Descente par coordonnées pour la minimisation du risque empirique sous contraintes de confidentialité différentielle

Paul Mangold, Aurélien Bellet, Joseph Salmon, Marc Tommasi
Univ. Lille, Inria, CNRS, Centrale Lille, UMR 9189 - CRIStAL, F-59000 Lille, France,
IMAG, Univ. Montpellier, CNRS, Montpellier, France

Email : paul.mangold@inria.fr

Mots Clés : Optimisation, Confidentialité des données, Descente par coordonnées.

Biographie – J'ai commencé ma thèse à l'Inria Lille en octobre 2020, sous la supervision de Marc Tommasi (Univ. Lille) et Aurélien Bellet (Inria Lille), et en étroite collaboration avec Joseph Salmon (Univ. Montpellier). Ma thèse porte très généralement sur l'optimisation sous contraintes de confidentialité différentielle dans un contexte d'apprentissage fédéré ou décentralisé.

Resumé :

Les modèles de machine learning révèlent des informations sur les données utilisées lors de leur entraînement [7]. Or, ces données sont souvent sensibles ou confidentielles, constituant un frein majeur à l'utilisation réelle de ces modèles. La confidentialité différentielle [4] permet de quantifier formellement les possibilités de fuites de données sensibles lors d'accès (successifs) à une base de données, et s'est imposée comme un critère de référénce en termes de confidentialité. Il est donc possible d'entraîner des modèles de machine learning en résolvant le problème de minimisation du risque empirique sous contraintes de confidentialité différentielle [3], limitant la possibilité de retrouver des informations sensibles à partir d'un modèle entraîné. Plusieurs algorithmes ont été proposés pour résoudre ce problème, généralement basés sur l'algorithme de descente de gradient stochastique [2, 8]. Ces algorithmes utilisent une version bruitée des gradients (stochastiques), de façon à masquer la contribution individuelle de chacun des points des données au résultat. Leur utilisation pratique repose sur le bornement de la norme des gradients, limitant l'ajout de bruit inutile [1].

Certains problèmes peuvent cependant être résolus de manière plus efficace grâce à d'autres méthodes, notamment la méthode de descente par coordonnées [5, 6]. Dans cette présentation, nous proposons un algorithme de descente par coordonnées pour le problème de minimisation du risque empirique sous contraintes de confidentialité différentielle. Nous prouvons que l'algorithme proposé respecte bien la contrainte de confidentialité différentielle, et donnons un résultat d'utilité (convergence). Notre analyse montre que la méthode de descente par coordonnées est pertinente pour le problème considéré, et qu'elle permet d'obtenir une utilité similaire à celles obtenues par les algorithmes privés existants [2, 8]. Nous montrons ensuite que notre analyse donne une règle naturelle pour adapter le seuil de bornement des gradients à chacune des coordonnées de la fonction minimiése, évitant d'avoir à le régler individuellement pour chacune d'elles. Finalement, afin de valider la pertinence et l'applicabilité de notre approche, nous proposons des expériences numériques, qui valident nos résultats théoriques sur des problèmes pratiques.

Références

[1] Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, pages 308–318, 2016.

[2] Raef Bassily, Adam Smith, and Abhradeep Thakurta. Private Empirical Risk Minimization: Efficient Algorithms and Tight Error Bounds. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pages 464–473, Philadelphia, PA, USA, October 2014. IEEE.

[3] Kamalika Chaudhuri, Claire Monteleoni, and Anand D Sarwate. Differentially Private Empirical Risk Minimization. page 41, 2011.

[4] Cynthia Dwork. Differential Privacy. *33rd International Colloquium on Automata, Languages and Programming*, 2006.

[5] Yu. Nesterov. Efficiency of Coordinate Descent Methods on Huge-Scale Optimization Problems. *SIAM Journal on Optimization*, 22(2):341–362, January 2010.

[6] Peter Richtárik and Martin Takáč. Iteration complexity of randomized block-coordinate descent methods for minimizing a composite function. *Mathematical Programming*, 144(1-2):1–38, April 2014.

[7] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership Inference Attacks against Machine Learning Models. *arXiv:1610.05820 [cs, stat]*, March 2017.

[8] Di Wang, Minwei Ye, and Jinhui Xu. Differentially Private Empirical Risk Minimization Revisited: Faster and More General. page 10, 2018.