Why all this?

Differential privacy is given w.r.t. datasets that "differ in only one entry", but the mechanisms we have for making a function differentially private measure the noise they add in terms of a sensitivity that is given w.r.t. e.g. the $L2$-distance. Hence we need to check sensitivity of functions w.r.t. different input- and output metrics.

Metric Spaces

(M, d) where M is a set and $d : M \times M \to \mathbb{R}$ s.t.

- $d(x, y) = 0 \Leftrightarrow x = y$
- $d(x, y) = d(y, x)$
- $d(x, z) \leq d(x, y) + d(y, z)$

Sensitivity

for metric spaces M, N a map $f : M \to N$ is s-sensitive if for all $x, y \in M$

$$d_N(f(x), f(y)) \leq s \cdot d_M(x, y)$$

"If the input is at most 1 apart, the output is at most s apart."

Gaussian Mechanism

Let $\mathcal{D}$ be some space equipped with the discrete metric (e.g. $(\mathbb{D}, L\infty)$). Given a function $f : \mathcal{D} \to \mathbb{R}^n$ that is s-sensitive in $L2$ norm, for every $\delta \in (0, 1)$ and $\epsilon \in (0, 1)$ the gaussian mechanism

$$\mathcal{M}_{\text{Gauss}}(f, \epsilon, \delta)(x) = f(x) + \mathcal{N}^n\left(\mu = 0, \sigma^2 = \frac{2\ln(1.25/\delta) \cdot s^2}{\epsilon^2}\right)$$

yields an (ϵ, δ)-differentially private function.

Metrics on Numbers

- On $\mathbb{R}$ the metric is standard:
$$d_{\mathbb{R}}(x, y) = |x - y|$$
- On $\mathbb{D}$ we just check if the numbers are equal:
$$d_{\mathbb{D}}(x, y) = (x == y ? 0 : 1)$$

Metrics on Vectors

- Vectors over $\mathbb{R}$:
$$d_{L1,\mathbb{R}}(v, w) = \sum_i d_{\mathbb{R}}(v_i, w_i)$$
$$d_{L2,\mathbb{R}}(v, w) = \sqrt{\sum_i d_{\mathbb{R}}(v_i, w_i)^2}$$
$$d_{L\infty,\mathbb{R}}(v, w) = \max_i d_{\mathbb{R}}(v_i, w_i)$$
- Vectors over $\mathbb{D}$:
$$d_{L1,\mathbb{D}}(v, w) = \sum_i d_{\mathbb{D}}(v_i, w_i) = \text{number of entries that differ}$$

$$d_{L2,\mathbb{D}}(v,w) = \sqrt{\sum_i d_{\mathbb{D}}(v_i,w_i)^2} = \sqrt{d_{L1,\mathbb{D}}(v,w)}$$

$$d_{L\infty,\mathbb{D}}(v,w) = \max_i d_{\mathbb{D}}(v_i,w_i) = \text{"0 if } v = w\text{, 1 otherwise"}$$

- some facts
  - for vectors $v \neq w$ we have
  $$1 = d_{L\infty,\mathbb{D}}(v,w) \leq d_{L2,\mathbb{D}}(v,w) \leq d_{L1,\mathbb{D}}(v,w) \tag{1}$$
  - hence if a vector-valued function $f : M \to \mathbb{D}^n$ is s-sensitive for a fixed input metric and output metric $d_{L1,\mathbb{D}}$, it is also s-sensitive under output metric $d_{L\infty,\mathbb{D}}$ because
  $$d_{L\infty,\mathbb{D}}(f(v),f(w)) \overset{(1)}{\leq} d_{L2,\mathbb{D}}(f(v),f(w)) \overset{(1)}{\leq} d_{L1,\mathbb{D}}(f(v),f(w)) \overset{f \text{ is } s\text{-sensitive}}{\leq} s \cdot d_M(v,w)$$
  - also all functions f from $(*,\mathbb{D})$-vectors to $(L\infty,\mathbb{D})$-vectors are 1-sensitve because for $v \neq w$ it is
  $$1 = d_{L\infty,\mathbb{D}}(f(v),f(w)) \overset{(1)}{\leq} 1 \cdot d_{L*,\mathbb{D}}(v,w)$$
  (This is true even for matrix input, see next section.)
  - Clipping $(L\infty,\mathbb{D})$ vectors is such a function and hence 1-sensitive. I don't think clipping vectors in general is 1-sensitive (even if it says so in the paper), because e.g. $d_{L1,\mathbb{D}}$ can become larger:
  $$d_{L1,\mathbb{D}}([1,1],[1,0]) = 1$$
  but for the clipped vectors
  $$d_{L1,\mathbb{D}}(clip^{L1}([1,1]), clip^{L1}([1,0])) = d_{L1,\mathbb{D}}([0.5,0.5],[1,0]) = 2$$

