_0 \geq 0$ with

$$MSE(\bar{\phi}(Y_{q_0})) > F(\bar{\phi}) - \frac{\epsilon}{2}.$$

Moreover as $\phi \to MSE(\phi(Y_{q_0}))$ is continuous on V, we can conclude that there is some $\delta > 0$ such that if $\|\phi - \bar{\phi}\| < \delta$, then

$$\left|MSE(\phi(Y_{q_0})) - MSE(\bar{\phi}(Y_{q_0}))\right| < \frac{\epsilon}{2}.$$

Combining the two previous inequalities shows that if $\|\phi - \bar{\phi}\| < \delta$ then $MSE(\phi(Y_{q_0})) > F(\bar{\phi}) - \epsilon$. This immediately implies that

$$F(\phi) \geq MSE(\phi(Y_{q_0})) > F(\bar{\phi}) - \epsilon,$$

which shows that F is lower semicontinuous as claimed. $\square$

Combining the previous lemmas with Theorem 3.8.1 proves the following result.

Theorem 3.8.5. *There exists $\hat{\phi} \quad V_+$ such that $F(\hat{\phi}) \leq F(\phi)$ for all $\phi \quad V_+$.*

Proof: By Lemma 3.8.2, V_+ is convex and closed; it is clearly nonempty. Combining Lemma 3.8.4 and Lemma 3.8.3, we know that F is convex, coer-

cive and lower semicontinuous on V_+. The result now follows direrctly from Theorem 3.8.1. □

Remark: Given a Laplace mechanism defined by a family of random variables $\{Y_q = q + L : q \geq\}$, Theorem 3.8.5 guarantees the existence of a function $\phi : \mathsf{R} \to \mathsf{R}_+$ such that:

(i) the first and second moments of all of the nonnegative random variables $\phi(Y_q)$ are finite;

(ii) the worst case mean square error of the mechanism $\phi(Y_q)$ is minimal among all functions satisfying (i).

This result naturally suggests the problem of determining the actual minimal value of the function F on V_+ and to develop algorithms to determine or approximate a function ϕ attaining this minimum. As a first step in this direction, it might be more tractable to restrict to a smaller class of functions such as those functions in V_+ that are piecewise linear or piecewise affine as these are generalisations of the function τ given by (3.6).

3.9 Conclusions

In this chapter, we considered two general approaches to constructing nonnegative differentially private mechanisms; post-processing and restriction. In Section 3.4, we gave explicit formulae for the bias of nonnegative Laplace mechanisms obtained by restriction and by post-processing with the simple ramp function. When we view boundary inflated truncation (to use the terminology of [75]) as post-processing with the ramp function, τ, we see that it is possible to use alternative post-processing functions in order to reduce bias. The results presented in Section 3.5 on translations of the ramp function show that this is indeed possible. In fact, we have given an explicit characterisation of the optimal post-processing function within this class. An interesting, and challenging, question for future research is to determine the minimal possible value of the maximal absolute bias of a nonnegative, post-processed Laplace mechanism where the mechanism is required to have finite first and second moments. In relation to this question, the work of Section 3.6 proves that the maximum absolute bias of any such mechanism must be strictly positive. In

Section 3.7, formulae for the mean square error of post-processed (using the simple truncation function) and restricted Laplace mechanisms are also derived and we have proven that there exists a square integrable post-processing function that minimises the worst case MSE, in Section 3.8.

In Chapter 4, we will briefly outline how the techniques in this chapter can be applied in a system theoretic setting to derive positive mechanisms for positive linear systems. In particular, this shows that they can be used to build mechanisms for positive observers. This is then the major topic of much of the rest of the thesis.

CHAPTER 4

Positive Linear Observers and l_1 Sensitivity

In this chapter, we show how to apply the results of the previous chapter to positive systems. Specifically, we show how to develop a positive ε di erential private observer using the Laplace mechanism. We first provide a general bound for the l_1 sensitivity of the map defined by a Luenberger observer for an LTI system. We then study the optimisation problem of minimising this bound for positive linear observers and provide a method for computing an optimal solution for systems with a single measured output.

4.1 Introduction

In Chapter 3, our main motivation was to derive mechanisms that ensure positivity when applying differential privacy to a nonnegative valued query. In this chapter, we are interested in applying these methods to positive dynamic systems. In this scenario the mapping from the input space to the output space of the positive dynamic system will take the role of the query. We show how the use the methods from Chapter 3 to ensure the outputs from a mechanism are nonnegative.

The main focus in this chapter is to achieve differential privacy using the Laplace distribution. As seen in Chapter 2, the l_1 sensitivity is a key parameter for Laplace mechanisms. Our main interest in this chapter and the following two chapters is positive linear observers, so in the latter part of this chapter,

we will concentrate on estimating the l_1 sensitivity of a positive linear observer. Here, the mapping from the measured output of the system to the observer will take the role of the query mapping.

As noted in Chapter 2, many motivating examples for privacy preserving control fall within the class of positive systems [103, 44, 19]. Previous work on privacy preserving control and observer design has not explicitly considered positive systems; however, positivity has a strong impact on system behaviour. In [52], a formal mathematical description of the positive observer design problem for linear systems, together with canonical forms appropriate to the positive setting was described. Further work on positive observer design, for more general classes of observer, can be found in [95]. Our objective here is to introduce the problem of differentially private positive observer design; starting from the work of [67] and concentrating on what can be said for the sensitivity of observers for positive linear systems. Before developing results for positive linear observers, we first show how to apply the work of the last chapter to positive dynamical systems.

4.2 Differential privacy and positive linear systems

In this section, we give a brief outline of how our results from Chapter 3 can be combined with recent work on differential privacy for control systems [72, 67] to design positive, differentially private mechanisms for positive linear systems. Our motivation comes from the positive linear observer problem [52, 10, 76] and the development of differentially private positive observers of Luenberger type.

Consider the positive linear system (with input)

$$\begin{aligned} \Sigma : x(t+1) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) \end{aligned} \tag{4.1}$$

where $A \quad \mathbb{R}_+^{n\times n}$, $C \quad \mathbb{R}_+^{p\times n}$, $B \quad \mathbb{R}_+^{n\times m}$. The system Σ defines a mapping between the input space $\mathcal{U}_+ := \left(\mathbb{R}_+^m\right)^{\mathbb{Z}_+}$ of sequences with entries in $\mathbb{R}_+^m$ and the output space $\mathcal{Y}_+ := (\mathbb{R}_+^p)^{\mathbb{Z}_+}$ of sequences with entries in $\mathbb{R}_+^p$. We shall use $\mathcal{Y}$ and $\mathcal{U}$ to denote the corresponding real-valued sequences (without the nonnegativity restriction).

As is standard in Probability Theory [18], we will work with the sigma algebra on these sequence spaces generated by finite dimensional projections; this is the sigma algebra generated by the algebra of cylinder sets of the form $\pi^{-1}(A)$ where $\pi : (\mathsf{R}^n)^{\mathsf{Z}_+} \to \mathsf{R}^k$ is a projection onto some finite set of k components and A is a Borel set in R^k. We denote these sigma-algebras by $\sigma(\mathsf{U}_+)$, $\sigma(\mathsf{Y}_+)$ respectively.

Given a system (4.1), a *mechanism* is a set of measurable mappings $Y^{(u)} : \Omega \to \mathsf{Y}_+$ indexed by $u \quad \mathsf{U}_+$. The system takes the role of a query and u corresponds to the database in our earlier discussion in Chapter 2 and 3.

We assume that U_+ is equipped with a reflexive, symmetric relation . The following definition of differential privacy for systems, taken from [72], is a direct extension of that for real-valued queries.

Let $\varepsilon > 0$ be given. The mechanism $Y^{(u)} : \Omega \to \mathsf{Y}_+$ is ε differentially private if

$$\mathsf{P}(Y^{(u)} \quad B) \leq e^{\varepsilon}\mathsf{P}(Y^{(u\,)} \quad B) \tag{4.2}$$

for all $B \quad \sigma(\mathsf{Y}_+)$ and all $u \quad u$ in U_+.

We will use the notation $Y^{(u)}_{t,i}$ to denote the ith component of the mechanism $Y^{(u)}$ at time $t \geq 0$, corresponding to the input u; this is then a real-valued random variable. Similarly, $y^{(u)}_{t,i}$ denotes the ith component of the output $y^{(u)}$ of the system at time t, corresponding to the input u.

Throughout this chapter, we will work exclusively with the l_1 norm and the corresponding induced norm for matrices, as these are the natural norms for use in connection with Laplace mechanisms for differential privacy [67, 38]. Recall from Chapter 2, the l_1 norm of $y = (y(t))$ in Y_+ is defined by

$$y \ _1 = \sum_{t=0}^{\infty} \ y(t) \ _1$$

where $y(t) \ _1$ is the usual l_1 norm on R^p and for $T \quad \mathsf{R}^{m\times n}$,

$$T \ _1 = \max_j \sum_{i=1}^{m} |t_{ij}|. \tag{4.3}$$

In Proposition 4.2.2, we present a technical result that will underpin some of our later arguments. In order to prove this result, we will make use of the

Monotone Class Theorem. We first recall a definition necessary to state this result.

Definition 4.2.1. A monotone class M is a collection of subsets of Ω with two properties:

(i) if A_i M for $i = 1, 2, \ldots,$ and for A_1 A_2 $\ldots,$ then $\bigcup_i A_i$ M

(ii) if B_i M for $i = 1, 2, \ldots,$ and for B_1 B_2 $\ldots,$ then $\bigcap_i B_i$ M

Theorem 4.2.1 (Monotone class theorem [73])**.** *Let Ω be a set and let A be an algebra of subsets of Ω such that Ω is in A and the empty set is also in A. Then there exists a smallest monotone class M that contains A. That class, M, is also the smallest sigma-algebra that contains A.*

With the Monotone class theorem we can now prove the following result.

Proposition 4.2.2. *Let $Y^{(u)} : \Omega \to Y_+$ be a mechanism and let $\varepsilon > 0$. Suppose that*

$$P(\pi(Y^{(u)}) \quad A) \leq e^{\varepsilon} P(\pi(Y^{(u\,)}) \quad A) \tag{4.4}$$

for all finite dimensional projections π, u u in U_+, and all Borel sets A in R_+^k where π maps into R_+^k. Then the mechanism $Y^{(u)}$ is ε differentially private.

Proof: By assumption, we know that (4.2) holds for all sets B in the algebra $A(Y_+)$ which generates $\sigma(Y_+)$. It can be easily verified that the collection of all sets B Y_+ satisfying (4.2) forms a monotone class M, [73]. As $A(Y_+)$ M, the Monotone Class Theorem 4.2.1 implies that $\sigma(Y_+)$ M; equivalently, (4.2) holds for all B in $\sigma(Y_+)$ as claimed. □

The result of Proposition 4.2.2 for real-valued signals was established, using different arguments, in Lemma 2 of [72]. The outline proof given above closely follows the argument used in Theorem 3 of [57] and is included here in the interest of completeness.

Recall from Chapter 2, that the l_1-sensitivity of the system Σ (4.1) with respect to the relation is defined by

$$\Delta_1(\Sigma) := \sup_{u \ u} \ y^{(u)} - y^{(u\,)} \ _1.$$

The following result from [72] and Theorem 2.4.1 in Chapter 2 applies to the design of the Laplace mechanism where the system Σ is not necessarily nonnegative.

Consider the system Σ and let $\varepsilon > 0$ be given. Let $L : \Omega \to \mathbb{R}$ be a Laplace random variable with mean value 0 and scale parameter $b = \frac{\Delta_1(\Sigma)}{\varepsilon}$. Then $Y^{(u)}$, defined by

$$Y^{(u)}_{t,i}(\omega) = y^{(u)}_{t,i} + L(\omega), \quad \omega \quad \Omega \tag{4.5}$$

is ε-differentially private.

The equation (4.5) describes how to construct a differentially private mechanism for a general linear system of the form (4.1) by adding the output of a Laplace random variable to each component of the output $y(t)$ of the system. If we use this result for a positive system, the mechanism can generate negative values. We shall now show how to use post-processing and restriction, as discussed in Chapter 3, to construct nonnegative mechanisms for a positive system (4.1).

Post-processing

We first outline how post-processing to achieve positivity can be extended to systems. This relies on the following more general form of Proposition 3.3.1, which can be proven in the same way.

Proposition 4.2.3. *Let $Y^{(u)} : \Omega \to E$ be an ε differentially private mechanism where E is a measurable space, and let $\phi : E \to G$ be a measurable map into another measurable space G. Then $\phi \circ Y^{(u)}$ is an ε differentially private mechanism.*

For a sequence y in $\mathbb{Y}$, we define $T : \mathbb{Y} \to \mathbb{Y}_+$ by applying τ given by (3.6) to each component of the sequence $y \quad \mathbb{Y}$. Formally:

$$[T(y)]_{t,i} = \tau(y_{t,i}) = \begin{cases} y_{t,i} & \text{if } y_{t,i} \geq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{4.6}$$

for $y \quad \mathbb{Y}$, $1 \leq i \leq p$, $t \geq 0$.

Our next result shows formally that if $Y^{(u)} : \Omega \to \mathbb{Y}$ is ε differentially private then $T(Y^{(u)})$ is a positive ε differentially private mechanism. Rather than

formally verifying the measurability of the infinite dimensional mapping T, we will work with the finite dimensional projections which are measurable. To simplify notation in the following proof, we let $x^+ = \tau(x)$.

Proposition 4.2.4. *Let $Y^{(u)} : \Omega \to \mathsf{Y}$ be an ε differentially private mechanism. Then $\hat{Y}^{(u)} : \Omega \to \mathsf{Y}_+$ defined by $\hat{Y}^{(u)} = T\left(Y^{(u)}\right)$, is ε differentially private.*

Proof: $Y^{(u)}$ is ε differentially private. Hence if k is any positive integer, π is a k-dimensional projection, and $u \quad u$,

$$\mathsf{P}\left(\pi(Y^{(u)}) \quad A\right) \leq e^{\varepsilon}\mathsf{P}\left(\pi(Y^{(u\,)}) \quad A\right)$$

for all Borel sets $A \quad \mathsf{R}^k$.

$T_k : \mathsf{R}^k \to \mathsf{R}_+^k$ is defined by $T_k(y_1, y_2, \ldots, y_k) = (y_1^+, y_2^+, \ldots, y_k^+)$ is measurable. Proposition 4.2.3 now implies that

$$\mathsf{P}\left(T_k(\pi(Y^{(u)})) \quad B\right) \leq e^{\varepsilon}\mathsf{P}\left(T_k(\pi(Y^{(u\,)})) \quad B\right) \tag{4.7}$$

for all $u \quad u$ and Borel sets $B \quad \mathsf{R}_+^k$.

Now we show that $\pi \circ T = T_k \circ \pi$. To see this note

$$\begin{aligned} \pi \circ T(y) &= \pi(y_1^+, y_2^+, y_3^+, \ldots) \\ &= (y_{t_1,i_1}^+, y_{t_2,i_2}^+, \ldots, y_{t_k,i_k}^+) \\ &= T_k(y_{t_1,i_1}, y_{t_2,i_2}, \ldots, y_{t_k,i_k}) \end{aligned}$$

Hence $\pi(\hat{Y}^{(u)}) = \pi(T(Y^{(u)})) = T_k(\pi(Y^{(u)}))$. It follows from (4.7) that

$$\mathsf{P}(\pi(\hat{Y}^{(u)}) \quad B) \leq e^{\varepsilon}\mathsf{P}(\pi(\hat{Y}^{(u\,)}) \quad B)$$

for all $u \quad u$ and Borel sets $B \quad \mathsf{R}_+^k$. Therefore by Proposition 4.2.2 the mechanism $\hat{Y}^{(u)}$ is ε differentially private. □

Restricted Mechanisms

To define a restricted Laplace mechanism $\hat{Y}^{(u)} : \Omega \to \mathsf{Y}_+$ we set $\hat{Y}_{t,i}^{(u)} = y_{t,i} + L_{y_{t,i}}$, where $L_{y_{t,i}}$ is the lower bounded Laplace random variable whose output is restricted to $[-y_{t,i}, \infty)$, with scale parameter $b = \frac{\Delta_1(\Sigma)}{\varepsilon}$. The next result is the key fact needed to establish conditions for $\hat{Y}^{(u)}$ to be differentially private. To simplify notation in the following result, let $\Delta_1(\Sigma) = \Delta$.

Proposition 4.2.5. *For a positive integer k let $\pi : \mathsf{Y} \to \mathsf{R}^k$ be a finite-dimensional projection and let $u \quad u$ in U be given. The restricted Laplace mechanism, $\hat{Y}^{(u)}$ with scale parameter $b = \frac{\Delta}{\varepsilon}$, satisfies*

$$\mathsf{P}(\pi(\hat{Y}^{(u)}) \quad A) \quad \geq \quad e^{-2\varepsilon}\mathsf{P}(\pi(\hat{Y}^{(u\ )}) \quad A)$$

for all Borel sets $A \quad \mathsf{R}_+^k$.

Proof: By definition

$$\mathsf{P}(\pi(\hat{Y}^{(u)}) \quad A) \quad = \quad \frac{\int_A e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi}{\int_{\mathsf{R}_+^k} e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi}$$

First we consider $\int_A e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi$:

$$\begin{aligned}
\int_A e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi \quad &= \quad \int_A e^{-\ \xi-\pi(y^{(u\ )})+\pi(y^{(u\ )})-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi \\
&\geq \quad \int_A e^{-(\ \xi-\pi(y^{(u\ )})\ _1+\ \pi(y^{(u\ )})-\pi(y^{(u)})\ _1) \frac{\varepsilon}{\Delta}} d\xi \\
&\geq \quad \int_A e^{-\ \xi-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta} - \varepsilon} d\xi \qquad (4.8) \\
&= \quad e^{-\varepsilon} \int_A e^{-\ \xi-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi
\end{aligned}$$

(4.8) follows from noting that $\pi(y^{(u\ )}) - \pi(y^{(u)})\ _1 \leq \ y^{(u)} - y^{(u\ )}\ _1 \leq \Delta$ by the definition of the l_1 sensitivity Δ. Similarly we can show that:

$$\begin{aligned}
\int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi \quad &= \quad \int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u)})+\pi(y^{(u)})-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi \\
&\geq \quad e^{-\varepsilon} \int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi
\end{aligned}$$

$$= \quad \frac{1}{\int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u)})\ _1 \frac{\varepsilon}{\Delta}} d\xi} \quad \geq \quad \frac{e^{-\varepsilon}}{\int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi}$$

It now follows immediately that

$$\begin{aligned}
\mathsf{P}(\pi(\hat{Y}^{(u)}) \quad A) \quad &\geq \quad e^{-2\varepsilon} \frac{1}{\int_{\mathsf{R}_+^q} e^{-\ \xi-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi} \int_A e^{-\ x-\pi(y^{(u\ )})\ _1 \frac{\varepsilon}{\Delta}} d\xi \\
&= \quad e^{-2\varepsilon}\mathsf{P}(\pi(\hat{Y}^{(u\ )}) \quad A)
\end{aligned}$$

as claimed. □

The next result follows immediately by combining the results of Propositions 4.2.5 and 4.2.2.

Corollary 4.2.6. *The restricted Laplace mechanism* $\hat{Y}^{(u)} : \Omega \to \mathsf{Y}_+$, *with scale parameter* $b = \frac{\Delta_1(\Sigma)}{\varepsilon}$ *is* 2ε *differentially private.*

The key point of this section has been to show that the methods of the last chapter can help build mechanisms for positive systems that take only non-negative values. For the rest of the chapter, we will be interested in the l_1 sensitivity of a positive linear observer.

4.3 Sensitivity for positive Luenberger observers

From our results in Chapter 3, and in the above section, we can see that the sensitivity is a crucial parameter in forming differentially private mechanisms. Our work is motivated by the design of differentially private observers for LTI systems in discrete time. For the remainder of this chapter, we concentrate on estimating the l_1 sensitivity for a positive linear observer and then aim to minimise the sensitivity bound.

We briefly recall some notation and terminology from Chapter 2 concerning LTI systems, Luenberger observers, adjacency relations, and differential privacy. We consider systems Σ of the form:

$$\begin{aligned} x(t+1) &= Ax(t) \\ y(t) &= Cx(t) \end{aligned} \tag{4.9}$$

where $A \quad \mathsf{R}^{n\times n}$, $C \quad \mathsf{R}^{p\times n}$. The design of a Luenberger observer for this system requires a matrix $L \quad \mathsf{R}^{n\times p}$ such that the solution $\hat{x}(\cdot)$ of the system Σ_0 given by

$$\hat{x}(t+1) = (A - LC)\hat{x}(t) + Ly(t) \tag{4.10}$$

satisfies $\hat{x}(t) - x(t) \to 0$ as $t \to \infty$ where x is the solution of (4.9).

Let $K > 0$ and $0 \leq \alpha < 1$ be given. We will work with the definition of adjacency in (2.24). Two sequences/signals $y, y \quad$ are *adjacent*, written $y \quad y$ if

$$t_0 \geq 0 \, s.t. \begin{cases} y(t) = y\,(t), & t < t_0 \\ y(t) - y\,(t)\ _1 \leq K\alpha^{t-t_0}, & t \geq t_0 \end{cases} \tag{4.11}$$

As our aim is to design a differentially private positive observer for positive linear system, as stated in Chapter 2, we need to calculate the sensitivity of the observer (4.10). From Definition 2.4.1, the l_1 sensitivity $\Delta_1(\Sigma_0)$ of the observer system Σ_0 is given by

$$\Delta_1(\Sigma_0) := \sup_{y \ y} \ \Sigma_0(y) - \Sigma_0(y\ )\ _1. \tag{4.12}$$

It is possible to define sensitivity with respect to other norms; in particular the l_2 norm is used in the definition of Gaussian mechanisms for *relaxed* differential privacy [72], this will be looked into in detail in Chapter 6.

To form an ε differentially private mechanism, we will add *iid* noise generated from the Laplace distribution with parameter $b = \frac{\Delta(\Sigma_0)}{\epsilon}$ to each component of each $\hat{x}(t)$ [72]. For this reason we are interested in characterising the l_1 sensitivity of the observer (4.10) mapping y to $\hat{x}$. This naturally motivates the problem of determining bounds for the l_1 sensitivity of (4.10).

Proposition 4.3.1. *Let* $A \quad \mathsf{R}^{n\times n}$, $C \quad \mathsf{R}^{p\times n}$, $L \quad \mathsf{R}^{n\times p}$ *be given and suppose that* $A - LC\ _1 < 1$. *Consider the Luenberger observer,* Σ_0 *given by* (4.10). *Then for the adjacency relation defined by* (4.11), *the* l_1 *sensitivity of* Σ_0 *(as given in (4.12)) is bounded by*

$$\Delta_1(\Sigma_0) \leq \left(\frac{K}{1-\alpha}\right)\left(\frac{L\ _1}{1 - \ A - LC\ _1}\right). \tag{4.13}$$

Proof: Let two adjacent sequences $y \quad y$ be given. The map from y to $\hat{x}$ corresponding to (4.10), with $\hat{x}_0$ as the common initial state, is described by

$$\hat{x}(t+1) = (A - LC)^{t+1}\hat{x}_0 + \sum_{i=0}^{t}(A - LC)^{t-i}Ly(i) \tag{4.14}$$

Write $\hat{x}$ for the observer output corresponding to y so that

$$\hat{x}\ (t+1) = (A - LC)^{t+1}\hat{x}_0 + \sum_{i=0}^{t}(A - LC)^{t-i}Ly\ (i). \tag{4.15}$$

As $y \quad y$, it follows that $\hat{x}\ (t) = \hat{x}(t)$ for $t \leq t_0$. Moreover, for $t > t_0$, we have

$$\hat{x}(t) - \hat{x}\ (t) = \sum_{i=t_0}^{t-1}(A - LC)^{t-i-1}L(y(i) - y\ (i)). \tag{4.16}$$

We need to bound $\|\hat{x}(t) - \hat{x}\,(t)\|_1$; for $t > t_0$, using the triangle inequality and the submultiplicative property of the induced matrix norm we have:

$$\begin{aligned}
\|\hat{x}(t) - \hat{x}\,(t)\| &= \sum_{i=t_0}^{t-1} \|(A - LC)^{t-i-1} L(y(i) - y\,(i))\|_1 \\
&\leq \sum_{i=t_0}^{t-1} \|(A - LC)^{t-i-1}\|_1 \|L\|_1 \|y(i) - y(i)\|_1 \\
&\leq \sum_{i=t_0}^{t-1} \|(A - LC)^{t-i-1}\|_1 \|L\|_1 K\alpha^{i-t_0} \\
&= \|L\|_1 K \sum_{i=t_0}^{t-1} \|(A - LC)^{t-i-1}\|_1 \alpha^{i-t_0} \\
&\leq \|L\|_1 K \sum_{i=t_0}^{t-1} \|(A - LC)\|_1^{t-i-1} \alpha^{i-t_0}.
\end{aligned}$$

The l_1 norm of $\hat{x}(t) - \hat{x}\,(t)$ will be given by the sum $\sum_{t=t_0+1}^{\infty} \|\hat{x}(t) - \hat{x}\,(t)\|_1$ which, in the light of the above calculation and remarks, will be bounded above by

$$\|L\|_1 K \sum_{t=t_0}^{\infty} \sum_{i=t_0}^{t} \|(A - LC)\|_1^{t-i} \alpha^{i-t_0}. \tag{4.17}$$

The infinite series above can be rearranged as follows (keeping in mind that the series is absolutely convergent as $\alpha < 1$, $\|A - LC\|_1 < 1$):

$$\begin{aligned}
\sum_{t=0}^{\infty} \sum_{i=0}^{t} \|(A - LC)\|_1^{t-i} \alpha^i &= \sum_{i=0}^{\infty} \alpha^i \left(\sum_{t=i}^{\infty} \|(A - LC)\|_1^{t-i} \right) \\
&= \sum_{i=0}^{\infty} \alpha^i \left(\sum_{t=0}^{\infty} \|(A - LC)\|_1^{t} \right) \\
&= \sum_{i=0}^{\infty} \alpha^i \left(\frac{1}{1 - \|A - LC\|_1} \right) \\
&= \left(\frac{1}{1 - \alpha} \right) \left(\frac{1}{1 - \|A - LC\|_1} \right).
\end{aligned}$$

Putting everything together, we see that the l_1 norm of $\hat{x} - \hat{x}$ is bounded above by

$$\left(\frac{K}{1 - \alpha} \right) \left(\frac{\|L\|_1}{1 - \|A - LC\|_1} \right)$$

which completes the proof as y y were arbitrary. $\square$

4.3.1 Tightness of upper bound

A natural question is whether or not the upper bound on the sensitivity of (4.10) given in Proposition 4.3.1 is in fact tight. The following example describes a situation in which the upper bound is attained.

Example 4.3.1. Consider the matrices

$$A = \begin{pmatrix} 1 & 1/2 \\ 1/4 & 3/4 \end{pmatrix}, \; C = \begin{pmatrix} 1/3 & 1/3 \end{pmatrix}, \; L = \begin{pmatrix} 1 \\ 1/2 \end{pmatrix}.$$

Direct calculation shows that

$$A - LC = \begin{pmatrix} 2/3 & 1/6 \\ 1/12 & 7/12 \end{pmatrix}.$$

Thus, $\|A - LC\|_1 = 3/4 < 1$. Moreover,

$$(A - LC)L = (3/4)L = \|A - LC\|_1 L$$

so that $(A - LC)^i L = \|A - LC\|_1^i L$ for all $i \geq 1$. Using this, we can see that for a pair of adjacent sequences y, y' where $y(t), y'(t)$ are in R for all t and satisfy (4.11) with equality replacing the inequality (as we are dealing with scalars, this is not difficult to achieve), the corresponding observer states $\hat{x}, \hat{x}'$ satisfy

$$\|\hat{x}' - \hat{x}\|_1 = \left(\frac{K}{1-\alpha}\right)\left(\frac{\|L\|_1}{1 - \|A - LC\|_1}\right)$$

so that the bound of Proposition 4.3.1 is tight for this particular choice of A, C, L.

Comment The point of the last example is to show that it is possible for the upper bound for the l_1 sensitivity of the system (4.10) given in Proposition 4.3.1 to be exact for some choices of A, C, L. It should be noted that the matrices A, C, L and $A - LC$ above are all nonnegative.

4.3.2 Relation to bounds given in [67]

In [67], the following nonlinear system was considered,

$$x(t+1) = f(x(t)) \tag{4.18}$$

$$y(t+1) = g(x(t)), \tag{4.19}$$

and a method of constructing a ε differentially private observer using Laplace noise was described. In particular, the result of Corollary 2 in [67], gives an upper bound of the l_1 sensitivity of the system, making use of results from contraction analysis for nonlinear systems. We will now translate the upper bound in [67] to compare it with our upper bound, (4.13) which we will denote by M.

Consider the linear observer (4.10), let $\eta > 0$ be give and $\beta > 0$ satisfy the following:

$$\|A - LC\|_1 \leq \beta, \ \gamma = \max\{\alpha + \frac{t\|L\|_1}{\eta}, \beta\}.$$

Corollary 2 of [67] shows that the l_1 sensitivity of (4.10) is bounded by

$$M_1 = \eta\left(\frac{1}{1-\gamma} - \frac{1}{1-\alpha}\right) \tag{4.20}$$

Manipulation of inequalities shows that

$$M_1 \geq \left(\frac{\beta-\alpha}{\gamma-\alpha}\right)\left(\frac{K}{1-\alpha}\right)\left(\frac{\|L\|_1}{1-\|A-LC\|_1}\right).$$

Thus $M_1 \geq \frac{\beta-\alpha}{\gamma-\alpha}M$ and in the case where $\beta = \gamma$, the upper bound M_1 is at best as tight as our bound (4.13). Further, it is important to note that we have shown that the bound (4.13) is attained for some systems.

4.4 Positive observers

We now specialise to the question of *positive observer design* [5, 52, 10] and consider the problem of minimising the bound for l_1 sensitivity given in Proposition 4.3.1 when the observer is required to be positive. Recall that the system (4.9) is positive if and only if the matrices A, C are nonnegative and that the positive observer design problem [5] requires the construction of a matrix L such that $A - LC \geq 0$, $LC \geq 0$ and $\rho(A - LC) < 1$ (see Theorem 2.3.4 in Chapter 2).

Before stating the optimisation problem we will consider for the remainder of the chapter, recall that K and α are fixed parameters determined by the definition of adjacency (4.11). Further, the bound given by (4.13) is only valid for matrices L with $\|A - LC\|_1 < 1$; otherwise, it is not guaranteed that the observer has finite l_1 sensitivity. With this in mind, we propose the following problem.

Problem 4.4.1. *Given* $A \in \mathbb{R}_+^{n\times n}$, $C \in \mathbb{R}_+^{p\times n}$, ***minimise***

$$\Phi(L) := \frac{\|L\|_1}{1 - \|A - LC\|_1} \tag{4.21}$$

subject to the constraints:

$$LC \geq 0,\ A - LC \geq 0, \quad \|A - LC\|_1 < 1 \tag{4.22}$$

If Φ is an optimal value for Problem 4.4.1, the minimal value of (4.13) is given by

$$\frac{K}{1-\alpha}\Phi\ .$$

Comment: While the constraints in (4.22) are convex, unfortunately the function Φ in general is not convex; hence we cannot directly apply results and algorithms on convex optimisation to our problem. The discussion that follows Problem 4.4.2 below about the single output case will show clearly that F is not in general a convex function.

We next characterise the feasibility and solution of Problem 4.4.1 for systems with a single output variable ($p = 1$). In this case (where $C \geq 0$) the constraint $LC \geq 0$ can be replaced by $L \geq 0$ [5].

4.4.1 The single-output case: feasibility

If the measured output y is 1-dimensional, so that $C \in \mathbb{R}^{1\times n}$, we will write c^T for C where $c \in \mathbb{R}^n$ is a column vector and $L = l$ where $l \in \mathbb{R}^n$. In this case, testing the feasibility of Problem 4.4.1 (the existence of a positive linear observer satisfying $\|A - lc^T\|_1 < 1$) is straightforward.

For a vector $c \in \mathbb{R}_+^n$ the *support* of c, $\mathrm{supp}(c)$ is given by $\mathrm{supp}(c) = \{j : c_j = 0\}$.

Proposition 4.4.1. *Let* $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n$, $c = 0$ *be given. There exists some* $l \in \mathbb{R}_+^n$ *satisfying* (4.22) *if and only if*

$$\sum_{i=1}^{n} \min_{j\ \mathrm{supp}(c)} \frac{a_{ij}}{c_j} > \max_{j\ \mathrm{supp}(c)} \frac{1}{c_j}\left(\sum_{i=1}^{n} a_{ij} - 1\right). \tag{4.23}$$

Proof: If such an l exists then it follows from $A - lc^T \geq 0$ that $l_i c_j \leq a_{ij}$ for all $1 \leq j \leq n$ and hence $l_i \leq \min_{j\ \mathrm{supp}(c)} \frac{a_{ij}}{c_j}$. It now follows from $\|A - lc^T\|_1 < 1$

that for all $1 \leq j \leq n$

$$\begin{aligned}
&\sum_{i=1}^{n}(a_{ij} - l_i c_j) < 1 \\
&c_j \sum_{i=1}^{n} l_i > \sum_{i=1}^{n} a_{ij} - 1 \\
&c_j \sum_{i=1}^{n} {}_j \min_{\mathrm{supp}(c)} \frac{a_{ij}}{c_j} > \sum_{i=1}^{n} a_{ij} - 1
\end{aligned}$$

and (4.23) follows immediately.

Conversely if (4.23) holds, then it is simple to check that the vector l defined by setting $l_i = \min_{j \ \mathrm{supp}(c)} \frac{a_{ij}}{c_j}$ will satisfy (4.22). □

4.4.2 The single output case: optimality

Continuing with the case where $p = 1$, the induced l_1 norm of L in $\mathbb{R}^{n\times 1}$ is simply the usual l_1 norm of the associated column vector l, so $\|L\|_1 = \sum_{i=1}^{n} l_i$. We next note that in this case, the function Φ in (4.21) can be written in a simpler form.

Lemma 4.4.2. *Given $A \in \mathbb{R}^{n\times n}_+$, $c, l \in \mathbb{R}^n$, we can write:*

$$\Phi(l) = \max_j \frac{\sum_{i=1}^{n} l_i}{(1 - \sum_{i=1}^{n} a_{ij}) + c_j \sum_{i=1}^{n} l_i}.$$

Proof: This is a simple calculation as:

$$\begin{aligned}
\Phi(l) &= \frac{\|l\|_1}{\|1 - A - lc^T\|_1} \\
&= \frac{\sum_{i=1}^{n} l_i}{1 - \max_j (\sum_{i=1}^{n}(a_{ij} - l_i c_j)} \\
&= \frac{\sum_{i=1}^{n} l_i}{\min_j (1 - \sum_{i=1}^{n}(a_{ij} - l_i c_j))} \\
&= \max_j \frac{\sum_{i=1}^{n} l_i}{(1 - \sum_{i=1}^{n} a_{ij}) + c_j \sum_{i=1}^{n} l_i}
\end{aligned}$$

as claimed. □

Taken together, Lemma 4.4.2 and Proposition 4.4.1 show that for the single output case, minimising the l_1 sensitivity bound (4.13) reduces to the following uni-variate constrained optimisation problem.

Problem 4.4.2. ***Minimise***

$$\phi(x) = \max_j \frac{x}{(1 - \sum_{i=1}^n a_{ij}) + c_j x}$$

subject to

$$x \geq 0 \ \& \ \max_j \frac{1}{c_j} \left(\sum_{i=1}^n a_{ij} - 1 \right) < x \leq \sum_{i=1}^n \min_j \frac{a_{ij}}{c_j} \tag{4.24}$$

Note that as one of the constraints is strict, our optimal solution may be an infimum rather than a minimum in some circumstances.

In the following, we will use F to denote the feasibility region defined by (4.24).

If we define

$$\phi_j(x) = \frac{x}{(1 - \sum_{i=1}^n a_{ij}) + c_j x}, \ 1 \leq j \leq n,$$

then the following facts can be easily verified by direct computation.

- If $\sum_{i=1}^n a_{ij} < 1$ then: ϕ_j is a strictly increasing concave function on $\left[0, \sum_{i=1}^n \min_j \frac{a_{ij}}{c_j}\right]$ and $\phi_j(0) = 0$;
- If $\sum_{i=1}^n a_{ij} > 1$ then: ϕ_j is a strictly decreasing convex function on $\left(\frac{1}{c_j}\left(\sum_{i=1}^n a_{ij} - 1\right), \sum_{i=1}^n \min_j \frac{a_{ij}}{c_j}\right]$ and $\phi_j(x) \to \infty$ as x tends to $\frac{1}{c_j}\left(\sum_{i=1}^n a_{ij} - 1\right)$ from the right.
- If $\sum_{i=1}^n a_{ij} = 1$ then $\phi_j(x) = \frac{1}{c_j}$.

The discussion above suggests the following simple graphical scheme for solving Problem 4.4.2.

1. Determine the feasibility region (4.24) from A and c.
2. Plot each ϕ_j in this region and mark off the graph of $\phi = \max \phi_j$.
3. Find the point x where ϕ attains its minimum in (4.24). This value of f will be the minimum of the l_1 sensitivity bound (4.13) for the positive observer problem.
4. A vector l satisfying (4.23) with $\sum_{i=1}^n l_i = x$ will be an optimal positive observer. It is not difficult to see that such an l will always exist.

Before describing the optimal solution in detail for 2-dimensional systems, we note that there are essentially 3 cases to consider in the above scheme that concern weather ϕ_j are concave or convex.

All ϕ_j are concave

If $\sum_{i=1}^{n} a_{ij} < 1$ for all j, then as every ϕ_j is strictly increasing, it is not hard to see that the optimal point for Problem 4.4.2 occurs at $x = 0$ corresponding to $l = 0$ and $\Delta_1(\Sigma_0) = 0$. This is not surprising as in this case the matrix A has l_1 induced norm less than 1. Note however that while $l = 0$ may minimise sensitivity, it will deliver a sub-optimal rate of convergence in most cases.

All ϕ_j convex

If $\sum_{i=1}^{n} a_{ij} > 1$ for all j, then as every ϕ_j is strictly decreasing, and we can see that the optimal point for Problem 4.4.2 occurs at the upper limit of the feasibility region. This means $x = \sum_{i=1}^{n} \min_{j \ \mathrm{supp}(c)} \frac{a_{ij}}{c_j}$, corresponding to the observer gain defined by $l_i = \min_{j \ \mathrm{supp}(c)} \frac{a_{ij}}{c_j}$ for $1 \leq i \leq n$. This is also true if some of the row sums are equal to 1. In this case, the gain matrix l that minimises f is also optimal with respect to l_1 observer convergence.

Mixed case

For this case, we define the following two sets $J_+ = \{j \mid \sum_{i=1}^{n} a_{ij} > 1\}$ and $J_- = \{j \mid \sum_{i=1}^{n} a_{ij} < 1\}$, which are both non-empty. We determine all points of intersection x that lie in feasible region F, where $\phi_j(x) = \phi_k(x)$ for $j \quad J_+$, $k \quad J_-$. This amounts to solving a finite set of quadratic equations. If no points of intersection are in F, then the optimal point, x will again occur at the upper limit of F. Otherwise, the optimal point x will be one of the points of intersection.

4.4.3 The 2-d case

To illustrate some of the points made above, we now describe how to find an optimal observer for a 2-d positive linear system.

Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, c^T = \begin{pmatrix} c_1 & c_2 \end{pmatrix}, l = \begin{pmatrix} l_1 \\ l_2 \end{pmatrix}.$$

Since $A - lc^T \geq 0$, we have

$$0 \leq l_1 \leq \min\left\{\frac{a_{11}}{c_1}, \frac{a_{12}}{c_2}\right\},\ 0 \leq l_2 \leq \min\left\{\frac{a_{21}}{c_1}, \frac{a_{22}}{c_2}\right\}$$

If $A_{\ 1} < 1$, then we minimise $F(l)$, by setting $l = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. In the case where $A_{\ 1} \leq 1$ and one column sum is equal to 1, the infimum of Φ in $\mathcal{F}$ is given by $\frac{1}{c_j}$ where j is the index of the column summing to 1. This can be approximated to any desired degree of accuracy by choosing $l > 0$ sufficiently small.

If $A_{\ 1} > 1$ and $\sum_{i=1}^{2} a_{ij} > 1$, for $j = 1, 2$, then the optimal observer gain is given by

$$l_1 = \min\left\{\frac{a_{11}}{c_1}, \frac{a_{12}}{c_2}\right\},\ l_2 = \min\left\{\frac{a_{21}}{c_1}, \frac{a_{22}}{c_2}\right\}. \tag{4.25}$$

If $A_{\ 1} > 1$ and $\sum_{i=1}^{2} a_{ij} < 1$, for some $j \in \{1, 2\}$, then let $x = L_{\ 1}$ and write $\alpha_j = 1 - \sum_{i=1}^{2} a_{ij}$ for $j = 1, 2$.

We need to find the intersection of the two curves defined by $\phi_1(x) = \frac{x}{\alpha_1 + c_1 x}$ and $\phi_2(x) = \frac{x}{\alpha_2 + c_2 x}$. By setting

$$\frac{x}{\alpha_1 + c_1 x} = \frac{x}{\alpha_2 + c_2 x}$$

we find that $x = 0$ or $x = \frac{\alpha_2 - \alpha_1}{c_1 - c_2}$. If x lies outside of our feasible set $\mathcal{F}$, then the optimal value of l is again given by (4.25).

If x is within $\mathcal{F}$ then it corresponds to an optimal l and we need to choose l_1 and l_2 such that $l_1 \leq \min\left\{\frac{a_{11}}{c_1}, \frac{a_{12}}{c_2}\right\}, l_2 \leq \min\left\{\frac{a_{21}}{c_1}, \frac{a_{22}}{c_2}\right\}$ and $l_1 + l_2 = x$. This can be done by setting

$$l_1 = \min\{\min_{j \in \text{supp}(c)} \frac{a_{ij}}{c_j}, x\},\ l_2 = \max\{0, x - l_1\}.$$

The discussion of the previous paragraphs can readily be codified as an algorithm to find an optimal l for Problem 4.4.1 for 2-dimensional positive systems.

Example 4.4.1. Consider the system defined by

$$A = \begin{pmatrix} 1/2 & 2/3 \\ 1/3 & 1/2 \end{pmatrix},\ c^T = \begin{pmatrix} 2 & 3 \end{pmatrix}.$$

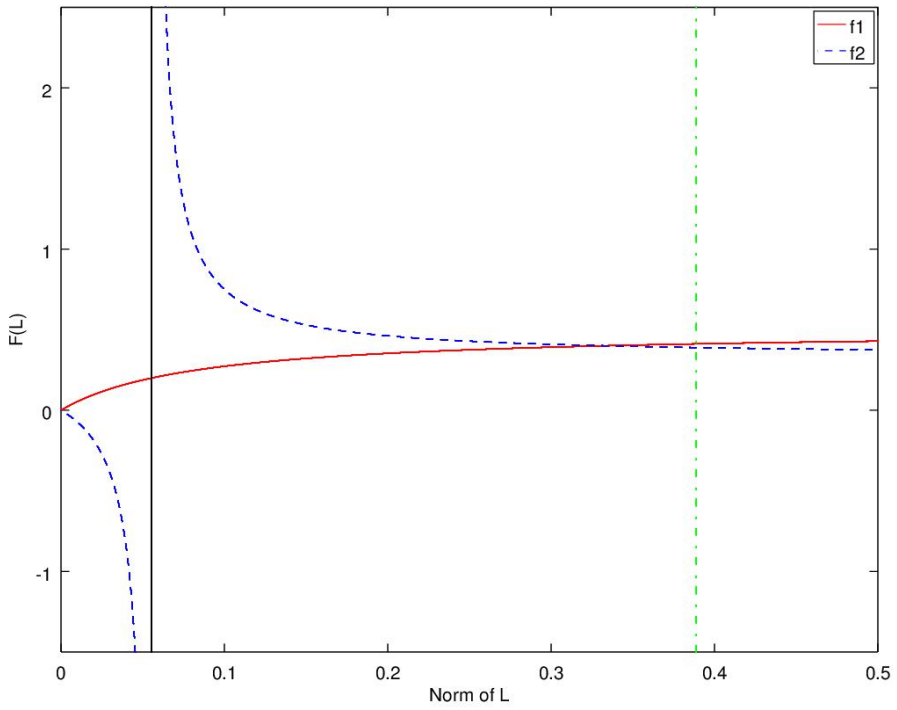

Figure 4.1: This graph shows the intersection of the curves $f_1(x)$ and $f_2(x)$, is within the range for L_1 $(\frac{1}{18}, \frac{7}{18}]$, where $\sum_{i=1}^{2} a_{i1} < 1$ and $\sum_{i=1}^{2} a_{i2} > 1$.

It is a straightforward computation to see that $F = (\frac{1}{18}, \frac{7}{18}]$. In this case, we have one column sum greater than 1 and one less than 1 so we compute the intersection point

$$x = \frac{7/6 - 9/6}{2 - 3} = \frac{1}{3}.$$

As $x \in F$, we can now compute the optimal l by setting $l_1 = \min\{2/9, 1/3\} = 2/9$ and $l_2 = \max\{0, 1/3 - 2/9\} = 1/9$ giving an optimal observer gain $l = (2/9\ 1/3)^T$. The curves corresponding to f_1, f_2 for this example are shown in Figure 4.1

4.4.3.1 n-dimensional l

Once we have solved for the optimal value x in Problem 4.4.2, to construct an optimal l for an n-dimensional system is a little more involved. However,

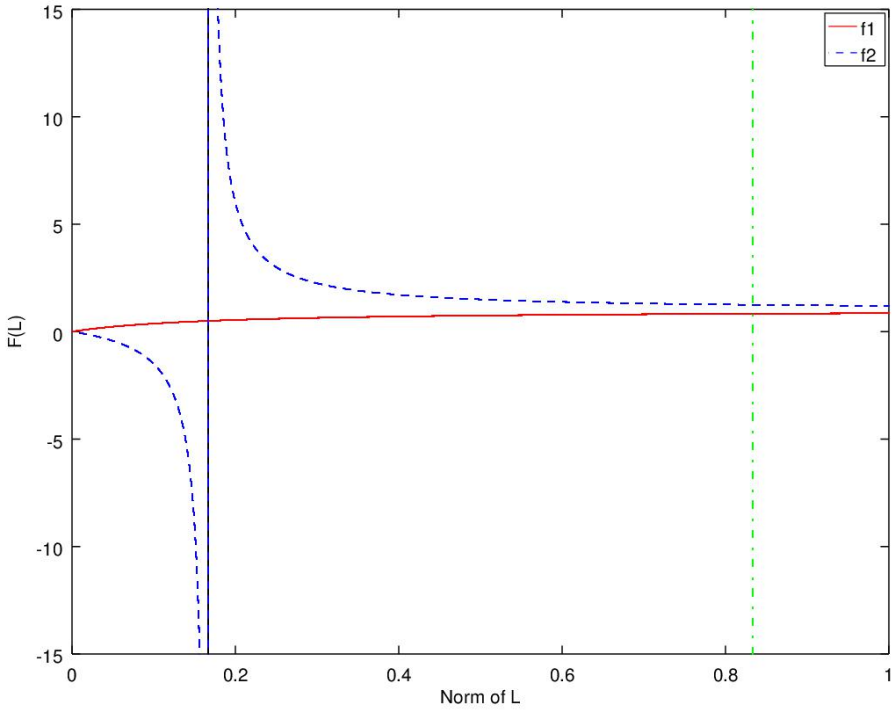

Figure 4.2: This graph shows the intersection of the curves $f_1(x)$ and $f_2(x)$, is outside the range for L_1 $(\frac{1}{6}, \frac{5}{6}]$, where $\sum_{i=1}^{2} a_{i1} < 1$ and $\sum_{i=1}^{2} a_{i2} > 1$

it is not too difficult to see that an algorithm for computing an optimal gain matrix can be defined using the following steps.

1. First set $r := x$. Remember that x defines the optimal value of l_1 so we are trying to construct an l satisfying the constraints with this norm.
2. Let $l_1 = \min\{\min_{j \in \text{supp}(c)} \frac{a_{1j}}{c_j}, r\}$.
3. For $2 \leq i \leq n$, set $r := r - l_{i-1}$. If $r > 0$, we then set $l_i = \min\{\min_{j \in \text{supp}(c)} \frac{a_{ij}}{c_j}, r\}$.
4. If for some i, $2 \leq i \leq n$, $r := r - l_{i-1} = 0$, then set $l_k = 0$ for $i \leq k \leq n$.
5. It is easy to see that l will satisfy the constraints of a positive observer and that $l_1 = x$.

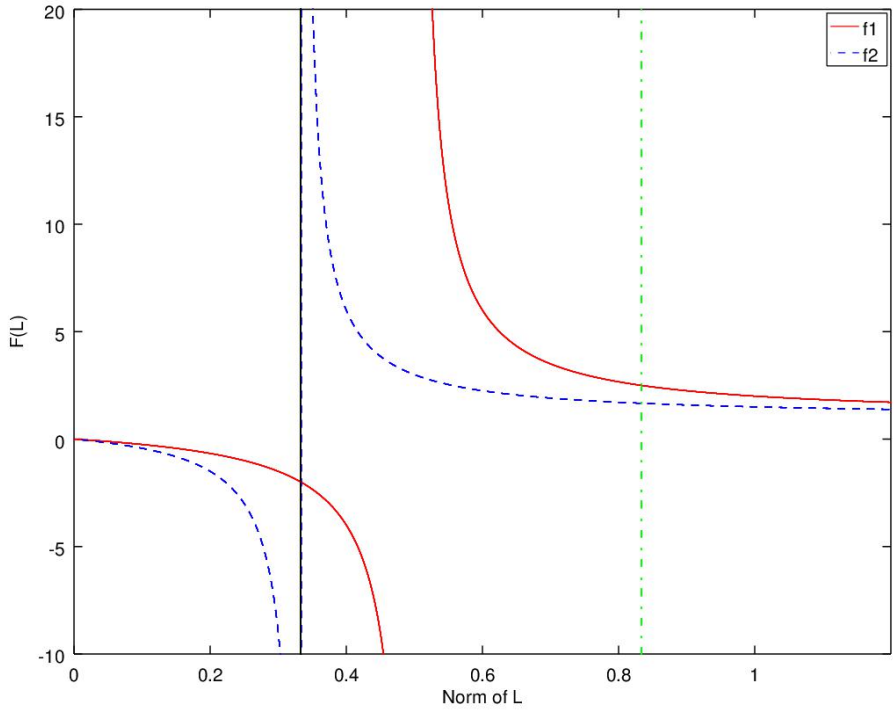

Figure 4.3: This graph shows the curves $f_1(x)$ and $f_2(x)$, where $\sum_{i=1}^{2} a_{i1} > 1$ and $\sum_{i=1}^{2} a_{i2} > 1$.

4.5 Conclusions

In this chapter, we have seen how to use the methods of post-processing and restriction developed in Chapter 3 to guarantee positivity when making a positive system and observer ε differentially private using the Laplace distribution. We then used these methods to build differentially private positive observers to guarantee positivity. Our first contribution was to calculate an upper bound for the l_1 sensitivity a linear Luenberger observer in Proposition 4.3.1. Our later results then describe how to minimise this bound for a single output linear system. Our approach here has been largely algorithmic. In the next chapter, we present a collection of more theoretical results on this problem.

CHAPTER 5

Further Aspects of l_1 Sensitivity: Compartmental Systems, Trade-offs, and Coordinate-Transformations

In this chapter, we derive explicit analytic expressions for positive observers that minimise the l_1 sensitivity bound for single-output and classes of multiple-output compartmental systems. We also consider the trade-o between the l_1 sensitivity bound of a positive linear observer and the rate at which it converges to the true system state. Specifically, for single-output systems, we derive an explicit expression for the minimum possible sensitivity bound for a given convergence rate, as quantified by the induced matrix norm of the observer. Some implications of this result for globally optimal observers are also derived. Finally, we make some observations on sensitivity for more general classes of positive observers constructed using coordinate transformations.

5.1 Introduction

In Chapter 4, one of our main results gave an upper bound for the l_1 sensitivity of a Luenberger observer for a linear system. We also considered the problem of minimising this bound for a positive linear observer. This problem is motivated by the natural wish to minimise the amount of noise needed to make

the observer differentially private in order to estimate the state as accurately as possible. We next present some further results on this problem as well as considering some new optimisation problems associated with it.

In this chapter, we present results for optimising the l_1 sensitivity for a compartmental system for the single output and multiple output cases. While we described numerical approaches in the last chapter, here our approach is more theoretical. Then, we consider the trade off between obtaining the lowest possible value for the sensitivity bound and the speed of convergence to the true state. With this in mind, the problem of minimising the l_1 sensitivity bound for a single output system where the norm of the observer system matrix is specified is considered. Lastly, the bound for l_1 sensitivity is extended to more general observers, which were introduced in [10] and we show that it is possible to improve on the optimal sensitivity for classical observers by considering this more general class.

5.1.1 Background

Before presenting our results for this chapter, we first fix our notation and recall the main concepts and results needed. We will consider the same system as in previous chapters; a positive LTI system:

$$\begin{aligned} x(t+1) &= Ax(t) \\ y(t) &= Cx(t), \end{aligned} \tag{5.1}$$

where $A \quad \mathsf{R}_+^{n\times n}$, $C \quad \mathsf{R}_+^{p\times n}$.

Recall that a classical Luenberger observer for (5.1) is given by

$$\hat{x}(t+1) = (A - LC)\hat{x}(t) + Ly(t) \tag{5.2}$$

where the matrix L is designed such that the solution $\hat{x}(t)$ of (5.2) satisfies $\lim_{t\to\infty} \ \hat{x}(t) - x(t) \ _1 = 0$ for any initial values $x(0)$, $\hat{x}(0)$.

Several of our main results in this chapter concern compartmental systems which arise in applications such as hydrology and population dynamics [62, 105, 104]. We only consider discrete time systems here.

Definition 5.1.1. A matrix A in $\mathsf{R}_+^{n\times n}$ is *compartmental* if $\sum_{i=1}^{n} a_{ij} \leq 1$ for all $1 \leq j \leq n$. If the system matrix A in (5.1) is compartmental, then (5.1) is a compartmental system.

Throughout this chapter, we work with the usual l_1 norm on R^n and the corresponding induced norm for matrices as defined in Chapter 2.

For a vector c R^n_+ the *support* of c, $\mathrm{supp}(c)$ is given by $\mathrm{supp}(c) = \{j : c_j = 0\}$.

We shall make use of the following characterisation of positive observers from [7], previously stated in Chapter 2.

Proposition 5.1.1. *Let A $\mathsf{R}^{n\times n}_+$, C $\mathsf{R}^{p\times n}_+$ be given. The system (5.2) is a positive observer for the positive system (5.1) if and only if the following conditions are satisfied.*

- $LC \geq 0$;
- $A - LC \geq 0$;
- $A - LC$ *is Schur-stable,* $\rho(A - LC) < 1$.

When calculating the upper bound for sensitivity of the more general observers from [11], we make use of the same definition of similarity of signals used in Chapter 4.

Definition 5.1.2. Let $K > 0$, $0 < \alpha < 1$ be given. Two sequences y, y from Y are similar, y y if there is some $t_0 \geq 0$ with

$$\begin{aligned} y(t) &= y(t) \qquad 0 \leq t < t_0 \\ y(t) - y(t)_1 &\leq K\alpha^{t-t_0} \qquad t \geq t_0. \end{aligned} \tag{5.3}$$

In Chapter 4, the following bound for the l_1 (as defined in Chapter 2, Definition 2.4.1) sensitivity of a linear observer was derived.

Proposition 5.1.2. *Consider the observer (5.2) with $A - LC_1 < 1$ and let $K > 0$, $0 < \alpha < 1$ be given. The sensitivity Δ of (5.2) with respect to the similarity relation (5.3) satisfies the following bound:*

$$\Delta \leq \frac{K}{1-\alpha}\left(\frac{L_1}{1 - A - LC_1}.\right) \tag{5.4}$$

In order to minimise the amount of noise added to the observer state $\hat{x}$, we want to find an observer gain L that minimises the upper bound in Proposition

5.1.2. As K and α are fixed parameters, we shall be interested in constructing observer gain matrices, L, that minimise the function

$$\Phi(L) := \frac{\|L\|_1}{1 - \|A - LC\|_1}, \tag{5.5}$$

for L satisfying $0 \leq LC \leq A$, $\|A - LC\|_1 < 1$. While Proposition 5.1.1 has the requirement $\rho(A - LC) < 1$, we need $\|A - LC\|_1 < 1$ in order for the observer to be sure to have finite sensitivity. After deriving a number of results related to this problem, we will consider bounds for more general observers, introduced in [10], in Section 5.4.

5.2 Compartmental Systems

In this section we consider the case where (5.1) is a compartmental system in the sense of Definition 5.1.1. Many fundamental results on the design of positive observers for compartmental systems, in continuous and discrete-time, were presented in [106]. Our interest is in minimising the function Φ (5.5) over observer gain matrices L that define a positive observer for the system (5.1).

Note that if $\|A\|_1 < 1$, we can choose $L = 0$ and then $\Phi(L) = 0$ so this case is trivial for the problem we are studying here. For this reason, we assume that the compartmental matrix A has $\|A\|_1 = 1$.

5.2.1 Single output systems: $p = 1$

We first consider the *rank one* case where $p = 1$, corresponding to a single output system.

Given a compartmental matrix $A \in \mathbb{R}_+^{n\times n}$ with $\|A\|_1 = 1$ and a column vector $c \in \mathbb{R}_+^n$, we say that (A, c) is a *feasible pair* if there exists some nonnegative $l \in \mathbb{R}_+^n$ with $\|A - lc^T\|_1 < 1$, $A - lc^T \geq 0$. Note that when $p = 1$, the conditions $lc^T \geq 0$, $l \geq 0$ are equivalent [7]. We denote the set of all such l by $\mathcal{F}_{A,c}$. We first characterise feasible pairs for the compartmental case.

Lemma 5.2.1. *Let a compartmental matrix $A \in \mathbb{R}_+^{n\times n}$ with $\|A\|_1 = 1$, and $c \in \mathbb{R}_+^n$ be given. Let $\mathcal{J} := \{j : \sum_{i=1}^n a_{ij} = 1\}$. Then (A, c) is a feasible pair if and only if the following conditions are satisfied.*

(i) $\mathcal{J} \subseteq$ *supp*(c).

(ii) There exists some i with $1 \leq i \leq n$ such that $a_{ij} > 0$ for all j supp(c).

Proof: First assume that (i) and (ii) hold. Choose some k such that $a_{kj} > 0$ for all j supp(c) and set $x = \min\{\frac{a_{kj}}{c_j} : j$ supp$(c)\}$. Clearly, $x > 0$. Now define l $\mathbb{R}^n_+$ by

$$l_i = \begin{cases} x & i = k \\ 0 & i = k. \end{cases} \tag{5.6}$$

It follows immediately that for $i = k$, $a_{ij} - l_i c_j = a_{ij} \geq 0$. Moreover, for $i = k$, $a_{kj} - l_k c_j = a_{kj} \geq 0$ for j / supp(c). For j supp(c), the definition of x implies that

$$a_{kj} - l_k c_j = a_{kj} - x c_j \geq 0.$$

It follows that $A - lc^T \geq 0$. Furthermore, $x > 0$ and J supp(c); these conditions imply that for j J,

$$\sum_{i=1}^{n}(a_{ij} - l_i c_j) = (\sum_{i=1}^{n} a_{ij}) - x c_j = 1 - x c_j < 1.$$

From the definition of J, we conclude that $\|A - lc^T\|_1 < 1$ and hence (A, c) is a feasible pair.

Conversely, assume that (A, c) is a feasible pair and let $l \geq 0$ be such that $A - lc^T \geq 0$ and $\|A - lc^T\|_1 < 1$. As $\|A\|_1 = 1$, it follows that J is non-empty and that $l = 0$. Let j J be given. Then $\sum_{i=1}^n a_{ij} = 1$ and, as $\|A - lc^T\|_1 < 1$, we must have $\sum_{i=1}^n (a_{ij} - l_i c_j) < 1$. This implies that $c_j > 0$ and hence j supp(c). This proves (i). As $l = 0$, we can choose some i with $l_i > 0$. Then as $a_{ij} - l_i c_j \geq 0$ for all i, j we must have $a_{ij} > 0$ for all j supp(c). This proves (ii) and completes the proof of the Lemma. □

When $p = 1$, the gain matrix L is simply a column vector l $\mathbb{R}^n_+$; hence, in the remainder of this subsection (where $p = 1$) we alter our notation slightly and consider the function defined on $F_{A,c}$:

$$\Phi(l) = \frac{\|l\|_1}{1 - \|A - lc^T\|_1}. \tag{5.7}$$

In Chapter 4, a numerical procedure for computing the minimum value of Φ for l $F_{A,c}$ was described for general A. In our next result, we give an explicit analytic characterisation of this minimum value for compartmental A.

Theorem 5.2.2. *Let a compartmental matrix $A \in \mathbb{R}_+^{n\times n}$ with $\|A\|_1 = 1$, and $c \in \mathbb{R}_+^n$ be given such that the set $\mathcal{F}_{A,c}$ is non-empty. Let $\mathcal{J} := \{j : \sum_{i=1}^n a_{ij} = 1\}$. There exists $\hat{l} \in \mathcal{F}_{A,c}$ such that*

$$\Phi(l) \geq \Phi(\hat{l}) = \frac{1}{\min_{j\in\mathcal{J}} c_j}. \tag{5.8}$$

Proof: We first note that for any $l \in \mathcal{F}_{A,c}$,

$$\begin{aligned}
\|A - lc^T\|_1 &= \max_{1\leq j\leq n} \sum_{i=1}^n a_{ij} - l_i c_j \\
&= \max_{1\leq j\leq n} (\sum_{i=1}^n a_{ij} - \|l\|_1 c_j) \\
&\geq \max_{j\in\mathcal{J}} (\sum_{i=1}^n a_{ij} - \|l\|_1 c_j) \\
&= 1 - \|l\|_1 \min_{j\in\mathcal{J}} c_j.
\end{aligned}$$

This implies that $1 - \|A - lc^T\|_1 \leq \|l\|_1 \min_{j\in\mathcal{J}} c_j$ and hence that

$$\Phi(l) \geq \frac{1}{\min_{j\in\mathcal{J}} c_j}.$$

Thus to complete the proof, we need to show that there exists some $\hat{l}$ in $\mathcal{F}_{A,c}$ with $\Phi(\hat{l}) = \frac{1}{\min_{j\in\mathcal{J}} c_j}$.

Denote by $\mathcal{J}^c$ the set $\{1,\ldots,n\} \setminus \mathcal{J}$ and, for each $k \in \mathcal{J}^c$, let $\alpha_k = \sum_{i=1}^n a_{ik}$ denote the corresponding column sum. Let j_0 be any index such that $c_{j_0} = \min\{c_j : j \in \mathcal{J}\}$ and let

$$M = \min\left\{\frac{1-\alpha_k}{c_{j_0} - c_k} : k \in \mathcal{J}^c, c_k < c_{j_0}\right\}.$$

Then as $\alpha_k < 1$ for all $k \in \mathcal{J}^c$, $M > 0$. By assumption, $\mathcal{F}_{A,c}$ is non-empty. Thus, by Lemma 5.2.1, $\mathcal{J} \cap \text{supp}(c)$ and we can choose some i_0 such that $a_{i_0 j} > 0$ for all $j \in \text{supp}(c)$. Define the vector $\hat{l} \in \mathbb{R}_+^n$ by:

$$\hat{l}_i = \begin{cases} 0 & i = i_0 \\ \min\left(\{M\} \cup \{\frac{a_{i_0 j}}{c_j} : j \in \text{supp}(c)\}\right) & i = i_0. \end{cases}$$

We note the following readily verifiable facts.

(i) $\hat{l} \geq 0$; $\|\hat{l}\|_1 \leq M$.

(ii) $a_{ij} - \hat{l}_i c_j \geq 0$ for all $1 \leq i, j \leq n$.

(iii) $\sum_{i=1}^{n}(a_{ij} - \hat{l}_i c_j) < 1$ for $1 \leq j \leq n$. This follows from the facts that A is compartmental, $\hat{l} = 0$, and $J \quad \text{supp}(c)$.

For the final part of the proof, we will show that for $\hat{l}$ constructed above, $A - \hat{l}c^T \ _1 = \frac{1}{c_{j_0}}$. First note that for any $k \quad J$, by the choice of j_0:

$$1 - \ \hat{l} \ _1 c_{j_0} \geq 1 - \ \hat{l} \ _1 c_k.$$

Now consider $k \quad J^c$. Then $\alpha_k < 1$ so if $c_k \geq c_{j_0}$,

$$1 - \ \hat{l} \ _1 c_{j_0} > \alpha_k - \ \hat{l} \ _1 c_k.$$

Finally, if $k \quad J^c$, and $c_k < c_{j_0}$,

$$\begin{aligned} & \hat{l} \ _1 \leq M \\ = \quad & \hat{l} \ _1 \leq \frac{1 - \alpha_k}{c_{j_0} - c_k} \\ = \quad \alpha_k - \ \hat{l} \ _1 c_k \leq \ & 1 - \ \hat{l} \ _1 c_{j_0}. \end{aligned}$$

Putting the previous calculations together, we see that

$$\begin{aligned} A - \hat{l}c^T \ _1 &= \max_{1 \leq j \leq n} \sum_{i=1}^{n} a_{ij} - \ \hat{l} \ _1 c_j \\ &= 1 - \ l \ _1 c_{j_0}. \end{aligned}$$

It now follows immediately that

$$\Phi(\hat{l}) = \frac{1}{c_{j_0}} = \frac{1}{\min_j \ _J \ c_j},$$

which completes the proof. □

Remark: The preceding result implies that for a single-output compartmental system, the minimum possible value of the sensitivity bound in Proposition 5.1.2 is

$$\frac{K}{(1 - \alpha) \min_j \ _J \ c_j}.$$

It also provides a constructive way of obtaining the gain vector $\hat{l}$ that minimises the sensitivity. A major advantage of the direct, linear algebraic approach in the above proof is that it gives insight into how this result may be extended to the case where $p \geq 2$, corresponding to multiple output systems. We address this issue in the next subsection.

5.2.2 Extension to multiple output systems ($p \geq 2$)

For the general case of a system of the form (5.1) with the matrix $C \in \mathbb{R}_+^{p\times n}$, $p \geq 2$, the necessary and sufficient conditions for $L \in \mathbb{R}^{n\times p}$ to define a positive observer are given in Proposition 5.1.1. In order for the bound for l_1 sensitivity in Proposition 5.1.2 to be finite, we consider the following, more restrictive set of conditions on L.

$$0 \leq LC \leq A; \qquad \|A - LC\|_1 < 1. \tag{5.9}$$

Given a compartmental matrix $A \in \mathbb{R}_+^{n\times n}$ with $\|A\|_1 = 1$ and $C \in \mathbb{R}_+^{p\times n}$, if there exists some L satisfying (5.9), we say that (A, C) is a feasible pair and denote the set of all such L by $\mathcal{F}_{A,C}$. We will be interested in minimising the function $\Phi(L)$ given by (5.5) over $L \in \mathcal{F}_{A,C}$.

Lemma 5.2.1 was important for our construction of the optimal observer gain vector l in Theorem 5.2.2. For this reason, we would like to generalise this lemma to the multiple output case. It is tempting to conjecture the following natural generalisation.

For $1 \leq k \leq p$, let $c^{(k)}$ denote the kth row of C. As above, let $\mathcal{J}$ denote the set $\{j : \sum_{i=1}^n a_{ij} = 1\}$. A natural conjecture generalising Lemma 5.2.1 is that (A, C) is a feasible pair if and only if the following two conditions are satisfied.

(F1) $\mathcal{J} \subseteq \bigcup_{k=1}^p \operatorname{supp}(c^{(k)})$.

(F2) For each k in $\{1, \ldots, p\}$, there exists some i_k such that $a_{i_k,j} > 0$ for all $j \in \operatorname{supp}(c^{(k)})$.

Unfortunately, this conjecture is not true as is shown by the following example.

Example 5.2.1. Consider the matrices:

$$A = \begin{pmatrix} 2/3 & 0 & 0 \\ 0 & 1/2 & 3/4 \\ 1/3 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Then clearly A is compartmental and $\|A\|_1 = 1$. Moreover, (A, C) is feasible as the matrix

$$L = \begin{pmatrix} 1/3 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

clearly satisfies (5.9). However, while it is true that $J \subseteq \bigcup_{k=1}^{p} \mathrm{supp}(c^{(k)})$, there is no i_k satisfying condition (F2) for $k = 2$.

We will revisit the previous example after our next result which extends Theorem 5.2.2 to multiple output compartmental systems satisfying conditions (F1) and (F2) above.

Theorem 5.2.3. *Let a compartmental $A \in \mathbb{R}_+^{n\times n}$ with $\|A\|_1 = 1$ and $C \in \mathbb{R}_+^{p\times n}$ with $p \geq 2$ be given. Assume that the pair (A, C) satisfies conditions (F1), (F2) above. Let $J = \{j : \sum_{i=1}^{n} a_{ij} = 1\}$ and for $1 \leq j \leq n$, let $\gamma_j = \sum_{i=1}^{p} c_{ij}$. Then the pair (A, C) is feasible and moreover there exists $\hat{L} \in \mathcal{F}_{A,C}$ such that for all L in $\mathcal{F}_{A,C}$:*

$$\Phi(L) \geq \Phi(\hat{L}) = \frac{1}{\min_{j \in J} \gamma_j}, \tag{5.10}$$

where Φ is given by (5.5).

Proof: Let $L \in \mathcal{F}_{A,C}$ be given. Then:

$$\begin{aligned} \|A - LC\|_1 &= \max_{1\leq j\leq n} \sum_{i=1}^{n} |[A - LC]_{ij}| \\ &= \max_{1\leq j\leq n} \sum_{i=1}^{n} [A - LC]_{ij} \\ &= \max_{1\leq j\leq n} \left(\sum_{i=1}^{n} a_{ij} - \sum_{i=1}^{n} [LC]_{ij} \right) \\ &\geq \max_{j \in J} \left(\sum_{i=1}^{n} a_{ij} - \sum_{i=1}^{n} [LC]_{ij} \right). \end{aligned} \tag{5.11}$$

Here we have used that $A - LC \geq 0$ in the second line. Now note that while we are not assuming $L \geq 0$ here, we do have $C \geq 0$ and hence for $1 \leq i, j \leq n$:

$$\begin{aligned} [LC]_{ij} &= \sum_{k=1}^{p} l_{ik} c_{kj} \\ &\leq \sum_{k=1}^{p} |l_{ik}| c_{kj}. \end{aligned}$$

It follows that for any j J:

$$\begin{aligned}\sum_{i=1}^{n}[LC]_{ij} &\leq \sum_{i=1}^{n}\sum_{k=1}^{p}|l_{ik}|c_{kj} \\ &= \sum_{k=1}^{p}(\sum_{i=1}^{n}|l_{ik}|)c_{kj} \\ &\leq L_{1}\sum_{k=1}^{p}c_{kj} = L_{1}\gamma_j.\end{aligned}$$

Combining this with (5.11), we see that

$$A - LC_{1} \geq \max_{j J}(1 - \sum_{i=1}^{n}[LC]_{ij}) \tag{5.12}$$

$$\geq \max_{j J}(1 - L_{1}\gamma_j) \tag{5.13}$$

$$= 1 - L_{1}\min_{j J}\gamma_j. \tag{5.14}$$

It now follows immediately that for any L $F_{A,C}$:

$$\Phi(L) = \frac{L_{1}}{1 - A - LC_{1}} \geq \frac{1}{\min_{j J}\gamma_j}.$$

It remains for us to show that there exists some $\hat{L}$ in $F_{A,C}$ such that $\Phi(\hat{L})$ attains this lower bound.

To begin, write J^{c} for the complement of J, $J^{c} = \{1,\ldots,n\} \setminus J$. Also, for $1 \leq j \leq n$, let $\alpha_j = \sum_{i=1}^{n} a_{ij}$; thus $\alpha_j < 1$ for all j J^{c}. It is easy to see that by choosing $x > 0$ sufficiently small, we can ensure that

$$1 - (\min_{j J}\gamma_j)x > \alpha_k - \gamma_k x, \quad k \quad J^{c}. \tag{5.15}$$

Now, assumption (F2) implies that for $1 \leq k \leq p$, there is some (not necessarily unique) i_k in $\{1,\ldots n\}$ such that $a_{i_k j} > 0$ for all j with $c_{kj} > 0$. We use this fact to construct $\hat{L}$.

First choose i_1 such that $c_{1j} > 0$ implies $a_{i_1 j} > 0$. Then, for some $x > 0$ (to be determined later) set $\hat{l}_{i_1 1} = x$, $\hat{l}_{s1} = 0$ for $s = i_1$. Repeat this, choosing i_k for $k = 2, 3, \ldots p$ and in each case setting $\hat{l}_{i_k k} = x$ and $\hat{l}_{sk} = 0$ otherwise. Note that all of the i_k selected need not necessarily be distinct. However, it can be seen from the construction of $\hat{L}$ that:

(i) each column of $\hat{L}$ has exactly one non-zero entry which is equal to x;

(ii) $\hat{l}_{sq} > 0$, $c_{qj} > 0$ implies that $a_{sj} > 0$ (as in this case $s = i_q$).

From (i), it follows that $\sum_{i=1}^{n} \hat{l}_{ij} = x$ for $1 \leq j \leq p$ and that $\|\hat{L}\|_1 = x$. From point (ii), it follows that by choosing x sufficiently small (and positive) we can ensure that $A - \hat{L}C \geq 0$. Clearly as $\hat{L} \geq 0$, $\hat{L}C \geq 0$. Finally, note that if $j \in \mathcal{J}$, there is some $k \in \{1, \ldots p\}$ such that $c_{kj} > 0$. Hence, by the construction of $\hat{L}$, $\hat{l}_{i_k k} = x > 0$. This implies that $\sum_{i=1}^{n} [A - \hat{L}C]_{ij} < 1$ for any such j and by the definition of $\mathcal{J}$, $\|A - \hat{L}C\|_1 < 1$. Thus $\hat{L} \in \mathcal{F}_{A,C}$. Finally, note that

$$\begin{aligned}
\|A - \hat{L}C\|_1 &= \max_{1 \leq j \leq n} \sum_{i=1}^{n} \left(a_{ij} - \sum_{s=1}^{p} \hat{l}_{is} c_{sj} \right) \\
&= \max_{1 \leq j \leq n} (\alpha_j - \sum_{i=1}^{n} \sum_{s=1}^{p} \hat{l}_{is} c_{sj}) \\
&= \max_{1 \leq j \leq n} (\alpha_j - \sum_{s=1}^{p} (\sum_{i=1}^{n} \hat{l}_{is}) c_{sj}) \\
&= \max_{1 \leq j \leq n} (\alpha_j - \sum_{s=1}^{p} x c_{sj}) \\
&= \max_{1 \leq j \leq n} (\alpha_j - x\gamma_j).
\end{aligned}$$

Now, if we choose $x > 0$ sufficiently small so that (5.15) holds, then we can ensure that

$$\max_{1 \leq j \leq n} (\alpha_j - x\gamma_j) = 1 - x \min_{j \in \mathcal{J}} \gamma_j.$$

As $\|\hat{L}\| = x$ by construction, it follows that for such a choice of $x > 0$:

$$\Phi(\hat{L}) = \frac{x}{x \min_{j \in \mathcal{J}} \gamma_j} = \frac{1}{\min_{j \in \mathcal{J}} \gamma_j}.$$

This completes the proof. □

Remarks:

(i) Theorem 5.2.3 explicitly characterises the minimum value of $\Phi(L)$ where L is the gain matrix of a positive observer for a multiple output compartmental system satisfying (F1), (F2). Further, the proof is constructive as it demonstrates how to construct an optimal observer gain matrix L.

(ii) It is possible to adapt the algorithmic approach to single output systems described in Chapter 4 to prove Theorem 5.2.2 for the case $p = 1$.

However the direct linear algebraic argument given here provides the insights needed for the generalisation to multiple-output systems developed in Theorem 5.2.2.

(iii) In the case $p \geq 2$, it is not necessary for the gain matrix L of a positive observer (5.9) to be nonnegative. It is worth noting that the optimal L constructed in Theorem 5.2.3 is indeed nonnegative. The problem of determining classes of positive linear systems for which this property holds is an interesting one for further research.

We now present an example to show that the result of Theorem 5.2.3 does not necessarily hold without the assumptions (F1), (F2) on the matrix pair (A, C).

Example 5.2.2. Recall the matrices A, C from Example 5.2.1.

$$A = \begin{pmatrix} 2/3 & 0 & 0 \\ 0 & 1/2 & 3/4 \\ 1/3 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

We saw earlier that the pair (A, C), while feasible, does not satisfy condition (F2). Now suppose that $L \quad \mathbb{R}^{3\times 2}$ is such that $LC \geq 0$ and $A - LC \geq 0$. A direct calculation shows that

$$LC = \begin{pmatrix} l_{11} + l_{12} & 0 & l_{12} \\ l_{21} + l_{22} & 0 & l_{22} \\ l_{31} + l_{32} & 0 & l_{32} \end{pmatrix}.$$

The conditions $LC \geq 0$, $A - LC \geq 0$ now imply that

$$l_{12} = l_{32} = 0; \quad l_{22} \geq 0; \quad l_{21} = -l_{22}.$$

Thus

$$L = \begin{pmatrix} l_{11} & 0 \\ -l_{22} & l_{22} \\ l_{31} & 0 \end{pmatrix}, \quad A - LC = \begin{pmatrix} 2/3 - l_{11} & 0 & 0 \\ 0 & 1/2 & 3/4 - l_{22} \\ 1/3 - l_{31} & 0 & 0 \end{pmatrix}.$$

It now follows that $\|L\|_1 = l_{11} + l_{22} + l_{31}$ and that $\|A - LC\|_1 \geq 1 - (l_{11} + l_{31}) \geq 1 - \|L\|_1$. This implies that

$$\frac{\|L\|_1}{1 - \|A - LC\|_1} \geq 1.$$

Thus, for any L with $0 \leq LC \leq A$, we must have $\Phi(L) \geq 1$. However, for this pair (A, C), $J = \{1\}$ and $\min_j \ _J \gamma_j = 2$. Thus there exists no L in $F_{A,C}$ with

$$\Phi(L) = \frac{1}{\min_j \ _J \gamma_j} = \frac{1}{2}.$$

5.3 Trade-offs for l_1 sensitivity

In the previous section, we studied the problem of minimising $\Phi(L)$ subject to (5.9) for compartmental systems. Optimal solutions were described for general compartmental systems with a single output ($p = 1$) and for a subclass of multiple-output compartmental systems. When designing an observer (5.2), the rate of convergence to the true state is also important, and this is determined by the norm $\|A - LC\|_1$ of the observer system matrix. In general, there will be a trade-off between obtaining the lowest possible value for the sensitivity bound and minimising the norm $\|A - LC\|_1$. In this section, we consider this trade-off for positive systems, not necessarily compartmental, with a single output.

Specifically, we consider a single-output positive system (5.1), where A is a nonnegative matrix, not necessarily compartmental, and C is a (non-zero) row vector, which we will write as c^T for some $c \in \mathbb{R}^n_+ \setminus \{0\}$. In this section, we go back to the notation of Section 5.2.1 and consider the interplay between the objective functions $\|A - lc^T\|_1$ and $\Phi(l)$ where $l \in \mathbb{R}^n_+$ is constrained to lie in the feasibility region $F_{A,c}$.

Formally, we consider the following problem.

Problem 5.3.1. *Given $A \in \mathbb{R}^{n\times n}_+$, $c \in \mathbb{R}^n_+$ and $\eta \in [0, 1)$, find the minimum value of $\Phi(l)$ subject to*

$$l \geq 0; \quad A - lc^T \geq 0; \quad \|A - lc^T\|_1 = \eta. \tag{5.16}$$

Of course, the constraints here will not be feasible for all values of η. With this in mind, we first characterise the possible values of $\|A - lc^T\|_1$ where l satisfies the first two conditions of (5.16).

Lemma 5.3.1. *Let $A \in \mathbb{R}^{n\times n}_+$, $c \in \mathbb{R}^n_+$ be given and suppose that $l \in \mathbb{R}^n_+$ is such that $A - lc^T \geq 0$. Define the vector $\hat{l}$ for $1 \leq i \leq n$ by*

$$\hat{l}_i = \min_{k \ supp(c)} \frac{a_{ik}}{c_k}. \tag{5.17}$$

Then

$$\|A - \hat{l}c^T\|_1 \leq \|A - lc^T\|_1 \leq \|A\|_1 \tag{5.18}$$

Proof: As $A - lc^T \geq 0$ and $l \geq 0$, it follows that for all $1 \leq i, j \leq n$

$$\begin{aligned} a_{ij} - l_i c_j &\geq 0 \\ = \quad l_i c_j &\leq a_{ij} \\ = \quad l_i &\leq \min_{k \ supp(c)} \frac{a_{ik}}{c_k}. \end{aligned}$$

If we set $\hat{l}_i = \min_{k \ \text{supp}(c)} \frac{a_{ik}}{c_k}$, then $l \leq \hat{l}$. It follows, as $c \geq 0$ that:

$$\begin{aligned} & A - \hat{l}c^T \leq A - lc^T \leq A \\ = \quad & \|A - \hat{l}c^T\|_1 \leq \|A - lc^T\|_1 \leq \|A\|_1 \end{aligned}$$

The implication follows from the monotonicity of the l_1 induced norm [59]. □

Remarks:

(i) For the rest of this section, given $A \in \mathbf{R}_+^{n \times n}$ and $c \in \mathbf{R}_+^n$, we shall use η_{min} and η_{max} to denote

$$\begin{aligned} \eta_{min} &= \|A - \hat{l}c^T\|_1 \\ \eta_{max} &= \|A\|_1. \end{aligned} \tag{5.19}$$

(ii) If $\eta_{min} = \eta_{max}$, then the only possible value of $\|A - lc^T\|_1$ for l satisfying the first two conditions of (5.16) is $\|A\|_1$. There are two possibilities in this case:

1. $\|A\|_1 \geq 1$: then there exists no l satisfying (5.16) with $\eta \in [0, 1)$ and the problem is not feasible;
2. $\|A\|_1 < 1$: then $l = 0$ gives a solution of Problem 5.3.1 with $\Phi(l) = 0$.

As the problem is either infeasible or trivial in this case, *we shall assume for the rest of this section that* $\eta_{min} < \eta_{max}$. Note that this implies that $\hat{l} = 0$.

(iii) Let $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n$ be such that $\eta_{min} < \eta_{max}$. Then it is not difficult to see that for any $\eta \in [\eta_{min}, \eta_{max}]$ there exists some $l \in \mathbb{R}_+^n$ that satisfies (5.16). This is essentially an application of the Intermediate Value Theorem coupled with the continuity of the norm.

(iv) We are interested in the function Φ as a bound for the l_1 sensitivity of a linear observer (5.2). This bound, given by Proposition 5.1.2, is only valid if $\|A - lc^T\|_1 < 1$ holds. For this reason, we will assume for the rest of this section that $\eta_{min} < 1$.

Given $\eta \in [\eta_{min}, \eta_{max}]$, we define the set $F(\eta)$ as follows:

$$F(\eta) = \{l \in \mathbb{R}_+^n : A - lc^T \geq 0, \ \|A - lc^T\|_1 = \eta\}. \tag{5.20}$$

In view of the assumption made in point (iii) above, $F(\eta) = \{0\}$.

Given, $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n$, and $\eta \in [\eta_{min}, \eta_{max}]$ we define $M(\eta)$ as:

$$M(\eta) = \max_{j \in \text{supp(c)}} \left(\frac{\sum_{i=1}^n a_{ij} - \eta}{c_j} \right) \tag{5.21}$$

The following lemma notes that under the assumptions made above in point (i), $M(\eta)$ is nonnegative.

Lemma 5.3.2. *Let $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n \setminus \{0\}$ be given. Assume that $\eta_{min} < \eta_{max}$. Then for any $\eta \in [\eta_{min}, \eta_{max}]$, $M(\eta) \geq 0$.*

Proof: By assumption, $\|A - \hat{l}c^T\|_1 < \|A\|_1$. This implies that for any j with $\sum_{i=1}^n a_{ij} = \|A\|_1$, we must have $c_j > 0$. Let $\sum_{i=1}^n a_{ik} = \|A\|_1$ for some k. It follows that $k \in \text{supp}(c)$ and that for $\eta \in [\eta_{min}, \eta_{max}]$:

$$\begin{aligned} M(\eta) &= \max_{j \in \text{supp(c)}} \left(\frac{\sum_{i=1}^n a_{ij} - \eta}{c_j} \right) \\ &\geq \frac{\sum_{i=1}^n a_{ik} - \eta}{c_k} \\ &= \frac{\|A\|_1 - \eta}{c_j} \\ &\geq 0. \end{aligned}$$

□

The next result characterises the norm of $l \in F(\eta)$ in terms of η and will prove useful in giving an answer to Problem 5.3.1.

Lemma 5.3.3. *Let* $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n \setminus \{0\}$ *be given and assume that* $\eta_{min} < \eta_{max}$. *Let* $l \in \mathcal{F}(\eta)$ *for some* $\eta \in [\eta_{min}, \eta_{max}]$. *Then*

$$\|l\|_1 \geq M(\eta).$$

Proof: As $\|A - lc^T\|_1 = \eta$:

$$\max_j \sum_{i=1}^n (a_{ij} - l_i c_j) = \eta$$

Therefore, for all $1 \leq j \leq n$,

$$\begin{aligned} \sum_{i=1}^n a_{ij} - c_j \|l\|_1 &\leq \eta \\ \Rightarrow \quad c_j \|l\|_1 &\geq \sum_{i=1}^n a_{ij} - \eta \end{aligned}$$

From the definition of $\text{supp}(c)$, it follows immediately that:

$$\|l\|_1 \geq \max_{j \in \text{supp(c)}} \left(\frac{\sum_{i=1}^n a_{ij} - \eta}{c_j} \right) = M(\eta)$$

□

Remark: The last result gives us a lower bound for $\|l\|_1$ where l is in $\mathcal{F}(\eta)$ and $\eta \in [\eta_{min}, \eta_{max}]$. We next show that this lower bound is in fact a minimum.

