On assessing the disclosure risk of controlled adjustment methods for statistical tabular data

Jordi Castro
Dept. of Statistics and Operations Research
Universitat Politècnica de Catalunya
Jordi Girona 1–3, 08034 Barcelona, Catalonia
jordi.castro@upc.edu

Report DR 2012-07
August 2012

Report available from http://www-eio.upc.es/~jcastro

ON ASSESSING THE DISCLOSURE RISK OF CONTROLLED ADJUSTMENT METHODS FOR STATISTICAL TABULAR DATA*

JORDI CASTRO

Department of Statistics and Operations Research, Universitat Politècnica de Catalunya
Jordi Girona 1–3, 08034 Barcelona, Catalonia

jordi.castro@upc.edu

Minimum distance controlled tabular adjustment is a recent perturbative approach for statistical disclosure control in tabular data. Given a table to be protected, it looks for the closest safe table, using some particular distance. Controlled adjustment is known to provide high data utility. However, the disclosure risk has only been partially analyzed using theoretical results from optimization. This work extends these previous results, providing both a more detailed theoretical analysis, and an extensive empirical assessment of the disclosure risk of the method. A set of 25 instances from the literature and four different attacker scenarios are considered, with several random replications for each scenario, both for L_1 and L_2 distances. This amounts to the solution of more than 2000 optimization problems. The analysis of the results shows that the approach has low disclosure risk when the attacker has no good information on the bounds of the optimization problem. On the other hand, when the attacker has good estimates of the bounds, and the only uncertainty is in the objective function (which is a very strong assumption), the disclosure risk of controlled adjustment is high and it should be avoided.

Keywords: Statistical disclosure control; Controlled tabular Adjustment; Disclosure risk; Optimization; Linear programming; Quadratic programming.

1. Introduction

Statistical data has to be protected before publication to guarantee that sensitive and confidential information of individuals is not released. There are several techniques available, both for microdata and for tabular data. Formally, a microdata set can be defined as a function

$$V : I \rightarrow D(V_1) \times D(V_2) \times \cdots \times D(V_t)$$

that maps individuals of set I to an array of t values for variables $V_1,\ldots, V_t$, $D()$ being the domain of those variables. Categorical variables have a discrete domain, whereas numerical variables can be both discrete or continuous. Tabular data is obtained by crossing one or more categorical variables. Formally, a table is a function

$$T : D(V_{i_1}) \times D(V_{i_2}) \times \cdots \times D(V_{i_l}) \rightarrow \mathbb{R} \text{ or } \mathbb{N},$$

l being the number of categorical variables that were crossed. The result of function T (cell values) belongs to $\mathbb{N}$ for a frequency table, and to $\mathbb{R}$ for a magnitude table.

*To appear in the *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*

For instance, the two-dimensional frequency table crossing the categorical variables "sex" and "smoke?" could be defined as $T : \{\text{"male"}, \text{"female"}\} \times \{\text{"yes"}, \text{"no"}\} \to \mathbb{N}$. Recent surveys and monographs provide detailed information about the different table structures, and, in general, about the statistical disclosure field. [3,4,14]

Any tabular data protection method can be seen as a map F such that $F(T) = T'$, i.e., table T is transformed to another table T' which is safe and, ideally, with minimum information loss. For the method to exhibit a low disclosure risk, the inverse map $T = F^{-1}(T')$ should not be available or difficult to compute by any attacker. Note that this applies to all the cells, since T was defined as a function whose domain are all the table cells.

Controlled adjustment methods [2,11] are an emerging technology for tabular data. [14] They have shown to perform well compared to other techniques in terms of efficiency and quality of the solution.[4,5] Given a table T the purpose is to obtain T' by solving an optimization problem that finds the closest table T' to T meeting some safety linear constraints.

The particular controlled adjustment method named *controlled tabular adjustment* (CTA) only considered L_1 norms and safety was obtained by disjunctive constraints that forced sensitive cells to be shifted either upward or downward; this decision was added to the problem through binary variables.[11] Other norms, such as L_2 and L_∞, were suggested in similar approaches where the protection sense (upper or lower) was a priori fixed resulting in more efficient continuous optimization problems.[2] This will be the scheme adopted in this work.

Controlled adjustment methods will have low disclosure risk if no attacker can obtain a good estimate $\hat{T} = \hat{F}^{-1}(T')$, $\hat{F}^{-1}$ being an estimate of F^{-1}. An incomplete theoretical analysis of the disclosure risk of minimum distance controlled adjustment methods has already been presented in previous works.[2] However they were based on a sensitivity analysis for only some coefficients of the optimization problem, not all of them. In addition, an empirical exhaustive analysis has not been made before to show the disclosure risk of the approach. This is specially relevant since some authors claim that protection approaches based on the minimization of information loss are not safe if a *minimality attack* is performed.[9] However, minimality attacks have been used for microdata, not for tabular data (e.g., the term table was used for "table in a relational database" not for "statistical table").[9] The purpose of this paper is to fill this gap by (1) providing a detailed attacker problem, considering several risk scenarios; (2) presenting a complete theoretical analysis of the disclosure risk of controlled adjustment; (3) presenting an exhaustive empirical evaluation of the disclosure risk of these approaches, by solving more than 2500 optimization attacker problems. As it will be shown, when the attacker has no good information about the original data, the disclosure risk is low. As expected, the computational results also confirmed that the more information by the attacker, the higher is the disclosure risk. And for certain scenarios with very well informed attackers (which in practice can be a very strong assumption), the method should not be recommended.

The paper is organized as follows. Section 2 provides a general formulation of

controlled adjustment methods, for L_1 and L_2. Section 3 formulates the problem the attacker should solve to re-compute the original data, and it describes several attacker scenarios. Sections 4 and 5 show, respectively, a theoretical and empirical analysis of the disclosure risk of the approach.

2. Formulation of the controlled adjustment approach

Any variant of controlled adjustment can be formulated from the following parameters:

- A set of cells $a_i, i \in \mathcal{N} = \{1, \ldots, n\}$, that satisfy $\mathcal{M} = \{1, \ldots, m\}$ linear relations $Ta = b$ (a being the vector of a_i's), $T \in \mathbb{R}^{m \times n}$ being the matrix representing the tabular constraints. Each tabular constraint imposes that the inner cells have to be equal to the total or marginal cell, i.e., if $\mathcal{I}_j \subset \mathcal{N}$ is the set of indices of inner cells of relation j, and t_j is the index of the total cell of relation j, $j \in \mathcal{M}$, the constraint associated to this relation is $\left(\sum_{i \in \mathcal{I}_j} a_i\right) - a_{t_j} = 0$.
- A lower and upper bound for each cell $i \in \mathcal{N}$, respectively l_{a_i} and u_{a_i}, which are considered to be known by any individual/attacker. If no previous knowledge is assumed for cell i and the table is positive (i.e., negative cell values are not allowed) then default bounds would be $l_{a_i} = 0$ and $u_{a_i} = +M$, $M \gg 0$ being a large value. For non-positive tables $l_{a_i} = -M$ can be used.
- Nonnegative cell weights $w_i, i \in \mathcal{N}$, needed to define the distance between the original and the perturbed released cell values. They are used in the objective function of the resulting optimization problem. Cell weights are usually a function of the cell value, i.e., $w_i(a_i)$. This dependence will only be explicited when needed in the rest of the paper.
- A set $\mathcal{S} = \{i_1, i_2, \ldots, i_s\} \subseteq \mathcal{N}$ of indices of confidential or sensitive cells. This set of cells is a priori selected using some sensitivity rules, such as the the (n-k) dominance rule, or the p% rule. These rules, out of the scope of this work, are discussed in some of the references.[3,10,12,14].
- Nonnegative lower and upper protection levels for each confidential cell $i \in \mathcal{S}$, respectively lpl_i and upl_i, such that the released values should be out of the interval $(a_i - lpl_i, a_i + upl_i)$. Depending on how this constraint is dealt with, several controlled adjustment variants can be obtained. For instance if we consider the disjunctive constraint "either $x_i \geq a_i + upl_i$ or $x_i \leq a_i - lpl_i$", the resulting method is known as *controlled tabular adjustment* (CTA)[11], and it results in a difficult combinatorial optimization problem. If, on the other hand, a protection sense is fixed, i.e., one of the two members of the disjunction is a priori selected, it results in a continuous optimization problem.[2] It is worth to mention that the protection levels lpl_i and upl_i are either computed as a certain fraction of the sensitive cell

