Arbitrages statistiques dans l'apprentissage automatique confidentiel.

Rapport de stage

Alexi Canesse
Sous la supervision d'Aurélien Garivier, Professeur,
UMPA et École Normale Supérieure de Lyon

Stage de recherche effectué dans le cadre de la
L3 informatique fondamental de l'ÉNS de Lyon

Département informatique
École Normale Supérieur de Lyon
France
30 juin 2022

Table des matières

1 Introduction

TODO

1.1 Présentation du problème

TODO

1.2 Définitions

La *differential privacy* [Dwo+06] quantifie la perte de confidentialité subit par un individue en étant dans une base de donné.

Définition 1.2.0.1 : *Bases de donnée voisines*
On dit que deux bases de données x et y sont voisines et on note $||x - y||_1 \leq 1$ si elles diffèrent sur au plus une entrée *ie* la distance de Hamming qui les sépare et majorée par 1.

Définition 1.2.0.2 : *Differential privacy*
On dit qu'un mécanisme aléatoire $\mathcal{M} : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ est (ε, δ)-***differentially private*** si pour tout $\mathcal{S} \subset \mathcal{T}$ mesurable,

$$\forall x, y \in \mathcal{X}^{(\mathbb{N})} \quad ||x - y|| \leq 1 \quad \Rightarrow \quad \mathbb{P}(\mathcal{M}(x) \in \mathcal{S}) \leq \exp(\varepsilon)\mathbb{P}(\mathcal{M}(y) \in \mathcal{S}) + \delta$$

De plus, si $\delta = 0$, on dit que $\mathcal{M}$ est ε-***differentially private***.

1.3 Contribution

TODO

2 Méthode des histogrammes

2.1 AboveThreshold

Répondre à de nombreuses requête est coûteux en confidentialité. Utiliser à algorithme naïf tel que le mécanisme de Laplace [Dwo+06] ne permet pas de répondre à de nombreuses requêtes avec une bonne précision tout en préservant un bon niveau de confidentialité (ε doit être petit). Dans certains cas nous ne sommes néanmoins pas intéressé par les réponses numériques, mais uniquement intéressé par le fait qu'une réponse dépasse ou non un seuil définit. Nous allons voir que `AboveThreshold` [DR14] permet cela tout en ne payant que pour les requêtes qui dépassent le seuil.

```
AboveThreshold(database, queries, threshold, epsilon){
    Assert("les requêtes sont toutes de sensibilité 1");
    result = 0;
    noisyThreshold = threshold + Lap(2/epsilon);
    for(querie in queries){
        nu = Lap(4/epsilon);
        if(querie(D) + nu > noisyThreshold)
            return result;
        else
            ++result;
    }
    return -1;
}
```

L'algorithme venant d'être décrit renvoie l'indice de la première requête à dépasser le seuil si une telle requête existe. C'est une version adaptée de l'algorithme initialement décrit par Dwork et Roth dans [DR14, page 57]. Icelui a du sens d'un point de vue informatique mais rend le formalisme mathématiques compliqué (les auteurs eux-même tombent dans ce travers) et nous n'utiliseront pas les légers avantages de leur version.

Théorème 2.1.0.1 :
Pour tout ensemble de requêtes $Q \in \left(\mathcal{X}^{(\mathbb{N})} \to \mathcal{T}\right)^{\mathbb{N}}$ de sensibilité 1, tout seuil $T \in \mathbb{R}$, tout $\varepsilon > 0$, $M : x \in \mathcal{X}^{(\mathbb{N})} \mapsto$ `AboveThreshold(x, Q, T, epsilon)` est ε-*differentially private.*

***Remarque** : La démonstration est une réécriture de celle du livre de référence [DR14, page57]. Une réécriture était nécessaire car cette démonstration présente de nombreux points limites en terme de rigueur mathématiques et de detail pas suffisant sur certains points non triviaux.*

Démonstration :
Soit $D, D' \in \mathcal{X}^{(\mathbb{N})}$ tels que $||D - D'|| \leq 1$, $\{f_i\}_i = Q \in \left(\mathcal{X}^{(\mathbb{N})} \to \mathcal{T}\right)^{\mathbb{N}}$ un ensemble de requêtes de sensibilité 1, $T \in \mathbb{R}$ un seuil, et $\varepsilon > 0$. On pose alors A la variable aléatoire `AboveThreshold(D, Q, T, epsilon)` et A' la variable aléatoire `AboveThreshold(D', Q, T, epsilon)`.

Soit alors $k \in \mathbb{N}$. *Montrons que* $\mathbb{P}(A = k) \leq \exp(\varepsilon)\mathbb{P}(A' = k)$. En reprenant les notations de l'algorithme [2.1], on fixe les éléments $(\nu_i)_{i<k}$ (qui suivent une loi de Laplace de paramètre $4/\varepsilon$).

On pose alors

$$\begin{cases} g_k &= \max_{i<k} \{f_i(D) + \nu_i\} \\ g'_k &= \max_{i<k} \{f_i(D') + \nu_i\} \end{cases}$$

Ces grandeurs représente la valeur plus grande comparée au seuil bruité avant l'indice k dans le cas de l'execution sur D et de l'execution sur D'. Les probabilité qui suivent seront prisent sur les deux variables aléatoires non fixées ν_k et $\hat{T}$ qui est la valeur du seuil bruitée. On pose enfin, pour tout $i \in \mathbb{N}$,

$$\begin{cases} y_i &= f_i(D) \\ y'_i &= f_i(D') \end{cases}$$

On note alors que, en notant l_2 la densité de la loi de Laplace de paramètre $2/\varepsilon$ et l_4 celle de paramètre $4/\varepsilon$,

$$\begin{aligned} \mathbb{P}(A = k) &= \mathbb{P}(\hat{T} \in]g_k, y_k + \nu_k]) \\ &= \int_{\mathbb{R}} \mathbb{P}(\hat{T} \in]g_k, y_k + \nu]) l_4(\nu) \mathrm{d}\nu \\ &= \int_{\mathbb{R}} \int_{g_k - T}^{y_k + \nu - T} l_2(t) l_4(\nu) \mathrm{d}t \mathrm{d}\nu \end{aligned}$$

On effectue alors un premier changement de variable affine

$$\hat{t} = t + g_k - g'_k$$

On obtient donc

$$\begin{aligned} \mathbb{P}(A = k) &= \int_{\mathbb{R}} \int_{g_k - T}^{y_k + \nu - T} l_2(\hat{t} - g_k + g'_k) l_4(\nu) \mathrm{d}t \mathrm{d}\nu \\ &= \int_{\mathbb{R}} \int_{g'_k - T}^{y_k + \nu - g_k + g'_k - T} l_2(\hat{t}) l_4(\nu) \mathrm{d}t \mathrm{d}\nu \end{aligned}$$

