Mathematical Programming
https://doi.org/10.1007/s10107-022-01811-w

FULL LENGTH PAPER

Series B

Utility/privacy trade-off as regularized optimal transport

Etienne Boursier[1] · Vianney Perchet[2,3]

Received: 30 January 2021 / Accepted: 16 March 2022

Abstract

Strategic information is valuable either by remaining private (for instance if it is sensitive) or, on the other hand, by being used publicly to increase some utility. These two objectives are antagonistic and leaking this information by taking full advantage of it might be more rewarding than concealing it. Unlike classical solutions that focus on the first point, we consider instead agents that optimize a natural trade-off between both objectives. We formalize this as an optimization problem where the objective mapping is regularized by the amount of information revealed to the adversary (measured as a divergence between the prior and posterior on the private knowledge). Quite surprisingly, when combined with the entropic regularization, the Sinkhorn loss naturally emerges in the optimization objective, making it efficiently solvable via better adapted optimization schemes. We empirically compare these different techniques on a toy example and apply them to preserve some privacy in online repeated auctions.

Keywords Privacy learning · Optimal transport · Non-convex optimization · Repeated auctions

Mathematics Subject Classification 90C90 · 49Q22 · 91A27 · 68P27

E. Boursier was a member of Centre Borelli, ENS Paris-Saclay when this work was completed. A preliminary version of this work [11] has been accepted at the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS 2020).

✉ Etienne Boursier
etienne.boursier1@gmail.com

Vianney Perchet
vianney.perchet@normalesup.org

[1] TML Lab, EPFL, Lausanne, Switzerland

[2] CREST, ENSAE Paris, Palaiseau, France

[3] Criteo AI Lab, Paris, France

Published online: 22 April 2022

1 Introduction

In many economic mechanisms and strategic games involving different agents, asymmetries of information (induced by a private type, some knowledge on the hidden state of Nature, etc.) can and should be leveraged to increase one's utility. When these interactions between agents are repeated over time, preserving some asymmetry (i.e., not revealing private information) can be crucial to guarantee a larger utility in the long run. Indeed, the small short term utility of publicly using information can be overwhelmed by the long term effect of revealing it [5].

Informally speaking, an agent should use, and potentially reveal some private information only if she gets a subsequent utility increase in return. Keeping this information private is no longer a constraint [22, as in other classical privacy concepts such as differential privacy] but becomes part of the objective, which is then to decide how and when to use it. For instance, it might happen that revealing everything is optimal or, on the contrary, that a non-revealing policy is the best one. This is roughly similar to a poker player deciding whether to bluff or not. In some situations, it might be interesting to focus solely on the utility even if it implies losing the whole knowledge advantage, while in other situations, the immediate profit for using this advantage is so small that playing independently of it (or bluffing) is better.

After a rigorous mathematical formulation of this utility vs. privacy trade-off, it appears that this problem can be recast as a regularized optimal transport minimization. In the specific case of entropic regularization, this problem has received a lot of interest in the recent years as it induces a computationally tractable way to approximate an optimal transport distance between distributions and has thus been used in many applications [18]. Our work showcases how the new Privacy Regularized Policy problem benefits in practice from this theory.

Private mechanisms Differential privacy is the most widely used private learning framework [21, 22, 63] and ensures that any single element of the whole dataset cannot be retrieved from the output of the algorithm. This constraint is often too strong for economic applications (as illustrated before, it is sometimes optimal to disclose publicly some private information). f-divergence privacy costs have thus been proposed in recent literature as a promising alternative [14]. These f-divergences, such as Kullback–Leibler, are also used by economists to measure the cost of information from a Bayesian perspective, as in the rational inattention literature [50, 51, 69]. It was only recently that this approach has been considered to measure "privacy losses" in economic mechanisms [23]. This model assumes that the designer of the mechanism has some prior belief on the unobserved and private information. After observing the action of the player, this belief is updated and the cost of information corresponds to the KL between the prior and posterior distributions of this private information.

Optimal privacy preserving strategies with privacy constraints have been recently studied in this setting under specific conditions [23]. Loss of privacy can however be directly considered as a cost in the overall objective and an optimal strategy reveals information only if it actually leads to a significant increase in utility. Meanwhile, constrained strategies systematically reveal as much as allowed by the constraints, without incorporating the additional cost of this revelation.

Optimal transport Finding an appropriate way to compare probability distributions is a major challenge in learning theory. Optimal Transport manages to provide powerful tools to compare distributions in metric spaces [78]. As a consequence, it has received an increasing interest these past years [66], especially for generative models [4, 29, 65]. With the exception of particular cases [7, 19, 41, see e.g.,], such powerful distances however come at the expense of heavy and intractable computations [6, 55], which might not be suitable to learning algorithms. It was recently showcased that adding an entropic regularization term enables fast computations of approximated distances using Sinkhorn algorithm [18, 70]. Since then, the Sinkhorn loss has also shown promising results for applications such as generative models [28, 29], domain adaptation [17] and supervised learning [26], besides having interesting theoretical properties [25, 30, 60].

Contributions and organization of the paper The new framework of Privacy Regularized Policy is motivated by several applications, presented in Sect. 2 and is formalized in Sect. 3. This problem is mathematically formulated as some optimization problem (yet eventually in an infinite dimensional space), which is convex if the privacy cost is an f-divergence, see Sect. 4. Also, if the private information space is discrete, this problem admits an optimal discrete distribution. The minimization problem then becomes dimensionally finite, but non-convex.

If the Kullback–Leibler divergence between the prior and the posterior is considered for the cost of information, the equivalence with a Sinkhorn loss minimization problem is shown in Sect. 5. Although non-convex, this new problem formulation allows different optimization techniques developed in Sect. 6 to efficiently compute partially revealing policies. Finally, with a linear utility cost, the problem is equivalent to the minimization of the difference of two convex functions. Using the theories of these specific problems, different optimization methods can be compared, which illustrate the practical aspect of our new model. This is done in Sect. 7, where we also compute partially revealing strategies for repeated auctions.

A preliminary version of this work appeared in [11]. This version provides an additional detailed study of existing optimization methods to minimize the Sinkhorn loss; as well as supplementary experiments, especially to compare these different possible methods.

2 Some applications

Our model is motivated by different applications described in this section: online repeated auctions and learning models on external servers.

2.1 Online repeated auctions

When a website wants to sell an advertisement slot, firms such as Google or Criteo take part in an auction to buy this slot for one of their customer, a process illustrated in Fig. 1. As this interaction happens each time a user lands on the website, this is no longer a one-time auction problem, but repeated auctions where the seller and/or the

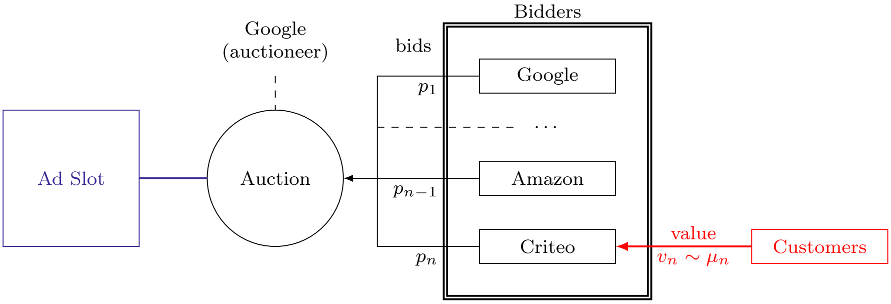


Fig. 1 Online advertisement auction system

competitor might observe not just one bid, but a distribution of bids. As a consequence, if a firm were bidding truthfully, seller and other bidders would have access to its true value distribution μ. This has two possible downsides.

First, if the value distribution μ was known to the auctioneer, she could maximize her revenue at the expense of the bidder utility [2, 3, 24, 32], for instance with personalized reserve prices. Second, the auctioneer can sometimes take part in the auction and becomes a direct concurrent of the bidder (this might be a unique characteristic of online repeated auctions for ads). For instance, Google is both running some auction platforms and bidding on some ad slots for their client. As a consequence, if the distribution μ was perfectly known to some concurrent bidder, he could use it in the future, by bidding more or less aggressively or by trying to conquer new markets.

It is also closely related to online pricing or repeated posted price auctions. When a user wants to buy a flight ticket (or any other good), the selling company can learn the value distribution of the buyer and then dynamically adapts its prices in order to increase its revenue. The user can prevent this behavior in order to maximize her long term utility, even if it means refusing some apparently good offers in the short term (in poker lingo, she would be “bluffing”).

As explained in Sect. 3.1 below, finding the best possible long term strategy is intractable, as the auctioneer could always adapt to the bidding strategy, leading to an arm race where the bidder and the auctioneer successively adapt to the other one’s strategy. Such an arm race is instead avoided by trading-off between the best possible response to the auctioneer’s fixed strategy as well as the leaked quantity of information. The privacy loss here aims at bounding the incurred loss in bidder’s utility if the auctioneer adapts her strategy using the revealed information.

2.2 Learning through external servers

Nowadays, several servers or clusters allow their clients to perform heavy computations remotely, for instance to learn some model parameters (say a deep neural net) for a given training set. The privacy concern when querying a server can sometimes be handled using homomorphic encryption [10, 31, 67], if the cluster is designed in that way (typically a public model has been learned on the server). In this case, the client sends an encrypted testing set to the server, receives encrypted predictions and locally recovers the accurate ones. This technique, when available, is powerful, but requires heavy local computations.

