Normalized Square Root: Sharper Matrix Factorization Bounds for Differentially Private Continual Counting

Monika Henzinger
Institute of Science and Technology Austria (ISTA), Klosterneuburg, Austria

Nikita Kalinin
Institute of Science and Technology Austria (ISTA), Klosterneuburg, Austria

Jalaj Upadhyay
Rutgers University, Piscataway, NJ, USA

Abstract

The factorization norms of the lower-triangular all-ones $n \times n$ matrix, $\gamma_2(M_{\mathsf{count}})$ and $\gamma_{\mathrm{F}}(M_{\mathsf{count}})$, play a central role in differential privacy as they are used to give theoretical justification of the accuracy of the only known production-level private training algorithm of deep neural networks by Google. Prior to this work, the best known upper bound on $\gamma_2(M_{\mathsf{count}})$ was $1 + \frac{\log(n)}{\pi}$ by Mathias (Linear Algebra and Applications, 1993), and the best known lower bound was $\frac{1}{\pi}\left(2 + \log\left(\frac{2n+1}{3}\right)\right) \approx 0.507 + \frac{\log(n)}{\pi}$ (Matoušek, Nikolov, Talwar, IMRN 2020), where $\log(\cdot)$ is the natural logarithm. Recently, Henzinger and Upadhyay (SODA 2025) gave the first explicit factorization that meets the bound of Mathias (1993) and asked whether there exists an explicit factorization that improves on Mathias' bound. We answer this question in the affirmative. Additionally, we improve the lower bound significantly. More specifically, we show that $o(1) + 0.701 + \frac{\log(n)}{\pi} \leq \gamma_2(M_{\mathsf{count}}) \leq 0.846 + \frac{\log(n)}{\pi} + o(1)$. That is, we reduce the gap between the upper and lower bound to $0.14 + o(1)$ and first improvement in over three decades. Additionally, we show that our factors achieve a better upper bound for $\gamma_{\mathrm{F}}(M_{\mathsf{count}})$ compared to prior work, and we also establish an improved lower bound for $\gamma_{\mathrm{F}}(M_{\mathsf{count}})$: $o(1) + 0.701 + \frac{\log(n)}{\pi} \leq \gamma_{\mathrm{F}}(M_{\mathsf{count}}) \leq 0.748 + \frac{\log(n)}{\pi} + o(1)$. That is, the gap between the lower and upper bound provided by our explicit factorization is $0.047 + o(1)$.

2012 ACM Subject Classification Security and privacy; Theory of computation → Theory and algorithms for application domains

Keywords and phrases Differential privacy, continual release, factorization norm

Digital Object Identifier 10.4230/LIPIcs.FORC.2026.5

Category Extended Abstract

Related Version *Full Version*: `https://arxiv.org/abs/2509.14334`

Funding *Monika Henzinger*: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (MoDynStruct, No. 101019564) and the Austrian Science Fund (FWF) grant DOI 10.55776/I5982. For open access purposes, the author has applied a CC BY public copyright license to any author-accepted manuscript version arising from this submission. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.
Nikita Kalinin: This work is supported in part by the Austrian Science Fund (FWF) [10.55776/COE12]. A part of this work was done while visiting University of Copenhagen.
Jalaj Upadhyay: This project was supported in my part by NSF CNS 2433628, Google Seed Fund grant, Google Research Scholar Award, Dean Research Seed Fund, and Decanal Research Grant. A part of this work was done while visiting the Institute of Science and Technology (ISTA), Austria.

7th Symposium on Foundations of Responsible Computing (FORC 2026).
Editor: Huijia (Rachel) Lin; Article No. 5; pp. 5:1–5:1
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany