

# 000 001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020 021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040 041 042 043 044 045 046 047 048 049 050 051 052 053

## LEARNING RATE SCHEDULING WITH MATRIX FACTORIZATION FOR PRIVATE TRAINING

**Anonymous authors**

Paper under double-blind review

### ABSTRACT

We study differentially private model training with stochastic gradient descent under learning rate scheduling and correlated noise. Although correlated noise, in particular via matrix factorizations, has been shown to improve accuracy, prior theoretical work focused primarily on the prefix-sum workload. That workload assumes a constant learning rate, whereas in practice learning rate schedules are widely used to accelerate training and improve convergence. We close this gap by deriving general upper and lower bounds for a broad class of learning rate schedules in both single- and multi-epoch settings. Building on these results, we propose a learning-rate-aware factorization that achieves improvements over prefix-sum factorizations under both MaxSE and MeanSE error metrics. Our theoretical analysis yields memory-efficient constructions suitable for practical deployment, and experiments on CIFAR-10 confirm that schedule-aware factorizations improve accuracy in private training.

### 1 INTRODUCTION

Privacy has become a major concern as machine learning systems are trained on sensitive data such as personal communications, financial transactions, and medical records. Beyond the risk of direct data exposure, models themselves may memorize and unintentionally reveal private information, creating serious ethical and security challenges. These concerns are especially pressing for production-level large language models trained on vast and heterogeneous datasets.

A widely studied approach to mitigating these risks is differential privacy (DP), which provides formal mathematical guarantees that the output of a learning algorithm does not reveal sensitive information about any individual training example (Dwork et al., 2006). In practice, DP is often achieved by injecting carefully calibrated noise into either the gradients, ensuring that an adversary cannot infer the presence or absence of a single data point with high confidence. More recently, large-scale efforts such as VaultGemma (VaultGemma Team, 2025) have demonstrated that it is possible to train billion-parameter models with rigorous privacy guarantees, showing that DP can be integrated into state-of-the-art architectures without prohibitive utility loss.

To make model training differentially private, algorithms typically inject noise into the gradients to mask the contribution of any individual data point. The most common approach, DP-SGD, adds independent Gaussian noise at each update, which provides strong privacy guarantees but can significantly reduce accuracy (Abadi et al., 2016). *Matrix factorization* has emerged as a more general alternative that introduces correlations in the injected noise, enabling improved accuracy while preserving privacy (Choquette-Choo et al., 2023a;b). The approach has also seen practical adoption, with Google reporting its use for training production on-device language models in their 2024 blog post “Advances in private training for production on-device language models” (Xu & Zhang, 2024).

Recent work has focused on making matrix factorization memory efficient (McKenna, 2025; Andersson & Pagh, 2025; Kalinin et al., 2025; McMahan et al., 2024), and it has also been analyzed theoretically, mostly in the setting of Toeplitz workloads (Fichtnerberger et al., 2023; Henzinger et al., 2024; Henzinger & Upadhyay, 2025; Dvijotham et al., 2024). However, existing utility analyses assume a constant learning rate. While Denisov et al. (2022) introduced a non-Toeplitz workload with varying learning rates, its theoretical properties remain largely unexplored. In this work, we address this gap by studying matrix factorization under learning rate schedules.

054 Learning rate scheduling plays a critical role in the optimization of machine learning models, and a  
 055 variety of strategies have been proposed in the literature. Popular approaches include cosine annealing  
 056 (Loshchilov & Hutter, 2017) and cyclical learning rates (Smith, 2017), which adapt the step size  
 057 during training to improve convergence. Another common technique is warm-starting (He et al.,  
 058 2016), where models begin with a small learning rate that is gradually increased, as used in large-  
 059 scale training setups (Goyal et al., 2017). In this work, we focus on learning rate decays available in  
 060 PyTorch Paszke et al. (2019) such as exponential, linear, polynomial and cosine, which are widely  
 061 used and can be easily applied in practice.

062 Learning rate scheduling can be particularly useful in private training when the number of iterations  
 063 is limited. By accelerating convergence, it enables higher accuracy in settings such as warm-up training  
 064 (Kurakin et al., 2022), private fine-tuning (Luo et al., 2021), and training under computational  
 065 constraints. It has also been combined with matrix factorization as a form of learning rate cool-down  
 066 (Choquette-Choo et al., 2023b;a; 2025), and was shown to provide improvements over fixed learning  
 067 rates in Denisov et al. (2022), where the workload of our interest was originally introduced.

## 068 Contribution

- 070 • We theoretically analyze the problem of matrix factorization under learning rate scheduling. We  
 071 establish general lower and upper bounds for MaxSE and MeanSE in single-epoch, as well as for  
 072 MeanSE in multi-epoch for a large class of schedulers. Here, MaxSE characterizes the maximum  
 073 variance of the added noise, while MeanSE captures the average variance across iterations.
- 074 • We propose a learning-rate-aware Toeplitz factorization, which for exponentially decaying learning  
 075 rate is provably optimal in MaxSE under single-epoch and improves upon the proposed upper  
 076 bound for MeanSE. We adopt this factorization for memory efficient, multi-epoch training by  
 077 making it banded inverse.
- 078 • We show numerically that the proposed factorization is close to optimal in all metrics.
- 079 • We show experimentally on CIFAR-10 that banded inverse factorizations benefit from learning  
 080 rate scheduling. Moreover, we demonstrate that the proposed learning-rate-aware factorization  
 081 achieves even further accuracy improvements.

## 082 2 BACKGROUND

083 The most common way to train differentially private models is by using *DP-SGD* (Abadi et al.,  
 084 2016). At each step we receive a gradient  $g_i \in \mathbb{R}^d$ , clip it to a fixed  $\ell_2$  norm  $\zeta > 0$ , and add  
 085 appropriately scaled independent Gaussian noise  $z_i \sim \mathcal{N}(0, I_d \sigma^2)$ , where  $\sigma$  depends on the target  
 086 privacy level  $(\epsilon, \delta)$ . The model is then updated as

$$087 \theta_i = \theta_{i-1} - \eta_i (\text{clip}(g_i, \zeta) + z_i), \quad (1)$$

088 where  $\eta_i$  is the learning rate at step  $i$ .

089 This procedure can be improved by correlating the noise across iterations. To formalize this, we  
 090 define a matrix  $G \in \mathbb{R}^{n \times d}$  of stacked gradients, a matrix  $\Theta \in \mathbb{R}^{n \times d}$  of intermediate models, and  
 091 a workload matrix  $A \in \mathbb{R}^{n \times n}$  that encodes the training process such that  $\Theta = AG$ . If we use a  
 092 constant learning rate, this matrix, denoted  $A_1$ , is a lower triangular matrix of ones. For varying  
 093 learning rates we instead use a matrix  $A_X$ , described later.

094 To ensure that the intermediate models are differentially private, we can apply a matrix factoriza-  
 095 tion mechanism. Specifically, we factorize  $A$  into two matrices  $B$  and  $C$ , then compute  $CG$ , add  
 096 Gaussian noise to ensure differential privacy, and finally multiply the result by  $B$  as post-processing:

$$097 \widehat{AG} = B(CG + Z) = A(G + C^{-1}Z), \quad (2)$$

098 which is equivalent to adding correlated Gaussian noise with covariance structure induced by  $C^{-1}$   
 099 to the gradients.

100 The remaining question is: *how much noise must be added, and does this procedure remain differ-  
 101 entially private when the gradients are not known in advance but depend on the current model?* The  
 102 foundational work of Denisov et al. (2022) shows that the procedure is indeed differentially private,  
 103 even when the gradients adaptively depend on the model, provided we add noise of scale

$$104 \sigma = \zeta \cdot \sigma_{\epsilon, \delta} \cdot \text{sens}(C) = \zeta \cdot \sigma_{\epsilon, \delta} \cdot \|C\|_{1 \rightarrow 2}, \quad (3)$$

108 **Algorithm 1** Differentially Private SGD with Matrix Factorization and Learning Rate Schedules109  
110 **Require:** Model initialization  $\theta_0 \in \mathbb{R}^d$ , dataset  $D$ , batchsize  $B$ , model loss  $\ell(\theta, d)$ , clipnorm  $\zeta > 0$ ,  
111 learning rate  $\eta$ , correlation matrix  $C \in \mathbb{R}^{n \times n}$ , learning rate scheduler  $\chi_i$ ,  
112 noise matrix  $Z \in \mathbb{R}^{n \times d}$  with i.i.d. entries  $\mathcal{N}(0, \text{sens}^2(C)\sigma_{\epsilon,\delta}^2\zeta^2)$ .113 **for**  $i = 1, 2, \dots, n$  **do**  
114      $S_i \leftarrow \{d_1, \dots, d_B\} \subseteq D$  (select a data batch)  
115      $g_i \leftarrow \nabla_{\theta}\ell(\theta_{i-1}, d_j)$  for  $j = 1, \dots, B$   
116      $x_i \leftarrow \sum_{j=1}^B \min(1, \zeta/||g_j||) \cdot g_j$  (clip gradients)  
117      $\hat{x}_i \leftarrow \frac{1}{B}(x_i + [C^{-1}Z]_{[i,:]})$   
118      $\theta_i \leftarrow \theta_{i-1} - (\chi_i \eta) \hat{x}_i$ 119 **Ensure:**  $\theta_n$ 120  
121 where  $\zeta$  denotes the clipping norm, and  $\sigma_{\epsilon,\delta}$  is the noise multiplier of the standard Gaussian mechanism,  
122 which can be computed numerically (Balle & Wang, 2018). The term  $\text{sens}(C)$  represents  
123 the global sensitivity of the Gaussian mechanism for the product  $CG$  when the row or rows corre-  
124 sponding to a single datapoint in  $G$  change; it can be computed explicitly as  $\|C\|_{1 \rightarrow 2}$ , the maximum  
125 column norm of  $C$ . The case of multi-participation (multi-epoch) is discussed in Section 4.1. Now  
126 we have all the steps to train the model with differential privacy as presented in Algorithm 1.  
127128 The choice of factorization  $A = BC$  significantly impacts the quality of the private estimation.  
129 Following the work of Denisov et al. (2022); Henzinger et al. (2024) we quantify the *approxima-*  
130 *tion quality* by either the mean squared error (MeanSE) or the maximum expected squared error  
131 (MaxSE), which can be computed as

132  
133 
$$\text{MeanSE}(B, C) = \sqrt{\frac{1}{n} \mathbb{E}_Z \|AG - \widehat{AG}\|_F^2} = \frac{1}{\sqrt{n}} \|B\|_F \|C\|_{1 \rightarrow 2} \sigma_{\epsilon,\delta} \zeta, \quad (4)$$
  
134  
135 
$$\text{MaxSE}(B, C) = \mathbb{E}_Z \|AG - \widehat{AG}\|_\infty = \|B\|_{2 \rightarrow \infty} \|C\|_{1 \rightarrow 2} \sigma_{\epsilon,\delta} \zeta,$$

136 where  $\|\cdot\|_F$  denotes the Frobenius norm and  $\|\cdot\|_{2 \rightarrow \infty}$  the maximum row  $\ell_2$ -norm. These approx-  
137 imation errors are independent of  $G$ , and the term  $\sigma_{\epsilon,\delta} \zeta$  is independent of the matrix factorization.  
138 To isolate the contribution of the factorization  $(B, C)$ , we will use the notation  $\text{MeanSE}(B, C)$ ,  
139  $\text{MaxSE}(B, C)$  assuming  $\zeta = \sigma_{\epsilon,\delta} = 1$  in the theoretical analysis.140  
141 

### 3 METHOD

142  
143 We now turn to the workload of stochastic gradient descent (SGD) with learning rate scheduling.  
144 Let  $\chi_1, \chi_2, \dots, \chi_n$  be a sequence with  $\min \chi_t = \beta > 0$  and  $\max \chi_t = 1$ , representing a learning  
145 rate scheduler such that the actual learning rate at time  $t$  is  $\eta_t = \eta \chi_t$ . We assume that  $\beta$  is reasonably  
146 separated from 1, as the regime  $\beta \rightarrow 1$  is not of interest since it nullifies the benefits of scheduling.  
147 Then the workload matrix of interest is:

148  
149  
150  
151  
152  
153  
154 
$$A_\chi = \begin{pmatrix} \chi_1 & 0 & 0 & \cdots & 0 \\ \chi_1 & \chi_2 & 0 & \cdots & 0 \\ \chi_1 & \chi_2 & \chi_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \chi_1 & \chi_2 & \chi_3 & \cdots & \chi_n \end{pmatrix} = A_1 \times D, \quad (5)$$

155 where  $A_1$  is a prefix-sum matrix (lower triangular matrix of all ones) and  $D$  is a diagonal matrix  
156 of learning rates, i.e.,  $D = \text{diag}(\chi_1, \dots, \chi_n)$ . We will study the problem of *optimal matrix factor-*  
157 *ization* in MaxSE and MeanSE metrics for the matrix  $A_\chi$  with the **learning rate decays** given in  
158 Table 1. For the experiments, we will also include the constant learning rate ( $\chi_k = 1$ ).159  
160 In this work, we prove general lower and upper bounds for the MaxSE and MeanSE errors. For the  
161 upper bound, we use a prefix-sum-based factorization given by  $B = A_\chi(A_1)^{-1/2}$  and  $C = A_1^{1/2}$ ,  
which has been shown to be nearly optimal up to the next asymptotic term for the prefix sum problem

Table 1: Learning rate decays.

Exponential	$\chi_k = \beta^{\frac{k-1}{n-1}}$
Polynomial	$\chi_k = \beta + (1-\beta) \frac{\left(\frac{n}{k}\right)^\gamma - 1}{n^\gamma - 1}, \gamma \geq 1$
Linear	$\chi_k = 1 - \frac{k-1}{n-1}(1-\beta)$
Cosine	$\chi_k = \beta + \frac{1-\beta}{2} \left(1 + \cos\left(\frac{k-1}{n-1}\pi\right)\right)$

( $\chi_k = 1$ ) (Henzinger et al., 2025). To further improve the bounds, we propose a learning-rate-aware factorization. To define it, let  $A_\chi^{\text{Toep}}$  denote the Toeplitz matrix with  $\chi_1, \dots, \chi_n$  on its subdiagonals.

$$A_\chi^{\text{Toep}} = \begin{pmatrix} \chi_1 & 0 & 0 & \dots & 0 \\ \chi_2 & \chi_1 & 0 & \dots & 0 \\ \chi_3 & \chi_2 & \chi_1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \chi_n & \chi_{n-1} & \chi_{n-2} & \dots & \chi_1 \end{pmatrix} \quad (6)$$

We propose  $C_\chi = (A_\chi^{\text{Toep}})^{1/2}$  as a learning-rate-aware correlation matrix. To analyze its properties, we consider the exponentially decaying learning rate  $\chi_t = \beta^{\frac{t-1}{n-1}} = \alpha^{t-1}$  with  $\alpha = \beta^{\frac{1}{n-1}}$ . In this setting, the correlation matrix can be computed explicitly as

$$C_\alpha = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha r_1 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1} r_{n-1} & \alpha^{n-2} r_{n-2} & \dots & 1 \end{pmatrix}, \quad (7)$$

where the coefficients are  $r_j = \left| \binom{-1/2}{j} \right| = \frac{1}{4^j} \binom{2j}{j}$ .

## 4 RESULTS

In this work, we derive upper and lower bounds on the MaxSE and MeanSE errors of the learning rate scheduling workload  $A_\chi$  for a large class of learning rate schedulers  $\chi_1, \dots, \chi_n$ . In the following theorem, we prove an upper bound based on the prefix-sum factorization  $A_\chi A_1^{-1/2} \times A_1^{1/2}$ .

**Theorem 1.** *Let  $(\chi_t)_{t=1}^n$  be a sequence on  $[\beta, 1]$  for some constant  $\beta > 0$ . For  $n \geq 2$  we define*

$$\Delta_t = |\chi_t - \chi_{t+1}| \quad (\text{for all } 1 \leq t \leq n-1). \quad (8)$$

*If either of the following two conditions holds ( $c > 0$  an absolute constant):*

$$\Delta_t \leq \frac{c}{t(1 + \log t)} \quad (\text{for all } 1 \leq t \leq n-1), \quad \text{or} \quad \sum_{t=1}^{n-1} \Delta_t^2 = o\left(\frac{\log n}{n}\right), \quad (9)$$

*then the factorization  $B_\chi \times A_1^{1/2}$ , where  $B_\chi := A_\chi (A_1)^{-1/2}$ , satisfies*

$$\text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\max_{m \in [n]} \chi_m^2 \log m}\right), \quad (10)$$

$$\text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m}\right). \quad (11)$$

The conditions assumed in Theorem 1 are satisfied for all learning rate decays presented in Table 1, more formally:

216 **Lemma 1.** Every learning rate schedule  $(\chi_t)_{t=1}^n$  with constant  $\beta \in (0, 1/e)$  presented in Table 1  
 217 satisfies the assumptions of Theorem 1.  
 218

219 Moreover, in this work we also prove general lower bounds for any learning rate schedules:  
 220

221 **Theorem 2.** Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi = \text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_t > 0$ . Then  
 222

$$\inf_{B \times C = A_\chi} \text{MaxSE}(B, C) \geq \max_{1 \leq t \leq n} \frac{1}{\pi} \left( \min_{j \leq t} \chi_j \right) \log t \quad (12)$$

$$\inf_{B \times C = A_\chi} \text{MeanSE}(B, C) \geq \max_{1 \leq t \leq n} \frac{1}{\pi} \sqrt{\frac{t}{n}} \left( \min_{j \leq t} \chi_j \right) \log t. \quad (13)$$

227 In particular, plugging in the exponential learning rate decay  $\chi_k = \beta^{\frac{k-1}{n-1}}$  yields the following upper  
 228 and lower bounds.  
 229

230 **Corollary 1.** For exponential learning rate decay  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ , the prefix-sum-  
 231 based factorization  $A_\chi = A_\chi (A_1)^{-1/2} \times A_1^{1/2}$  gives the following values for MaxSE and MeanSE:  
 232

$$\text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta \left( \sqrt{\log n} \sqrt{\log \frac{n}{\log(1/\beta)}} \right), \quad (14)$$

$$\text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta \left( \frac{\log n}{\sqrt{\log(1/\beta)}} \right). \quad (15)$$

238 **Corollary 2.** Suppose  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then  
 239

$$\inf_{B \times C = A_\chi} \text{MaxSE}(B, C) = \Omega \left( \log \frac{n}{\log(1/\beta)} \right) \quad (16)$$

$$\inf_{B \times C = A_\chi} \text{MeanSE}(B, C) = \Omega \left( \frac{1}{\sqrt{\log(1/\beta)}} \log \frac{n}{\log(1/\beta)} \right). \quad (17)$$

246 We further improve the upper bound by considering a learning-rate-aware factorization  $C =$   
 247  $(A_\chi^{\text{Toep}})^{1/2}$ , which can be computed explicitly for the exponential learning rate decay  $\chi_k = \beta^{\frac{k-1}{n-1}} =$   
 248  $\alpha^{k-1}$ . This yields the factorization  $A_\chi = B_\alpha \times C_\alpha$ , where  $C_\alpha$  is defined in equation (7), and  $B_\alpha$  is  
 249 obtained as  $A_\chi (C_\alpha)^{-1/2}$ .  
 250

251 In Lemma 7 of Kalinin & Lampert (2024), the sensitivity of the matrix  $C_\alpha$  has been computed as:  
 252

$$\|C_\alpha\|_{1 \rightarrow 2} = \mathcal{O} \left( \frac{1}{\alpha} \sqrt{\log \frac{1}{1-\alpha^2}} \right) = \mathcal{O} \left( \sqrt{\log \frac{n}{\log(1/\beta)}} \right). \quad (18)$$