Il est alors temps de faire un second changement de variable affine

$$\hat{\nu} = \nu + g_k - g'_k + y'_k - y_k$$

Ainsi,

$$\begin{aligned}
\mathbb{P}(A = k) &= \int_{\mathbb{R}} \int_{g'_k - T}^{y_k + \nu - g_k + g'_k - T} l_2(\hat{t}) l_4(\hat{\nu} - g_k + g'_k - y'_k + y_k) \mathrm{d}\hat{t} \mathrm{d}\nu \\
&= \int_{\mathbb{R}} \int_{g'_k - T}^{y_k + \nu - g_k + g'_k + g_k - g'_k + y'_k - y_k - T} l_2(\hat{t}) l_4(\hat{\nu}) \mathrm{d}t \mathrm{d}\nu \\
&= \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} l_2(\hat{t}) l_4(\hat{\nu}) \mathrm{d}t \mathrm{d}\nu
\end{aligned}$$

Par définition de l_2 et l_4 nous avons donc

$$\mathbb{P}(A = k) = \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} \exp\left(-\frac{|\hat{t}|\varepsilon}{2}\right) \exp\left(-\frac{|\hat{\nu}|\varepsilon}{4}\right) \mathrm{d}t \mathrm{d}\nu$$

L'inégalité triangulaire assure alors que

$$\begin{aligned}
\mathbb{P}(A = k) &\leq \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} \exp\left(\frac{|\hat{t} - t|\varepsilon}{2}\right) \exp\left(-\frac{|t|\varepsilon}{2}\right) \exp\left(\frac{|\hat{\nu} - \nu|\varepsilon}{4}\right) \exp\left(-\frac{|\nu|\varepsilon}{4}\right) \mathrm{d}t \mathrm{d}\nu \\
&= \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} \exp\left(\frac{|g_k - g'_k|\varepsilon}{2}\right) \exp\left(-\frac{|t|\varepsilon}{2}\right) \exp\left(\frac{|g_k - g'_k + y'_k - y_k|\varepsilon}{4}\right) \exp\left(-\frac{|\nu|\varepsilon}{4}\right) \mathrm{d}t \mathrm{d}\nu
\end{aligned}$$

Les requêtes étant de sensibilité 1, nous avons

$$\begin{cases}
2 & \geq |g_k - g'_k| + |y'_k - y_k| \quad \geq |g_k - g'_k + y'_k - y_k| \\
1 & = |g_k - g'_k|
\end{cases}$$

Enfin, la croissance de l'intégrale assure que

$$\begin{aligned}
\mathbb{P}(A = k) &\leq \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} \exp\left(\frac{\varepsilon}{2}\right) \exp\left(-\frac{|t|\varepsilon}{2}\right) \exp\left(\frac{\varepsilon}{2}\right) \exp\left(-\frac{|\nu|\varepsilon}{4}\right) \mathrm{d}t \mathrm{d}\nu \\
&= \exp\left(\frac{2\varepsilon}{2}\right) \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} \exp\left(-\frac{|t|\varepsilon}{2}\right) \exp\left(-\frac{|\nu|\varepsilon}{4}\right) \mathrm{d}t \mathrm{d}\nu \\
&= \exp(\varepsilon) \int_{\mathbb{R}} \int_{g'_k - T}^{y'_k + \nu - T} l_2(t) l_4(\nu) \mathrm{d}t \mathrm{d}\nu \\
&= \exp(\varepsilon) \int_{\mathbb{R}} \mathbb{P}(\hat{T} \in]g'_k, y'_k + \nu]) l_4(\nu) \mathrm{d}\nu \\
&= \exp(\varepsilon)\, \mathbb{P}(\hat{T} \in]g'_k, y'_k + \nu_k]) \\
&= \exp(\varepsilon)\, \mathbb{P}(A' = k)
\end{aligned}$$

2.2 La méthode des histogramme

2.2.1 Présentation de la méthode des histogrammes

La méthode des histogramme est une méthode que nous avons proposé durant ce stage. Il s'agit d'une instanciation particulière de `AboveThreshold` permettant de calculer l'ensemble des déciles (ou n'importe quel quantiles). Une transformation affine permet d'obtenir la réponse finale à partir de la réponse du mécanisme.

```
1  HistogramMethod(database, epsilon, steps, a, b){
2      /* composition theorem */
3      epsilon /= 9;
4
5      result = {};
6      for(d in {1 ... 9}){ /* which decile */
7          T = d*card(database)/10;
8          for(i in {1 ... steps}){
9              fi = x -> card({element in x | element < i*(b-a)/steps});
10             queries.push_back(fi);
11         }
12         T = d*card(database)/10;
13         result.push_back(AboveThreshold(database, queries, T, epsilon)
14                          *(b-a)/steps});
15     }
16     return result;
17 }
```

Les entrée a et b donnent une minoration et une majoration de l'ensemble des valeurs d'entrées. L'algorithme découpe alors l'intervalle $[a, b]$ en `steps` intervalles de même tailles. Pour chaque décile, l'entier renvoyé par `Abovethreshold` est l'indice de la première valeur à dépasser ce décile.

FIGURE 1 – Le découpage pour $a = 0$, $b = 1$, `steps` $= 4$

Théorème 2.2.1.1 :
`HistogramMethod` est ε-*differentially private.*

Démonstration : Les requêtes envoyé par l'algorithme à `AboveThreshold` sont bien de sensibilité 1. Chacun des neuf appels à cette fonction est donc $\varepsilon/9$-*differentially private.* Le théorème de composition assure alors que `HistogramMethod` est ε-*differentially private.*

Maintenant que nous avons vu que cet algorithme est bien *differentially private*, nous allons essayer d'évaluer sa précision. Cela ne sera pas évident car la précision de l'algorithme dépend beaucoup du jeu de donné en entré.

Lemme 2.2.1.1 : *`AboveThreshold` est* $(\alpha, \beta) -$ *accurate*
Pour tout $\beta \in]0, 1[$, tout $x \in \mathcal{X}^{(\mathbb{N})}$, tout $\{f_i\}_i = Q \in \left(\mathcal{X}^{(\mathbb{N})} \to \mathcal{T}\right)^{\mathbb{N}}$, tout $\varepsilon > 0$, tout $T \in \mathbb{R}$, en posant $\alpha = 8\left(\log(k) + \log(2/\beta)\right)/\varepsilon$ et $k =$ `AboveThreshold(x, Q, T, epsilon)`, on a, en reprenant les notations de l'algorithme,

$$\mathbb{P}\left(\forall i < k \ f_i(x) + \nu_i < T + \alpha \wedge f_k(x) + \nu_k > T - \alpha\right) \geq 1 - \beta$$

Remarque : *Ce lemme est due à [DR14, page 61]. Nous reprenons aussi la démonstration ici car la démonstration originale ne nous semble pas assez claire et trop bancale mathématiquement.*