Consider instead a client wanting to learn a new model (say, a linear/logistic regression or any neural net) on a dataset that has some confidential component. Directly sending the training set would reveal the whole data to the server owner, besides the risk of someone else observing it. The agent might instead prefer to send noised data, so that the computed model remains close to the accurate one, while keeping secret the true data. If the data contain sensitive information on individuals, then differential privacy is an appropriate solution. However, it is often the case that the private part is just a single piece of information of the client itself (say, its margin, its current wealth or its total number of users for instance) that is crucial to the final learned model but should not be totally revealed to a competitor. Then differential privacy is no longer the solution, as there is only a single element to protect and/or to use. Indeed, some privacy leakage is allowed and can lead to much more accurate parameters returned by the server and a higher utility at the end; the Privacy Regularized Policy aims at computing the best dataset to send to the server, in order to maximize the utility-privacy trade-off.

3 Model

We first introduce a simple toy example in Sect. 3.1 giving insights into the more general problem, whose formal and general formulation is given in Sect. 3.2.

3.1 Toy Example

Suppose an agent is publicly playing an action $x \in \mathcal{X}$ to minimize a loss $x^\top c_k$, where c_k is some vector. The true type $k \in [K]$ is only known to the agent and drawn from a prior p_0. Without privacy concern, the agent would then solve for every k: $\min_{x \in \mathcal{X}} x^\top c_k$.

Let us denote by x_k^* the optimal solution of that problem. Besides maximizing her reward, the agent actually wants to protect the secret type k. After observing the action x taken by the agent, an adversary updates her posterior distribution of the hidden type p_x.

If the agent were to play deterministically x_k^* when her type is k, then the adversary could infer the true value of k based on the played action. The agent should instead choose her action randomly to hide her true type to the adversary. Given a type k, the strategy of the agent is then a probability distribution μ_k over $\mathcal{X}$ and her expected reward is $\mathbb{E}_{x \sim \mu_k}\left[x^\top c_k\right]$. In this case, the posterior distribution after playing the action x is computed using Bayes rule and if the different μ_k have overlapping supports, then the posterior distribution is no longer a Dirac mass, i.e., some asymmetry of information is maintained.

The agent aims at simultaneously minimizing both the utility loss and the amount of information given to the adversary. A common way to measure the latter is given by the Kullback–Leibler (KL) divergence between the prior and the posterior [69]:

$\mathrm{KL}(p_x, p_0) = \sum_{k=1}^K \log\left(\frac{p_x(k)}{p_0(k)}\right) p_x(k)$, where $p_x(k) = \frac{p_0(k)\mu_k(x)}{\sum_{l=1}^K p_0(l)\mu_l(x)}$. If the information cost scales in utility with $\lambda > 0$, the regularized loss of the agent is then $x^\top c_k + \lambda \mathrm{KL}(p_x, p_0)$ instead of $x^\top c_k$. Overall, the global objective of the agent is the following minimization:

$$\min_{\mu_1,\ldots,\mu_K} \sum_{k=1}^K p_0(k)\mathbb{E}_{x\sim\mu_k}\left[x^\top c_k + \lambda \mathrm{KL}(p_x, p_0)\right].$$

In the limit case $\lambda = 0$, the agent follows a totally revealing strategy and deterministically plays x_k^* given k. When $\lambda = \infty$, the agent focuses on perfect privacy and looks for the best action chosen independently of the type: $x \perp\!\!\!\perp k$. It corresponds to a so called non-revealing strategy in game theory and the best strategy is then to play $\arg\min_x x^\top c[p_0]$ where $c[p_0] = \sum_{k=1}^K p_0(k)c_k$. For a positive λ, the behavior of the player will then interpolate between these two extreme strategies.

This problem is related to repeated games with incomplete information [5], where players have private information affecting their utility functions. Playing some action leaks information to the other players, who then change their strategies in consequence. The goal is then to control the amount of information leaked to the adversaries in order to maximize one's own utility. In practice, it can be impossible to compute the best adversarial strategy, e.g., the player is unaware of how the adversaries would adapt. The utility loss caused by adversarial actions is then modeled as a function of the amount of revealed information.

3.2 General model

We now introduce formally the general model sketched by the previous toy example. The agent (or player) has a private type $y \in \mathcal{Y}$ drawn according to a prior p_0 whose support can be infinite. She then chooses an action $x \in \mathcal{X}$ to maximize her utility, which depends on both her action and her type. Meanwhile, she wants to hide the true value of her type y. A strategy is thus a mapping $\mathcal{Y} \to \mathcal{P}(\mathcal{X})$, where $\mathcal{P}(\mathcal{X})$ denotes the set of distributions over $\mathcal{X}$; for the sake of conciseness, we denote by $X|Y \in \mathcal{P}(\mathcal{X})^{\mathcal{Y}}$ such a strategy. In the toy example, this mapping was given by $k \mapsto \mu_k$. The adversary observes her action x and tries to infer the type of the agent. We assume a perfect adversary, i.e., she can compute the exact posterior distribution p_x.

Let $c(x, y)$ be the utility loss for playing $x \in \mathcal{X}$ with the type $y \in \mathcal{Y}$. The privacy cost is $c_{\mathrm{priv}}(X, Y)$ where (X, Y) is the joint distribution of the action and the type. In the toy example given in Sect. 3.1, the utility cost was given by $c(x, k) = x^\top c_k$ and the privacy cost was the expected KL divergence between p_x and p_0. Previous works aimed at minimizing the utility loss with a privacy cost below some threshold $\varepsilon > 0$, i.e., minimize $\mathbb{E}_{(x,y)\sim(X,Y)}\left[c(x, y)\right]$ such that $c_{\mathrm{priv}}(X, Y) \leq \varepsilon$. Instead, as explained in the toy example, this privacy loss here has some utility scaling with $\lambda > 0$, which can be seen as the value of information. The final objective of the agent is then to minimize the following loss:

$$\inf_{X|Y\in\mathcal{P}(\mathcal{X})^{\mathcal{Y}}} \mathbb{E}_{(x,y)\sim(X,Y)}\big[c(x,y)\big] + \lambda\, c_{\text{priv}}(X,Y). \tag{1}$$

As mentioned above, the privacy cost is here defined as a measure between the posterior p_x and the prior distribution p_0 of the type, i.e., $c_{\text{priv}}(X,Y) = \mathbb{E}_{x\sim X} D(p_x, p_0)$ for some function D. In the toy example of Sect. 3.1, $D(p_x, p_0) = \text{KL}(p_x, p_0)$, which is a classical cost of information in economics.

Note that the cost is minimized in expectation with respect to both the action x and the type y, as ex-ante costs are generally considered in repeated games with asymmetric information[1] [5]. It is also motivated by the online ad-auctions problem, where a central controller runs multiple auctions for different firms and preserves privacy for each of them.

For a distribution $\gamma \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, we denote by $\pi_{1\#}\gamma$ (resp. $\pi_{2\#}\gamma$) the marginal distribution of X (resp. Y): $\pi_{1\#}\gamma(A) = \gamma(A\times\mathcal{Y})$ and $\pi_{2\#}\gamma(B) = \gamma(\mathcal{X}\times B)$. In order to have a simpler formulation of the problem, we remark that instead of defining a strategy by the conditional distribution $X|Y$, it is equivalent to see it as a joint distribution γ of (X,Y) with a marginal over the type equal to the prior: $\pi_{2\#}\gamma = p_0$. The remaining of the paper focuses on the problem below, which we call *Privacy Regularized Policy[.]* With the privacy cost defined as above, the minimization problem (1) is equivalent to

$$\inf_{\substack{\gamma\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})\\ \pi_{2\#}\gamma=p_0}} \int_{\mathcal{X}\times\mathcal{Y}} [c(x,y) + \lambda\, D(p_x, p_0)]\,\mathrm{d}\gamma(x,y). \tag{PRP}$$

4 A convex minimization problem

In this section, we study some theoretical properties of the Problem (PRP). We first recall the definition of an f-divergence.

Definition 1 D is an f-divergence if for all distributions P, Q such that P is absolutely continuous w.r.t. Q, $D(P,Q) = \int_{\mathcal{Y}} f\left(\frac{\mathrm{d}P(y)}{\mathrm{d}Q(y)}\right)\mathrm{d}Q(y)$ where f is a convex function defined on $\mathbb{R}_+^*$ with $f(1) = 0$.

The set of f-divergences includes common divergences such as the Kullback–Leibler divergence, the reverse Kullback–Leibler or the Total Variation distance.

Also, the min-entropy defined by $D(P,Q) = \log(\operatorname{ess\,sup} \mathrm{d}P/\mathrm{d}Q)$ is widely used for privacy [71, 76]. It corresponds to the limit of the Renyi divergence $\log\left(\sum_{i=1}^n p_i^\alpha q_i^{1-\alpha}\right)/(\alpha-1)$, when $\alpha\to+\infty$ [54, 64]. Although it is not an f-divergence, the Renyi divergence derives from the f-divergence associated with the convex function $t\mapsto(t^\alpha-1)/(\alpha-1)$. f-divergence costs have been recently considered in the computer science literature in a non-Bayesian case and then present the good properties of convexity, composition and post-processing invariance [14].