255 We then bound both the maximum row norm and the Frobenius norm of  $B_\alpha$ , which leads to the  
 256 following lemma.  
 257

258 **Lemma 2.** Let  $\beta \in (0, 1/e)$  and  $\alpha = \beta^{1/(n-1)}$ . For the factorization  $A_\chi = B_\alpha \times C_\alpha$ ,  
 259

$$\text{MaxSE}(B_\alpha, C_\alpha) = \mathcal{O} \left( \log \frac{n}{\log(1/\beta)} \right), \quad (19)$$

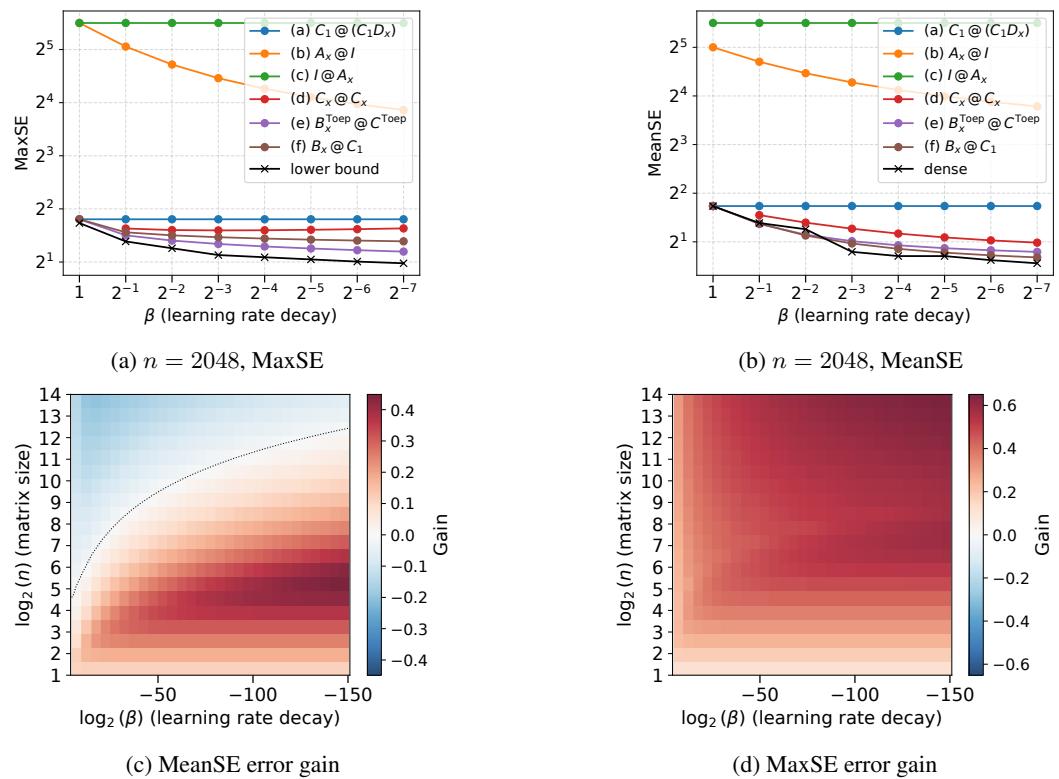
$$\text{MeanSE}(B_\alpha, C_\alpha) = \mathcal{O} \left( \sqrt{\frac{\log n}{\log(1/\beta)}} \sqrt{\log \frac{n}{\log(1/\beta)}} \right). \quad (20)$$

263 This factorization achieves the **optimal rate for the MaxSE error** and, asymptotically, performs  
 264 better than alternative factorizations for the MeanSE error.  
 265

266 We summarize the errors for the exponential learning rate decay in Table 2. In addition, we consider  
 267 four alternative factorizations: the trivial factorizations  $A_\chi \times I$  and  $I \times A_\chi$ , two prefix-sum-inspired  
 268 factorizations  $A_1^{1/2} \times A_1^{1/2} D$ , and the square-root factorization  $A_\chi^{1/2} \times A_\chi^{1/2}$ . The square-root fac-  
 269 torization is highly nontrivial to obtain since the matrix is not Toeplitz; due to space constraints, we  
 defer the detailed discussion to Appendix B.

270  
271 Table 2: Factorizations with corresponding MaxSE and MeanSE errors for exponential learning rate  
272 scheduling  $\chi_t = \beta^{\frac{t-1}{n-1}}$  for  $\beta \in (0, 1/e)$ . The proof of the first three bounds is rather technical and  
273 can be found in Lemma 6 in Appendix. The errors for square root factorization (d) can be found in  
274 Corollary 5. Learning-rate-aware factorization (e) is computed in Lemma 2. The prefix-sum-based  
275 factorization (f) is computed in Corollary 6. The lower bounds are computed in Corollary 2 in the  
276 appendix.

Factorization	MaxSE	MeanSE
(a) $A_\chi = A_1^{1/2} \times A_1^{1/2} D$	$\Theta(\log n)$	$\Theta(\log n)$
(b) $A_\chi = A_\chi \times I$	$\Theta\left(\sqrt{\frac{n}{\log 1/\beta}}\right)$	$\Theta\left(\sqrt{\frac{n}{\log 1/\beta}}\right)$
(c) $A_\chi = I \times A_\chi$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$
(d) $A_\chi = A_\chi^{1/2} \times A_\chi^{1/2}$	$\Omega\left(\sqrt{\log n} \sqrt{\log \frac{n}{\log 1/\beta}}\right)$	$\Omega\left(\frac{\log n}{\sqrt{\log(1/\beta)}}\right)$
(e) $A_\chi = A_\chi (A_\chi^{\text{Toep}})^{-1/2} \times (A_\chi^{\text{Toep}})^{1/2}$	$\mathcal{O}\left(\log \frac{n}{\log 1/\beta}\right)$	$\mathcal{O}\left(\sqrt{\frac{\log n}{\log 1/\beta}} \sqrt{\log \frac{n}{\log 1/\beta}}\right)$
(f) $A_\chi = A_1 D A_1^{-1/2} \times A_1^{1/2}$	$\Theta\left(\sqrt{\log n} \sqrt{\log \frac{n}{\log 1/\beta}}\right)$	$\Theta\left(\frac{\log n}{\sqrt{\log 1/\beta}}\right)$
Lower Bound	$\Omega\left(\log \frac{n}{\log 1/\beta}\right)$	$\Omega\left(\frac{1}{\sqrt{\log 1/\beta}} \log\left(\frac{n}{\log 1/\beta}\right)\right)$



318 Figure 1: Comparison of MaxSE and MeanSE errors under an **exponentially decaying** learning rate,  
319 for the proposed factorizations (see Table 2), with fixed matrix size  $n = 2048$  and varying decay  $\beta$ .  
320 We refer to the approximately optimal value of MeanSE computed by dense factorization (Denisov  
321 et al., 2022) as “dense.” For MaxSE, we report a lower bound since no scalable and accurate solution  
322 for its optimal value is available. The bottom row compares our learning-rate aware factorization  
323 with the prefix-sum based one, validating the theoretical improvements in both MeanSE and MaxSE.

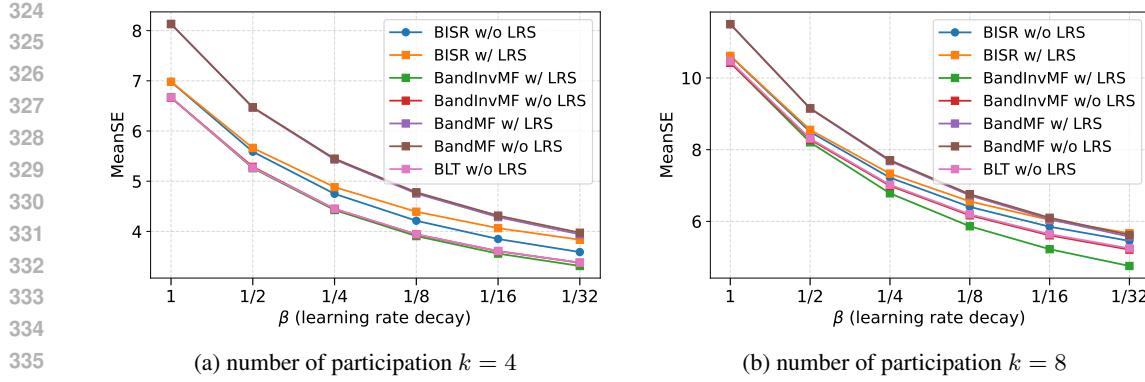


Figure 2: Multi-participation MeanSE error with matrix size  $n = 2048$ . Lines are computed for bandwidth  $p = 64$ . For the exponential workload, we observe that with a larger participation number it becomes beneficial to optimize the factorization with respect to the learning rate decay workload. However, for the considered values of  $n$  and  $\beta$ , we do not observe any benefit from incorporating learning rate scheduling for BISR.

We then numerically compare the proposed factorizations in the single-epoch (single-participation) setting using the MaxSE and MeanSE metrics, as functions of the learning rate decay  $\beta$  and the matrix size  $n$  (see Figure 1 for exponential decay and Figure 4 in the appendix for other learning rate decays). As an approximation of the actual optimal value for MeanSE, we use a dense factorization (Denisov et al., 2022) implemented in jax-privacy library (Balle et al., 2025). On the plots, we refer to this approximation as “dense”. For MaxSE, it is computationally infeasible to compute the exact optimal value for large matrix sizes. Therefore, we rely on the lower bound derived in Theorem 2, which we denote on the plots as “lower bound”. We observe that our learning-rate-aware factorization outperforms the others in terms of MaxSE. However, for the proposed values of  $n$  and  $\beta$ , it performs worse than the prefix sum based factorization in terms of MeanSE. To further investigate this, we plot the colormap of the gain over the prefix sum based approach (see Figure 1). In the blue regions, our method performs worse, while in the red regions it performs better. As can be seen, for any fixed  $n$ , sufficiently small values of  $\beta$  lead to the learning-rate-aware factorization outperforming the prefix sum based approach, thereby numerically validating our theoretical findings.

#### 4.1 MULTI-PARTICIPATION

Following the line of work on multi-participation matrix factorization (Choquette-Choo et al., 2023b;a; Kalinin & Lampert, 2024; McKenna, 2025; Kalinin et al., 2025), we allow each user or datapoint to participate multiple times. Without imposing any restriction on the participation pattern, the guarantees would be no stronger than those obtained via the privacy composition. To overcome this, we adopt the notion of *b-min separation*, which requires that the gap between any two consecutive participations of the same user be at least  $b > 0$ . Under this condition, each user may participate up to  $k = \lceil n/b \rceil$  times. This naturally affects the definition of sensitivity, which we refine as

$$\text{sens}_{k,b}(C) = \sup_{G \sim G'} \|CG - CG'\|_F, \quad (21)$$

where  $G$  and  $G'$  differ in the participations of a single user, with the corresponding rows separated by at least  $b$ . We then generalize the notion of MeanSE error to the multi-participation setting:

$$\mathcal{E}(B, C) = \frac{1}{\sqrt{n}} \|B\|_F \cdot \text{sens}_{k,b}(C). \quad (22)$$

In this section, we establish both upper and lower bounds on the optimal value  $\mathcal{E}(B, C)$  among all factorizations, for the learning-rate workload. This extends the results of Kalinin et al. (2025) on SGD with momentum and weight-decay workloads to the non-Toeplitz case. For the prefix-sum workload, it was shown that the **Banded Inverse Square Root (BISR)** factorization is asymptotically optimal in the multi-participation setting. The BISR is defined as follows: given a workload

matrix  $A$ , we compute the square root of its inverse,  $C = A^{-1/2}$ , band it to width  $p$  by nullifying all elements below the  $p$ -th diagonal and then invert the result. The corresponding correlation matrix is denoted  $C^p$ . Then there exists a unique matrix  $B^p$  such that  $B^p C^p = A$ . By using the BISR matrix corresponding to the prefix-sum workload  $A_1$ , we establish a general upper bound in the multi-participation setting for workloads with learning rates  $A_\chi$ .

**Theorem 3.** *Under the same assumptions on learning rate scheduling  $\chi_t$  as in Theorem 1, the following holds.*

$$\mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \sqrt{\frac{k}{n} \left( \log p + \frac{p}{b} \right) \sum_{m=1}^n \left[ \chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2 \right]} \right). \quad (23)$$

For exponential decay the upper bound (after optimizing over  $p$ ) has the following form:

**Corollary 3.** *Let  $\chi_t = \beta^{\frac{t-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then, in multi-participation with  $b$ -min-separation and at most  $k = \lceil \frac{n}{b} \rceil$  participations, we have for  $p^* \sim b \log b$  the following optimized upper bound:*

$$\mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \frac{\sqrt{k} \log n + k}{\sqrt{\log(1/\beta)}} \right). \quad (24)$$

We prove a general lower bound for multi-participation error with arbitrary learning rate scheduling.

**Theorem 4** (Lower bound for multi-participation). *Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi = \text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_t > 0$ . Assume any factorization  $A_\chi = B \times C$ . Then, in multi-participation with  $b$ -min-separation and at most  $k = \lceil \frac{n}{b} \rceil$  participations, we have*

$$\mathcal{E}(B, C) \geq \max \left\{ \max_{t \leq n} \frac{\sqrt{k} t \chi_t}{\pi \sqrt{2n}} (\min_{j \leq t} \chi_j) \log(t), \sum_{j=0}^{k-1} \chi_{1+jb} \left( 1 - \frac{j}{k-1} \right) \right\}. \quad (25)$$

For the exponential learning rate decay we can simplify the lower bound in the following Corollary.

**Corollary 4.** *Let  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then Theorem 4 yields*

$$\mathcal{E}(B, C) = \Omega \left( \frac{\sqrt{k}}{\log(1/\beta)} \log \frac{n}{\log(1/\beta)} + \frac{k}{\log(1/\beta)} \right). \quad (26)$$

For the numerical comparison in the multi-participation we study several recently proposed memory-efficient factorizations. Including banded matrix factorization McKenna (2025), banded inverse factorization BandInvMF and BISR (Kalinin et al., 2025) and Buffered Linear Toeplitz (BLT) (McMahan et al., 2024). We can optimize banded and banded inverse matrices, accounting for the learning rate decay, as well as like if it was a prefix-sum workload with constant learning rate, we refer to this difference as “w/ LRS” and “w/o LRS”. See the plots in the Figure 2 for the exponential decay, and Figure 5 in the Appendix for other learning rate schedulers.

## 5 EXPERIMENTS

We demonstrate the practical benefits of learning rate scheduling in Figure 3 on CIFAR-10 dataset. All experiments satisfy  $(9, 10^{-5})$ -DP and use a 3-block CNN trained for 10 epochs with batch size 128 and clipping norm 1. For privacy accounting, we use Poisson subsampling with PLD accounting (Koskela et al., 2021) for DP-SGD and amplification by ball-and-bins subsampling with MCMC accounting (Choquette-Choo et al., 2025) for all factorizations. Subfigure (a) shows validation accuracy across different initial learning rates, where exponential learning rate scheduling improves performance compared to DP-SGD with a fixed learning rate ( $\beta = 1$ ). Subfigure (b) reports test accuracy using the best learning rate chosen on the validation set. All factorizations benefit substantially from scheduling, and the learning-rate-aware factorization (denoted as BISR w/ LRS) achieves even further improvements. However, optimizing the factorization with respect to learning rate workload does not lead to additional gains: while RMSE can serve as a proxy for performance,

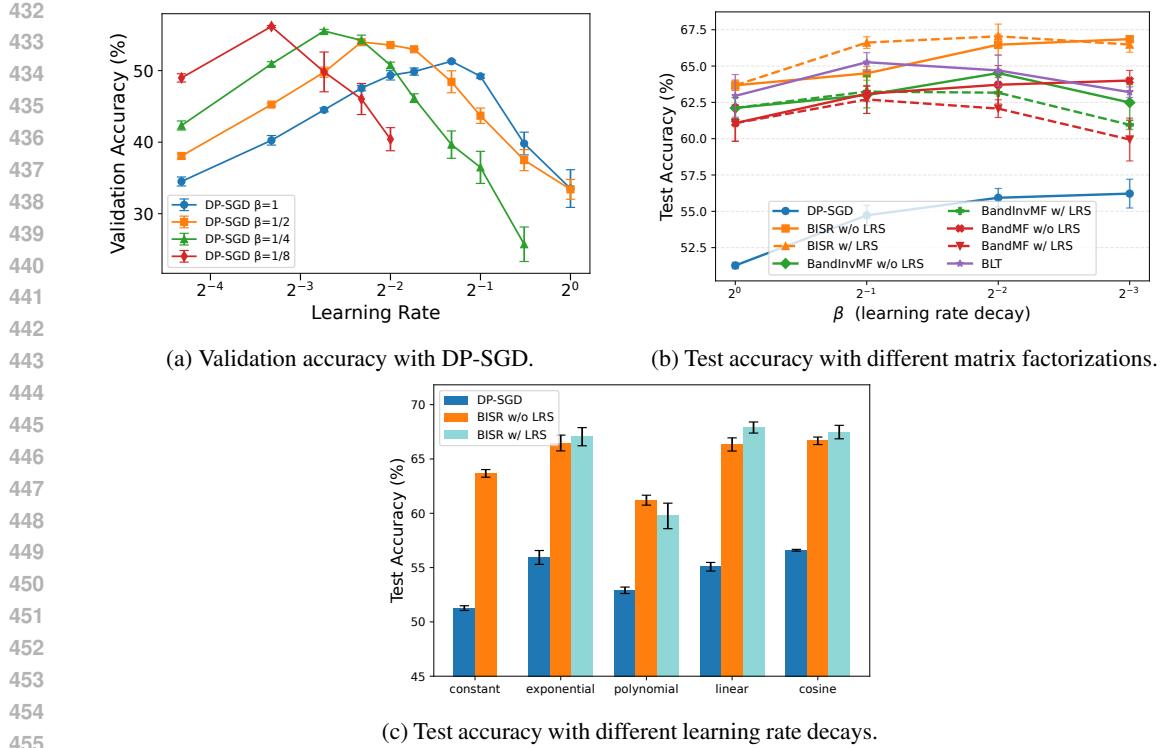


Figure 3: **CIFAR-10** results under  $(9, 10^{-5})$ -differential privacy. (a) Validation accuracy with **exponential learning rate scheduling** for different learning rates in DP-SGD. We report the points corresponding to the lowest learning rate; for example, a learning rate of  $1/2$  for  $\beta = 1/4$  indicates that training starts with a learning rate of  $2$  and decays to  $1/2$ . (b) Test accuracy across different matrix factorizations with **exponential learning rate scheduling**. Training hyperparameters are provided in Table 3. (c) Test accuracy for different learning rate decays. Training hyperparameters are provided in Table 4.

it does not perfectly predict it. In practice, workload optimization increases the added noise per iteration, and this effect is not fully compensated during training due to the non-linearity introduced by large noise.

In Subfigure (c), we compare different learning rate schedulers with a constant one. We observed that learning rate scheduling improves accuracy for DP-SGD for all types. For BISR, we found that polynomial learning rate decay with  $\gamma = 2$  deteriorates the quality and is perhaps not a good choice for the scheduler. The other schedulers substantially improve the accuracy of BISR. Moreover, our proposed learning-rate-aware factorization (BISR w/ LRS) further improves the quality, with the largest improvement for linear LRS, making it a suitable factorization for high-performance private training.

## 6 CONCLUSION AND FUTURE DIRECTIONS

Learning rate scheduling has been shown to improve convergence in both private and non-private machine learning. In this work, we combine learning rate scheduling with matrix factorization and propose a learning-rate-aware factorization, which in the case of exponential learning rate decay is theoretically shown to improve the error. Through numerical experiments using the MaxSE and MeanSE metrics, as well as CIFAR-10 model training, we demonstrate its benefits.

