Random Reshuffling is Not Always Better

Christopher De Sa
Department of Computer Science
Cornell University
cdesa@cs.cornell.edu

Abstract

Many learning algorithms, such as stochastic gradient descent, are affected by the order in which training examples are used. It is generally believed that sampling the training examples without-replacement, also known as *random reshuffling*, causes learning algorithms to converge faster. We give a counterexample to the Operator Inequality of Noncommutative Arithmetic and Geometric Means, a longstanding conjecture that relates to the performance of random reshuffling in learning algorithms [19]. We use this to give an example of a learning task and algorithm for which with-replacement random sampling outperforms random reshuffling.

1 Introduction

Many machine learning algorithms work by iteratively updating a model based on one of a number of possible steps. For example, in stochastic gradient descent (SGD), each model update is performed based on a single example selected from a training dataset. The *order* in which the samples are selected—in which the update steps are performed—can have an impact on the convergence rate of the algorithm. There is a general sense in the community that the *random reshuffling* method, which selects the order by without-replacement sampling of the steps in an epoch (where an *epoch* means a single pass through the data, and different epochs may use different random orders), is better (for convergence) than ordinary with-replacement sampling for these algorithms [7, 8, 19].

There are two intuitive reasons why we might expect random reshuffling to outperform sampling with replacement. The first applies when our model updates are in some sense *noisy*: each one could perturb us away from the desired optimum, and they are only guaranteed to approach the optimum *on average*. In this case, random reshuffling ensures that the noise in some sense "cancels out" over an epoch in which all samples are used. Most previous work on random reshuffling has studied this noisy case, and this intuition has been borne out in a series of results that show random-reshuffling results in a convergence rate of $O(1/t^2)$ rather than $O(1/t)$ for convex SGD [8, 10, 16, 18, 20].

The second intuitive reason is that, because sampling without replacement avoids using the same update step repeatedly, it should tend to be "more contractive" than sampling with replacement. This intuition applies even for "noiseless" algorithms that converge at a linear rate of $O(1)^t$. In contrast to the noisy case, the belief that random reshuffling should be better in general for these algorithms that converge at a linear rate is backed up theoretically only with conjectures. The main conjecture in this space is the *Operator Inequality of Noncommutative Arithmetic and Geometric Means*, stated as Conjecture 1 of Recht and Ré [19]. That conjecture, which is motivated by algorithms such as the randomized Kaczmarz method [23] that converge at a linear rate, asserts the following.

Conjecture 1 (Operator Inequality of Noncommutative Arithmetic and Geometric Means)**.** *Let $A_1, \ldots, A_n \in \mathbb{R}^{d\times d}$ be a collection of (symmetric) positive semidefinite matrices. Then it is*

34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada.

conjectured that the following inequalities always hold:

$$\left\| \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \prod_{i=1}^{n} A_{\sigma(i)} \right\| \leq \left\| \left(\frac{1}{n} \sum_{i=1}^{n} A_i \right)^n \right\|, \tag{1}$$

$$\left\| \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\prod_{i=1}^{n} A_{\sigma(i)} \right)^T \left(\prod_{i=1}^{n} A_{\sigma(i)} \right) \right\| \leq \left\| \frac{1}{n^n} \sum_{f \in \{1,\dots,n\}^n} \left(\prod_{i=1}^{n} A_{f(i)} \right)^T \left(\prod_{i=1}^{n} A_{f(i)} \right) \right\|, \tag{2}$$

where $\mathcal{P}(n)$ denotes the set of permutations of the set $\{1, \dots, n\}$ and $\|\cdot\|$ denotes the ℓ_2 induced operator norm (the magnitude of the largest-magnitude eigenvalue for symmetric matrices).

A variant of the conjecture, which moves the sums to the outside of the norms, was given by [7].

Conjecture 2. *Let $A_1, \dots, A_n \in \mathbb{R}^{d \times d}$ be a collection of (symmetric) positive semidefinite matrices. Then it is conjectured that the following inequality always holds:*

$$\frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left\| \prod_{i=1}^{n} A_{\sigma(i)} \right\| \leq \frac{1}{n^n} \sum_{f \in \{1,\dots,n\}^n} \left\| \prod_{i=1}^{n} A_{f(i)} \right\|. \tag{3}$$

Conjecture 1 is a quite natural generalization of the ordinary arithmetic-mean-geometric-mean (AMGM) inequality of real numbers, which states that for non-negative numbers x_i,

$$\textstyle\prod_{i=1}^{n} x_i \leq \left(\frac{1}{n} \sum_{i=1}^{n} x_i \right)^n.$$

In Conjecture 1, positive semidefinite matrices (matrices with non-negative eigenvalues) take the place of the non-negative scalars of the AMGM inequality, and indeed Conjecture 1 reduces to the AMGM inequality when $d = 1$. Conjecture 1 was proven by the original authors in the case of $n = 2$, and has been proven subsequently for $n = 3$ [12, 29]. It also seems to be true for random ensembles of matrices [2, 19], and random testing seems to suggest that Conjecture 1 is always true. However, recent work has shown non-constructively that Conjecture 1 is false [3, 14].[1] These non-constructive disproofs are interesting, but deliver limited insight about random reshuffling, both because they involve complicated proof techniques and because they do not translate to concrete counterexamples of matrices $A_1, A_2, \dots, A_n$ that can be used to study learning algorithms empirically.

In this paper, we propose simple counterexamples for these conjectures—to our knowledge this is the first explicit counterexample known for any of these conjectures, and the first disproof of Conjecture 2. We explore the consequences and limitations of this counterexample throughout the paper, and end by showing concrete problems for which SGD with random reshuffling converges asymptotically slower than SGD using with-replacement sampling. Our paper is structured as follows.

- In Section 2, we construct a family of counterexamples for Conjectures 1 and 2, showing constructively that all three conjectured inequalities are false.
- In Section 3, we adapt the counterexample to give concrete ML algorithms for which with-replacement sampling outperforms without-replacement sampling, contrary to folklore.
- In Section 4, we prove that for non-trivial matrix ensembles (1) always holds with strict inequality for sufficiently small step sizes. Thus, for algorithms with a slowly decreasing step, without-replacement sampling always outperforms with-replacement sampling. On the other hand, we show that when optimal step sizes are chosen separately for with- and without-replacement sampling (but may not decrease to zero), with-replacement sampling can still perform better.
- In Section 5, we give an example convex learning task for which SGD using with-replacement sampling converges asymptotically faster than random-reshuffling.

1.1 Notation

In this paper, $\|\cdot\|$ of a vector always denotes the Euclidean ℓ_2 norm, and $\|\cdot\|$ of an operator denotes the ℓ_2 induced norm. We have $\mathbf{1}$ denote the all-1s vector. We let $\otimes$ denote the Kronecker product and $\oplus$ denote the matrix direct sum, such that $x \oplus y$ is the block diagonal matrix $\left[\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right]$. We let $\mathcal{S}_d$ denote

[1] Lai and Lim [14] can be considered parallel work to this paper.

the set of symmetric $d \times d$ matrices over $\mathbb{R}$, and let $\mathcal{P}_d$ denote the set of symmetric positive definite $d \times d$ matrices. We let $\preceq$ denote inequality with respect to the positive definite ordering (i.e. $A \preceq B$ when $B - A \in \mathcal{P}_d$). When $\mathcal{K} \subset \mathbb{R}^d$ is a convex cone (a set closed under sums and non-negative scalar multiplication), and $x, y \in \mathbb{R}^d$, we say $x \preceq_{\mathcal{K}} y$ if and only if $y - x \in \mathcal{K}$, and for $A, B \in \mathbb{R}^{d \times d}$. We let $M(\mathcal{K})$ denote the set $\{A \in \mathcal{S}_d \mid \forall x \in \mathcal{K},\ Ax \in \mathcal{K}\}$ of matrices that preserve the convex cone $\mathcal{K}$, and we note that $M(\mathcal{K})$ is also a convex cone. For brevity, we let $\mathsf{rr}_k : \mathcal{S}_d \times \mathcal{S}_d \times \cdots \times \mathcal{S}_d \to \mathcal{S}_d$ denote the "random reshuffling" function

$$\mathsf{rr}_k(A_1, A_2, \ldots, A_n) = \tfrac{1}{n!} \textstyle\sum_{\sigma \in \mathcal{P}(n)} \prod_{i=1}^{k} A_{\sigma(i)},$$

and define srr_k similarly as the "symmetric random reshuffling" function

$$\mathsf{srr}_k(A_1, A_2, \ldots, A_n) = \tfrac{1}{n!} \textstyle\sum_{\sigma \in \mathcal{P}(n)} \left(\prod_{i=1}^{k} A_{\sigma(i)}\right)^T \left(\prod_{i=1}^{k} A_{\sigma(i)}\right).$$

Note that this lets us write (1) more compactly as $\|\mathsf{rr}_n(A_1, \ldots)\| \leq \|\mathsf{rr}_1(A_1, \ldots)\|^n$.

1.2 Related Work

Conjecture 1 was a generalization of a line of older work on matrix arithmetic-mean geometric-mean inequalities for two matrices [4, 5]. It was proved by Recht and Ré [19] in the case of $n = 2$ and by Zhang [29] for $n = 3$. Duchi [7] proposed a variant, Conjecture 2, in which the sum appears outside the norm and proved it for $n = 2$, and it was extended to the $n = 3$ case by Israel et al. [12]. Albar et al. [2] proves a version of the inequality of Conjecture 1 that is weaker by a constant. Albar et al. [3] provides a non-constructive disproof of (2), and very recently Lai and Lim [14] gave a non-constructive disproof of (1) via a transformation to the noncommutative Positivstellensatz. Alaifari et al. [1] studies a related class of matrix rearrangement inequalities.

Several prior works have studied SGD on "noisy" learning problems, for which at the optimum w^* it is not the case that $\nabla f_i(w^*) = 0$ for every component loss function f_i. Gürbüzbalaban et al. [8] exhibited an SGD variant for which random reshuffling converges at a $\Theta(1/t^2)$ rate, which improves on the $\Omega(1/t)$ rate of standard with-replacement-sampled SGD; similar results were also proved for the "noisy" case in other settings [10, 20, 22] Ying et al. [25] and Ying et al. [26] show that random reshuffling converges for variance-reduced algorithms, and Ying et al. [27] analyzes random reshuffling in the constant-step-size case. Meng et al. [15] studies a distributed variant of SGD with random shuffling, albeit one different from the one we study here (Algorithm 1). Beyond SGD, Oswald and Zhou [17] analyzes random reshuffling for methods such as Gauss-Seidel and Kaczmarz, and He et al. [11] studies scan order for Gibbs sampling.

2 Constructing a Counterexample

We start by outlining the main idea that underlies our counterexample. Fix some dimension $d \in \mathbb{N}$, and let $n = d$. For any permutation $\sigma \in \mathcal{P}(n)$, let P_σ denote the *permutation matrix* over $\mathbb{R}^n$, such that $(P_\sigma x)_i = x_{\sigma(i)}$ for any vector $x \in \mathbb{R}^n$. The main idea is to construct a sequence of matrices $A_1, A_2, \ldots, A_n$ such that $P_\sigma A_i P_\sigma^T = A_{\sigma(i)}$ for any σ. For any permutation matrix P_ς,

$$\begin{aligned}\mathsf{rr}_k(A_1, A_2, \ldots, A_n) &= \mathsf{rr}_k(P_\varsigma A_1 P_\varsigma^T, P_\varsigma A_2 P_\varsigma^T, \ldots, P_\varsigma A_n P_\varsigma^T) = \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \prod_{i=1}^{k} \left(P_\varsigma A_{\sigma(i)} P_\varsigma^T\right) \\ &= P_\varsigma \left(\tfrac{1}{n!} \textstyle\sum_{\sigma \in \mathcal{P}(n)} \prod_{i=1}^{k} A_{\sigma(i)}\right) P_\varsigma^T = P_\varsigma \left(\mathsf{rr}_k(A_1, A_2, \ldots, A_n)\right) P_\varsigma^T,\end{aligned}$$

where the first equality holds because rr_k is a symmetric function, and the fourth holds because $P_\varsigma^T P_\varsigma = I$. This shows that $\mathsf{rr}_k(A_1, \ldots)$ is preserved by any permutation of its coordinates, and the only such matrices are of the form $X = \alpha \mathbf{1}\mathbf{1}^T + \beta I$, where $\mathbf{1}$ denotes the all-1s vector. With careful choice of the A_i, we can find formulas for α and β, and show that they violate Conjecture 1.

2.1 A Counterexample for the First Inequality

Define a family of vectors y_k for $k \in \{1, \ldots, n\}$ such that for $i \neq k$ we have

$$(y_k)_k = \frac{\sqrt{n-1}}{n} \qquad \text{and} \qquad (y_k)_i = \frac{-1}{n \cdot \sqrt{n-1}}.$$

Consider the matrices $A_k = I + \mathbf{1}y_k^T + y_k\mathbf{1}^T$. For example, when $n = 5$, the matrices look like

$$A_1 = \begin{bmatrix} 1.8 & 0.3 & 0.3 & 0.3 & 0.3 \\ 0.3 & 0.8 & -0.2 & -0.2 & -0.2 \\ 0.3 & -0.2 & 0.8 & -0.2 & -0.2 \\ 0.3 & -0.2 & -0.2 & 0.8 & -0.2 \\ 0.3 & -0.2 & -0.2 & -0.2 & 0.8 \end{bmatrix},\ A_2 = \begin{bmatrix} 0.8 & 0.3 & -0.2 & -0.2 & -0.2 \\ 0.3 & 1.8 & 0.3 & 0.3 & 0.3 \\ -0.2 & 0.3 & 0.8 & -0.2 & -0.2 \\ -0.2 & 0.3 & -0.2 & 0.8 & -0.2 \\ -0.2 & 0.3 & -0.2 & -0.2 & 0.8 \end{bmatrix},\ \dots$$

It is clear by construction that for any $\sigma \in \mathcal{P}(n)$, then $P_\sigma^T A_k P_\sigma = A_{\sigma(k)}$. It is also easily seen that the sum of the y_k is zero, from which we can see immediately that

$$\mathsf{rr}_1(A_1, \dots, A_n) = \frac{1}{n}\sum_{i=1}^n A_i = I + \mathbf{1}\left(\frac{1}{n}\sum_{i=1}^n y_i\right)^T + \left(\frac{1}{n}\sum_{i=1}^n y_i\right)\mathbf{1}^T = I.$$

So, $\|\mathsf{rr}_1(A_1, \dots, A_n)\| = 1$. It is less immediate but still straightforward to show the following.