Matrix Type

The duet matrix type has the following parameters:

$$\mathbb{M}_l^c \tau[i,j]$$

is the type of matrices where

- the matrix has i rows and j columns
- all rows have $d_{c,\mathbb{R}}(r,0) \leq 1$ (note that this is the $\mathbb{R}$ norm no matter what τ is. This differs from what is said on p.44 of the paper, but it makes no sense otherwise and in their implementation it's like we think, see last item of "Implications")
- the elements are of type τ and the metric is chosen accordingly
- sensitivities of variables with this type are given w.r.t. $d_{\mathbb{M}_l^\star \tau}$

Metrics over Matrices

- For matrices $m, n \vdash \mathbb{M}_l^\star \tau$ the metric sums over rows:
$$d_{\mathbb{M}_l^\star \tau}(m,n) = \sum_j d_{l,\tau}(m_j,n_j)$$
- In particular,
$$d_{\mathbb{M}_{L1}^\star \mathbb{D}}(m,n) = \text{number of matrix entries that differ}$$
$$d_{\mathbb{M}_{L\infty}^\star \mathbb{D}}(m,n) = \text{number of matrix rows that differ somewhere}$$

- some facts
  - all functions f from $(*, \mathbb{D})$-matrices to $(L\infty, \mathbb{D})$-vectors are 1-sensitve because for $v \neq w$ it is

    $$d_{L*,\mathbb{D}}(v, w) >= 1$$

    and hence

    $$1 = d_{L\infty,\mathbb{D}}(f(v), f(w)) \overset{(1)}{\leq} 1 \cdot d_{L*,\mathbb{D}}(v, w)$$

`discf`

The function `discf` $: \mathbb{R} \to \mathbb{D}$ is claimed to be 1-sensitive in the paper. Taking the numbers 0.1 and 0.2 as an example, we get

$$1 = d_{\mathbb{D}}(\texttt{discf}(0.1), \texttt{discf}(0.2)) = 10 \cdot d_{\mathbb{R}}(0.1, 0.2)$$

so using our notion of sensitivity `discf` must be at least 10-sensitive...

I suspect they used a different definition for sensitivity, namely a function $f : M \to N$ to be s-sensitive iff

$$\max_{d_M(x,y)=1} d_N(f(x), f(y)) = s$$

This definition is equivalent to the above one if $M = \mathbb{D}$ but not in general.

`convert`

We can convert $\mathbb{M}^l_\star\mathbb{D}$ to $\mathbb{M}^l_l\mathbb{R}$ because all rows of the first type have l-norm ≤ 1 so for any two rows m_i, n_i with $d_{\star,\mathbb{D}}(m_i, n_i) \leq 1$ we have

$$d_{l,\mathbb{R}}(m_i, n_i) \leq d_{l,\mathbb{R}}(m_i, 0) + d_{l,\mathbb{R}}(0, n_i) =\leq 1 + 1$$

The inequality is met, e.g. by the vectors $[1, 0]$ and $[-1, 0]$, as they have $\mathbb{D}$-distance 1 and $L2$-norm 1, but $L2$-distance 2 from each other.

This implies conversion of the rows is 2-sensitive, but in the paper it is declared 1-sensitive. Also the paper version does not preserve clipping on the matrix, even though in their interpreter the `convert` function is simply the identity.

`black boxes`

All functions f from $(*, \mathbb{D})$-matrices (also vectors) to $(L\infty, \mathbb{D})$-vectors are 1-sensitve.