We have primarily studied learning rate decay, but similar techniques can be applied to warm-starting, where the learning rate is initially small and then gradually increased. Optimization-based approaches for matrix factorization are generally agnostic to the choice of learning rate scheduling, but adapting our learning-rate-aware factorization to this setting may pose extra challenges.

486 REFERENCES  
487

488 Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and  
489 Li Zhang. Deep learning with differential privacy. In *Conference on Computer and Communica-*  
490 *tions Security (CCS)*, 2016.

491 Joel Daniel Andersson and Rasmus Pagh. Streaming private continual counting via binning. In  
492 *Conference on Secure and Trustworthy Machine Learning (SaTML)*, 2025.

493

494 Borja Balle and Yu-Xiang Wang. Improving the Gaussian mechanism for differential privacy: An-  
495 alytical calibration and optimal denoising. In *International Conference on Machine Learning*  
496 (*ICML*), 2018.

497 Borja Balle, Leonard Berrada, Zachary Charles, Christopher A Choquette-Choo, Soham De,  
498 Vadym Doroshenko, Dj Dvijotham, Andrew Galen, Arun Ganesh, Sahra Ghalebikesabi, Jamie  
499 Hayes, Peter Kairouz, Ryan McKenna, Brendan McMahan, Aneesh Pappu, Natalia Pono-  
500 mareva, Mikhail Pravilov, Keith Rush, Samuel L Smith, and Robert Stanforth. JAX-Privacy:  
501 Algorithms for privacy-preserving machine learning in JAX, 2025. [http://github.com/google-  
502 deepmind/jax\\_privacy](http://github.com/google-<br/>502 deepmind/jax_privacy).

503 Christopher A Choquette-Choo, Arun Ganesh, Ryan McKenna, H Brendan McMahan, John Rush,  
504 Abhradeep Guha Thakurta, and Zheng Xu. (amplified) banded matrix factorization: A unified  
505 approach to private training. In *Conference on Neural Information Processing Systems (NeurIPS)*,  
506 2023a.

507

508 Christopher A. Choquette-Choo, Hugh Brendan McMahan, J. Keith Rush, and Abhradeep Guha  
509 Thakurta. Multi epoch matrix factorization mechanisms for private machine learning. In *Inter-  
510 national Conference on Machine Learning (ICML)*, 2023b.

511 Christopher A Choquette-Choo, Arun Ganesh, Saminul Haque, Thomas Steinke, and Abhradeep  
512 Thakurta. Near exact privacy amplification for matrix mechanisms. In *International Conference  
513 on Learning Representations (ICLR)*, 2025.

514

515 Sergey Denisov, H Brendan McMahan, John Rush, Adam Smith, and Abhradeep Guha Thakurta.  
516 Improved differential privacy for SGD via optimal private linear operators on adaptive streams.  
517 In *Conference on Neural Information Processing Systems (NeurIPS)*, 2022.

518 Krishnamurthy Dj Dvijotham, H Brendan McMahan, Krishna Pillutla, Thomas Steinke, and  
519 Abhradeep Thakurta. Efficient and near-optimal noise generation for streaming differential pri-  
520 vacy. In *Symposium on Foundations of Computer Science (FOCS)*, 2024.

521

522 Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity  
523 in private data analysis. *Journal of Privacy and Confidentiality*, 2006.

524 Hendrik Fichtenberger, Monika Henzinger, and Jalaj Upadhyay. Constant matters: Fine-grained er-  
525 ror bound on differentially private continual observation. In *International Conference on Machine  
526 Learning (ICML)*, 2023.

527

528 Priya Goyal, Piotr Dollár, Ross Girshick, Pieter Noordhuis, Lukasz Wesolowski, Aapo Kyrola, An-  
529 drew Tulloch, Yangqing Jia, and Kaiming He. Accurate, large minibatch sgd: Training imagenet  
530 in 1 hour, 2017. arXiv:1706.02677.

531 Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recog-  
532 nition. In *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

533

534 M. Henzinger, J. Upadhyay, and S. Upadhyay. A unifying framework for differentially private sums  
535 under continual observation. In *Symposium on Discrete Algorithms (SODA)*, 2024.

536

537 Monika Henzinger and Jalaj Upadhyay. Improved differentially private continual observation using  
538 group algebra. In *Symposium on Discrete Algorithms (SODA)*, 2025.

539 Monika Henzinger, Jalaj Upadhyay, and Sarvagya Upadhyay. Almost tight error bounds on differ-  
540 entially private continual counting. In *Symposium on Discrete Algorithms (SODA)*, 2023.

540 Monika Henzinger, Nikita P. Kalinin, and Jalaj Upadhyay. Normalized square root: Sharper  
 541 matrix factorization bounds for differentially private continual counting, 2025. arXiv preprint  
 542 arXiv:2509.14334.

543

544 Nikita P Kalinin and Christoph Lampert. Banded square root matrix factorization for differentially  
 545 private model training. In *Conference on Neural Information Processing Systems (NeurIPS)*,  
 546 2024.

547 Nikita P Kalinin, Ryan McKenna, Jalaj Upadhyay, and Christoph H Lampert. Back to square roots:  
 548 An optimal bound on the matrix factorization error for multi-epoch differentially private SGD,  
 549 2025. arXiv preprint arXiv:2505.12128.

550

551 Antti Koskela, Joonas Jälkö, Lukas Prediger, and Antti Honkela. Tight differential privacy for  
 552 discrete-valued mechanisms and for the subsampled Gaussian mechanism using FFT. In *Confer-  
 553 ence on Uncertainty in Artificial Intelligence (AISTATS)*, 2021.

554 Alexey Kurakin, Shuang Song, Steve Chien, Roxana Geambasu, Andreas Terzis, and Abhradeep  
 555 Thakurta. Toward training at imagenet scale with differential privacy. *arXiv preprint*  
 556 arXiv:2201.12328, 2022.

557

558 Ilya Loshchilov and Frank Hutter. SGDR: Stochastic gradient descent with warm restarts. In *Inter-  
 559 national Conference on Learning Representations (ICLR)*, 2017.

560

561 Zelun Luo, Daniel J Wu, Ehsan Adeli, and Li Fei-Fei. Scalable differential privacy with sparse  
 562 network finetuning. In *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021.

563

564 Jiří Matoušek, Aleksandar Nikolov, and Kunal Talwar. Factorization norms and hereditary discrep-  
 565 ancy. *International Mathematics Research Notices*, 2020.

566

567 Ryan McKenna. Scaling up the banded matrix factorization mechanism for differentially private  
 568 ML. In *International Conference on Learning Representations (ICLR)*, 2025.

569

570 Hugh Brendan McMahan, Zheng Xu, and Yanxiang Zhang. A hassle-free algorithm for strong  
 571 differential privacy in federated learning systems. In *Conference on Empirical Methods in Natural  
 572 Language Processing (EMNLP)*, 2024.

573

574 Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor  
 575 Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-  
 576 performance deep learning library. In *Conference on Neural Information Processing Systems  
 577 (NeurIPS)*, 2019.

578

579 Leslie N Smith. Cyclical learning rates for training neural networks. In *Winter Conference on  
 580 Applications of Computer Vision (WACV)*, 2017.

581

582 VaultGemma Team. VaultGemma: the world's most capable differentially pri-  
 583 vate LLM, september 2025. URL [https://research.google/blog/  
 584 vaultgemma-the-worlds-most-capable-differentially-private-llm/](https://research.google/blog/vaultgemma-the-worlds-most-capable-differentially-private-llm/).  
 585 Google Research Blog.

586

587 Zheng Xu and Yanxiang Zhang. Advances in private training for production on-device language  
 588 models, 2024. Google Research Blog.

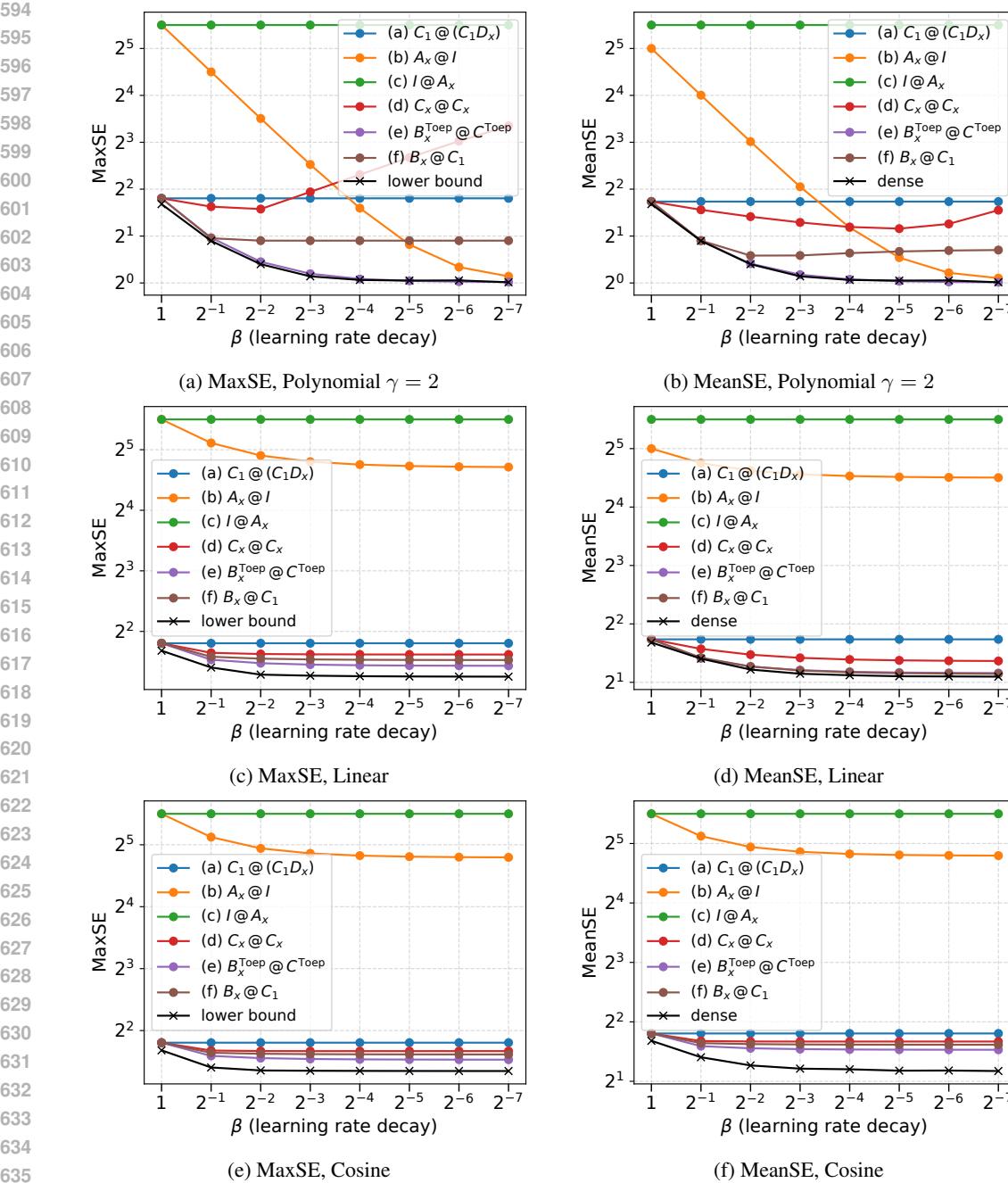
589

590

591

592

593

Figure 4: Comparison of different LR schedulers ( $n = 2048$ ) in single participation.

## A ADDITIONAL EXPERIMENTS

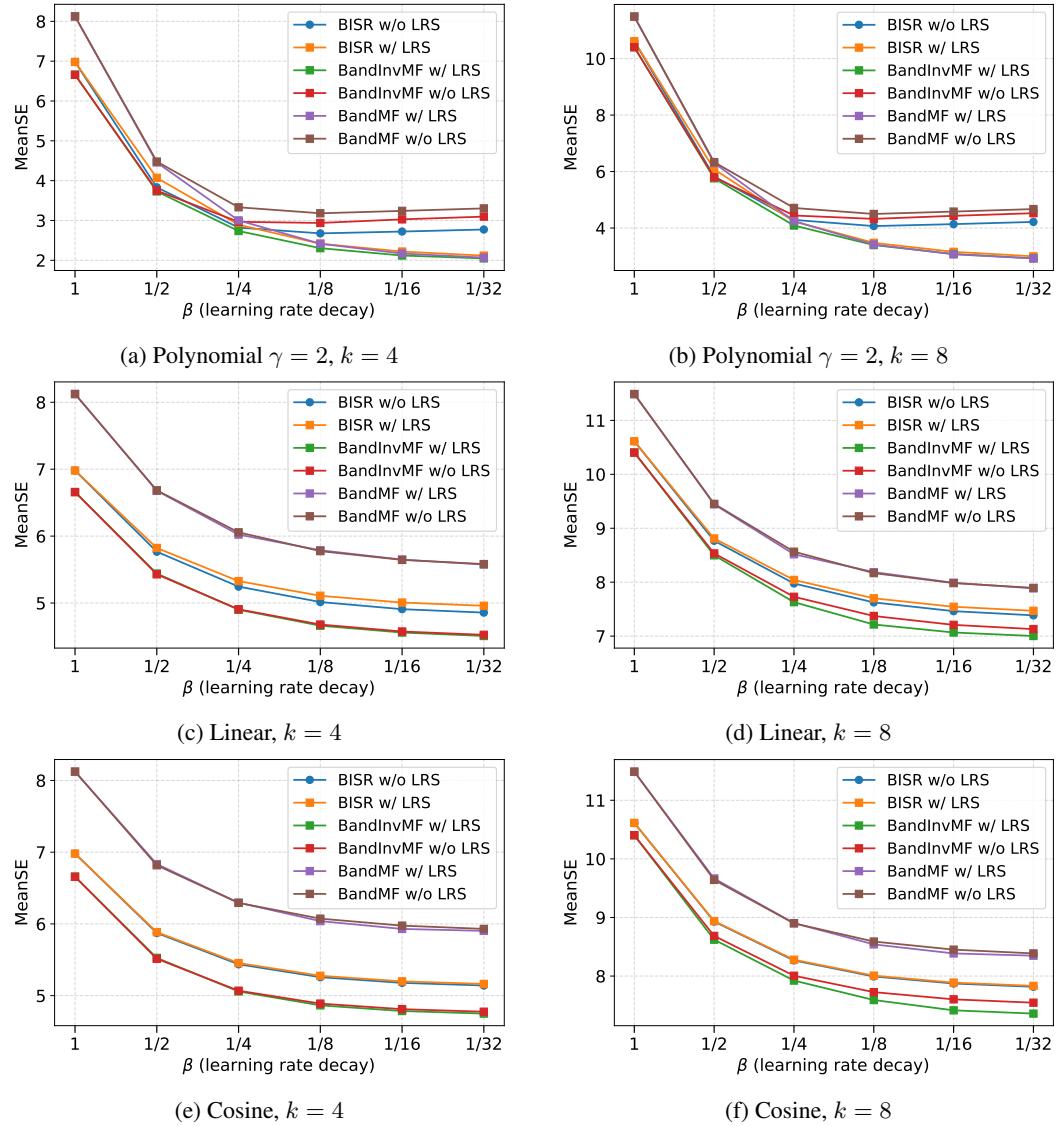


Figure 5: Multi-participation MeanSE error under different learning-rate schedulers (Polynomial  $\gamma = 2$ , Linear, Cosine) for  $k = 4$  and  $k = 8$ . Matrix size  $n = 1024$ , bandwidth  $p = 64$ .

702  
 703  
 704  
 705  
 706  
 707  
 708 Table 3: We train four different methods for matrix optimization: DP-SGD, BISR, BandInvMF, and  
 709 BandMF. Each factorization method can be computed either with a workload induced by learning  
 710 rate scheduling (w/ LRS) or with a constant workload corresponding to prefix sums (w/o LRS). All  
 711 experiments use clipping norm  $\zeta = 1$  and batch size 128. For each method, the noise multiplier  $\sigma$   
 712 is computed using a privacy accountant: Poisson accounting for DP-SGD and bins-and-balls sam-  
 713 pling with an MCMC accountant Choquette-Choo et al. (2025) for the matrix factorization methods.  
 714 Learning rates  $\eta$  are tuned on a validation set separately for each method and decay setting.

Method	$\zeta$	BS	$p$	$\beta = 1$		$\beta = \frac{1}{2}$		$\beta = \frac{1}{4}$		$\beta = \frac{1}{8}$	
				$\eta$	$\sigma$	$\eta$	$\sigma$	$\eta$	$\sigma$	$\eta$	$\sigma$
DP-SGD	1	128	1	0.4	0.479	0.4	0.479	0.6	0.479	0.8	0.479
BISR (w/o LRS)	1	128	64	0.8	1.910	1.6	1.910	1.8	1.910	1.8	1.910
BISR (w/ LRS)	1	128	64	0.8	1.908	1.6	1.901	1.9	1.894	2.0	1.888
BandInvMF (w/o LRS)	1	128	64	1.0	2.597	1.5	2.597	1.6	2.597	1.7	2.597
BandInvMF (w/ LRS)	1	128	64	1.0	2.597	1.5	2.681	1.6	2.814	1.6	2.870
BandMF (w/o LRS)	1	128	64	0.9	2.921	1.5	2.921	1.6	2.921	1.7	2.921
BandMF (w/ LRS)	1	128	64	0.9	2.921	1.1	3.053	1.6	3.158	1.7	3.222
BLT	1	128	64	0.9	2.580	1.3	2.580	1.4	2.580	1.8	2.580

727  
 728  
 729  
 730  
 731  
 732  
 733  
 734  
 735  
 736  
 737  
 738 Table 4: Comparison of different learning rate schedulers for training with matrix factorization with  
 739 fixed learning rate decay  $\beta = \frac{1}{4}$ . We evaluate DP-SGD, BISR (w/o LRS), and BISR (w/ LRS) under  
 740 four learning rate decay strategies: exponential, polynomial, linear, and cosine. All experiments use  
 741 clipping norm  $\zeta = 1$  and batch size 128, for BISR we use bandwidth  $p = 64$ . Noise multipliers  $\sigma$  are  
 742 computed using Poisson accounting for DP-SGD and bins-and-balls MCMC accounting Choquette-  
 743 Choo et al. (2025) for BISR. Learning rates  $\eta$  are tuned on a validation set for each decay setting.

Method	$\zeta$	BS	$p$	Exponential		Polynomial		Linear		Cosine	
				$\eta$	$\sigma$	$\eta$	$\sigma$	$\eta$	$\sigma$	$\eta$	$\sigma$
DP-SGD	1	128	1	0.6	0.479	1.1	0.479	0.6	0.479	0.5	0.479
BISR (w/o LRS)	1	128	64	1.8	1.910	1.8	1.910	1.6	1.910	1.5	1.910
BISR (w/ LRS)	1	128	64	1.9	1.894	1.8	1.366	1.6	1.900	1.4	1.907

756 **B SINGLE-PARTICIPATION: SQUARE ROOT OF THE WORKLOAD**  
 757

758 As one of the baseline factorizations we propose the square root factorization  
 759

760 
$$761 A_\chi = A_\chi^{1/2} \times A_\chi^{1/2}, \quad \text{where} \quad A_\chi = \begin{pmatrix} 762 \chi_1 & 0 & 0 & \cdots & 0 \\ 763 \chi_1 & \chi_2 & 0 & \cdots & 0 \\ 764 \chi_1 & \chi_2 & \chi_3 & \cdots & 0 \\ 765 \vdots & \vdots & \vdots & \ddots & \vdots \\ 766 \chi_1 & \chi_2 & \chi_3 & \cdots & \chi_n \end{pmatrix} \quad (27)$$

767 In the case of exponential learning rate decay we can compute the matrix square root explicitly and  
 768 tightly bound its values from below.