In the remaining of the paper, D is an f-divergence. (PRP) then becomes a convex minimization problem.

[1] Ex-ante costs also suggest that the value of information can be heterogeneous among types [23].

Theorem 1 *If D is an f-divergence,* (PRP) *is a convex problem in $\gamma \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$.*[2]

Proof The constraint set is obviously convex. The first part of the integral is linear in γ. It thus remains to show that the privacy loss is also convex in γ. As D is an f-divergence, the privacy cost is

$$\begin{aligned} c_{\text{priv}}(\gamma) &:= \int_{\mathcal{X}\times\mathcal{Y}} D\left(p_x, p_0\right) \mathrm{d}\gamma(x, y) \\ &= \int_{\mathcal{X}} \int_{\mathcal{Y}} f\left(\frac{\mathrm{d}\gamma(x, y)}{\mathrm{d}\gamma_1(x)\mathrm{d}p_0(y)}\right) \mathrm{d}p_0(y)\mathrm{d}\gamma_1(x), \end{aligned}$$

where $\gamma_1 = \pi_{1\#}\gamma$. For $t \in (0, 1)$ and two distributions γ and μ, we can define the convex combination $\nu = t\gamma + (1-t)\mu$. By linearity of the projection π_1, $\nu_1 = t\gamma_1 + (1-t)\mu_1$. The convexity of c_{priv} actually results from the convexity of the *perspective* of f defined by $g(x_1, x_2) = x_2 f(x_1/x_2)$ [12]. It indeed implies

$$f\left(\frac{\mathrm{d}\nu}{\mathrm{d}\nu_1\mathrm{d}p_0}\right)\mathrm{d}\nu_1 \leq tf\left(\frac{\mathrm{d}\gamma}{\mathrm{d}\gamma_1\mathrm{d}p_0}\right)\mathrm{d}\gamma_1 + (1-t)f\left(\frac{\mathrm{d}\mu}{\mathrm{d}\mu_1\mathrm{d}p_0}\right)\mathrm{d}\mu_1.$$

The result then directly follows when summing over $\mathcal{X} \times \mathcal{Y}$. □

Although $\mathcal{P}(\mathcal{X} \times \mathcal{Y})$ has generally an infinite dimension, it is dimensionally finite if both sets $\mathcal{X}$ and $\mathcal{Y}$ are discrete. A minimum can then be found using classical optimization methods. In the case of bounded low dimensional spaces $\mathcal{X}$ and $\mathcal{Y}$, they can be approximated by finite grids. However, the size of the grid grows exponentially with the dimension and another approach is needed for large dimensions of $\mathcal{X}$ and $\mathcal{Y}$.

4.1 Discrete type space

We assume here that $\mathcal{X}$ is an infinite action space and $\mathcal{Y}$ is of cardinality K (or equivalently, p_0 is a discrete prior of size K), so that $p_0 = \sum_{k=1}^{K} p_0^k \delta_{y_k}$. For a fixed joint distribution γ, let the measure μ_k be defined for any $A \subset \mathcal{X}$ by $\mu_k(A) = \gamma(A \times \{y_k\})$ and $\mu = \sum_{k=1}^{K} \mu_k = \pi_{1\#}\gamma$. The function $p^k(x) = \frac{\mathrm{d}\mu_k(x)}{\mathrm{d}\mu(x)}$, defined over the support of μ by absolute continuity, is the posterior probability of having the type k when playing x. The tuple $(\mu, (p^k)_k)$ exactly determines γ (PRP) is then equivalent to:

$$\begin{aligned} &\inf_{\substack{\mu,(p^k(\cdot)) \\ p^k \geq 0, \sum_{l=1}^{K} p^l(\cdot)=1}} \sum_k \int_{\mathcal{X}} \left[p^k(x)c(x, y_k) + \lambda p_0^k f\left(\frac{p^k(x)}{p_0^k}\right)\right] \mathrm{d}\mu(x) \\ &\text{such that for all } k \leq K, \int_{\mathcal{X}} p^k(x)\mathrm{d}\mu(x) = p_0^k. \end{aligned} \tag{2}$$

For fixed posterior distributions p^k, this is a generalized moment problem on the distribution μ [43]. The same types of arguments can then be used for the existence and the form of optimal solutions.

[2] It is convex in a usual sense and not geodesically here.

Theorem 2 *If the prior is discrete of size K, for all $\varepsilon > 0$, (PRP) has an ε-optimal solution such that $\pi_{1\#}\gamma = \mu$ has a finite support of at most $K+2$ points.*

Furthermore, if $\mathcal{X}$ is compact and $c(\cdot, y_k)$ is lower semi-continuous for every k, then it also holds for $\varepsilon = 0$.

Proof For $\varepsilon > 0$, let $(p^k)_k$ and μ be an ε-optimal solution. We define

$$\begin{cases} g_0(x) := \sum_k \left[p^k(x) c(x, y_k) + \lambda p_0^k(x) f\left(\frac{p^k(x)}{p_0^k}\right)\right], \\ g_k(x) := p^k(x) \text{ for } k \in \{1, \ldots, K\}. \end{cases}$$

Let $\alpha_j(\mu) = \int_{\mathcal{X}} g_j \mathrm{d}\mu$ for any $j \in \{0, \ldots, K\}$. The considered solution μ is included in a convex hull as follows:

$$(\alpha_j(\mu))_{0 \le j \le K} \in \operatorname{Conv}\{(g_j(x))_{0 \le j \le K} / x \in \mathcal{X}\}.$$

By Caratheodory theorem, there are $K+2$ points $x_i \in \mathcal{X}$ and $(t_i) \in \Delta_{K+2}$ such that $\alpha_j(\mu) = \sum_{i=1}^{K+2} t_i g_j(x_i)$ for any j. Let $\mu' = \sum_{i=1}^{K+2} t_i \delta_{x_i}$. We then have $\alpha_j(\mu') = \alpha_j(\mu)$ for all j, which means that $(\mu', (p^k)_k)$ is also an ε-optimal solution of the problem (2) and the support of μ' is of size at most $K+2$. □

Now assume that $\mathcal{X}$ is compact and the $c(\cdot, y_k)$ are lower semi-continuous. The first part of Theorem 2 that we just proved leads to Corollary 1, which is given below and claims that (PRP) is equivalent to its discrete version given by Eq. (3). We consider the formulation of Eq. (3) in the remaining of the proof.

Define $h_k(\gamma_i) := \left(\sum_{m=1}^K \gamma_{i,m}\right) f\left(\frac{\gamma_{i,k}}{p_0^k \sum_{m=1}^K \gamma_{i,m}}\right)$, with the conventions $f(0) = \lim_{x \to 0} f(x) \in \mathbb{R} \cup \{+\infty\}$ and $h_k(\gamma_i) = 0$ if $\sum_{m=1}^K \gamma_{i,m} = 0$.

The privacy cost is then the sum of the $h_k(\gamma_i)$ for all k and i. The case $\varepsilon = 0$ comes from the lower semi-continuity of the objective function, as claimed by Lemma 1 proven below.

Lemma 1 *For any k in $\{1, \ldots, K\}$, h_k is lower semi-continuous.*

Let $(\gamma^{(n)}, x^{(n)})_n$ be a feasible sequence whose value converges to this infimum. By compacity, we can assume after extraction that $(x^{(n)}, \gamma^{(n)}) \to (x, \gamma)$. As $c(\cdot, y_k)$ and h_k are all lower semi-continuous, the infimum is reached in (γ, x). □

Proof of Lemma 1 f is convex and thus continuous on $\mathbb{R}_+^*$. If $\lim_{x \to 0^+} f(x) \in \mathbb{R}$, then f can be extended as a continuous function on $\mathbb{R}_+$ and all the h_k are thus continuous. Otherwise by convexity, $\lim_{x \to 0^+} f(x) = +\infty$. Thus, h_k is continuous at γ_i as soon as $\gamma_{i,j} > 0$ for every j. If $\gamma_{i,k} = 0$, but the sum $\sum_{l=1}^K \gamma_{i,l}$ is strictly positive, then $h_k(\gamma_i) = +\infty$; but as soon as $\rho \to \gamma$, we also have an infinite limit.

If $\sum_{l=1}^K \gamma_{i,l} = 0$, then $\liminf_{\rho \to \gamma} f\left(\frac{\rho_{i,k}}{p_0^k \sum_l \rho_{i,l}}\right) \in \mathbb{R} \cup \{+\infty\}$. This term is multiplied by a factor going to 0, so $\liminf_{\rho \to \gamma} h_k(\rho_i) \ge 0 = h_k(\gamma_i)$. Finally, h_k is lower semi-continuous in all the cases. □

If the support of γ is included in $\{(x_i, y_k) \mid 1 \leq i \leq K+2,\ 1 \leq k \leq K\}$, it can be denoted as a matrix $\gamma_{i,k} := \gamma(\{(x_i, y_k)\})$.