value a_i, or directly derived from the sensitivity rules that provide the set of sensitive cells $\mathcal{S}$.[14] In both cases, the protection levels implicitly depend on the cell value, i.e., $lpl_i(a_i)$ and $upl_i(a_i)$. As for the cell weights, in the rest of the work this dependence will only be clearly shown when needed.

The controlled adjustment method attempts to find the closest values $x_i, i \in \mathcal{N}$ —according to some distance $L(w)$, $w \in \mathbb{R}^n$ being the vector of cell weights—, that make the released table safe. This involves the solution of the following optimization problem:

$$\min_x \quad ||x - a||_{L(w)} \tag{1a}$$

$$\text{s. to} \quad Tx = b \tag{1b}$$

$$l_{a_i} \leq x_i \leq u_{a_i} \quad i \in \mathcal{N} \tag{1c}$$

$$x_i \text{ for all } i \in \mathcal{S} \text{ are safe values.} \tag{1d}$$

The formulation of (1d) depends on the particular controlled adjustment variant considered. For instance, in the standard CTA approach, this constraint is

$$(x_i \leq a_i - lpl_i) \text{ or } (x_i \geq a_i + upl_i) \quad i \in \mathcal{S}, \tag{2}$$

which, by introducing a vector of binary variables $y \in \mathbb{R}^s$ can be written as

$$\begin{array}{ll} x_i \geq -M(1 - y_i) + (a_i + upl_i)y_i & i \in \mathcal{S}, \\ x_i \leq My_i + (a_i - lpl_i)(1 - y_i) & i \in \mathcal{S}, \\ y_i \in \{0, 1\} & i \in \mathcal{S}, \end{array} \tag{3}$$

$0 \ll M \in \mathbb{R}$ being a large positive value. Constraints (3) impose either "upper protection sense" $x_i \geq a_i + upl_i$, when $y_i = 1$, or "lower protection sense" $x_i \leq a_i - lpl_i$ when $y_i = 0$. The CTA problem (1a)–(1c), (3) is a mixed integer linear optimization problem (MILP), which can be time consuming for medium-large instances.

An alternative would be to a priori fix the binary variables $y_i, i \in \mathcal{S}$, thus obtaining a CTA formulation with only continuous variables, as suggested in previous works.[2] Although this variant will provide a solution with a higher information loss (since it does not explore all the possible combinations of binary variables), the resulting optimization problem will be solved much more efficiently. Thus, it is specially suited for the real-time protection in on-line tabular data servers.[7] In this work we will focus on this continuous controlled adjustment method. It is worth to note that if this variant is shown to be "safe", the problem with binary variables would also be "safe" (even "safer"), since in the former case the decision on the particular value of y_i is governed by a combinatorial optimization procedure (impossible to be reproduced if the values a are not completely known), and not a priori fixed by some rule. Possible infeasibilities in the resulting problem due to the particular choices of y_i, $i \in \mathcal{S}$, could be treated with approaches for fixing infeasible instances in optimization.[8] Some of them have already been used in the context of CTA.[6] Formulating problem (1) in terms of cell deviations $z = x - a$,

$z \in \mathbb{R}^n$, and fixing the binary variables, the resulting continuous CTA problem can be formulated as the general convex optimization problem

$$\begin{array}{ll} \min\limits_{z} & ||z||_{L(w)} \\ \text{s. to} & Tz = 0 \\ & l(a) \leq z \leq u(a), \end{array} \tag{4}$$

where

$$\begin{aligned} l_i(a_i) &= \begin{cases} upl_i(a_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ l_{a_i} - a_i & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0) \end{cases} \\ u_i(a_i) &= \begin{cases} -lpl_i(a_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ u_{a_i} - a_i & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1), \end{cases} \end{aligned} \tag{5}$$

for $i \in \mathcal{N}$. Note we made explicit the relation $l(a)$, $u(a)$ in (4)–(5). It is worth to mention that the a priori assignment of y_i to either 0 or 1 should always be the same if cell $i \in \mathcal{S}$ appears in two different tables, otherwise we could be both disclosing information and providing inconsistent tables (the same cell would appear with two different values in two released tables). This can be avoided if the value for y_i is computed from local information to the cell, e.g., from the set of respondents or contributors to this particular cell.[7] A particular implementation of this general idea is based on the use of *microdata keys*.[13]

Problem (4) can be specialized for several norms, L_1 and L_2 being the two most relevant. For L_1, defining $z = z^+ - z^-$, we obtain the following linear optimization problem (LP):

$$\begin{array}{ll} \min\limits_{z^+, z^-} & \sum\limits_{i=1}^{n} w_i(a_i)(z_i^+ + z_i^-) \\ \text{s. to} & T(z^+ - z^-) = 0 \\ & l^+(a) \leq z^+ \leq u^+(a) \\ & l^-(a) \leq z^- \leq u^-(a), \end{array} \tag{6}$$

$w(a) \in \mathbb{R}^n$ being a vector of nonnegative cell weights, $z^+ \in \mathbb{R}^n$ and $z^- \in \mathbb{R}^n$ the vector of positive and negative deviations in absolute value, and $l^+(a), l^-(a), u^+(a), u^-(a) \in \mathbb{R}^n$ lower and upper bounds for the positive and nega-

tive deviations defined as

$$
\begin{aligned}
l_i^+(a_i) &= \begin{cases} upl_i(a_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ 0 & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0) \end{cases} \\
u_i^+(a_i) &= \begin{cases} 0 & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ u_{a_i} - a_i & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1) \end{cases} \\
l_i^-(a_i) &= \begin{cases} lpl_i(a_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ 0 & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1) \end{cases} \\
u_i^-(a_i) &= \begin{cases} 0 & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ a_i - l_{a_i} & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0), \end{cases}
\end{aligned}
\tag{7}
$$

for $i \in \mathcal{N}$. For L_2, problem (4) can be directly recast as the following quadratic optimization problem (QP) without introducing additional variables:

$$
\begin{aligned}
\min_z \quad & \sum_{i=1}^{n} w_i(a_i) z_i^2 \\
\text{s. to} \quad & Tz = 0 \\
& l(a) \le z \le u(a).
\end{aligned}
\tag{8}
$$

In practice, values $w_i = 1/a_i$ and $w_i = 1/a_i^2$ are sensible choices for respectively L_1 and L_2, such that the objective function models the sum of relative deviations in (6) and relative deviations to square in (8). These will be the values used in Section 5 for the computational results.

