Private optimization without constraint violations

Andrés Muñoz Medina, Umar Syed, Sergei Vassilvitskii, Ellen Vitercik

Google Research and UC Berkeley
AISTATS’21
Goal: Privately find $x \in \mathbb{R}^n$ maximizing $g(x)$ such that $Ax \leq b(D)$

Solution can’t violate any constraint
Crucial in many applications, such as resource allocation
Example: linear programming

**Goal:** Decide which pharmacies should supply which hospitals

**RHS of constraints is private:**
Indicates number of patients with disease at each hospital

If constraints violated, hospital can’t treat all patients
Our contributions

1. Differentially-private algorithm

2. **Main result:** Nearly-matching lower bound on loss
   Matching up to log factors
Most related prior research

Differentially private linear programming
Hsu et al., ICALP’14; Cummings et al., WINE’15

Primary distinctions:
• Specific to linear programming
• Allow constraints to be violated by bounded amount
• Constraints \((A, b)\) and objective function can be private
Outline

1. Introduction
2. **Background: Differential privacy**
3. Algorithm
4. Lower bound
5. Experiments
6. Conclusion
Differential privacy

\( x(D) \in \mathbb{R}^n \): algorithm’s output given database \( D \)

Algorithm is **differentially private** if:

\( x(D) \) reveals (almost) nothing more about a record in \( D \) than it would have if the record wasn’t in \( D \)
Differential privacy

\( x(D) \in \mathbb{R}^n \): algorithm’s output given database \( D \)
Differential privacy

\(x(D) \in \mathbb{R}^n: \text{algorithm's output given database } D\)
Differential privacy

Two databases $D, D'$ are neighboring if differ on $\leq 1$ element.
Denoted $D \sim D'$

Algorithm is $(\varepsilon, \delta)$-differentially private if:
For any $D \sim D'$ and $V \subseteq \mathbb{R}^n$, $\mathbb{P}[x(D) \in V] \leq e^{\varepsilon} \mathbb{P}[x(D') \in V] + \delta$
Outline

1. Introduction
2. Background: Differential privacy
3. **Algorithm**
4. Lower bound
5. Experiments
6. Conclusion
Feasibility assumption

If feasible region changes too much between databases:
Private optimization w/o constraint violations is **impossible**

Assumption: $\bigcap_{D \subseteq X} \{x : Ax \leq b(D)\} \neq \emptyset$
E.g., it includes the origin

In particular, $\bigcap_{D \subseteq X} \{x : Ax \leq b(D)\} = \{x : Ax \leq (b_1^*, ..., b_m^*)\}$

There’s no $(\epsilon, \delta)$-DP algorithm with $\delta < 1$
Algorithm

1. Map constraint vector $b(D) \mapsto \overline{b}(D)$ such that $\overline{b}(D) \leq b(D)$ using the Truncated Laplace Mechanism
Algorithm

1. Map constraint vector $\mathbf{b}(D) \mapsto \overline{\mathbf{b}}(D)$ such that $\overline{\mathbf{b}}(D) \leq \mathbf{b}(D)$:
   - Sensitivity: $\Delta = \max_{D \sim D'} \|\mathbf{b}(D) - \mathbf{b}(D')\|_1$
   - $s = \frac{\Delta}{\varepsilon} \ln \left( \frac{m(e^\varepsilon - 1)}{\delta} + 1 \right)$
   - $\eta_i = \text{Truncated Laplace noise with scale } \frac{\Delta}{\varepsilon} \text{ and support } [-s, s]$
   - $\overline{\mathbf{b}}(D)_i = \max\{\mathbf{b}(D)_i - s + \eta_i, b_i^*\}$
Algorithm

1. Map constraint vector $\mathbf{b}(D) \mapsto \bar{\mathbf{b}}(D)$ such that $\bar{\mathbf{b}}(D) \leq \mathbf{b}(D)$ using the Truncated Laplace Mechanism
2. Return $\mathbf{x} \in \mathbb{R}^n$ maximizing $g(\mathbf{x})$ such that $A\mathbf{x} \leq \bar{\mathbf{b}}(D)$

Important properties:

1. Satisfies **constraints** with probability 1
   \[ A\mathbf{x} \leq \bar{\mathbf{b}}(D) \leq \mathbf{b}(D) \]
2. Satisfies $(\varepsilon, \delta)$-DP
   Truncated Laplace is private
Outline

