Notes sur

Rényi Differential Privacy

arXiv:1702.07476

Cet article d'août 2 017 d'Ilya Mironov (Google Brain) présente cette relaxation de la confidentialité différentielle « classique », basée sur la divergence de Rényi.

1 Variantes de confidentialité différentielle (DP)

- La définition originelle de Dwork (**ε-DP**) revient à majorer un coefficient multiplicatif, quant au changement des probabilités d'une base de donnée à une autre « adjacente » autrement dit différente d'un unique enregistrement, donc à se baser sur le pire cas. Le coefficient ε représente le **budget de confidentialité** qu'on s'alloue. Lors d'une composition de mécanismes DP, il est additionné.
  Si une fonction a une **ℓ_1-sensibilité** donnée Δ_1 (définie comme étant $\max ||f(D) - f(D')||_1$ pour des bases D et D' adjacentes), alors l'ajout d'un bruit laplacien centré de paramètre Δ_1/ε aboutit à un **mécanisme laplacien** ε-DP.

- Le relâchement proposé par la **(ε,δ)-DP** est l'ajout du paramètre additif δ, quantifiant la probabilité que la garantie de confidentialité ne soit pas assurée, en queue de distribution (« ε-DP garantie avec une probabilité de $1 - \delta$ »). De préférence, on prend $\delta \ll 1/N$ où N est le nombre d'enregistrements de la base.
  Elle fonctionne typiquement avec un **mécanisme gaussien** (*ajout de bruit suivant une loi normale et plus de Laplace, plus « naturel » et dont la queue de distribution décroît plus vite*). Ici, on n'a plus un paramètre optimal unique, mais une « courbe » de $(\varepsilon(\delta), \delta)$-DP avec une infinité de choix possibles : si f a pour **ℓ_2-sensibilité** Δ_2 ($\max ||f(D) - f(D')||_2$ pour D et D' adjacentes), alors pour tout $\varepsilon < 1$ et tout $\sigma > \sqrt{2 \ln 1{,}25/\delta}\, \Delta_2/\varepsilon$, l'ajout de bruit gaussien d'écart-type σ rend le mécanisme $(\varepsilon(\delta), \delta)$-DP. Mais le choix particulier pour lequel on opte peut trahir d'importantes informations sur le mécanisme.
  Elle est également utile pour **les théorèmes avancés de compo-**

sition, où l'on peut consommer moins du budget global de confidentialité. Pour un enchaînement de k mécanismes adaptatifs $(\varepsilon(\delta), \delta)$-DP, pour tout $\delta' > 0$, la composée est $(\varepsilon', k\delta + \delta')$-DP pour $\varepsilon' = \sqrt{2k\ln(1/\delta')}\,\varepsilon + k\varepsilon(\mathrm{e}^{\varepsilon} - 1)$. Mais l'infinité des paramètres envisageables amène à une **explosion combinatoire** qui rend difficile un choix optimal.

- (*Concentrated*-DP et *zero concentrated*-DP sont présentées, comme ayant introduit le principe du *moments accountant* et la descente de gradient stochastique SGD, et d'autres sont mentionnées en fin de `II.`)

- Pour surmonter ces difficultés, l'idée a été d'utiliser les « moments d'ordre supérieur », pour majorer (les queues de distribution de) la variable de perte de confidentialité, introduisant ainsi la **Rényi-DP**, adaptée à la composition de mécanismes hétérogènes et performante quant à la consommation du budget de confidentialité. [1]

2 Rényi-DP

2.1 Définitions

- La **Rényi-divergence d'ordre $\alpha > 1$** de deux distributions de probabilité P et Q [2] est

$$D_\alpha(P||Q) = \frac{1}{\alpha - 1} \ln \mathbb{E}_{x\sim Q} \left(\frac{P(x)}{Q(x)}\right)^{\alpha}$$