769 **Theorem 5.** *For any  $n \geq 1$  and  $\alpha \in (0, 1)$ , with learning rates  $\chi_i = \alpha^{i-1}$  the following lower  
 770 bound holds:*

771 
$$(A_\chi^{1/2})_{m,l} = \alpha^{(l-1)/2} \prod_{k=1}^{m-l} \frac{1 - \alpha^{k-1/2}}{1 - \alpha^k} \geq \alpha^{(l-1)/2} \max \left\{ \left| \binom{-1/2}{n} \right|, \frac{\sqrt{1 - \alpha^2}}{\Gamma_{\alpha^2}(1/2)} \right\}, \quad (28)$$

772 where  $\Gamma_q(x)$  denotes the  $q$ -Gamma function, and  $\lim_{\alpha \rightarrow 1^-} \Gamma_{\alpha^2}(1/2) = \Gamma(1/2) = \sqrt{\pi}$ .

773 We can also compute the inverse of this matrix (see Appendix, Lemma 5). Using the lower bound,  
 774 we now establish the following bounds for the MaxSE and MeanSE errors under an exponentially  
 775 decaying learning rate.

776 **Corollary 5.** *Let  $\beta \in (0, 1/e)$  and  $\alpha = \beta^{1/(n-1)}$ . For the square-root factorization  $A_\chi =$   
 777  $A_\chi^{1/2} A_\chi^{1/2}$ , we have*

778 
$$\text{MaxSE}(A_\chi^{1/2}, A_\chi^{1/2}) = \Omega \left( \sqrt{\log n} \sqrt{\log \frac{n}{\log(1/\beta)}} \right), \quad (29)$$

779 
$$\text{MeanSE}(A_\chi^{1/2}, A_\chi^{1/2}) = \Omega \left( \frac{\log n}{\sqrt{\log(1/\beta)}} \right). \quad (30)$$

780 We prove these statements next, beginning with necessary lemmas.

781 **Lemma 3.** *For a specific choice of the learning rate coefficients  $\chi_i = \alpha^{2i}$  with  $\alpha \in (0, 1)$ , we have:*

782 
$$(A_\chi^{1/2})_{m,l} = \alpha^l \prod_{k=1}^{m-l} \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} \quad (31)$$

783 *Proof.* To prove that the coefficients of the square root have the proposed form, we need to show  
 784 that the square of this matrix is equal to the original one. That is, for all  $1 \leq l \leq m \leq n$ , we show  
 785 that:

786 
$$\sum_{j=l}^m \alpha^j \prod_{k=1}^{m-j} \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} \cdot \alpha^l \prod_{k=1}^{j-l} \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} = \alpha^{2l} \quad (32)$$

787 or equivalently,

788 
$$\sum_{j=0}^{m-l} \alpha^j \prod_{k=1}^{m-l-j} \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} \prod_{k=1}^j \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} = 1, \quad (33)$$

789 which is a convolution of the sequences  $a_j$  and  $a_j \alpha^j$ , where

790 
$$a_j = \prod_{k=1}^j \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} = \frac{(\alpha; \alpha^2)_j}{(\alpha^2; \alpha^2)_j}, \quad (34)$$

810 and  $(a; q)_n$  denotes the  $q$ -Pochhammer symbol, given by  $\prod_{k=0}^{n-1} (1 - aq^k)$ . We will prove the identity  
 811 using generating functions. First, we find the generating function of  $a_j$ :  
 812

$$813 \quad 814 \quad 815 \quad f(x) = \sum_{j=0}^{\infty} a_j x^j = \sum_{j=0}^{\infty} \frac{(\alpha; \alpha^2)_j}{(\alpha^2; \alpha^2)_j} x^j = \frac{(\alpha x; \alpha^2)_{\infty}}{(x; \alpha^2)_{\infty}}, \quad (35)$$

816 where the last equality follows from the  $q$ -binomial theorem. Therefore, the generating function of  
 817 the convolution of  $a_j$  and  $a_j \alpha^j$  is:  
 818

$$820 \quad 821 \quad 822 \quad f(x)f(\alpha x) = \frac{(\alpha x; \alpha^2)_{\infty}}{(x; \alpha^2)_{\infty}} \cdot \frac{(\alpha^2 x; \alpha^2)_{\infty}}{(\alpha x; \alpha^2)_{\infty}} = \frac{(\alpha^2 x; \alpha^2)_{\infty}}{(x; \alpha^2)_{\infty}} = \prod_{n=0}^{\infty} \frac{1 - x\alpha^{2n+2}}{1 - x\alpha^{2n}} = \frac{1}{1 - x}, \quad (36)$$

823 as the product telescopes, yielding the generating function of the unit sequence  $(1, 1, 1, \dots)$ , thus  
 824 concluding the proof.  $\square$

825 **Lemma 4.** *For any  $n \geq 1$  and  $\alpha \in (0, 1)$ , the following lower bound holds:*

$$827 \quad 828 \quad 829 \quad \prod_{k=1}^n \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} \geq \max \left\{ \left| \binom{-1/2}{n} \right|, \frac{\sqrt{1 - \alpha^2}}{\Gamma_{\alpha^2}(1/2)} \right\}, \quad (37)$$

830 where  $\Gamma_q(x)$  denotes the  $q$ -Gamma function, and  $\lim_{\alpha \rightarrow 1^-} \Gamma_{\alpha^2}(1/2) = \Gamma(1/2) = \sqrt{\pi}$ .  
 831

832 *Proof.* First, we show that  $f_n(\alpha) = \prod_{k=1}^n \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}}$  is a decreasing function of  $\alpha$ . Therefore,  
 833

$$834 \quad 835 \quad 836 \quad f_n(\alpha) \geq f_n(1) = \prod_{k=1}^n \frac{2k-1}{2k} = \left| \binom{-1/2}{n} \right|. \quad (38)$$

837 To prove this, we observe that each individual term is a decreasing function of  $\alpha$ :  
 838

$$839 \quad \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} = 1 - \frac{\alpha^{2k-1} - \alpha^{2k}}{1 - \alpha^{2k}} = 1 - \frac{\alpha^{-1} - 1}{\alpha^{-2k} - 1} = 1 - \frac{1}{1 + \alpha^{-1} + \dots + \alpha^{-(2k-1)}}. \quad (39)$$

841 For the second part of the inequality, we show that  
 842

$$843 \quad 844 \quad 845 \quad f_n(\alpha) \geq f_{\infty}(\alpha) = \prod_{k=1}^{\infty} \frac{1 - \alpha^{2k-1}}{1 - \alpha^{2k}} = \frac{(\alpha; \alpha^2)_{\infty}}{(\alpha^2; \alpha^2)_{\infty}} = \frac{\sqrt{1 - \alpha^2}}{\Gamma_{\alpha^2}(1/2)}, \quad (40)$$

846 where the inequality holds because each term of the product is less than 1, the infinite product  
 847 converges, and the  $q$ -Gamma function is defined by

$$848 \quad 849 \quad 850 \quad \Gamma_q(x) = (1 - q)^{1-x} \frac{(q; q)_{\infty}}{(q^x; q)_{\infty}}. \quad (41)$$

851 This concludes the proof.  $\square$

853 *Proof of Theorem 5.* The proof follows from combining Lemma 3 for the equality and Lemma 4 for  
 854 the lower bound. For convenience, we considered  $\chi_i = \alpha^{2i}$  in those lemmas. To achieve  $\alpha^{i-1}$ , we  
 855 first divide the square root matrix by  $\alpha$  so that we start from learning rates of 1 rather than  $\alpha^2$ . Then,  
 856 we replace  $\alpha$  with  $\alpha^{1/2}$ , which concludes the proof.  $\square$

857 *Proof of Corollary 5.* To use Lemma 3 and Lemma 4, we need to adjust the choice of  $\alpha$ , as previous  
 858 lemmas consider  $\chi_k = \alpha^{2k}$  while here  $\chi_k = \alpha^{k-1}$ . This gives  
 859

$$860 \quad 861 \quad (A_{\chi}^{1/2})_{m,l} \geq \alpha^{(l-1)/2} r_{m-l}. \quad (42)$$

862 Thus the maximum column norm of  $A_{\chi}^{1/2}$  is at least the norm of its first column, which in turn is at  
 863 least the maximum column norm of  $A_1^{1/2}$ , the latter is  $\Theta(\log n)$ .

864 For the  $m$ -th row-sum of squares,

$$866 \quad \sum_{l=1}^m (A_\chi^{1/2})_{m,l}^2 \geq \sum_{l=1}^m \alpha^{l-1} r_{m-l}^2 \geq \frac{\alpha^m}{\pi} \sum_{l=1}^m \frac{1}{l \alpha^l} \geq \frac{\alpha^m}{\pi} \log m.$$

869 **MaxSE.** Taking the maximum over  $m$  and applying Lemma 10 yields

$$871 \quad \max_{1 \leq m \leq n} \sum_{l=1}^m (A_\chi^{1/2})_{m,l}^2 = \Omega\left(\log \frac{n}{\log(1/\beta)}\right),$$

873 so the maximum row norm is  $\Omega(\sqrt{\log \frac{n}{\log(1/\beta)}})$ . Multiplying by the maximum column norm  
874  $\Omega(\log n)$  gives the first bound.

876 **MeanSE.** Averaging over  $m$  and using Lemma 11,

$$878 \quad \frac{1}{n} \sum_{m=1}^n \sum_{l=1}^m (A_\chi^{1/2})_{m,l}^2 = \Theta\left(\frac{\log n}{\log(1/\beta)}\right),$$

881 so the average row norm is  $\Omega(\sqrt{\frac{\log n}{\log(1/\beta)}})$ . Multiplying by the maximum column norm  $\Omega(\log n)$   
882 gives the second bound.  $\square$

884 We also give the following lemma on the inverse of  $A_\chi^{1/2}$ .

885 **Lemma 5.** *The inverse matrix  $A_\chi^{-1/2}$  for a specific choice of the learning rate coefficients  $\chi_i = \alpha^{2i}$  with  $\alpha \in (0, 1)$  has the following form:*

$$888 \quad (A_\chi^{-1/2})_{m,l} = \frac{-(1-\alpha)}{\alpha^{l+1}(1-\alpha^{2(m-l)-1})} \prod_{k=1}^{m-l} \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}}. \quad (43)$$

892 *Proof.* To prove that  $A_\chi^{-1/2}$  corresponds to the inverse square root matrix, we will show that its  
893 product with the square root matrix  $A_\chi^{1/2}$  yields the identity matrix:

$$896 \quad \sum_{j=l}^m (A_\chi^{1/2})_{m,j} (A_\chi^{-1/2})_{j,l} = \sum_{j=l}^m \alpha^j \left[ \prod_{k=1}^{m-j} \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} \right] \cdot \frac{\alpha-1}{\alpha^{l+1}(1-\alpha^{2(j-l)-1})} \left[ \prod_{k=1}^{j-l} \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} \right] = \mathbb{1}_{l=m}. \quad (44)$$

900 This is equivalent to proving the following identity:

$$902 \quad \sum_{j=0}^{m-l} \alpha^j \left[ \prod_{k=1}^{m-l-j} \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} \right] \cdot \frac{\alpha-1}{\alpha(1-\alpha^{2j-1})} \left[ \prod_{k=1}^j \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} \right] = \mathbb{1}_{l=m}. \quad (45)$$

906 This can be interpreted as a convolution of two sequences  $a_j$  and  $\alpha^j b_j$ , defined as follows:

$$908 \quad a_j = \prod_{k=1}^j \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} = \frac{(\alpha; \alpha^2)_j}{(\alpha^2; \alpha^2)_j}, \quad b_j = \frac{\alpha-1}{\alpha(1-\alpha^{2j-1})} \prod_{k=1}^j \frac{1-\alpha^{2k-1}}{1-\alpha^{2k}} = \frac{(1/\alpha; \alpha^2)_j}{(\alpha^2; \alpha^2)_j}, \quad (46)$$

912 where  $(a; q)_n$  denotes the  $q$ -Pochhammer symbol, given by  $\prod_{k=0}^{n-1} (1 - aq^k)$ .

913 Analogously to Lemma 3, we will prove the identity via generating functions. Since the generating  
914 function  $f(x)$  of  $a_j$  is already known, it remains to find the generating function of  $b_j$ :

$$916 \quad g(x) = \sum_{j=0}^{\infty} x^j b_j = \sum_{j=0}^{\infty} x^j \frac{(1/\alpha; \alpha^2)_j}{(\alpha^2; \alpha^2)_j} = \frac{(x/\alpha; \alpha^2)_{\infty}}{(x; \alpha^2)_{\infty}}. \quad (47)$$

918 Therefore, the generating function of the convolution of  $a_j$  and  $\alpha^j b_j$  is given by the product of the  
 919 generating functions  $f(x)$  and  $g(\alpha x)$ , resulting in:  
 920

$$921 \quad 922 \quad 923 \quad f(x)g(\alpha x) = \frac{(ax; \alpha^2)_\infty}{(x; \alpha^2)_\infty} \cdot \frac{(x; \alpha^2)_\infty}{(\alpha x; \alpha^2)_\infty} = 1, \quad (48)$$

924 which concludes the proof.  $\square$

## 925 C SINGLE PARTICIPATION: NAIVE FACTORIZATIONS

### 928 Lemma 6.

$$929 \quad 930 \quad (a) \text{MaxSE}(A_1^{1/2}, A_1^{1/2}D) = \Theta(\log n) \quad \text{MeanSE}(A_1^{1/2}, A_1^{1/2}D) = \Theta(\log n) \\ 931 \quad (b) \text{MaxSE}(A_\chi, I) = \Theta\left(\sqrt{\frac{n}{\log 1/\beta}}\right) \quad \text{MeanSE}(A_\chi, I) = \Theta\left(\sqrt{\frac{n}{\log 1/\beta}}\right) \\ 932 \quad (c) \text{MaxSE}(I, A_\chi) = \Theta(\log n) \quad \text{MeanSE}(I, A_\chi) = \Theta(\log n)$$

934 *Proof.* (a) Since  $\chi_1 = 1$  and all other  $\chi_t \leq 1$ , the maximum column norm is still achieved in the  
 935 first column and is exactly the same as that of  $A_1^{1/2}$ . Thus,  
 936

$$937 \quad \text{MaxSE}(A_1^{1/2}, A_1^{1/2}D) = \text{MaxSE}(A_1^{1/2}, A_1^{1/2}) = \Theta(\log n), \\ 938 \quad \text{MeanSE}(A_1^{1/2}, A_1^{1/2}D) = \text{MeanSE}(A_1^{1/2}, A_1^{1/2}) = \Theta(\log n),$$

940 which follows from the analysis of the prefix-sum square root factorization by Henzinger et al.  
 941 (2024).

942 (b) The maximum column norm of  $I$  is 1. The maximum row norm of  $A_\chi$  is

$$944 \quad 945 \quad \sqrt{\sum_{k=1}^n \chi_k^2} = \sqrt{\sum_{k=0}^{n-1} \beta^{\frac{2k}{n-1}}} = \sqrt{\frac{1 - \beta^{\frac{2n}{n-1}}}{1 - \beta^{\frac{2}{n-1}}}} = \Theta\left(\sqrt{\frac{n}{\log(1/\beta)}}\right). \quad (49)$$

948 The normalized Frobenius norm  $\frac{1}{\sqrt{n}}\|A_\chi\|_F$  is

$$950 \quad 951 \quad \frac{1}{\sqrt{n}}\|A_\chi\|_F = \frac{1}{\sqrt{n}}\sqrt{\sum_{k=1}^n (n+1-k)\chi_k^2} = \frac{1}{\sqrt{n}}\sqrt{\sum_{k=1}^n (n+1-k)\beta^{\frac{2(k-1)}{n-1}}} \\ 952 \quad 953 \quad = \frac{1}{\sqrt{n}}\sqrt{\sum_{k=0}^{n-1} (n-k)\beta^{\frac{2k}{n-1}}} = \sqrt{\frac{\alpha^{2(n+1)} - \alpha^2(n+1) + n}{n(1 - \alpha^2)^2}},$$

957 where  $\alpha = \beta^{\frac{1}{n-1}}$ . Hence  $1 - \alpha^2 \sim \frac{2\log(1/\beta)}{n}$  and  $\alpha^{2n} \sim \beta^2$ , which results in

$$959 \quad 960 \quad \text{MeanSE}(A_\chi, I) = \frac{1}{\sqrt{n}}\|A_\chi\|_F = \Theta\left(\sqrt{\frac{1}{1-\alpha^2}}\right) = \Theta\left(\sqrt{\frac{n}{\log(1/\beta)}}\right).$$

961 (c) The maximum row norm of  $I$  is 1, as is its normalized Frobenius norm. The maximum column  
 962 norm of  $A_\chi$  is attained in the first column and is exactly  $\sqrt{n}$ , which concludes the proof.  $\square$

## 964 D SINGLE-PARTICIPATION: LEARNING-RATE-AWARE TOEPLITZ 965 SQUARE-ROOT

968 **Lemma 2.** Let  $\beta \in (0, 1/e)$  and  $\alpha = \beta^{1/(n-1)}$ . For the factorization  $A_\chi = B_\alpha \times C_\alpha$ ,

$$969 \quad 970 \quad \text{MaxSE}(B_\alpha, C_\alpha) = \mathcal{O}\left(\log \frac{n}{\log(1/\beta)}\right), \quad (19)$$

$$971 \quad \text{MeanSE}(B_\alpha, C_\alpha) = \mathcal{O}\left(\sqrt{\frac{\log n}{\log(1/\beta)}} \sqrt{\log \frac{n}{\log(1/\beta)}}\right). \quad (20)$$

972 *Proof.* For the exponential learning rate  $\chi_k = \beta^{\frac{k-1}{n-1}} = \alpha^{k-1}$ , consider the factorization  
 973  
 974

$$A_\chi = A_\chi C_\alpha^{-1} \times C_\alpha = B_\alpha \times C_\alpha,$$

975 with  
 976

$$C_\alpha = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha r_1 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1} r_{n-1} & \alpha^{n-2} r_{n-2} & \dots & 1 \end{pmatrix}, \quad C_\alpha^{-1} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha \tilde{r}_1 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1} \tilde{r}_{n-1} & \alpha^{n-2} \tilde{r}_{n-2} & \dots & 1 \end{pmatrix}, \quad (50)$$

981 where  $(r_k)$  and  $(\tilde{r}_k)$  are the coefficients of  $A_1^{1/2}$  and  $A_1^{-1/2}$ , respectively. By equation (18),  
 982  
 983

$$\|C_\alpha\|_{1 \rightarrow 2} = \mathcal{O}\left(\frac{1}{\alpha} \sqrt{\log \frac{1}{1-\alpha^2}}\right) = \mathcal{O}\left(\sqrt{\log \frac{n}{\log(1/\beta)}}\right). \quad (51)$$

984 The corresponding left matrix is  $B_\alpha$ , which can be computed as  
 985  
 986

$$(B_\alpha)_{m,l} = \alpha^l \sum_{t=0}^{m-l} \tilde{r}_t \alpha^{2t}.$$

987 Then, applying summation by parts:  
 988  
 989

$$(B_\alpha)_{m,l} = \alpha^{2m-l} r_{m-l} + \alpha^l (1-\alpha^2) \sum_{t=0}^{m-l-1} \alpha^{2t} r_t. \quad (52)$$