1. Introduction
2. Background: Differential privacy
3. Algorithm
   - Quality guarantee
4. Lower bound
5. Experiments
6. Conclusion
Linear system condition number

\[ \alpha_{p,q}(A) = \sup_{u \geq 0} \left\{ \|u\|_{p^*} : \|A^T u\|_{q^*} = 1 \text{ & the rows of } A \text{ corresponding to nonzero components of } u \text{ are linearly independent} \right\} \]

E.g., when \( p = q = 2 \) and \( A \) is nonsingular, \( \alpha_{p,q}(A) = \sigma_{\min}^{-1}(A) \)

**Theorem [Li, '93]:**

- Let \( S = \{ x : Ax \leq b \} \) and \( S' = \{ x : Ax \leq b' \} \)
- For all \( x \in S, \inf_{x' \in S'} \|x - x'\|_q \leq \alpha_{p,q}(A) \|b - b'\|_p \)
Quality guarantee

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x) \leq \Delta \cdot L \cdot \inf \quad \alpha^*, A$$

Optimal solution
Quality guarantee

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $||\cdot||_q$. Then

$$g(x^*) - g(x(D))$$
Quality guarantee

Upper bound: Suppose $g$ is $L$-Lipschitz under $\| \cdot \|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta$$
Quality guarantee

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta \cdot L \cdot \inf_{p \geq 1} \{ \alpha_{p,q}(A)^p \sqrt{m} \}$$

Number of constraints
Quality guarantee

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta \cdot L \cdot \inf_{p \geq 1} \{\alpha_{p,q}(A)^p \sqrt{m}\} \cdot \frac{2}{\varepsilon} \cdot \ln \left( \frac{m(e^\varepsilon - 1)}{\delta} + 1 \right)$$

(\varepsilon, \delta)-differential privacy
Nearly-matching lower bound

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta \cdot L \cdot \inf_{p \geq 1} \{ \alpha_{p,q}(A)^p \sqrt{m} \} \cdot \frac{2}{\varepsilon} \cdot \ln \left( \frac{m(e^{\varepsilon} - 1)}{\delta} + 1 \right)$$

**Lower bnd (informal):** Exist problems s.t. for any $(\varepsilon, \delta)$-DP alg,

$$g(x^*) - \mathbb{E}[g(x(D))] \geq \Delta \cdot L \cdot \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{1}{4\varepsilon} \cdot \ln \left( \frac{e^{\varepsilon} - 1}{2\delta} + 1 \right)$$
Nearly-matching lower bound

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta \cdot L \cdot \inf_{p \geq 1} \left\{ \alpha_{p, q}(A)^p \right\} \cdot \frac{2}{\varepsilon} \cdot \ln \left( \frac{m(e^\varepsilon - 1)}{\delta} + 1 \right)$$

**Lower bnd (informal):** Exist problems s.t. for any $(\varepsilon, \delta)$-DP alg,

$$g(x^*) - \mathbb{E}[g(x(D))] \geq \Delta \cdot L \cdot \inf_{p \geq 1} \left\{ \alpha_{p, 1}(A)^p \right\} \cdot \frac{1}{4\varepsilon} \cdot \ln \left( \frac{e^\varepsilon - 1}{2\delta} + 1 \right)$$

**Takeaway:** Matching up to $O(\ln m)$
Quality upper bound

**Upper bound:** Suppose $g$ is $L$-Lipschitz under $\|\cdot\|_q$. Then

$$g(x^*) - g(x(D)) \leq \Delta \cdot L \cdot \inf_{p \geq 1} \{ \alpha_{p,q}(A)^{\frac{p}{2}} \sqrt{m} \} \cdot \frac{2}{\varepsilon} \cdot \ln \left( \frac{m(e^\varepsilon - 1)}{\delta} + 1 \right)$$

**Proof:**

- $b$: Arbitrary vector in support of $\bar{b}(D)$ and $S = \{x : Ax \leq b\}$
- From Li ['93]: $\inf_{x \in S} \|x^* - x\|_q \leq \alpha_{p,q}(A) \|b(D) - b\|_p$
- $\|b(D) - b\|_p \leq 2s^p \sqrt{m}$
Outline

1. Introduction
2. Background: Differential privacy
3. Algorithm
4. **Lower bound**
5. Experiments
6. Conclusion
Nearly-matching lower bound