Démonstration : Reprenons les notations de l'énoncé. Montrons déjà qu'il suffit de démontrer que

$$\mathbb{P}\left(\max_{i \leq k} |\nu_i| + |T - \hat{T}| < \alpha\right) \geq 1 - \beta \tag{1}$$

où $\hat{T}$ est le seuil bruité défini à la ligne 4 de l'algorithme [2.1]. Or, nous avons, en posant pour tout $i \leq k$, $y_i = f_i(x)$

$$y_k + \nu_k \geq \hat{T} \overset{\text{IT}}{\geq} T - |T - \hat{T}|$$

Mutatis mutandis

$$\forall i < k \quad y_i \leq \hat{T} + |\nu_i| \leq T + |T - \hat{T}| + |\nu_i|$$

Ainsi,

$$\mathbb{P}\left(\forall i < k \ f_i(x) + \nu_i < T + \alpha \wedge f_k(x) + \nu_k > T - \alpha\right) \geq 1 - \beta$$

Démontrons enfin (1)! La variable aléatoire $T - \hat{T}$ suit une loi de Laplace de paramètre $2/\varepsilon$. Ainsi,

$$\mathbb{P}\left(|T - \hat{T}| \geq \frac{\alpha}{2} = \frac{\alpha\varepsilon}{4}\frac{2}{\varepsilon}\right) = \exp\left(-\frac{\varepsilon\alpha}{4}\right) = \exp\left(-2\left(\log k + \log\frac{2}{\beta}\right)\right) \leq \exp\left(-2\left(\log\frac{2}{\beta}\right)\right) \leq \frac{\beta}{2}$$

De même,

$$\mathbb{P}\left(\max_i |\nu_i| \geq \frac{\alpha}{2}\right) \leq \sum_{j=1}^{k} \mathbb{P}\left(|\nu_j| \geq \frac{\alpha}{2}\right) = k\exp\left(-\frac{-\alpha\varepsilon}{8}\right) = k\exp\left(-\log k - \log\frac{2}{\beta}\right) = \frac{k}{k}\frac{\beta}{2}$$

Enfin,

$$\begin{aligned}
\mathbb{P}\left(\max_{i\leq k} |\nu_i| + |T - \hat{T}| < \alpha\right) &\geq \mathbb{P}\left(\max_{i\leq k} |\nu_i| < \frac{\alpha}{2} \ \wedge \ |T - \hat{T}| < \frac{\alpha}{2}\right) \\
&= 1 - \mathbb{P}\left(\max_{i\leq k} |\nu_i| \geq \frac{\alpha}{2} \ \cup \ |T - \hat{T}| \geq \frac{\alpha}{2}\right) \\
&\geq 1 - \mathbb{P}\left(\max_{i\leq k} |\nu_i| \geq \frac{\alpha}{2}\right) - \mathbb{P}\left(|T - \hat{T}| \geq \frac{\alpha}{2}\right) \\
&\geq 1 - \frac{\beta}{2} - \frac{\beta}{2}
\end{aligned}$$

Finalement,

$$\mathbb{P}\left(\max_{i\leq k} |\nu_i| + |T - \hat{T}| < \alpha\right) \geq 1 - \beta$$

Ce qui démontre bien (1) et donc le lemme.

2.2.2 Analyse de complexité

La complexité de `AboveThreshold` est de l'ordre de la somme des complexité des requêtes sur le jeu de données d'entré. En notant n la taille de la base de donnée, les requêtes envoyé à `AboveThreshold` par `HistogramMethod` sont toute de complexité linéaire en n. La variable `step` a aussi pour valeur le nombre de requêtes envoyées que l'on nommera k. L'algorithme a alors une complexité en $\mathcal{O}(nk)$.

2.2.3 Analyse de précision - le cas de la distribution uniforme

Nous allons évaluer la précision de l'algorithme à l'aide de l'erreur quadratique moyenne entre la valeur renvoyé par le programme et la valeur attendue. Il y a plusieurs manière de penser ce qu'est la valeur attendue : elle pourrait être la valeur des déciles de l'échantillons d'entré. Néanmoins, elle peut tout aussi bien être l'ensemble des déciles de la loi. En effet, nous cherchons à répondre à des questions de statistique, l'entré peut-être un simple échantillon "représentatif" ; au quel cas nous sommes principalement intéressé par les réponses statistiques sur l'ensemble de la population et non juste sur notre échantillon.

Ces deux choix ont un réel sens. Nous avons d'abord essayé d'évaluer les performances de l'algorithme dans le premier cas. Les calculs était difficiles et menaient à des résultats difficilement exploitables. Nous avons donc choisi de réaliser les calculs sur la seconde option afin de pouvoir mener des calculs légèrement plus simples et ainsi avoir des résultats.

Nous allons commencer par démontrer quelques lemmes intermédiaires afin de démontrer les résultats de précision.

Lemme 2.2.3.1 : *Estimation de l'écard entre les déciles empiriques et ceux de la loi uniforme.* Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1] et soit $\gamma \in [0, 0.1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi. Pour tout $i \in [\![1, 9]\!]$

$$\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) \geq 1 - \exp\left(-\frac{1}{6}n\gamma^2\right) - \exp\left(-\frac{1}{12}n\gamma^2\right)$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1]. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ ceux de la loi. Soit $\gamma \in [0, 0.1]$. On note que

$$\begin{aligned}\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) &= 1 - \mathbb{P}(d_i \notin [d_i^l - \gamma/2, d_i^l + \gamma/2]) \\ &= 1 - \mathbb{P}(d_i \leq d_i^l - \gamma/2 \vee d_i \geq d_i^l + \gamma/2])\end{aligned}$$

On pose alors $A =$ "il y a au moins $in/10$ valeurs plus petites que $d_i^l - \gamma/2$" et $B =$ "il y a au plus $in/10$ valeurs plus petites que $d_i^l + \gamma/2$". On pose donc pour tout j, $A_j = \mathbb{1}_{x_j < d_i^l - \gamma/2}$ et $B_j = \mathbb{1}_{x_j < d_i^l + \gamma/2}$. On pose alors $A_s = \sum_{j=0}^{n-1} A_j$ et $B_s = \sum_{j=0}^{n-1} B_j$

$$\begin{aligned}\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) &= 1 - \mathbb{P}(A \cup B) \\ &\geq 1 - \mathbb{P}(A) - \mathbb{P}(B) \\ &\geq 1 - \mathbb{P}(A_s \geq in/10) - \mathbb{P}(B_s \leq in/10)\end{aligned}$$

Les événements $(A_j)_j$ suivent une loi de Bernouilli de paramètre $d_i^l - \gamma/2$ et les événements $(B_j)_j$ suivent une loi de Bernouilli de paramètre $d_i^l + \gamma/2$. Ainsi,

$$\begin{aligned}\mathbb{P}\left(A_s \geq in/10\right) &\overset{d_i^l = i/10}{=} \mathbb{P}\left(A_s \geq \left(d_i^l - \frac{\gamma}{2}\right) n \left(1 + \left(\frac{d_i^l}{d_i^l - \gamma/2} - 1\right)\right)\right) \\ &\leq \exp\left(-\frac{1}{3}n\left(d_i^l - \frac{\gamma}{2}\right)\left(\frac{\gamma/2}{d_i^l - \gamma/2}\right)^2\right) \\ &= \exp\left(-\frac{1}{12}n\gamma^2\frac{1}{d_i^l - \gamma/2}\right) \\ &\overset{d_i^l \geq \gamma}{\leq} \exp\left(-\frac{1}{6}n\gamma^2\right)\end{aligned}$$