  Et en prolongeant par continuité ou en passant à la limite, on pose

$$D_1(P||Q) = \mathbb{E}_{x\sim P} \ln \frac{P(x)}{Q(x)}$$

$$D_\infty(P||Q) = \sup_{x\in \mathrm{supp} Q} \ln \frac{P(x)}{Q(x)}$$

- La propriété 10 en annexe en permet une interprétation un peu plus concrète : pour deux distributions P et Q à support identique, pour tout événement A, on a

$$P(A) \leqslant \left[\mathsf{e}^{D_\alpha(P\,||\,Q)} \cdot Q(A)\right]^{(\alpha-1)/\alpha}$$

1. **Note perso. hors article** : la RDP n'est pas forcément ce qu'on fait de mieux à l'heure actuelle, *cf.* `https://arxiv.org/abs/1911.11607` de décembre 2019 que je n'ai pas étudié...)

2. Une divergence ou « quasi-distance » quantifie la différence entre deux distributions, voir `https://fr.wikipedia.org/wiki/Divergence_(statistiques)`.

- Un mécanisme aléatoire f défini sur D est dit **(α, ε)-RDP** si pour toutes bases D et D' adjacentes, on a

$$D_\alpha(f(D)||f(D')) \leqslant \varepsilon$$

2.2 Conséquence sur les propriétés classiques

**** Certaines sont relâchées. Incomplet pour l'instant... ****

2.2.1 Garantie sur les « réponses gênantes »

Cette *« bad outcomes » guarantee* est l'assurance que la probabilité d'observer en sortie une propriété potentiellement gênante pour un individu est peu modifiée (elle l'est à un facteur multiplicatif près), qu'un enregistrement particulier soit présent ou non dans la base, c'est une conséquence immédiate de la DP.

La propriété est relâchée pour la RDP. On obtient, pour toutes bases D et D' adjacentes et tout ensemble de valeurs de sortie S

$$\mathrm{e}^{-\varepsilon}\mathbb{P}[f(D') \in S]^{\alpha/(\alpha-1)} \leqslant \mathbb{P}[f(D) \in S] \leqslant \left(\mathrm{e}^{\varepsilon}\mathbb{P}[f(D') \in S]\right)^{(\alpha-1)/\alpha}$$

conséq. cf. VII.

2.2.2 Robustesse aux informations auxiliaires

relâchement : prop. probabiliste ici, par partout...

2.2.3 Compatibilité avec les post-traitements

Comme pour les autres formulations, la RDP est heureusement insensible aux post-traitements : si on applique une fonction g aux sorties d'un mécanisme f qui est (α, ε)-RDP, alors la composée $g \circ f$ l'est encore.

2.2.4 Préservation lors de compositions séquentielles adaptatives

Si l'on enchaîne les mécanismes f défini sur D et (α, ε_1)-RDP, suivi de g défini sur $f(D) \times D$ (ce qui lui autorise à s'adapter aux sorties de f) et (α, ε_2)-RDP, alors la séquence $(f(D), g(f(D),D))$ est $(\alpha, \varepsilon_1 + \varepsilon_2)$-RDP.
Cela permet la gestion du budget de confidentialité (la variété des paramètres possibles étant donnée par une « courbe de budget », paramétrée par α). À noter que α reste constant dans ces compositions. *****

2.3 Confidentialité de groupe

On passe de la garantie basée sur deux bases adjacentes à une situation où elles sont distinctes d'un nombre plus important. **... cf. fin III.**

**** Fin de la partie à compléter ****

3 De la RDP à la (ε,δ)-DP et réciproquement

- La (ε,δ)-DP est équivalent à la ε-RDP.
- Cette (∞,ε)-RDP implique la (α,ε)-RDP pour tout α fini.
- Inversement, si un mécanisme f est (α,ε)-RDP, alors il est ($\varepsilon + \frac{\ln 1/\delta}{\alpha-1}, \delta$)-DP pour tout $0 < \alpha < 1$. **+ de détails au VII.**

4 Théorème avancé de composition

Ce type de propriété est *justifiée* ici avec les outils de la RDP, pour montrer que ce concept permet d'établir de telles garanties concernant la composition de mécanismes, qu'il contient suffisamment d'information.