Statement 1. *If we define λ (for any $k \in \mathbb{N}$) as*

$$\lambda = \left(1 + \frac{1}{n-1}\right)^{k/2} \cdot \cos\left(k \cdot \arcsin\left(\frac{1}{\sqrt{n}}\right)\right),$$

then the random-reshuffled product of these matrices can be written as

$$\mathsf{rr}_k(A_1, \dots, A_n) = \lambda \cdot \frac{\mathbf{1}\mathbf{1}^T}{n} + \left(\frac{\lambda - 1}{n-1} + 1\right)\left(I - \frac{\mathbf{1}\mathbf{1}^T}{n}\right)$$

and so λ will be an eigenvalue of $\mathsf{rr}_n(A_1, \dots, A_n)$ with corresponding eigenvector $\mathbf{1}$.

We include a full derivation of this result—which is relatively easy to derive by hand—in the appendix. It is easy to find n for which $|\lambda|$ is greater than 1. The smallest such n is $n = 5$, where

$$\mathsf{rr}_n(A_1, \dots, A_n) = \frac{29}{64} \cdot \left(I - \frac{\mathbf{1}\mathbf{1}^T}{5}\right) - \frac{19}{16} \cdot \frac{\mathbf{1}\mathbf{1}^T}{5}, \qquad \text{and} \qquad \lambda = \frac{-19}{16}.$$

This fact can be easily verified numerically, by computing rr_n directly for $n = 5$. Note that we can also have $\lambda > 1$, e.g. for $n = 40$, $\lambda \approx 1.655$. This shows directly that (1) is false. Note that while this setup may seem to suggest that a counterexample requires $n = d$ (while usually in linear regression $n \gg d$), it is straightforward to construct examples for which n and d are arbitrary (but no less than 5) by either adding additional I matrices to the ensemble or adding additional dimensions containing only a 1 on the diagonal: this will change the norms of neither the arithmetic nor the geometric mean.

2.2 A Counterexample for the Second Inequality

Using our construction from the previous section, define a collection of positive semidefinite symmetric matrices B_i such that $B_i^2 = A_i$. For these matrices, $\mathsf{srr}_1(B_1, \dots, B_n) = \frac{1}{n}\sum_{i=1}^n B_i^2 = I$, so by induction

$$\frac{1}{n^n}\sum_{(s_1,\dots,s_n)\in\{1,\dots,n\}^n}\left(\prod_{i=1}^n B_{s_i}\right)^T\left(\prod_{i=1}^n B_{s_i}\right) = I.$$

Thus, its norm will be 1. Just as before, these matrices have the property that $P_\sigma B_i P_\sigma^T = B_{\sigma(i)}$ for any σ, so $P_\sigma \mathsf{srr}_n(B_1, \dots) P_\sigma^T = \mathsf{srr}_n(B_1, \dots)$ and the symmetrized random-reshuffled product can also be written as $\alpha\mathbf{1}\mathbf{1}^T + \beta I$. It is possible to perform the same sort of analysis as done in Section 2.1 to find an expression for the eigenvalues of $\mathsf{srr}_n(B_1, \dots)$ explicitly as an analytic expression in n; however, since it is much more complicated and does not deliver additional insight, for lack of space we will just state the result for the particular case of $n = 10$. This case is convenient because $10 - 1 = 3^2$, and so A_i is rational and thus B_i is over $\mathbb{Q}(\sqrt{2})$, and so we can do exact arithmetic easily. In this case, the eigenvalue of $\mathsf{srr}_n(B_1, \dots, B_n)$ with corresponding eigenvector $\mathbf{1}$ is exactly

$$\lambda = \frac{16623165607286458}{16677181699666569} + \frac{2195717144015980}{16677181699666569}\sqrt{2} \approx 1.183,$$

which shows directly that (2) is false, because if it were true this number could be at most 1.

2.3 A Counterexample for the Third Inequality

We can construct a counterexample to Conjecture 2 based on the "tight frame" example of Recht and Ré [19]. The "tight frame" example for $n = 2$ consists of symmetric projection matrices $A_k \in \mathbb{R}^{2\times 2}$ for $k \in \{1, \dots, n\}$ defined as $A_k = u_k u_k^T$, where $u_k = \begin{bmatrix}\cos\left(\frac{\pi k}{n}\right) & \sin\left(\frac{\pi k}{n}\right)\end{bmatrix}^T$. These matrices have the interesting property that their fixed order product $A_1 \cdot A_2 \cdots A_n$ has an asymptotically larger norm than the nth power of their mean, and they are used by Recht and Ré [19] to motivate why symmetrizing the order (by sampling without replacement rather than just going with some arbitrary fixed order) is important.

Starting with this, we construct the family of matrices B_k defined by $B_k = \bigoplus_{\varsigma\in\mathcal{P}(n)} A_{\varsigma(k)}$, where $\bigoplus$ here denotes an indexed matrix direct sum (which constructs a block diagonal matrix). The direct sum has the important properties that $\|X \oplus Y\| = \max(\|X\|, \|Y\|)$ and that (if the dimensions match) $(X_1 \oplus X_2) \cdot (Y_1 \oplus Y_2) = (X_1Y_1) \oplus (X_2Y_2)$. As a consequence, for any permutation σ,

$$\begin{aligned}\left\|\prod_{i=1}^n B_{\sigma(i)}\right\| &= \left\|\prod_{i=1}^n \left(\bigoplus_{\varsigma\in\mathcal{P}(n)} A_{\varsigma(\sigma(i))}\right)\right\| = \left\|\bigoplus_{\varsigma\in\mathcal{P}(n)} \left(\prod_{i=1}^n A_{\varsigma(\sigma(i))}\right)\right\| \\ &= \max_{\varsigma\in\mathcal{P}(n)} \left\|\prod_{i=1}^n A_{\varsigma(\sigma(i))}\right\| = \max_{\varsigma\in\mathcal{P}(n)} \left\|\prod_{i=1}^n A_{\varsigma(i)}\right\| = \left\|\prod_{i=1}^n A_i\right\|,\end{aligned}$$

where the last equality is a known property of the tight frame example, and the other equalities follow from properties of the direct sum. This means that all the terms on the left side of (3) for this example will be the same, and in particular

$$\tfrac{1}{n!}\textstyle\sum_{\sigma\in\mathcal{P}(n)} \left\|\prod_{i=1}^n B_{\sigma(i)}\right\| = \left\|\prod_{i=1}^n A_i\right\|.$$

By a similar argument, the right side of that equation will be

$$\frac{1}{n^n}\sum_{f:\{1,\dots,n\}^n} \left\|\prod_{i=1}^n B_{f(i)}\right\| = \frac{1}{n^n}\sum_{f:\{1,\dots,n\}^n} \max_{\varsigma\in\mathcal{P}(n)} \left\|\prod_{i=1}^n A_{\varsigma(f(i))}\right\|.$$

These formulas make it straightforward to compute these values, even though the matrices in question are of dimension $2 \cdot n!$. For the particular case of $n = 6$,

$$\frac{1}{n!}\sum_{\sigma\in\mathcal{P}(n)} \left\|\prod_{i=1}^n B_{\sigma(i)}\right\| = \frac{9}{32}\sqrt{3} \approx 0.487 \quad \text{and} \quad \frac{1}{n^n}\sum_{f:\{1,\dots,n\}^n} \left\|\prod_{i=1}^n B_{f(i)}\right\| = \frac{26761}{124416} + \frac{29965}{248832}\sqrt{3} \approx 0.424.$$

This is a counterexample to Conjecture 2.

3 A Machine Learning Example

Stochastic gradient descent is perhaps the central example in ML of an algorithm where sample order can affect convergence. Consider the parallel SGD algorithm described in Algorithm 1. Here, for every epoch, each of M parallel workers runs n iterations of SGD, using either with-replacement or without-replacement sampling. Then, the resulting weights are averaged among the workers to produce the starting value for the next epoch. This once-per-epoch averaging in some sense "simulates" the expected value in Conjecture 1, which makes Algorithm 1 a natural SGD-like algorithm to explore with the conjecture.[2] This is equivalent to the method of local SGD with periodic averaging [9, 28] with the averaging period equal to the epoch length. Based on folklore, random reshuffling should outperform standard sampling for this sort of algorithm. We will show that this is not always the case by constructing an example for which standard sampling converges at a linear rate, but random reshuffling fails to converge at all.

Consider the following matrix-completion-like task. We have an unknown rank-1 matrix $X \succeq 0$, and we are given noisy "measurements" from it of the form $u_i^T X v_i \approx a_i$ where we know (u_i, v_i, a_i). We want to recover X by solving the regularized least-squares minimization problem

$$\text{minimize: } \frac{1}{n}\sum_{i=1}^n \left(u_i^T X v_i - a_i\right)^2 + \frac{1}{2}\gamma \cdot \mathbf{tr}\left(X\right) \qquad \text{subject to } X \in \mathcal{P}_d,\ \operatorname{rank}(X) \le 1.$$

[2]Note that the parallelism itself is not necessary here; what is necessary for our purposes is the *averaging*. The averaging is necessary (even for large n) because it models the expected value in the original inequality (1): without it the convergence rate may be effected by higher-order moments (not just the expected value). We study parallel SGD because it is a "real" method from the literature that uses averaging [9, 28].

Algorithm 1 Parallel SGD

given: n loss functions f_i, step size scheme $\alpha_1, \alpha_2, \ldots$, initial state $w_0 \in \mathbb{R}^d$
given: number of epochs K, parallel machines M, replacement policy RP
for $k = 1$ **to** K **do**
  for all $m \in \{1, \ldots, M\}$ **do in parallel on machine** m
    $u_{k,m,0} \leftarrow w_{k-1}$
    if RP $=$ `with-replacement` **a.k.a** `standard sampling` **then**
      sample $\sigma_{k,m}$ uniformly from the set of functions from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$
    else if RP $=$ `without-replacement` **a.k.a** `random reshuffling` **then**
      sample $\sigma_{k,m}$ uniformly from $\mathcal{P}(n)$
    for $t = 1$ **to** n **do**
      $u_{k,m,t} \leftarrow u_{k,m,t-1} - \alpha_k \nabla f_{\sigma_{k,m}(t)}\left(u_{k,m,t-1}\right)$
  average $w_k \leftarrow \frac{1}{M}\sum_{m=1}^{M} u_{k,m,n}$
return w_K

To solve this more efficiently, we apply Algorithm 1 to a quadratic factorization [6] $X = yy^T$, a common technique which results in the equivalent unconstrained problem

$$\text{minimize: } f(y) = \frac{1}{n}\sum_{i=1}^{n} f_i(y) = \frac{1}{n}\sum_{i=1}^{n}\left(u_i^T y y^T v_i - a_i\right)^2 + \frac{1}{2}\gamma\left\|y\right\|^2 \qquad \text{subject to: } y \in \mathbb{R}^d.$$

We are now going to pick a particular dataset of (u_i, v_i, a_i) such that the global optimum of f is at $y = 0$, and where nearby $y = 0$, Algorithm 1 behaves like our counterexample of Section 2. To do this, notice that nearby $y = 0$,

$$\begin{aligned} I - \alpha\nabla f_i(y) &= \left((1-\alpha\gamma I) - 2\alpha\left(u_i^T y y^T v_i - a_i\right)\left(v_i u_i^T + u_i v_i^T\right)\right) y \\ &= \left((1-\alpha\gamma I) + 2\alpha a_i\left(v_i u_i^T + u_i v_i^T\right)\right) y + \mathcal{O}(y^3). \end{aligned}$$

So, if we choose α, γ, a_i, v_i, and u_i such that $(1-\alpha\gamma I) + 2\alpha a_i\left(v_i u_i^T + u_i v_i^T\right) = (1-\alpha\gamma)A_i$ where this A_i is from our counterexample of Section 2, then when the algorithm is sufficiently close to $y = 0$, applying an iteration of SGD will behave like multiplying by a single matrix A_i, and averaging across multiple parallel workers will concentrate around the expected value over the sampled scan order. Concretely, we pick $n = 40$, a constant step size $\alpha = 0.1$, $\gamma = 0.05$, $M = 1000$, $K = 100$, $u_i = \mathbf{1}$, $v_i = y_i$ (the y_i of Section 2), and $a_i = \frac{1-\alpha\gamma}{2\alpha}$; we initialize w_0 randomly such that $\|w_0\| = 1$. It is easy to see that the global optimum of this task is at $w^* = 0$, and it has no other stationary points. Note that this is not necessarily a very realistic setting (the number of parallel workers is large and the dataset is relatively small): the artificial setting is chosen to make the comparison stand out clearly. Running Algorithm 1 on this example produces the results shown in Figure 1. This shows empirically that, counter-intuitively, standard with-replacement random sampling can outperform random reshuffling for this algorithm.

4 Taking Step Size into Account

Many algorithms, including SGD, use a step size or learning rate that often decreases over time. Much of the previous work on random reshuffling has been done in such cases [8, 10, 20]. In this section, we develop a variant of Conjecture 1 that incorporates a step size, and prove that statement must hold true for sufficiently small step sizes. Our step-size-incorporating variant of Conjecture 1 is based on the following intuition. For a smooth objective, for w close to the optimum w^* where $\nabla f_i(w^*) = 0$,

$$w - \alpha\nabla f_i(w) \approx (I - \alpha\nabla^2 f_i(w))(w - w^*) + w^*;$$

for a quadratic function f_i, this approximation is exact. So we can model SGD with step size α by allowing the matrices A_i in Conjecture 1 to vary as a function of a step size α. We prove the following theorem about this modified inequality.

Theorem 1 (Matrix AMGM Inequality, Sufficiently Small Step Size)**.** *Let $A_1, \ldots, A_n$ be a collection of continuously twice-differentiable functions from $\mathbb{R}_+$ to $\mathcal{S}_d$, that all satisfy $A_i(0) = I$ and that are non-trivial in the sense that they have no eigenvalue/eigenvector pairs shared among all the matrices*

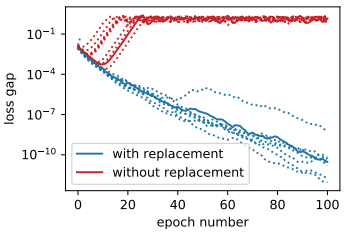

Figure 1: Loss gap of multiple random runs of Algorithm 1 on task of Section 3. Notice that random reshuffling fails to converge to the minimal loss.