3. Formulation of the attacker problem

Once either problem (6) or (8) has been solved, the released cell values are $x = a + z$. To recompute the original values a, the attacker should know z, i.e, the solution of either (6) or (8). For this purpose, the attacker should know all the parameters of the above optimization problems. In practice, however, once the table is published, the attacker only knows

- the released values x;
- the structure of the table, that is, the constraint matrix T.

For the rest of parameters the attacker may only have partial information:

- the particular distance used may be unknown, that is, which of the two problems were solved by the data protector, either (6) or (8); however, providing information about the distance used may be seen as a good practice, so we considered it is known by the attacker;
- cell weights $w(a)$ are unknown, since they depend on the original data;
- the lower and upper bounds ($l^+(a), l^-(a), u^+(a), u^-(a)$ in (6), $u(a)$, $l(a)$ in (8)) are unknown because: (i) they depend on a; (ii) the set of sensitive

cells $\mathcal{S}$ is unknown to the attacker; (iii) the a priori assignment of y_i will also be unknown to the attacker.

The goal of the attacker is then to obtain a *good* estimate $\hat{a}$ of a. In this context, a *good* estimate may have two meanings: either to obtain the original value a_i for some sensitive cell, or —the weaker condition— a value not too far from a_i. Both meanings will be analyzed in the computational results. To get such an estimate the attacker should try to recompute $\hat{a}$ from x by using that $x = a + z$ was obtained from the solution of (1)–(2). From (2), the problem to be solved by the attacker is thus

$$\begin{array}{ll} \min\limits_{\hat{a}} & ||\hat{a} - x||_{L(w)} \\ \text{s. to} & T\hat{a} = b \\ & l_{a_i} \leq \hat{a}_i \leq u_{a_i} \quad i \in \mathcal{N} \\ & (\hat{a}_i \leq x_i - upl_i) \text{ or } (\hat{a}_i \geq x_i + lpl_i) \quad i \in \mathcal{S}. \end{array} \tag{9}$$

Defining $\hat{z} = x - \hat{a}$ as the estimate of the cell deviations, such that $x - \hat{z} = (a+z) - \hat{z} = \hat{a}$, problem (9) can be formulated in terms of $\hat{z}$ as

$$\begin{array}{ll} \min\limits_{\hat{z}} & ||\hat{z}||_{L(w)} \\ \text{s. to} & T\hat{z} = 0 \\ & \hat{l}(x) \leq \hat{z} \leq \hat{u}(x), \end{array} \tag{10}$$

where

$$\begin{aligned} \hat{l}_i(x_i) &= \begin{cases} upl_i(x_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ x_i - u_{a_i} & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0) \end{cases} \\ \hat{u}_i(x_i) &= \begin{cases} -lpl_i(x_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ x_i - l_{a_i} & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1), \end{cases} \end{aligned} \tag{11}$$

for $i \in \mathcal{N}$. Note that the data protector and attacker problems (4) and (10) are very similar, the only change being the definition of the bounds (5) and (11), which depend on a_i and x_i, respectively. This also holds for the upper and lower protection levels, which are a function of a_i in (5) and of x_i in (11). Specializing the general model (10), the final problem to be solved by the attacker for L_1would be

$$\begin{array}{ll} \min\limits_{\hat{z}^+, \hat{z}^-} & \sum\limits_{i=1}^{n} w_i(x_i)(\hat{z}_i^+ + \hat{z}_i^-) \\ \text{s. to} & T(\hat{z}^+ - \hat{z}^-) = 0 \\ & \hat{l}^+(x) \leq \hat{z}^+ \leq \hat{u}^+(x) \\ & \hat{l}^-(x) \leq \hat{z}^- \leq \hat{u}^-(x), \end{array} \tag{12}$$

where

$$\hat{l}_i^+(x_i) = \begin{cases} upl_i(x_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ 0 & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0) \end{cases}$$

$$\hat{u}_i^+(x_i) = \begin{cases} 0 & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ x_i - l_{a_i} & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1) \end{cases}$$

$$\hat{l}_i^-(x_i) = \begin{cases} lpl_i(x_i) & \text{if } i \in \mathcal{S} \text{ and } y_i = 0 \\ 0 & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 1) \end{cases} \tag{13}$$

$$\hat{u}_i^-(x_i) = \begin{cases} 0 & \text{if } i \in \mathcal{S} \text{ and } y_i = 1 \\ u_{a_i} - x_i & \text{if } (i \in \mathcal{N} \setminus \mathcal{S}) \text{ or } (i \in \mathcal{S} \text{ and } y_i = 0), \end{cases}$$

for $i \in \mathcal{N}$. For L_2 the attacker problem would be

$$\begin{aligned} \min_{\hat{z}} \ & \sum_{i=1}^{n} w_i(x_i)\hat{z}_i^2 \\ \text{s. to } \ & T\hat{z} = 0 \\ & \hat{l}(x) \le \hat{z} \le \hat{u}(x), \end{aligned} \tag{14}$$

$\hat{l}(x)$, $\hat{u}(x)$ defined as in (11). Note that $w_i(x_i)$ instead of $w_i(a_i)$ were used in the objective functions of (12) (14) since a_i are unknown to the attacker. Similar derivations could be done for more general perturbation approaches (e.g., combining stochastic noise with controlled adjustment).

Problems (6) and (12) for L_1, and (8) and (14) for L_2 to be solved by the data protector and attacker only differ in the objective function ($w_i(a_i)$ vs $w_i(x_i)$) and the bounds ((7) vs (13), and (5) vs (11)). If the attacker had full information about the objective and bounds the solution of the problem would be $\hat{z} = z$. However he/she has to approximate the values that depend on a (objective function weights and bounds on variables) from x. To estimate bounds from x, the attacker should also know:

- how the protection levels upl_i and lpl_i depend on a, to use the same rule for x;
- the cell bounds l_{a_i} and u_{a_i}, or rather, the difference $a_i - l_{a_i}$ and $u_{a_i} - a_i$ $i \in \mathcal{N}$;
- the set of sensitive cells $\mathcal{S}$;
- the values $y_i \in \{0, 1\}$ used by the data protector.

Therefore, we may consider different scenarios according to the knowledge of the attacker. In this work (in particular, in the computational results of Section 5) we will consider the four following scenarios (where "B" and "C" are related to, respectively, changes in Bounds and Costs of the optimizations problems):

B. The attacker has incomplete information about both the bounds and objective function. We have three subscenarios, listed below. In all these sub-

scenarios we assume the attacker knows the subset $\mathcal{S}$ of sensitive cells, and the original cell bounds l_{a_i} and u_{a_i}, $i \in \mathcal{N}$ (which are quite strong assumptions), but not $a_i - l_{a_i}$ and $u_{a_i} - a_i$ $i \in \mathcal{N}$.

B1. The attacker neither knows the protection levels $upl_i, lpl_i, i \in \mathcal{S}$, nor the protection sense $y_i \in \{0,1\}, i \in \mathcal{S}$.