De même

$$\mathbb{P}\left(B_s \leq \frac{in}{10}\right) \leq \exp\left(-\frac{1}{12}n\gamma^2\right)$$

Finalement,

$$\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) \geq 1 - \exp\left(-\frac{1}{6}n\gamma^2\right) - \exp\left(-\frac{1}{12}n\gamma^2\right)$$

Lemme 2.2.3.2 :
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1] dont on note $(d_i^l)_i$ les déciles. Soit $\gamma \in [0, 0.1]$, $i \in [\![1, 9]\!]$ et $\alpha \in \mathbb{N}$. Il y a au moins α valeurs de X dans chacun des intervalles $[d_i^l - \gamma, d_i^l - \gamma/2]$ et $[d_i^l + \gamma/2, d_i^l + \gamma]$ avec une probabilité au moins $1 - \beta$ avec

$$\beta = 2\exp\left(-\frac{n\gamma}{4}\left(1 - \frac{2\alpha}{n\gamma}\right)^2\right)$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1] dont on note $(d_i^l)_i$ les déciles. Soit $\gamma \in [0, 0.1]$, $i \in [\![1, 9]\!]$ et $\alpha \in \mathbb{N}$. On pose alors pour tout j, $A_j = \mathbb{1}_{x_j \in d_i^l - \gamma, d_i^l - \gamma/2}$ et $B_j = \mathbb{1}_{x_j \in d_i^l + \gamma/2, d_i^l + \gamma}$. On peut alors noter $A = \sum_{j=0}^{n-1} A_j$ et $B = \sum_{j=0}^{n-1} B_j$.

$$\mathbb{P}\left(A \geq \alpha \ \wedge \ B \geq \alpha\right) \geq \mathbb{P}(A \geq \alpha) + \mathbb{P}(B \geq \alpha) - 1$$

Or, on a, à l'aide d'une nouvelle utilisation d'une borne de Chernoff,

$$\begin{cases} \mathbb{P}(A \geq \alpha) &= 1 - \mathbb{P}\left(A < \dfrac{n\gamma}{2}\left(1 - \left(1 - \dfrac{2\alpha}{n\gamma}\right)\right)\right) \geq 1 - \exp\left(-\dfrac{n\gamma}{4}\left(1 - \dfrac{2\alpha}{n\gamma}\right)^2\right) \\ \mathbb{P}(B \geq \alpha) &= 1 - \mathbb{P}\left(B < \dfrac{n\gamma}{2}\left(1 - \left(1 - \dfrac{2\alpha}{n\gamma}\right)\right)\right) \geq 1 - \exp\left(-\dfrac{n\gamma}{4}\left(1 - \dfrac{2\alpha}{n\gamma}\right)^2\right) \end{cases}$$

Ainsi,

$$\mathbb{P}\left(A \geq \alpha \ \wedge \ B \geq \alpha\right) \geq 1 - 2\exp\left(-\frac{n\gamma}{4}\left(1 - \frac{2\alpha}{n\gamma}\right)^2\right)$$

La combinaison des trois lemmes précédents permet d'obtenir un résultat de précision utile sur `HistogramMethod`.

Théorème 2.2.3.1 : (α, β)*-précision de* `HistogramMethod` *dans le cas uniforme sur* $[0, 1]$
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1]. Soit $\gamma \in [0, 0.1]$, $i \in [\![1, 9]\!]$, $k \in \mathbb{N}$ et $\beta \in [0, 1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i)_i$ ceux de la loi. Posons A la variable aléatoire `HistogramMethod(X, epsilon, k, a, b)`.

$$\mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) \geq 1 - \beta - \eta - \mu$$

Avec

$$\alpha = \frac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon} \wedge \mu = 2\exp\left(-\frac{n\gamma}{4}\left(1 - \frac{2\alpha}{n\gamma}\right)^2\right) \wedge \eta = \exp\left(-\frac{1}{6}n\gamma^2\right) + \exp\left(-\frac{1}{12}n\gamma^2\right)$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1]. Soit $\gamma \in [0, 0.1]$, $i \in [\![1, 9]\!]$, $k \in \mathbb{N}$ et $\beta \in [0, 1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ ceux de la loi. Posons A la variable aléatoire `HistogramMethod(X, epsilon, k, a, b)`.

On pose

$$\alpha = \frac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon}$$

Notons alors E_α l'événement "Il y a au moins α valeurs de X dans chacun des intervalles $[d_i^l - \gamma, d_i^l - \gamma/2]$ et $[d_i^l + \gamma/2, d_i^l + \gamma]$" Et E_{A_i} l'événement "moins de α valeurs de X séparent d_i et A_i". Nous avons alors

$$\begin{aligned} \mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) &\geq \mathbb{P}\left(E_{A_i} \wedge E_\alpha \wedge d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]\right) \\ &\geq \mathbb{P}\left(E_{A_i}\right) + \mathbb{P}\left(E_\alpha\right) + \mathbb{P}\left(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]\right) - 2 \end{aligned}$$

Les trois précédents lemmes assurent que

$$\begin{aligned} \mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) &\geq (1 - \beta) + (1 - \mu) + (1 - \eta) - 2 \\ &\geq 1 - \beta - \mu - \eta \end{aligned}$$

Avec

$$\alpha = \frac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon} \wedge \mu = 2\exp\left(-\frac{n\gamma}{4}\left(1 - \frac{2\alpha}{n\gamma}\right)^2\right) \wedge \eta = \exp\left(-\frac{1}{6}n\gamma^2\right) + \exp\left(-\frac{1}{12}n\gamma^2\right)$$

2.2.4 Analyse de précision - le cas de la loi normale centrée réduite

Les lois normales est très utilisées en statistique notamment car elle permettent de modéliser les phénomènes issues de plusieurs événement aléatoires. Le théorème central limite viens jouer un rôle clé dans la prépondérance de l'utilisation de ces lois. Il semble alors crucial d'étudier la précision de notre algorithme dans le cas où les données d'entré suivent une loi normale.

Le théorème de précision est très analogue à celui obtenue dans le cas uniforme. Nous ne détaillons pas ici les lemmes intermédiaires et la démonstration car il s'agit formellement de la même chose. Il est néanmoins nécessaire d'introduire quelques objets usuels en plus car la loi normale est plus complexe que la loi uniforme.