990 Using  $(a+b)^2 \leq 2a^2 + 2b^2$  and summing over  $l$ ,  
 991  
 992

$$\sum_{l=1}^m (B_\alpha)_{m,l}^2 \leq 2 \sum_{l=1}^m \alpha^{4m-2l} r_{m-l}^2 + 2(1-\alpha^2)^2 \sum_{l=1}^m \alpha^{2l} \left( \sum_{t=0}^{m-l-1} \alpha^{2t} r_t \right)^2. \quad (53)$$

993 *First term.* Since  $\sum_{u=0}^{m-1} r_u^2 \leq 1 + \frac{1}{\pi} + \frac{1}{\pi} \log(m-1)$ ,  
 994  
 995

$$2 \sum_{l=1}^m \alpha^{4m-2l} r_{m-l}^2 = 2\alpha^{2m} \sum_{u=0}^{m-1} \alpha^{2u} r_u^2 \leq \frac{2}{\pi} \alpha^{2m} \log m + \mathcal{O}(1). \quad (54)$$

996 *Second term.* With  $r_0 = 1$  and  $r_t \leq \frac{1}{\sqrt{\pi t}}$  for  $t \geq 1$ ,  
 997  
 998

$$\sum_{t=0}^{m-l-1} \alpha^{2t} r_t \leq 1 + \frac{1}{\sqrt{\pi}} \sum_{t=1}^{\infty} \frac{\alpha^{2t}}{\sqrt{t}}, \quad \sum_{l=1}^m \alpha^{2l} \leq \frac{\alpha^2}{1-\alpha^2},$$

1000 and  
 1001

$$\sum_{t=1}^{\infty} \frac{\alpha^{2t}}{\sqrt{t}} \leq \int_0^{\infty} \frac{e^{2x \log \alpha}}{\sqrt{x}} dx = \frac{\sqrt{\pi}}{\sqrt{2 \log(1/\alpha)}}. \quad (55)$$

1002 Hence  
 1003

$$2(1-\alpha^2)^2 \sum_{l=1}^m \alpha^{2l} \left( \sum_{t=0}^{m-l-1} \alpha^{2t} r_t \right)^2 \leq 2\alpha^2(1-\alpha^2) \left( 1 + \frac{1}{\sqrt{2 \log(1/\alpha)}} \right)^2 = \mathcal{O}(1). \quad (56)$$

1004 Combining (54)–(56),  
 1005  
 1006

$$\sum_{l=1}^m (B_\alpha)_{m,l}^2 \leq \frac{2}{\pi} \alpha^{2m} \log m + \mathcal{O}(1). \quad (57)$$

1007 **MaxSE.** From (57),  
 1008  
 1009

$$\|B_\alpha\|_{2 \rightarrow \infty}^2 = \max_m \sum_{l=1}^m (B_\alpha)_{m,l}^2 \leq \max_m \left( \frac{2}{\pi} \alpha^{2m} \log m + \mathcal{O}(1) \right) = \mathcal{O}\left(\log \frac{n}{\log(1/\beta)}\right)$$

1026 by Lemma 10 with  $\alpha \mapsto \alpha^2$ . Multiplying by  $\|C_\alpha\|_{1 \rightarrow 2} = \mathcal{O}\left(\frac{1}{\alpha}\sqrt{\log \frac{1}{1-\alpha^2}}\right)$  (Kalinin & Lampert, 1027 2024, Lemma 7) gives the stated bound.

1028 **MeanSE.** From (57),

$$1029 \frac{1}{n}\|B_\alpha\|_F^2 = \frac{1}{n} \sum_{m=1}^n \sum_{l=1}^m (B_\alpha)_{m,l}^2 \leq \frac{2}{\pi} \cdot \frac{1}{n} \sum_{m=1}^n \alpha^{2m} \log m + \mathcal{O}(1) = \mathcal{O}\left(\frac{\log n}{\log(1/\beta)}\right)$$

1030 by Lemma 11 with  $\alpha \mapsto \alpha^2$ . Thus  $\frac{1}{\sqrt{n}}\|B_\alpha\|_F = \mathcal{O}\left(\sqrt{\frac{\log n}{\log(1/\beta)}}\right)$ , and multiplying by  $\|C_\alpha\|_{1 \rightarrow 2}$  (as 1031 above) yields the claimed bound.  $\square$

## 1032 E SINGLE-PARTICIPATION: PREFIX-SUM FACTORIZATION

1033 **Lemma 7.** Let  $(\chi_t)_{t=1}^n$  be a positive sequence taken from  $[\beta, \infty)$  where  $\beta > 0$  is a constant, and

$$1034 Q = \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} |\chi_{l+t} - \chi_{l+t+1}| r_t \right)^2 = o(\log n).$$

1035 Then

$$1036 \text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\max_{m \in [n]} \chi_m^2 \log m}\right),$$

$$1037 \text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m}\right).$$

1038 *Proof.* We have that

$$1039 (B_\chi)_{m,l} = \chi_l + \sum_{t=1}^{m-l} \tilde{r}_t \chi_{t+l}$$

1040 where  $\tilde{r}_t = \frac{-r_t}{2t-1}$  are the coefficients of  $A_1^{-1/2}$ . Applying summation by parts (also known as Abel's 1041 transformation), we obtain:

$$1042 (B_\chi)_{m,l} = \chi_m \sum_{t=0}^{m-l} \tilde{r}_t - \sum_{t=0}^{m-l-1} (\chi_{l+t+1} - \chi_{l+t}) \sum_{j=0}^t \tilde{r}_j$$

$$1043 = \chi_m r_{m-l} + \sum_{t=0}^{m-l-1} (\chi_{l+t} - \chi_{l+t+1}) r_t. \quad (58)$$

1044 Defining  $\Delta_k = |\chi_k - \chi_{k+1}|$ , and using  $(a + b)^2 \leq 2a^2 + 2b^2$ , we get for its squared row sum:

$$1045 \sum_{l=1}^m (B_\chi)_{m,l}^2 \leq 2 \sum_{l=1}^m \chi_m^2 r_{m-l}^2 + 2 \underbrace{\sum_{l=1}^{m-1} \left( \sum_{t=0}^{m-l-1} \Delta_{l+t} r_t \right)^2}_{Q_m}$$

1046 Similarly, using the inequality  $(a + b)^2 \geq \frac{1}{2}a^2 - b^2$ :

$$1047 \sum_{l=1}^m (B_\chi)_{m,l}^2 \geq \frac{1}{2} \chi_m^2 \sum_{l=1}^m r_{m-l}^2 - Q_m$$

1048 Using the bounds  $\frac{1}{\sqrt{\pi(t+1)}} \leq r_t \leq \frac{1}{\sqrt{\pi t}}$ , we arrive at

$$1049 \frac{1}{2\pi} \chi_m^2 \log m + \mathcal{O}(1) - Q_m \leq \sum_{l=1}^m (B_\chi)_{m,l}^2 \leq \frac{2}{\pi} \chi_m^2 \log m + \mathcal{O}(1) + 2Q_m.$$

1080 As  $Q_m \leq Q$  (observe that  $Q_m$  is a truncated sum of positive summands), we can write  
 1081

$$1082 \sum_{l=1}^m (B_\chi)_{m,l}^2 = \Theta(\chi_m^2 \log m) \pm \mathcal{O}(Q). \\ 1083 \\ 1084$$

1085 For the requisite norms, we get:  
 1086

$$1087 \|B_\chi\|_{2 \rightarrow \infty}^2 = \max_{m \in [n]} \sum_{l=1}^m (B_\chi)_{m,l}^2 = \underbrace{\Theta\left(\max_{1 \leq m \leq n} \chi_m^2 \log m\right)}_{\Theta(\log n)} \pm \mathcal{O}(Q) = \Theta\left(\max_{1 \leq m \leq n} \chi_m^2 \log m\right) \\ 1088 \\ 1089 \\ 1090 \\ 1091 \frac{1}{n} \|B_\chi\|_F^2 = \frac{1}{n} \sum_{m=1}^n \sum_{l=1}^m (B_\chi)_{m,l}^2 = \underbrace{\Theta\left(\frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m\right)}_{\Theta(\log n)} \pm \mathcal{O}(Q) = \Theta\left(\frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m\right) \\ 1092 \\ 1093 \\ 1094$$

1095 as  $Q = o(\log n)$  by assumption. The final statement is derived from taking the square-root of the  
 1096 requisite norm and multiplying by  $\|A_1^{1/2}\|_{1 \rightarrow 2} = \Theta(\log n)$ .  $\square$   
 1097

1098 **Lemma 8.** Let  $(\chi_t)_{t=1}^n$  be a positive sequence. Fix  $n \geq 2$  and define  $(\Delta_t)_{t=1}^{n-1}$  via  
 1099

$$1100 \Delta_t = |\chi_t - \chi_{t+1}| \quad (\text{for all } 1 \leq t \leq n-1). \\ 1101$$

1102 Then

$$1103 Q = \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} |\chi_{l+t} - \chi_{l+t+1}| r_t \right)^2 = \mathcal{O}\left(n \sum_{k=1}^{n-1} \Delta_k^2\right). \\ 1104 \\ 1105 \\ 1106$$

1107 *Proof.* Define the two sequences  $(a_t)_{t \in \mathbb{Z}}, (b_t)_{t \in \mathbb{Z}}$  via  
 1108

$$1109 a_t = \begin{cases} \Delta_t & \text{for } 1 \leq t \leq n-1 \\ 0 & \text{otherwise} \end{cases} \quad b_t = \begin{cases} r_{-t} & \text{for } 2-n \leq t \leq 0 \\ 0 & \text{otherwise} \end{cases} \\ 1110 \\ 1111$$

1112 Note that  $a, b$  and  $a * b$  are all in  $\ell^p(\mathbb{Z})$  as they are zero-padded finite sequences, moreover  
 1113

$$1114 (a * b)_l = \sum_{t=-\infty}^{\infty} a_t b_{l-t} = \sum_{t=1}^{n-1} \Delta_t b_{l-t} = \sum_{t=l}^{n-1} \Delta_t r_{t-l} = \sum_{t=0}^{n-l-1} \Delta_{l+t} r_t. \\ 1115 \\ 1116$$

1117 We can thus write  
 1118

$$1119 Q \leq \sum_{l=-\infty}^{\infty} (a * b)_l^2 = \|a * b\|_2^2 \leq \|a\|_2^2 \cdot \|b\|_1^2 = \mathcal{O}\left(n \sum_{t=1}^{n-1} \Delta_t^2\right) \\ 1120 \\ 1121$$

1122 where the second inequality is Young's convolution inequality, and the last step uses  $\sum_{t=0}^{n-2} r_t =$   
 1123  $\mathcal{O}(\sqrt{n})$ .  $\square$   
 1124

1125 **Lemma 9.** Fix  $n \geq 2$ , and let  $(\chi_t)_{t=1}^n$  be a positive sequence satisfying  
 1126

$$1127 \Delta_k = |\chi_k - \chi_{k+1}| \leq \frac{C}{k(1 + \log k)} \\ 1128 \\ 1129$$

1130 for some absolute constant  $C > 0$ . Then  
 1131

$$1132 Q = \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} |\chi_{l+t} - \chi_{l+t+1}| r_t \right)^2 = \mathcal{O}(1). \\ 1133$$

1134 *Proof.* We consider the (coarse) upper bound  $r_t \leq \frac{1}{\sqrt{\pi t}} < \frac{1}{\sqrt{t+1}}$ , and start manipulating  $Q$ :  
 1135

$$\begin{aligned} 1136 \quad Q &= \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} \Delta_{l+t} r_t \right)^2 \leq \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} \frac{\Delta_{l+t}}{\sqrt{t+1}} \right)^2 = \sum_{l=1}^{n-1} \left( \sum_{t=l}^{n-1} \frac{\Delta_t}{\sqrt{t-l+1}} \right)^2 \\ 1137 \quad &= \sum_{l=1}^{n-1} \sum_{j=l}^{n-1} \sum_{k=l}^{n-1} \frac{\Delta_j \Delta_k}{\sqrt{j-l+1} \sqrt{k-l+1}} \\ 1138 \quad &= \sum_{j=1}^{n-1} \sum_{k=1}^{n-1} \Delta_j \Delta_k \sum_{l=1}^{\min\{j,k\}} \frac{1}{\sqrt{j-l+1} \sqrt{k-l+1}} = S \\ 1139 \quad & \\ 1140 \quad & \\ 1141 \quad & \\ 1142 \quad & \\ 1143 \quad & \\ 1144 \quad & \end{aligned}$$

1145 Our task is now reduced to showing that  $S = \mathcal{O}(1)$ . For  $1 \leq j \leq k$ , define  $H(j, k) = \sum_{r=1}^j \frac{1}{\sqrt{r} \sqrt{r+k-j}}$ . We can now write  
 1146

$$\begin{aligned} 1147 \quad S &= \sum_{k=1}^{n-1} \Delta_k^2 H(k, k) + 2 \sum_{k=1}^{n-1} \sum_{j < k} \Delta_j \Delta_k H(j, k) \\ 1148 \quad &= \underbrace{\sum_{k=1}^{n-1} \Delta_k^2 H(k, k)}_D + 2 \underbrace{\sum_{k=1}^{n-1} \sum_{j=1}^{\lceil k/2 \rceil} \Delta_j \Delta_k H(j, k)}_F + 2 \underbrace{\sum_{k=1}^{n-1} \sum_{j=\lceil k/2 \rceil+1}^{k-1} \Delta_j \Delta_k H(j, k)}_N \\ 1149 \quad & \\ 1150 \quad & \\ 1151 \quad & \\ 1152 \quad & \\ 1153 \quad & \\ 1154 \quad & \\ 1155 \quad & = D + 2F + 2N. \end{aligned}$$

1156 We bound each separately.  
 1157

1158 **Bounding  $D$ .** For  $D$ , we have that  $H(k, k) = \sum_{r=1}^k r^{-1} = \mathcal{O}(1 + \log k)$ , and so  
 1159

$$1160 \quad D = \sum_{k=1}^{n-1} \Delta_k^2 H(k, k) \leq \sum_{k=1}^{n-1} \frac{C'}{k^2(1 + \log k)} = \mathcal{O}(1).$$

1161 **Bounding  $F$ .** We have that  $k - j \geq k - \lceil k/2 \rceil \geq k/2$ , and so  
 1162

$$1163 \quad H(j, k) = \sum_{r=1}^j \frac{1}{\sqrt{r} \sqrt{r+k-j}} \leq \sqrt{\frac{2}{k}} \sum_{r=1}^j \frac{1}{\sqrt{r}} \leq 2\sqrt{2} \sqrt{\frac{j}{k}}.$$

1164 Plugging into our expression for  $F$ :  
 1165

$$1166 \quad F = \sum_{k=1}^{n-1} \sum_{j=1}^{\lceil k/2 \rceil} \Delta_j \Delta_k H(j, k) \leq 2\sqrt{2} C^2 \sum_{k=1}^{n-1} \frac{1}{k^{3/2}(1 + \log k)} \underbrace{\sum_{j=1}^{\lceil k/2 \rceil} \frac{1}{\sqrt{j}(1 + \log j)}}_{T(\lceil k/2 \rceil)}.$$

1167 We will show that  $T(K) = \mathcal{O}(\frac{\sqrt{K}}{1 + \log K})$  via integral inequality and integration by parts:  
 1168

$$\begin{aligned} 1169 \quad T(K) &= \sum_{j=1}^K \frac{1}{\sqrt{j}(1 + \log j)} = \mathcal{O}(1) + \sum_{j=\lceil e^2 \rceil}^K \frac{1}{\sqrt{j}(1 + \log j)} \\ 1170 \quad & \\ 1171 \quad & \\ 1172 \quad & \\ 1173 \quad & \\ 1174 \quad & \\ 1175 \quad & \\ 1176 \quad & \\ 1177 \quad & \\ 1178 \quad & \\ 1179 \quad & \leq \mathcal{O}(1) + \int_{e^2}^K \frac{dz}{\sqrt{z}(1 + \log z)} = \mathcal{O}(1) + 2 \int_e^{\sqrt{K}} \frac{du}{1 + 2 \log u} \end{aligned}$$

1180 where the last step uses a variable substitution  $z = u^2$  ( $dz = 2u du$ ). Continuing from the integral:  
 1181

$$\begin{aligned} 1182 \quad \int_e^{\sqrt{K}} \frac{du}{1 + 2 \log u} &= \left[ \frac{u}{1 + 2 \log u} \right]_{u=e}^{u=\sqrt{K}} + \int_e^{\sqrt{K}} \frac{2}{(1 + 2 \log u)^2} du \\ 1183 \quad & \\ 1184 \quad & \\ 1185 \quad & \\ 1186 \quad & \\ 1187 \quad & \leq \frac{\sqrt{K}}{1 + \log K} + 2 \int_e^{\sqrt{K}} \frac{du}{(1 + 2 \log u)^2} \\ & \\ & \leq \frac{\sqrt{K}}{1 + \log K} + \frac{2}{3} \int_e^{\sqrt{K}} \frac{du}{1 + 2 \log u}, \end{aligned}$$

1188 where the last step follows from  $f(u) = \frac{1}{1+2\log u}$  taking on values in  $(0, 1/3]$  for  $u \in [e, \sqrt{K}]$ , and  
 1189 so  $f(u)^2 \leq f(u)/3$ . Solving for the integral, we have that  
 1190

$$1191 \int_e^{\sqrt{K}} \frac{du}{1+2\log u} \leq \frac{3\sqrt{K}}{1+\log K}$$

1193 and so  $T(K) = \mathcal{O}(\frac{\sqrt{K}}{1+\log K})$ . Going back to bounding  $F$ , we have that  
 1194

$$1195 F \leq 2\sqrt{2}C^2 \sum_{k=1}^{n-1} \frac{T(\lceil k/2 \rceil)}{k^{3/2}(1+\log k)} \leq C'' \sum_{k=1}^{n-1} \frac{1}{k(1+\log k)^2} \\ 1196 \leq C'' \left( 1 + \int_1^\infty \frac{dz}{z(1+\log z)^2} \right) = C'' \left( 1 + \int_0^\infty \frac{du}{(1+u)^2} \right) = 2C'',$$

1200 where the integral step uses the variable substitution  $u = \log z$  ( $dz = z du$ ), and  $C''$  is an absolute  
 1201 constant.  
 1202

1203 **Bounding  $N$ .** Here we have that  $\lceil k/2 \rceil + 1 \leq j < k$  (and so  $k - j \leq k/2 - 1$ ). It follows that  
 1204

$$1205 H(j, k) = \sum_{r=1}^j \frac{1}{\sqrt{r(r+k-j)}} \leq \frac{1}{\sqrt{1+k-j}} + \int_1^j \frac{dz}{\sqrt{z(z+k-j)}} \\ 1206 = \frac{1}{\sqrt{1+k-j}} + \left[ 2 \operatorname{arsinh} \sqrt{\frac{z}{k-j}} \right]_{z=1}^{z=j} \leq \frac{1}{\sqrt{1+k-j}} + 2 \operatorname{arsinh} \sqrt{\frac{j}{k-j}}.$$

1207 Noting that  $\operatorname{arsinh}(u) \leq \log(1+2u) \leq \log 3u$  for  $u \geq 1$ , and that  $\frac{k}{k-j} \geq \frac{j}{k-j} \geq 1$ , we can simplify  
 1208 further:  
 1209

$$1210 H(j, k) \leq \frac{1}{\sqrt{1+k-j}} + 2 \log \left( 3 \sqrt{\frac{j}{k-j}} \right) \leq 2 \log \left( \frac{9k}{k-j} \right)$$

