Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 50-1 (2017) 3111–3116

Differential Privacy and the l_1 Sensitivity of Positive Linear Observers [★]

Aisling McGlinchey [*] **Oliver Mason** [**]

[*] *Dept. of Mathematics and Statistics, Maynooth University,*
Maynooth, Co. Kildare, Ireland & Lero, the Irish Software Research
Centre (e-mail: aisling.mcglinchey.2009@mumail.ie).
[**] *Dept. of Mathematics and Statistics/Hamilton Institute, Maynooth*
University, Maynooth, Co. Kildare, Ireland & Lero, the Irish Software
Research Centre (e-mail: oliver.mason@nuim.ie)

Abstract: We consider the design of differentially private observers for positive linear systems in discrete time. In particular, we first provide a general bound for the l_1 sensitivity of the map defined by a Luenberger observer for a linear time invariant (LTI) system and show that this can be tight as well as describing how it relates to previous work. We then define an optimisation problem for minimising this bound for positive linear observers and provide a characterisation of optimal solutions for systems with a single measured output. Finally, we show how the addition of Laplacian noise can violate positivity, even for the optimally designed positive observer and discuss directions for future work.

Keywords: Positive systems; linear time-invariant systems; observers for linear systems; differential privacy; optimization.

1. INTRODUCTION

Modern cyber-physical systems in domains such as transport, public health and logistics often require the transmission and processing of sensitive or personal data (Lucia et al. (2016)). Hence, it is important to develop control methodologies for such systems that protect user privacy while delivering near optimal performance in order to maintain public confidence in their adoption. In the past decade, quantitative privacy paradigms have been proposed in the computer science community; *differential privacy* (Dwork (2006)) has emerged as one of the most promising frameworks for privacy preserving control design, and we adopt it as our quantitative privacy paradigm here. Our results build on the recent work of Le Ny and Pappas (2014); Le Ny (2015) and others on differentially private filtering and control and efforts to extend differential privacy to more general data types (Holohan et al. (2015)). Other recent noteworthy contributions in the area include: Dong et al. (2015) which describes differentially private mechanisms for routing people through a transportation network; while in Venkitasubramaniam (2013), a Markov decision process model was used to design optimal data sharing policies for a social network, based on an information theoretic measure of privacy.

Le Ny and Pappas (2014) defined a system theoretic formulation of differential privacy as well as two fundamental mechanisms to provide differential privacy for inputs. These extended appropriately the Laplacian and Gaussian mechanisms used in earlier work for static databases. In both cases, the *sensitivity* of the input-output map plays a crucial role in determining the magnitude of noise required to ensure differential privacy. In a subsequent paper (Le Ny (2015)) these results were used to construct differentially private observers for nonlinear systems satisfying appropriate contraction properties.

Many motivating examples for privacy preserving control fall within the class of positive systems (Valcher (1996), Fornasini and Valcher (2012), Blanchini et al. (2015)). 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 Hardin and van Schuppen (2007), 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 Shu et al. (2008). Our objective here is to introduce the problem of differentially private positive observer design; starting from the work of Le Ny (2015) and concentrating on what can be said for the sensitivity of observers for positive linear systems.

1.1 Outline of paper/contributions

In Section 2 we introduce our notation and provide background on differential privacy for dynamical systems. In Section 3, we derive an upper bound for the l_1 sensitivity of a linear observer of Luenberger type and show that this bound can be attained. In Section 4 we specialise to positive systems and define an optimization problem for designing a positive observer that also minimises the bound from Section 3.

[★] This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie)

2405-8963 © 2017, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.317

2. BACKGROUND ON DIFFERENTIAL PRIVACY AND OBSERVERS

Throughout the paper, $\mathbb{R}^n$ denotes the vector space of n-tuples of real numbers and $\mathbb{R}^{n\times n}$ the space of $n\times n$ matrices with real entries. For $x \in \mathbb{R}^n$: $x \geq 0$ means that $x_i \geq 0$ for $1 \leq i \leq n$. $\mathbb{R}^n_+$ denotes the nonnegative orthant

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

Analogous notation is also used for matrices throughout. A^T denotes the transpose of $A \in \mathbb{R}^{n\times n}$ and $\rho(A)$ is used to denote its spectral radius.