Définition 2.2.4.1 : *Fonction d'erreur*
On appel fonction d'erreur la fonction suivant :

$$\text{erf} : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \frac{2}{\sqrt{\pi}} \int_0^z \exp\left(-t^2\right) \mathrm{d}t \end{cases}$$

Lemme 2.2.4.1 : *Déciles de $\mathcal{N}(0,1)$.*
Les déciles de $\mathcal{N}(0,1)$, notés $(d_i^l)_i$ sont

$$\forall i \in [\![1,9]\!] \quad d_i^l = \sqrt{2}\,\text{erf}^{-1}(2 \times 0.1i - 1)$$

Démonstration : Soit $i \in [\![1,9]\!]$. On note que

$$\begin{aligned} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{d_i^l} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t &= \frac{\sqrt{2}}{\sqrt{2\pi}} \int_{-\infty}^{\text{erf}^{-1}(2\times 0.1i-1)} \exp\left(-t^2\right) \mathrm{d}t \\ &= \frac{1}{2}\frac{2}{\sqrt{\pi}} \int_{-\infty}^{\text{erf}^{-1}(2\times 0.1i-1)} \exp\left(-t^2\right) \mathrm{d}t \\ &= \frac{1}{2}\,\text{erf}\left(\text{erf}^{-1}(2 \times 0.1i - 1)\right) + \frac{1}{2}\frac{2}{\sqrt{\pi}} \int_{-\infty}^{0} \exp\left(-t^2\right) \mathrm{d}t \\ &= 0.1i - \frac{1}{2} + \frac{1}{2} \\ &= 0.1i \end{aligned}$$

La démonstration dans le cas d'une loi normale est analogue à celle du cas uniforme. Nous aurons donc des lemmes similaires. Les démonstrations seront néanmoins laissées en appendix [A].

Lemme 2.2.4.2 : *Estimation de l'écard entre les déciles empiriques et ceux de la loi normale centrée réduite.*
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite et soit $\gamma \in [0, d_i^l]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi normale centrée réduite. Pour tout $i \in [\![1,9]\!]$

$$\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) \geq 1 - \eta$$

Avec

$$\begin{aligned} \eta = 2 &- \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ &+ \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \end{aligned}$$

Lemme 2.2.4.3 :
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la normale

centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$ et $k \in \mathbb{N}$. Il y a au moins α valeurs de X dans chacun des intervalles $[d_i^l - \gamma, d_i^l - \gamma/2]$ et $[d_i^l + \gamma/2, d_i^l + \gamma]$ avec une probabilité au moins $1 - \beta$ avec

$$\beta = \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k}$$
$$+ \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k}$$

Théorème 2.2.4.1 : (α, β)*-précision de* `HistogramMethod` *dans le cas de la loi normale centrée réduite*
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$, $k \in \mathbb{N}$ et $\beta \in [0, 1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi normale centrée réduite. Posons A la variable aléatoire `HistogramMethod(X, epsilon, k, a, b)`.

$$\mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) \geq 1 - \beta - \eta - \mu$$

Avec

$$\begin{cases} \alpha & = \dfrac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon} \\ \mu & = \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\ & \quad + \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\ \eta & = 2 - \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\ & \quad + \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} \end{cases}$$

3 Le mécanisme de sensibilité inverse

3.1 Présentation du mécanisme

Le mécanisme de sensibilité inverse est introduit par Hilal Asi and John C. Duchi dans *Near Instance-Optimality in Differential Privacy* [AD20]. Le mécanisme considère l'inverse du nombre de valeurs à modifié dans un ensemble de donnée pour passer à un autre ensemble de donné sur lequel la requête a une autre valeur recherchée. Cela définit alors l'utilité d'une valeur pour instancier le mécanisme exponentiel [MT07].

Définition 3.1.0.1 : *Longueur*
Soit $x \in \mathcal{X}^{(\mathbb{N})}$, $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ et $t \in \mathcal{T}$. La longueur est le nombre minimum de valeurs à modifier dans x pour obtenir x' tel que $f(x') = t$.

$$\mathrm{len}_f(x, t) = \inf_{x' \in \mathcal{X}^{(\mathbb{N})}} \{||x - x'||_1 \mid f(x') = t\}$$

Définition 3.1.0.2 : *Mécanisme de sensibilité inverse*
Soit $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ et $\varepsilon \in \mathbb{R}_+$. Pour une mesure μ sur $\mathcal{T}$, on définit le mécanisme aléatoire $M(x)$ par sa fonction de densité

$$t \mapsto \frac{\exp(-\mathrm{len}_f(x, t)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-\mathrm{len}_f(x, s)\varepsilon/2)\mathrm{d}\mu(s)}$$

Il n'y a qu'en $f(x)$ que $\mathrm{len}_f(x,)$ est nulle. Ainsi le dénominateur pourrait être petit est donné une grande probabilité à des valeurs distantes de $f(x)$. On [MT07] introduit alors une version lisse du

mécanisme.

Définition 3.1.0.3 : *Longueur lisse*
Soit $x \in \mathcal{X}^{(\mathbb{N})}$, $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ et $\rho \in \mathbb{R}_+$. Si $\mathcal{N}$ est une norme sur $\mathcal{T}$,

$$\text{len}_f^\rho : \left\{ \begin{array}{ccc} \mathcal{T} & \to & \mathbb{N} \\ t & \mapsto & \inf_{s \in \mathcal{T}, \mathcal{N}(s,t) \leq \rho} \{\text{len}_f(x,s)\} \end{array} \right.$$

Définition 3.1.0.4 : *Mécanisme de sensibilité inverse ρ-lisse*
Soit $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ et $\rho, \varepsilon \in \mathbb{R}_+$. Pour une mesure μ sur $\mathcal{T}$, on définit le mécanisme aléatoire $M_{\text{cont}}(x)$ par sa fonction de densité

$$t \mapsto \frac{\exp(-\text{len}_f^\rho(x,t)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-\text{len}_f^\rho(x,s)\varepsilon/2)\mathrm{d}\mu(s)}$$

Théorème 3.1.0.1 :
Pour tout $\rho, \varepsilon \in \mathbb{R}_+$, le mécanisme de sensibilité inverse ρ-lisse est ε-*differentially private.*

Démonstration : Soit $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$, $\rho, \varepsilon \in \mathbb{R}_+$, μ une mesure sur $\mathcal{T}$, $\mathcal{S} \subset \mathcal{T}$ mesurable et $x, x' \in \mathcal{X}^{(\mathbb{N})}$ voisines.