Corollary 1 *In the case of a discrete prior,* (PRP) *is equivalent to:*

$$\begin{aligned} &\inf_{(\gamma,x)\in\mathbb{R}_+^{(K+2)\times K}\times\mathcal{X}^{K+2}} \sum_{i,k}\gamma_{i,k}\, c(x_i, y_k) + \lambda \sum_{i,k}\gamma_{i,k} D(p_{x_i}, p_0) \\ &\text{such that } \forall k \leq K,\ \sum_i \gamma_{i,k} = p_0^k. \end{aligned} \tag{3}$$

Proof Theorem 2 claims that (PRP) is equivalent to the problem of Corollary 1 if we also impose $x_i \neq x_j$ for $i \neq j$. The value of problem (3) is thus lower than the value of (PRP) as we consider a larger feasible set. Let us consider a redundant solution (γ, x) with $x_i = x_j$ for $i \neq j$. It remains to show that a non redundant version of this solution has a lower value.

The functions h_k defined in the proof of Theorem 2 are convex as the perspectives of convex functions [12]. Also, they are obviously homogeneous of degree 1. These two properties imply that the h_k are subadditive. Thus, let (γ', x') be defined by

$$\begin{cases} \gamma'_{l,k} := \gamma_{l,k} \text{ for any } l \notin \{i, j\}, \\ \gamma'_{i,k} := \gamma_{i,k} + \gamma_{j,k}, \\ \gamma'_{j,k} := 0 \end{cases} \quad \text{and} \quad \begin{cases} x'_l := x_l \text{ for any } l \neq j, \\ x'_j \in \mathcal{X} \setminus \{x_l | 1 \leq l \leq K+2\}. \end{cases}$$

The subadditivity of h_k and $h_k(0) = 0$ implies $h_k(\gamma'_i) + h_k(\gamma'_j) \leq h_k(\gamma_i) + h_k(\gamma_j)$ for any k. The other terms in the objective function will be the same for (γ, x) and (γ', x'). It thus holds

$$\sum_{i,k}\gamma_{i,k}c(x_i, y_k) + \lambda\sum_{i,k} p_0^k h_k(\gamma_i) \geq \sum_{i,k}\gamma'_{i,k}c(x'_i, y_k) + \lambda\sum_{i,k} p_0^k h_k(\gamma'_i).$$

The tuple (γ', x') is in the feasible set of the problem of Corollary 1 and we removed a redundant condition from x. We can thus iteratively construct a solution $(\tilde{\gamma}, \tilde{x})$ until reaching non redundancy. We then have $(\tilde{\gamma}, \tilde{x})$ a non redundant solution with a lower value than (γ, x), i.e., allowing redundancy does not change the infimum. □

Although it seems easier to consider the dimensionally finite problem given by Corollary 1, it is not jointly convex in (γ, x). No general algorithms exist to efficiently minimize non-convex problems. We refer the reader to [37] for an introduction to non-convex optimization.

The next sections reformulate the problem to better understand its structure, leading to optimization methods reaching better local minima.

5 Sinkhorn loss minimization

Formally, (PRP) is expressed as Optimal Transport Minimization for the utility cost c with a regularization given by the privacy cost. This section considers the Kullback–Leibler divergence for privacy cost. In this case, the problem becomes a Sinkhorn loss minimization, which presents computationally tractable schemes [60]. If the privacy cost is the KL divergence between the posterior and the prior, i.e., $f(t) = t\log(t)$, then the regularization term corresponds to the mutual information $I(X;Y)$, which is the classical cost of information in economics.

The Sinkhorn loss for distributions $(\mu,\nu) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y})$ is defined by

$$\begin{aligned} \mathrm{OT}_{c,\lambda}(\mu,\nu) := \min_{\gamma \in 5(\mu,\nu)} & \int c(x,y)\mathrm{d}\gamma(x,y) \\ & + \lambda \int \log\left(\frac{\mathrm{d}\gamma(x,y)}{\mathrm{d}\mu(x)\mathrm{d}\nu(y)}\right)\mathrm{d}\gamma(x,y), \end{aligned} \tag{4}$$

where $5(\mu,\nu) = \{\gamma \in \mathcal{P}(\mathcal{X}\times\mathcal{Y}) \mid \pi_{1\#}\gamma = \mu \text{ and } \pi_{2\#}\gamma = \nu\}$. In Optimal Transport, $c(x,y)$ is the transportation cost from x to y and the goal is to find a transport map (or a joint distribution γ with Kantorovich relaxation) minimizing the total transportation cost between the distributions μ and ν. The second term is an entropic regularization term on γ allowing fast approximation schemes [18]. The term $t\log(t)$ of the KL divergence appears, when replacing $\mathrm{d}\gamma(x,y)$ by $\frac{\mathrm{d}\gamma(x,y)}{\mathrm{d}\mu(x)\mathrm{d}\nu(y)}\mathrm{d}\mu(x)\mathrm{d}\nu(y)$. When developing the logarithm, the difference between the entropies of $\mu \otimes \nu$ and γ appears.

Problem (PRP) with the privacy cost given by the Kullback–Leibler divergence is actually a Sinkhorn loss minimization problem.

Theorem 3 *Problem* (PRP) *with* $D = \mathrm{KL}$ *is equivalent to*

$$\inf_{\mu \in \mathcal{P}(\mathcal{X})} \mathrm{OT}_{c,\lambda}(\mu, p_0). \tag{5}$$

Proof Observe that $\frac{\mathrm{d}\gamma(x,y)}{\mathrm{d}\mu(x)}$ is the posterior probability $\mathrm{d}p_x(y)$, thanks to Bayes rule. The regularization term in Eq. (4) then corresponds to $\mathbb{E}_x[D(p_x,p_0)]$ as $p_0 = \nu$ and $D = \mathrm{KL}$ here. The minimization problem given by Eq. (4) is thus equivalent to Eq. (PRP) with the additional constraint $\pi_{1\#}\gamma = \mu$. Minimizing without this constraint is thus equivalent to minimizing the Sinkhorn loss over all action distributions μ. □

While the regularization term is usually only added to speed up the computations of optimal transport, it here directly appears in the cost of the original problem since it corresponds to the privacy cost! An approximation of $\mathrm{OT}_{c,\lambda}(\mu,\nu)$ can then be quickly computed for discrete distributions using Sinkhorn algorithm [18], described in Sect. 5.1.

Notice that the definition of Sinkhorn loss sometimes differs in the literature and instead uses $\int \log\left(\mathrm{d}\gamma(x,y)\right)\mathrm{d}\gamma(x,y)$ for the regularization term, thus ignoring the entropy of $\mu \otimes \nu$. When μ and ν are both fixed, the optimal transport plan γ remains the same. As μ is varying here, these notions yet become different. For this alternative definition, a minimizing distribution μ would actually be easy to compute. It is much more complex in our problem because of the presence of μ in the denominator of the logarithmic term.

With a discrete prior, we can then look for a distribution $\mu = \sum_{j=1}^{K+2} \alpha_j \delta_{x_j}$. In case of a continuous prior, it could still be approximated using sampled discrete distributions as previously done for generative models [29, 30].

Besides being a new interpretation of Sinkhorn loss, this reformulation allows a better understanding of the problem structure and reduces the dimension of the considered distributions.

5.1 Computing Sinkhorn loss

It was recently suggested to use the Sinkhorn algorithm, which has a linear convergence rate, to compute $\mathrm{OT}_{c,\lambda}(\mu, \nu)$ for distributions $\mu = \sum_{i=1}^{n} \alpha_i \delta_{x_i}$ and $\nu = \sum_{j=1}^{m} \beta_j \delta_{y_j}$ [18, 42]. With K the exponential cost matrix defined by $K_{i,j} = e^{-\frac{c(x_i, y_j)}{\lambda}}$, the unique matrix γ solution of the problem (4) has the form $\mathrm{diag}(u) K \mathrm{diag}(v)$. The Sinkhorn algorithm then updates alternatively $u \leftarrow \alpha / K v$ and $v \leftarrow \beta / K^\top u$ (with component-wise division) for n iterations or until convergence.

6 Minimization schemes

Despite the equivalence between (PRP) and the minimization of Sinkhorn loss given by Eq. (5), minimizing this quantity remains an open problem. This section suggests different possible optimization methods in this direction.

6.1 Optimization methods

This section presents different formulations of problem (5), leading to several possible optimization schemes, described in Sect. 6.2.

Convex minimization over distribution Problems (PRP) and (5) are both of the form

$$\min_{\mu \in \mathcal{P}(\mathcal{X})} J(\mu), \tag{6}$$

with J convex. Although solving such a problem is unknown in general, some methods are possible in specific cases (see e.g., [15] for a short overview).

For polynomial costs, this problem can be solved using generalized moment approaches [43], but the complexity explodes with the degree of the polynomial.

$\mathcal{P}(\mathcal{X})$ is the convex hull of Dirac distributions on $\mathcal{X}$, so Frank-Wolfe algorithm might be a good choice [38], especially to guarantee sparsity of the returned distribution using *away-steps* technique [16, 33]. Unfortunately, the Franke-Wolfe algorithm requires at each step to solve a subproblem, which is here equivalent to

$$\arg\max_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p_0(y)\exp\left(\frac{g(y)-c(x,y)}{\varepsilon}\right),$$

where g depends on the previous optimization step. This problem is computationally intractable for most cost functions, making Frank–Wolfe methods unadapted to our problem.