Throughout this paper, 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 (Le Ny and Pappas (2014); Dwork (2006)). As no confusion will arise, we use $\|x\|$ for the l_1 norm of $x \in \mathbb{R}^n$ and for $T \in \mathbb{R}^{m\times n}$, $\|T\|$ denotes the l_1 induced (operator) norm of T. It is standard (Horn and Johnson (2012)) that this is given by

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

Our work is motivated by the design of differentially private observers for linear time-invariant (LTI) systems in discrete time. Following Hardin and van Schuppen (2007); Ait Rami and Tadeo (2006), we consider systems of the form:

$$\begin{aligned} x(k+1) &= Ax(k) \\ y(k) &= Cx(k) \end{aligned} \tag{2}$$

where $A \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{p\times n}$. The design of a Luenberger observer for this system requires a matrix $L \in \mathbb{R}^{n\times p}$ such that the solution $z(\cdot)$ of the system $\mathcal{L}$ given by

$$\begin{aligned} z(k+1) &= Az(k) + L(y(k) - Cz(k)) \qquad (3) \\ &= (A - LC)z(k) + Ly(k) \end{aligned}$$

satisfies $\|z(k) - x(k)\| \to 0$ as $k \to \infty$ where x is the solution of (2). In the absence of additional constraints, the classical solution is to construct a matrix L such that $A - LC$ is *Schur-stable* (Sontag (1998)).

When the signal y contains sensitive or personal information we wish to release a noisy observer signal $\hat{z}$ such that the mapping $y \to \hat{z}$ is differentially private. We now recall the relevant definition in a system theoretic context from Le Ny and Pappas (2014); Le Ny (2015).

Let $K > 0$ and $0 \leq \alpha < 1$ be given. Then two sequences/signals y, y' are *adjacent*, written $y \sim y'$ if

$$\exists\, k_0 \geq 0\, s.t. \begin{cases} y(k) = y'(k), & k < k_0 \\ \|y(k) - y'(k)\| \leq K\alpha^{k-k_0}, & k \geq k_0 \end{cases} \tag{4}$$

The intuition is that adjacent signals correspond to a change in the entries of a small number of individuals at a particular time; the initial magnitude of the change is K and its magnitude then decays geometrically at rate α.

Given a system G mapping input sequences y in $\mathcal{Y}$ to output signals z in $\mathcal{Z}$, a differentially private mechanism is defined by a set of random variables $\{Z_{G,y} \mid y \in \mathcal{Y}\}$ taking values in $\mathcal{Z}$ satisfying:

$$\mathbb{P}(Z_{G,y} \in A) \leq e^{\epsilon}\mathbb{P}(Z_{G,y'} \in A) \tag{5}$$

for all measurable sets A of $\mathcal{Z}$ and all $y \sim y'$.

For a sequence/signal $y(k)$, $0 \leq k < \infty$ with $y(k) \in \mathbb{R}^n$ for all k, we follow Le Ny (2015) and define its l_1 norm by

$$\|y\| = \sum_{k=0}^{\infty} \|y(k)\|.$$

We next recall the key concept of sensitivity which determines the magnitude of noise required to ensure differential privacy.

Definition 2.1. The l_1 sensitivity $\Delta(G)$ of a system G is defined as

$$\Delta(G) := \sup_{y\sim y'} \|G(y) - G(y')\|. \tag{6}$$

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 (Le Ny and Pappas (2014)).

An ϵ differentially private mechanism can be defined by adding *iid* noise generated from the Laplace distribution with parameter $b = \frac{\Delta(\mathcal{L})}{\epsilon}$ to each component of each $z(k)$ (Le Ny and Pappas (2014)). For this reason we are interested in characterising the l_1 sensitivity of the observer (3) mapping y to z.