On note que

$$\begin{aligned}
\mathbb{P}\left(M_{\text{cont}}(x) \in \mathcal{S}\right) &= \int_{\mathcal{S}} \frac{\exp(-\text{len}_f^\rho(x,t)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-\text{len}_f^\rho(x,s)\varepsilon/2)\mathrm{d}\mu(s)}\mathrm{d}\mu(t) \\
&\leq \int_{\mathcal{S}} \frac{\exp(-(\text{len}_f^\rho(x',t)-1)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-(\text{len}_f^\rho(x',s)+1)\varepsilon/2)\mathrm{d}\mu(s)}\mathrm{d}\mu(t) \\
&= \frac{\exp(\varepsilon/2)}{\exp(-\varepsilon/2)} \int_{\mathcal{S}} \frac{\exp(-\text{len}_f^\rho(x',t)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-\text{len}_f^\rho(x,s)\varepsilon/2)\mathrm{d}\mu(s)}\mathrm{d}\mu(t) \\
&= \exp(\varepsilon)\mathbb{P}\left(M_{\text{cont}}(x') \in \mathcal{S}\right)
\end{aligned}$$

3.2 Quasi-optimalité du mécanisme de sensibilité inverse

L'article présentant le mécanisme de sensibilité inverse [AD20] détail une borne de précision sur la médiane. Nous allons ici étendre cette démonstration au cas des déciles. Dans cette section nous nous plaçons dans le cas où les données sont identiquement distribuées à partir d'une loi ayant une distribution continue π_P au voisinage de ses déciles $(d_i^l)_i$. Commençons par énoncé le résultat.

Théorème 3.2.0.1 :
Soit $\gamma \in \mathbb{R}_+^\star$, $u \in [0, \gamma/4]$, $\rho \in \mathbb{R}_+$ et $X \in [0,R]^n$ dont les éléments sont obtenues à partir d'une loi P de densité π_P continue au voisinage de ses déciles. On pose $p_{\min,i} = \inf_{t \in [d_i^l - 2\gamma, d_i^l + 2\gamma]} \pi_P(t)$. On note $(d_i)_i$ les déciles empirique de X et $(d_i^l)_i$ les déciles de la loi. Notons alors enfin M_{cont} le mécanisme de sensibilité inverse ρ-lisse.

$$\mathbb{P}\left(|M_{\text{cont},i} - d_i| > 2u + \rho\right) \leq \frac{R}{2\rho} \exp\left(-\frac{np_{\min,i}u\varepsilon}{4}\right) + 4\exp\left(-\frac{n\gamma^2 p_{\min,i}^2}{8}\right) + \frac{2\gamma}{u}\exp\left(-\frac{np_{\min,i}u}{8}\right)$$

démonstration : Ce théorème donne une borne exponentielle sur la précision de l'algorithme. Le démonstration est longue.

Découpons l'intervalle $[d_i^l - \gamma, d_i^l + \gamma]$ en intervalles $(I_j)_j$ de taille u. Pour tout j, on pose $N_j = \#I_j$. On note alors A l'événement "pour tout j, $N_j \geq nup_{\min,i}/2$" et B_i l'événement

"$|d_i^l - d_i| \geq \gamma/2$".

$$\begin{aligned}
\mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho\right) &= \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) \mathbb{P}\left(A \wedge B_i\right) \\
&\quad + \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid \overline{A} \vee \overline{B}_i\right) \mathbb{P}\left(\overline{A} \vee \overline{B}_i\right) \\
&\leq \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) + \mathbb{P}\left(\overline{A} \vee \overline{B}_i\right) \\
&= \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) + \mathbb{P}\left((\overline{A} \wedge B_i) \vee \overline{B}_i\right) \\
&\leq \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) + \mathbb{P}\left(\overline{A} \wedge B_i\right) + \mathbb{P}\left(\overline{B}_i\right) \\
&= \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) + \mathbb{P}\left(\overline{A} \mid B_i\right) \mathbb{P}(B_i) + \mathbb{P}\left(\overline{B}_i\right) \\
&\leq \mathbb{P}\left(|M_{\text{cont},i} - d_i^l| > 2u + \rho \mid A \wedge B_i\right) + \mathbb{P}\left(\overline{A} \mid B_i\right) + \mathbb{P}\left(\overline{B}_i\right)
\end{aligned}$$

Nous savons que si les événements A et B surviennent, pour tout t tel que $|t - d_i| > 2u$, au moins $nup_{\min,i}/2$ éléments séparent d_i et t. Pour de tels t nous avons alors $\text{len}_f(x,t) \geq nup_{\min,i}/2$. Ainsi, pour tout s tel que $|s - d_i| > 2u + \rho$, $\text{len}_f^\rho(x,s) \geq nup_{\min,i}/2$. Enfin, pour tout t tel que $|t - d_i| > 2u + \rho$,

$$\begin{aligned}
\pi_P\left(t \mid A \wedge B\right) &= \frac{\exp\left(-\text{len}_f^\rho(x,t)\varepsilon/2\right)}{\int_{\mathcal{T}} \exp\left(-\text{len}_f^\rho(x,s)\varepsilon/2\right) \mathrm{d}\mu(s)} \\
&\leq \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{\int_{\mathcal{T}} \exp\left(-\text{len}_f^\rho(x,s)\varepsilon/2\right) \mathrm{d}\mu(s)} \\
&\leq \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{\int_{d_i-\rho}^{d_i+\rho} \exp\left(-\text{len}_f^\rho(x,s)\varepsilon/2\right) \mathrm{d}\mu(s)} \\
&= \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{\int_{d_i-\rho}^{d_i+\rho} \mathrm{d}\mu(s)} \\
&= \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{2\rho}
\end{aligned}$$

Ainsi,

$$\begin{aligned}
\mathbb{P}\left(|M_{\text{cont}} - d_i| > 2u + \rho \mid A \wedge B_i\right) &\leq \int_{\mathcal{T}} \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{2\rho} \mathbb{1}_{|t-d_i|>2u+\rho} \mathrm{d}\mu(t) \\
&\leq \frac{\exp\left(-nup_{\min,i}\varepsilon/4\right)}{2\rho} \mu(\mathcal{T}) \\
&= \frac{R}{2\rho} \exp\left(-nup_{\min,i}\varepsilon/4\right)
\end{aligned}$$

Nous allons maintenant calculer la probabilité de l'événement $\overline{B}_i$. Pour cela, on pose $\alpha = \gamma/2$, pour tout $j \in [\![0, n-1]\!]$ on pose $C_j^i = \mathbb{1}_{x_i > d_i^l + \alpha}$ et $C^i = \sum_{j=0}^{n-1} C_j$. L'événement C^i dénote le nombre d'éléments de X plus grands que $d_i^l + \alpha$. Par définition de $p_{\min,i}$ assure que

$$\begin{aligned}
\hat{p} &:= \mathbb{P}(C_j^i = 1) \\
&= 1 - \int_0^{d_i^l} \pi_P(t) \mathrm{d}\mu(t) - \int_{d_i^l}^{d_i^l+\alpha} \pi_P(t) \mathrm{d}\mu(t) \\
&\overset{\text{déf de } d_i^l}{=} 1 - \frac{i}{10} - \int_{d_i^l}^{d_i^l+\alpha} \pi_P(t) \mathrm{d}\mu(t) \\
&\leq \frac{10-i}{10} - p_{\min,i} \int_{d_i}^{d_i^l+\alpha} \mathrm{d}\mu(t) \\
&= \frac{10-i}{10} - \alpha p_{\min,i}
\end{aligned}$$