Proposition 5.3.4. *Let* $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n \setminus \{0\}$ *be given. Assume that* $\eta_{min} < \eta_{max}$. *For any* $\eta \in [\eta_{min}, \eta_{max}]$ *let* $M(\eta)$ *be given by* (5.21). *Then:*

$$\min\{\|l\|_1 : l \in \mathcal{F}(\eta)\} = M(\eta).$$

Proof: From Lemma 5.3.3, it is enough to show that there exists $l \in \mathcal{F}(\eta)$ with $\|l\|_1 = M(\eta)$. As $\eta_{min} < \eta_{max}$, it follows that there exists $l \in \mathcal{F}(\eta)$ such that $\|l\|_1 > 0$; choose such an l.

As $\|A - lc^T\|_1 = \eta$, for all $j \in \{1, \ldots, n\}$, we have that $\sum_{i=1}^n a_{ij} - c_j \|l\|_1 \leq \eta$. Furthermore, as $A \geq 0$, $c \geq 0, l \geq 0$, it follows that

$$\{j : \sum_{i=1}^n a_{ij} > \eta\} \subseteq \text{supp}(c)$$

Hence for all $j \notin \text{supp}(c)$, $\sum_{i=1}^n a_{ij} \leq \eta$.

Define

$$l \;= \left(\frac{M(\eta)}{l \;_1}\right) l.$$

This is possible as we have chosen l with $l \;_1 > 0$. Moreover, as $\eta_{min} < \eta_{max}$, $M(\eta) \geq 0$ by Lemma 5.3.2 and $l \;_1 = M(\eta)$.

It remains to show that $l \quad F(\eta)$. By Lemma 5.3.3, $\frac{M(\eta)}{l \;_!} \leq 1$, thus $0 \leq l \;\leq l$ and $A - l\; c^T \geq A - lc^T \geq 0$. To finish we need to show that $A - l\; c^T \;_1 = \eta$.

First of all, note that for all $j \;/\; \mathrm{supp}(c)$,

$$\sum_{i=1}^{n} a_{ij} - c_j \; l \;_1 = \sum_{i=1}^{n} a_{ij} \leq \eta$$

Next note that the definition of $M(\eta)$ implies that:

1. $M(\eta) \geq \frac{\sum_{i=1}^{n} a_{ij} - \eta}{c_j}$ for all $j \quad \mathrm{supp}(c)$;
2. $M(\eta) = \frac{\sum_{i=1}^{n} a_{ij} - \eta}{c_j}$ for some $j_0 \quad \mathrm{supp}(c)$.

As $l \;_1 = M(\eta)$, it follows that for all $j \quad \mathrm{supp}(c)$,

$$\sum_{i=1}^{n} a_{ij} - c_j \; l \;_1 \leq \eta$$

while for j_0,

$$A - l\; c^T \;_1 = \sum_{i=1}^{n} a_{ij} - c_j \; l \;_1 = \eta.$$

Thus $l \quad F(\eta)$ and $l \;_1 = M(\eta)$. This completes the proof. □

Remark: It is now straightforward to apply Proposition 5.3.4 to answer Problem 5.3.1. With the application to differential privacy in mind, we make the assumption that $\eta_{min} < 1$ (in order to ensure the bound in Proposition 5.1.2 is valid). The next result follows immediately from the definition of Φ in (5.5) and the set $F(\eta)$.

Corollary 5.3.5. *Let $A \quad \mathbb{R}_+^{n \times n}$, $c \quad \mathbb{R}_+^n \; \{0\}$ be such that $\eta_{min} < \eta_{max}$ and $\eta_{min} < 1$. Set $\eta_1 = \min\{\eta_{max}, 1\}$. Let $\eta \quad [\eta_{min}, \eta_1)$ be given. Then*

$$\min_{l \;\; F(\eta)} \Phi(l) = \left(\frac{M(\eta)}{1 - \eta}\right). \tag{5.22}$$

Remark: In the corollary, if $\eta_{max} < 1$ we can include the right endpoint η_1 (we can allow $\eta \in [\eta_{min}, \eta_{max}]$) but this makes no significant difference to the argument or conclusion.

5.3.1 Implications for globally optimising the sensitivity bound

The last thing we do in this section is to show how to apply Corollary 5.3.5 to the problem of finding a global minimum of Φ over l in $\mathsf{F}_{A,c}$.

Proposition 5.3.6. *Let $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n \setminus \{0\}$ be given. Assume that $\eta_{min} < \eta_{max}$ and $\eta_{min} < 1$. If $\sum_{i=1}^n a_{ij} \geq 1$ for all $j \in supp(c)$, then the infimum of $\Phi(l)$ for l in $\mathsf{F}_{A,c}$ is $\frac{M(\eta_{min})}{1-\eta_{min}}$.*

Proof: Set $\eta_1 = \min\{\eta_{max}, 1\}$. For a given $\eta \in [\eta_{min}, \eta_1)$ (as above, if $\eta_1 < 1$ we can include the right endpoint here but it makes no material difference to the argument or conclusions), let

$$\frac{M(\eta)}{1-\eta} = \max_{j \in \text{supp(c)}} \phi_j(\eta)$$

$$\text{with } \phi_j(\eta) = \left(\frac{\sum_{i=1}^n a_{ij} - \eta}{c_j}\right)\frac{1}{1-\eta}.$$

For each $j \in \text{supp}(c)$, as $\sum_{i=1}^n a_{ij} \geq 1$, it can be easily verified by differentiation that each ϕ_j is a non-decreasing function for all $\eta \in [\eta_{min}, \eta_1)$. Hence, $M(\eta)$ is a non-decreasing function and

$$\frac{M(\eta_{min})}{1-\eta_{min}} \leq \frac{M(\eta)}{1-\eta}$$

for all $\eta \in [\eta_{min}, \eta_1)$. The result now follows from Corollary 5.3.5. □

Finally for this section, we prove a simple result for the case where the non-zero entries of c are all equal.

Proposition 5.3.7. *Let $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n \setminus \{0\}$ be given. Assume that $\eta_{min} < \eta_{max}$ and $\eta_{min} < 1$. Suppose that there is some real number $\lambda > 0$ such that $c_j = \lambda$ for all $j \in supp(c)$. If $\max_{j \in supp(c)} \sum_{i=1}^n a_{ij} > 1$, then the infimum of $\Phi(l)$ for l in $\mathsf{F}_{A,c}$ is $\frac{M(\eta_{min})}{1-\eta_{min}}$.*

Proof: Again, set $\eta_1 = \min\{1, \eta_{max}\}$. For a given $\eta \quad [\eta_{min}, \eta_1)$, if $c_j = \lambda$ for all $j \quad \text{supp}(c)$

$$\begin{aligned}\frac{M(\eta)}{1-\eta} &= \frac{\max_{j \ \text{supp(c)}} \left(\frac{\sum_{i=1}^{n} a_{ij} - \eta}{c_j} \right)}{1-\eta} \\ &= \frac{\max_{j \ \text{supp(c)}} \left(\frac{\sum_{i=1}^{n} a_{ij} - \eta}{\lambda} \right)}{1-\eta} \\ &= \frac{\max_{j \ \text{supp(c)}} \left(\sum_{i=1}^{n} a_{ij} - \eta \right)}{\lambda(1-\eta)} \\ &= \frac{\max_{j \ \text{supp(c)}} \left(\sum_{i=1}^{n} a_{ij} \right) - \eta}{\lambda(1-\eta)}\end{aligned}$$

If $\max_{j \ \text{supp(c)}} \sum_{i=1}^{n} a_{ij} > 1$, then $\frac{M(\eta)}{1-\eta}$ is an increasing function for all η in $[\eta_{min}, \eta_1)$. The result follows immediately. □

5.4 The l_1 sensitivity of positive observers with coordinate transformation

In [11] and [10], a more general form of positive observer was studied for continuous time systems. The goal was to obtain less conservative conditions for a positive observer by allowing suitable coordinate transformations. We now outline the construction of these papers for the discrete time systems considered here. given by:

$$\begin{aligned} z(t+1) &= Fz(t) + Gy(t) \\ \hat{x}(t) &= T^{-1}z(t). \end{aligned} \tag{5.23}$$

In order for this to define a positive observer for (5.1), the following conditions are sufficient.

- $F \geq 0$, $\rho(F) < 1$;
- $TA - FT = GC$;
- T is inverse positive, meaning $T^{-1} \geq 0$.

In this section, we first derive an upper bound for the l_1 sensitivity of an observer of the form (5.23); as for the Luenberger observer (5.2), we require

that $\|F\| < 1$ in order to ensure that the sensitivity bound is finite. In the next result, we do not require the observer to be positive. The calculation needed to establish the bound below is a direct generalisation of that previously derived in Chapter 4 for the more restricted observer (5.2).

Proposition 5.4.1. *Consider the observer given by (5.23) with* $\|F\|_1 < 1$. *Let* $K > 0$, $0 < \alpha < 1$ *be given. The sensitivity* Δ *of (5.23) with respect to the similarity relation (5.3) satisfies the following bound:*

$$\Delta \leq \frac{K}{1-\alpha}\left(\frac{\|T^{-1}\|_1 \|G\|_1}{1-\|F\|_1}.\right) \tag{5.24}$$

Proof: Let two adjacent output signals y y satisfying (5.3) be given. Denote by z, z and $\hat{x}, \hat{x}$ the state and outputs from the observer (5.23) corresponding to y, y respectively (we assume the same initial conditions for the observer so $z(0) = z(0)$). A direct computation of the system response shows that for $t > 0$:

$$\begin{aligned} z(t) &= F^t z(0) + \sum_{j=0}^{t-1} F^{t-1-j} G y(j) \\ z(t) &= F^t z(0) + \sum_{j=0}^{t-1} F^{t-1-j} G y(j). \end{aligned}$$

It is immediate that $z(t) = z(t)$, $\hat{x}(t) = \hat{x}(t)$ for $0 \leq t \leq t_0$. For $t \geq t_0 + 1$ we have that

$$z(t) - z(t) = \sum_{j=t_0}^{t-1} F^{t-1-j} G(y(j) - y(j)).$$

This implies that the l_1 norm of $\hat{x}(t) - \hat{x}(t)$ satisfies

$$\begin{aligned} \|\hat{x}(t) - \hat{x}(t)\| &\leq \|T^{-1}\| \sum_{j=t_0}^{t-1} \|F\|^{t-1-j} \|G\| \|y(j) - y(j)\| \\ &\leq K \|T^{-1}\| \|G\| \sum_{j=t_0}^{t-1} \|F\|^{t-1-j} \alpha^{j-t_0}. \end{aligned} \tag{5.25}$$

Making the simple change of index variable $i = j - t_0$ gives:

$$\|\hat{x}(t) - \hat{x}(t)\| \leq K \|T\|^{-1} \|G\| \sum_{i=0}^{t-t_0-1} \|F\|^{t-i-t_0-1} \alpha^i.$$

This implies that the l_1 norm of $\hat{x} - \hat{x}$ satisfies:

$$\hat{x} - \hat{x} \quad \leq K \ T^{-1} \quad G \sum_{t=t_0+1}^{\infty} \sum_{i=0}^{t-(t_0+1)} \quad F \ ^{t-i-(t_0+1)} \alpha^i.$$

Another simple change of variable, $s = t - (t_0 + 1)$, shows that

$$\hat{x} - \hat{x} \quad \leq K \ T^{-1} \quad G \sum_{s=0}^{\infty} \sum_{i=0}^{s} \quad F \ ^{s-i} \alpha^i.$$

Keeping in mind that $0 < \alpha < 1$, $0 < \quad F \quad < 1$ by assumption, we can now conclude that:

$$\hat{x} - \hat{x} \quad \leq K \ T^{-1} \quad G \ \left(\frac{1}{1 - \alpha} \right) \left(\frac{1}{1 - \quad F} \right).$$

As $y \quad y$ were arbitrary, this completes the proof. □

Remark: As a classical Luenberger observer (5.2) corresponds to the choice $T = I$, $F = A - LC$, $G = L$, Proposition 5.1.2 can be derived as a corollary of Proposition 5.4.1.

5.4.1 Positive observers defined by the Sylvester equation

In this section we consider the general type of observer (5.23) where the original system is a single-output compartmental system. This means that an observer is defined by a triple (F, T, g) in $\mathbb{R}_+^{n \times n} \times \mathbb{R}^{n \times n} \times \mathbb{R}_+^n$ satisfying:

$$F \ _1 < 1; \quad T^{-1} \geq 0; \quad TA - FT = gc^T. \tag{5.26}$$

The bound for the sensitivity of the associated observer is then given by (5.24). The following question arises naturally in this context. Is it possible to construct observers of this more general form such that the value of the bound $\frac{T^{-1} \ _1 \ g \ _1}{1 - \ F \ _1}$ is less than the minimum given by Theorem 5.2.2 for the classical observer? If so, this would make it possible to achieve the same level of differential privacy by adding less noise for observers of this class.

As a guide to answering this question, we next present a simple, and rather crude, lower bound for $\frac{T^{-1} \ _1 \ g \ _1}{1 - \ F \ _1}$ where T, g, F define a positive observer. Here $\cdot \ _\infty$ is the usual l_∞ norm on $\mathbb{R}^n$.

Lemma 5.4.2. *Let* $A \in \mathbb{R}_+^{n\times n}$ *be compartmental with* $\|A\|_1 = 1$, *and* $c \in \mathbb{R}_+^n \setminus \{0\}$. *Moreover, suppose that* $F \geq 0$, $\|F\|_1 < 1$, $T \in \mathbb{R}_+^{n\times n}$ *is inverse positive,* $g \geq 0$, *and* $TA - FT = gc^T$. *Then*

$$\frac{\|T^{-1}\|_1 \|g\|_1}{1 - \|F\|_1} \geq \frac{1}{\|c\|_\infty}\left(\frac{1 - \|T^{-1}FT\|_1}{1 - \|F\|_1}\right).$$

Proof: As $TA - FT = gc^T$ and T is invertible,

$$A - T^{-1}FT = T^{-1}gc^T.$$

It follows immediately that

$$\begin{aligned} \|T^{-1}gc^T\|_1 &= \|A - T^{-1}FT\|_1 \\ &\geq \|A\|_1 - \|T^{-1}FT\|_1 \\ &= 1 - \|T^{-1}FT\|_1. \end{aligned}$$

The result now follows by noting that $\|T^{-1}gc^T\|_1 \leq \|T^{-1}\|\|g\|\|c\|_\infty$, and dividing across by $1 - \|F\|_1$. $\square$

Remark: The crude lower bound in the last result suggests that in cases where the maximal component of c, $\|c\|_\infty$ is significantly larger than $\min_{j\in J} c_j$, it may be possible to construct observers where $\frac{\|T^{-1}\|_1\|g\|_1}{1-\|F\|_1}$ is less than the minimum possible via a classical observer. The next example shows that this is indeed possible.

Example 5.4.1. Consider:

$$A = \begin{pmatrix} 1/2 & 1/4 \\ 1/2 & 1/3 \end{pmatrix}, \quad c^T = \begin{pmatrix} 1/3 & 1/2 \end{pmatrix}.$$

Next choose:

$$T = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, F = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/30 \end{pmatrix}$$

and $g^T = (1/2\ 1/10)$. Then it is readily verified that

- $\frac{1}{\min_{j\in J} c_j} = 3$.
- $TA - FT = gc^T$.
- $T^{-1} \geq 0$, $\|F\|_1 < 1$.

- $\frac{T^{-1}{}_{1}\ g_{1}}{1-F_{1}} = \frac{9}{5}$.

Remark: The key point of the last example is as follows. If we consider a classical positive observer and the upper bound on sensitivity given by Proposition 5.1.2, then the optimal gain matrix l will give a value of $\frac{3K}{1-\alpha}$ for the sensitivity bound. In contrast, by using the more general form of positive observer and the corresponding sensitivity bound given in Proposition 5.4.1, we have show that it is possible to construct an observer giving a value of $\frac{9K}{5(1-\alpha)}$ for the bound. This means that, by using the more general form of observer, we can achieve the same level of differential privacy via a Laplace mechanism whose variance is only 0.6 that required by the optimal possible for a classical observer.

5.5 Conclusions

In this chapter, we looked at a number of questions related to the construction of differentially private positive observers. We first studied the problem of minimising the bound on l_1 sensitivity from Chapter 4 for compartmental systems. For this problem, we have proven two results, each of which provides a simple, usable expression for the minimum value of the bound. Both Theorems 5.2.2 and 5.2.3 are constructive and they describe how to select the optimal observer gain matrix.

In constructing an observer that is required to be differentially private, it is important to take both the sensitivity and convergence speed into account. The work of Section 5.3 presents initial results on how these two objective functions interact for the case of single-output systems. Two simple results are also derived to show how understanding this trade-off can help find solutions to the global optimisation problem. In Section 5.4, we considered the l_1 sensitivity of the more general class of positive observers introduced in [10]. We derived a natural generalisation of the bound of the l_1 sensitivity from Chapter 4 to this class of observers in Proposition 5.4.1. Interestingly, Example 5.4.1 shows that we can build differentially private observers while adding less noise if we work with the more general type of observer.

CHAPTER 6

Positive Observers, Gaussian Mechanisms and l_2 Sensitivity

In this chapter, we consider the use of the Gaussian mechanism for di erentially private Luenberger observers for positive linear systems. In particular, we derive a bound for the l_2 sensitivity of Luenberger observers, which is used to quantify the noise required to achieve relaxed, (ε, δ) di erential privacy via the Gaussian mechanism. An approach to minimise this bound for positive observers is described and several bounds relevant to this problem are derived.

6.1 Introduction

In Chapter 4, our focus was on Laplace mechanisms to achieve ε differential privacy. For the Laplace mechanism, the l_1 sensitivity is the key parameter needed to determine the magnitude of noise needed for ε differential privacy. Our work in Chapter 4 and Chapter 5 focused on various questions about an upper bound for the l_1 sensitivity of positive linear observers. In this chapter, we will consider the relaxed form of differential privacy, (ε, δ) differential privacy. The most popular method for this is the Gaussian mechanism and the key parameter needed is the l_2 sensitivity of the observer.

As we have done in Chapter 4, we will calculate an upper bound for the l_2 sensitivity of a positive linear observer. When designing an observer for a positive linear system, we wish to find a gain matrix L that will minimise this sensitivity bound so that we add as little noise as possible. With this in mind

we develop an algorithm to find a matrix L that minimises the sensitivity bound and satisfies the constraints for a positive linear observer detailed in Chapter 2.

6.2 Differential Privacy and Systems Theory

As in Chapter 4, we consider Luenberger observers for linear systems, but with a view to the design of (ϵ, δ) differentially private observers, we shall derive a bound on the l_2 sensitivity of such observers.

As in previous chapter, we consider a system Σ of the form:

$$\begin{aligned} x(t+1) &= Ax(t) \\ y(t) &= Cx(t) \end{aligned} \tag{6.1}$$

where A $\mathbb{R}^{n\times n}$, C $\mathbb{R}^{p\times n}$. For a Luenberger observer, we need a matrix L $\mathbb{R}^{n\times p}$ such that the solution $\hat{x}(\cdot)$ of the system Σ_0 given by

$$\hat{x}(t+1) \;=\; (A - LC)\hat{x}(t) + Ly(t) \tag{6.2}$$

satisfies $\hat{x}(t) - x(t) \to 0$ as $k \to \infty$ where x is the solution to (6.1).

We work with the same definition of similarity on the space of output sequences $y(t)$, $t \geq 0$ that we have used in the last 2 chapters. So we assume $K > 0$ and $0 \leq \alpha < 1$ are given and say that two sequences y, y are adjacent, y y if they satisfy (2.24).

We will work exclusively with the l_2 norm and the corresponding induced norm for matrices in this chapter. These norms are the natural norms for use in connection with Gaussian mechanisms for differential privacy [72, 38].

Recall from Chapter 2, for M $\mathbb{R}^{m\times n}$, the l_2 induced (spectral) norm of M [59] is given by

$$\|M\|_2 = \sqrt{\rho(M^T M)}. \tag{6.3}$$

The l_2 norm of a sequence $y = (y(t))$, $0 \leq t < \infty$ with $y(t)$ $\mathbb{R}^p$ for all t is given by

$$\|y\|_2 = \sum_{t=0}^{\infty} \|y(t)\|_2 \tag{6.4}$$

where $\|y(t)\|_2$ is the usual l_2 norm in $\mathbb{R}^p$.

In some later sections, we will use the following result on the monotonicity of the spectral norm [59].

Lemma 6.2.1. *Let A, B in $\mathsf{R}_+^{m \times n}$ be given with $A \leq B$. Then $\|A\|_2 \leq \|B\|_2$.*

Relaxed Differentially Private Mechanisms

For the observer Σ_0, let $\mathcal{Y}, \hat{\mathcal{X}}$ denote the spaces of measured output sequences, $y(t)$, and observer state sequences, $\hat{x}(t)$, respectively. Given $\epsilon > 0$, $\delta > 0$, and the observer system Σ_0 in (6.1), an (ϵ, δ) differentially private mechanism is defined by specifying a set of random variables $\{\hat{X}_{\Sigma,y} \mid y \in \mathcal{Y}\}$ taking values in $\hat{\mathcal{X}}$ satisfying:

$$\mathsf{P}(\hat{X}_{\Sigma,y} \in A) \leq e^{\epsilon}\mathsf{P}(\hat{X}_{\Sigma,y'} \in A) + \delta \tag{6.5}$$

for all Borel sets A of $\hat{\mathcal{X}}$ and all $y \sim y'$.

To achieve (ϵ, δ)-differentially private mechanism we will add *iid* Gaussian noise to each component of the observer state [72]. As stated in Chapter 2, we need the Q-function defined as $Q(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{u^2}{2})du$. Now for $\epsilon > 0$, $0 \leq \delta \leq 0.5$, let $K = Q^{-1}(\delta)$ and define $\kappa_{\delta,\epsilon} = \frac{1}{2\epsilon}(K + \sqrt{K^2 + 2\epsilon})$. The mechanism $M(u) = \Sigma_0(y) + w$, where w_k is white Gaussian noise with covariance matrix $\kappa^2_{\delta,\epsilon}(\Delta_2(\Sigma_0))^2 I_p$, is (ϵ, δ)-differentially private.

The key quantity for us is the l_2 sensitivity $\Delta_2(\Sigma_0)$ which we have previously defined in Definition 2.4.1. Recall that:

$$\Delta_2(\Sigma_0) := \sup_{y \sim y'} \|\Sigma_0(y) - \Sigma_0(y')\|_2. \tag{6.6}$$

It is important to note that $\Delta_2(\Sigma_0)$ depends on both the norm and the adjacency relation. For the remainder of this chapter, we shall be interested in bounds for the l_2 sensitivity of observers for linear systems, with particular focus on positive linear systems.

6.3 Bounding the l_2 sensitivity for Luenberger observers

In this section, we first derive an upper bound of the l_2 sensitivity of the observer (6.2) without imposing positivity constraints. Later we shall present results on minimising this bound for positive observers.

Proposition 6.3.1. *Let* $A \quad \mathsf{R}^{n\times n}$, $C \quad \mathsf{R}^{p\times n}$, $L \quad \mathsf{R}^{n\times p}$ *be given and suppose that* $A - LC_{\ 2} < 1$. *Consider the Luenberger observer,* Σ_0 *given by* (6.2). *Then for the adjacency relation defined by* (2.24), *the* l_2 *sensitivity of* Σ_0 *(as given in (6.6)) is bounded by*

$$\Delta(\Sigma_0)^2 \leq \frac{K^2}{1-\alpha^2}\left(\frac{1+N\alpha}{1-N\alpha}\right)\left(\frac{L\ _2^2}{1-N^2}\right) \tag{6.7}$$

where $N = A - LC_{\ 2}$.

Proof: Let two adjacent sequences $y \quad y$ be given. The map from the sequence y to $\hat{x}$ and from y to $\hat{x}$ corresponding to (6.2), with the common initial observer state $\hat{x}_0$, is defined by

$$\hat{x}(t+1) = (A-LC)^{t+1}\hat{x}_0 + \sum_{i=0}^{t}(A-LC)^{t-i}Ly(i)$$

$$\hat{x}\,(t+1) = (A-LC)^{t+1}\hat{x}_0 + \sum_{i=0}^{t}(A-LC)^{t-i}Ly\,(i).$$

As $y \quad y$, it follows that $\hat{x}\,(t) = \hat{x}(t)$ for $t \leq t_0$. Moreover, for $t > t_0$, we have

$$\hat{x}(t) - \hat{x}\,(t) = \sum_{i=t_0}^{t-1}(A-LC)^{t-i-1}L(y(i) - y\,(i)). \tag{6.8}$$

We need to bound $\hat{x}(t) - \hat{x}\,(t)_{\ 2}$; for $t > t_0$. Using the triangle inequality and the submultiplicative property of the spectral norm, as done in Proposition 4.3.1 in Chapter 4, we have:

$$\begin{aligned}\hat{x}(t) - \hat{x}\,(t)_{\ 2} &= \sum_{i=t_0}^{t-1}(A-LC)^{t-i-1}L(y(i) - y\,(i))_{\ 2} \\ &\leq L_{\ 2}K\sum_{i=t_0}^{t-1} A - LC_{\ 2}^{\ t-1-i}\alpha^{i-t_0}\end{aligned}$$

To simplify the notation in the following calculations we write N for $A - LC_{\ 2}$. The l_2 norm of the sequence $\hat{x} - \hat{x}$ is given by (6.4) which applied to the above calculation shows that the square of this norm, $\hat{x} - \hat{x}\ _2^2$, is bounded above by:

$$L\ _2^2K^2\sum_{t=t_0+1}^{\infty}\left(\sum_{i=t_0}^{t-1}N^{t-1-i}\alpha^{i-t_0}\right)^2$$

A simple shift of indices shows that the series in the above expression is equal to:

$$\sum_{t=0}^{\infty}\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2} \tag{6.9}$$

In order to evaluate the above sum, we shall show that the series $\sum_{t=0}^{\infty}\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2}$ is equal to the following sum of two series:

$$\sum_{i=1}^{\infty} i\alpha^{i-1}\frac{N^{i-1}}{1-N^{2}} + \sum_{i=1}^{\infty} iN^{i-1}\frac{\alpha^{i+1}}{1-\alpha^{2}} \tag{6.10}$$

Intuitively, it is possible to see why this decomposition holds by examining the pattern of the terms $\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2}$ for $t = 0, 1, 2, 3, 4$.

$$1$$
$$N^2 + 2N\alpha + \alpha^2$$
$$N^4 + 2N^3\alpha + 3N^2\alpha^2 + 2N\alpha^3 + \alpha^4$$
$$N^6 + 2N^5\alpha + 3N^4\alpha^2 + 4N^3\alpha^3 + 3N^2\alpha^4 + 2N\alpha^5 + \alpha^6$$
$$N^8 + 2N^7\alpha + 3N^6\alpha^2 + 4N^5\alpha^3 + 5N^4\alpha^4 + 4N^3\alpha^5 + 3N^2\alpha^6 + 2N\alpha^7 + \alpha^8$$

To see why (6.10) holds, we need to make the following observations.

- The total power of each monomial term $N^p\alpha^q$ in $\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2}$ is $2t$. This implies that each monomial in (6.9) appears for exactly one value of t.
- Each term in $\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2}$ is of the form $N^{2t-(i+j)}\alpha^{i+j}$, where i, j $\{0, 1, \ldots, t\}$. We now have two cases:
  1. If $t - (i+j) > 0$, then let $p = 2t - (i+j)$ and $s = (i+j) - t$, where $s > 0$. This implies $N^{2t-(i+j)}\alpha^{i+j} = N^p\alpha^{p+2s}$.
  2. If $t - (i+j) \leq 0$, let $p = i + j$ and $s = t - (i+j)$, where $s \geq 0$. This implies $N^{2t-(i+j)}\alpha^{i+j} = N^{p+2s}\alpha^p$.

  Hence, each term in (6.9) is either of the form $N^p\alpha^{p+2s}$ for some integers $p \geq 0$, $s > 0$ or of the form $\alpha^p N^{p+2s}$ for integers $p \geq 0$, $s \geq 0$.
- The coefficient of the monomial $N^p\alpha^q$ in $\left(\sum_{i=0}^{t} N^{t-i}\alpha^{i}\right)^{2}$, also comes down to two cases:

1. If $\min\{p, q\} = q$, then $q \leq t$ and the term $N^p\alpha^q$ occurs as the product $(N^{t-i}\alpha^i)(N^{t-(q-i)}\alpha^{q-i})$, for $i = 0, 1, \ldots, q$. So its coefficient is $q + 1$.
2. Similarly, if $\min\{p, q\} = p$, then $p \leq t$ and $N^p\alpha^q = (N^i\alpha^{t-i})(N^{p-i}\alpha^{t-(p-i)})$, for $i = 0, 1, \ldots, p$. So this time, its coefficient is $p + 1$.

Hence, The coefficient of the monomial $N^p\alpha^q$ is given by $\min\{p, q\} + 1$.

From the above observations, it follows that we can split the terms in (6.9) into those of the form $i(\alpha^{i-1}N^{(i-1)+2s})$ for $1 \leq i < \infty$, $s \geq 0$ and those of the form $i(N^{i-1}\alpha^{(i-1)+2s})$ for $1 \leq i < \infty$, $s > 0$. The equality of (6.9) and (6.10) now follows from the above points as we can write:

$$\begin{aligned}
&\sum_{t=0}^{\infty}\left(\sum_{i=0}^{t} N^{t-i}\alpha^i\right)^2 \\
=\ &\sum_{i=1}^{\infty}\left(\sum_{s=0}^{\infty} i(\alpha^{i-1}N^{(i-1)+2s})\right) + \sum_{i=1}^{\infty}\left(\sum_{s=1}^{\infty} i(N^{i-1}\alpha^{(i-1)+2s})\right) \\
=\ &\sum_{i=1}^{\infty} i\alpha^{i-1}\frac{N^{i-1}}{1-N^2} + \sum_{i=1}^{\infty} iN^{i-1}\frac{\alpha^{i+1}}{1-\alpha^2}.
\end{aligned}$$

The series (6.10) can now be rearranged as follows:

$$\begin{aligned}
&\sum_{i=1}^{\infty} i\alpha^{i-1}\frac{N^{i-1}}{1-N^2} + \sum_{i=1}^{\infty} iN^{i-1}\frac{\alpha^{i+1}}{1-\alpha^2} \\
=\ &\frac{1}{1-N^2}\sum_{i=1}^{\infty} i\alpha^{i-1}N^{i-1} + \frac{\alpha^2}{1-\alpha^2}\sum_{i=1}^{\infty} iN^{i-1}\alpha^{i-1} \\
=\ &\left(\frac{1}{1-N^2} + \frac{\alpha^2}{1-\alpha^2}\right)\sum_{i=1}^{\infty} i(N\alpha)^{i-1} \\
=\ &\left(\frac{1}{1-N^2} + \frac{\alpha^2}{1-\alpha^2}\right)\sum_{i=1}^{\infty} i\beta^{i-1}
\end{aligned}$$

where $\beta = N\alpha < 1$. To evaluate $\sum_{i=1}^{\infty} i\beta^{i-1}$, we simply note that it is the derivative of the absolutely convergent (for $|\beta| < 1$) power series $\sum_{i=0}^{\infty} \beta^i$ and

thus

$$\begin{aligned}\sum_{i=1}^{\infty} i\beta^{i-1} &= \frac{d}{d\beta}\left(\sum_{i=0}^{\infty}\beta^i\right)\\ &= \frac{d}{d\beta}\left(\frac{1}{1-\beta}\right)\\ &= \frac{1}{(1-\beta)^2}\\ &= \frac{1}{(1-N\alpha)^2}.\end{aligned}$$

Therefore, we may write

$$\begin{aligned}\sum_{t=0}^{\infty}\left(\sum_{i=0}^{t} N^{t-i}\alpha^i\right)^2 &= \left(\frac{1}{1-N^2}+\frac{\alpha^2}{1-\alpha^2}\right)\sum_{i=1}^{\infty} i\beta^{i-1}\\ &= \left(\frac{1}{1-N^2}+\frac{\alpha^2}{1-\alpha^2}\right)\frac{1}{(1-N\alpha)^2}\\ &= \frac{1}{(1-N\alpha)^2}\left(\frac{1-N^2\alpha^2}{(1-N^2)(1-\alpha^2)}\right)\\ &= \frac{1}{1-\alpha^2}\left(\frac{1+N\alpha}{1-N\alpha}\right)\left(\frac{1}{1-N^2}\right)\end{aligned}$$

Combining everything, the square of the l_2 norm of $\hat{x}-\hat{x}$ is bounded above by:

$$\frac{K^2}{1-\alpha^2}\left(\frac{1+N\alpha}{1-N\alpha}\right)\left(\frac{L\ _2^2}{1-N^2}\right)$$

which completes the proof as $y \quad y$ were arbitrary. □

Remark: Recall that the upper bound for the l_1 sensitivity of a Luenberger observer that we derived in Chapter 4 was given by:

$$\Delta_1(\Sigma_0) \leq \left(\frac{K}{1-\alpha}\right)\left(\frac{L\ _1}{1-\ A-LC\ _1}\right), \tag{6.11}$$

where the induced matrix norms are with respect to the l_1 vector norm. This bound has a simpler form than our l_2 bound in Proposition 6.3.1 as we are able to isolate K and α. For this reason, when we were trying to minimise the l_1 bound, we only had to consider the function

$$\frac{L\ _1}{1-\ A-LC\ _1}.$$

The parameter α cannot be separated in this way for the l_2 bound.

6.3.1 Tightness of upper bound

As we did for the l_1 bound, we now describe a simple example to illustrate how the bound in Proposition 6.3.1 can be attained for certain matrices A, L, C. The matrices used in the following example are all nonnegative.

Example 6.3.1. Consider

$$A = \begin{pmatrix} 1/4 & 1/2 \\ 1/2 & 1 \end{pmatrix}, \; C = \begin{pmatrix} 1/3 & 2/3 \end{pmatrix}, \; L = \begin{pmatrix} 1/3 \\ 2/3 \end{pmatrix}.$$

A straightforward calculation shows that

$$A - LC = \begin{pmatrix} 5/36 & 5/18 \\ 5/18 & 5/9 \end{pmatrix}.$$

Direct calculation shows that $\|A - LC\|_2 = 25/36 < 1$. Moreover, we can verify that

$$(A - LC)L = (25/36)L = \|A - LC\|_2^2 L$$

so that $(A - LC)^i L = (\|A - LC\|_2^2)^i L$ for all $i \geq 1$. Now pick a pair of adjacent sequences y, y' where $y(t), y'(t)$ are in R for all t, satisfy the adjacency relation $y \sim y'$ (2.24) but with equality in place of the inequality. As each $y(t)$ is a real number, this can be done. For such a pair, the corresponding observer outputs $\hat{x}, \hat{x}'$ satisfy

$$\|\hat{x} - \hat{x}'\|_2^2 = \frac{K^2}{1 - \alpha^2} \left(\frac{1 + N\alpha}{1 - N\alpha}\right) \left(\frac{\|L\|_2^2}{1 - N^2}\right)$$

6.4 Observer design and sensitivity bounds

Now, we will look at the question of positive observer design [5, 52, 10] and the problem of minimising the bound for l_2 sensitivity presented in Proposition 6.3.1 when a positive observer is required.

The system (6.1) is positive if A and C are nonnegative. Recall from Theorem 2.3.4 in Chapter 2 [5] that the existence of a positive observer is equivalent to the existence of a matrix L such that $A - LC \geq 0$, $LC \geq 0$ and $\rho(A - LC) < 1$. As our interest is in the bound on the l_2 sensitivity of such an observer, we shall replace the requirement that $\rho(A - LC) < 1$ with $\|A - LC\|_2 < 1$. Without making this assumption, the observer need not have finite l_2 sensitivity and our bound is not valid.

6.4.1 Minimising the sensitivity bound

First, consider the question of characterising the infimal or minimal value of the bound in Proposition 6.3.1 and of determining an observer matrix L that either attains or approximates this value.

As K and α are fixed parameters determined by the adjacency (2.24) we address the following problem:

Problem 6.4.1. *Given* $A \in \mathbb{R}_+^{n\times n}$, $C \in \mathbb{R}_+^{p\times n}$, *consider*

$$F(L) = \|L\|_2 \left(\frac{1+\|A-LC\|_\alpha}{1-\|A-LC\|_\alpha}\right)\left(\frac{1}{1-\|A-LC\|_2}\right). \tag{6.12}$$

Determine $\inf F(L)$ *subject to the constraints:*

$$LC \geq 0,\ A-LC \geq 0, \quad \|A-LC\|_2 < 1 \tag{6.13}$$

For the rest of this chapter, we avoid the question of feasibility and assume throughout that the set defined by (6.13) is non-empty: in the case where it is empty, most statements are satisfied vacuously (or by adopting the convention that the infimum of an empty set is ∞).

In this section, we shall present results that can be used to develop methods to minimise $F(L)$ subject to (6.13). A major contribution is to show how to reduce this question to a simple 1-dimensional question via a family of optimisation problems with a convex objective function.

The next lemma show that in the case where $\|A\|_2 > 1$, the infimum above is in fact a minimum that is attained for some L in the feasible set.

Lemma 6.4.1. *Let* $A \in \mathbb{R}_+^{n\times n}$, $C \in \mathbb{R}_+^{p\times n}$ *be given with* $\|A\|_2 > 1$ *and assume that there is some* L *satisfying* (6.13). *Then there exists some* κ *with* $0 < \kappa < 1$ *such that* $\inf F(L)$ *subject to* (6.13) *is given by* $\min F(L)$ *subject to*

$$LC \geq 0,\ A-LC \geq 0, \quad \|A-LC\|_2 \leq \kappa \tag{6.14}$$

Proof: We first note that for any κ with $0 < \kappa < 1$, F is a well-defined continuous function on the compact set given by (6.14) and hence attains its minimum on this set.

As $\|A\|_2 > 1$, it follows that there must exist some $\epsilon > 0$ such that for any L such that $\|A - LC\|_2 < 1$, we have $\|L\|_2 \geq \epsilon$. It follows readily that for any L satisfying (6.13), we must have

$$F(L) \geq \frac{\epsilon^2}{1 - \|A - LC\|_2^2}.$$

Now choose some L_1 satisfying (6.13) and suppose $F(L_1) = f_1^2$. If $f_1 = 0$, then clearly F attains its minimum at L_1 and the result follows. Otherwise, set $\epsilon_1 = \min\{\epsilon, \frac{f_1}{2}\}$. Then a simple calculation shows that for any L satisfying (6.13) with $\|A - LC\|_2 > 1 - \frac{\epsilon_1}{f_1}$, we must have $F(L) > f_1$. The result now follows with $\kappa = 1 - \frac{\epsilon_1}{f_1}$. □

For the remainder of the chapter, we assume that $\|A\|_2 > 1$. The case where $\|A\|_2 < 1$ is trivial as we can simply take $L = 0$ to minimise the function $F(L)$; the boundary situation where $\|A\|_2 = 1$ may be more subtle however and we will not consider it here.

To present our next results, we will write $F(L) = \|L\|_2^2 H(\|A - LC\|_2)$, where the function $H : [0, 1) \to \mathbb{R}$ is given by

$$H(N) = \left(\frac{1 + N\alpha}{1 - N\alpha}\right)\left(\frac{1}{1 - N^2}\right) \tag{6.15}$$

The next lemma will be important in our approach to solving Problem 6.4.1.

Lemma 6.4.2. *The function H defined by (6.15) is an increasing function on the interval $[0, 1)$.*

Proof: The first derivative of H is given by:

$$\begin{aligned} H'(N) &= \left(\frac{1}{1 - N^2}\right)\left(\frac{(1 + N\alpha)\alpha}{(1 - N\alpha)^2} + \frac{\alpha}{1 - N\alpha}\right) \\ &+ \left(\frac{1 + N\alpha}{1 - N\alpha}\right)\left(\frac{2N}{(1 - N^2)^2}\right) \end{aligned}$$

As α is a fixed value with $0 \leq \alpha \leq 1$ we can see that $H'(N) > 0$ for N in the interval $[0, 1)$. □

6.4.1.1 Algorithm

In this subsection, we will describe the key steps of an algorithm for solving problem 6.4.1.

1. *Determine upper and lower bounds, ζ_{min}, ζ_{max} for $\|L\|_2$ for L satisfying (6.13).*

   - We only want to be sure that $\|L\|_2$ lies between the bounds for this step (we are not requiring that they be tight). For any system, we can clearly take 0 as a lower bound. However, we shall shortly describe how to obtain a less conservative lower bound than this.
   - For a single output system ($p = 1$), an upper bound can be calculated as follows. $L \in \mathbb{R}_+^{n\times 1}$ so we can consider L as a column vector $l \in \mathbb{R}_+^n$; similarly we can take C to be given by a row vector c^T for $c \in \mathbb{R}_+^n$. Since $A - lc^T \geq 0$, $l_i \leq \frac{a_{ij}}{c_j} \quad \forall j \in \mathrm{supp}(c)$ $\Rightarrow$ $l_i \leq \min_{j \in \mathrm{supp}(c)} \frac{a_{ij}}{c_j}$, for $1 \leq i \leq n$. This gives an upper bound on the l_2 norm of L: namely

   $$\|L\|_2 \leq \sqrt{\sum_i \left(\min_{j \in \mathrm{supp}(c)} \frac{a_{ij}}{c_j} \right)^2} = \zeta_{max}.$$

   Later we shall describe how to calculate an upper bound for general multiple output systems.

2. *For $\zeta \in [\zeta_{min}, \zeta_{max}]$ solve the optimisation problem $M(\zeta) = \min H(N(L))$ such that $\|L\|_2 = \zeta$.*

   - As H is an increasing function of N, this is equivalent to solving the simpler problem of determining for each $\zeta \in [\zeta_{min}, \zeta_{max}]$:

   $$N(\zeta) = \min_{\|L\|_2 = \zeta} \|A - LC\|_2 \tag{6.16}$$

   subject to L satisfying (6.13).
   - This problem may be solved for each ζ using optimisation packages based on techniques such as sequential quadratic programming (SQP). We shall show below that for the single output case, this step is in fact a convex problem.

3. Finally solve $\min \zeta^2 M(\zeta)$ for $\zeta \in [\zeta_{min}, \zeta_{max}]$.

   - This is a simple single variable optimisation problem so we have reduced the original multivariable, non-convex problem to optimising a single variable function in a closed interval.