1211 Plugging our bound into the expression for  $N$  yields:  
 1212

$$1213 N = \sum_{k=1}^{n-1} \sum_{j=\lceil k/2 \rceil + 1}^{k-1} \Delta_j \Delta_k H(j, k) \\ 1214 \leq \sum_{k=1}^{n-1} \sum_{d=1}^{\lceil k/2 \rceil} \Delta_k \Delta_{k-d} H(k, k-d) \\ 1215 \leq 2C^2 \sum_{k=1}^{n-1} \sum_{d=1}^{\lceil k/2 \rceil} \frac{\log(9k/d)}{k(1+\log k)(k-d)(1+\log(k-d))} \\ 1216 \leq 4C^2 \sum_{k=1}^{n-1} \frac{1}{k^2(1+\log(k/2))^2} \sum_{d=1}^{\lceil k/2 \rceil} \log(9k/d).$$

1217 For the inner sum, we note that  
 1218

$$1219 \sum_{d=1}^{\lceil k/2 \rceil} \log(9k/d) = \lceil k/2 \rceil \log(9k) - \log(\lceil k/2 \rceil!) \\ 1220 \leq \lceil k/2 \rceil \log(9k) - \lceil k/2 \rceil \log(\lceil k/2 \rceil) + \lceil k/2 \rceil \\ 1221 \leq (1+\log 18)\lceil k/2 \rceil$$

1222 where the first inequality uses Stirling's lower bound:  $\log(t!) \geq t \log t - t$ . Continuing, we have  
 1223 thus shown  
 1224

$$1225 N \leq 4C^2(1+\log 18) \sum_{k=1}^{n-1} \frac{\lceil k/2 \rceil}{k^2(1+\log(k/2))^2} \leq C''' \sum_{k=1}^{n-1} \frac{1}{k(1+\log k)^2} \\ 1226 \leq C''' \left( 1 + \int_1^\infty \frac{1}{k(1+\log k)^2} \right) \leq 2C'''$$

1242 where the last integral was already computed in bounding  $F$ , and  $C'''$  is an absolute constant. Taking  
 1243 it all together, we have shown that

$$1244 \quad 1245 \quad S = D + 2F + 2N = \mathcal{O}(1),$$

1246 proving the theorem statement.  $\square$

1247 **Theorem 1.** *Let  $(\chi_t)_{t=1}^n$  be a sequence on  $[\beta, 1]$  for some constant  $\beta > 0$ . For  $n \geq 2$  we define*

$$1248 \quad 1249 \quad \Delta_t = |\chi_t - \chi_{t+1}| \quad (\text{for all } 1 \leq t \leq n-1). \quad (8)$$

1250 *If either of the following two conditions holds ( $c > 0$  an absolute constant):*

$$1251 \quad 1252 \quad \Delta_t \leq \frac{c}{t(1 + \log t)} \quad (\text{for all } 1 \leq t \leq n-1), \quad \text{or} \quad \sum_{t=1}^{n-1} \Delta_t^2 = o\left(\frac{\log n}{n}\right), \quad (9)$$

1254 *then the factorization  $B_\chi \times A_1^{1/2}$ , where  $B_\chi := A_\chi(A_1)^{-1/2}$ , satisfies*

$$1256 \quad 1257 \quad \text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\max_{m \in [n]} \chi_m^2 \log m}\right), \quad (10)$$

$$1259 \quad 1260 \quad \text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m}\right). \quad (11)$$

1262 *Proof.* Statement follows immediately from invoking Lemma 7 with the bounds on  $Q$  derived from  
 1263 Lemma 8 and 9.  $\square$

1265 **Lemma 1.** *Every learning rate schedule  $(\chi_t)_{t=1}^n$  with constant  $\beta \in (0, 1/e)$  presented in Table 1  
 1266 satisfies the assumptions of Theorem 1.*

1268 *Proof.* The result will be derived from invoking Corollary 1. We split the treatment of the learning  
 1269 schedules based on if their change over time is, roughly, uniform (exponential/linear/cosine  
 1270 schedules), or not (polynomial schedule). For the first case we show that  $\|\Delta\|_2 = \sqrt{\sum_{t=1}^{n-1} \Delta_t^2} =$   
 1271  $o\left(\sqrt{\log(n)/n}\right)$ ; for the second we show that  $\Delta_t = \mathcal{O}(1/(t \log t))$ . We begin with the uniform  
 1272 case.

1274 **Exponential schedule.**  $\chi_k = \beta^{\frac{k-1}{n-1}}$  and so

$$1276 \quad 1277 \quad \Delta_t = |\chi_t - \chi_{t+1}| = \beta^{\frac{t-1}{n-1}} (1 - \beta^{\frac{1}{n-1}}) \leq 1 - e^{-\frac{\log(1/\beta)}{n-1}} = \mathcal{O}\left(\frac{\log(1/\beta)}{n}\right).$$

1278 It follows that  $\|\Delta\|_2 = \mathcal{O}(\log(1/\beta)/\sqrt{n}) = o\left(\sqrt{\log(n)/n}\right)$ ,

1281 **Linear schedule.**  $\chi_k = 1 - (1 - \beta)^{\frac{k-1}{n-1}}$  and so

$$1283 \quad 1284 \quad \Delta_t = |\chi_t - \chi_{t+1}| = \frac{1 - \beta}{n-1}$$

1285 and so  $\|\Delta\|_2 = \mathcal{O}(1/\sqrt{n-1}) = o\left(\sqrt{\log(n)/n}\right)$ .

1287 **Cosine schedule.**  $\chi_k = \beta + \frac{1-\beta}{2} \left(1 + \cos\left(\frac{(k-1)}{n-1} P\pi\right)\right)$ , and so

$$1290 \quad 1291 \quad \Delta_t = |\chi_t - \chi_{t+1}| = \frac{1 - \beta}{2} \left| \cos\left(\frac{t-1}{n-1} \pi\right) - \cos\left(\frac{t}{n-1} \pi\right) \right| \\ 1292 \quad 1293 \quad = \frac{(1 - \beta)}{2} \cdot \frac{\pi}{n-1} \left| \sin\left(\frac{\xi}{n-1} \pi\right) \right| \leq \frac{(1 - \beta)\pi}{2(n-1)} = \mathcal{O}(1/n)$$

1294 where the third equality uses the mean value theorem applied to  $f(z) = \cos(cz)$  on  $[t-1, t]$  with  
 1295  $\xi \in (t-1, t)$ . It follows that  $\|\Delta\|_2 = \mathcal{O}(1/\sqrt{n})$ , which is  $o\left(\sqrt{\log(n)/n}\right)$ .

1296 Table 5: MaxSE and MeanSE errors for the factorization  $B_\chi \times A_1^{1/2} = A_\chi(A_1)^{-1/2} \times A_1^{1/2} = A_\chi$   
 1297 under single participation, listed for each of the learning rate schedules in Table 1.  $\beta \in (0, 1/e)$  is  
 1298 assumed throughout. (a) Exponential decay, proven in Corollary 6; (b) polynomial decay, proven in  
 1299 Corollary 7; (c) linear decay, proven in Corollary 8; (d) cosine decay, proven in Corollary 9.

1301 <b>Learning rate</b> $\chi_t$	1302 <b>MaxSE</b>	1303 <b>MeanSE</b>
1303 (a) $\chi_t = \beta^{\frac{t-1}{n-1}}$	1304 $\Theta\left(\sqrt{\log n} \sqrt{\log \frac{n}{\log(1/\beta)}}\right)$	1305 $\Theta\left(\frac{\log n}{\sqrt{\log(1/\beta)}}\right)$
1305 (b) $\chi_t = \beta + (1-\beta)\frac{(n/t)^\gamma - 1}{n^\gamma - 1}$ , $\gamma \geq 1$	1306 $\Theta\left(\sqrt{\log n \left(\beta^2 \log n + \frac{(1-\beta)^2}{\gamma}\right)}\right)$	1307 $\Theta(\beta \log n)$
1307 (c) $\chi_t = \beta + (1-\beta)\frac{t-1}{n-1}$	1308 $\Theta(\log n)$	1309 $\Theta(\log n)$
1308 (d) $\chi_t = \beta + \frac{1-\beta}{2} \left(1 + \cos\left(\frac{t-1}{n-1}\pi\right)\right)$	1309 $\Theta(\log n)$	

1310  
 1311 **Polynomial schedule.**  $\chi_k = \beta + (1-\beta)\frac{(\frac{n}{k})^\gamma - 1}{n^\gamma - 1}$ ,  $\gamma > 0$ , and so

$$1313 \Delta_k = |\chi_k - \chi_{k+1}| = \frac{1-\beta}{n^\gamma - 1} \left[ \left(\frac{n}{k}\right)^\gamma - \left(\frac{n}{k+1}\right)^\gamma \right] \\ 1314 = \frac{(1-\beta)n^\gamma}{(n^\gamma - 1)k^\gamma} \left[ 1 - \left(\frac{k}{k+1}\right)^\gamma \right] = \mathcal{O}\left(k^{-(\gamma+1)}\right).$$

1318 This also implies  $\Delta_k = \mathcal{O}\left(\frac{1}{k \log k}\right)$ , completing the last case.  $\square$

## 1320 E.1 ERROR FOR SPECIFIC LEARNING RATES

1322 In this section we give tight error bounds for the prefix-sum factorization for each of the learning  
 1323 rate schedules discussed in this paper (see Table 1 for the list). In Table 5 we give the corresponding  
 1324 error bounds, all of which are proved later in the section.

### 1326 E.1.1 EXPONENTIAL LEARNING RATE DECAY

1327 **Lemma 10.** Let  $\beta \in (0, 1/e)$  and  $\alpha = \beta^{1/(n-1)}$ . Then

$$1329 \max_{1 \leq m \leq n} \alpha^m \log m = \Theta\left(\log \frac{n}{\log(1/\beta)}\right). \quad (59)$$

1332 *Proof.* For the lower bound, take  $m_0 = \lceil 1/\log(1/\alpha) \rceil$ . Since  $\log(1/\alpha) = \frac{1}{n-1} \log(1/\beta)$ , we have  
 1333  $m_0 \leq (n-1)/\log(1/\beta) < n$ , so  $m_0$  is admissible. Moreover,  $\alpha^{m_0} \geq e^{-1}\alpha$  and  $\log m_0 \geq$   
 1334  $\log \frac{1}{\log(1/\alpha)}$ , giving

$$1336 \max_{1 \leq m \leq n} \alpha^m \log m \geq \Omega\left(\log \frac{1}{\log(1/\alpha)}\right).$$

1338 For the upper bound, write  $f(m) = \alpha^m \log m$  with real  $m > 1$ . Then  $\frac{d}{dm} \log f(m) = \log \alpha +$   
 1339  $1/(m \log m)$ , so the maximizer satisfies  $m \log m = 1/\log(1/\alpha)$ . At this point,  $\log m \sim \log \frac{1}{\log(1/\alpha)}$   
 1340 and  $\alpha^m = e^{-1/\log m} = \Theta(1)$ , hence  $f(m) = \mathcal{O}(\log \frac{1}{\log(1/\alpha)})$ .

1341 Thus

$$1343 \max_{1 \leq m \leq n} \alpha^m \log m = \Theta\left(\log \frac{1}{\log(1/\alpha)}\right).$$

1345 Finally, since  $\log \frac{1}{\log(1/\alpha)} = \log \frac{n-1}{\log(1/\beta)} = \Theta(\log \frac{n}{\log(1/\beta)})$ , the claim follows.  $\square$

1346 **Lemma 11.** Let  $\beta \in (0, 1/e)$  and  $\alpha = \beta^{1/(n-1)}$ . Then

$$1348 \frac{1}{n} \sum_{m=1}^n \alpha^m \log m = \Theta\left(\frac{\log n}{\log(1/\beta)}\right). \quad (60)$$

1350 *Proof.* Splitting  $\log m = \log n + \log(m/n)$  gives  
 1351

$$1352 \quad \frac{1}{n} \sum_{m=1}^n \alpha^m \log m = \frac{\log n}{n} \sum_{m=1}^n \alpha^m + \frac{1}{n} \sum_{m=1}^n \alpha^m \log(m/n).$$

1355 The first sum is geometric:  $\sum_{m=1}^n \alpha^m = \alpha(1 - \alpha^n)/(1 - \alpha)$ . Since  $\alpha = 1 - \frac{\log(1/\beta)}{n-1} + o(1/n)$ ,  
 1356 we have  $1 - \alpha \sim \frac{\log(1/\beta)}{n-1}$  and  $\alpha^n \rightarrow \beta$ . Thus  $\frac{1}{n} \sum_{m=1}^n \alpha^m \sim (1 - \beta)/\log(1/\beta)$ , so the first term  
 1357 is  $\sim \frac{1-\beta}{\log(1/\beta)} \log n = \Theta(\frac{\log n}{\log(1/\beta)})$ .  
 1358

1360 The second sum is a Riemann sum, converging to  $I(\beta) = \int_0^1 \beta^x \log x dx$ . Since  $I$  is monotone  
 1361 decreasing with  $I(0) = 0$ ,  $I(1) = -1$ , we have  $I(\beta) = \Theta(1)$ . Hence the first term dominates, and  
 1362 the result follows.  $\square$

1363 **Corollary 6.** *For exponential learning rate decay  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ , the prefix-sum-  
 1364 based factorization  $A_\chi = A_\chi(A_1)^{-1/2} \times A_1^{1/2}$  gives the following values for MaxSE and MeanSE:*  
 1365

$$1366 \quad \text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta\left(\sqrt{\log n} \sqrt{\log \frac{n}{\log(1/\beta)}}\right), \quad (61)$$

$$1369 \quad \text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta\left(\frac{\log n}{\sqrt{\log(1/\beta)}}\right). \quad (62)$$

1373 *Proof.* Invoking Lemma 1 we have that  
 1374

$$1375 \quad \text{MaxSE}\left(B_\chi, A_1^{1/2}\right) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\max_{1 \leq t \leq n} \beta^{2\frac{t-1}{n-1}} \log t}\right) = \Theta\left(\sqrt{\log n} \sqrt{\frac{n}{\log(1/\beta)}}\right)$$

$$1378 \quad \text{MeanSE}\left(B_\chi, A_1^{1/2}\right) = \Theta\left(\sqrt{\log n} \cdot \sqrt{\frac{1}{n} \sum_{t=1}^n \beta^{2\frac{t-1}{n-1}} \log t}\right) = \Theta\left(\sqrt{\frac{\log n}{\log(1/\beta)}}\right),$$

1381 where the last step of each equation invokes Lemma 10 and 11 respectively for  $\beta' = \beta^2 \in (0, 1/e)$ .  
 1382  $\square$

### 1383 E.1.2 POLYNOMIAL LEARNING RATE DECAY

1385 **Lemma 12.** *Let  $1 \leq m \leq n$  be integers,  $\beta \in (0, 1/e)$ ,  $\gamma \geq 1$  and  $n$  sufficiently large. Let  
 1386  $\chi_k = \beta + (1 - \beta) \frac{(\frac{n}{k})^\gamma - 1}{n^\gamma - 1}$ . Then*

$$1389 \quad \max_{1 \leq m \leq n} \chi_m^2 \log m = \Theta\left(\beta^2 \log n + \frac{(1 - \beta)^2}{\gamma}\right).$$

1391 *Proof.* Before we start, we will find the following inequality useful:  
 1392

$$1393 \quad \chi_m = \beta + (1 - \beta)m^{-\gamma} + \frac{(1 - \beta)(m^{-\gamma} - 1)}{n^\gamma - 1} \geq \left(1 - \frac{1 - \beta}{\beta(n^\gamma - 1)}\right) (\beta + (1 - \beta)m^{-\gamma})$$

1395 In particular for large enough  $n$ , and  $1 \leq m \leq n$ , we have that  
 1396

$$1397 \quad \chi_m \geq \frac{1}{2} (\beta + (1 - \beta)m^{-\gamma}),$$

1399 and for all  $n$ , and  $1 \leq m \leq n$ , also that  
 1400

$$1401 \quad \chi_m \leq \beta + (1 - \beta)m^{-\gamma},$$

1402 implying that it suffices for us to argue about  
 1403

$$\chi_m = \Theta(\beta + (1 - \beta)m^{-\gamma}) \quad (63)$$

1404 when convenient. We now begin with the upper bound. Using  $(a+b)^2 \leq 2a^2 + 2b^2$  in the first step:

$$\begin{aligned} 1406 \quad \max_{1 \leq m \leq n} \chi_m^2 \log m &\leq \max_{1 \leq m \leq n} 2(\beta^2 + (1-\beta)^2 m^{-2\gamma}) \log m \\ 1407 \quad &\leq 2\beta^2 \log n + 2(1-\beta)^2 \max_{1 \leq m \leq n} m^{-2\gamma} \log m \\ 1408 \end{aligned}$$

1409 Defining  $f(z) = z^{-2\gamma} \log z$ , we have that  $f'(z) = z^{-2\gamma-1}(1-2\gamma \log z)$ . Solving  $f(z) = 0$  yields  
1410 the maximizer  $z = e^{\frac{1}{2\gamma}}$ , and so  
1411

$$1412 \quad \max_m \chi_m^2 \log m \leq 2 \left( \beta^2 \log n + \frac{(1-\beta)^2}{2e\gamma} \right) = \mathcal{O} \left( \beta^2 \log n + \frac{(1-\beta)^2}{\gamma} \right).$$

1414 For the lower bound, we note that setting  $m_0 = n$  yields  $\chi_{m_0}^2 \log m_0 = \beta^2 \log n$ .

1415 Instead choosing  $m_0 = \lceil e^{\frac{1}{2\gamma}} \rceil$  yields  
1416

$$1417 \quad \chi_{m_0}^2 \log m_0 \geq \frac{1}{4} (\beta + (1-\beta)e^{-\frac{1}{2}})^2 \log(e^{\frac{1}{2\gamma}} - 1) \geq \frac{(1-\beta)^2}{4e} \log(e^{\frac{1}{2\gamma}} - 1) = \Omega \left( \frac{(1-\beta)^2}{\gamma} \right)$$

1419 Combining the two lower bounds, we get  
1420

$$1421 \quad \max_m \chi_m^2 \log m = \Omega \left( \max \left\{ \beta^2 \log n, \frac{(1-\beta)^2}{\gamma} \right\} \right) = \Omega \left( \beta^2 \log n + \frac{(1-\beta)^2}{\gamma} \right),$$

1423 finishing the proof.  $\square$

1424 **Lemma 13.** *Let  $1 \leq m \leq n$  be integers,  $\beta \in (0, 1/e)$ ,  $\gamma \geq 1$  and  $n$  sufficiently large. Let  
1425  $\chi_k = \beta + (1-\beta) \frac{(\frac{n}{k})^{\gamma}-1}{n^{\gamma}-1}$ . Then*

$$1428 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m = \Theta(\beta^2 \log n).$$

1431 *Proof.* We will again use that

$$1432 \quad \frac{1}{2}(\beta + (1-\beta)^2 m^{-\gamma}) \leq \chi_m \leq \beta + (1-\beta)^2 m^{-\gamma}$$

1434 as shown in the proof of Lemma 12. First the upper bound. We write  
1435

$$\begin{aligned} 1436 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m &\leq \frac{1}{n} \sum_{m=1}^n 2(\beta^2 + (1-\beta)^2 m^{-2\gamma}) \log m \leq \frac{2 \log n}{n} \sum_{m=2}^n \beta^2 + (1-\beta)^2 m^{-2\gamma} \\ 1437 \quad &\leq 2\beta^2 \log n + \frac{2(1-\beta)^2 \log n}{n} \int_{t=1}^n t^{-2\gamma} dt \\ 1438 \quad &= 2\beta^2 \log n + \frac{2(1-\beta)^2 \log n}{n} \cdot \frac{n^{2\gamma-1} - 1}{2\gamma - 1} = \mathcal{O}(\beta^2 \log n), \\ 1439 \quad & \end{aligned}$$