3. SENSITIVITY FOR POSITIVE LUENBERGER OBSERVERS

The results described at the end of the last section naturally motivate the problem of determining bounds for the l_1 sensitivity of (3).

Proposition 3.1. Let $A \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{p\times n}$, $L \in \mathbb{R}^{n\times p}$ be given and suppose that $\|A - LC\| < 1$. Consider the Luenberger observer, $\mathcal{L}$ given by (3). Then for the adjacency relation defined by (4), the l_1 sensitivity of $\mathcal{L}$ (as given in (6)) is bounded by

$$\Delta(\mathcal{L}) \leq \left(\frac{K}{1-\alpha}\right)\left(\frac{\|L\|}{1 - \|A - LC\|}\right). \tag{7}$$

Proof: Let two adjacent sequences $y \sim y'$ be given. The (zero-initial state) map from y to z corresponding to (3) is described by

$$z(k+1) = \sum_{i=0}^{k} (A - LC)^{k-i} Ly(i) \tag{8}$$

Write z' for the observer output corresponding to y' so that

$$z'(k+1) = \sum_{i=0}^{k} (A - LC)^{k-i} Ly'(i). \tag{9}$$

As $y \sim y'$, it follows that $z'(k) = z(k)$ for $k \leq k_0$. Moreover, for $k > k_0$, we have

$$z(k) - z'(k) = \sum_{i=k_0}^{k-1} (A - LC)^{k-i-1} L(y(i) - y'(i)). \tag{10}$$

We need to bound $\|z(k) - z'(k)\|$; for $k > k_0$, using the triangle inequality and the submultiplicative property of the induced matrix norm we have:

$$\|z(k) - z'(k)\| = \| \sum_{i=k_0}^{k-1} (A - LC)^{k-i-1} L(y(i) - y'(i))\|$$
$$\leq \|L\| \, K \sum_{i=k_0}^{k-1} \|(A - LC)\|^{k-i-1} \alpha^{i-k_0}$$

The l_1 norm of $z(k) - z'(k)$ will be given by the sum $\sum_{k=0}^{\infty} \|z(k) - z'(k)\|$ which, in the light of the above calculation and remarks, will be bounded above by

$$\|L\| \, K \sum_{k=k_0}^{\infty} \sum_{i=k_0}^{k} \|(A - LC)\|^{k-i} \alpha^{i-k_0}. \tag{11}$$

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

$$\sum_{k=0}^{\infty} \sum_{i=0}^{k} \|(A - LC)\|^{k-i} \alpha^{i}$$
$$= \left(\frac{1}{1-\alpha}\right) \left(\frac{1}{1 - \|A - LC\|}\right).$$

Putting everything together, we see that the l_1 norm of $z - z'$ is bounded above by

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

which completes the proof as $y \sim y'$ were arbitrary.

3.1 Tightness of upper bound

It is natural to ask whether the upper bound on the sensitivity of (3) derived in Proposition 3.1 is tight. To this end, we next describe a simple example for which the bound is indeed attained.

Example 3.1. Consider

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

A straightforward calculation shows that

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

so that $\|A - LC\| = 3/4 < 1$. Moreover,

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

so that $(A - LC)^i L = \|A - LC\|^i L$ for all $i \geq 1$. Using this, we can see that for a pair of adjacent sequences y, y' where $y(k), y'(k)$ are in $\mathbb{R}$ for all k and satisfy (4) with equality replacing the inequality (as we are dealing with scalars, this is not difficult to achieve), the corresponding observer states z, z' satisfy

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

so that the bound of Proposition 3.1 is attained for this choice of A, C, L.

Comment The previous example demonstrates that it is possible for the upper bound for the l_1 sensitivity of the system (3) given in Proposition 3.1 to be exact for certain choices of A, C, L. Note also that the matrices A, C, L and $A - LC$ above are all nonnegative.

3.2 Relation to bounds given in Le Ny (2015)

Corollary 2 of Le Ny (2015), which applies to contractive nonlinear systems can be used to obtain an alternative expression for an upper bound of the l_1 sensitivity of (3). For comparison, we briefly describe how this earlier result relates to the bound in Proposition 3.1. We write M for the upper bound (7).

The bound in Le Ny (2015) is:

$$M_1 = \eta \left(\frac{1}{1-\gamma} - \frac{1}{1-\alpha}\right) \tag{12}$$

where $\eta > 0$ is arbitrary and, in our notation:

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

Manipulation of inequalities shows that

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

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 in (7). Further, it is important to note that we have shown that the bound (7) is attained for some systems.

4. POSITIVE OBSERVERS

In applications such as epidemiology and social network analysis, the underlying dynamical system is typically a positive system. When considering observer design for a positive system, it is natural to require that the observer system (3) and all the signals involved respect the positivity constraint of the underlying system (Ait Rami and Tadeo (2006); Hardin and van Schuppen (2007); Back and Astolfi (2008)). This defines the problem of *positive observer design* which is distinct to classical observer design due to the positivity constraint. In the remainder of this paper, we address the design of a positive observer that minimises the bound for the l_1 sensitivity given in Proposition 3.1.

The system (2) is positive if and only if the matrices A, C are nonnegative. The positive observer design problem (Ait Rami and Tadeo (2006)) is equivalent to: construct a matrix L such that $A - LC \geq 0$, $LC \geq 0$ and $\rho(A - LC) < 1$.

K and α are fixed parameters determined by the definition of adjacency (4) and the bound given by (7) is valid for L with $\|A - LC\| < 1$. With this in mind, we propose the following problem.

Problem 4.1. Given $A \in \mathbb{R}_+^{n\times n}$, $C \in \mathbb{R}_+^{p\times n}$, **minimise**

$$F(L) := \frac{\|L\|}{1 - \|A - LC\|} \tag{13}$$

subject to the constraints:

$$LC \geq 0\,, \; A - LC \geq 0, \; \|A - LC\| < 1 \tag{14}$$

If F^* is an optimal value for Problem 4.1, the minimal value of (7) is given by

$$\frac{K}{1-\alpha}F^*.$$

Comment: It is worth noting that the function F in general is not convex so algorithms for convex optimisation cannot be directly applied. Further, to the best of our knowledge, no prior work has been done on the specific question of minimising the l_1 sensitivity of positive Luenberger observers.

We next characterise the feasibility and solution of Problem 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 $L \geq 0$ (Ait Rami and Tadeo (2006)).

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 4.1 (the existence of a positive linear observer satisfying $\|A - lc^T\| < 1$) is straightforward. In the following result, we adopt the notational convention that $\frac{0}{0} = 0$ and $\frac{t}{0} = \infty$ for $t > 0$.

Proposition 4.1. Let $A \in \mathbb{R}_+^{n\times n}$, $c \in \mathbb{R}_+^n$, $c \neq 0$ be given. There exists some $l \in \mathbb{R}_+^n$ satisfying (14) if and only if

$$\sum_{i=1}^{n} \min_j \frac{a_{ij}}{c_j} > \max_j \frac{1}{c_j}\left(\sum_{i=1}^{n} a_{ij} - 1\right). \tag{15}$$

Proof. If such an l exists then it follows from $A - lc^T \geq 0$ that $l_i \leq \frac{a_{ij}}{c_j}$ for all j and hence $l_i \leq \min_j \frac{a_{ij}}{c_j}$. It now follows from $\|A - lc^T\| < 1$ that for all j

$$\begin{aligned}
&\sum_{i=1}^{n}(a_{ij} - l_i c_j) < 1\\
&\Rightarrow c_j \sum_{i=1}^{n} l_i > \sum_{i=1}^{n} a_{ij} - 1\\
&\Rightarrow c_j \sum_{i=1}^{n} \min_j \frac{a_{ij}}{c_j} > \sum_{i=1}^{n} a_{ij} - 1
\end{aligned}$$

and (15) follows immediately.

Conversely if (15) holds, then it is simple to check that the vector l defined by setting $l_i = \min_j \frac{a_{ij}}{c_j}$ will satisfy (14).