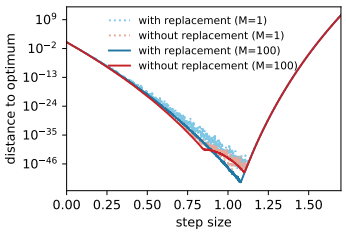

Figure 2: Distance to optimum of Algorithm 1 for task of Section 4 after $K = 20$ epochs. Light dotted series indicate non-parallel SGD ($M = 1$).

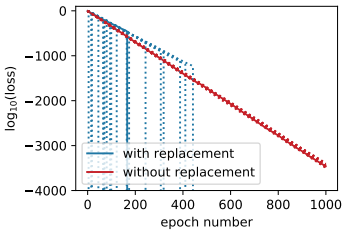

Figure 3: Asymptotic convergence of SGD using with- and without-replacement sampling for multiple trials on the example of Section 5.

$A_1'(0), A_2'(0), \ldots, A_n'(0)$. *Then for any* $2 \le k \le n$, *there exists an* $\alpha_{\max} > 0$ *and a constant* $C > 0$ *such that such that for all* $0 < \alpha \le \alpha_{\max}$,

$$\|\mathsf{rr}_k(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))\| < \|\mathsf{rr}_1(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))\|^k - \alpha^2 C.$$

The proof of Theorem 1 is a straightforward combination of the following two lemmas. The main idea is that we can expand the rr_k expression approximately as a polynomial in α, and then consider only the dominant quadratic α^2 term, which we can bound directly. We defer the proof of the theorem and both lemmas to the appendix.

Lemma 1 (Binomial Theorem for Random Reshuffling)**.** *For any symmetric matrices* $X_1, \ldots, X_n$, *and any constants* α *and* β,

$$\mathsf{rr}_k(\alpha I + \beta X_1, \alpha I + \beta X_2, \ldots, \alpha I + \beta X_n) = \textstyle\sum_{i=0}^{k} \binom{k}{i} \alpha^{k-i} \beta^k \mathsf{rr}_i(X_1, X_2, \ldots, X_n).$$

Lemma 2. *For any symmetric matrices* $X_1, \ldots, X_n \in \mathbb{R}^d$, *and for any* $u \in \mathbb{R}^d$ *such that* $\|u\| = 1$,

$$u^T \left(\mathsf{rr}_2(X_1, \ldots, X_n)\right) u \le \|\mathsf{rr}_1(X_1, \ldots, X_n)\|^2$$

and equality can hold only if there exists a $\lambda \in \mathbb{R}$ *such that for all* $i \in \{1, \ldots, n\}$, u *is an eigenvector of* X_i *with eigenvalue* λ, *that is* $X_i u = \lambda u$.

We can use Theorem 1 to show that random reshuffling must outperform standard with-replacement sampling for slowly decaying step size schemes for noiseless convex quadratic problems, which can be thought of as a simplified model for optimization problems satisfying the strong growth condition of Schmidt and Roux [21]. Specifically, we study the following simplified class of problems.

Definition 1. We say that a set of loss functions $f_1, \ldots, f_n$ is a *noiseless convex quadratic problem* if the following conditions hold.

- **(Noiselessness.)** There exists a unique $w^* \in \mathbb{R}^d$ such that for all i, $\nabla f_i(w^*) = 0$.
- **(Convex quadratics.)** Each loss function f_i is a convex quadratic $f_i(w) = w^T H_i w/2 + b_i^T w$.
- **(Lipschitz gradients.)** For some L, each loss function f_i satisfies $\nabla^2 f_i(w) \preceq LI$.

Additionally, we say that the problem is *non-trivial* if the Hessian matrices $H_i = \nabla^2 f_i(w^*)$ share no eigenvalue/eigenvector pairs, i.e. there is no (λ, u) with $u \neq 0$ such that for all i, $H_i u = \lambda u$.

Note that the last condition here is designed to rule out trivial cases such as all the loss functions f_i being the same. Such trivial cases only happen on a set of measure 0 within the space of all possible loss functions $f_1, \ldots, f_n$ and initializations, so it is reasonable for us to exclude them. The class of problems described by Definition 1 includes the setting of the Randomized Kaczmarz method originally studied in Recht and Ré [19], as well as well-known tasks such as linear regression and ridge regression.

Theorem 1 now directly implies the following useful corollary, which says that without-replacement sampling outperforms with-replacement sampling whenever a diminishing but not square-summable step size scheme is used—including for the important case of $M = 1$ in Algorithm 1, which corresponds to the most common case of ordinary single-worker SGD.[3]

[3]Note also that it should be straightforward to extend Corollary 1 to the case of "nice" convex losses, on the basis of the idea that any such functions must behave like quadratics locally in the neighborhood of w^*. But since this is not deliver any new insight, we do not present such a result here.

Corollary 1. *Consider Algorithm 1 on a non-trivial noiseless convex quadratic (using any M). Suppose that the step size scheme satisfies $0 < \alpha_i L < 1$ and is diminishing but not square-summable, i.e. $\lim_{k\to\infty} \alpha_k = 0$ and $\sum_{k=1}^{\infty} \alpha_k^2 = \infty$. Then for almost all initial values $w_0 \neq w^*$,*

$$\lim_{k\to\infty} \frac{\left\|\mathbf{E}[w_{k,\texttt{without-replacement}}] - w^*\right\|}{\left\|\mathbf{E}[w_{k,\texttt{with-replacement}}] - w^*\right\|} = 0.$$

Although it seems that Theorem 1 and Corollary 1 suggests that random reshuffling *is* indeed better when we allow the use of small step sizes, it has a significant limitation that would make that conclusion invalid: Corollary 1 only compares with-replacement and without-replacement sampling *using the same learning rate scheme for both*. Instead, when comparing two algorithms in the most fair way, we should select the best learning rate scheme for each algorithm individually. Surprisingly, when we allow this, we can give an example of a convex learning task for which with-replacement sampling, with a particular constant step size, converges faster than without-replacement sampling no matter what fixed step size scheme it uses.

The convex functions in question can be constructed directly from our counterexample of Section 2. Let $f_i(w) = \frac{1}{2} w^T H_i w$, where $H_i = \left(I - \frac{1}{2} A_i\right) \oplus \frac{1}{2} \oplus \frac{3}{2}$, where $\oplus$ denotes the matrix direct sum (such that $X \oplus Y$ is a block diagonal matrix with diagonal blocks X and Y). This function must be convex because H_i is positive semidefinite (which follows from the fact that the eigenvalues of A_i are 0, 1, and 2). The main idea of this construction is to "force" the step size to be $\alpha = 1$, since otherwise either the $1/2$ or $3/2$ coordinate will end up converging at a suboptimal rate. Although a theoretical analysis of this would be straightforward, as such analysis delivers no new insight, we only validate that this example works empirically on a concrete example. We pick $n = 8$, $M = 100$, and $K = 20$, and we initialize w_0 from a Gaussian with less power on the last two coordinates, which makes the effect more visible. In Figure 2 we plot the distance to optimum after K epochs for all step sizes $\alpha \in \{0, 0.001, 0.002, \ldots, 1.7\}$. Observe that while for smaller step sizes, random-reshuffling outperforms standard sampling—which validates Theorem 1—the best convergence overall is achieved by standard with-replacement sampling. Interestingly, the averaging of Algorithm 1 is necessary for this effect to happen for this task: in Figure 2 we also display results for standard SGD on the same problem (equivalent to setting $M = 1$) for which without-replacement sampling seems to consistently outperform with-replacement sampling.

5 Random Reshuffling Can be Worse Asymptotically Even for SGD

While we have shown Conjecture 1 is false, this does not necessarily imply random reshuffling can be worse with stochastic gradient descent, because the averaging present in Conjecture 1 is not present in plain SGD. Our counterexamples so far do *not* show random reshuffling performing worse with no averaging (Figure 2), so it remains consistent with our observations so far that random reshuffling *could* always outperform with-replacement sampling for SGD. But is this necessarily true?

In this section we will show that it is not: even for SGD without any averaging (Algorithm 1 with $m = 1$), we can construct a learning task for which with-replacement sampling converges strictly faster than random reshuffling—albeit one not based on a counterexample to any of the conjectures we have studied. Here, when we say it converges "strictly faster," we mean that for any coupling of the two algorithms, with-replacement sampling almost surely eventually achieves lower loss than random reshuffling and its loss remains lower for all time. The main idea behind this construction, which is based on the idea that any rank-deficient square matrix can be written as the product of three symmetric positive semidefinite matrices [24], is as follows. Consider the matrices

$$A_1 = \frac{1}{4}\begin{bmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -1 & 1 \end{bmatrix},\ A_2 = \frac{1}{4}\begin{bmatrix} 2 & 0 & -1 \\ 0 & 1 & 1 \\ -1 & 1 & 2 \end{bmatrix},\ A_3 = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 2 \end{bmatrix}, \text{ and } R = \frac{uu^T}{6} \text{ where } u = \begin{bmatrix} 1 \\ -2 \\ -1 \end{bmatrix}.$$

It is easy to check that all these matrices are symmetric and positive semidefinite (and $\preceq I$), and that $(A_1 A_2 A_3)^3 = 0$. Now, consider the behavior of SGD with step size $\alpha = 1/2$ on the problem where

$$f_1(w) = w^T(I - A_1)w,\ \ f_2(w) = w^T(I - A_2)w,\ \ f_3(w) = w^T(I - A_3)w,\ \ f_4(w) = w^T(I - R)w.$$

Observe that all these functions are convex, and that choosing to do a step with f_1 has the effect of multiplying w by A_1, etc. This means that, for with-replacement sampling, if we sample our examples in the order $(1, 2, 3, 1, 2, 3, 1, 2, 3)$, the result after running those SGD steps will be to have

$w = 0$, *regardless of what value of* w *we started with* (because $(A_1 A_2 A_3)^3 = 0$). Since we are guaranteed to sample that run of examples eventually, it follows that almost surely, after some finite amount of time with-replacement SGD achieves $w_t = 0 = w^*$, which minimizes the loss.

On the other hand, this sequence of samples can not occur for sampling without replacement. Instead, every epoch of SGD will contain an R, which "disrupts" the sequence. The sequence of matrices that are multiplied by w will consist of sequences of A_i matrices of length no more than 6 broken up by R matrices. Because of the structure of R, for any matrix X, $6RXR = R \cdot u^T Xu$: this means that the sequences of matrices $RA_\star \cdots A_\star R$ will reduce to the product of scalars $u^T A_\star \cdots A_\star u$. It is straightforward to verify numerically that this scalar is nonzero for any sequence of $A_\star$ matrices that can occur for sampling without replacement. So, for almost all initializations w_0, SGD with random reshuffling on this task *will never reach 0*, while SGD using with-replacement sampling is guaranteed to reach 0 in finite time. We conclude that with-replacement sampling converges asymptotically faster than random reshuffling for this task and step size.

In fact, we can say something even more general: among all step sizes α that satisfy $\alpha L \leq 1$, where L is the smallest constant such that each f_i is has L-Lipschitz gradients, SGD with $\alpha = 1/2$ using with-replacement sampling converges asymptotically faster than all other settings. That is, here with-replacement sampling is still converging asymptotically faster, even if we choose the optimal learning rates for both sampling strategies separately. We can see that this holds immediately from the fact that for $0 < \alpha < 1$, taking a step with respect to f_i has the effect of multiplying w by a full-rank matrix; such a step can never reach 0.

We explore this task empirically in Figure 3, where we ran a thousand epochs of SGD using both with- and without-replacement sampling on the example task we constructed in this section. Observe that for every run (we ran 20 independent runs), with-replacement sampling starts off a little worse, but quickly moves to zero loss, while without-replacement sampling continues to have nonzero loss for all time. Note that we needed to use exact arithmetic and look at points *very* close to the optimum for this effect to be observable: the figure ranges down to losses of 10^{-4000}. Although not practical, this experiment does conclusively illustrate empirically that it is possible for with-replacement SGD to converge asymptotically faster than random-reshuffling, even when no averaging is used and when step sizes are chosen optimally for both algorithms.[4] In future work, it may be interesting to study whether and to what extent this sort of effect can occur in real learning tasks.

6 Conclusion

In this paper, we compared random reshuffling to with-replacement sampling for stochastic learning algorithms on noiseless problems. We found a counterexample to two longstanding conjectures from the literature (Conjectures 1 and 2) that would have implied random reshuffling is always no worse for many learning algorithms. Using this counterexample, we constructed concrete learning tasks for which with-replacement sampling outperforms without-replacement sampling in a way that can be observed empirically, even when step size is allowed to vary. This shows that, contrary to folklore, random-reshuffling *can* actually cause learning algorithms to converge asymptotically slower than with-replacement sampling on a particular problem. New insights will be required to develop theory that gets around our counterexamples to explain why random-reshuffling appears to consistently perform better on individual tasks in practice—even for noiseless problems. We hope that this work will bring us closer to a deeper understanding of the effect of scan order in machine learning.

Broader Impact

We expect that the counterexamples presented in this work will have an impact on the ML theory community as we further try to understand the effect of scan order in large-scale optimization. We hope that these counterexamples will help guide future researchers towards proving more variants of Conjectures 1 and 2 that are true. Beyond this impact on the ML community, this work is primarily theoretical and does not present any foreseeable societal consequence.

[4] Observe that this example could also be applied to a "noisy" dataset case with SVRG [13], showing that the phenomenon of random reshuffling sometimes being worse is limited neither to SGD nor to noisy datasets. Since the transformation is straightforward it is left as an exercise for the reader.

Funding Disclosure

No external funding (apart from usual faculty support by Cornell University) was used in support of this work. The author has an engagement with SambaNova Systems, but funding from SambaNova was not used to directly support this work.

References

[1] Rima Alaifari, Xiuyuan Cheng, Lillian B Pierce, and Stefan Steinerberger. On matrix rearrangement inequalities. *arXiv preprint arXiv:1904.05239*, 2019.

[2] Wafaa Albar, Marius Junge, and Mingyu Zhao. Noncommutative versions of the arithmetic-geometric mean inequality. *arXiv preprint arXiv:1703.00546*, 2017.

[3] Wafaa Albar, Marius Junge, and Mingyu Zhao. On the symmetrized arithmetic-geometric mean inequality for operators. *arXiv preprint arXiv:1803.02435*, 2018.

[4] Rajendra Bhatia and Priyanka Grover. Norm inequalities related to the matrix geometric mean. *Linear Algebra and its Applications*, 437(2):726–733, 2012.

[5] Rajendra Bhatia and Fuad Kittaneh. The matrix arithmetic–geometric mean inequality revisited. *Linear Algebra and its Applications*, 428(8-9):2177–2191, 2008.

