
Simple Stochastic and Online Gradient Descent Algorithms for Pairwise Learning

Zhenhuan Yang^{1*} Yunwen Lei^{2*} Puyu Wang³ Tianbao Yang⁴ Yiming Ying¹

¹University at Albany, SUNY, Albany, NY ²University of Birmingham, Birmingham

³City University of Hong Kong, Hong Kong ⁴University of Iowa City, IA

zyang6@albany.edu, y.lei@hbam.ac.uk, puyuwang@cityu.edu.hk,
tianbao-yang@uiowa.edu, yying@albany.edu

Abstract

Pairwise learning refers to learning tasks where the loss function depends on a pair of instances. It instantiates many important machine learning tasks such as bipartite ranking and metric learning. A popular approach to handle streaming data in pairwise learning is an online gradient descent (OGD) algorithm, where one needs to pair the current instance with a buffering set of previous instances with a sufficiently large size and therefore suffers from a scalability issue. In this paper, we propose simple stochastic and online gradient descent methods for pairwise learning. A notable difference from the existing studies is that we only pair the current instance with the previous one in building a gradient direction, which is efficient in both the storage and computational complexity. We develop novel stability results, optimization, and generalization error bounds for both convex and nonconvex as well as both smooth and nonsmooth problems. We introduce novel techniques to decouple the dependency of models and the previous instance in both the optimization and generalization analysis. Our study resolves an open question on developing meaningful generalization bounds for OGD using a buffering set with a very small fixed size. We also extend our algorithms and stability analysis to develop differentially private SGD algorithms for pairwise learning which significantly improves the existing results.

1 Introduction

Many important learning tasks involve pairwise loss functions which are often referred to as pairwise learning. Such notable learning tasks include AUC maximization [14, 22, 28, 35, 43, 45], metric learning [4, 24, 37, 38, 41], and a minimum error entropy principle [18]. For instance, AUC maximization aims to rank positive instances above negative ones which involves a loss $f(\mathbf{w}; (x, y), (x', y')) = (1 - \mathbf{w}^\top (x - x'))_+ \mathbb{I}_{[y=1 \wedge y'=-1]}$ with $x, x' \in \mathcal{X} \subseteq \mathbb{R}^d$ and $y, y' \in \mathcal{Y} = \{\pm 1\}$. The aim of metric learning is to learn a distance function $h_{\mathbf{w}}(x, x') = (x - x')^\top \mathbf{w} (x - x')$ where \mathbf{w} is positive semi-definite matrix in $\mathbb{R}^{d \times d}$. A typical pairwise loss can be $f(\mathbf{w}; (x, y), (x', y')) = (1 + \tau(y, y') h_{\mathbf{w}}(x, x'))_+$ where $\tau(y, y') = 1$ if $y = y'$ and -1 otherwise. Given a training data $S = \{z_i = (x_i, y_i) \in \mathcal{X} \times \mathcal{Y} : i \in [n]\}$ where $[n] = \{1, 2, \dots, n\}$, the ERM formulation for pairwise learning is defined as $\min_{\mathbf{w} \in \mathcal{W}} \frac{1}{n(n-1)} \sum_{i,j \in [n], i \neq j} f(\mathbf{w}; z_i, z_j)$ where \mathcal{W} denotes the parameter space. This scheme has been well studied theoretically using algorithmic stability [1] and U-statistics tools [10]. At the same time, there are considerable interests

* Equal contributions. The corresponding author is Yiming Ying.

on developing and studying online gradient descent (OGD) or stochastic gradient descent (SGD) algorithms for pairwise learning due to their scalability in practice.