Propriété 4 : la composée f de n mécanismes adaptatifs ε-DP vérifie, pour toutes bases D et D' adjacentes et tout ensemble S de valeurs de sortie,

$$\mathbb{P}[f(D) \in S] \leqslant \exp\left(2\varepsilon\sqrt{n \ln \frac{1}{\mathbb{P}[f(D') \in S]}}\right) \cdot \mathbb{P}[f(D') \in S]$$

À noter que la garantie dépend ici de la probabilité de l'événement $f(D') \in S$.

Corollaire 1 : la composée de n mécanismes ε-DP est (ε', δ)-DP, pour tout $0 < \delta < 1$ tel que $\ln(1/\delta) \geqslant \varepsilon^2 n$, pour $\varepsilon' = 4\varepsilon\sqrt{2n \ln(1/\delta)}$. *****

5 Mécanismes de référence

Vu nos objectifs, on délaisse pour l'instant les deux premiers

5.1 Réponse randomisée

5.2 Bruit laplacien

5.3 Bruit gaussien

Pour une fonction f) valeurs réelles, le mécanisme gaussien $\mathbf{G}_\sigma$ est défini par l'ajout d'un bruit suivant la loi normale centrée d'écart-type $\sigma, \mathcal{N}(0,\sigma^2)$.[3]

De la propriété $D_\alpha(\mathcal{N}(0,\sigma^2)\,||\,\mathcal{N}(\mu,\sigma^2)) = \alpha\mu^2/(2\sigma^2)$, on déduit que si f a comme sensibilité 1, alors le **mécanisme gaussien** de paramètre σ est $(\alpha, \alpha/(2\sigma^2))$-RDP (**corollaire 3**). La courbe de budget RDP (autrement dit $\varepsilon = \alpha/(2\sigma^2)$ fonction de α) du mécanisme gaussien est donc une simple droite passant par l'origine.

En utilisant la propriété concernant la composition de mécanismes RDP, on montre que l'enchaînement de n mécanismes gaussiens tous de paramètre σ, offre la garantie RDP d'un mécanisme gaussien de paramètre $(\alpha/\sqrt{n})$ (il a la même courbe RDP). *****

5.4 Composition de mécanismes de référence

On l'a vu (partie 4), la garantie offerte par la RDP dépend de la probabilité de la probabilité de l'événement $f(D) \in S$, ce qui est plus complexe à gérer qu'avec les autres approches de DP. L'avantage est cependant de permettre la plupart du temps des majorations plus serrées...
+ Expérimentations du `VI.` hors bruit gaussien...

6 Discussion

On revient dans le `VII.` sur la comparaison des garanties entre (ε, δ)-DP et RDP, pour montrer qu'elles sont fortement comparables, malgré des différences importantes. **plutôt à inclure dans le 3. ?**

La RDP n'autorise pas de rupture absolue de la garantie de confidentialité (contrairement à la (ε, δ)-DP, avec une probabilité δ). En ce sens, elle est plus stricte.

Les bornes induites par la RDP (*voir la propriété 4 et corollaire 1*) se dégradent (s'éloignent) quand la probabilité de $f(D) \in S$ diminue. Cependant, si l'on fixe un niveau minimal de référence (*baseline*), il devient aisé de trouver la valeur optimale **de quoi ? Je m'y perds, revoir VII. !**

Par ailleurs (*voir fin du `VII.`*), choisir α peut être fait de manière quasi-optimale parmi un ensemble fini de valeurs tel que

3. Il y a me semble-t-il une coquille dans l'article avec un carré en trop pour l'écart-type dans l'explication de cette notation, page 8 juste sous la table II dans la seconde colonne

$\{1{,}5; 1{,}75; 2; 2{,}5; 3; 4; 5; 6; 8; 16; 32; 64; +\infty\}$ *