B2. The attacker knows the protection sense $y_i \in \{0,1\}, i \in \mathcal{S}$, but not the protection levels upl_i, lpl_i, $i \in \mathcal{S}$.

B3. The attacker knows both the protection sense $y_i \in \{0,1\}$ and protection levels upl_i, lpl_i, $i \in \mathcal{S}$. The only unknown terms to reproduce the real bounds are then $a_i - l_{a_i}$ and $u_{a_i} - a_i$, $i \in \mathcal{N}$.

C. The attacker has complete information about the bounds, i.e, he/she knows $\hat{l}_i(a_i), \hat{u}_i(a_i), \hat{l}_i^+(a_i), \hat{u}_i^+(a_i), \hat{l}_i^-(a_i), \hat{u}_i^-(a_i), i \in \mathcal{N}$, and the only uncertainty is in the use of $w_i(x_i)$ instead of $w_i(a_i)$. Note this is a very strong assumption, since it means the attacker knows or has accurate information about the original cell values a.

In addition, since the attacker knows x is a perturbation or adjustment of the true value a, he/she may try to consider different values $\tilde{x}$ around x (either randomly, or using some distribution for x if this information is at hand for some particular data) to get a closer estimate $\hat{z}$. Therefore we will consider that several attacker problems (12) and (14) for $w(\tilde{x})$, $\hat{l}(\tilde{x})$, $\hat{u}(\tilde{x})$, $\hat{l}^+(\tilde{x})$, $\hat{u}^+(\tilde{x})$, $\hat{l}^-(\tilde{x})$ and $\hat{u}^-(\tilde{x})$ will be solved by the attacker.

If the solutions of the data protector and attacker problems are close, the method will have a high disclosure risk. As shown above, both problems only differ in the objective function and in the lower and upper bounds. The question is thus how close will be both solutions? Next two sections answer this question theoretically and empirically, respectively.

4. Theoretical analysis of the disclosure risk

The attacker problems (12) and (14) and the data protector problems (6) and (8) only differ in the objective function weights, and in the upper and lower bounds. The attacker problem can thus be seen as a perturbed version of the data protector problem, and could be written, in general, as the following convex optimization problem:

$$\begin{aligned} f(\epsilon_w, \epsilon_l, \epsilon_u) = \min_z \ & ||z||_{L(w+\epsilon_w)} \\ \text{s. to } & Tz = 0 \\ & l + \epsilon_l \leq z \leq u + \epsilon_u, \end{aligned} \tag{15}$$

where $\epsilon_w, \epsilon_l, \epsilon_u, \in \mathbb{R}^n$ denote the perturbation of the weights and lower and upper bounds. Although we will focus on the general model (15), we also provide the

explicit perturbed formulation for the L_1 and L_2 norms:

$$\begin{array}{ll} \min\limits_{z^+,z^-} & (w+\epsilon_w)^T z^+ + (w+\epsilon_w)^T z^- \\ \text{s. to} & T(z^+ - z^-) = 0 \\ & l^+ + \epsilon_l^+ \leq z^+ \leq u^+ + \epsilon_u^+ \\ & l^- + \epsilon_l^- \leq z^- \leq u^- + + \epsilon_l^-, \end{array} \tag{16}$$

for L_1, and

$$\begin{array}{ll} \min\limits_{z} & z^T(W+E)z \\ \text{s. to} & Tz = 0 \\ & l + \epsilon_l \leq z \leq u + \epsilon_u \end{array} \tag{17}$$

for L_2, where $\epsilon_u, \epsilon_l^+, \epsilon_u^+, \epsilon_l^-, \epsilon_u^- \in \mathbb{R}^n$, and $W = \text{diag}(w) \in \mathbb{R}^{n\times n}$, $E = \text{diag}(\epsilon) \in \mathbb{R}^{n\times n}$ are diagonal matrices,

Problem (15) consists on the minimization of a convex objective function over a feasible region defined by the polyhedral set $S = \{z \in \mathbb{R}^n : Tz = 0, l + \epsilon_l \leq z \leq u+\epsilon_u\}$. S is bounded since all variables are lower and upper bounded. f is also lower bounded by 0, since it is the minimization of a norm. For $(\epsilon_w, \epsilon_l, \epsilon_u) = (0, 0, 0)$, (15) is equal to (4) and provides the protected solution of optimal objective function $f(0, 0, 0)$. If $(\epsilon_w, \epsilon_l, \epsilon_u) \neq (0, 0, 0)$ we will obtain a different solution, of optimal objective $f(\epsilon_w, \epsilon_l, \epsilon_u)$. Optimization theory provides several information about f, which are summarized without proof in the following theorem:[1,16]

Theorem 1. *Given the convex optimization problem (15), then*

(1) The optimal objective f is a convex function of ϵ_l, ϵ_u.
(2) If the objective function is linear (L_1 norm), then f is a piecewise linear convex function of ϵ_l, ϵ_u.
(3) The optimal objective f is a concave function of ϵ_w.
(4) If the objective function is linear (L_1 norm), then f is a piecewise linear concave function of ϵ_w.
(5) If $\mu_l \in \mathbb{R}^n$ and $\mu_u \in \mathbb{R}^n$ are the nonnegative Lagrange multiplier vectors of the inequalities (lower and upper bounds, respectively), then the local change of f at $(\epsilon_w, \epsilon_l, \epsilon_u) = (0, 0, 0)$ is

$$\nabla_{\epsilon_l} f(\epsilon_w, \epsilon_l, \epsilon_u) = -\mu_l \quad \nabla_{\epsilon_u} f(\epsilon_w, \epsilon_l, \epsilon_u) = \mu_u. \tag{18}$$

From Theorem 1, perturbations in the bounds change the objective function according to the Lagrange multipliers μ_l and μ_u of the bounds constraints. Since both bounds can not be active (except when they are the same, but in this case the value $z_i, i \in \mathcal{N}$, is fixed and it is no longer a variable), we have from the optimality conditions of an optimization problem that either $\mu_{l_i} = 0$ or $\mu_{u_i} = 0$, $i \in \mathcal{N}$. If the one-norm of the vector (μ_l, μ_u) (information reported in Table 1 of Section 5 for all the test instances) is close to 0, then the optimal solution may not be affected by small changes in the bounds. In general, however, even small changes to the bounds

would change the optimal solution. This result only gives a local explanation; it does not explain what would happen to the optimal solution when the perturbations are large. This analysis is better done empirically, as in below Section 5, using the scenarios B1, B2 and B3 described in Section 3.

Clearly, changes in the weights due to ϵ_w also affect the optimal objective. As in the case of changes in the bounds due to ϵ_l , ϵ_u, our interest is in the optimal solution, not the optimal objective. However the situation is now a bit different: changes in the active bounds would in general mean a different solution, but this may not happen when we change the objective function (mainly if the change is small). For instance, for LPs (L_1 norm), optimal solutions are found in a vertex of the feasible polyhedral set S, and this vertex can be optimal for several similar objective functions. For QPs (L_2) the situation is not so straightforward; the optimal solution may be even in the interior of S. Section 5 analyzes this situation, which corresponds to the scenario C of Section 3. As suggested by theory, it will be shown that the values obtained by the attacker are equal to the true values in many cases for L_1 and scenario C (considering small changes in the weights); therefore, for scenario C, the disclosure risk of the method is very high.

Table 1. Dimensions, solution times of all the runs, and $||\mu||_1$, for the test instances.