The critical issue for designing such stochastic algorithms is to construct intersecting pairs of instances for updating the model parameter upon receiving individual instances. For the offline (finite-sum) setting where the prescribed training data $S = \{z_1, \dots, z_n\}$ is available, one natural approach is to, at each time t , randomly select a pair of instances (z_{i_t}, z_{j_t}) from $n(n-1)/2$ pairs and update \mathbf{w} based on the gradient of the local error $f(\mathbf{w}_{t-1}; z_{i_t}, z_{j_t})$. The excess generalization and stability was nicely established in [27]. One popular approach [22, 36, 42, 45] is to consider the online setting where the data is continuously arriving. This approach pairs the current datum $z_t = (x_t, y_t)$, which is received at time t , with all previous instances $S_{t-1} = \{z_1, \dots, z_{t-1}\}$ and then performs the update based on the gradient of the local error $f(\mathbf{w}_{t-1}; S_{t-1}) = \frac{1}{t-1} \sum_{z \in S_{t-1}} f(\mathbf{w}_{t-1}; z_t, z)$. It requires a high gradient complexity $\mathcal{O}(t)$ (i.e. the number of computing gradients) which is expensive when t becomes large. To mitigate this potential limitation, [22, 35, 45] proposed to use a buffering set $B_{t-1} \subseteq S_{t-1}$ of size s and the local error $f(\mathbf{w}_{t-1}; B_{t-1}) = \frac{1}{s} \sum_{z \in B_{t-1}} f(\mathbf{w}_{t-1}; z_t, z)$ which reduces the gradient complexity to $\mathcal{O}(s)$. The excess generalization bound $\mathcal{O}(\frac{1}{\sqrt{s}} + \frac{1}{\sqrt{n}})$ was established in [22] using the online-to-batch conversion method [8] which is only meaningful for a very large s . In particular, this bound tends to zero only when $s = s(n)$ tends to infinity as n tends to infinity. It was mentioned in [22] (see the discussion at the end of Section 7 there) as an open question on how to get a meaningful bound for a fixed constant s .

In this paper, we show that optimal generalization bounds can be achieved for simple SGD and OGD algorithms for pairwise learning where, at time t , the current instance z_t is only paired with the previous instance z_{t-1} . This is equivalent to the First-In-First-Out (FIFO) buffering strategy [22, 35] while keeping the size s of the buffering set B_{t-1} to be $s = 1$, where, in this FIFO policy, the data z_t arriving at time $t > 1$ is included into the buffer by removing $\{z_1, \dots, z_{t-2}\}$ from the buffer. In particular, our main contributions are summarized as follows.

- We propose simple SGD and OGD algorithms for pairwise learning where the t -th update of the model parameter is based on the interacting of the current instance and the previous one which has a constant gradient complexity $\mathcal{O}(1)$.
- We establish the stability results of the proposed SGD algorithms for pairwise learning and apply them to derive optimal excess generalization bounds $\mathcal{O}(1/\sqrt{n})$ for the proposed simple SGD algorithm for pairwise learning with both convex and nonconvex as well as both smooth and nonsmooth losses in the offline (finite-sum) setting where the training data of size n is given. We introduce novel techniques to decouple the dependency of the current SGD iterate with the previous instance in both the generalization and optimization error analysis, which resolves the open question in [22] on how to develop meaningful generalization bounds when the buffering set of FIFO has a very small size.
- We further develop a localization version of our SGD algorithms under (ϵ, δ) -differential privacy (DP) constraints, and apply the obtained stability results to derive an optimal utility (excess generalization) bound $\tilde{\mathcal{O}}(1/\sqrt{n} + \sqrt{d}/n\epsilon)$. In contrast to the existing work [21] which requires the loss function to be smooth and an at least quadratic gradient complexity, our proposed DP algorithms only need a linear gradient complexity $\tilde{\mathcal{O}}(n)$ for smooth convex losses to achieve the optimal utility bound and can also be applied to non-smooth convex losses.

The paper is organized as follows. Section 2 reviews the related work and Section 3 describes the proposed algorithms. In Section 4, we present excess generalization bounds, stability results, and optimization errors of our algorithms. Section 5 is devoted to the differentially private SGD for pairwise learning and its utility bounds. Section 6 provides experimental validation of theoretical findings. The paper is concluded in Section 7. All the main proofs are postponed to the Appendix.

2 Motivating Examples and Related Work

In this section, we list examples of pairwise learning and discuss some related work.

2.1 Motivating Examples

AUC maximization. Area under the ROC curve (AUC) of a prediction function $h_{\mathbf{w}}$ is the probability that the function ranks a random positive example higher than a random negative example. The empirical risk of AUC maximization is given by $F_S(\mathbf{w}) = \frac{1}{n(n-1)} \sum_{i,j \in [n], i \neq j} \ell(h_{\mathbf{w}}(\mathbf{x}_i) - h_{\mathbf{w}}(\mathbf{x}_j)) \mathbb{I}_{[y_i=1]} \mathbb{I}_{[y_j=-1]}$, where the loss $\ell(\cdot)$ can be the least square loss $\ell(t) = (1-t)^2$ or the hinge loss $\ell(t) = (1-t)_+$.