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 $\|L\| = \sum_{i=1}^{n} l_i$. We next note that in this case, the function F in (13) can be written in a simpler form.

Lemma 4.1. Given $A \in \mathbb{R}_+^{n\times n}$, $c, l \in \mathbb{R}^n$, we can write:

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

Proof. This is a simple calculation as:

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

as claimed.

Taken together, Lemma 4.1 and Proposition 4.1 show that for the single output case, minimising the l_1 sensitivity bound (7) reduces to the following uni-variate constrained optimisation problem.

Problem 4.2. **Minimise**

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

subject to

$$x \geq 0 \,\&\, \max_j \frac{1}{c_j}\left(\sum_{i=1}^{n} a_{ij} - 1\right) < x \leq \sum_{i=1}^{n} \min_j \frac{a_{ij}}{c_j} \tag{16}$$

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 $\mathcal{F}$ to denote the feasibility region defined by (16).

If we define

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

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

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

The discussion above suggests the following simple graphical scheme for solving Problem 4.2.

(1) Determine the feasibility region (16) from A and c.
(2) Plot each f_j in this region and mark off the graph of $f = \max f_j$.
(3) Find the point x^* where f attains its minimum in (16). This value of f will be the minimum of the l_1 sensitivity bound (7) for the positive observer problem.
(4) A vector l satisfying (15) 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.

All f_j concave

If $\sum_{i=1}^{n} a_{ij} < 1$ for all j, then as every f_j is strictly increasing, it is not hard to see that the optimal point for Problem 4.2 occurs at $x = 0$ corresponding to $l = 0$ and $\Delta(\mathcal{L}) = 0$. 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.

If $\sum_{i=1}^{n} a_{ij} = 1$ for some indices j, then $x = 0$ will again be an optimal point but in this case, the minimum of f will be given by $\max_{j \in J_1} \frac{1}{c_j}$ where J_1 is the set of those indices for which the column sum is equal to one.

All f_j convex

If $\sum_{i=1}^{n} a_{ij} > 1$ for all j, then as every f_j is strictly decreasing, it is not hard to see that the optimal point for Problem 4.2 occurs at the upper limit of the feasibility region, $x = \sum_{i=1}^{n} \min_j \frac{a_{ij}}{c_j}$, corresponding to the observer gain defined by $l_i = \min_j \frac{a_{ij}}{c_j}$ for $1 \le i \le n$. 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

In the case where $J_+ = \{j \mid \sum_{i=1}^{n} a_{ij} > 1\}$ and $J_- = \{j \mid \sum_{i=1}^{n} a_{ij} < 1\}$ are both non-empty, we proceed as follows. Determine all points of intersection x in $\mathcal{F}$ where $f_j(x) = f_k(x)$ for $j \in J_+$, $k \in J_-$. This amounts to solving a finite set of quadratic equations. If there are no such points in $\mathcal{F}$, then the optimal point will again occur at the upper limit of $\mathcal{F}$. Otherwise, the optimal point x^* will be one of the points of intersection.

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

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

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

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

If $\|A\| < 1$, then we minimise $F(l)$, by setting $l = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. In the case where $\|A\| \le 1$ and one column sum is equal to 1, the infimum of F 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 $\|A\| > 1$ and $\sum_{i=1}^{2} a_{ij} > 1$, for $j = 1, 2$, then the optimal observer gain is given by

$$l_1 = \min\left\{\frac{a_{11}}{c_1}, \frac{a_{12}}{c_2}\right\}, l_2 = \min\left\{\frac{a_{21}}{c_1}, \frac{a_{22}}{c_2}\right\}. \quad (17)$$

If $\|A\| > 1$ and $\sum_{i=1}^{2} a_{ij} < 1$, for some $j \in \{1, 2\}$, then let $x = \|L\|$ 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 $f_1(x) = \frac{x}{\alpha_1 + c_1 x}$ and $f_2(x) = \frac{x}{\alpha_2 + c_2 x}$. Setting

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

we find $x = 0$ 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 (17).