Problem (PRP) resembles the problem solved for computing a single step of discrete Wasserstein gradient flow [39], which is of the form

$$\min_{\mu} W_p^p(\mu,\nu)+\tau F(\mu),$$

where W_p is the p-Wasserstein distance and F a regularizing functional. Computing its minimizer is possible under some conditions (see e.g.,[60]; Chap. 9.3 [9, 27, 44, 52, 53]. However, we here minimize over the joint distribution instead of the marginal one. Moreover, we do not consider a Wasserstein distance as the cost function c is not necessarily an euclidean distance. The methods known for solving this kind of problem are unfortunately not adapted to the more general conditions considered in Problem (PRP).

Non-convex minimization Minimizing over the set of distributions remains solved only for specific cases. The most common approach instead approximates problem (6) by discretizing it as

$$\min_{\substack{x\in\mathcal{X}^m\\ \alpha\in\Delta_m}} J\left(\sum_{i=1}^{m}\alpha_i\delta_{x_i}\right). \tag{7}$$

Although this dimensionally finite problem is not convex, recent literature has shown the absence of spurious local minima for a large number of particles m (over-parameterization). These results yet hold only under restrictive conditions on the loss function and problem structure [15, 46, 72, 73, 77], which are adapted to optimization with neural networks. None of these conditions are satisfied here, making the benefit from over-parameterization uncertain. The empirical results in Sect. 7.2 yet suggest that such a phenomenon might also hold in our setting.

In general, reaching global optimality in non-convex minimization is intractable [34, 68], so we only aim at computing local minima. In practice, RMSProp and ADAM are often considered as the best algorithms in such cases, as they tend to avoid bad local minima thanks to the use of specific momentums [35, 40]. They yet remain little understood in theory [62, 80].

Minimax formulation Note that the dual formulation ([60] Proposition 4.4) of Eq. (4) allows the following formulation of the optimization problem (5):

$$\min_{\mu\in\mathcal{P}(\mathcal{X})}\max_{\substack{f\in\mathcal{C}(\mathcal{X})\\ g\in\mathcal{C}(\mathcal{Y})}} \langle\mu,f\rangle+\langle p_0,g\rangle-\lambda\langle\mu\otimes p_0,\ \exp((f\oplus g-c)/\lambda)\rangle, \tag{8}$$

where $\langle \mu, f \rangle := \int_{\mathcal{X}} f(x)\mathrm{d}\mu(x)$ for a distribution μ and a continuous function f on $\mathcal{X}$, $\mu \otimes p_0$ is the product distribution and $f \oplus g(x, y) = f(x) + g(y)$. This corresponds to a minimax problem of the form $\min_x \max_y \psi(x, y)$ where $\psi(\cdot, y)$ is convex for any y and $\psi(x, \cdot)$ is concave for any x. Such problems appear in many applications and have been extensively studied. We refer to [13, 48, 57, 75] for detailed surveys on the topic.

As we are considering the discretized problem (7), we are actually in the nonconvex-concave setting where ψ is nonconvex on its first variable and concave on its second. Algorithms with theoretical convergence rates to local minima have been studied in this specific setting [47–49, 58, 59, 61, 75]. Most of them alternate (accelerated) gradient descent on x and gradient ascent on y, while considering a regularized version ψ_ε of ψ.

Their interests are mostly theoretical as ADAM and RMSProp on the first coordinate instead of gradient descent should converge to better local minima in practice, similarly to nonconvex minimization. In practice, they still provide good heuristics as shown in Sect. 7.2.

On minimizing Sinkhorn divergence Ballu et al. [8] recently proposed a method to solve the minimization problem (5). Unfortunately, they consider discrete distributions and focus on reducing the dependency in the size of their supports. More importantly, this method adds a regularization term $\eta KL(\mu, \beta)$ for some reference measure β and requires this regularizer to be more significant than the one originally in the Sinkhorn loss, i.e., $\eta \geq \lambda$. While this does not add any trouble when considering regimes where both are close to 0, we here consider fixed λ, potentially far from 0 as explained in Sect. 5. The scaling factor η thus cannot be negligible, making this method unadapted to our case.

6.2 Different algorithms

Using the previous formulations, we propose several algorithms to solve the optimization problem (5), which are compared experimentally in Sect. 7.2. As explained above, we consider the discrete but non-convex formulation:

$$\min_{\substack{x \in \mathcal{X}^m \\ \alpha \in \Delta_m}} \mathrm{OT}_{c,\lambda}\left(\sum_{i=1}^{m} \alpha_i \delta_{x_i}, p_0\right). \tag{9}$$

We first consider ADAM and RMSProp algorithms for this problem. Note that the gradient of the Sinkhorn loss [25] is given by $\nabla \mathrm{OT}_{c,\lambda}(\mu, \nu) = (f, g)$, where f and g are the solutions of the dual problem given by Eq. (8), i.e., $(f, g) = \lambda(\log(u), \log(v))$ where u and v are the vectors computed by the Sinkhorn algorithm presented in Sect. 5.1. The gradient of $\mathrm{OT}_{c,\lambda}$ can then only be approximated, as it is the solution of an optimization problem. Luckily, first order optimization methods can still be used with inexact gradients [20]. Two approximations of the gradient are possible.

Analytic differentiation: $\nabla \mathrm{OT}_{c,\lambda}(\mu, \nu)$ is approximated by $(f^{(n)}, g^{(n)})$, which are the dual variables obtained after n iterations of the Sinkhorn algorithm.

Automatic differentiation: the gradient is computed via the chain rule over the successive operations processed during the Sinkhorn algorithm.

These two methods have been recently compared by Ablin et al. [1] and showed to perform similarly for a fixed computation time.

For each optimization step, the gradient $\nabla \mathrm{OT}_{c,\lambda}$ is approximated by computing $(u_t^{(k+1)}, v_t^{(k+1)}) \leftarrow (\alpha/Kv_t^{(k)}, \beta/K^\top u_t^{(k+1)})$ for n iterates. However, if the distribution μ_t did not significantly change since the last step, the gradient does not change too much as well. Instead of starting the Sinkhorn algorithm from scratch ($u_t^{(0)} = \mathbf{1}$), we instead want to use the last optimization step ($u_t^{(0)} = u_{t-1}^{(n)}$) to converge faster. Note that this technique, which we call *warm restart*, cannot be coupled with *automatic differentiation* as it would require nt backpropagation operations for the optimization step t.

The iteration step $(u, v) \leftarrow (\alpha/Kv, \beta/K^\top u)$ actually corresponds to a gradient ascent step on (f, g) in the minimax formulation given by Eq. (8). The *warm restart* technique then just corresponds to alternating optimization steps between the primal and dual variables, which is classical in minimax optimization.

To summarize, here are the different features of the optimization scheme to compare in Sect. 7.2.

Optimizer: the general used algorithm, i.e., ADAM, RMSProp or accelerated gradient descent (AGD).

Differentiation: whether we use automatic or analytic differentiation.

Warm restart: whether we use the warm restart technique, which is only compatible with analytic differentiation.

7 Experiments and particular cases

In this section, the case of linear utility cost is first considered and shown to have relations with DC programming. The performances of different optimization schemes are then compared on a simple example. Simulations based on the Sinkhorn scheme are then run for the real problem of online repeated auctions. The code is publicly available at https://github.com/eboursier/regularized_private_learning.

7.1 Linear utility cost

Section 4 described a general optimization scheme for (PRP) with a discrete type prior. Its objective is to find local minima, for a dimensionally finite, non-convex problem, using classical algorithms [79]. However in some particular cases, better schemes are possible as claimed in Sects. 5 and 6 for the particular case of entropic regularization. In the case of a linear utility for any privacy cost, it is related to DC programming [37]. A standard DC program is of the form $\min_{x \in \mathcal{X}} f(x) - g(x)$, where both f and g are convex functions. Specific optimization schemes are then possible [36, 37, 74]. In the case of linear utility costs over a hyperrectangle, (PRP) can be reformulated as a DC program stated in Theorem 4.