**Theorem (more details):**

- $A$: arbitrary diagonal matrix
- $g(x) = \langle 1, x \rangle$
- For any $\Delta > 0$, exists mapping from databases $D$ to $b(D)$ s.t.:
  1. Sensitivity of $b(D)$ is $\Delta$
  2. For any $\epsilon > 0$, $\delta \in (0, \frac{1}{2}]$ and any $(\epsilon, \delta)$-DP algorithm,

\[
g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{\alpha_{p,1}(A)^p \sqrt{m}\} \cdot \frac{\Delta}{4\epsilon} \ln \left(\frac{e^{\epsilon-1}}{2\delta} + 1\right)
\]
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \)

*Proof sketch for 1D special case* (\( \max g(x) = x \) s.t. \( Ax \leq b(D) \)):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Lambda}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \)

Proof sketch for 1D special case \((\max g(x) = x \text{ s.t. } Ax \leq b(D))\):

- For all \(i \in \mathbb{Z}\), let \(D_i\) be a database with \(D_i \sim D_{i+1}\) & \(b(D_i) = \Delta i\)
- For any \(V \subseteq \mathbb{R}\), \(\mathbb{P}[x(D_i) \in V] \leq e^\varepsilon \mathbb{P}[x(D_{i-1}) \in V] + \delta\)

Density of \(x(D_i)\)

Only \(\delta\) mass

\[
\frac{b(D_{i-1})}{A} \quad \frac{b(D_i)}{A} = \text{optimal given } D_i
\]
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{\alpha \geq 1} \alpha_p(A)^{p \sqrt{m}} \cdot \frac{\Delta}{4\epsilon} \ln \left( \frac{e^{\epsilon-1}}{2\delta} + 1 \right) \)

Proof sketch for 1D special case \((\max g(x) = x \text{ s.t. } Ax \leq b(D))\):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
- For any \( V \subseteq \mathbb{R} \), \( \mathbb{P}[x(D_i) \in V] \leq e^{\epsilon} \mathbb{P}[x(D_{i-1}) \in V] + \delta \)

Density of \( x(D_i) \) only has \( \delta \) mass in this interval

\( \frac{b(D_{i-2})}{A} \quad \frac{b(D_{i-1})}{A} \quad \frac{b(D_i)}{A} = \text{optimal given } D_i \)
Lower bound: Proof sketch

**Theorem:** 
\[ g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \left\{ \alpha_{p,1}(A)^p \sqrt{m} \right\} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \]

Proof sketch for 1D special case (\( \max g(x) = x \) s.t. \( Ax \leq b(D) \)):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
- For any \( V \subseteq \mathbb{R} \), \( \mathbb{P}[x(D_i) \in V] \leq e^\varepsilon \mathbb{P}[x(D_{i-1}) \in V] + \delta \)

Density of \( x(D_i) \)

Only \( e^\varepsilon \delta + \delta \) mass
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \)

**Proof sketch for 1D special case** (\( \max g(x) = x \) s.t. \( Ax \leq b(D) \)):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
- For any \( V \subseteq \mathbb{R} \), \( \mathbb{P}[x(D_i) \in V] \leq e^{\varepsilon} \mathbb{P}[x(D_{i-1}) \in V] + \delta \)

Only \( \delta \sum_{\ell=0}^{t-1} e^{\varepsilon \ell} \) mass
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))]) \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A) \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon - 1}}{2\delta} + 1 \right) \)

Proof sketch for 1D special case (\( \max g(x) = x \) s.t. \( Ax \leq b(D) \)):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
- For any \( V \subseteq \mathbb{R} \), \( P[x(D_i) \in V] \leq e^{\varepsilon} P[x(D_{i-1}) \in V] + \delta \)

Only \( \delta \sum_{\ell=0}^{t-1} e^{\varepsilon \ell} \) mass
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \)

*Proof sketch for 1D special case* \((\max g(x) = x \text{ s.t. } Ax \leq b(D))\):

- For all \( i \in \mathbb{Z} \), let \( D_i \) be a database with \( D_i \sim D_{i+1} \) & \( b(D_i) = \Delta i \)
- For any \( V \subseteq \mathbb{R} \), \( \mathbb{P}[x(D_i) \in V] \leq e^{\varepsilon} \mathbb{P}[x(D_{i-1}) \in V] + \delta \)