[6] Samuel Burer and Renato DC Monteiro. A nonlinear programming algorithm for solving semidefinite programs via low-rank factorization. *Mathematical Programming*, 95(2):329–357, 2003.

[7] John C Duchi. Commentary on "Towards a noncommutative arithmetic-geometric mean inequality" by B. Recht and C. Ré. *Ré. J. Mach. Learn. Res*, 23:11–25, 2012.

[8] Mert Gürbüzbalaban, Asu Ozdaglar, and Pablo Parrilo. Why random reshuffling beats stochastic gradient descent. *Mathematical Programming*, 2019.

[9] Farzin Haddadpour, Mohammad Mahdi Kamani, Mehrdad Mahdavi, and Viveck Cadambe. Local sgd with periodic averaging: Tighter analysis and adaptive synchronization. In *Advances in Neural Information Processing Systems*, pages 11080–11092, 2019.

[10] Jeffery Z HaoChen and Suvrit Sra. Random shuffling beats sgd after finite epochs. *arXiv preprint arXiv:1806.10077*, 2018.

[11] Bryan He, Christopher De Sa, Ioannis Mitliagkas, and Christopher Ré. Scan order in Gibbs sampling: Models in which it matters and bounds on how much. *NIPS*, 2016.

[12] Arie Israel, Felix Krahmer, and Rachel Ward. An arithmetic–geometric mean inequality for products of three matrices. *Linear Algebra and its Applications*, 488:1–12, 2016.

[13] Rie Johnson and Tong Zhang. Accelerating stochastic gradient descent using predictive variance reduction. In *Advances in neural information processing systems*, pages 315–323, 2013.

[14] Zehua Lai and Lek-Heng Lim. Recht-ré noncommutative arithmetic-geometric mean conjecture is false. *ICML*, 2020.

[15] Qi Meng, Wei Chen, Yue Wang, Zhi-Ming Ma, and Tie-Yan Liu. Convergence analysis of distributed stochastic gradient descent with shuffling. *Neurocomputing*, 337:46–57, 2019.

[16] Dheeraj Nagaraj, Prateek Jain, and Praneeth Netrapalli. SGD without replacement: Sharper rates for general smooth convex functions. volume 97 of *Proceedings of Machine Learning Research*, pages 4703–4711, Long Beach, California, USA, 09–15 Jun 2019. PMLR. URL `http://proceedings.mlr.press/v97/nagaraj19a.html`.

[17] Peter Oswald and Weiqi Zhou. Random reordering in sor-type methods. *Numerische Mathematik*, 135(4):1207–1220, 2017.

[18] Shashank Rajput, Anant Gupta, and Dimitris Papailiopoulos. Closing the convergence gap of sgd without replacement. *arXiv preprint arXiv:2002.10400*, 2020.

[19] Benjamin Recht and Christopher Ré. Toward a noncommutative arithmetic-geometric mean inequality: conjectures, case-studies, and consequences. In *Conference on Learning Theory*, pages 11–1, 2012.

[20] Itay Safran and Ohad Shamir. How good is sgd with random shuffling? *arXiv preprint arXiv:1908.00045*, 2019.

[21] Mark Schmidt and Nicolas Le Roux. Fast convergence of stochastic gradient descent under a strong growth condition. *arXiv preprint arXiv:1308.6370*, 2013.

[22] Ohad Shamir. Without-replacement sampling for stochastic gradient methods. In *Advances in neural information processing systems*, pages 46–54, 2016.

[23] Thomas Strohmer and Roman Vershynin. A randomized kaczmarz algorithm with exponential convergence. *Journal of Fourier Analysis and Applications*, 15(2):262, 2009.

[24] Pei Yuan Wu. Products of positive semidefinite matrices. *Linear Algebra and Its Applications*, 111:53–61, 1988.

[25] Bicheng Ying, Kun Yuan, and Ali H Sayed. Convergence of variance-reduced stochastic learning under random reshuffling. *arXiv preprint arXiv:1708.01383*, 2(3):6, 2017.

[26] Bicheng Ying, Kun Yuan, and Ali H Sayed. Variance-reduced stochastic learning under random reshuffling. *arXiv preprint arXiv:1708.01383*, 2017.

[27] Bicheng Ying, Kun Yuan, Stefan Vlaski, and Ali H Sayed. On the performance of random reshuffling in stochastic learning. In *2017 Information Theory and Applications Workshop (ITA)*, pages 1–5. IEEE, 2017.

[28] Jian Zhang, Christopher De Sa, Ioannis Mitliagkas, and Christopher Ré. Parallel SGD: When does averaging help? *OptML: Optimization Methods for the Next Generation of Machine Learning*, 2016.

[29] Teng Zhang. A note on the non-commutative arithmetic-geometric mean inequality. *arXiv preprint arXiv:1411.5058*, 2014.

A Additional Results

In this section, we present additional results that we believe are interesting, but that the main body of the paper was too short to contain.

A.1 Violating the Conjecture by a Larger Margin

The expression in Section 2.1 makes it seem that our counterexample can violate Conjecture 1 only by at most a factor of $\exp(1/2)$, since this is an upper bound on the magnitude of λ. However, it is straightforward to use the counterexample to construct violations by an arbitrary factor. If we start with a sequence of n matrices $A_1, \ldots, A_n \in \mathbb{R}^d$, we can use the Kronecker product to construct a sequence of $2n$ matrices in $\mathbb{R}^{d^2}$ as $A_1 \otimes I, A_2 \otimes I, \ldots, A_n \otimes I, I \otimes A_1, \ldots, I \otimes A_n$. In this case,

$$\mathsf{rr}_{2n}\left(A_1 \otimes I, A_2 \otimes I, \ldots, A_n \otimes I, I \otimes A_1, \ldots, I \otimes A_n\right) = \mathsf{rr}_n\left(A_1, \ldots, A_n\right) \otimes \mathsf{rr}_n\left(A_1, \ldots, A_n\right),$$

and so its norm will be

$$\left\|\mathsf{rr}_{2n}\left(A_1 \otimes I, A_2 \otimes I, \ldots, A_n \otimes I, I \otimes A_1, \ldots, I \otimes A_n\right)\right\| = \left\|\mathsf{rr}_n\left(A_1, \ldots, A_n\right)\right\|^2$$

and similarly for $\mathsf{srr}_{2n}(\cdots)$. On the other hand, the arithmetic means (rr_1 and srr_1, respectively) of these matrices will still be the identity matrix I. This sort of construction can be used to produce matrix ensembles that violate the inequalities of Conjecture 1 by arbitrarily large factors. Starting from the case of $n = 5$ of Section 2.1, we can show that for any $q \in \mathbb{N}$, there exists an ensemble of $n = 5q$ matrices $C_1, \ldots, C_n$ in dimension $d = 5^q$ such that

$$\|\mathsf{rr}_n(C_1, \ldots, C_n)\| = (19/16)^q \approx (1.035)^n \qquad \text{but} \qquad \mathsf{rr}_1(C_1, \ldots, C_n) = I.$$

Similarly, there exists an ensemble of $n = 10q$ matrices $C_1, \ldots, C_n$ in dimension $d = 10^q$ such that

$$\|\mathsf{srr}_n(C_1, \ldots, C_n)\| \approx (1.183)^q \approx (1.017)^n \qquad \text{but} \qquad \mathsf{srr}_1(C_1, \ldots, C_n) = I.$$

This places a non-trivial lower bound on any "loose" version of Conjecture 1. Note that Albar et al. [2] proved the dimension-free bound $\|\mathsf{rr}_n(A_1, \ldots, A_n)\| \leq n^n \cdot \|\mathsf{rr}_1(A_1, \ldots, A_n)\|^n$. Our lower bound here shows that this constant n^n could only at best be improved to $O(1)^n$.

B Another Example: Markov chain Monte Carlo

In the main body of the text, we presented examples of learning tasks that were based on stochastic gradient descent. Another common class of ML algorithms where scan order matters is Markov chain Monte Carlo. Suppose that we have some unknown distribution π over some sample space Ω we wish to sample from, and $P_1, P_2, \ldots, P_n$ are Markov transition operators each of which is reversible and has stationary distribution π (but which are not necessarily ergodic). The classic example of this sort of setup is *Gibbs sampling*, in which each operator P_i corresponds to the action of resampling a single variable from a joint distribution π conditioned on the values of the other variables.

We consider two different ways of combining the individual transition operators into a single compound operator. *With-replacement* scan involves running n inner iterations, where at each iteration the algorithm chooses a transition operator from $P_1, \ldots, P_n$ with replacement, then transitions the state according to that operator. We denote this compound operator P_{with}. *Without-replacement* scan does the same thing, but samples without replacement. We denote this compound operator P_{without}. Note that

$$P_{\text{with}} = \left(\frac{1}{n}\sum_{i=1}^{n} P_i\right)^n \qquad \text{and} \qquad P_{\text{without}} = \frac{1}{n!}\sum_{\sigma \in \mathcal{P}(n)} \prod_{i=1}^{n} P_{\sigma(i)},$$

from which we can see the connection to Conjecture 1.

It is natural to ask the question: how fast do these algorithms converge? The standard way to measure this is with the standard *total variation distance* from stationarity after t steps, which is the maximum over all possible initial states of the total variation distance between the distribution of the Markov chain after t steps and its stationary distribution. That is,

$$d(P, t) = \max_{x \in \Omega} \left\|P^t(x, \cdot) - \pi\right\|_{\text{TV}} = \max_{x \in \Omega} \frac{1}{2}\sum_{y \in \Omega} \left|P^t(x, y) - \pi(y)\right|.$$

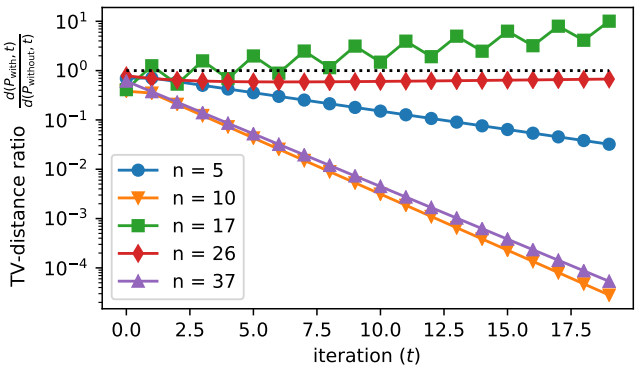

Figure 4: Distance-to-stationarity ratio of with-replacement versus without-replacement scan order for our constructed MCMC task. Notice that the without-replacement algorithm converges at a faster rate than the with-replacement algorithm for most values of n.

It would be intuitive to conjecture that it always holds (at least for sufficiently large t) that random reshuffling converges faster than standard with-replacement random sampling of the P_i, that is,

$$d\left(P_{\text{without}}, t\right) \leq d\left(P_{\text{with}}, t\right). \tag{4}$$

However, here we show that this is not necessarily always the case, by adapting our counterexample from Section 2. Consider the matrices

$$P_i = \frac{1}{2n \cdot (A_i)_{ii}} \cdot A_i \otimes \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \frac{1}{2n} \cdot \mathbf{1}\mathbf{1}^T.$$

Notice that, since $(A_i)_{ii}$ is the largest-magnitude entry of A_i, this matrix is guaranteed to be non-negative, and since

$$P_i\mathbf{1} = \frac{1}{2n \cdot (A_i)_{ii}} \cdot (A_i\mathbf{1}) \otimes \left(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \mathbf{1} \right) + \frac{1}{2n} \cdot \mathbf{1}\mathbf{1}^T\mathbf{1} = \frac{1}{2n \cdot (A_i)_{ii}} \cdot (A_i\mathbf{1}) \otimes (0) + \frac{1}{2n} \cdot \mathbf{1} \cdot 2n = \mathbf{1},$$

it is a stochastic matrix (and so it is a Markov operator over a state space of size $2n$). Additionally, since P_i is symmetric (by construction, since the Kronecker product of symmetric matrices is symmetric), it follows that each P_i must be reversible with stationary distribution $\pi = \frac{\mathbf{1}}{2n}$. When $n-1$ is a perfect square, A_i is rational, and so it is straightforward to compute the compound operators P_{with} and P_{without} directly in exact arithmetic. We did this and computed the distances to stationarity $d\left(P_{\text{without}}, t\right)$ and $d\left(P_{\text{with}}, t\right)$ for $n \in \{5, 10, 17, 26, 37\}$ and for $T = 20$ total outer iterations. Figure 4 plots the ratio of these distances to stationarity. Notice that if (4) were true, we would expect these series to all lie above the dotted black line, at least for sufficiently large t. This shows that random reshuffling *can* converge more slowly than standard with-replacement random sampling, even for Markov chain Monte Carlo.

We should note here that our example is extremely artificial for MCMC, especially because both the with-replacement and without-replacement chains converge *very* fast. In practice even one iteration of either the with-replacement or without-replacement chains would produce estimates that are more than accurate enough. It is possible—even likely—that some analogue of the random-reshuffling-is-better conjecture holds for MCMC methods under more typical conditions, such as Gibbs sampling.

C Derivation of Section 2.1

In this section, we provide the derivation for Statement 1, the formula for the random-reshuffled product of our counterexample matrices.