Or, si $d_i > d_i^l$, $C^i \geq in/10$. Ainsi, en utilisant une borne de Chernoff (C^i est d'espérance $\hat{p}n$ et les $(C_j^i)_j$ sont indépendantes),

$$\begin{aligned}
\mathbb{P}\left(d_i > d_i^l + \alpha\right) &\leq \mathbb{P}\left(C^i \geq \frac{in}{10}\right) \\
&= \mathbb{P}\left(\sum_{j=0}^{n-1} C_j^i \geq \hat{p}n\left(1 - \left(1 - \frac{i}{\hat{p}10}\right)\right)\right) \\
&\leq \exp\left(-\left(1 - \frac{i}{\hat{p}10}\right)^2 \frac{n\hat{p}}{2}\right) \\
&= \exp\left(-\left(\hat{p} - \frac{i}{10}\right)^2 \frac{n}{2\hat{p}}\right) \\
&\leq \exp\left(-\left(\alpha p_{\min,i}\right)^2 \frac{n}{2\hat{p}}\right) \\
&\leq \exp\left(-\alpha^2 p_{\min,i}^2 \frac{n}{i/5 - 2\alpha p_{\min,i}}\right) \\
&\leq \exp\left(-\frac{1}{2}\alpha^2 p_{\min,i}^2 n\right)
\end{aligned}$$

On montre alors de même que $\mathbb{P}\left(d_i < d_i^l - \alpha\right) < \exp\left(-\frac{1}{2}\alpha^2 p_{\min,i}^2 n\right)$. Nous avons donc montré que

$$\mathbb{P}\left(B_i\right) \geq 1 - 2\exp\left(-\frac{1}{8}n\gamma^2 p_{\min,i}^2\right)$$

Finalement, il ne nous reste plus qu'à minorer $\mathbb{P}(A \mid B_i)$! Pour cela, notons que

$$\mathbb{P}(A \mid B_i) \geq (A \mid B_i)\mathbb{P}(B_i) = \mathbb{P}(A) - \mathbb{P}\left(A \wedge \overline{B}_i\right) \geq \mathbb{P}(A) - \mathbb{P}(\overline{B}_i)$$

Pour tout $k \leq n-1$ on pose alors $Z_k = \mathbb{1}_{x_k \in I_j}$ et on a $N_j = \sum_{k=0}^{n-1} Z_k$. On note que $\mathbb{P}(Z_j = 1) \geq up_{\min,i}$. Utiliser une nouvelle fois une borne de Chernoff assure enfin que

$$\mathbb{P}\left(N_j < nup_{\min,i}/2\right) = \mathbb{P}\left(N_j < nup_{\min,i}\left(1 - \frac{1}{2}\right)\right) < \exp\left(-\frac{1}{8}nup_{\min,i}\right)$$

Enfin,

$$\mathbb{P}\left(\overline{A}\right) = \mathbb{P}\left(\bigcup_{j=0}^{2\gamma/u} N_j < nup_{\min,i}/2\right) \leq \sum_{j=0}^{2\gamma/u} \mathbb{P}\left(N_j < nup_{\min,i}/2\right) \leq \frac{2\gamma}{u}\exp\left(-\frac{1}{8}nup_{\min,i}\right)$$

On obtient alors

$$\mathbb{P}(A \mid B_i) \geq 1 - \frac{2\gamma}{u}\exp\left(-\frac{1}{8}nup_{\min,i}\right) - 2\exp\left(-\frac{1}{8}n\gamma^2 p_{\min,i}^2\right)$$

Ce que nous permet alors d'obtenir le résultat recherché !

A HistogramMethod : Analyse de précision - le cas de la loi normale centrée réduite

A.1 Démonstration du lemme [2]

Lemme A.1.0.1 : *Estimation de l'écard entre les déciles empiriques et ceux de la loi normale centrée réduite.*
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite et soit $\gamma \in [0, d_i^l]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi normale centrée réduite. Pour tout $i \in [\![1, 9]\!]$

$$\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) \geq 1 - \eta$$

Avec

$$\begin{aligned}\eta = 2 &- \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\ &+ \frac{1}{(2\pi)^{n/2}} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k}\end{aligned}$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi uniforme sur [0,1]. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ ceux de la loi. Soit $\gamma \in [0, d_i^l]$. On note que

$$\begin{aligned}\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma + 2]) &= 1 - \mathbb{P}(d_i \notin [d_i^l - \gamma/2, d_i^l + \gamma/2]) \\ &= 1 - \mathbb{P}(d_i \leq d_i^l - \gamma/2 \vee d_i \geq d_i^l + \gamma/2)\end{aligned}$$

On pose alors $A =$ "il y a au moins $in/10$ valeurs plus petites que $d_i^l - \gamma/2$" et $B =$ "il y a au moins $(10-i)n/10$ valeurs plus grandes que $d_i^l - \gamma/2$". Pour tout $j \in [\![0, n-1]\!]$ on pose $A_j = \mathbb{1}_{x_j \leq d_i^l + \gamma/2}$, $B_j = \mathbb{1}_{x_j \geq d_i^l - \gamma/2}$, $A_s = \sum_{j=0}^{n-1} A_j$ et $B_s = \sum_{j=0}^{n-1}$. On a alors, $A = \{A_s \geq in/10\}$ et $B = \{B_s \geq n - in/10\}$. Une application d'une borne de Chernoff assure alors que

$$\begin{aligned}\mathbb{P}(A) &= \mathbb{P}(A_s \geq in/10) \\ &= \mathbb{P}\left(A_s \geq \frac{n}{\sqrt{2\pi}} \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \left(1 + \frac{i\sqrt{2\pi}}{10 \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(-t^2/2\right) \mathrm{d}t} - 1 \right) \right) \\ &\overset{d_i^l \geq \gamma}{\leq} \exp\left(-\frac{n}{3\sqrt{2\pi}} \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \left(\frac{i\sqrt{2\pi}}{10 \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(-t^2/2\right) \mathrm{d}t} - 1 \right)^2 \right) \\ &= \exp\left(-\frac{n}{3} \left(\frac{i}{10} - \frac{1}{\sqrt{2\pi}} \int_{d_i^l - \gamma/2}^{d_i^l} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right) \left(\frac{i\sqrt{2\pi}}{10 \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(-t^2/2\right) \mathrm{d}t} - 1 \right)^2 \right) \\ &\leq \exp\left(-\frac{n}{3} \left(\frac{i}{10} - \exp\left(-\frac{(d_i^l)^2}{2}\right) / \sqrt{2\pi} \right) \left(\frac{i\sqrt{2\pi}}{10 \int_{-\infty}^{d_i^l - \gamma/2} \exp\left(-t^2/2\right) \mathrm{d}t} - 1 \right)^2 \right)\end{aligned}$$