Theorem 4 *If $\mathcal{X} = \prod_{l=1}^{d}[a_l,\ b_l]$ and $c(x, y) = x^\top y$, define $\phi(y)^l := (b_l - a_l)y^l/2$ and $h_k(\gamma_i) := \left(\sum_{m=1}^{K} \gamma_{i,m}\right) f\left(\frac{\gamma_{i,k}}{p_0^k \sum_{m=1}^{K} \gamma_{i,m}}\right)$. Then (PRP) is equivalent to the following DC program:*

$$\min_{\gamma \in \mathbb{R}_+^{(K+2)\times K}} \lambda \sum_{i,k} p_0^k h_k(\gamma_i) - \sum_{i=1}^{K+2} \left\| \sum_{k=1}^{K} \gamma_{i,k}\phi(y_k) \right\|_1,$$

$$\text{such that for all } k \leq K,\ \sum_{i=1}^{K+2} \gamma_{i,k} = p_0^k.$$

Proof Let ψ be the rescaling of $\mathcal{X}$ to $[-1, 1]^d$, i.e., $\psi(x)^l := \frac{2x^l - b_l - a_l}{b_l - a_l}$. Then, $c(x, y) = \psi(x)^T\phi(y) + \eta(y)$ where $\phi(y)^l := (b_l - a_l)\frac{y^l}{2}$ and $\eta(y) = \sum_{l=1}^{d} \frac{a_l + b_l}{b_l - a_l} y^l$. The problem given by Corollary 1 is then equivalent to minimizing

$$\sum_{i,k} \gamma_{i,k}(x_i^\top \phi(y_k) + \eta(y_k)) + \lambda \sum_{i,k} p_0^k h_k(\gamma_i),$$

for $x \in [-1, 1]^{d\times(K+2)}$. Because of the marginal constraints, $\sum_{i,k} \gamma_{i,k}\eta(y_k) = \sum_k p_0^k \eta(y_k)$. This sum does depend neither on x nor γ, so that the terms $\eta(y_k)$ can be omitted, i.e., we minimize

$$\sum_i x_i^\top \left(\sum_k \gamma_{i,k}\phi(y_k) \right) + \lambda \sum_{i,k} p_0^k h_k(\gamma_i).$$

It is clear that for a fixed γ, the best x_i corresponds to $x_i^l = -\mathrm{sign}(\sum_k \gamma_{i,k}\phi(y_k)^l)$ and the term $x_i^\top \left(\sum_k \gamma_{i,k}\phi(y_k)\right)$ then corresponds to the opposite of the 1-norm of $\sum_k \gamma_{i,k}\phi(y_k)$, i.e., the problem then minimizes

$$-\sum_i \left\| \sum_k \gamma_{i,k}\phi(y_k) \right\|_1 + \lambda \sum_{i,k} p_0^k h_k(\gamma_i).$$

□

More generally, if the cost c is concave and the action space $\mathcal{X}$ is a polytope, optimal actions are located on the vertices of $\mathcal{X}$. In that case, $\mathcal{X}$ can be replaced by the set of its vertices and the problem becomes dimensionally finite. Unfortunately, for some polytopes such as hyperrectangles, the number of vertices grows exponentially with the dimension and the optimization scheme is no longer tractable in large dimensions.

7.2 Minimize Sinkhorn loss on the toy example

This section compares empirically different ways of minimizing the Sinkhorn loss as described in Sect. 6.2. We consider the linear utility loss $c(x, y) = x^\top y$ over the space

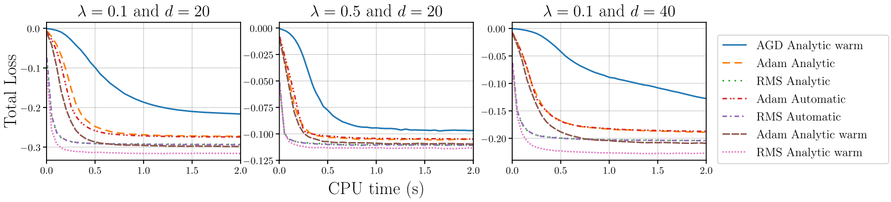


Fig. 2 Comparison of different features for Sinkhorn minimization

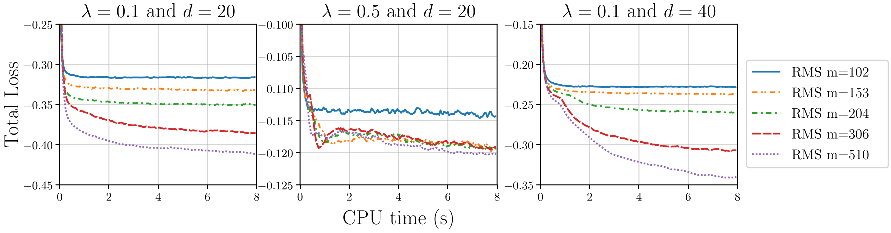


Fig. 3 Influence of number of actions m

$\mathcal{X} = [-1, 1]^d$ and the Kullback–Leibler divergence for privacy cost, so that both DC and Sinkhorn schemes are possible. The comparison with DC scheme is available in Sect. 7.3.

We optimized using well tuned learning rates. The prior p_0^k is chosen proportional to e^{Z_k} for any $k \in [K]$, where Z_k is drawn uniformly at random in $[0, 1]$ and $K = 100$. Each y_k^i is taken uniformly at random in $[-1, 1]$ and is rescaled so that $\|y_k\|_1 = 1$. The values are averaged over 200 runs.

Figure 2 compares the different features described at the end of Sect. 6.2 for different problem parameters. As suggested by Ablin et al. [1], the algorithms perform similarly with automatic and analytic differentiation. However, the analytic differentiation allows to use the *warm restart* technique which, coupled with RMSProp, yields better performances as shown in Fig. 2.

Figure 3 on the other hand studies the influence of the chosen number of actions,[3] which is the parameter m in Eq. (9). As expected, the larger the number of actions, the better. Note that for $\lambda = 0.5$, increasing the number of actions has no real influence after $m \geq 153$. The global minimum might always be reached in this case; and this minimum does not depend on m as soon as it is greater than $K + 2$, thanks to Theorem 2. It yet remains unkown whether the reached minima are global minima when the number of actions tends to infinity (over-parameterization).

7.3 Comparing methods on the toy example

We now compare the performance of Sinkhorn minimization with different algorithms on the toy example described in Sect. 7.2 for $m = K + 2$ actions.

[3] The comparison is done with RMSProp and warm restart, since it yields the best results for a fixed number of actions.

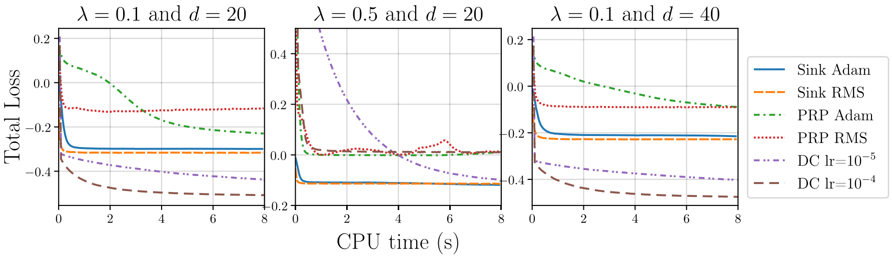


Fig. 4 Comparison of optimization schemes. `lr` is the learning rate used for DC

Different methods exist for DC programming and they compute either a local or a global minimum. We here choose the DCA algorithm [74] as it computes a local minimum and is thus comparable to the other considered schemes. Figure 4 compares the best Sinkhorn scheme in Sect. 7.2 with DCA and PRP method, which uses ADAM or RMSProp optimizers for the minimization problem (3).

The DC method finds better local minima than the other ones. This was already observed in practice [74] and confirms that it is more adapted to the structure of the problem, despite being only applicable in very specific cases such as linear cost on hyperrectangles. Also, the PRP method converges to worse spurious local minima as it optimizes in higher dimensional spaces than the Sinkhorn method. We also observed in our experiments that PRP method is more sensitive to problem parameters than Sinkhorn method.

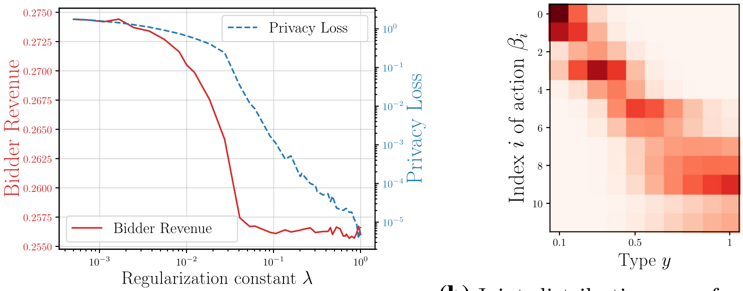
The Sinkhorn method seems to perform better for larger values of λ. Indeed, given the actions, the Sinkhorn method computes the best joint distribution for each iteration and thus performs well when the privacy cost is predominant, while DCA computes the best actions given a joint distribution and thus performs well when the utility cost is predominant. It is thus crucial to choose the method which is most adapted to the problem structure as it can lead to significant improvement in the solution.

7.4 Utility-privacy in repeated auctions

For repeated second price auctions following a precise scheme [45], there exist numerical methods to implement an optimal strategy for the bidder [56]. However, if the auctioneer knows that the bidder plays such a strategy, he can still infer the bidder's type and adapt to it. We thus require to add a privacy cost to avoid this kind of behavior from the auctioneer as described in Sect. 2.1.

For simplicity, bidder's valuations are assumed to be exponential distributions, so that the private type y is the parameter of this distribution, i.e., its expectation: $y = \mathbb{E}_{v \sim \mu_y}[v]$. Moreover, we assume that the prior p_0 over y is the discretized uniform distribution on [0, 1] with a support of size $K = 10$; let $\{y_k\}_{k=1,\ldots,K}$ be the support of p_0.

In repeated auctions, values v are repeatedly sampled from the distribution μ_{y_k} and a bidder policy is a mapping $\beta(\cdot)$ from values to bids, i.e., she bids $\beta(v)$ if her value is v. So a type y_k and a policy $\beta(\cdot)$ generate the bid distribution $\beta_{\#}\mu_{y_k}$, which



(a) Evolution of privacy-utility with λ.

(b) Joint distribution map for $\lambda = 0.01$. The intensity of a point (i, k) corresponds to the value of $\gamma(\beta_i, y_k)$.

Fig. 5 Privacy-utility trade-off in online repeated auctions

corresponds to an action in $\mathcal{X}$ in our setting. As a consequence, the set of actions of the agent are the probability distributions over $\mathbb{R}_+$ and an action ρ_i is naturally generated from the valuation distribution via the optimal monotone transport map denoted by β_k^i, i.e., $\rho_i = \beta_{k\#}^i \mu_{y_k}$ [66]. In the particular case of exponential distributions, this implies that $\beta_i^k(v) = \beta_i(v/y_k)$ where β_i is the unique monotone transport map from Exp(1) to ρ_i. The revenue of the bidder is then deduced for exponential distributions [56] as

$$\begin{aligned} r(\beta_i, y_k) &= 1 - c(\beta_i, y_k) \\ &= \mathbb{E}_{v \sim \text{Exp}(1)}\left[\left(y_k v - \beta_i(v) + \beta_i'(v)\right) G\left(\beta_i(v)\right) \mathbb{1}_{\beta_i(v) - \beta_i'(v) \geq 0}\right], \end{aligned}$$

where G is the *c.d.f.* of the maximum bid of the other bidders. We here consider a single truthful opponent with a uniform value distribution on $[0, 1]$, so that $G(x) = \min(x, 1)$. This utility is averaged over 10^3 values drawn from the corresponding distribution at each training step and 10^6 values for the final evaluation.

Considering the KL for privacy cost, we compute a strategy (γ, β) using the Sinkhorn scheme yielding the best results in Sect. 7.2. Every action β_i is parametrized as a single layer neural network of 100 ReLUs. Figure 5a represents both utility and privacy as a function of the regularization factor λ.

Naturally, both the bidder revenue and the privacy loss decrease with λ, going from revealing strategies for $\lambda \simeq 10^{-3}$ to non-revealing strategies for larger λ. They significantly drop at a critical point near 0.05, which can be seen as the cost of information here. There is a 7% revenue difference[4] between the non revealing strategy and the partially revealing strategy shown in Fig. 5b. The latter randomizes the type over its neighbors and reveals more information when the revenue is sensible to the action, i.e., for low types y_k here. This strategy thus takes advantage from the fact that the value of information is here heterogeneous among types, as desired in the design of our model.

Figure 6 shows the most used action for different types and λ. In the revealing strategy ($\lambda = 0$), the action significantly scales with the type. But as λ grows, this

[4] Which is significant for large firms such as those presented in Figure 1 besides the revenue difference brought by considering non truthful strategies [56].

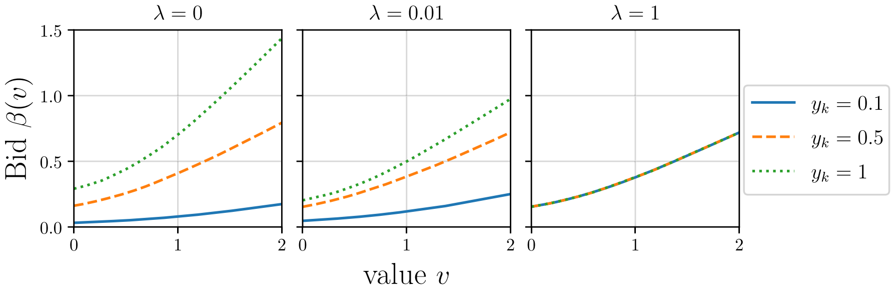


Fig. 6 Evolution of the bidding strategy with the type and the regularization constant

rescaling shrinks so that the actions perform for several types, until having a single action in the non-revealing strategy. This shrinkage is also more important for large values of y_k. This confirms the observation made above: the player loses less by hiding her type for large values than for low values and she is thus more willing to hide her type when it is large.

Besides confirming expected results, this illustrates how the Privacy Regularized Policy is adapted to complex utility costs and action spaces, such as distributions or function spaces.

8 Conclusion

We formalized a new utility-privacy trade-off problem to compute strategies revealing private information only if it induces a significant increase in utility. For classical Bayesian costs, it benefits from recent advances in Optimal Transport. It yet leads to a non-convex minimization problem for which only heuristics are available. The computation of global minima yet remains open.

We believe that this work is a step towards the design of optimal utility vs. privacy trade-offs in economic mechanisms as well as for other applications. Its numerous connexions with recent topics of interest motivate a better understanding of them as future work.

Funding Open access funding provided by EPFL Lausanne Etienne Boursier was supported by an AMX scholarship. Vianney Perchet was supported by a public grant as part of the Investissement d'avenir project, reference ANR-11-LABX-0056-LMH, LabEx LMH, in a joint call with Gaspard Monge Program for optimization, operations research and their interactions with data sciences and by the French Agence Nationale de la Recherche under the Grant Number ANR19-CE23-0026-04.

Data Availability Not applicable

Code Availability All the code used in this paper is publicly available at https://github.com/eboursier/regularized_private_learning.

Declarations

Conflict of interest No relevant CoI to declare.

References

1. Ablin, P., Peyré, G., Moreau, T.: Super-efficiency of automatic differentiation for functions defined as a minimum. arXiv preprint arXiv:2002.03722 (2020)
2. Amin, K., Rostamizadeh, A., Syed, U.: Learning prices for repeated auctions with strategic buyers. In: Advances in Neural Information Processing Systems, pp. 1169–1177 (2013)
3. Amin, K., Rostamizadeh, A., Syed, U.: Repeated contextual auctions with strategic buyers. In: Advances in Neural Information Processing Systems, pp. 622–630 (2014)
4. Arjovsky, M., Chintala, S., Bottou, L.: Wasserstein generative adversarial networks. In: International Conference on Machine Learning, pp. 214–223 (2017)
5. Aumann, R., Maschler, M., Stearns, R.: Repeated Games with Incomplete Information. MIT Press (1995)
6. Balinski, M.L., Gomory, R.E.: A primal method for the assignment and transportation problems. Manage. Sci. **10**(3), 578–593 (1964)
7. Balinski, M.L., Rispoli, F.J.: Signature classes of transportation polytopes. Math. Progr. **60**(1), 127–144 (1993)
8. Ballu, M., Berthet, Q., Bach, F.: Stochastic optimization for regularized Wasserstein estimators. arXiv preprint arXiv:2002.08695 (2020)
9. Benamou, J.-D., Carlier, G., Mérigot, Q., Oudet, E.: Discretization of functionals involving the Monge–Ampère operator. Numer. Math. **134**(3), 611–636 (2016)
10. Bourse, F., Minelli, M., Minihold, M., Paillier, P.: Fast homomorphic evaluation of deep discretized neural networks. In: Annual International Cryptology Conference, pp. 483–512 (2018)
11. Boursier, E., Perchet, V.: Utility/privacy trade-off through the lens of optimal transport. In: International Conference on Artificial Intelligence and Statistics, pp. 591–601 (2020)
12. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press (2004)
13. Chambolle, A., Pock, T.: An introduction to continuous optimization for imaging. Acta Numer. **25**, 161–319 (2016)
14. Chaudhuri, K., Imola, J., Machanavajjhala, A.: Capacity bounded differential privacy. In: Advances in Neural Information Processing Systems, pp. 3469–3478 (2019)
15. Chizat, L., Bach, F.: On the global convergence of gradient descent for over-parameterized models using optimal transport. In: Advances in Neural Information Processing Systems, pp. 3036–3046 (2018)
16. Clarkson, K.L.: Coresets, sparse greedy approximation, and the Frank–Wolfe algorithm. ACM Trans. Algorithms (TALG) **6**(4), 1–30 (2010)
17. Courty, N., Flamary, R., Tuia, D.: Domain adaptation with regularized optimal transport. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, pp. 274–289 (2014)
18. Cuturi, M.: Sinkhorn distances: Lightspeed computation of optimal transport. In: Advances in Neural Information Processing Systems, pp. 2292–2300 (2013)
19. Delon, J., Salomon, J., Sobolevski, A.: Local matching indicators for transport problems with concave costs. SIAM J. Discret. Math. **26**(2), 801–827 (2012)
20. Devolder, O., Glineur, F., Nesterov, Y.: First-order methods of smooth convex optimization with inexact oracle. Math. Progr. **146**(1–2), 37–75 (2014)
21. Dwork, C.: Differential privacy. In: Encyclopedia of Cryptography and Security, pp. 338–340 (2011)
22. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Theory of Cryptography Conference, pp. 265–284. Springer (2006)