We first state without proof the following facts about the vectors y_i, which can be easily checked.

$$\begin{aligned}
\mathbf{1}^T y_i &= 0, \\
y_i^T y_j &= \frac{-1}{n(n-1)}, \\
\sum_{i=1}^{n} y_i &= 0, \qquad \text{and} \\
\sum_{i \neq j} y_i y_j^T = -\sum_{i=1}^{n} y_i y_i^T &= \frac{1}{n(n-1)} \mathbf{1}\mathbf{1}^T - \frac{1}{n-1} I.
\end{aligned}$$

Starting from the matrix family as defined in Section 2.1, for any permutation σ and for any $k > 0$, the product of an even number of the permuted matrices $A_k - I$ can be written as

$$\begin{aligned}
\prod_{i=1}^{2k} \left(A_{\sigma(i)} - I\right) &= \prod_{i=1}^{2k} \left(\mathbf{1} y_i^T + y_i \mathbf{1}^T\right) \\
&= \left(\frac{-1}{n(n-1)}\right)^k \cdot n^{k-1} \mathbf{1}\mathbf{1}^T + \left(\frac{-1}{n(n-1)}\right)^{k-1} n^k y_{\sigma(1)} y_{\sigma(2k)}^T \\
&= \left(\frac{-1}{n-1}\right)^k \left(\frac{\mathbf{1}\mathbf{1}^T}{n} - n(n-1) \cdot y_{\sigma(1)} y_{\sigma(2k)}^T\right),
\end{aligned}$$

and similarly for an odd number of matrices

$$\prod_{i=1}^{2k-1} \left(A_{\sigma(i)} - I\right) = \left(\frac{-1}{n-1}\right)^{k-1} \left(\mathbf{1} y_{\sigma(2k-1)}^T + y_{\sigma(1)} \mathbf{1}^T\right)$$

because there are only two "paths" through the product since any $\mathbf{1}^T y_i = 0$. Therefore,

$$\begin{aligned}
\mathsf{rr}_{2k-1}(A_1 - I, \ldots, A_n - I) &= \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{-1}{n-1}\right)^{k-1} \left(\mathbf{1} y_{\sigma(2k-1)}^T + y_{\sigma(1)} \mathbf{1}^T\right) \\
&= \left(\frac{-1}{n-1}\right)^{k-1} \left(\mathbf{1} \left(\frac{1}{n} \sum_{i=1}^{n} y_i\right)^T + \left(\frac{1}{n} \sum_{i=1}^{n} y_i\right) \mathbf{1}^T\right) = 0,
\end{aligned}$$

and

$$\begin{aligned}
\mathsf{rr}_{2k}(A_1 - I, \ldots, A_n - I) &= \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{-1}{n-1}\right)^k \left(\frac{\mathbf{1}\mathbf{1}^T}{n} - n(n-1) \cdot y_{\sigma(1)} y_{\sigma(2k)}^T\right) \\
&= \frac{1}{n(n-1)} \sum_{i \neq j} \left(\frac{-1}{n-1}\right)^k \left(\frac{\mathbf{1}\mathbf{1}^T}{n} - n(n-1) \cdot y_i y_j^T\right) \\
&= \left(\frac{-1}{n-1}\right)^k \left(\frac{\mathbf{1}\mathbf{1}^T}{n} - \sum_{i \neq j} y_i y_j^T\right) \\
&= \left(\frac{-1}{n-1}\right)^k \left(\frac{1}{n-1} I + \frac{n-2}{n(n-1)} \mathbf{1}\mathbf{1}^T\right).
\end{aligned}$$

We can write these in a single expression as, for $k > 0$,

$$\mathsf{rr}_k(A_1 - I, \ldots, A_n - I) = \frac{1}{2} \left(\left(\frac{\mathrm{i}}{\sqrt{n-1}}\right)^k + \left(\frac{-\mathrm{i}}{\sqrt{n-1}}\right)^k\right) \left(\frac{1}{n-1} I + \frac{n-2}{n(n-1)} \mathbf{1}\mathbf{1}^T\right)$$

where i is the imaginary unit. If we define

$$C_n = \frac{1}{n-1} I + \frac{n-2}{n(n-1)} \mathbf{1}\mathbf{1}^T,$$

then by the binomial theorem, for any $m \in \mathbb{N}$, the original random-reshuffled product can be written as

$$\begin{aligned}
\mathsf{rr}_m(A_1, \ldots, A_n) &= I + \sum_{k=1}^{m} \binom{m}{k} \mathsf{rr}_k(A_1 - I, \ldots, A_n - I) \\
&= I + \frac{1}{2} \cdot C_n \cdot \sum_{k=1}^{m} \binom{m}{k} \left(\left(\frac{\mathrm{i}}{\sqrt{n-1}} \right)^k + \left(\frac{-\mathrm{i}}{\sqrt{n-1}} \right)^k \right) \\
&= I + \frac{1}{2} \cdot C_n \cdot \left(\left(1 + \frac{\mathrm{i}}{\sqrt{n-1}} \right)^m - 1 + \left(1 - \frac{\mathrm{i}}{\sqrt{n-1}} \right)^m - 1 \right) \\
&= I + C_n \cdot \left(\left(1 + \frac{1}{n-1} \right)^{m/2} \cdot \cos\left(m \cdot \arctan\left(\frac{1}{\sqrt{n-1}} \right) \right) - 1 \right).
\end{aligned}$$

In particular, since $C_n \mathbf{1} = \mathbf{1}$, it follows that one eigenvalue of this will be

$$\lambda = \left(1 + \frac{1}{n-1} \right)^{m/2} \cdot \cos\left(m \cdot \arctan\left(\frac{1}{\sqrt{n-1}} \right) \right).$$

This is what we set out to prove. Also note that for large n, if $m = n$,

$$\lambda \approx \exp\left(\frac{1}{2} \right) \cdot \cos\left(\sqrt{n} \right),$$

so we should expect to find n for which $|\lambda| > 1$ fairly easily.

D Derivation for Section 2.2

In this section, we provide derivation details for our claims in Section 2.2. First, we note that since A_i has eigenvalues in $\{0, 1, 2\}$ with multiplicity 1 on the 0 and 2, the matrix $A_i(A_i - I)$ is just $2uu^T$ where u is the unit eigenvector with eigenvalue 2. So, if $B_i^2 = A_i$,

$$A_i + \frac{\sqrt{2} - 2}{2} \cdot A_i(A_i - I) = B_i.$$

Now, recall that B_i satisfies $P_\sigma B_i P_\sigma^T = B_{\sigma(i)}$. So,

$$\begin{aligned}
\mathsf{srr}_n(B_1, \ldots, B_n) &= \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\prod_{i=1}^{n} B_{\sigma(i)} \right)^T \left(\prod_{i=1}^{n} B_{\sigma(i)} \right) \\
&= \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\prod_{i=1}^{n} P_\sigma B_i P_\sigma^T \right)^T \left(\prod_{i=1}^{n} P_\sigma B_i P_\sigma^T \right) \\
&= \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} P_\sigma \left(\prod_{i=1}^{n} B_i \right)^T \left(\prod_{i=1}^{n} B_i \right) P_\sigma^T.
\end{aligned}$$

Now, since we know that $\mathbf{1}$ must be an eigenvector of $\mathsf{srr}_n(B_1, \ldots, B_n)$, it follows that the corresponding eigenvalue must be

$$\begin{aligned}
\lambda &= \frac{1}{\mathbf{1}^T \mathbf{1}} \cdot \mathbf{1}^T \mathsf{srr}_n(B_1, \ldots, B_n) \mathbf{1} \\
&= \frac{1}{n} \cdot \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \mathbf{1}^T P_\sigma \left(\prod_{i=1}^{n} B_i \right)^T \left(\prod_{i=1}^{n} B_i \right) P_\sigma^T \mathbf{1} \\
&= \frac{1}{n} \cdot \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \mathbf{1}^T \left(\prod_{i=1}^{n} B_i \right)^T \left(\prod_{i=1}^{n} B_i \right) \mathbf{1} \\
&= \frac{1}{n} \cdot \mathbf{1}^T \left(\prod_{i=1}^{n} B_i \right)^T \left(\prod_{i=1}^{n} B_i \right) \mathbf{1}.
\end{aligned}$$

We can easily compute this directly to get the eigenvalue. Doing this produces the value given in the body of the paper. We can validate this with the following Julia code.

```
using LinearAlgebra

# define a type for numbers of the form [x + y * sqrt(2)]
struct QR2 <: Number
    x :: Rational{BigInt};
    y :: Rational{BigInt};
end

import Base: +, -, *, //, ==, zero, one, Float64, promote_rule
*(a::QR2, b::QR2) = QR2(a.x * b.x + 2 * a.y * b.y, a.x * b.y + a.y * b.x);
+(a::QR2, b::QR2) = QR2(a.x + b.x, a.y + b.y);
-(a::QR2, b::QR2) = QR2(a.x - b.x, a.y - b.y);
-(b::QR2) = QR2(-b.x, -b.y);
//(a::QR2, q) = QR2(a.x // BigInt(q), a.y // BigInt(q));
zero(::Type{QR2}) = QR2(0, 0);
one(::Type{QR2}) = QR2(1, 0);
zero(a::QR2) = QR2(0, 0);
one(a::QR2) = QR2(1, 0);
Float64(a::QR2) = Float64(BigFloat(a.x) + sqrt(BigFloat(2)) * BigFloat(a.y));
==(a::QR2, b::QR2) = (a.x == b.x) && (a.y == b.y);
QR2(x::Rational) = QR2(x, 0);
QR2(x::Int64) = QR2(BigInt(x) // 1, 0);
promote_rule(::Type{QR2}, ::Type{Integer}) = QR2
promote_rule(::Type{QR2}, ::Type{Int64}) = QR2
promote_rule(::Type{QR2}, ::Type{Rational}) = QR2
promote_rule(::Type{QR2}, ::Type{Rational{BigInt}}) = QR2

# the parameters for the example
n = 10;
sqrtn1 = BigInt(sqrt(n-1));

# define the A matrices
ys = [[(k == i) ? sqrtn1//n : -1//(n*sqrtn1) for i = 1:n] for k = 1:n];
As = [I + ones(BigInt,n) * y' + y * ones(BigInt,n)' for y in ys];

# define the B matrices
Bs = [A .+ ((QR2(0,1) - QR2(2,0))//2) * A * (A - I) for A in As];

# assert that, indeed, B^2 = A
for i = 1:n
        @assert(Bs[i]^2 == QR2.(As[i]));
end

# compute the eigenvalue
lambda = sum(transpose(prod(Bs)) * (prod(Bs))) // n
println(lambda);
println(Float64(lambda));

# assert that it is the value in the paper
@assert(lambda == QR2(16623165607286458//16677181699666569,
↪  2195717144015980//16677181699666569));

# validate that this also works in floating point
Asfp = [Float64.(A) for A in As];
Bsfp = [A .+ ((sqrt(2) - 2)/2) * (A^2 - A) for A in Asfp];

# assert that, indeed, B^2 = A, up to some tolerance, and that B is PSD
tol = 1e-8;
for i = 1:n
        @assert(all(eigvals(Bsfp[i]) .>= -tol));
        @assert(maximum(Bsfp[i]^2 .- Asfp[i]) < tol);
```

```
end

# compute the floating-point estimate of the eigenvalue
lambdafp = sum(transpose(prod(Bsfp)) * (prod(Bsfp))) / n;
println(lambdafp);

# check that it's equal to the value we computed exactly
@assert(abs(lambdafp - Float64(lambda)) < tol);
```

E Code to Verify the Counterexample to Conjecture 2

Here, we include our Julia code to verify that the counterexample described in Section 2.3 is actually a counterexample to Conjecture 2. Our code here also re-computes the numeric constants given in that section for the norms of the various matrices.

```
using Statistics
using Combinatorics
using LinearAlgebra

# we first construct a number type to do arithmetic in the field of Q(sqrt(3))
struct QR3 <: Number
    x :: Rational{BigInt};
    y :: Rational{BigInt};
end

import Base.+
import Base.-
import Base.*
import Base.//
import Base.==
import Base.zero
import Base.conj
import Base.sqrt
import Base.one
import Base.isless
import Base.Float64
import Base.promote_rule

function *(a::QR3, b::QR3)
    return QR3(a.x * b.x + 3 * a.y * b.y, a.x * b.y + a.y * b.x);
end

function +(a::QR3, b::QR3)
    return QR3(a.x + b.x, a.y + b.y);
end

function -(a::QR3, b::QR3)
    return QR3(a.x - b.x, a.y - b.y);
end

function -(b::QR3)
    return QR3(-b.x, -b.y);
end

function //(a::QR3, q::I) where {I <: Integer}
    return QR3(a.x // BigInt(q), a.y // BigInt(q));
end

function zero(::Type{QR3})
    return QR3(0, 0);
end

```

```
function one(::Type{QR3})
    return QR3(1, 0);
end

function zero(a::QR3)
    return QR3(0, 0);
end

function conj(a::QR3)
    return a;
end

function isless(a::QR3, b::QR3)
        cx = a.x - b.x;
        cy = a.y - b.y;
        if (cx >= 0)&&(cy >= 0)
                return false;
        elseif (cx < 0)&&(cy < 0)
                return true;
        elseif (cx < 0)
                return cx^2 > 3 * cy^2;
        elseif (cy < 0)
                return 3 * cy^2 > cx^2;
        else
                error();
        end
end

function one(a::QR3)
    return QR3(1, 0);
end

function Float64(a::QR3)
    return Float64(BigFloat(a.x) + sqrt(BigFloat(3)) * BigFloat(a.y));
end

function ==(a::QR3, b::QR3)
        return (a.x == b.x) && (a.y == b.y);
end

function QR3(x::Rational)
    return QR3(x, 0);
end

function QR3(x::Int64)
    return QR3(BigInt(x) // 1, 0);
end

function Rational(a::QR3)
        @assert(a.y == 0);
        return a.x;
end

promote_rule(::Type{QR3}, ::Type{Integer}) = QR3
promote_rule(::Type{QR3}, ::Type{Int64}) = QR3
promote_rule(::Type{QR3}, ::Type{Rational}) = QR3
promote_rule(::Type{QR3}, ::Type{Rational{BigInt}}) = QR3

# a function to try to compute the square root of a rational number, or error
↪ otherwise
function sqrtq3(x::Rational{BigInt})
    n = x.num * x.den;
    if (sqrt(n) == floor(sqrt(n)))
        return QR3(BigInt(sqrt(n))//x.den, 0);
    elseif (sqrt(n/3) == floor(sqrt(n/3)))
```

```
        return QR3(0, BigInt(sqrt(n/3))//x.den);
    else
        error();
    end
end

# every matrix we'll be computing the norm of is rank-1,
# so its l2 norm is equal to the square root of the trace of A*A'
function l2norm(A::Array{QR3,2})
    return sqrtq3(Rational(tr(A*A')));
end

# define the counterexample dataset
n = 6;
us = [[QR3(0,1//2), QR3(1//2,0)], [QR3(1//2,0), QR3(0,1//2)], [QR3(0,0), QR3(1,0)],
    [QR3(-1//2,0), QR3(0,1//2)], [QR3(0,-1//2), QR3(1//2,0)], [QR3(-1,0),
    QR3(0,0)]];
As = [u*u' for u in us];


# on the left side of the inequality of Conjecture 2
left_expr = maximum(l2norm(prod(p)) for p in permutations(As));
println("left side = $left_expr = $(Float64(left_expr))")


# on the right side of the inequality of Conjecture 2
NX = [l2norm(As[i1]*As[i2]*As[i3]*As[i4]*As[i5]*As[i6]) for i1=1:n, i2=1:n, i3=1:n,
    i4=1:n, i5=1:n, i6=1:n];

RX = -1 * ones(QR3,6,6,6,6,6,6);
for i1=1:n, i2=1:n, i3=1:n, i4=1:n, i5=1:n, i6=1:n
    if (RX[i1,i2,i3,i4,i5,i6] == -1)
        lmax = maximum(NX[p[i1],p[i2],p[i3],p[i4],p[i5],p[i6]] for p in
        permutations(1:n));
        for p in permutations(1:n)
            RX[p[i1],p[i2],p[i3],p[i4],p[i5],p[i6]] = lmax;
        end
    end
end

right_expr = sum(RX)//length(RX);
println("right side = $right_expr = $(Float64(right_expr))")
```

F Proof of Theorem 1

The proof of Theorem 1 is, as stated in the main body of the paper, a straightforward combination of the following two lemmas. The main idea is that we can expand the rr_k expression approximately as a polynomial in α, and then consider only the dominant quadratic α^2 term, which we can bound directly.