On a alors

$$
\begin{aligned}
&\mathbb{P}(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]) \\
&= 1 - \mathbb{P}(A \cup B) \\
&\geq 1 - \mathbb{P}(A) - \mathbb{P}(B) \\
&= \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{d_i^l}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\
&\qquad + \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{-\infty}^{d_i^l} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} - 1 \\
&= \frac{1}{\sqrt{2\pi}^n} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\
&\qquad + \frac{1}{\sqrt{2\pi}^n} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \right)^{n-k} - 1
\end{aligned}
$$

A.2 Démonstration du lemme [3]

Lemme A.2.0.1 :
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la normale centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$ et $k \in \mathbb{N}$. Il y a au moins α valeurs de X dans chacun des intervalles $[d_i^l - \gamma, d_i^l - \gamma/2]$ et $[d_i^l + \gamma/2, d_i^l + \gamma]$ avec une probabilité au moins $1 - \beta$ avec

$$
\begin{aligned}
\beta = &\sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\
&+ \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k}
\end{aligned}
$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$ et $\alpha \in \mathbb{N}$. On note que

$$
\begin{aligned}
&\mathbb{P}\left(\#\{x \in X | x \in [d_i^l - \gamma, d_i^l - \gamma/2]\} \geq \alpha \wedge \#\{x \in X | x \in [d_i^l + \gamma/2, d_i^l + \gamma]\} \geq \alpha\right) \\
&\geq \mathbb{P}\left(\#\{x \in X | x \in [d_i^l - \gamma, d_i^l - \gamma/2]\} \geq \alpha\right) \\
&\quad + \mathbb{P}\left(\#\{x \in X | x \in [d_i^l + \gamma/2, d_i^l + \gamma]\} \geq \alpha\right) - 1 \\
&= 1 - \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l - \gamma}^{d_i^l - \gamma/2} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k} \\
&\quad - \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^k \left(1 - \int_{d_i^l + \gamma/2}^{d_i^l + \gamma} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) \mathrm{d}t \right)^{n-k}
\end{aligned}
$$

A.3 Démonstration du théorème [1]

Théorème A.3.0.1 : *(α, β)-précision de `HistogramMethod` dans le cas de la loi normale centrée réduite*
Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$, $k \in \mathbb{N}$ et $\beta \in [0, 1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi normale centrée réduite. Posons A la variable aléatoire `HistogramMethod(X, epsilon, k, a, b)`.

$$\mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) \geq 1 - \beta - \eta - \mu$$

Avec

$$\begin{cases} \alpha & = \dfrac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon} \\ \mu & = \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l-\gamma}^{d_i^l-\gamma/2} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^k \left(1 - \int_{d_i^l-\gamma}^{d_i^l-\gamma/2} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ & \quad + \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l+\gamma/2}^{d_i^l+\gamma} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^k \left(1 - \int_{d_i^l+\gamma/2}^{d_i^l+\gamma} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ \eta & = 2 - \dfrac{1}{(2\pi)^{n/2}} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ & \quad + \dfrac{1}{(2\pi)^{n/2}} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \end{cases}$$

Démonstration : Soit X un ensemble de n variables aléatoires $(X_i)_i$ indépendantes et suivant toutes la loi normale centrée réduite. Soit $\gamma \in [0, d_i^l]$, $i \in [\![1, 9]\!]$, $k \in \mathbb{N}$ et $\beta \in [0, 1]$. Notons $(d_i)_i$ les déciles empiriques de X et $(d_i^l)_i$ les déciles de la loi normale centrée réduite. Posons A la variable aléatoire `HistogramMethod(X, epsilon, k, a, b)`.

On pose

$$\alpha = \frac{8\left(\log k + \log(2/\beta)\right)}{\varepsilon}$$

Notons alors E_α l'événement "Il y a au moins α valeurs de X dans chacun des intervalles $[d_i^l - \gamma, d_i^l - \gamma/2]$ et $[d_i^l + \gamma/2, d_i^l + \gamma]$" Et E_{A_i} l'événement "moins de α valeurs de X séparent d_i et A_i". Nous avons alors

$$\begin{aligned} \mathbb{P}\left(A_i \in [d_i^l - \gamma, d_i^l + \gamma]\right) &\geq \mathbb{P}\left(E_{A_i} \wedge E_\alpha \wedge d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]\right) \\ &\geq \mathbb{P}\left(E_{A_i}\right) + \mathbb{P}\left(E_\alpha\right) + \mathbb{P}\left(d_i \in [d_i^l - \gamma/2, d_i^l + \gamma/2]\right) - 2 \end{aligned}$$

Les lemmes précédent assurent alors que

$$\begin{aligned} \mathbb{P}\left(A_i \in [0.1i - \gamma, 0.1i + \gamma]\right) &\geq (1 - \beta) + (1 - \mu) + (1 - \eta) - 2 \\ &\geq 1 - \beta - \mu - \eta \end{aligned}$$

Avec

$$\begin{cases} \mu & = \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l-\gamma}^{d_i^l-\gamma/2} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^k \left(1 - \int_{d_i^l-\gamma}^{d_i^l-\gamma/2} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ & \quad + \sum_{k=0}^{\alpha} \binom{n}{k} \left(\int_{d_i^l+\gamma/2}^{d_i^l+\gamma} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^k \left(1 - \int_{d_i^l+\gamma/2}^{d_i^l+\gamma} \dfrac{1}{\sqrt{2\pi}} \exp\left(\dfrac{-t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ \eta & = 2 - \dfrac{1}{(2\pi)^{n/2}} \sum_{k=0}^{in/10} \binom{n}{k} \left(\int_{-\infty}^{d_i^l} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{d_i^l}^{+\infty} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \\ & \quad + \dfrac{1}{(2\pi)^{n/2}} \sum_{k=0}^{(10-i)n/10} \binom{n}{k} \left(\int_{d_i^l}^{+\infty} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^k \left(\int_{-\infty}^{d_i^l} \exp\left(-\dfrac{t^2}{2}\right) \mathrm{d}t\right)^{n-k} \end{cases}$$

Références

Asi, Hilal et John C. Duchi. “Near Instance-Optimality in Differential Privacy”. In : *ArXiv* abs/2005.10630 (mai 2020). url : https://arxiv.org/pdf/2005.10630.pdf.

Dwork, Cynthia et Aaron Roth. “The Algorithmic Foundations of Differential Privacy”. In : *Foundations and Trends in Theoretical Computer Science* 9 (août 2014), p. 211-407. url : https://www.microsoft.com/en-us/research/publication/algorithmic-foundations-differential-privacy/.

Dwork, Cynthia et al. “Calibrating Noise to Sensitivity in Private Data Analysis”. In : *Theory of Cryptography*. Sous la dir. de Shai Halevi et Tal Rabin. Berlin, Heidelberg : Springer Berlin Heidelberg, 2006, p. 265-284. isbn : 978-3-540-32732-5.

McSherry, Frank et Kunal Talwar. “Mechanism Design via Differential Privacy”. In : *Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE, oct. 2007. url : https://www.microsoft.com/en-us/research/publication/mechanism-design-via-differential-privacy/.