1443 where the second term in the second-to-last expression can be identified as  $o(\log n)$  for any value of  
1444  $\gamma > 0$ . For the lower bound,

$$\begin{aligned} 1445 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m &\geq \frac{1}{n} \sum_{m=1}^n \frac{1}{4} (\beta + (1-\beta)m^{-\gamma})^2 \log m \geq \frac{1}{4n} \sum_{m=1}^n \beta^2 \log m \\ 1446 \quad &\geq \frac{\beta^2}{4n} \sum_{m=\lceil m/2 \rceil}^n \log m \geq \frac{\beta^2(n/2 - 1) \log(n/2)}{4n} = \Omega(\beta^2 \log n). \quad \square \\ 1447 \quad & \end{aligned}$$

1451 **Corollary 7.** *For polynomial learning rate decay  $\chi_k = \beta + (1-\beta) \frac{(\frac{n}{k})^{\gamma}-1}{n^{\gamma}-1}$  with constant  $\beta \in (0, 1/e)$   
1452 and  $\gamma \geq 1$ , the prefix-sum-based factorization  $A_\chi = A_\chi (A_1^{-1/2}) \times A_1^{1/2}$  gives the following values  
1453 for MaxSE and MeanSE:*

$$1455 \quad \text{MaxSE}(B_\chi, A_1^{-1/2}) = \Theta \left( \sqrt{\log n \left( \beta^2 \log n + \frac{(1-\beta)^2}{\gamma} \right)} \right),$$

$$1456 \quad \text{MeanSE}(B_\chi, A_1^{-1/2}) = \Theta(\beta \log n).$$

1458 *Proof.* Result is immediate from invoking Lemma 1, together with Lemma 12 and 13 for the MaxSE  
 1459 and MeanSE errors respectively.  $\square$

### 1461 E.1.3 LINEAR LEARNING RATE DECAY

1463 **Lemma 14.** *Let  $\chi_k = 1 - (1 - \beta) \frac{k-1}{n-1}$ ,  $\beta \in (0, 1/e)$  and  $n \geq 2$ . Then*

$$1465 \max_{1 \leq m \leq n} \chi_m^2 \log m = \Theta(\log n).$$

1468 *Proof.* For the upper bound, using  $\chi_k \leq 1$ , we directly get

$$1470 \max_{1 \leq m \leq n} \chi_m^2 \log m \leq \log n.$$

1472 For the lower bound, pick  $m_0 = \lfloor (n+1)/2 \rfloor$  where  $\chi_{m_0} \geq (1+\beta)/2$ :

$$1474 \max_{1 \leq m \leq n} \chi_m^2 \log m \geq \chi_{m_0}^2 \log m_0 = \frac{(1+\beta)^2}{4} \log \left\lfloor \frac{n+1}{2} \right\rfloor = \Omega(\log n),$$

1476 finishing the proof.  $\square$

1478 **Lemma 15.** *Let  $\chi_k = 1 - (1 - \beta) \frac{k-1}{n-1}$ ,  $\beta \in (0, 1/e)$  and  $n \geq 2$ . Then*

$$1480 \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m = \Theta(\log n).$$

1484 *Proof.* For the upper bound, again using  $\chi_k \leq 1$ , and  $\log m \leq \log n$  we directly get

$$1486 \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m \leq \frac{1}{n} \cdot n \log n = \log n.$$

1489 For the lower bound, we truncate the sum at  $m_0 = \lfloor (n+1)/2 \rfloor$  and use the bound  $\chi_k \geq \frac{1+\beta}{2}$  for  
 1490 all  $k \leq m_0$ :

$$1492 \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m \geq \frac{1}{n} \sum_{m=1}^{m_0} \chi_m^2 \log m \geq \frac{(1+\beta)^2}{4n} \sum_{m=1}^{m_0} \log m \geq \Omega(\log n),$$

1494 where the last step can be seen by truncating the sum, taking the upper half of the indices, and lower  
 1495 bounding each of the  $\Omega(n)$  logarithms by  $\log \lceil m_0/2 \rceil = \Omega(\log n)$ . This finishes the proof.  $\square$

1498 **Corollary 8.** *For linear learning rate decay  $\chi_k = 1 - (1 - \beta) \frac{k-1}{n-1}$  with  $\beta \in (0, 1/e)$ , the prefix-  
 1499 sum-based factorization  $A_\chi = A_\chi (A_1)^{-1/2} \times A_1^{1/2}$  gives the following values for MaxSE and  
 1500 MeanSE:*

$$1501 \text{MaxSE}(B_\chi, A_1^{1/2}) = \Theta(\log n), \quad \text{MeanSE}(B_\chi, A_1^{1/2}) = \Theta(\log n). \quad (64)$$

1504 *Proof.* Result is immediate from invoking Lemma 1, together with Lemma 14 and 15 for the MaxSE  
 1505 and MeanSE errors respectively.  $\square$

### 1507 E.1.4 COSINE LEARNING RATE DECAY.

1509 **Lemma 16.** *Let  $1 \leq m \leq n$  be integers,  $\beta \in (0, 1/e)$ , and  $n$  sufficiently large. Let  $\chi_k = \beta +$   
 1510  $\frac{1-\beta}{2}(1 + \cos(\frac{k-1}{n-1}\pi))$ . Then*

$$1511 \max_{1 \leq m \leq n} \chi_m^2 \log m = \Theta(\log n).$$

1512 *Proof.* First the upper bound. We use that  $\chi_k \leq 1$ :

$$1514 \quad \max_{1 \leq m \leq n} \chi_m^2 \log m \leq \max_{1 \leq m \leq n} \log m = \log n.$$

1516 For the lower bound, we set  $m_0 = \lfloor (n+1)/2 \rfloor$ .

$$\begin{aligned} 1517 \quad \max_{1 \leq m \leq n} \chi_m^2 \log m &\geq \left( \beta + \frac{1-\beta}{2} \left( 1 + \cos \left( \frac{\lfloor (n+1)/2 \rfloor - 1}{n-1} \pi \right) \right) \right)^2 \log \left\lfloor \frac{n+1}{2} \right\rfloor \\ 1518 \quad &\geq \left( \beta + \frac{1-\beta}{2} \left( 1 + \cos \left( \frac{\pi}{2} \right) \right) \right)^2 \log \left( \frac{n-1}{2} \right) \\ 1519 \quad &= \frac{(1+\beta)^2}{4} \log \left( \frac{n-1}{2} \right) = \Omega(\log n). \end{aligned} \quad \square$$

1525 **Lemma 17.** Let  $1 \leq m \leq n$  be integers,  $\beta \in (0, 1/e)$ , and  $n$  sufficiently large. Let  $\chi_k = \beta +$   
 1526  $\frac{1-\beta}{2} \left( 1 + \cos \left( \frac{k-1}{n-1} \pi \right) \right)$ . Then  
 1527

$$1528 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m = \Theta(\log n).$$

1531 *Proof.* For the upper bound, we again use that  $\chi_k \leq 1$ .

$$1533 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m \leq \frac{1}{n} \cdot n \log n = \log n$$

1536 We prove the lower bound by truncating the sum.

$$\begin{aligned} 1538 \quad \frac{1}{n} \sum_{m=1}^n \chi_m^2 \log m &\geq \frac{1}{n} \sum_{m=\lceil n/4 \rceil}^{\lfloor (n+1)/2 \rfloor} \left( \beta + \frac{(1-\beta)}{2} \left( 1 + \cos \left( \frac{m-1}{n-1} \pi \right) \right) \right)^2 \log m \\ 1539 \quad &\geq \frac{1}{n} \sum_{m=\lceil n/4 \rceil}^{\lfloor (n+1)/2 \rfloor} \left( \beta + \frac{(1-\beta)}{2} \left( 1 + \cos \left( \frac{\lfloor (n+1)/2 \rfloor - 1}{n-1} \pi \right) \right) \right)^2 \log \left\lceil \frac{n}{4} \right\rceil \\ 1540 \quad &\geq \frac{1}{n} \sum_{m=\lceil n/4 \rceil}^{\lfloor (n+1)/2 \rfloor} \left( \frac{1+\beta}{2} \right)^2 \log \left( \frac{n}{4} \right) \\ 1541 \quad &= \frac{(1+\beta)^2}{4n} \left( \left\lfloor \frac{n+1}{2} \right\rfloor - \left\lceil \frac{n}{4} \right\rceil + 1 \right) \log \left( \frac{n}{4} \right) = \Omega(\log n). \end{aligned} \quad \square$$

1549 **Corollary 9.** For cosine learning rate decay  $\chi_k = \beta + \frac{1-\beta}{2} \left( 1 + \cos \left( \frac{k-1}{n-1} \pi \right) \right)$  with  $\beta \in (0, 1/e)$ ,  
 1550 the prefix-sum-based factorization  $A_\chi = A_\chi (A_1)^{-1/2} \times A_1^{1/2}$  gives the following values for MaxSE  
 1551 and MeanSE:  
 1552

$$1554 \quad \text{MaxSE}(B_\chi, A_1^{-1/2}) = \Theta(\log n), \quad \text{MeanSE}(B_\chi, A_1^{-1/2}) = \Theta(\log n).$$

1555 *Proof.* Result is immediate from invoking Lemma 1, together with Lemma 16 and 17 for the MaxSE  
 1556 and MeanSE errors respectively.  $\square$

## 1559 F SINGLE-PARTICIPATION: LOWER BOUNDS

1561 **Theorem 2.** Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi = \text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_t > 0$ . Then

$$1563 \quad \inf_{B \times C = A_\chi} \text{MaxSE}(B, C) \geq \max_{1 \leq t \leq n} \frac{1}{\pi} (\min_{j \leq t} \chi_j) \log t \quad (12)$$

$$1565 \quad \inf_{B \times C = A_\chi} \text{MeanSE}(B, C) \geq \max_{1 \leq t \leq n} \frac{1}{\pi} \sqrt{\frac{t}{n}} (\min_{j \leq t} \chi_j) \log t. \quad (13)$$

1566 *Proof.* We prove each bound separately in Lemmas 18 and 19.  $\square$   
 1567

1568 **Lemma 18.** *Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi = \text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_1, \chi_2, \dots, \chi_n$ . Then*  
 1569

$$1570 \quad \gamma_2(A_\chi) := \inf_{B \times C = A_\chi} \text{MaxSE}(B, C) \geq \max_{1 \leq k \leq n} \frac{1}{\pi} (\min_{j \leq k} \chi_j) \log k. \\ 1571$$

1572 *Proof.* The optimal factorization error can be written as  
 1573

$$1574 \quad \gamma_2(A) = \max \left\{ \|P^{1/2} A Q^{1/2}\|_* : P, Q \text{ diag., nonneg., } \text{Tr } P = \text{Tr } Q = 1 \right\}, \\ 1575$$

1576 where  $\|\cdot\|_*$  denotes the nuclear norm of a matrix. It was observed in Matoušek et al. (2020) that  
 1577 this norm is monotonic with respect to taking submatrices: if  $A = B \times C$ , then removing rows  
 1578 from  $B$  cannot increase the maximum row norm, and removing columns from  $C$  cannot increase  
 1579 the maximum column norm. Thus, we can lower bound  $\gamma_2(A)$  by the  $k \times k$  principal submatrix  
 1580 consisting of the first  $k$  rows and columns:

$$1581 \quad \gamma_2(A_\chi) \geq \gamma_2((A_\chi)_{:k,:k}). \\ 1582$$

1583 For the lower bound, let us assume  $P = \frac{1}{k} I_k$  and  $Q = \frac{1}{\text{Tr}(D_{:k,:k}^{-2})} D_{:k,:k}^{-2}$ , which gives  
 1584

$$1585 \quad \gamma_2((A_\chi)_{:k,:k}) \geq \frac{\|(A_1)_{:k,:k}\|_*}{\sqrt{k} \sqrt{\sum_{j=1}^k \chi_j^{-2}}}. \\ 1586 \\ 1587 \\ 1588$$

1589 Using the bound  $\|(A_1)_{:k,:k}\|_* \geq \frac{k}{\pi} \log k$  and the fact that  $\sum_{j=1}^k \chi_j^{-2} \leq k (\min_{j \leq k} \chi_j)^{-2}$ , we conclude  
 1590

$$1591 \quad \gamma_2(A_\chi) \geq \frac{1}{\pi} (\min_{j \leq k} \chi_j) \log k. \\ 1592 \\ 1593$$

1594 Maximizing over  $k$  yields the lemma.  $\square$   
 1595

1596 **Lemma 19.** *Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi = \text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_1, \chi_2, \dots, \chi_n$ . Then*  
 1597

$$1598 \quad \gamma_F(A_\chi) = \inf_{A_\chi = BC} \text{MeanSE}(B, C) \geq \max_{1 \leq k \leq n} \frac{1}{\pi} \sqrt{\frac{k}{n}} (\min_{j \leq k} \chi_j) \log k. \\ 1599$$

1600 *Proof.* By definition,  
 1601

$$1602 \quad \gamma_F(A) = \inf_{A=BC} \frac{1}{\sqrt{n}} \|B\|_F \|C\|_{1 \rightarrow 2}, \\ 1603$$

1604 where  $\|C\|_{1 \rightarrow 2} = \max_j \|C_{:,j}\|_2$  is the maximum column norm.  
 1605

1606 Fix  $k \leq n$ . For any factorization  $A = BC$ , the principal  $k \times k$  submatrix satisfies  
 1607

$$1608 \quad A_{:k,:k} = B_{:k,:} C_{:,k}.$$

1609 Since removing rows can only decrease the Frobenius norm,  $\|B_{:k,:}\|_F \leq \|B\|_F$ , and removing  
 1610 columns can only decrease the  $\|\cdot\|_{1 \rightarrow 2}$  norm,  $\|C_{:,k}\|_{1 \rightarrow 2} \leq \|C\|_{1 \rightarrow 2}$ . Therefore  
 1611

$$1612 \quad \frac{1}{\sqrt{n}} \|B\|_F \|C\|_{1 \rightarrow 2} \geq \frac{1}{\sqrt{n}} \|B_{:k,:}\|_F \|C_{:,k}\|_{1 \rightarrow 2} = \sqrt{\frac{k}{n}} \left( \frac{1}{\sqrt{k}} \|B_{:k,:}\|_F \|C_{:,k}\|_{1 \rightarrow 2} \right).$$

1613 Taking the infimum over all factorizations gives  
 1614

$$1615 \quad \gamma_F(A) \geq \sqrt{\frac{k}{n}} \gamma_F(A_{:k,:k}). \tag{65} \\ 1616$$

1617 For the submatrix, we use the bound from Henzinger et al. (2023):  
 1618

$$1619 \quad \gamma_F((A_\chi)_{:k,:k}) \geq \frac{\|(A_\chi)_{:k,:k}\|_*}{k}, \tag{66}$$

1620 where  $\|\cdot\|_*$  denotes the nuclear norm. Recall that the nuclear norm is dual to the spectral norm:  
1621

$$1622 \|M\|_* = \sup_{\|Y\|_2 \leq 1} \text{tr}(MY^\top), \\ 1623$$

1624 where the supremum is over all matrices  $Y$  with operator norm at most 1. Write  $(A_\chi)_{:k,:k} =$   
1625  $(A_1)_{:k,:k} D_k$  with  $D_k = \text{diag}(\chi_1, \dots, \chi_k)$ . If  $W$  is a dual certificate for  $(A_1)_{:k,:k}$ , so that  $\|W\|_2 \leq 1$   
1626 and  $\|(A_1)_{:k,:k}\|_* = \text{tr}((A_1)_{:k,:k} W^\top)$ , then consider  
1627

$$1628 Y = \frac{WD_k^{-1}}{\|D_k^{-1}\|_2}. \\ 1629$$

1630 Since  $\|W\|_2 \leq 1$ , we have  $\|Y\|_2 \leq 1$ . Thus  
1631

$$1632 \|(A_\chi)_{:k,:k}\|_* \geq \text{tr}((A_1)_{:k,:k} D_k Y^\top) = \frac{1}{\|D_k^{-1}\|_2} \text{tr}((A_1)_{:k,:k} W^\top) = \frac{1}{\|D_k^{-1}\|_2} \|(A_1)_{:k,:k}\|_*. \\ 1633$$

1634 The largest diagonal entry of  $D_k^{-1}$  is  $(\min_{j \leq k} \chi_j)^{-1}$ , so  
1635

$$1636 \|(A_\chi)_{:k,:k}\|_* \geq (\min_{j \leq k} \chi_j) \|(A_1)_{:k,:k}\|_*. \quad (67) \\ 1637$$

1638 Finally, using the standard estimate  $\|(A_1)_{:k,:k}\|_* \geq \frac{k}{\pi} \log k$ , combining (65), (66), and (67) gives  
1639

$$1640 \gamma_F(A_\chi) \geq \sqrt{\frac{k}{n}} \cdot \frac{1}{k} \cdot \frac{k}{\pi} (\min_{j \leq k} \chi_j) \log k = \frac{1}{\pi} \sqrt{\frac{k}{n}} (\min_{j \leq k} \chi_j) \log k. \\ 1641$$

1642 Maximizing over  $k$  proves the lemma.  $\square$   
1643

1644 **Corollary 2.** Suppose  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then  
1645

$$1646 \inf_{B \times C = A_\chi} \text{MaxSE}(B, C) = \Omega\left(\log \frac{n}{\log(1/\beta)}\right) \quad (16) \\ 1647$$

$$1648 \inf_{B \times C = A_\chi} \text{MeanSE}(B, C) = \Omega\left(\frac{1}{\sqrt{\log(1/\beta)}} \log \frac{n}{\log(1/\beta)}\right). \quad (17) \\ 1649$$

1650 *Proof.* By Theorem 2, for any  $t$ ,  
1651

$$1652 \inf_{A_\chi = BC} \text{MaxSE}(B, C) \geq \frac{\chi_t}{\pi} \log t, \quad \inf_{A_\chi = BC} \text{MeanSE}(B, C) \geq \frac{\chi_t}{\pi} \sqrt{\frac{t}{n}} \log t. \\ 1653$$

1654 Choose

$$1655 t^* = \left\lceil \frac{n}{\log(1/\beta)} \right\rceil, \\ 1656$$

1657 which satisfies  $1 \leq t^* \leq n$  since  $\beta \in (0, 1/e)$ . Then  
1658

$$1659 \chi_{t^*} = \beta^{\frac{t^*-1}{n-1}} = \exp\left(-\frac{\log(1/\beta)}{n-1} (t^* - 1)\right) = \Theta(1). \\ 1660$$

1661 Hence

$$1662 \inf_{A_\chi = BC} \text{MaxSE}(B, C) \geq \frac{\chi_{t^*}}{\pi} \log t^* = \Omega\left(\log \frac{n}{\log(1/\beta)}\right), \\ 1663$$

1664 and, using  $t^*/n = \Theta(1/\log(1/\beta))$ ,  
1665

$$1666 \inf_{A_\chi = BC} \text{MeanSE}(B, C) \geq \frac{\chi_{t^*}}{\pi} \sqrt{\frac{t^*}{n}} \log t^* = \Omega\left(\frac{1}{\sqrt{\log(1/\beta)}} \log \frac{n}{\log(1/\beta)}\right). \\ 1667$$

1668  $\square$

1674 **G MULTI-PARTICIPATION: PREFIX-SUM FACTORIZATION**  
16751676 **Lemma 20.** Let  $(\chi_t)_{t=1}^n$  be a positive sequence taken from  $[\beta, \infty)$  where  $\beta > 0$  is a constant, and  
1677