Lemma 3 (Binomial Theorem for Random Reshuffling)**.** *For any symmetric matrices $X_1, \ldots, X_n$, and any constants α and β,*

$$\mathsf{rr}_k(\alpha I + \beta X_1, \alpha I + \beta X_2, \ldots, \alpha I + \beta X_n) = \sum_{i=0}^{k} \binom{k}{i} \alpha^{k-i} \beta^k \mathsf{rr}_i(X_1, X_2, \ldots, X_n).$$

Lemma 4. *For any symmetric matrices $X_1, \ldots, X_n \in \mathbb{R}^d$, and for any $u \in \mathbb{R}^d$ such that $\|u\| = 1$,*

$$u^T \left(\mathsf{rr}_2(X_1, \ldots, X_n)\right) u \leq \|\mathsf{rr}_1(X_1, \ldots, X_n)\|^2$$

and equality can hold only if there exists a $\lambda \in \mathbb{R}$ such that for all $i \in \{1, \ldots, n\}$, u is an eigenvector of X_i with eigenvalue λ, that is $X_i u = \lambda u$.

We start by proving the lemmas, then prove the theorem.

F.1 Proofs of Lemmas

In this section, we prove the lemmas presented in Section 4. We start by proving the following lemma, which will be useful for proving Lemma 4.

Lemma 5. *Let ω be a primitive nth root of unity. Then, for any symmetric real matrices $X_1, \ldots, X_n$,*

$$\frac{1}{n \cdot (n-1)} \sum_{i=1}^{n} \sum_{j \neq i} X_i X_j = \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right)^2 - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right).$$

Proof. It is clear that the expressions on both sides of this equation will contain only terms of the form $X_i X_j$, where possibly $i = j$. When $i = j$, the left side will have no terms in X_i^2, and the right side will have

$$\begin{aligned} \frac{1}{n^2} X_i^2 - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \omega^{\sigma(i)} X_i \right) &= \frac{1}{n^2} X_i^2 - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n^2} X_i^2 \right) \\ &= \frac{1}{n^2} X_i^2 - \left(\frac{1}{n^2} X_i^2 \right) \\ &= 0, \end{aligned}$$

where this holds since $\left(\omega^k\right) \cdot \left(\omega^k\right)^* = 1$ because ω is a root of unity. This is what we want for the $i = j$ case.

On the other hand, for $i \neq j$, the left side will have just the term $\frac{1}{n \cdot (n-1)} \cdot X_i X_j$. On the right side, we have

$$\begin{aligned} &\frac{1}{n^2} X_i X_j - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \omega^{\sigma(j)} X_j \right) \\ &\quad = \frac{1}{n^2} X_i X_j - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n^2} \omega^{\sigma(j) - \sigma(i)} X_i X_j \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 - \frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \omega^{\sigma(i) - \sigma(j)} \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 - \frac{1}{n \cdot (n-1)} \sum_{i=1}^{n} \sum_{j \neq i} \omega^{j-i} \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 - \frac{1}{n \cdot (n-1)} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \omega^{j-i} - \sum_{i=1}^{n} \omega^{i-i} \right) \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 - \frac{1}{n \cdot (n-1)} \left(\left(\sum_{i=1}^{n} \omega^{-i} \right) \left(\sum_{j=1}^{n} \omega^{j} \right) - \sum_{i=1}^{n} 1 \right) \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 - \frac{1}{n \cdot (n-1)} \left(0 - n \right) \right) \\ &\quad = \frac{1}{n^2} X_i X_j \left(1 + \frac{1}{n-1} \right) \\ &\quad = \frac{1}{n \cdot (n-1)} X_i X_j. \end{aligned}$$

This is the desired result. □

Using this lemma, we can now prove Lemma 4.

Lemma 4. *For any symmetric matrices $X_1, \ldots, X_n \in \mathbb{R}^d$, and for any $u \in \mathbb{R}^d$ such that $\|u\| = 1$,*

$$u^T \left(\mathsf{rr}_2(X_1, \ldots, X_n)\right) u \leq \left\|\mathsf{rr}_1(X_1, \ldots, X_n)\right\|^2$$

and equality can hold only if there exists a $\lambda \in \mathbb{R}$ such that for all $i \in \{1, \ldots, n\}$, u is an eigenvector of X_i with eigenvalue λ, that is $X_i u = \lambda u$.

Proof. By Lemma 5,

$$u^T \left(\frac{1}{n \cdot (n-1)} \sum_{i=1}^{n} \sum_{j \neq i} X_i X_j \right) u = u^T \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right)^2 u - u^T \left(\frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right) \right) u.$$

Since each term in the rightmost part of this expression is of the form A^*A, it follows that the resulting quadratic form must be positive semidefinite, and so

$$u^T \left(\frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right) \right) u \geq 0.$$

So,

$$u^T \left(\frac{1}{n \cdot (n-1)} \sum_{i=1}^{n} \sum_{j \neq i} X_i X_j \right) u \leq u^T \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right)^2 u.$$

The first part of the lemma follows from the simple observation that by definition

$$u^T \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right)^2 u = \left\| \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right) u \right\|^2 \leq \left\| \frac{1}{n} \sum_{i=1}^{n} X_i \right\|^2 \|u\|^2 = \left\| \frac{1}{n} \sum_{i=1}^{n} X_i \right\|^2.$$

To prove the second part of the theorem, notice that since we just showed that

$$u^T \left(\frac{1}{n \cdot (n-1)} \sum_{i=1}^{n} \sum_{j \neq i} X_i X_j \right) u \leq u^T \left(\frac{1}{n} \sum_{i=1}^{n} X_i \right)^2 u \leq \left\| \frac{1}{n} \sum_{i=1}^{n} X_i \right\|^2,$$

equality between the left and right terms of this statement can only hold if *both* stated inequalities hold with equality. It is well-known that for symmetric matrices A and unit vectors u, $u^T A^2 u = \|A\|^2$ only if u is an eigenvector of A. Thus, our right inequality will hold with equality only if there exists a $\lambda \in \mathbb{R}$ such that

$$\left(\frac{1}{n} \sum_{i=1}^{n} X_i \right) u = \lambda u.$$

On the other hand, by Lemma 1, the left inequality will hold with equality only when

$$u^T \left(\frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right) \right) u = 0.$$

This only happens when

$$\frac{1}{n!} \sum_{\sigma \in \mathcal{P}(n)} u^T \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right) u = 0.$$

Since each of the matrices of the form AA^* produces a positive semidefinite quadratic form, it follows that for every permutation σ,

$$u^T \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right)^* \left(\frac{1}{n} \sum_{i=1}^{n} \omega^{\sigma(i)} X_i \right) u \geq 0.$$

But then, equality can be attained only when *all* of these terms are 0, that is

$$u^T \left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right)^* \left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right) u = 0 \qquad \text{for every } \sigma \in \mathcal{P}(n).$$

Since

$$u^T \left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right)^* \left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right) u = \left\| \left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right) u \right\|^2,$$

it follows that this only holds when

$$\left(\frac{1}{n}\sum_{i=1}^{n} \omega^{\sigma(i)} X_i\right) u = 0 \qquad \text{for every } \sigma \in \mathcal{P}(n).$$

Since this holds for *any* permutation, it follows that it holds for any scaling vector in the span of the permutations. Explicitly,

$$\sum_{i=1}^{n} b_i X_i u = 0 \qquad \text{for every } b \in \operatorname{span}\left(\begin{bmatrix} \omega^{\sigma(1)} \\ \vdots \\ \omega^{\sigma(n)} \end{bmatrix} \;\middle|\; \sigma \in \mathcal{P}(n) \right).$$

It is not hard to see that this span is just the set

$$\operatorname{span}\left(\begin{bmatrix} \omega^{\sigma(1)} \\ \vdots \\ \omega^{\sigma(n)} \end{bmatrix} \;\middle|\; \sigma \in \mathcal{P}(n) \right) = \left\{ b \;\middle|\; \sum_{i=1}^{n} b_i = 0 \right\}.$$

In particular, it must hold that, for any j

$$X_j u - \frac{1}{n}\sum_{i=1}^{n} X_i u = 0.$$

Now adding our earlier derivation that

$$\left(\frac{1}{n}\sum_{i=1}^{n} X_i\right) u = \lambda u$$

gives us

$$X_j u = \lambda u,$$

which proves the lemma. □

Next, we prove Lemma 3, the binomial theorem for random reshuffling.

Lemma 3 (Binomial Theorem for Random Reshuffling) For any symmetric matrices $X_1, \ldots, X_n$, and any constants α and β,

$$\mathsf{rr}_k(\alpha I + \beta X_1, \alpha I + \beta X_2, \ldots, \alpha I + \beta X_n) = \sum_{i=0}^{k} \binom{k}{i} \alpha^{k-i} \beta^k \mathsf{rr}_i(X_1, X_2, \ldots, X_n).$$

Proof. First, note that for any $A_1, A_2, \ldots, A_n$, we can write

$$\mathsf{rr}_k(A_1, A_2, \ldots, A_n) = \frac{1}{n!} \frac{\partial}{\partial \eta_1} \frac{\partial}{\partial \eta_2} \cdots \frac{\partial}{\partial \eta_n} \left(\sum_{i=1}^{n} \eta_i A_i\right)^k \cdot \left(\sum_{i=1}^{n} \eta_i\right)^{n-k}.$$

This holds because

$$\left(\sum_{i=1}^{n} \eta_i A_i\right)^k \cdot (\sum_{i=1}^{n} \eta_i)^{n-k} = \sum_{\sigma:\{1,\ldots,n\}\to\{1,\ldots,n\}} \left(\prod_{i=1}^{k} \eta_{\sigma(i)} A_{\sigma(i)}\right) \left(\prod_{i=k+1}^{n} \eta_i\right),$$

where this sum ranges over all functions σ from $\{1, \ldots, n\}$ to itself. The only terms of this sum that will survive the differentiation operation are those for which σ is a permutation (since otherwise there will be some η_i that does not appear in the term, and it will be zeroed out by the partial differentiation with respect to that η_i). So,

$$\frac{1}{n!}\frac{\partial}{\partial \eta_1}\frac{\partial}{\partial \eta_2}\cdots\frac{\partial}{\partial \eta_n}\left(\sum_{i=1}^n \eta_i A_i\right)^k \cdot \left(\sum_{i=1}^n \eta_i\right)^{n-k} = \frac{1}{n!}\sum_{\sigma\in\mathcal{P}(n)}\prod_{i=1}^k (\alpha I + \beta X_i)$$

which is $\mathsf{rr}_k(A_1, A_2, \ldots, A_n)$ by definition.

Applying this to our expression in the lemma statement,

$$\begin{aligned}\mathsf{rr}_k(\alpha I + \beta X_1, \ldots, \alpha I + \beta X_n) &= \frac{1}{n!}\frac{\partial}{\partial \eta_1}\cdots\frac{\partial}{\partial \eta_n}\left(\sum_{i=1}^n \eta_i\left(\alpha I + \beta X_i\right)\right)^k \cdot \left(\sum_{i=1}^n \eta_i\right)^{n-k} \\ &= \frac{1}{n!}\frac{\partial}{\partial \eta_1}\cdots\frac{\partial}{\partial \eta_n}\left(\alpha\sum_{i=1}^n \eta_i I + \beta\sum_{i=1}^n \eta_i X_i\right)^k \cdot \left(\sum_{i=1}^n \eta_i\right)^{n-k}\end{aligned}$$

Applying the binomial theorem to this inner term gives us

$$\begin{aligned}\left(\alpha\sum_{i=1}^n \eta_i I + \beta\sum_{i=1}^n \eta_i X_i\right)^k &= \sum_{j=0}^k \binom{k}{j}\left(\alpha\sum_{i=1}^n \eta_i I\right)^{k-j}\left(\beta\sum_{i=1}^n \eta_i X_i\right)^j \\ &= \sum_{j=0}^k \binom{k}{j}\alpha^{k-j}\beta^k\left(\sum_{i=1}^n \eta_i\right)^{k-j}\left(\sum_{i=1}^n \eta_i X_i\right)^j.\end{aligned}$$

Substituting this into our expression above gives

$$\begin{aligned}\mathsf{rr}_k(\alpha I + \beta X_1, \ldots, \alpha I + \beta X_n) &= \frac{1}{n!}\frac{\partial}{\partial \eta_1}\cdots\frac{\partial}{\partial \eta_n}\sum_{j=0}^k \binom{k}{j}\alpha^{k-j}\beta^k\left(\sum_{i=1}^n \eta_i X_i\right)^j \cdot \left(\sum_{i=1}^n \eta_i\right)^{n-j} \\ &= \sum_{j=0}^k \binom{k}{j}\alpha^{k-j}\beta^k\frac{1}{n!}\frac{\partial}{\partial \eta_1}\cdots\frac{\partial}{\partial \eta_n}\left(\sum_{i=1}^n \eta_i X_i\right)^j \cdot \left(\sum_{i=1}^n \eta_i\right)^{n-j} \\ &= \sum_{j=0}^k \binom{k}{j}\alpha^{k-j}\beta^k\mathsf{rr}_j(X_1, \ldots, X_n).\end{aligned}$$

This proves the lemma. □

F.2 Main Body of Proof of Theorem 1

In this section, we prove Theorem 1, which shows that Conjecture 1 holds with strict inequality for sufficiently small step sizes (as long as the matrix ensemble is nontrivial).