6.4.2 Bounding $\|L\|_2$

Now consider the problem of determining lower and upper bounds for $\|L\|_2$ where L satisfies (6.13) and the matrix C has *full rank* p (we make the reasonable assumption that $p \leq n$).

Proposition 6.4.3. *Let $A \in \mathbb{R}_+^{n\times n}$, $C \in \mathbb{R}_+^{p\times n}$ ($p \leq n$) be given and suppose that $L \in \mathbb{R}^{n\times p}$ satisfies (6.13). Assume that C has rank p and let $C^\dagger$ be the pseudo-inverse of C satisfying $CC^\dagger = I_p$ where I_p is the $p \times p$ identity matrix. Then*

$$\frac{\|A\|_2 - 1}{\|C\|_2} \leq \|L\|_2 \leq \|A\|_2 \, \|C^\dagger\|_2 \tag{6.17}$$

where $C^\dagger$ is the pseudo-inverse of C.

Proof: As $p \leq n$ and we are assuming that C has rank p, it follows easily from considering the singular value decomposition of C that the pseudo-inverse $C^\dagger$ of C exists satisfying $CC^\dagger = I_p$ where I_p is the $p \times p$ identity matrix. From this, the upper bound above follows readily as

$$\begin{aligned} \|L\|_2 &= \|LCC^\dagger\|_2 \\ &\leq \|LC\|_2 \, \|C^\dagger\|_2 \\ &\leq \|A\|_2 \, \|C^\dagger\|_2 \end{aligned}$$

where the last inequality follows as $0 \leq LC \leq A$ and the monotonicity of the spectral norm on nonnegative matrices.

For the lower bound, note that

$$\|A\|_2 - \|LC\|_2 \leq \|A - LC\|_2 < 1$$

which implies that

$$\|L\|_2 \, \|C\|_2 \geq \|LC\|_2 > \|A\|_2 - 1.$$

The lower bound now follows immediately. □

6.4.3 The single output case $p = 1$

In this subsection, we show that when dealing with a single output system, $p = 1$, step 2 of our algorithm for minimising $F(L)$ is equivalent to a convex problem.

Lemma 6.4.4. *Let* $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^p$ *and* $\zeta > 0$ *be given where* $\zeta < \zeta_{\max}$. *Define:*

$$\begin{aligned} m_1 &:= \min\{ \|A - lc^T\|_2 : l \geq 0, A - lc^T \geq 0, \ \|l\|_2 = \zeta\}; \\ m_2 &:= \min\{ \|A - lc^T\|_2 : l \geq 0, A - lc^T \geq 0, \ \|l\|_2 \leq \zeta\}. \end{aligned}$$

Then $m_1 = m_2$.

Proof: It suffices to show that for any l such that $lc^T \geq 0$, $A - lc^T \geq 0$ and $\|l\|_2 \leq \zeta$, there exists some l_1 with $l_1c^T \geq 0$, $A - l_1c^T \geq 0$ and $\|l_1\|_2 = \zeta$ such that

$$\|A - l_1c^T\|_2 \leq \|A - lc^T\|_2.$$

To this end, let such an l be given. Take $\hat{l}$ to be the vector with $\hat{l}_i = \min_{j \in \text{supp}(c)} \frac{a_{ij}}{c_j}$ so that $l \leq \hat{l}$ for any l satisfying (6.13) and $\|\hat{l}\|_2 \geq \zeta$. It is not difficult to see that $\hat{l}$ lies in the convex feasible set F (assumed to be non-empty) determined by (6.13). For $\alpha \in [0,1]$ consider

$$\hat{l}(\alpha) = \alpha\hat{l} + (1 - \alpha)l.$$

As F is convex, $\hat{l}(\alpha)$ is in F for all $\alpha \in [0,1]$. Also, as $l \leq \hat{l}$, $\hat{l}(\alpha) \geq l$ for all $\alpha \in [0,1]$. Moreover, as $\|\hat{l}(0)\|_2 = \|l\|_2 < \zeta$ and $\|\hat{l}(1)\|_2 = \|\hat{l}\|_2 \geq \zeta$, it follows that for some α_1 we must have $\|\hat{l}(\alpha_1)\|_2 = \zeta$. The result follows setting $l_1 = \hat{l}(\alpha_1)$. $\square$

The equality of m_1 and m_2 established in the lemma shows that, when $p = 1$, in Step 2 of the algorithm in Section 6.4.1.1, we can replace the problem of determining the value of m_1 by the convex optimisation problem of determining m_2.

We now present a 2-dimensional example to illustrate how to use these ideas to minimise $F(L)$ given by (6.12) for a given A, C.

Example 6.4.1. Consider

$$A = \begin{pmatrix} 1/4 & 1/2 \\ 1/2 & 1 \end{pmatrix}, \ C = \begin{pmatrix} 1/3 & 2/3 \end{pmatrix}$$

with $\alpha = 0.2$ and $K = 0.5$.

To apply algorithm 6.4.1.1, we need to first determine values for ζ_{min} and ζ_{max}. As mentioned previously, we can always take $\zeta_{min} = 0$. Using Proposition

6.4.3, we calculate $\zeta_{max} = 1.6771$. Applying the algorithm gives us an observer gain matrix $L = [0.47692 \;\; 0.95385]^T$. The value of the l_2 sensitivity bound for this observer is 1.2958.

6.4.4 Convergence Vs Sensitivity Trade-off

Our approach to Problem 6.4.1 could also provide insight into the fundamental trade-off between utility and privacy, as considered in Chapter 5. Some of the results may help to clarify the relationship between the achievable sensitivity values and observer convergence rates quantified by the system norm $\|A - LC\|_2$.

In the design of differentially private observers there is a trade-off between the sensitivity bound described by the function $F(L)$ and the norm of $\|A - LC\|_2$ which determines the rate of convergence of the observer to the value of the state. As we have done in Chapter 5 for l_1 sensitivity of single output systems, it would be interesting to characterise the interplay between these two quantities for the l_2 case. The following two problems seem natural in this context.

- The construction of a positive observer with minimal sensitivity for a prescribed performance level, expressed in terms of the l_2 norm of $A - LC$.
- The construction of a positive observer with optimal convergence for a specified level of sensitivity.

Formally, the first of these questions amounts to determining the minimal value of $F(L)$ subject to $\|A - LC\|_2 = \eta$, $A - LC \geq 0$, $LC \geq 0$. It is trivial to see that once $\|A - LC\|_2 = \eta$, then

$$F(L) = \|L\|_2^2 \frac{1 + \alpha\eta}{1 - \alpha\eta} \frac{1}{1 - \eta^2}.$$

Thus the question of determining the minimum sensitivity amounts to finding L such that $\|L\|_2$ is minimal while $\|A - LC\|_2 = \eta$. This question is related to the second step in Algorithm 6.4.1.1.

Formally, the second question amounts to determining the minimum value of $\|A - LC\|_2$ subject to $F(L) = \eta$, $A - LC \geq 0$, $LC \geq 0$.

6.5 Conclusions

In this chapter, we first derived an upper bound for the l_2 sensitivity of a Luenberger observer for a linear system. We then considered the problem of minimising this bound for positive systems where we also require that the observer be positive. In particular, we have described an algorithm that reduces this problem to a single variable optimisation and have given upper and lower bounds for the variable in this simple problem. When the system has a single output, we show that the key step in the minimisation algorithm is a convex problem and have given simple bounds for this case also.

In Chapter 3, methods of ensuring that the output from a mechanism is positive were described. The technique of post-processing can be applied directly to Gaussian mechanisms, using the bounds for l_2 sensitivity derived in the current chapter. However, more work would be required in order to develop mechanisms based on restriction as the methods in Chapter 3 apply to the Laplace mechanism.

CHAPTER 7

A Brief Look at Opacity for Positive Systems

We present preliminary results on initial state opacity for positive linear systems. In particular, we consider the problem of initial state opacity when the secret and non-secret states are defined by convex cones in R^n_+*. A result characterising opacity in this situation is given; the proof relies on an application of Farkas' Lemma.*

7.1 Introduction

In the last 3 chapters, we have discussed results on differentially private positive observers for positive linear systems. We have mentioned in Chapter 2 that *opacity* is an alternative concept of privacy for dynamic systems. While differential privacy relies on methods from Probability Theory, the main versions of opacity are deterministic in nature. Recall that the idea behind opacity is to protect *private* information by making it difficult for an outside observer to determine a 'secret' of the system; in particular, observers should be unable to clearly distinguish secret executions from non-secret ones.

Our interest in this short chapter is in the problem of *initial state opacity* for a positive linear system. We shall make use of the recent formulation of this concept for general linear systems in [89, 90], which has been discussed in Chapter 2. We study opacity for a simple positive linear system with output; in contrast with the previous 3 chapters, we will not consider the design of positive observers here.

7.2 Opacity for Positive Linear Systems

Consider the positive linear system

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t), \end{aligned} \tag{7.1}$$

where $A \quad \mathsf{R}_+^{n\times n}$, $B \quad \mathsf{R}_+^{n\times m}$, $C \quad \mathsf{R}_+^{p\times n}$. As in previous chapters, our state space is R_+^n, our input space is R_+^m and our output space is R_+^p.

In keeping with the discussion in Chapter 2 and the papers [89, 90] we assume that two sets $X_s \quad \mathsf{R}_+^n$, $X_{ns} \quad \mathsf{R}_+^n$ of initial states are specified: X_s contains the *secret* initial states while X_{ns} contains the non-secret states. We also assume that some time τ is specified; this is the time at which the observer measures the output $y(\tau)$. We are interested in τ-step strong initial state opacity in the following sense.

For an initial state $x(0) = x_0$ and input sequence $u = (u(0), \ldots, u(\tau - 1))$, we denote the output of (7.1) at time τ by $y_{x_0,u}(\tau)$. The system (7.1) satisfies τ-step strong initial state opacity (τ-ISO) if for any $x_0 \quad X_s$ and any input sequence $u = (u(0), u(1), \ldots u(\tau - 1))$, there is some $x_0 \quad X_{ns}$ and $u = (u(0), u(1), \ldots, u(\tau - 1))$ such that

$$y_{x_0,u}(\tau) = y_{x_0,u}(\tau).$$

Informally, this definition means that the system makes sure that for any secret initial state and input sequence, there is some non-secret state and some input sequence which give rise to the same output value at time τ. In the paper [89], a condition for τ-ISO was formulated in terms of the reachability set of the system (7.1) at time τ. In the next section, we will present some initial results for positive systems that are in the same spirit. We impose some extra structure on the sets X_s and X_{ns} however.

7.3 Characterising Opacity for Conic Secret and Non-Secret Sets

For our results, we assume that both the set X_s of secret states, and the set X_{ns} of non-secret states are finitely generated convex cones in R_+^n [16]; this

means that they are the *conic hull* of finitely many points in R^n_+ [14]. We first recall the relevant definition.

Definition 7.3.1. The set $X \quad \mathsf{R}^n_+$ is the conic hull of the finite set $\{x_1, \ldots x_q\} \quad \mathsf{R}^n_+$ if:

$$X = \left\{ \sum_{i=1}^{q} \alpha_i x_i : \alpha_i \quad \mathsf{R}_+, 1 \leq i \leq q \right\}.$$

We say that a set is a finitely generated cone if it is the conic hull of a finite set of points. When X is the conic hull of $\{x_1, \ldots, x_q\}$, we write $X = co(\{x_1, \ldots, x_q\})$.

We assume from now on that there are two finite sets $\{x_1, \ldots, x_q\}$, $\{x_1, \ldots, x_r\}$ of points in R^n_+ such that

$$\begin{aligned} X_s &= co(\{x_1, \ldots, x_q\}) \\ X_{ns} &= co(\{x_1, \ldots, x_r\}) \end{aligned} \tag{7.2}$$

Furthermore, we assume that X_s and X_{ns} are disjoint; otherwise the problem of initial state opacity is not practical.

We first present a simple lemma that simplifies the condition for τ-ISO. Essentially, it allows us to focus on the case where the output from secret initial state is driven by the zero input sequence.

Lemma 7.3.1. *Consider the system (7.1) and let the set of secrets states, X_s, and the set of non-secret states, X_{ns} satisfy (7.2). Then (7.1) is τ-ISO with respect to X_s, X_{ns} if and only if for every $x_0 \quad X_s$, there is some x_s in X_{ns} and some sequence $u = (u(0), u(1), \ldots, u(\tau - 1))$ such that*

$$CA^\tau x_0 = y_{x_0,u}(\tau). \tag{7.3}$$

Proof: First suppose that (7.1) is τ-ISO with respect to X_s, X_{ns} and let $x_0 \quad X_s$ be given. Then for the input sequence $u = (0, 0, \ldots, 0)$, there is some x_s in X_{ns} and some sequence $u = (u(0), u(1), \ldots, u(\tau - 1))$ such that

$$y_{x_0,u}(\tau) = CA^\tau x_0 = y_{x_0,u}(\tau).$$

For the converse direction, let $x_0 \quad X_s$ and an input sequence $u = (u(0), u(1), \ldots, u(\tau - 1))$ be given. Let $x_0 \quad X_{ns}$ and the input sequence

$u = (u(0), \ldots u(\tau - 1))$ be such that

$$CA^{\tau}x_0 = y_{x_0,u}(\tau).$$

Then it is readily verified that

$$\begin{aligned} y_{x_0,u}(\tau) &= CA^{\tau}x_0 + \sum_{i=0}^{\tau-1} CA^{\tau-1-i}Bu(i) \\ &= y_{x_0,u}(\tau) + \sum_{i=0}^{\tau-1} CA^{\tau-1-i}Bu(i) \\ &= y_{x_0,u+u}(\tau). \end{aligned}$$

Thus the system (7.1) is τ-ISO. □

7.3.1 Opacity and Farkas' Lemma

Assume from now on that X_s and X_{ns} are given by (7.2) and that some time $\tau > 0$ is given. By Lemma 7.3.1, the system (7.1) is τ-ISO if and only if for every x_0 in X_s, there is some x_0 in X_{ns} and some sequence of nonnegative inputs $u(0), u(1), \ldots, u(\tau - 1)$ such that

$$CA^{\tau}x_0 = CA^{\tau}x_0 + \sum_{i=0}^{\tau-1} CA^{i}Bu(i).$$

In this subsection, we will make use of the conic structure of the sets X_s, X_{ns} to apply Farkas' Lemma and obtain a condition for (7.1) to be τ-ISO.

First note the following simple fact.

Lemma 7.3.2. *Let X_s, X_{ns} be given by (7.2) and let $\tau > 0$ be a positive integer. The system (7.1) is τ-ISO if and only if for every i, $1 \leq i \leq q$, there is some v_i in X_{ns} and some input sequence u_i such that*

$$CA^{\tau}x_i = y_{v_i,u_i}(\tau).$$

Proof: If the system is τ-ISO, it is immediate that the given condition much hold. For the converse, let x_0 in X_s be given. Then there are nonnegative real numbers $\lambda_1, \lambda_2, \ldots, \lambda_q$ such that $x_0 = \lambda_1 x_1 + \cdots + \lambda_q x_q$. Moreover, for $1 \leq i \leq q$, there exist initial vectors v_i in X_{ns} and input sequences u_i with

$$CA^{\tau}x_i = y_{v_i,u_i}(\tau).$$

Hence

$$\begin{aligned} CA^{\tau}x_0 &= \sum_{i=1}^{q} \lambda_i CA^{\tau}x_i \\ &= \sum_{i=1}^{q} \lambda_i y_{v_i,u_i}(\tau) \\ &= y_{x_0,u} \end{aligned}$$

where $x_0 = \sum_{i=1}^{q} \lambda_i v_i \quad X_{ns}$ and $u = \sum_{i=1}^{q} \lambda_i u$ is a nonnegative input sequence. It now follows from Lemma 7.3.1 that (7.1) is τ-ISO as claimed. □

Remarks:

- The last result reduces the problem of τ-ISO where the secret and non-secret states are finitely generated cones to finding nonnegative solutions to a system of linear equations.
- To see this, note that (7.1) will be τ-ISO if and only if for every vector $y_i = CA^{\tau}x_i$, $1 \leq i \leq q$, there exist nonnegative real numbers α_{ij}, $1 \leq j \leq r$ and some nonnegative input sequence $u_i = (u_i(0), u_i(1), \ldots, u_i(\tau - 1))$ such that
$$y_i = \sum_{j=1}^{r} \alpha_{ij} CA^{\tau}x_j + \sum_{j=0}^{\tau-1} CA^{\tau-j-1}Bu_i(j). \tag{7.4}$$
- Using (7.4), define the block matrix M by
$$M = \left[CA^{\tau}x_1\ CA^{\tau}x_2\ \ldots CA^{\tau}x_r\ CA^{\tau-1}B\ \ldots\ CB\right]. \tag{7.5}$$
- In terms of the matrix M, (7.4) shows that (7.1) is τ-ISO if and only if for all i, $1 \leq i \leq q$ there is some nonnegative vector z_i with
$$y_i = Mz_i. \tag{7.6}$$

The remarks above show that the property of τ-ISO for the case we are considering comes down to the existence of nonnegative solutions z_i, of the equations (7.6) for $1 \leq i \leq q$. This simple observation suggests the use of Farkas' Lemma (or a so-called Theorem of the Alternative) to gain insight into this question.

Farkas' Lemma

We now recall the statement of Farkas' Lemma. The version stated here is taken from [109] where it appears as Theorem 1.30.

Theorem 7.3.3. *Let* $M \quad \mathsf{R}^{m \times n}$ *and* $y \quad \mathsf{R}^m$ *be given. Then exactly one of the following conditions holds.*

1. *There exists some* $z \quad \mathsf{R}^n_+$ *with* $Mz = y$.
2. *There exists some* $w \quad \mathsf{R}^m$ *such that* $w^T y < 0$ *and* $w^T M \geq 0$.

To finish off this brief chapter, we note some simple consequences of applying Farkas' Lemma to the problem of τ-ISO for (7.1) under the assumptions (7.2) on X_s and X_{ns}.

Proposition 7.3.4. *Let the sets* X_s, X_{ns} *satisfy* (7.2), *let* $\tau > 0$ *be a positive integer and let the matrix* M *be given by* (7.5). *The system* (7.1) *is* τ*-ISO if and only if for* $1 \leq i \leq q$

$$w^T M \geq 0 \quad = \quad w^T C A^\tau x_i \geq 0.$$

Proof: From the remarks after Lemma 7.3.2, it follows that (7.1) is τ-ISO if and only if for $1 \leq i \leq q$, there is some nonnegative vector $z_i \geq 0$ with $Mz_i = CA^\tau x_i$. Farkas' Lemma (Theorem 7.3.3) implies that this is equivalent to the following condition.

For each i with $1 \leq i \leq q$, there is no vector w satisfying the inequalities $w^T C A^\tau x_i < 0$, $w^T M \geq 0$. This condition is equivalent to the condition that $w^T M \geq 0$ implies $w^T C A^\tau x_i \geq 0$ for $1 \leq i \leq q$ which proves the result. □

Remarks:

- The purpose of this short chapter is to present some initial thoughts on opacity for positive linear systems. The result of Proposition 7.3.4 can be used to obtain conditions for opacity for certain classes of systems.
- For example, consider Proposition 7.3.4 for the case where the system (7.1) has a single output; so $p = 1$ and $C = c^T \geq 0$ is a row vector. In this case, clearly M is also a row vector of nonnegative real numbers and $w^T M \geq 0$ implies that w is a nonnegative real number (unless M consists entirely of zeros). Trivially, the condition of Proposition 7.3.4 is satisfied so the system is τ-ISO for any $\tau > 0$.

- If for every i with $1 \leq i \leq p$, there is some column of M, with index j_i say, such that $m_{ij_i} > 0$ and $m_{kj_i} = 0$ for $k = i$. Informally, for each such i there is some column of M which has exactly one non-zero entry in position i. It is relatively straightforward to see that in this case, (7.1) is τ-ISO also.

7.4 Concluding Remarks

In this very brief chapter, we have considered the problem of initial state opacity for positive systems. Opacity is an interesting, alternative privacy framework and its use for linear systems is very recent [89, 90]. The aim of this chapter was to present preliminary results on opacity for positive systems where the secret and non-secret states lie in finitely generated cones which seem a natural choice when dealing with positive systems. The result of Proposition 7.3.4 shows that τ-ISO is equivalent to one convex cone being a subset of another. This simple result could be combined with results from convex analysis to derive usable conditions for opacity. This opens an interesting possible direction for future research.

CHAPTER 8

Conclusions

In this chapter, we review and summarise the work presented in this thesis and highlight some open questions for future work based on it.

8.1 Summary

In Chapter 2 we discussed some of the most relevant results from the literature on differential privacy, the positive observer problem, and opacity for discrete event and linear systems.

In order to apply differentially private mechanisms to positive systems, we need ways of guaranteeing that the output of these mechanisms takes only nonnegative values. Rather than constructing entirely new mechanisms, in Chapter 3 we considered ways of using existing mechanisms, such as the Laplace or Gaussian mechanism, to build nonnegative mechanisms. The two main approaches considered were *post-processing* and *restriction*. We have shown that bias is inevitable for both approaches, but post-processing leads to a bias that is always strictly less than that caused by restriction for the Laplace mechanism. For a different accuracy measure, we considered the MSE of both the post-processing and restriction mechanism. Similarly for the bias, the MSE for post-processing is always strictly less than the MSE of the restricted Laplace mechanism. In relation to the post-processing mechanism, we considered alternative post-processing functions and show that lower bias

can be achieved by using translated ramp functions and show the existence of a post-processing function that minimises the worst case MSE for the Laplace mechanism.