23. Eilat, R., Eliaz, K., Mu, X.: Optimal Privacy-Constrained Mechanisms. C.E.P.R. Discussion Papers, Technical Report (2019)
24. Feldman, M., Koren, T., Livni, R., Mansour, Y., Zohar, A.: Online pricing with strategic and patient buyers. In: Advances in Neural Information Processing Systems, pp. 3864–3872 (2016)
25. Feydy, J., Séjourné, T., Vialard, F.-X., Amari, S.I., Trouve, A., Peyré, G.: Interpolating between optimal transport and mmd using Sinkhorn divergences. In: The 22nd International Conference on Artificial Intelligence and Statistics, pp. 2681–2690 (2019)
26. Frogner, C., Zhang, C., Mobahi, H., Araya-Polo, M., Poggio, T.: Learning with a Wasserstein loss. In: Advances in Neural Information Processing Systems (2015)
27. Gallouët, T.O., Mérigot, Q.: A Lagrangian scheme à la Brenier for the incompressible Euler equations. Found. Comput. Math. **18**(4), 835–865 (2018)
28. Genevay, A., Cuturi, M., Peyré, G., Bach, F.: Stochastic optimization for large-scale optimal transport. In: Advances in Neural Information Processing Systems, pp. 3440–3448 (2016)
29. Genevay, A., Peyre, G., Cuturi, M.: Learning generative models with Sinkhorn divergences. In: International Conference on Artificial Intelligence and Statistics, pp. 1608–1617 (2018)
30. Genevay, A., Chizat, L., Bach, F., Cuturi, M., Peyré, G.: Sample complexity of Sinkhorn divergences. In: The 22nd International Conference on Artificial Intelligence and Statistics, pp. 1574–1583 (2019)
31. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., Wernsing, J.: Cryptonets: applying neural networks to encrypted data with high throughput and accuracy. In: International Conference on Machine Learning, pp. 201–210 (2016)
32. Golrezaei, N., Javanmard, A., Mirrokni, V.: Dynamic incentive-aware learning: robust pricing in contextual auctions. In: Advances in Neural Information Processing Systems, pp. 9756–9766 (2019)
33. Guélat, J., Marcotte, P.: Some comments on Wolfe's 'away step'. Math. Progr. **35**(1), 110–119 (1986)
34. Hendrix, E., Boglárka, G., et al.: Introduction to Nonlinear and Global Optimization, vol. 37. Springer (2010)
35. Hinton, G., Srivastava, N., Swersky, K.: Neural networks for machine learning lecture 6a overview of mini-batch gradient descent. Cited on **14**(8), 2 (2012)
36. Horst, R., Thoai, N.: DC programming: overview. J. Optim. Theory Appl. **103**(1), 1–43 (1999)
37. Horst, R., Pardalos, P., Thoai, N.V.: Introduction to Global Optimization. Springer (2000)
38. Jaggi, M.: Revisiting Frank–Wolfe: projection-free sparse convex optimization. In: Proceedings of the 30th International Conference on Machine Learning, pp. 427–435 (2013)
39. Jordan, R., Kinderlehrer, D., Otto, F.: The variational formulation of the Fokker–Planck equation. SIAM J. Math. Anal. **29**(1), 1–17 (1998)
40. Kingma, D., Ba, J.: Adam: a method for stochastic optimization. arXiv preprint arXiv:1412.6980 (2014)
41. Kleinschmidt, P., Lee, C.W., Schannath, H.: Transportation problems which can be solved by the use of Hirsch-paths for the dual problems. Math. Progr. **37**(2), 153–168 (1987)
42. Knight, P.: The Sinkhorn–Knopp algorithm: convergence and applications. SIAM J. Matrix Anal. Appl. **30**(1), 261–275 (2008)
43. Lasserre, J.: Global optimization with polynomials and the problem of moments. SIAM J. Optim. **11**(3), 796–817 (2001)
44. Leclerc, H., Mérigot, Q., Santambrogio, F., Stra, F.: Lagrangian discretization of crowd motion and linear diffusion. SIAM J. Numer. Anal. **58**(4), 2093–2118 (2020)
45. Leme, R.P., Pal, M., Vassilvitskii, S.: A field guide to personalized reserve prices. In: Proceedings of the 25th International Conference on World Wide Web, pp. 1093–1102 (2016)
46. Li, Y., Yuan, Y.: Convergence analysis of two-layer neural networks with Relu activation. In: Advances in Neural Information Processing Systems, pp. 597–607 (2017)
47. Lin, T., Jin, C., Jordan, M.: On gradient descent ascent for nonconvex-concave minimax problems. arXiv preprint arXiv:1906.00331 (2019)
48. Lin, T., Jin, C., Jordan, M.: Near-optimal algorithms for minimax optimization. arXiv preprint arXiv:2002.02417 (2020)
49. Lu, S., Tsaknakis, I., Hong, M., Chen, Y.: Hybrid block successive approximation for one-sided nonconvex min-max problems: algorithms and applications. IEEE Trans. Signal Process. **68**, 3676–3691 (2020)
50. Maćkowiak, B., Wiederholt, M.: Business cycle dynamics under rational inattention. Rev. Econ. Stud. **82**(4), 1502–1532 (2015)

51. Matějka, F., McKay, A.: Rational inattention to discrete choices: a new foundation for the multinomial logit model. Am. Econ. Rev. **105**(1), 272–98 (2015)
52. Mérigot, Q., Mirebeau, J.-M.: Minimal geodesics along volume-preserving maps, through semidiscrete optimal transport. SIAM J. Numer. Anal. **54**(6), 3465–3492 (2016)
53. Mérigot, Q., Santambrogio, F., Sarrazin, C.: Non-asymptotic convergence bounds for Wasserstein approximation using point clouds. Adv. Neural Inf. Process. Syst. **34** (2021)
54. Mironov, I.: Rényi differential privacy. In: Proceedings of 30th IEEE Computer Security Foundations Symposium (CSF), pp. 263–275 (2017)
55. Munkres, J.: Algorithms for the assignment and transportation problems. J. Soc. Ind. Appl. Math. **5**(1), 32–38 (1957)
56. Nedelec, T., Karoui, N.E., Perchet, V.: Learning to bid in revenue-maximizing auctions. In: International Conference on Machine Learning, pp. 4781–4789 (2019)
57. Nedić, A., Ozdaglar, A.: Subgradient methods for saddle-point problems. J. Optim. Theory Appl. **142**(1), 205–228 (2009)
58. Nouiehed, M., Sanjabi, M., Huang, T., Lee, J., Razaviyayn, M.: Solving a class of non-convex min-max games using iterative first order methods. In: Advances in Neural Information Processing Systems, pp. 14934–14942 (2019)
59. Ostrovskii, D., Lowy, A., Razaviyayn, M.: Efficient search of first-order Nash equilibria in nonconvex-concave smooth min-max problems. arXiv preprint arXiv:2002.07919 (2020)
60. Peyré, G., Cuturi, M.: Computational optimal transport. Found. Trends® Mach. Learn. 11(5–6): 355–607 (2019)
61. Rafique, H., Liu, M., Lin, Q., Yang, T.: Non-convex min-max optimization: provable algorithms and applications in machine learning. arXiv preprint arXiv:1810.02060 (2018)
62. Reddi, S., Kale, S., Kumar, S.: On the convergence of adam and beyond. arXiv preprint arXiv:1904.09237 (2019)
63. Reed, J., Pierce, B.: Distance makes the types grow stronger: a calculus for differential privacy. ACM Sigplan Not. **45**, 157–168 (2010)
64. Rényi, A.: On measures of entropy and information. In: Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics (1961)
65. Salimans, T., Metaxas, D., Zhang, H., Radford, A.: Improving gans using optimal transport. In: 6th International Conference on Learning Representations, ICLR 2018 (2018)
66. Santambrogio, F.: Optimal transport for applied mathematicians. Birkäuser, NY **55**, 58–63 (2015)
67. Sanyal, A., Kusner, M., Gascon, A., Kanade, V.: Tapas: tricks to accelerate (encrypted) prediction as a service. In: International conference on machine learning, pp. 4497–4506 (2018)
68. Sergeyev, Y., Strongin, R., Lera, D.: Introduction to Global Optimization Exploiting Space-filling Curves. Springer (2013)
69. Sims, C.: Implications of rational inattention. J. Monet. Econ. **50**(3), 665–690 (2003)
70. Sinkhorn, R.: Diagonal equivalence to matrices with prescribed row and column sums. Am. Math. Mon. **74**(4), 402–405 (1967)
71. Smith, G.: On the foundations of quantitative information flow. In: International Conference on Foundations of Software Science and Computational Structures, pp. 288–302 (2009)
72. Soltanolkotabi, M., Javanmard, A., Lee, J.: Theoretical insights into the optimization landscape of over-parameterized shallow neural networks. IEEE Trans. Inf. Theory **65**(2), 742–769 (2018)
73. Soudry, D., Hoffer, E.: Exponentially vanishing sub-optimal local minima in multilayer neural networks. arXiv preprint arXiv:1702.05777 (2017)
74. Tao, P., An, L.: Convex analysis approach to DC programming: theory, algorithms and applications. Acta Math. Vietnam **22**(1), 289–355 (1997)
75. Thekumparampil, K., Jain, P., Netrapalli, P., Oh, S.: Efficient algorithms for smooth minimax optimization. In: Advances in Neural Information Processing Systems, pp. 12680–12691 (2019)
76. Tóth, G., Hornák, Z., Vajda, F.: Measuring anonymity revisited. In: Proceedings of the 9th Nordic Workshop on Secure IT Systems, pp. 85–90 (2004)
77. Venturi, L., Bandeira, A., Bruna, J.: Spurious valleys in two-layer neural network optimization landscapes. arXiv preprint arXiv:1802.06384 (2018)
78. Villani, C.: Optimal Transport: Old and New, vol. 338. Springer (2008)
79. Wright, S.: Coordinate descent algorithms. Math. Progr. **151**(1), 3–34 (2015)

80. Zou, F., Shen, L., Jie, Z., Zhang, W., Liu, W.: A sufficient condition for convergences of adam and rmsprop. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 11127–11135 (2019)