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 $l_1 \le \min\left\{\frac{a_{11}}{c_1}, \frac{a_{12}}{c_2}\right\}, l_2 \le \min\left\{\frac{a_{21}}{c_1}, \frac{a_{22}}{c_2}\right\}$ and $l_1 + l_2 = x$. This can be done by setting

$$l_1 = \min\{\min_j \frac{a_{ij}}{c_j}, x\}, \; l_2 = \max\{0, x - l_1\}.$$

The discussion of the previous paragraphs can readily be codified as an algorithm to find an optimal l for Problem 4.1 for 2-dimensional positive systems. While technically more involved, it is not too difficult to see how this may be extended to provide an algorithm for computing an optimal gain matrix for n-dimensional systems.

Example 4.1. Consider the system defined by

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

It is a straightforward computation to see that $\mathcal{F} = (\frac{1}{18}, \frac{7}{18}]$. 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 $x \in \mathcal{F}$, 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 1

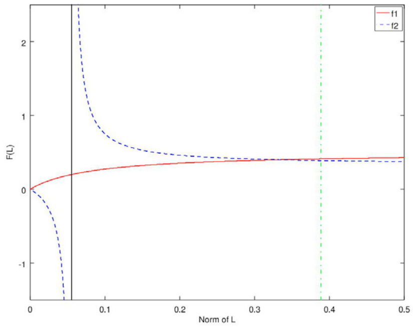

Fig. 1. This graph shows the intersection of the curves $f_1(x)$ and $f_2(x)$, is within the range for $\|L\| \in (\frac{1}{18}, \frac{7}{18}]$, where $\sum_{i=1}^{2} a_{i1} < 1$ and $\sum_{i=1}^{2} a_{i2} > 1$.

Figures 2 and 3 illustrate two of the other scenarios that can arise in the solution of Problem 4.2 for 2-d systems. In all figures, the limits of the feasible region $\mathcal{F}$ are indicated by vertical lines.

5. CONCLUSIONS AND FUTURE WORK

We have considered the design of differentially private positive linear observers and described how to minimise

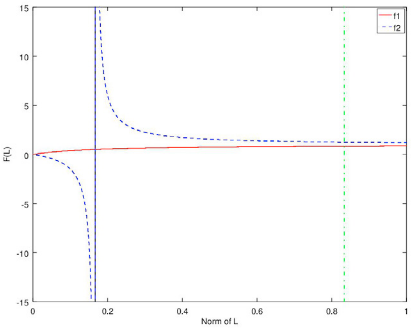

Fig. 2. This graph shows the intersection of the curves $f_1(x)$ and $f_2(x)$, is outside the range for $\|L\| \in (\frac{1}{6}, \frac{5}{6}]$, where $\sum_{i=1}^{2} a_{i1} < 1$ and $\sum_{i=1}^{2} a_{i2} > 1$

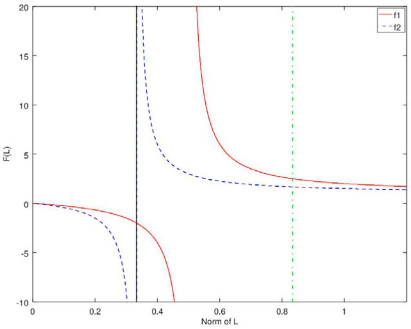

Fig. 3. This graph shows the curves $f_1(x)$ and $f_2(x)$, where $\sum_{i=1}^{2} a_{i1} > 1$ and $\sum_{i=1}^{2} a_{i2} > 1$.

a bound for the l_1 sensitivity of a positive Luenberger observer. We have also shown that this bound can be tight and explained how it relates to that given in Le Ny (2015).

It should be noted that even when we design an optimal positive observer in the sense of Problem 4.1, it is possible to violate the positivity constraint when we add Laplacian noise to the observer state z.