The results of Chapter 3 focussed on 1-dimensional, real-valued queries. In the early part of Chapter 4, we showed how to extend these results so that they can be applied to the outputs of positive systems. This work then allowed us to construct differentially private positive observers, which was the major focus of much of the following chapters. A major contribution of Chapter 4 is a bound on the l_1 sensitivity of a linear observer, which can be used to construct a differentially private observer using the Laplace mechanism. When we specialise to positive linear systems and the positive observer problem, we are presented with some novel questions. The most obvious of these is the question of finding an observer which minimises the amount of noise to be added. Our work in the later sections of Chapter 4 gives a technique that can be used to approach this problem for positive systems with a single output. It is not immediately clear how the graphical approach could be extended to systems with multiple outputs.

A more theoretical approach to the problem of minimising sensitivity is adopted in Chapter 5. Here we derived a constructive, analytical characterisation of the optimal observer gain matrices for compartmental systems with a single output. We also developed a similar result for a class of compartmental systems with multiple outputs. Alongside minimising the sensitivity, this chapter also gives some insight into the trade-off between minimising the sensitivity and the rate of convergence of the observer to the true state for a positive single output system. In particular, for a fixed rate of convergence we calculate a minimum of the bound of the sensitivity of the observer. We also derived an upper bound for the l_1 sensitivity of a more general class of observer. Through a specific example, we saw that this class of observer allow us to add less noise to the observer to achieve differential privacy than for a Luenberger observer.

In Chapter 6 the main focus was on deriving an upper bound on the l_2 sensitivity of a linear observer, which can be used to construct a differentially private observer using the Gaussian mechanism. The algorithm presented here can be used to find a gain matrix that minimises the sensitivity bound for a multiple output system. This was done by reducing the multiple variable, non-convex

problem down to iterations of a single variable convex problem through different constraints.

In contrast to the majority of this thesis that addresses differential privacy for positive linear system and positive linear observers, in Chapter 7, we introduced the problem of initial state opacity for positive systems. Here, we give preliminary results on opacity when the secret and non-secret states lie in finitely generated cones. We saw that the property of τ-ISO is equivalent to one convex cone being a subset of another. This result could be used to obtain conditions for opacity of certain classes of positive systems.

8.2 Future Works

There are a number different questions that arise from the results of this thesis, some of which are listed below.

- In Chapter 3, we applied post-processing and restriction to Laplace mechanism to obtain an ε differentially private mechanism that only takes nonnegative values. It would be interesting to consider similar questions for other base mechanisms such as the Gaussian mechanism featured in Chapter 6 to from a (ε, δ) differentially private mechanism. Again, obtaining similar results on the bias and the mean square error of nonnegative Gaussian mechanisms would be an interesting research direction.

- In Chapter 5, we have shown that it is possible to reduce the amount of noise needed using the more general observer class, but it is not clear that this is always the case. Identifying precisely systems for which this can be done and obtaining results for the more general observers of a compartmental system similar to those for Luenberger observers is another possible direction for future work.

- Is it possible to extend results from Chapter 5 to a broader class of multiple-output compartmental systems? Specifically, can we relax the assumptions (F1) and (F2) of Section 5.2.2 and obtain a result like Theorem 5.2.3? The insights of the paper [7] combined with Theorem 5.2.3 suggest the following interesting question. Can we identify matrix pairs

(A, C) with $p \geq 2$ for which the minimum value of $\Phi(L)$ for $L \quad \mathsf{F}_{A,C}$ occurs at a nonnegative matrix L?

- The work of Chapter 7 is only a first step on opacity for positive systems. This could be developed to obtain usable conditions for opacity for classes of positive systems. Another question here is to apply it to designing opaque positive observers.
- As a final point, all of our work concerns linear positive systems. Extending this to nonlinear systems would be a significant challenge.

We have only discussed a sample of possible future questions here. There are many other interesting and challenging questions related to applying privacy concepts to positive systems theory.

Bibliography

[1] P. Abara, F. Ticozzi, and C. Altafini. Spectral conditions for stability and stabilization of positive equilibria for a class of nonlinear cooperative systems. *IEEE Transactions on Automatic Control*, 63(2):402–417, 2017. 12

[2] P. Ahm. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 58(2):1701–1777, 2010. 2

[3] M. Ait Rami and F. Tadeo. Controller synthesis for positive linear system with bounded controls. In *IFAC World Congress*, 2005. 19

[4] M. Ait Rami and F. Tadeo. Linear programming approach to impose positiveness in closed-loop and estimated states. In *17th International Symposium on Mathematical Theory of Network and Sytems*, 2006. 19

[5] M. Ait Rami and F. Tadeo. Positive observation problem for linear discrete positive systems. In *Proc. IEEE 45th Annual Conference on Decision and Control (CDC)*, 2006. 11, 19, 22, 78, 79, 117

[6] M. Ait Rami and F. Tadeo. Controller synthesis for positive linear system with bounded controls. *IEEE Transactions on Circuits and Systems-II*, 54:151–155, 2007. 19

[7] M. Ait Rami, F. Tadeo, and U. Helmke. Positive observers for linear positive systems, and their implications. *International Journal of Control*, 84(4):716–725, 2011. 2, 14, 19, 20, 24, 89, 90, 134

[8] G. Bachman and L. Narici. *Functional Analysis*. Dover Publications (republication), 2000. 62, 64

[9] J. Back and A. Astolfi. Positive linear observers for positive linear systems: a sylvester equation approach. *Proc. American Control Conference*, 2006. 21, 22, 23

[10] J. Back and A. Astolfi. Design of positive linear observers for positive linear systems via coordinate transformations and positive realizations. *SIAM J. Control & Opt.*, 47(1):345–373, 2008. 2, 14, 21, 22, 23, 68, 78, 88, 90, 105, 109, 117

[11] J. Back, A. Astolfi, and H. Cho. Design of positive linear observers for linear compartmental systems. In *Proc. SICE-ICASE International Joint Conference*, 2006. 89, 105

[12] R. Bapat. *Nonnegative Matrices and Applications*. Cambridge Univ. Press, 2009. 7, 9

[13] R. B. Bapat. *Graphs and Matrices*. Springer-Verlag, 2014. 8

[14] A. Barvinok. *A Course in Convexity*. American Mathematical Society, 2002. 127

[15] L. Benvenuti and L. Farina. A tutorial on the positive realization problem. *IEEE Transactions on Automatic Control*, 49(5):651–664, 2004. 2, 23

[16] A. Berman, M. Neumann, and R. J. Stern. *Nonnegative Matrices in Dynamic Systems*. Wiley, 1989. 7, 126

[17] A. Berman and R. J. Plemmons. *Nonnegative Matrices in the Mathematical Sciences*. Society for industrial and Applied Mathematics (Siam), 1994. 7

[18] P. Billingsley. *Probability and Measure*. Wiley, 1995. 69

[19] F. Blanchini, P. Colaneri, and M. Valcher. Switched positive linear systems. *Foundations and Trends in Systems and Control*, 2(2):101–273, 2015. 68

[20] F. Blanchini, P. Colaneri, and M.-E. Valcher. Co-positive lyapunov functions for the stabilization of positive switched systems. *IEEE Transactions on Automatic Control*, 57(12):3038–3050, 2012. 12

[21] V. Bokharaie, O. Mason, and M. Verwoerd. D-stability and delay-independent stability of homogeneous cooperative systems. *IEEE Transactions on Automatic Control*, 55(12):2882–2885, 2010. 12

[22] V. Bokharaie, O. Mason, and F. Wirth. Stability and positivity of equilibria for subhomogeneous cooperative systems. *Nonlinear Analysis: Theory, Methods, and Applications*, 74(17):6416–6426, 2011. 12

[23] B. Brian, J. Wang, and Z. Qu. Nonlinear positive observer design for positive dynamical systems. In *American Control Conference*, 2010. 14

[24] R. Bru, S. Romero-Vivo, and E. Sanchez. Spectral conditions for stability and stabilization of positive equilibria for a class of nonlinear cooperative systems. *Linear Algebra and Applications*, 310:49–71, 2000. 15

[25] J. W. Bryans, M. Koutny, and P. Y. Ryan. Modelling opacity using petri nets. *Electronic Notes in Theoretical Computer Science*, 121:101–115, 2005. 33

[26] F. Cacace, A. Germani, and C. Manes. A positive observer for linear systems. *IFAC, World Congress*, 47(3):14330–14334, 2014. 14

[27] L. Caccetta and V. G. Rumchev. A survey of reachability and controllability for positive linear systems. *Annals of Operations Research*, 98:101–122, 2000. 15

[28] B. Canto, R. Canto, and S. Kostova. Stabilization of positive linear discrete-time systems by using a Brauer's theorem. *The Scientific World Journal*, 2014. 12

[29] B. Canto, C. Coll, and E. Sanchez. Positive solutions of a discrete-time descriptor system. *International Journal of Systems Science*, 39(1):81–88, 2008. 2, 12

[30] B. Canto, C. Coll, and E. Sanchez. Stabilization of an epidemic model via an n-periodic approach. *International Journal of Applied Mathematics and Computer Science*, 28(1):185—195, 2018. 10

[31] C.-T. Chen. *Linear system theory and design*. Oxford University Press, Inc., 1970. 14, 21

[32] C. Commault. A simple graph theoretic characterization of reachability for positive linear systems. *Systems and Control Letters*, 52(3–4):275–282, 2004. 15

[33] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas. Differential privacy in control and network systems. In *Proc. IEEE 55th Annual Conference on Decision and Control (CDC)*, 2016. 7

[34] P. De Leenheer and D. Aeyels. Extension of the perron–frobenius theorem to homogeneous systems. *SIAM Journal of Control and Optimization*, 41(2):563–582, 2002. 12

[35] X. Ding, L. Shu, and X. Liu. On linear copositive lyapunov functions for switched positive systems. *Journal of the Franklin Institute*, 348(8):2099–2107, 2011. 12

[36] T. N. Dinh, S. Bonnabel, and R. Sepulchre. Contraction-based design of positive observers. In *Proc. IEEE 52nd Annual Conference on Decision and Control (CDC)*, 2013. 14

[37] J. Domingo-Ferrer and J. Soria-Comas. From t-closeness to differential privacy and vice versa in data anonymization. *Knowledge Based Systems*, 74:151–158, 2015. 2

[38] C. Dwork. Differential privacy. In *Proceedings of the 33rd Annual Interna- tional Colloquium on Automata, Languages and Programming, LNCS 4051*, pages 1–12. Springer-Verlag, 2006. 7, 25, 39, 69, 111

[39] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. *Theory of Cryptography, Springer*, pages 265–284, 2006. 27

[40] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Theoretical Computer Science*, 9(3):211–407, 2014. 2, 25, 39, 42, 43

[41] D. Efimov, W. Perruquetti, T. Raïssi, and A. Zolghadri. Interval observers for time-varying discrete-time systems. *IEEE Transactions on Automatic Control*, 58(12):3218–3224, 2013. 24

[42] L. Farina and S. Rinaldi. *Positive Linear Systems: Theory and Applications*. Wiley, 2000. 1, 7, 8, 10, 11, 12

[43] H. Feyzmahdavian, B. Besselink, and M. Johansson. Stability analysis of monotone systems via max-separable lyapunov functions. *IEEE Transactions on Automatic Control*, 63(3):643–656, 2017. 12

[44] E. Fornasini and M. Valcher. Stability and stabilizability criteria for discrete-time positive switched systems. *IEEE Tran. Aut. Cont.*, 57(5):1208–1221, 2012. 68

[45] E. Fornasini and M.-E. Valcher. Linear copositive lyapunov functions for continuous-time positive switched systems. *IEEE Transactions on Automatic Control*, 55(8):1933–1937, 2010. 12

[46] B. Fristedt, N. Jain, and K. N. *Filtering and prediction: A Primer*. American Mathematical Society, 2007. 48

[47] B. C. M. Fung, K. Wang, A. W.-C. Fu, and P. S. Yu. *Introduction to privacy-preserving data publishing: Concepts and techniques*. Taylor and Francis Group, 2011. 25

[48] J.-L. Gouze, A. Rapaport, and M. Z. Hadj-Sadok. Interval observers for uncertain biological systems. *Ecological Modelling*, 133:45–56, 2000. 24

[49] G. Grimmett and D. Stirzaker. *Probability and Random Processes*. Oxford University Press, 2001. 54, 55

[50] W. Haddad and V. Chellaboina. Stability theory for nonnegative and compartmental dynamical systems with time delay. *Systems and Control Letters*, 51(5):355–361, 2004. 2, 12

[51] R. Hall, A. Rinaldi, and L. Wasserman. Random differential privacy. *Journal of Privacy and Confidentiality*, 2(2):43–59, 2012. 2

[52] H. M. Hardin and J. H. van Schuppen. Observers for linear positive systems. *Lin. Alg. and its Appl.*, 425:571–607, 2007. 2, 14, 15, 16, 18, 20, 68, 78, 117

[53] L. Hardouin, C. A. Maia, B. Cottenceau, and M. Lhommeau. Observer design for max plus linear systems. *IEEE Transactions on Automatic Control*, 55(2):538–543, 2010. 24

[54] L. Hardouin, Y. Shang, C. A. Maia, and B. Cottenceau. Observer-based controllers for max-plus linear systems. *IEEE Transactions on Automatic Control*, 62(5):2153–2165, 2017. 24

[55] B. Heidergott, G.-J. Olsder, and J. Van der Woude. *Max Plus at Work*. Princeton University Press, 2006. 24

[56] N. Holohan, S. Antonatos, S. Braghin, and P. Mac Aonghusa. The bounded laplace mechanism in differential privacy. *arXiv:1808.10410 [cs.CR]*, 2018. 39, 44

[57] N. Holohan, D. Leith, and O. Mason. Differential privacy in metric spaces: Numerical, categorical and functional data under the one roof. *Information Sciences*, 305(1):256–268, 2015. 40, 43, 70

[58] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge Univ. Press, 1991. 7

[59] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge Univ. Press, 2012. 7, 8, 9, 100, 111, 112

[60] A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Glessing, E. Nordholt, K. Spicer, and P. de Wolf. *Statistical Disclosure Control*. Wiley, 2012. 2

[61] R. Jacob, J.-j. Lesage, and J.-M. Faure. Overview of discrete event systems opcaity: Models, validation, and quantification. *Annual Reviews in Control*, 41:135–146, 2016. 7, 33

[62] J. A. Jacquez and C. P. Simon. Qualitative theory of compartmental systems. *The Scientific World Journal*, 35(1):43–79, 1993. 1, 17, 88

[63] T. Kaczorek. *Positive 1D and 2D Systems*. De Gruyter, 2002. 1, 7, 10

[64] T. Kailath. *Linear System*. Prentice-Hall, Inc, 1980. 10, 21

[65] F. Knorn, O. Mason, and R. Shorten. On linear co-positive lyapunov functions for sets of linear positive systems. *Automatica*, 45(8):1943–1947, 2009. 12

[66] U. Krause. *Positive Systems in Discrete Time*. De Gruyter, 2015. 1, 7, 10

[67] J. Le Ny. Privacy-preserving nonlinear observer design using contraction analysis. *Proc. IEEE 54th Annual Conference on Decision and Control (CDC)*, 2015. iii, 6, 29, 68, 69, 77, 78

[68] J. Le Ny. Differentially private nonlinear observer design using contraction analysis. *International Journal of Robust and Nonlinear Control, Special Issue on Privacy and Security of Cyber-Physical Systems*, 2018. 3, 29, 30

[69] J. Le Ny and G. J. Pappas. Differentially private filtering. In *Proc. IEEE 51st Annual Conference on Decision and Control (CDC)*, 2012. 27, 28, 31

[70] J. Le Ny and G. J. Pappas. Differentially private kalman filtering. In *50th Annual Allerton Conference*, 2012. 27, 31

[71] J. Le Ny and G. J. Pappas. Privacy-preserving release of aggregate dynamic models. In *Proc.Proceedings of the 2nd ACM international conference on High confidence networked systems (HiCoNS*, 2013. 38, 49

[72] J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Control*, 59(2):341–354, 2014. 27, 29, 30, 31, 68, 69, 70, 71, 75, 111, 112

[73] E. Lieb and M. Loss. *Analysis*. American Mathematical Society, 2001. 70

[74] F. Lin. Opacity of discrete event systems and its applications. *Automatica*, 47:496–503, 2011. 32, 33, 34

[75] F. Liu. Statistical properties of sanitized results from differentially private laplace mechanism with bounding constraints. *arXiv:1607.08554v4 [stat.ME]*, 2016. 39, 43, 44, 65

[76] L. Liu, H. R. Karimi, and X. Zhao. New approaches to positive observer design for discrete-time positive linear systems. *Journal of the Franklin Institute*, 355:4336–4350, 2018. 14, 24, 39, 68

[77] X. Liu. Stability analysis of switched positive systems: A switched linear copositive lyapunov function method. *IEEE Transactions on Circuits and Systems II*, 56(5):414–418, 2009. 12

[78] X. Liu, W. Yu, and L. Wang. Stability analysis for continuous-time positive systems with time-varying delays. *IEEE Transactions on Automatic Control*, 55(4):1024–1028, 2010. 12

[79] D. G. Luenberger. Observing the state of a linear system. *IEEE Transactions on Military Electronics*, 8:74–80, 1964. 2, 13

[80] D. G. Luenberger. Observers for multivariable systems. *IEEE Transactions on Automatic Control*, 11(2):190–197, 1966. 13

[81] D. G. Luenberger. An introduction to observers. *IEEE Transactions on Automatic Control*, 16(6):596–602, 1971. 13

[82] O. Mason. Diagonal riccati stability and positive time-delay systems. *Systems and Control Letters*, 61(1):6–10, 2012. 2, 12

[83] O. Mason and R. Shorten. On linear copositive lyapunov functions and the stability of switched positive linear systems. *IEEE Transactions on Automatic Control*, 52(7):1346–1349, 2007. 2, 12

[84] F. Mazenc, T. N. Dinh, and S. I. Niculescu. Interval observers for discrete-time systems. *International Journal of Robust and Nonlinear Control*, 24(17):2867–2890, 2014. 24

[85] F. McSherry and K. Talwar. Mechanism disign via differential privacy. *IEEE Symposium on Foundations of Computer Science*, pages 94–103, 2007. 27, 43

[86] Netflix. Netflix prize. `https://www.netflixprize.com/index.html`, 2009. Accessed: 2020-04-10. 2

[87] R. Rajamani. Observer for lipschitz nonlinear systems. *IEEE Transactions on Automatic Control*, 43(3):397–401, 1998. 14

[88] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. A framework for decentralized opacity in linear systems. In *Annual Allerton Conference on Communications, Control, and Computing*, 2016. 35, 36

[89] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. A framework for opacity in linear systems. In *IEEE American Control Conference (ACC)*, pages 6337–6344, 2016. 34, 35, 36, 125, 126, 131

[90] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus. Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control*, 47:496–503, 2019. 36, 125, 126, 131

[91] W. J. Rugh. *Linear system theory*. Prentice-Hall, Inc, 1996. 10, 14, 15, 16

[92] A. Saboori and C. N. Hadjicostis. Notions of security and opacity in discrete event systems. In *46th IEEE Conference on Decision and Control*, 2007. 33

[93] W. Schirotzek. *Nonsmooth Analysis*. Springer-Verlag, 2007. 61, 62, 63

[94] E. Seneta. *Non-Negative Matrices: An Introduction to Theory and Applications*. George Allen and Unwin, 1973. 7, 9

[95] Z. Shu, J. Lam, H. Gao, B. Du, and L. Wu. Positive observer and dynamic output-feedback controllers for interval positive linear systems. *IEEE Transactions on Circuits and Systems*, 55(10):3209–3222, 2008. 14, 68

[96] H. Smith. *Monotone Dynamical Systems*. American Mathematical Society, 1995. 12

[97] E. D. Sontag. *Mathematical Control Theory*. Springer-Verlag, 1998. 13

[98] J. Soria-Comas and J. Domingo-Ferrer. Optimal data-independent noise for differential privacy. *Information Sciences*, 250:200–214, 2013. 2

[99] J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and D. Megias. Individual differential privacy: A utility-preserving formulation of differential privacy guarantees. *IEEE Tran. Information Forensics and Data Security*, 12(6):1418–1429, 2017. 2, 39

[100] L. Sweeney. Uniqueness of simple demographics in the us population. Technical report, Carnegie Mellon University, 2000. 2

[101] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002. 25

[102] V. Torra. *Data Privacy: Foundations, New Developments and the Big Data Challenge*. Springer-Verlag, 2017. 2

[103] M. Valcher. Controllability and reachability criteria for discrete time positive systems. *Int. J. of Cont.*, 65(3):511–536, 1996. 15, 68

[104] M.-E. Valcher and I. Zorzan. State–feedback stabilization of multi-input compartmental systems. *Systems and Control Letters*, 119:81–91, 2018. 1, 88

[105] P. Van den Driessche and J. Watmough. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. *Mathematical Biosciences*, 180(1):29–48, 2002. 1, 10, 88

[106] J. M. Van Den Hof. Positive linear observers for linear compartmental systems. *SIAM Journal on Control and Optimization*, 36(2):590–608, 1998. 1, 2, 14, 17, 18, 19, 20, 24, 90

[107] E. Virnik. Stability analysis of positive descriptor systems. *Linear Algebra and its Applications*, 429(10):2640–2659, 2008. 2, 12

[108] G. Wang, B. Li, Q. Zhang, and C. Yang. Positive observers design for discrete-time positive systems with missing data in output. *Neurocomputing*, 168:427–434, 2015. 14

[109] X. Zhan. *Matrix Theory*. American Mathematical Society, 2013. 129

[110] X. Zhao, T. Wu, X. Zheng, and R. Li. Discussions on observer design of nonlinear positve systems via t-s fuzzy modeling. *Neurocomputing*, 157:70–75, 2015. 14