1678 
$$1679 Q = \sum_{l=1}^{n-1} \left( \sum_{t=0}^{n-l-1} |\chi_{l+t} - \chi_{l+t+1}| r_t \right)^2 = o(\log n).$$
  
1680  
1681

1682 *Then*

1683 
$$1684 \|B_\chi^p\|_{2 \rightarrow \infty} = \Theta \left( \sqrt{\max_{1 \leq m \leq n} \chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2} \right),$$
  
1685  
1686 
$$1687 \frac{1}{\sqrt{n}} \|B_\chi^p\|_F = \Theta \left( \sqrt{\frac{1}{n} \sum_{m=1}^n \left[ \chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2 \right]} \right).$$
  
1688  
1689  
1690

1691 *Proof.* The entries of  $B_\chi^p$  can be expressed as follows:  
1692

1693 
$$1694 (B_\chi^p)_{m,l} = \chi_l + \sum_{t=1}^{\min\{m-l, p-1\}} \tilde{r}_t \chi_{t+l} = \chi_l + \sum_{t=1}^{m-l} \tilde{r}_t \chi_{t+l} \mathbb{1}_{t \leq p-1}, \quad (68)$$
  
1695  
1696

1697 where again  $\tilde{r}_t = \frac{-r_t}{2t-1}$ . Following the proof of Lemma 7 and applying summation of parts:  
1698

1699 
$$1700 (B_\chi^p)_{m,l} = \chi_m \sum_{t=0}^{m-l} \tilde{r}_t \mathbb{1}_{t \leq p-1} - \sum_{t=0}^{m-l-1} (\chi_{l+t+1} - \chi_{l+t}) \sum_{j=0}^t \tilde{r}_j \mathbb{1}_{j \leq p-1}$$
  
1701  
1702 
$$1703 = \chi_m r_{\min\{m-l, p-1\}} + \sum_{t=0}^{m-l-1} (\chi_{l+t} - \chi_{l+t+1}) r_{\min\{t, p-1\}}.$$
  
1704  
1705

1706 For notational convenience, let  $\delta_t = \chi_t - \chi_{t+1}$  and  $\Delta_t = |\delta_t|$ . We have two distinct cases for these  
1707 sums:  $m - l \leq p - 1$  and  $m - l > p - 1$ . Starting with the first case, we get  
1708

1709 
$$1710 (B_\chi^p)_{m,l} = \chi_m r_{m-l} + \sum_{t=0}^{m-l-1} \delta_{l+t} r_t.$$
  
1711

1712 as in the case without bandedness ( $p = n$ ). For the second case, where  $m - l > p - 1$ , we get  
1713

1714 
$$1715 (B_\chi^p)_{m,l} = \chi_m r_{p-1} + \sum_{t=0}^{p-2} \delta_{l+t} r_t + \underbrace{\sum_{t=p-1}^{m-l-1} \delta_{l+t} r_{p-1}}_{= (\chi_{l+p-1} - \chi_m) r_{p-1}} = \chi_{l+p-1} r_{p-1} + \sum_{t=0}^{p-2} \delta_{l+t} r_t.$$
  
1716  
1717  
1718

1719 Combining the two expressions, we can express the squared row sums:  
1720

1721 
$$1722 \sum_{l=1}^m (B_\chi^p)_{m,l}^2 = \sum_{l=1}^{\max\{m-p, 0\}} (B_\chi^p)_{m,l}^2 + \sum_{l=\max\{m-p, 0\}+1}^m (B_\chi^p)_{m,l}^2$$
  
1723  
1724 
$$1725 = \underbrace{\sum_{l=1}^{\max\{m-p, 0\}} \left( \chi_{l+p-1} r_{p-1} + \sum_{t=0}^{p-2} \delta_{l+t} r_t \right)^2}_{S_1} + \underbrace{\sum_{l=\max\{m-p, 0\}+1}^m \left( \chi_m r_{m-l} + \sum_{t=0}^{m-l-1} \delta_{l+t} r_t \right)^2}_{S_2}.$$
  
1726  
1727

We will argue that we can characterize  $S_1 + S_2$  tightly. Beginning with upper bounds, using  $(a + b)^2 \leq 2a^2 + 2b^2$ , and letting  $q = \max\{m - p, 0\}$ :

$$S_1 \leq \sum_{l=1}^q \left( \chi_{l+p-1} r_{p-1} + \sum_{t=0}^{p-2} \Delta_{l+t} r_t \right)^2 \leq 2 \underbrace{r_{p-1}^2 \sum_{l=1}^q \chi_{l+p-1}^2}_{P_1} + 2 \underbrace{\sum_{l=1}^q \left( \sum_{t=0}^{p-2} \Delta_{l+t} r_t \right)^2}_{Q_1},$$

$$S_2 \leq \sum_{l=q+1}^m \left( \chi_m r_{m-l} + \sum_{t=0}^{m-l-1} \Delta_{l+t} r_t \right)^2 \leq 2 \underbrace{\chi_m^2 \sum_{l=q+1}^m r_{m-l}^2}_{P_2} + 2 \underbrace{\sum_{l=q+1}^{m-1} \left( \sum_{t=0}^{m-l-1} \Delta_{l+t} r_t \right)^2}_{Q_2}.$$

Repeating the exercise to get a lower bound on  $S_1 + S_2$  via  $(a + b)^2 \geq \frac{1}{2}a^2 - b^2$ :

$$S_1 = \sum_{l=1}^q \left( \chi_{l+p-1} r_{p-1} + \sum_{t=0}^{p-2} \delta_{l+t} r_t \right)^2 \geq \frac{1}{2} P_1 - \sum_{l=1}^q \left( \sum_{t=0}^{p-2} \delta_{l+t} r_t \right)^2 \geq \frac{1}{2} P_1 - Q_1,$$

$$S_2 = \sum_{l=q+1}^m \left( \chi_m r_{m-l} + \sum_{t=0}^{m-l-1} \delta_{l+t} r_t \right)^2 \geq \frac{1}{2} P_2 - \sum_{l=q+1}^{m-1} \left( \sum_{t=0}^{m-l-1} \delta_{l+t} r_t \right)^2 \geq \frac{1}{2} P_2 - Q_2,$$

where the last step in each derivation uses that the expression is made smaller when we replace  $\delta_{l+t}$  by  $\Delta_{l+t}$ . It follows that

$$\sum_{l=1}^m (B_\chi^p)_{m,l}^2 = S_1 + S_2 = \Theta(P_1 + P_2) \pm \mathcal{O}(Q_1 + Q_2).$$

We have that

$$P_1 = r_{p-1}^2 \sum_{l=1}^{\max\{m-p, 0\}} \chi_{l+p-1}^2 = r_{p-1}^2 \sum_{l=p}^{m-1} \chi_l^2 = \Theta\left(\frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2\right),$$

$$P_2 = \chi_m^2 \sum_{l=q+1}^m r_{m-l}^2 = \chi_m^2 \sum_{t=0}^{\min\{m,p\}-1} r_t^2 = \Theta(\chi_m^2 \log \min\{m, p\}),$$

from using the bound  $r_t = \Theta(1/\sqrt{t})$ , and

$$Q_1 + Q_2 \leq \sum_{l=1}^{m-1} \left( \sum_{t=0}^{m-l-1} \Delta_{l+t} r_t \right)^2 \leq Q,$$

from increasing the upper limit of the inner sum of  $Q_1$  to  $m - l - 1$ , then setting  $m = n$ . And so,

$$\sum_{l=1}^m (B_\chi^p)_{m,l}^2 = \Theta\left(\chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2\right) \pm \mathcal{O}(Q).$$

Computing the norms:

$$\frac{1}{n} \|B_\chi^p\|_F^2 = \frac{1}{n} \sum_{m=1}^n \sum_{l=1}^m (B_\chi^p)_{m,l}^2 = \Theta\left(\frac{1}{n} \sum_{m=1}^n \left[ \log \min\{m, p\} + \frac{\max\{m-p, 0\}}{p} \right]\right) \pm \mathcal{O}(Q)$$

$$\|B_\chi^p\|_{2 \rightarrow \infty}^2 = \max_{1 \leq m \leq n} \sum_{l=1}^m (B_\chi^p)_{m,l}^2 = \max_{1 \leq m \leq n} \Theta\left(\log \min\{m, p\} + \frac{\max\{m-p, 0\}}{p}\right) \pm \mathcal{O}(Q)$$

For each of the two norms, the first term has smallest asymptotic growth for  $p \sim n$ , yielding  $\Theta(\log n)$ , and so is  $\Omega(\log n)$  for all choices of  $p$ , thus dominating  $\pm \mathcal{O}(Q)$ . Taking a square-root finishes the proof.  $\square$

1782 **Theorem 3.** *Under the same assumptions on learning rate scheduling  $\chi_t$  as in Theorem 1, the*  
 1783 *following holds.*

$$1785 \quad 1786 \quad 1787 \quad \mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \sqrt{\frac{k}{n} \left( \log p + \frac{p}{b} \right) \sum_{m=1}^n \left[ \chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2 \right]} \right). \quad (23)$$

1788 *Proof.* As shown in the proof of Theorem 1, the condition on  $\chi_t$  is sufficient to enforce  $Q =$   
 1789  $o(\log n)$ , and so  
 1790

$$1792 \quad 1793 \quad 1794 \quad \frac{1}{\sqrt{n}} \|B_\chi^p\|_F = \Theta \left( \sqrt{\frac{1}{n} \sum_{m=1}^n \left[ \chi_m^2 \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \chi_t^2 \right]} \right)$$

1795 from invoking Lemma 20. For the sensitivity  $\text{sens}(C_1^p)$ , we use the following bound from (Kalinin  
 1796 et al., 2025, Theorem 2 proof)  
 1797

$$1798 \quad 1799 \quad 1800 \quad \text{sens}(C_1^p) = \mathcal{O} \left( \sqrt{k \log p + \frac{kp}{b}} \right).$$

1801 Inserting the two bounds into  $\mathcal{E}(B_\chi^p, C_1^p) = \frac{1}{\sqrt{n}} \|B_\chi^p\|_F \cdot \text{sens}(C_1^p)$  gives the statement.  $\square$   
 1802

1803 **Corollary 3.** *Let  $\chi_t = \beta^{\frac{t-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then, in multi-participation with b-min-separation*  
 1804 *and at most  $k = \lceil \frac{n}{b} \rceil$  participations, we have for  $p^* \sim b \log b$  the following optimized upper bound:*  
 1805

$$1806 \quad 1807 \quad 1808 \quad \mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \frac{\sqrt{k \log n + k}}{\sqrt{\log(1/\beta)}} \right). \quad (24)$$

1809 *Proof.* As  $\chi_t$  satisfies the condition of Theorem 3, we have that  
 1810

$$1812 \quad 1813 \quad 1814 \quad \mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \sqrt{\frac{k}{n} \left( \log p + \frac{p}{b} \right) \sum_{m=1}^n \left[ \alpha^{2(m-1)} \log(\min\{m, p\}) + \frac{1}{p} \sum_{t=p}^{m-1} \alpha^{2(t-1)} \right]} \right),$$

1815 where  $\alpha = \beta^{\frac{1}{n-1}}$ . We will evaluate each of the two terms in the outer sum. First off,  
 1816

$$1817 \quad 1818 \quad 1819 \quad \sum_{m=1}^n \alpha^{2(m-1)} \log(\min\{m, p\}) \leq \log p \sum_{m=1}^n \alpha^{2(m-1)} = \Theta \left( \frac{n \log p}{\log(1/\beta)} \right),$$

1820 where the last step follows from the proof of Lemma 11. Proceeding with the second term:  
 1821

$$1822 \quad 1823 \quad 1824 \quad \frac{1}{p} \sum_{m=1}^n \sum_{t=p}^{m-1} \alpha^{2(t-1)} = \frac{1}{p} \sum_{t=p}^{n-1} (n-t) \alpha^{2(t-1)} \leq \frac{n-p}{p} \sum_{t=p}^{n-1} \alpha^{2(t-1)} = \mathcal{O} \left( \frac{n^2}{p \log(1/\beta)} \right),$$

1825 where the last step again uses the proof of Lemma 11. It follows that  
 1826

$$1827 \quad 1828 \quad 1829 \quad \mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \sqrt{\frac{k}{\log(1/\beta)} \left( \log p + \frac{p}{b} \right) \left( \log p + \frac{n}{p} \right)} \right).$$

1830 As this exactly matches the error given in (Kalinin et al., 2025, Theorem 2), up to the  $1/\sqrt{\log(1/\beta)}$   
 1831 factor, the upper bound is minimized for the choice of  $p^* \sim b \log b$  achieving error  
 1832

$$1833 \quad 1834 \quad 1835 \quad \mathcal{E}(B_\chi^p, C_1^p) = \mathcal{O} \left( \frac{\sqrt{k \log n + k}}{\sqrt{\log(1/\beta)}} \right),$$

1836 completing the proof.  $\square$

## 1836 H MULTI-PARTICIPATION: LOWER BOUNDS

1838 **Theorem 4** (Lower bound for multi-participation). *Let  $A_\chi = A_1 D_\chi$ , where  $D_\chi =$   
1839  $\text{diag}(\chi_1, \dots, \chi_n)$  with positive  $\chi_t > 0$ . Assume any factorization  $A_\chi = B \times C$ . Then, in multi-*  
1840 *participation with  $b$ -min-separation and at most  $k = \lceil \frac{n}{b} \rceil$  participations, we have*

$$1842 \quad \mathcal{E}(B, C) \geq \max \left\{ \max_{t \leq n} \frac{\sqrt{k} t \chi_t}{\pi \sqrt{2n}} (\min_{j \leq t} \chi_j) \log(t), \sum_{j=0}^{k-1} \chi_{1+jb} \left(1 - \frac{j}{k-1}\right) \right\}. \quad (25)$$

1845 *Proof.* We start with the first bound, by definition,

$$1847 \quad \mathcal{E}(B, C) = \frac{1}{\sqrt{n}} \|B\|_F \cdot \text{sens}_{k,b}(C). \quad (69)$$

1849 If we restrict to the principal submatrices  $B_{:,t,:}$  and  $C_{:,t,:}$ , then removing the rows can only decrease  
1850 the Frobenius norm, and removing the last  $n - t$  columns can only decrease the sensitivity, since  
1851 any participation pattern for the matrix  $C_{:,t,:}$  would be a valid pattern for the full matrix. Hence

$$1852 \quad \mathcal{E}(B, C) \geq \frac{1}{\sqrt{n}} \|B_{:,t,:}\|_F \cdot \text{sens}_{k,b}(C_{:,t,:}). \quad (70)$$

1854 Following the proof of Lemma 9 in (Kalinin et al., 2025), we have

$$1856 \quad \text{sens}_{k,b}(C_{:,t,:}) \geq \frac{1}{\sqrt{2b}} \|C_{:,t,:}\|_F. \quad (71)$$

1858 Therefore,

$$1859 \quad \mathcal{E}(B, C) \geq \frac{1}{\sqrt{2nb}} \|B_{:,t,:}\|_F \cdot \|C_{:,t,:}\|_F. \quad (72)$$

1861 Applying the Schatten inequality for Frobenius and nuclear norms,

$$1862 \quad \|B_{:,t,:}\|_F \cdot \|C_{:,t,:}\|_F \geq \|(A_\chi)_{:,t,:}\|_*, \quad (73)$$

1863 which gives

$$1865 \quad \mathcal{E}(B, C) \geq \frac{1}{\sqrt{2nb}} \|(A_\chi)_{:,t,:}\|_*. \quad (74)$$

1866 Finally, by Lemma 19,

$$1868 \quad \|(A_\chi)_{:,t,:}\|_* \geq \frac{1}{\pi} (\min_{j \leq t} \chi_j) t \log t, \quad (75)$$

1870 which implies

$$1871 \quad \mathcal{E}(B, C) \geq \max_{t \leq n} \frac{\sqrt{k} t}{\pi \sqrt{2n}} (\min_{j \leq t} \chi_j) \log t. \quad (76)$$

1873 For the second bound, we use the proof of Theorem 1 from Kalinin et al. (2025), which shows that

$$1875 \quad \mathcal{E}(B, C) \geq \frac{1}{\sqrt{n}} \|BC\pi_1\|_2 = \frac{1}{\sqrt{n}} \|A_\chi\pi_1\|_2, \quad (77)$$

1878 where  $\pi_1$  is a vector with ones in positions  $1 + jb$  for  $j \in [0, k-1]$ , and zeros elsewhere. We can  
1879 lower bound the norm explicitly:

$$1881 \quad \frac{1}{\sqrt{n}} \|A_\chi\pi_1\|_2 = \sqrt{\frac{1}{n} \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} \chi_{1+jb} \chi_{1+ib} (n - jb)}$$

$$1882 \quad = \sqrt{\sum_{i=0}^{k-1} \sum_{j=0}^{k-1} \chi_{1+jb} \chi_{1+ib} \left(1 - \frac{j}{n/b}\right)}$$

$$1883 \quad \geq \sum_{j=0}^{k-1} \chi_{1+jb} \left(1 - \frac{j}{n/b}\right) \geq \sum_{j=0}^{k-1} \chi_{1+jb} \left(1 - \frac{j}{k-1}\right),$$

1890 which concludes the proof. □  
 1891  
 1892

1893 **Corollary 4.** *Let  $\chi_k = \beta^{\frac{k-1}{n-1}}$  with  $\beta \in (0, 1/e)$ . Then Theorem 4 yields*

$$1895 \quad 1896 \quad 1897 \quad \mathcal{E}(B, C) = \Omega\left(\frac{\sqrt{k}}{\log(1/\beta)} \log \frac{n}{\log(1/\beta)} + \frac{k}{\log(1/\beta)}\right). \quad (26)$$

1898 *Proof.* We substitute  $\chi_k = \beta^{\frac{k-1}{n-1}}$  in the general lower bound:  
 1899

$$1900 \quad 1901 \quad 1902 \quad 1903 \quad \mathcal{E}(B, C) \geq \max \left\{ \max_{t \leq n} \frac{\sqrt{k} t \chi_t \log(t)}{\pi \sqrt{2n}}, \sum_{j=0}^{k-1} \chi_{1+jb} \left(1 - \frac{j}{k-1}\right) \right\}. \quad (78)$$

1904 For the first term, we substitute  $t = \lceil \frac{n}{\log(1/\beta)} \rceil$ , which gives  $\chi_t = \Theta(1)$ , resulting in  
 1905

$$1906 \quad 1907 \quad 1908 \quad \mathcal{E}(B, C) = \Omega\left(\frac{\sqrt{k}}{\log(1/\beta)} \log \frac{n}{\log(1/\beta)}\right). \quad (79)$$

1909 The second term, we compute explicitly:  
 1910

$$1911 \quad 1912 \quad 1913 \quad \sum_{j=0}^{k-1} \chi_{1+jb} \left(1 - \frac{j}{k-1}\right) = \alpha \frac{\alpha^{bn} + (1 - \alpha^b)n - 1}{(1 - \alpha^b)^2(n-1)}, \quad (80)$$

1914 where  $\alpha = \beta^{1/(n-1)}$ . Asymptotically this is equal to  $\frac{1}{1-\alpha^b}$ , giving the lower bound  
 1915

$$1916 \quad 1917 \quad 1918 \quad \mathcal{E}(B, C) = \Omega\left(\frac{n}{b \log(1/\beta)}\right) = \Omega\left(\frac{k}{\log(1/\beta)}\right). \quad (81)$$

1919 Combining those lower bounds as an average, we conclude the proof. □  
 1920

1921  
 1922  
 1923  
 1924  
 1925  
 1926  
 1927  
 1928  
 1929  
 1930  
 1931  
 1932  
 1933  
 1934  
 1935  
 1936  
 1937  
 1938  
 1939  
 1940  
 1941  
 1942  
 1943