Example 5.1. Consider

$$A = \begin{pmatrix} 0.74905 & 0.76393 \\ 0.41093 & 0.29756 \end{pmatrix}, \; C = \begin{pmatrix} 0.61685 \\ 0.53626 \end{pmatrix}$$

We find that the optimal value for L is $L = (1.21431\ 0.55489)^T$ Using initial conditions: $x(0) = (6\ 17)^T$ and $z(0) = (23\ 28)^T$, $x(k)$, $y(k)$ and $z(k)$ will always be nonnegative. However using the optimal upper bound for the sensitivity of 3.988 and adding on Laplace noise with $\epsilon = 0.5$, $K = 1$ and $\alpha = 0.5$, it is possible to get negative values for $z'(k)$. For example, in one simulation run, we find $z'(1) = (-1.9324\ 15.5667)^T$ and $z'(2) = (26.1538\ -13.6552)^T$.

This motivates the following problem: design randomised mechanisms that deliver differential privacy for positive systems and still remain positive after the addition of noise.

A natural next step is to extend the work here to sensitivities with respect to other norms and corresponding mechanisms. For instance, can we bound l_2 sensitivity for positive systems and obtain a corresponding characterisation of near-optimal observers for mechanisms based on Gaussian noise? Another question concerns extensions to nonlinear positive systems and to systems with multiple outputs. These questions are the focus of ongoing work by the authors and we hope to publish results on them in the near future.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. David Malone and the anonymous reviewers and editor.

REFERENCES

Ait Rami, M. and Tadeo, F. (2006). Positive observation problem for linear discrete positive systems. *Proc. IEEE 45th Annual Conference on Decision and Control (CDC).*

Back, J. and Astolfi, A. (2008). Design of positive linear observers for positive linear systems via coordinate transformations and positive realizations. *SIAM J. Control & Opt.*, 47(1), 345–373.

Blanchini, F., Colaneri, P., and Valcher, M. (2015). Switched positive linear systems. *Foundations and Trends in Systems and Control*, 2(2), 101–273.

Dong, R., Krichene, W., Bayen, A.M., and Sastry, S.S. (2015). Differential privacy of populations in routing games. *Proc. IEEE 54th Annual Conference on Decision and Control (CDC).*

Dwork, C. (2006). Differential privacy. In *Proceedings of the 33rd Annual Interna- tional Colloquium on Automata, Languages and Programming, LNCS 4051*, 1–12. Springer-Verlag.

Fornasini, E. and Valcher, M. (2012). Stability and stabilizability criteria for discrete-time positive switched systems. *IEEE Tran. Aut. Cont.*, 57(5), 1208–1221.

Hardin, H. and van Schuppen, J. (2007). Observers for linear positive systems. *Lin. Alg. and its Appl.*, 425, 571–607.

Holohan, N., Leith, D., and Mason, O. (2015). Differential privacy in metric spaces: Numerical, categorical and functional data under the one roof. *Information Sciences*, 305(1), 256–268.

Horn, R. and Johnson, C. (2012). *Matrix Analysis.* Cambridge Univ. Press.

Le Ny, J. (2015). Privacy-preserving nonlinear observer design using contraction analysis. *Proc. IEEE 54th Annual Conference on Decision and Control (CDC).*

Le Ny, J. and Pappas, G. (2014). Differentially private filtering. *IEEE Tran. Aut. Cont.*, 59(2), 341–354.

Lucia, S., Kögel, M., Zometa, P., Quevedo, D.E., and Findeisen, R. (2016). Predictive control, embedded cyberphysical systems and systems of systems - a perspective. *Ann. Rev. in Cont.*, 1–15.

Shu, Z., Lam, J., Gao, H., Du, B., and Wu, L. (2008). Positive observers and dynamic output-feedback controllers for interval positive linear systems. *IEEE Tran. Circ. and Sys. I*, 55(10), 3209–3222.

Sontag, E. (1998). *Mathematical Control Theory.* Springer-Verlag.

Valcher, M. (1996). Controllability and reachability criteria for discrete time positive systems. *Int. J. of Cont.*, 65(3), 511–536.

Venkitasubramaniam, P. (2013). Decision making under privacy restrictions. *Proc. IEEE 52nd Annual Conference on Decision and Control (CDC).*