					L_1		L_2	
instance	n	s	m	nz	CPU	$\|\|\mu\|\|_1$	CPU	$\|\|\mu\|\|_1$
australia_ABS	24420	918	274	13224	55.43	97.12	36.16	0
bts4	36570	2260	36310	136912	1219.97	10.8	1006.14	0
cbs	11163	2467	244	22326	29.26	270.69	51.95	24.19
dale	16514	4923	405	33028	102.23	2811.44	74.98	26.69
destatis	5940	621	1464	18180	185.32	43.23	254.98	20.26
hier13	2020	112	3313	11929	127.19	0.72	88.25	0
hier13x13x13a	2197	108	3549	11661	73.5	1.4	85.43	0.02
hier13x13x7d	1183	75	1443	5369	36.2	0.84	27.02	0
hier13x7x7d	637	50	525	2401	6.53	0.35	6.19	0
hier16	3564	224	5484	19996	541.69	1.78	429.36	0
hier16x16x16a	4096	224	5376	21504	676.15	5.44	607.93	0.04
nine12	10399	1178	11362	52624	1559.99	5.02	1105.86	0
nine5d	10733	1661	17295	58135	885.92	10.54	1172.9	0
ninenew	6546	858	7340	32920	832.61	3.94	909.22	0
osorio	10201	7	202	20402	59.6	9.38	30.54	0.01
table1	1584	146	510	4752	16.07	16.95	11.13	0
table3	4992	517	2464	19968	335.48	1298.26	443.69	25.75
table4	4992	517	2464	19968	331.77	1298.26	430.72	25.75
table5	4992	517	2464	19968	330.61	1298.26	429.31	25.75
table6	1584	146	510	4752	15.19	16.94	12.3	0
table7	624	17	230	1872	6.78	20.27	4.69	29.49
table8	1271	3	72	2542	6.88	0.08	4.75	0
targus	162	13	63	360	1.82	4.15	1.53	0.46
toy3dsarah	2890	376	1649	9690	95.52	0	73.05	0
two5in6	5681	720	9629	34310	345.26	7.4	368.32	0

5. Empirical analysis of the disclosure risk

For the empirical assessment we have considered a set of both real and synthetic 25 instances widely used in the literature about statistical data protection.[2,4] They can be obtained from `http://webpages.ull.es/users/casc/#CSPlib:`. Table 1 shows the main dimensions of these tables: number of cells (column n), number or sensitive cells (s), number of tabular constraints (m), and number of nonzero coefficients in the matrix of tabular constraints ("nz").

Table 2. Results for scenario B1 and norm L_1. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	0.0	1.2	1.3	37.4	5.9	6.3	10.3	37.3
bts4	0.0	9.1	24.0	24.8	20.5	19.3	2.1	0.1
cbs	0.0	4.3	4.6	8.8	8.4	19.6	32.9	21.4
dale	0.0	4.0	4.0	8.1	9.7	15.5	24.4	34.3
destatis	0.0	15.3	17.1	23.7	18.6	17.1	6.6	1.6
hier13	0.0	28.3	15.5	26.5	17.8	11.2	0.7	0.0
hier13x13x13a	0.0	28.7	14.6	26.5	20.5	9.5	0.2	0.0
hier13x13x7d	0.0	22.0	15.2	19.1	22.8	18.4	2.5	0.0
hier13x7x7d	0.0	17.2	22.0	20.8	22.4	16.6	1.0	0.0
hier16	0.0	22.2	20.0	20.9	19.2	16.5	1.1	0.1
hier16x16x16a	0.0	22.1	21.2	19.7	19.2	16.6	1.2	0.0
nine12	0.0	17.2	14.4	23.2	22.8	20.0	2.0	0.3
nine5d	0.0	21.3	20.4	27.2	19.9	10.8	0.4	0.0
ninenew	0.0	19.5	14.7	22.1	22.2	18.8	2.2	0.5
osorio	0.0	7.1	8.6	20.0	11.4	25.7	12.9	14.3
table1	0.0	17.3	17.5	21.8	23.5	14.7	2.6	2.7
table3	0.0	9.0	13.8	27.2	17.8	20.8	7.5	4.0
table4	0.0	9.0	13.8	27.2	17.8	20.8	7.5	4.0
table5	0.0	9.0	13.8	27.2	17.8	20.8	7.5	4.0
table6	0.0	17.3	17.4	21.8	23.4	14.7	2.6	2.7
table7	0.0	1.8	0.0	0.0	1.2	1.8	3.5	91.8
table8	0.0	16.7	10.0	20.0	20.0	30.0	3.3	0.0
targus	0.0	9.2	3.1	7.7	15.4	34.6	29.2	0.8
toy3dsarah	0.0	28.0	12.5	22.8	18.5	14.2	3.3	0.6
two5in6	0.0	18.8	21.4	26.8	20.3	12.0	0.7	0.2

Each instance was first protected by solving both (6) for L_1 and (8) for L_2, using some a priori assignment of the binary variables (they were set to 1 for all the sensitive cells). Note that no infeasibilities appeared in this phase. Weights $w_i = 1/a_i$ and $w_i = 1/a_i^2$ were used for L_1 and L_2, respectively. From Theorem 1, the local change in the objective function due to small changes in the lower and upper bounds is governed by the Lagrange multipliers associated to these bounds. Columns $||\mu||_1$ of Table 1 show the one-norm of the vector of Lagrange multipliers (μ_l, μ_u), for the L_1 and the L_2 problems. The zero values which appear are indeed

Table 3. Results for scenario B1 and norm L_2. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	0.0	3.4	3.7	10.3	7.9	12.3	19.1	43.2
bts4	0.0	12.2	21.0	24.5	20.6	19.4	2.1	0.1
cbs	0.0	4.3	4.6	8.8	8.4	19.2	33.1	21.6
dale	0.0	4.0	4.0	8.1	9.7	15.5	24.4	34.3
destatis	0.0	9.0	9.3	23.1	22.6	24.4	9.5	2.1
hier13	0.0	25.4	17.3	27.8	17.8	11.1	0.7	0.0
hier13x13x13a	0.0	26.1	16.9	27.0	19.9	9.8	0.3	0.0
hier13x13x7d	0.0	19.7	13.6	23.1	22.7	18.1	2.8	0.0
hier13x7x7d	0.0	15.4	18.4	25.2	23.4	16.6	1.0	0.0
hier16	0.0	21.1	17.3	24.2	19.6	16.6	1.1	0.1
hier16x16x16a	0.0	19.2	19.8	23.9	19.2	16.8	1.0	0.0
nine12	0.0	15.1	14.7	24.7	23.3	20.1	1.8	0.3
nine5d	0.0	19.6	20.8	28.5	19.9	10.7	0.5	0.0
ninenew	0.0	15.8	14.7	24.2	22.6	19.8	2.5	0.5
osorio	0.0	2.9	5.7	12.9	11.4	20.0	18.6	28.6
table1	0.0	6.8	8.4	21.6	23.8	31.0	5.7	2.7
table3	0.0	11.1	13.2	23.0	19.4	21.5	7.8	4.1
table4	0.0	11.1	13.2	23.0	19.4	21.5	7.8	4.1
table5	0.0	11.1	13.2	23.0	19.4	21.5	7.8	4.1
table6	0.0	7.0	9.0	19.9	19.1	28.8	10.8	5.3
table7	0.0	0.6	0.0	1.2	0.0	3.5	4.1	90.6
table8	0.0	16.7	10.0	20.0	20.0	30.0	3.3	0.0
targus	0.0	7.7	6.2	11.5	23.1	36.2	15.4	0.0
toy3dsarah	0.0	9.7	10.1	22.1	18.4	18.0	6.1	15.6
two5in6	0.0	18.0	20.3	28.4	20.5	12.0	0.7	0.2

very small values, i.e., the objective function is not (too much) affected by small changes ϵ in the bounds; this mostly happens for L_2. L_2, in general, also provides smaller one-norms of μ.