Theorem 1 (Matrix AMGM Inequality, Sufficiently Small Step Size) *Let $A_1, \ldots, A_n$ be a collection of continuously twice-differentiable functions from $\mathbb{R}$ to $\mathcal{S}_d$, that all satisfy $A_i(0) = I$ and that are non-trivial in the sense that they have no eigenvalue/eigenvector pairs shared among all the matrices $A_1'(0), A_2'(0), \ldots, A_n'(0)$. Then for any $2 \le k \le n$, there exists an $\alpha_{\max} > 0$ and a constant $C > 0$ such that such that for all $0 < \alpha \le \alpha_{\max}$,*

$$\|\mathsf{rr}_k(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))\| < \|\mathsf{rr}_1(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))\|^k - \alpha^2 C.$$

Proof. First, note that since when $\alpha = 0$,

$$\mathsf{rr}_k(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha)) = \mathsf{rr}_1(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha)) = I,$$

by continuity of these expressions in α, for sufficiently small positive α it must hold that both

$$\mathsf{rr}_k(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))$$

and

$$\mathsf{rr}_1(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))$$

are positive definite. We will restrict our attention to α in this range (by setting $\alpha_{\max}$ appropriately). Next, define $\beta > 0$ as some number such that for any α in this range,

$$\frac{A_i(\alpha) - I}{\alpha} + \beta I \succeq 0.$$

The existence of such a β is guaranteed because A_i is continuously differentiable. Define

$$H_i(\alpha) = \frac{A_i(\alpha) - I}{\alpha} + \beta I.$$

Notice now that

$$A_i(\alpha) = \alpha H_i + (1 - \alpha\beta)I$$

So, by Lemma 3,

$$\begin{aligned}\mathsf{rr}_k(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha)) &= \mathsf{rr}_k(\alpha H_1(\alpha) + (1-\alpha\beta)I, \ldots, \alpha H_n(\alpha) + (1-\alpha\beta)I) \\ &= \sum_{i=0}^{k} \binom{k}{i} \alpha^i (1-\alpha\beta)^{k-i} \mathsf{rr}_i(H_1(\alpha), \ldots, H_n(\alpha)).\end{aligned}$$

On the other hand, on the right side, by the binomial theorem,

$$\begin{aligned}\left(\mathsf{rr}_1(A_1(\alpha), A_2(\alpha), \ldots, A_n(\alpha))\right)^k &= \left(\mathsf{rr}_1(\alpha H_1 + (1-\alpha\beta)I, \ldots, \alpha H_n + (1-\alpha\beta)I)\right)^k \\ &= \left((1-\alpha\beta)I + \frac{\alpha}{n}\sum_{i=1}^{n} H_i(\alpha)\right)^k \\ &= \sum_{i=0}^{k} \binom{k}{i} \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot \left(\frac{1}{n}\sum_{i=1}^{n} H_i(\alpha)\right)^k \\ &= \sum_{i=0}^{k} \binom{k}{i} \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot \left(\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\right)^k.\end{aligned}$$

Next, note that we can complete H_i to be a continuously differentiable function by defining

$$H_i(0) = \lim_{\alpha \to 0} H_i(\alpha) = A_i'(0) + \beta I.$$

This means that, by our assumption, $H_1(0), H_2(0), \ldots, H_n(0)$ do not share any eigenvalue/eigenvector pairs. Therefore, by Lemma 4, we know that for any u

$$u^T \mathsf{rr}_2(H_1(0), H_2(0), \ldots, H_n(0))u < \left\|\mathsf{rr}_1(H_1(0), H_2(0), \ldots, H_n(0))\right\|^2,$$

(since this can not hold with equality because of our assumption about the eigenvectors of the H_i). Define b as the constant such that

$$2b = \left\|\mathsf{rr}_1(H_1(0), H_2(0), \ldots, H_n(0))\right\|^2 - \lambda_{\max}\left(\mathsf{rr}_2(H_1(0), H_2(0), \ldots, H_n(0))\right).$$

We know that $b > 0$ because of our result from Lemma 4. By continuity of the H_i and all these other expressions, for all sufficiently small α,

$$\left\|\mathsf{rr}_1(H_1(\alpha), H_2(\alpha), \ldots, H_n(\alpha))\right\|^2 - \lambda_{\max}\left(\mathsf{rr}_2(H_1(\alpha), H_2(\alpha), \ldots, H_n(\alpha))\right) \geq b.$$

We will restrict our attention to α such that this holds (again by setting $\alpha_{\max}$ appropriately). In a similar way, we also restrict our attention to α such that $1 - \alpha\beta > 0$.

Let c be a constant such that for any $i \in \{1, \ldots, n\}$, and any α in our range.

$$\left\|\mathsf{rr}_i(H_1(\alpha), \ldots, H_n(\alpha))\right\| \leq c^i$$

Such a c must exist because it is a bound on a continuous function over a bounded interval. For any unit vector u, and any $\alpha > 0$ in our restricted sufficiently-small range

$$
\begin{aligned}
&u^T \mathsf{rr}_k(A_1(\alpha), \ldots, A_n(\alpha))u \\
&\quad = \sum_{i=0}^{k} \binom{k}{i} \alpha^i (1-\alpha\beta)^{k-i} u^T \mathsf{rr}_i(H_1(\alpha), \ldots, H_n(\alpha))u \\
&\quad = (1-\alpha\beta)^k + \binom{n}{1} \cdot \alpha \cdot (1-\alpha\beta)^{k-1} \cdot u^T \mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))u \\
&\qquad + \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot u^T \mathsf{rr}_2(H_1(\alpha), \ldots, H_n(\alpha))u \\
&\qquad + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i (1-\alpha\beta)^{k-i} u^T \mathsf{rr}_i(H_1(\alpha), \ldots, H_n(\alpha))u \\
&\quad \leq (1-\alpha\beta)^k + \binom{n}{1} \cdot \alpha \cdot (1-\alpha\beta)^{k-1} \cdot \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\| \\
&\qquad + \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot \left(\|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\|^2 - b\right) \\
&\qquad + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i (1-\alpha\beta)^{k-i} \|\mathsf{rr}_i(H_1(\alpha), \ldots, H_n(\alpha))\| \\
&\quad \leq (1-\alpha\beta)^k + \binom{n}{1} \cdot \alpha \cdot (1-\alpha\beta)^{k-1} \cdot \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\| \\
&\qquad + \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot \left(\|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\|^2 - b\right) \\
&\qquad + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i \\
&\quad \leq (1-\alpha\beta)^k + \binom{n}{1} \cdot \alpha \cdot (1-\alpha\beta)^{k-1} \cdot \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\| \\
&\qquad + \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot \left(\|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\|^2 - b\right) \\
&\qquad + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot \left(c^i + \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\|^i\right) \\
&\quad \leq \left((1-\alpha\beta) + \alpha \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\|\right)^k \\
&\qquad - \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot b \\
&\qquad + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i.
\end{aligned}
$$

Since all the H_i are positive semidefinite,

$$
\begin{aligned}
(1-\alpha\beta) + \alpha \|\mathsf{rr}_1(H_1(\alpha), \ldots, H_n(\alpha))\| &= (1-\alpha\beta) + \frac{\alpha}{n} \left\| \sum_{i=1}^{n} H_i(\alpha) \right\| \\
&= \left\| (1-\alpha\beta) I + \frac{\alpha}{n} \sum_{i=1}^{n} H_i(\alpha) \right\| \\
&= \|\mathsf{rr}_1(A_1(\alpha), \ldots, A_n(\alpha))\|.
\end{aligned}
$$

So, for any unit vector u,

$$u^T \mathsf{rr}_k(A_1(\alpha), \ldots, A_n(\alpha))u \leq \|\mathsf{rr}_1(A_1(\alpha), \ldots, A_n(\alpha))\|^k - \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot b + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i.$$

Since we chose α small enough that $\mathsf{rr}_k(A_1(\alpha), \ldots, A_n(\alpha))$ is positive semidefinite, and for any positive semidefinite matrix X there exists a unit vector u such that $\|X\| = u^T X u$, it follows that

$$\|\mathsf{rr}_k(A_1(\alpha), \ldots, A_n(\alpha))\| \leq \|\mathsf{rr}_1(A_1(\alpha), \ldots, A_n(\alpha))\|^k - \binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot b + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i.$$

Since the expression

$$-\binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot b + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i = -\frac{n(n-1)b}{2} \cdot \alpha^2 + \mathcal{O}(\alpha^3),$$

it follows that for sufficiently small α,

$$-\binom{n}{2} \cdot \alpha^2 \cdot (1-\alpha\beta)^{k-2} \cdot b + \sum_{i=3}^{k} \binom{k}{i} \cdot \alpha^i \cdot (1-\alpha\beta)^{k-i} \cdot c^i < -\frac{n(n-1)b}{4} \cdot \alpha^2.$$

Now letting $C = \frac{n(n-1)b}{4}$ and letting $\alpha_{\max}$ denote the smallest bound on α we have assumed during this proof (including the "sufficiently small" bound we just invoked), it follows that

$$\|\mathsf{rr}_k(A_1(\alpha), \ldots, A_n(\alpha))\| < \|\mathsf{rr}_1(A_1(\alpha), \ldots, A_n(\alpha))\|^k - \alpha^2 C.$$

This is what we wanted to prove. □

G Proof of Corollary 1

In this section, we prove Corollary 1, which characterizes the convergence of with-replacement versus without-replacement parallel SGD when a diminishing step size scheme is used.

Corollary 1 *Consider Algorithm 1 on a non-trivial noiseless convex quadratic using any M (including $M = 1$, ordinary sequential SGD). Suppose that the step size scheme satisfies $0 < \alpha_i L < 1$ and is diminishing but not square-summable, i.e. $\lim_{k\to\infty} \alpha_k = 0$ and $\sum_{k=1}^{\infty} \alpha_k^2 = \infty$. Then for almost all initial values $w_0 \neq w^*$,*

$$\lim_{k\to\infty} \frac{\left\|\mathbf{E}[w_{k,\texttt{without-replacement}}] - w^*\right\|}{\left\|\mathbf{E}[w_{k,\texttt{with-replacement}}] - w^*\right\|} = 0.$$

Proof. Without loss of generality, suppose $w^* = 0$. Also for simplicity let $m = 1$ (referring to the one parallel worker in the algorithm, since $M = 1$). In this case, our loss functions are

$$f_i(w) = \frac{1}{2} w^T H_i w.$$

With this, the updates of Algorithm 1 can be written as

$$\begin{aligned} u_{k,m,t} &= u_{k,m,t-1} - \alpha_k \nabla f_{\sigma_{k,m}(t)}\left(u_{k,m,t-1}\right) \\ &= u_{k,m,t-1} - \alpha_k H_{\sigma_{k,m}(t)} u_{k,m,t-1} \\ &= \left(I - \alpha_k H_{\sigma_{k,m}(t)}\right) u_{k,m,t-1}. \end{aligned}$$

Now, by induction,

$$u_{k,m,n} = \left(\prod_{t=1}^{n} \left(I - \alpha_k H_{\sigma_{k,m}(t)}\right)\right) w_k,$$

and so

$$w_k = \frac{1}{M}\sum_{m=1}^{M}\left(\prod_{t=1}^{n} \left(I - \alpha_k H_{\sigma_{k,m}(t)}\right)\right) w_{k-1}.$$

Now taking the expected value, for random reshuffling

$$\mathbf{E}\left[w_{k,\texttt{without-replacement}}\right] = \mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n) \cdot \mathbf{E}\left[w_{k-1,\texttt{without-replacement}}\right]$$

and for with-replacement sampling

$$\mathbf{E}\left[w_{k,\texttt{with-replacement}}\right] = \mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)^n \cdot \mathbf{E}\left[w_{k-1,\texttt{with-replacement}}\right].$$

Let λ be the smallest eigenvalue of

$$\mathsf{rr}_1(H_1, \ldots, H_n) = \frac{1}{n}\sum_{i=1}^{n} H_i$$

with corresponding eigenvalue u. It follows that

$$\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)u = (1 - \alpha_k\lambda)u = \|\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\|\, u.$$

And so, for with-replacement sampling,

$$\left|u^T \mathbf{E}\left[w_{k,\texttt{with-replacement}}\right]\right| = \|\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\|^n \cdot \left|u^T \mathbf{E}\left[w_{k-1,\texttt{with-replacement}}\right]\right|.$$

Applying this recursively,

$$\begin{aligned}&\left|u^T \mathbf{E}\left[w_{K,\texttt{with-replacement}}\right]\right| \\ &\quad = \left|u^T \mathbf{E}\left[w_{0,\texttt{with-replacement}}\right]\right| \cdot \prod_{k=1}^{K} \|\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\|^n.\end{aligned}$$

For almost all initial values, $\left|u^T \mathbf{E}\left[w_{0,\texttt{with-replacement}}\right]\right| \neq 0$. Call this nonzero quantity ρ. Then by Cauchy-Schwarz,

$$\left\|\mathbf{E}\left[w_{K,\texttt{with-replacement}}\right]\right\| \geq \rho \cdot \prod_{k=1}^{K} \|\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\|^n.$$

On the other hand, for random reshuffling

$$\left\|\mathbf{E}\left[w_{k+1,\texttt{without-replacement}}\right]\right\| \leq \|\mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\| \cdot \left\|\mathbf{E}\left[w_{k,\texttt{without-replacement}}\right]\right\|.$$

By Theorem 1, there exists some $\alpha_{\max} > 0$ and some C such that for all $0 < \alpha < \alpha_{\max}$,

$$\|\mathsf{rr}_1(I - \alpha H_1, \ldots, I - \alpha H_n)\| < \|\mathsf{rr}_1(I - \alpha H_1, \ldots, I - \alpha H_n)\|^n - \alpha^2 C.$$

Since $\lim_{k\to\infty} \alpha_k = 0$, there exists some κ such that for all $k \geq \kappa$, $\alpha_k < \alpha_{\max}$. So, we can bound our random-reshuffled distance recursively, for any $K > \kappa$ as

$$\begin{aligned}&\left\|\mathbf{E}\left[w_{K,\texttt{without-replacement}}\right]\right\| \\ &\quad \leq \left\|\mathbf{E}\left[w_{0,\texttt{without-replacement}}\right]\right\| \cdot \prod_{k=1}^{K} \|\mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\| \\ &\quad = \left\|\mathbf{E}\left[w_{0,\texttt{without-replacement}}\right]\right\| \cdot \prod_{k=1}^{\kappa-1} \|\mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\| \\ &\qquad \cdot \prod_{k=\kappa}^{K} \|\mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\| \\ &\quad \leq \left\|\mathbf{E}\left[w_{0,\texttt{without-replacement}}\right]\right\| \cdot \prod_{k=1}^{\kappa-1} \|\mathsf{rr}_n(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\| \\ &\qquad \cdot \prod_{k=\kappa}^{K} \left(\|\mathsf{rr}_1(I - \alpha_k H_1, \ldots, I - \alpha_k H_n)\|^n - \alpha_k^2 C\right)\end{aligned}$$

If we let $\left\|\mathbf{E}\left[w_{0,\texttt{without-replacement}}\right]\right\| = \phi$ and divide this by the with-replacement term, we get

$$\begin{aligned}
&\frac{\left\|\mathbf{E}\left[w_{K,\texttt{without-replacement}}\right]\right\|}{\left\|\mathbf{E}\left[w_{K,\texttt{with-replacement}}\right]\right\|} \\
&\quad\leq \frac{\phi}{\rho}\cdot\prod_{k=1}^{\kappa-1}\frac{\|\mathsf{rr}_n(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|}{\|\mathsf{rr}_1(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|^n} \\
&\qquad\cdot\prod_{k=\kappa}^{K}\left(1-\frac{\alpha_k^2 C}{\|\mathsf{rr}_1(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|^n}\right)
\end{aligned}$$

Since each H_i is positive semidefinite, and each α_k is sufficiently small, it follows that

$$\|\mathsf{rr}_1(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|\leq 1.$$

So,

$$\begin{aligned}
&\frac{\left\|\mathbf{E}\left[w_{K,\texttt{without-replacement}}\right]\right\|}{\left\|\mathbf{E}\left[w_{K,\texttt{with-replacement}}\right]\right\|} \\
&\quad\leq \frac{\phi}{\rho}\cdot\prod_{k=1}^{\kappa-1}\frac{\|\mathsf{rr}_n(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|}{\|\mathsf{rr}_1(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|^n} \\
&\qquad\cdot\prod_{k=\kappa}^{K}\left(1-\alpha_k^2 C\right) \\
&\quad\leq \frac{\phi}{\rho}\cdot\prod_{k=1}^{\kappa-1}\frac{\|\mathsf{rr}_n(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|}{\|\mathsf{rr}_1(I-\alpha_k H_1,\ldots,I-\alpha_k H_n)\|^n}\cdot\exp\left(-\sum_{k=\kappa}^{K}\alpha_k^2 C\right).
\end{aligned}$$

Since by assumption this sum diverges as $K\to\infty$, it follows that this entire expression converges to 0. This is what we wanted to show. □

H Code to Reproduce Figures

Here, for completeness, and because the code is relatively short, we provide Julia code to reproduce the figures in this paper.