Only \( \delta \sum_{\ell=0}^{\lceil t \rceil-1} e^{\varepsilon \ell} \) mass, which is \( \leq \frac{1}{2} \)

\[
\frac{b(D_i)}{A} = \frac{\Delta(i-|t|)}{A} \quad \text{for} \quad t = \frac{1}{\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \]

\[
\frac{b(D_i)}{A} = \text{optimal given } D_i
\]
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon - 1}}{2\delta} + 1 \right) \)

**Proof sketch for 1D special case** (\( \max g(x) = x \) s.t. \( Ax \leq b(D) \)):

Law of total exp.: \( \mathbb{E}[g(x(D_i))] \leq \frac{\Delta i}{A} - \frac{\Delta |t|}{A} \cdot \mathbb{P}[x(D_i) \leq [t]] \)

\[ \leq g(x^*) - \frac{\Delta t}{4A} \]

\[ = g(x^*) - \frac{\Delta t}{4} \cdot \alpha_{q,1}(A) \quad (\forall q) \]

\( \frac{b(D_i - [t])}{A} = \frac{\Delta(i - [t])}{A} \text{ for } t = \frac{1}{\varepsilon} \ln \left( \frac{e^{\varepsilon - 1}}{2\delta} + 1 \right) \)

\( \frac{b(D_i)}{A} = \text{optimal given } D_i \)
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{\alpha_{p,1}(A)^p \sqrt{m}\} \cdot \frac{\Delta}{4\epsilon} \ln \left( \frac{e^{\epsilon-1}}{2\delta} + 1 \right) \)

**Proof sketch:** Diagonal matrix \( A \) with entries \( a_1, \ldots, a_m > 0 \)

Feasible set \( Ax \leq b(D') \) with \( D' \sim D \)

Only \( \delta \) probability mass on \( x(D) \)

Feasible set \( Ax \leq b(D) \)
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \)

**Proof sketch:** Diagonal matrix \( A \) with entries \( a_1, \ldots, a_m > 0 \)

\[ g(x^*) - \mathbb{E}[g(x(D))] \geq \left( \sum \frac{1}{a_i} \right) \cdot \frac{\Delta}{4\varepsilon} \cdot \ln \left( \frac{e^{\varepsilon-1}}{2\delta} + 1 \right) \]
Lower bound: Proof sketch

**Theorem:** \( g(x^*) - \mathbb{E}[g(x(D))] \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \ln \left( \frac{e^\varepsilon - 1}{2\delta} + 1 \right) \)

**Proof sketch:** Diagonal matrix \( A \) with entries \( a_1, \ldots, a_m > 0 \)

- \( g(x^*) - \mathbb{E}[g(x(D))] \geq \left( \sum \frac{1}{a_i} \right) \cdot \frac{\Delta}{4\varepsilon} \cdot \ln \left( \frac{e^\varepsilon - 1}{2\delta} + 1 \right) \)
- \( \alpha_{\infty,1}(A) = \sup_{u \geq 0} \{ \| u \|_1 : \| A^T u \|_\infty = 1 \} = \sum \frac{1}{a_i} \)
- \( g(x^*) - \mathbb{E}[g(x(D))] \geq \alpha_{\infty,1}(A) \cdot \sqrt[m]{m} \cdot \frac{\Delta}{4\varepsilon} \cdot \ln \left( \frac{e^\varepsilon - 1}{2\delta} + 1 \right) \)

\[ \geq \inf_{p \geq 1} \{ \alpha_{p,1}(A)^p \sqrt{m} \} \cdot \frac{\Delta}{4\varepsilon} \cdot \ln \left( \frac{e^\varepsilon - 1}{2\delta} + 1 \right) \]
Outline

1. Introduction
2. Background: Differential privacy
3. Algorithm
4. Lower bound
5. Experiments
6. Conclusion
Experiments with Dow Jones data

Individuals pool money to invest
  Amount private except to investment manager

**Goal:** Minimize variance subject to minimum expected return
Outline

1. Introduction
2. Background: Differential privacy
3. Algorithm
4. Lower bound
5. Experiments
6. Conclusion
Conclusions

Algorithm for linearly-constrained optimization
Solution never violates the constraints

Algorithm’s loss is optimal up to log factors

Future research: What if matrix $A$ is private?