Once the released values $x = a + z$ were obtained from the solutions of (6) and (8), we solved the attacker problems for the four different scenarios listed in Section 3: B1, B2, B3 and C. For each of the 200 different tuples (instance, distance, scenario) we considered ten realizations of the attacker problems for different $\tilde{x}_i$ values, randomly obtained within the interval $[x_i\,(1-\beta)\,, x_i\,(1+\beta)]$, $i \in \mathcal{N}$. We used as β the maximum relative deviation between the released values x and the original ones a, such that for all the cells $i \in \mathcal{S}$, $a_i \in [x_i(1-\beta), x_i(1+\beta)]$. This is a realistic assumption, since the maximum relative deviation could be published by the data protector and thus known by the attacker. For scenario B1 (unknown protection senses) the values y_i are randomly obtained from $\{0, 1\}$ (equiprobable Bernoulli distribution). For scenarios B1 and B2 (unknown protection levels) the lower and upper protection levels were randomly obtained within the intervals $\left[x_i \max\left\{0, \frac{lpl_i}{a_i+\delta} - \Delta\right\}, x_i\left(\frac{lpl_i}{a_i+\delta} + \Delta\right)\right]$ and

Table 4. Results for scenario B2 and norm L_1. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	0.0	2.1	2.4	44.7	6.2	6.6	10.2	27.5
bts4	0.0	12.9	11.6	26.6	36.6	12.2	0.0	0.0
cbs	0.0	8.2	8.3	16.6	15.4	27.2	17.3	7.0
dale	0.0	7.9	7.9	16.4	16.1	16.9	18.5	16.3
destatis	0.0	24.2	17.7	28.1	16.4	11.4	2.0	0.2
hier13	0.0	1.4	2.8	9.8	53.4	32.6	0.0	0.0
hier13x13x13a	0.0	3.0	1.8	12.9	55.9	26.5	0.0	0.0
hier13x13x7d	0.0	3.7	4.4	19.7	49.1	23.1	0.0	0.0
hier13x7x7d	0.0	8.6	6.8	27.2	46.8	10.6	0.0	0.0
hier16	0.0	4.3	5.5	18.5	55.0	16.7	0.0	0.0
hier16x16x16a	0.0	4.8	4.9	21.7	50.3	18.3	0.0	0.0
nine12	0.0	14.7	11.9	25.8	34.2	13.2	0.1	0.0
nine5d	0.0	1.1	1.4	7.8	49.9	39.8	0.0	0.0
ninenew	0.0	10.9	9.3	24.3	39.7	15.7	0.1	0.0
osorio	0.0	18.6	15.7	25.7	17.1	5.7	12.9	4.3
table1	0.0	16.0	9.0	30.1	36.3	8.2	0.4	0.0
table3	0.0	11.1	11.9	22.9	33.2	19.6	1.2	0.0
table4	0.0	11.1	11.9	22.9	33.2	19.6	1.2	0.0
table5	0.0	11.1	11.9	22.9	33.2	19.6	1.2	0.0
table6	0.0	16.0	9.0	30.1	36.3	8.2	0.4	0.0
table7	0.0	0.0	1.2	1.2	1.8	9.4	15.3	71.2
table8	0.0	13.3	10.0	36.7	30.0	10.0	0.0	0.0
targus	0.0	10.8	6.9	20.8	40.0	18.5	3.1	0.0
toy3dsarah	0.0	2.2	2.3	19.4	58.6	17.5	0.1	0.0
two5in6	0.0	1.4	1.8	12.0	54.8	30.1	0.0	0.0

$\left[x_i \max\left\{0, \frac{upl_i}{a_i+\delta} - \Delta\right\}, x_i\left(\frac{upl_i}{a_i+\delta} + \Delta\right)\right]$, respectively, δ being a small value for the case $a_i \approx 0$. The above expressions are an attempt to apply to x_i the same fraction of protection that was applied to a_i; since this is unknown to the attacker, an error term Δ is considered ($\Delta = 0.2$ in all the runs performed). Possible infeasibilities derived from the values $\tilde{x}$ are dealt with by reformulating the inequalities of (12) and (14) as soft-constraints.[8] This amounts to the solution of 1025 linear optimization problems for L_1 and 1025 quadratic optimization problems for L_2 (including the protection problems). The CPU time needed for all of them is shown in columns "CPU" of Table 1. Since the problems do not involve binary variables they are very efficiently solved. All runs were carried out on a Fujitsu Primergy RX300 server with 3.33GHz Intel Xeon X5680 CPUs and 144 GB of RAM, under a GNU/Linux operating system (Suse 11.4), without exploitation of parallelism capabilities (these continuous LP and QP problems can also be solved in a much smaller laptop or desktop PC). The interior-point algorithm of the CPLEX 12.4 optimization solver was used for all the executions. Interior-point methods have shown to be the most efficient approach for controlled tabular adjustment problems with L_1 norms,[2] and

Table 5. Results for scenario B2 and norm L_2. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	0.0	6.1	5.9	13.1	10.2	14.9	23.1	26.4
bts4	0.0	13.0	11.6	26.7	36.7	12.1	0.0	0.0
cbs	0.0	8.5	8.6	17.4	16.6	25.6	16.7	6.5
dale	0.0	8.0	8.0	16.6	16.3	17.2	19.0	14.9
destatis	0.0	11.0	13.5	26.9	19.4	20.2	7.4	1.5
hier13	0.0	1.4	2.8	9.8	53.6	32.4	0.0	0.0
hier13x13x13a	0.0	3.0	1.8	12.9	55.9	26.5	0.0	0.0
hier13x13x7d	0.0	3.7	4.4	19.9	48.9	23.1	0.0	0.0
hier13x7x7d	0.0	8.6	6.8	27.2	46.8	10.6	0.0	0.0
hier16	0.0	4.3	5.5	18.5	55.0	16.7	0.0	0.0
hier16x16x16a	0.0	4.8	4.9	21.7	50.3	18.3	0.0	0.0
nine12	0.0	14.8	11.8	26.3	35.0	12.1	0.0	0.0
nine5d	0.0	1.1	1.4	7.9	50.3	39.3	0.0	0.0
ninenew	0.0	10.8	9.5	24.9	41.5	13.4	0.0	0.0
osorio	0.0	15.7	18.6	14.3	15.7	4.3	14.3	17.1
table1	0.0	4.5	2.0	10.8	11.6	19.1	51.6	0.3
table3	0.0	10.0	10.3	23.6	36.2	19.9	0.0	0.0
table4	0.0	10.0	10.3	23.6	36.2	19.9	0.0	0.0
table5	0.0	10.0	10.3	23.6	36.2	19.9	0.0	0.0
table6	0.0	1.3	1.2	6.2	8.4	23.4	59.0	0.5
table7	0.0	1.8	0.6	1.2	2.4	10.6	17.1	66.5
table8	0.0	13.3	10.0	36.7	30.0	10.0	0.0	0.0
targus	0.0	6.9	5.4	21.5	36.2	23.8	6.2	0.0
toy3dsarah	0.0	1.0	1.9	6.1	25.8	54.9	5.2	5.1
two5in6	0.0	1.3	1.8	12.1	54.7	30.0	0.0	0.0

are known to be the most efficient option for quadratic optimization problems (L_2 norm).[15]