H.1 Code to Reproduce Figure 1

```
using Random
using Statistics
using LinearAlgebra
using PyPlot

# Code to implement parallel SGD

abstract type SampleStrategy end;
abstract type WithReplacement <: SampleStrategy end;
abstract type WithoutReplacement <: SampleStrategy end;

function grad_fi(w::Array{Float64,1}, u::Array{Float64,1}, v::Array{Float64,1},
    a::Float64, gamma::Float64)
    return 2 * (dot(u,w)*dot(v,w) - a) * (dot(u,w)*v + dot(v,w)*u) + gamma * w;
end

function par_sgd_epoch(w0::Array{Float64,1}, us::Array{Array{Float64,1},1},
    vs::Array{Array{Float64,1},1}, as::Array{Float64,1}, alpha::Float64,
    gamma::Float64, ::Type{WithReplacement})
    w = w0;
    n = length(as);
```

```
    for t = 1:n
        i = rand(1:n);
        w = w - alpha * grad_fi(w, us[i], vs[i], as[i], gamma);
    end
    return w;
end

function par_sgd_epoch(w0::Array{Float64,1}, us::Array{Array{Float64,1},1},
↪   vs::Array{Array{Float64,1},1}, as::Array{Float64,1}, alpha::Float64,
↪   gamma::Float64, ::Type{WithoutReplacement})
    w = w0;
    n = length(as);
    s = randperm(n)
    for t = 1:n
        i = s[t];
        w = w - alpha * grad_fi(w, us[i], vs[i], as[i], gamma);
    end
    return w;
end

function par_sgd(w0::Array{Float64,1}, us::Array{Array{Float64,1},1},
↪   vs::Array{Array{Float64,1},1}, as::Array{Float64,1}, alpha::Float64,
↪   gamma::Float64, M::Int64, K::Int64, ::Type{RS}) where {RS<:SampleStrategy}
    w = w0;
    ws = [copy(w0)];
    for k = 1:K
        w = mean([par_sgd_epoch(w, us, vs, as, alpha, gamma, RS) for m = 1:M]);
        # println("at iter k,norm(w) =(norm(w))");
        push!(ws, w);
    end
    return ws;
end

function mc_loss(w::Array{Float64,1}, us::Array{Array{Float64,1},1},
↪   vs::Array{Array{Float64,1},1}, as::Array{Float64,1}, gamma::Float64)
    n = length(as);
    return mean((dot(w,us[i])*dot(w,vs[i]) - as[i])^2 for i = 1:n) + gamma *
    ↪   norm(w)^2 / 2;
end


# Parameters

n = 40;
alpha = 0.1;
gamma = 0.05;
y_ii = sqrt(n-1)/n;
y_ij = -1.0/(n*sqrt(n-1));

us = [ones(n) for i = 1:n];
vs = [[(i == j) ? y_ii : y_ij for j = 1:n] for i = 1:n];
as = [(1 - alpha * gamma)/(2 * alpha) for i = 1:n];

M = 1000;
K = 100;

# Run experiments and produce figure

Random.seed!(1234567);

w0 = randn(n); w0 = w0 / norm(w0);

optimal_loss = mc_loss(zeros(n),us,vs,as,gamma);

figure(figsize=(4.0, 2.75));
```

```

for RUN = 1:10
    w0 = 0.1 * randn(n);
    ws_with = par_sgd(w0, us, vs, as, alpha, gamma, M, K, WithReplacement);
    ws_without = par_sgd(w0, us, vs, as, alpha, gamma, M, K, WithoutReplacement);
    losses_with = [mc_loss(w,us,vs,as,gamma) for w in ws_with];
    losses_without = [mc_loss(w,us,vs,as,gamma) for w in ws_without];
    if RUN == 10
        semilogy(losses_with .- optimal_loss; c="#1f77a4", label="with
        ↪  replacement");
        semilogy(losses_without .- optimal_loss; c="#c62028", label="without
        ↪  replacement");
    else
        semilogy(losses_with .- optimal_loss; c="#1f77a4", linestyle=":");
        semilogy(losses_without .- optimal_loss; c="#c62028", linestyle=":");
    end
end

legend();
ylabel("loss gap");
xlabel("epoch number");

tight_layout();

savefig("parsgdexample.pdf");
```

H.2 Code to Reproduce Figure 2

```
using Random
using Statistics
using LinearAlgebra
using PyPlot


abstract type SampleStrategy end;
abstract type WithReplacement <: SampleStrategy end;
abstract type WithoutReplacement <: SampleStrategy end;

function grad_fi(w::Array{Float64,1}, H::Array{Float64})
    return H*w;
end

function par_sgd_epoch(w0::Array{Float64,1}, Hs::Array{Array{Float64,2},1},
↪  alpha::Float64, ::Type{WithReplacement})
    w = w0;
    n = length(Hs);
    for t = 1:n
        i = rand(1:n);
        w = w - alpha * grad_fi(w, Hs[i]);
    end
    return w;
end

function par_sgd_epoch(w0::Array{Float64,1}, Hs::Array{Array{Float64,2},1},
↪  alpha::Float64, ::Type{WithoutReplacement})
    w = w0;
    n = length(Hs);
    s = randperm(n)
    for t = 1:n
        i = s[t];
        w = w - alpha * grad_fi(w, Hs[i]);
    end
```

```
    return w;
end

function par_sgd(w0::Array{Float64,1},  Hs::Array{Array{Float64,2},1},
↪  alpha::Float64, M::Int64, K::Int64, ::Type{RS}) where {RS<:SampleStrategy}
    w = w0;
    ws = [copy(w0)];
    for k = 1:K
        w = mean([par_sgd_epoch(w, Hs, alpha, RS) for m = 1:M]);
        # println("at iter k, norm(w) = (norm(w))");
        push!(ws, w);
    end
    return ws;
end

function blockdiag(Xs::Array{T}...) where {T<:Number}
    m = sum(size(X,1) for X in Xs);
    n = sum(size(X,2) for X in Xs);
    rv = zeros(T,m,n);
    i = 0;
    j = 0;
    for X in Xs
        rv[i.+(1:size(X,1)),j.+(1:size(X,2))] .= X;
        i += size(X,1);
        j += size(X,2);
    end
    return rv;
end

# construct the example

n = 8

A_kij = -2/(n*sqrt(n-1));
A_kii = 1 - 2/(n*sqrt(n-1));
A_kki = (n-2)/(n*sqrt(n-1));
A_kkk = 1 + (2*sqrt(n-1))/n;

As = [[(i == j) ? ((i == k) ? A_kkk : A_kii) : (((i==k)(j==k)) ? A_kki : A_kij) for
↪  i = 1:n, j = 1:n] for k = 1:n];

beta = 0.5;

Hs = [blockdiag(I - beta * A, [1 - beta], [1 + beta]) for A in As];


# problem settings
M = 100;
K = 20;
alphas = 0.0:0.001:1.7;

# initial value
Random.seed!(8675309)
w0 = vcat(randn(n), 1e-20*randn(2)); # note smaller magnitude in extra component

# run experiments
y_with = [norm(par_sgd(w0, Hs, alpha, M, K, WithReplacement)[end]) for alpha in
↪  alphas];
y_without = [norm(par_sgd(w0, Hs, alpha, M, K, WithoutReplacement)[end]) for alpha
↪  in alphas];

y_with1 = [norm(par_sgd(w0, Hs, alpha, 1, K, WithReplacement)[end]) for alpha in
↪  alphas];
y_without1 = [norm(par_sgd(w0, Hs, alpha, 1, K, WithoutReplacement)[end]) for alpha
↪  in alphas];
```

```
figure(figsize=(4.0, 2.75));

semilogy(alphas, y_with1; label="with replacement (M=1)", c="#7fc7e4",
↪  linestyle=":");
semilogy(alphas, y_without1; label="without replacement (M=1)", c="#e6a798",
↪  linestyle=":");
semilogy(alphas, y_with; label="with replacement (M=100)", c="#1f77a4");
semilogy(alphas, y_without; label="without replacement (M=100)", c="#c62028");
xlim((0.0,1.7));
xlabel("step size");
ylabel("distance to optimum");
legend(frameon=false, fontsize="small");

tight_layout();

savefig("convexsgdexample.pdf");
```

H.3 Code to Reproduce Figure 3

```
using LinearAlgebra
using Random
using PyPlot

A1 = BigInt.([2 -1 1; -1 2 -1; 1 -1 1])//4
A2 = BigInt.([2 0 -1; 0 1 1; -1 1 2])//4
A3 = BigInt.([0 0 0; 0 1 -1; 0 -1 2])//4
u = BigInt.([1, -2, -1])//1;
R = (u*u')//6;

# assert that the product of the matrices is in fact nilpotent
@assert((A1*A2*A3)^3 == zeros(Rational{BigInt},3,3))

# check that all the matrices are in fact positive semidefinite
@assert(all(eigvals(Float64.(A1)) .>= 0))
@assert(all(eigvals(Float64.(A2)) .>= 0))
@assert(all(eigvals(Float64.(A3)) .>= 0))
@assert(all(eigvals(Float64.(R)) .>= -1e-8))

# check that all the matrices are in fact all \preceq I
@assert(all(eigvals(Float64.(A1)) .<= 1))
@assert(all(eigvals(Float64.(A2)) .<= 1))
@assert(all(eigvals(Float64.(A3)) .<= 1))
@assert(all(eigvals(Float64.(R)) .<= 1))

# all sequences of matrices that can occur in a single permutation of A1, A2, and
↪  A3
Ls = [BigInt.(Matrix(I,3,3))//1,
        A1,A2,A3,
        A1*A2,A1*A3,A2*A1,A2*A3,A3*A1,A3*A2,
        A1*A2*A3,A1*A3*A2,A2*A1*A3,A2*A3*A1,A3*A1*A2,A3*A2*A1];

# assert that no possible sequence can be 0
for L1 in Ls
    for L2 in Ls
        @assert(u'*L1*L2*u != 0)
    end
end

# function for SGD using without-replacement sampling
```

```
function sgd_rr(x0::Array{Rational{BigInt},1},
↪  DS::Array{Array{Rational{BigInt},2},1}, alpha::Rational{BigInt},
↪  num_epochs::Int64)
    rv = Float64[];
    x = x0;
    for iepoch = 1:num_epochs
        for s in shuffle(DS)
                x = x - alpha * 2 * s * x;
        end
        loss = sum(x'*s*x for s in DS)//length(DS);
        push!(rv, Float64(log10(BigFloat(loss))));
    end
    return rv;
end

# function for SGD using with-replacement sampling
function sgd_wr(x0::Array{Rational{BigInt},1},
↪  DS::Array{Array{Rational{BigInt},2},1}, alpha::Rational{BigInt},
↪  num_epochs::Int64)
    rv = Float64[];
    x = x0;
    for iepoch = 1:num_epochs
        for i = 1:length(DS)
                x = x - alpha * 2 * rand(DS) * x;
        end
        loss = sum(x'*s*x for s in DS)//length(DS);
        push!(rv, Float64(log10(BigFloat(loss))));
    end
    return rv;
end

# random initial value
Random.seed!(8765309)
x0 = big.(Rational.(randn(Float32,3)))

# dataset
DS = [I - A1, I - A2, I - A3, I - R]

# step size
alpha = BigInt(1)//2

# number of epochs and trials to run
nepochs = 1000
ntrials = 20

# run experiments
log10_losses_wr = [sgd_wr(x0, DS, alpha, nepochs) for i = 1:ntrials]
log10_losses_rr = [sgd_rr(x0, DS, alpha, nepochs) for i = 1:ntrials]

# modify wo replacement experiments to show very small number instead of minus
↪  infinity
# this is an adjustment for display, since that small number will be out of the
↪  range of the axis
# we will get nice vertical lines in the plot slowing the with-replacement curve has
↪  jumped to 0
log10_losses_wr_adjusted = [[(x == -Inf) ? -1e8 : x for x in ld] for ld in
↪  log10_losses_wr]

# actually make the plot
figure(figsize=(4.0, 2.75));
plot(log10_losses_wr_adjusted[1]; label="with replacement", color="#1f77a4")
plot(log10_losses_rr[1]; label="without replacement", color="#c62028")
for dd in log10_losses_wr_adjusted[2:end]
    plot(dd; color="#1f77a4", linestyle=":")
end
```

```
for dd in log10_losses_rr[2:end]
    plot(dd; color="#c62028", linestyle=":")
end
legend()
ylim([-4000,100])
xlabel("epoch number")
ylabel("\$\\log_{10}\$(loss)")
tight_layout()

savefig("asymptotic.pdf")
```