Tables 2–9 summarize the results obtained for the 2000 attacker problems solved. We computed for each sensitive cell the ten percentage differences between a and $\hat{a}$, the true cell values and the ten attacker estimations, i.e., $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$. The particular estimation $\hat{a}_i$ depends on the information assumed known by the attacker, i.e., the scenario B1, B2, B3 or C, and the norm used, L_1 or L_2. Tables 2–9 provide, for each of the four scenarios and two norms, the distribution (as percentages) of the percentage differences between a and $\hat{a}$, considering the intervals 0 (i.e., the true value was re-computed by the attacker), (0,5], (5,10], (10,20], (20,30], (30,50], (50,100] and (100,—], for all the ten realizations of each instance. Distributions skewed to the left (long left tail, and the mass of the distribution is concentrated on the right part, i.e., on medium-large intervals) mean the attacker could not get good estimates, and the data can be considered safely protected. The opposite holds for right-skewed distributions. The following conclusions can be derived from tables 2–9:

Table 6. Results for scenario B3 and norm L_1. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	91.2	0.6	0.3	1.6	0.8	0.6	1.3	3.5
bts4	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
cbs	94.9	0.1	0.1	0.1	0.1	3.6	0.9	0.3
dale	98.8	0.0	0.0	0.0	0.0	0.1	0.3	0.7
destatis	98.4	1.0	0.4	0.1	0.1	0.0	0.0	0.0
hier13	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x13a	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x7d	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x7x7d	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier16	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier16x16x16a	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
nine12	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
nine5d	99.9	0.1	0.0	0.0	0.0	0.0	0.0	0.0
ninenew	99.8	0.2	0.0	0.0	0.0	0.0	0.0	0.0
osorio	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table1	99.9	0.0	0.0	0.0	0.1	0.0	0.0	0.0
table3	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
table4	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
table5	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
table6	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table7	83.5	0.0	1.2	5.9	5.9	0.0	0.0	3.5
table8	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
targus	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
toy3dsarah	98.3	1.7	0.0	0.0	0.0	0.0	0.0	0.0
two5in6	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

- Scenarios B1 and B2 can be considered safe, in general. The estimate $\hat{a}_i$ was never equal to the true cell value a_i, and the distribution is not concentrated on the left intervals. Although scenario B1 should be safer than B2 (the attacker has less information), in some cases the opposite holds (such as for instances "hier*"). This was an unexpected result. Therefore, in principle, it can be concluded that if the attacker has not good information about the protection levels (and to which cells to apply them), then controlled adjustment methods exhibit a low disclosure risk, and at the same time, a high data utility (as it was already known).[5]
- Comparing L_1 and L_2, the latter seems to reduce the disclosure risk: the distribution is more left-skewed for L_2 in scenarios B1 and B2. This is a new and unexpected result (however, it cannot be generalized to other datasets). L_2 is thus a good candidate norm for controlled adjustment methods, since in some instances it may exhibit both a lower disclosure risk and a higher data utility than L_1.
- On the other hand, for scenarios B3 and C the attacker was able to re-compute

Table 7. Results for scenario B3 and norm L_2. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	26.2	36.0	5.6	6.6	3.9	5.1	4.9	11.5
bts4	98.9	1.1	0.0	0.0	0.0	0.0	0.0	0.0
cbs	14.4	81.0	0.2	0.4	0.7	2.9	0.4	0.0
dale	57.2	41.2	0.1	0.2	0.2	0.4	0.8	0.0
destatis	13.8	53.3	5.0	8.4	7.4	11.0	1.1	0.0
hier13	90.7	9.3	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x13a	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x7d	84.0	16.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x7x7d	84.6	15.4	0.0	0.0	0.0	0.0	0.0	0.0
hier16	95.1	4.9	0.0	0.0	0.0	0.0	0.0	0.0
hier16x16x16a	93.4	6.6	0.0	0.0	0.0	0.0	0.0	0.0
nine12	93.3	6.7	0.0	0.0	0.0	0.0	0.0	0.0
nine5d	95.3	4.7	0.0	0.0	0.0	0.0	0.0	0.0
ninenew	95.4	4.6	0.0	0.0	0.0	0.0	0.0	0.0
osorio	10.0	51.4	0.0	5.7	2.9	7.1	7.1	15.7
table1	1.0	19.0	0.3	0.1	3.5	66.5	9.5	0.0
table3	95.3	4.7	0.0	0.0	0.0	0.0	0.0	0.0
table4	95.3	4.7	0.0	0.0	0.0	0.0	0.0	0.0
table5	95.3	4.7	0.0	0.0	0.0	0.0	0.0	0.0
table6	1.0	49.2	8.9	1.2	2.4	32.8	4.4	0.1
table7	41.8	36.5	5.9	7.6	5.3	1.2	1.2	0.6
table8	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
targus	28.5	5.4	9.2	19.2	17.7	20.0	0.0	0.0
toy3dsarah	0.0	2.2	2.4	18.1	67.6	6.5	2.5	0.7
two5in6	96.9	3.1	0.0	0.0	0.0	0.0	0.0	0.0

in almost 100% of the cases the original values a. For instance, for scenario C and norm L_1, a 100% of success was obtained by the attacker in most of the instances; similar figures are shown for (B2, L_1). Results are slightly better when L_2 is used (as stated above), but the disclosure risk is still very high. Therefore, it can be concluded that if the attacker has good information about the protection levels, protection senses, set of sensitive cells, and lower and upper bounds, then controlled adjustment methods exhibit a high disclosure risk. Although it could be stated that we are assuming the attacker has "too much" information, it is worth to keep in mind the above recommendation when protecting data through these techniques.

- Scenario C assumes the attacker perfectly knows the bounds of problems (12) and (14), the only uncertain parameters being in the objective function. According to Section 4, different objective functions may theoretically provide different (even very different) solutions. However, as observed empirically, this is not happening.
- It is worth to remind that we are assuming in all the scenarios tested that the

Table 8. Results for scenario C and norm L_1. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	55.0	0.4	0.6	1.3	1.3	1.1	39.3	0.7
bts4	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
cbs	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
dale	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
destatis	99.9	0.1	0.0	0.0	0.0	0.0	0.0	0.0
hier13	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x13a	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x7d	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier13x7x7d	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier16	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier16x16x16a	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
nine12	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
nine5d	99.9	0.1	0.0	0.0	0.0	0.0	0.0	0.0
ninenew	99.9	0.1	0.0	0.0	0.0	0.0	0.0	0.0
osorio	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table1	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table3	99.7	0.3	0.0	0.0	0.0	0.0	0.0	0.0
table4	99.7	0.3	0.0	0.0	0.0	0.0	0.0	0.0
table5	99.7	0.3	0.0	0.0	0.0	0.0	0.0	0.0
table6	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table7	0.0	0.0	0.0	0.0	0.0	58.8	41.2	0.0
table8	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
targus	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
toy3dsarah	97.7	1.9	0.1	0.2	0.0	0.2	0.0	0.0
two5in6	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

attacker knows: (1) which is the subset $\mathcal{S} \subseteq \mathcal{N}$ of sensitive cells; and (2) the lower and upper cell bounds l_{a_i} and u_{a_i} for all cells $i \in \mathcal{N}$. Without these assumptions, extra randomness would be added to the attacker problems, thus reducing the disclosure risk.

6. Conclusions

The disclosure risk of controlled adjustment methods for statistical tabular data never before had been analyzed empirically, and few results only based on the theory of optimization could be found in the literature. This work presented such an empirical assessment of the disclosure risk of controlled adjustment methods. The main conclusion is that, as observed from the extensive computational results, if the attacker does not have good knowledge on the original data, he/she could hardly obtain good estimates of the sensitive cells, in general. However, if the attacker has good information about the protection levels and which are the sensitive cells, or he/she knows the lower and upper bounds of the optimization problem (which is a stronger condition), then the method has a high disclosure risk. We also observed,

Table 9. Results for scenario C and norm L_2. For each instance and different intervals of the values $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in \mathcal{S}$ (percentage difference between the real and estimated cell value of sensitive cells), the table gives the percentage of sensitive cells within each interval. Results shown for all the attacker problems.

instance	0	(0,5]	(5,10]	(10,20]	(20,30]	(30,50]	(50,100]	(100,—]
australia_ABS	31.4	18.2	2.1	3.2	2.5	4.7	37.0	0.7
bts4	99.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0
cbs	44.7	55.2	0.0	0.0	0.0	0.0	0.0	0.0
dale	84.2	15.7	0.0	0.0	0.0	0.0	0.0	0.0
destatis	31.9	11.2	1.4	18.6	36.9	0.0	0.0	0.0
hier13	98.2	1.8	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x13a	94.4	5.6	0.0	0.0	0.0	0.0	0.0	0.0
hier13x13x7d	97.3	2.7	0.0	0.0	0.0	0.0	0.0	0.0
hier13x7x7d	81.2	18.8	0.0	0.0	0.0	0.0	0.0	0.0
hier16	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
hier16x16x16a	99.5	0.5	0.0	0.0	0.0	0.0	0.0	0.0
nine12	97.2	2.8	0.0	0.0	0.0	0.0	0.0	0.0
nine5d	98.6	1.4	0.0	0.0	0.0	0.0	0.0	0.0
ninenew	97.4	2.6	0.0	0.0	0.0	0.0	0.0	0.0
osorio	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
table1	0.0	10.0	0.0	0.0	0.0	87.2	2.8	0.0
table3	95.5	4.5	0.0	0.0	0.0	0.0	0.0	0.0
table4	95.5	4.5	0.0	0.0	0.0	0.0	0.0	0.0
table5	95.5	4.5	0.0	0.0	0.0	0.0	0.0	0.0
table6	0.0	0.7	0.0	3.7	7.0	85.5	3.2	0.0
table7	31.8	32.4	7.1	10.6	1.2	2.4	7.1	7.6
table8	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
targus	97.7	2.3	0.0	0.0	0.0	0.0	0.0	0.0
toy3dsarah	0.0	2.7	2.3	23.4	63.2	7.6	0.6	0.1
two5in6	99.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0

unexpectedly, that L_2 in general provides solutions of lower disclosure risk, which combined with the good data utility exhibited by this norm,[5] makes it a suitable choice for controlled tabular adjustment.

Acknowledgments

This paper has been supported by grants MTM2009-08747 of the Spanish Ministry of Science and Innovation, SGR-2009-1122 of the Government of Catalonia, and INFRA-2010-262608 of the European Union. We also thank Krish Muralidhar for exciting discussions about this topic when he was on sabbatical leave at the Universitat Rovira i Virgili, which were the original motivation for this paper.

References

1. D. Bertsimas and J.N. Tsitsiklis, *Introduction to Linear Optimization* (Athena Scientific, Belmont MA, 1997).
2. J. Castro, "Minimum-distance controlled perturbation methods for large-scale tabular data protection", *Eur. J. Oper. Res.* **171** (2006) 39–52.

3. J. Castro, "Statistical disclosure control in tabular data", in *Privacy and Anonymity in Information Management Systems: New Techniques for New Practical Problems*, eds. J. Nin and J. Herranz (Springer, London, 2010), pp. 113-131.
4. J. Castro, "Recent advances in optimization techniques for statistical tabular data protection", *Eur. J. Oper. Res.* **216** (2012) 257–269.
5. J. Castro, "Comparing L_1 and L_2 distances for CTA", in *Privacy in Statistical Databases. Lect. N. Comp. Sci.*, eds. J. Domingo-Ferrer and I. Tinnirello (Springer, Berlin, 20102), to appear.
6. J. Castro and J.A. González, "A tool for analyzing and fixing infeasible RCTA instances", in *Privacy in Statistical Databases. Lect. N. Comp. Sci.* ***6344***, eds. J. Domingo-Ferrer and E. Magkos (Springer, Berlin, 2010), pp. 17–28.
7. J. Castro and J.A. González, "Present and future research on controlled tabular adjustment", in *Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality*, Tarragona, Oct. 2011. Available online at `http://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2011/48_Castro-Gonzalez.pdf`
8. J.W. Chinneck, *Feasibility and Infeasibility in Optimization: Algorithms and Computational Methods* (Springer, New York, 2008).
9. R. Chi-Wing Wong, A. Wai-Chee Fu, K. Wang and J. Pei, "Minimality attack in privacy preserving data publishing" *Proc. 33rd International Conference on Very Large Data Bases*, Vienna, Austria, Sept. 2007, pp. 553–554.
10. L. Cox, "Disclosure risk for tabular economic Data", in *Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies*, eds. P. Doyle, J. Lane, J. Theeuwes and L. Zayatz (North-Holland, Amsterdam, 2001).
11. R.A. Dandekar and L.H. Cox, "Synthetic tabular Data: an alternative to complementary cell suppression", manuscript, Energy Information Administration, U.S. 2002.
12. J. Domingo-Ferrer and V. Torra, "A critique of the sensitivity rules usually employed for statistical table protection", *Int. J. of Uncertainty Fuzziness and Knowledge-Based Systems* **10** (2002) 545–556.
13. B. Fraser and J. Wooton, "A proposed method for confidentialising tabular output to protect against differencing", in *Monographs of Official Statistics. Work session on Statistical Data Confidentiality*, (Eurostat, Luxembourg, 2006), 299-302.
14. A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, R. Lenz, J. Naylor, E. Schulte-Nordholt, G. Seri and P.P. de Wolf, *Handbook on Statistical Disclosure Control (v. 1.2)* (Network of Excellence in the European Statistical System in the field of Statistical Disclosure Control, 2010). Available on-line at `http://neon.vb.cbs.nl/casc/SDC_Handbook.pdf`.
15. S.J. Wright, *Primal-Dual Interior-Point Methods* (SIAM, Philadelphia, 1997).
16. S.J. Wright and J. Nocedal *Numerical Optimization* (Springer, New York, 2003).