Minimum error entropy principle. Minimum error entropy (MEE) is a principle of information theoretical learning [18–20], which has found applications in blind source separation, clustering, feature selection and some other topics. The MEE principle aims to find a predictor $h : \mathcal{X} \mapsto \mathcal{Y}$ that contains the most information of the response variable by minimizing the information entropy of the variable $E = Y - h(X)$. For a random variable E with probability density function p_E , the Rényi’s entropy of order 2 is defined as $H(E) = -\log \mathbb{E}[p_E] = -\log \int p_E^2(e) de$. The probability density function p_E can be approximated by Parzen windowing $\hat{p}_E(e) = \frac{1}{n\gamma} \sum_{i=1}^n G\left(\frac{(e-e_i)^2}{2\gamma^2}\right)$, where $e_i = y_i - h(x_i)$, $\gamma > 0$ is an MEE scaling parameter and $G : \mathbb{R} \mapsto \mathbb{R}^+$ is a windowing function. The approximation of Rényi’s entropy is given by its empirical version $\hat{H} = -\log \frac{1}{n^2\gamma} \sum_{i,j \in [n]} G\left(\frac{(e_i-e_j)^2}{2\gamma^2}\right)$. The maximization of \hat{H} then leads to a pairwise learning problem since each loss function involves a pair of training examples [18].

2.2 Related Work

The work [22, 35, 36, 45] assumed the online learning setting in which a stream of i.i.d. data $\{z_1, z_2, \dots, z_t, \dots\}$ is continuously arriving. Upon receiving z_t at time t , it is paired with all previous instances and then the model parameter is updated based on the local error $F_t(\mathbf{w}_{t-1}) = \frac{1}{t-1} \sum_{j=1}^{t-1} f(\mathbf{w}_{t-1}; \mathbf{z}_t, \mathbf{z}_j)$. In particular, the work [35, 36] provided the first excess generalization bound for online learning methods by obtaining online-to-batch conversion bounds [8] using covering numbers of function classes. Kar et al. [22] significantly improved the results using the so-called symmetrization of expectations which reduce excess risk estimates to Rademacher complexities. To further reduce the expensive gradient complexity $\mathcal{O}(t)$ at a large time t , the work [22, 36, 45] proposed to use a buffering set B_{t-1} with size s instead of all previous instances. It was shown that such OGD algorithms have an excess generalization bound $\mathcal{O}(\frac{1}{\sqrt{s}} + \frac{1}{\sqrt{n}})$ for convex and Lipschitz-continuous losses. In the offline learning setting where the training data $S = \{z_1, z_2, \dots, z_n\}$ of size n is fixed, the work [40] considered the stochastic version of the algorithm in [22, 35] where, at time t , a random instance z_{i_t} with random index $i_t \in \{1, \dots, n\}$ is paired with all previous instances $\{z_1, \dots, z_{i_t-1}\}$. They derived stability and generalization results of such algorithms in expectation.

Lei et al. [27] considered the offline learning setting and, at time t , the algorithm there randomly picks a pair of instances $(\mathbf{z}_{i_t}, \mathbf{z}_{j_t})$ from all $\binom{n}{2}$ pairs of instances. An excess risk bound $\tilde{\mathcal{O}}(1/\sqrt{n})$ with high probability was derived for convex, Lipschitz and strongly smooth losses. Here the notation $\tilde{\mathcal{O}}(\cdot)$ means $\mathcal{O}(\cdot)$ up to some logarithmic terms. In the particular case of AUC maximization with the least square loss, [43] considered the online learning setting and reformulated the problem as a stochastic saddle point (min-max) problem which decouples the pairwise structure. From this reformulation, efficient SGD-type algorithms [29, 41] have been developed.

Recently, differentially private pairwise learning has been studied where the construction of pairs of instances follows [22, 35, 45] or all pairs are used at each iteration. In particular, Huai et al. [21] considered both online and offline learning settings and the pairs of instances at time t follow [22, 35, 45]. They provided a utility bound $\tilde{\mathcal{O}}(\sqrt{d}/(\sqrt{n}\epsilon))$ for convex and smooth loss functions. The study [40] also paired the current instance with all previous ones and showed that SGD with output perturbation for pairwise learning has a utility bound $\tilde{\mathcal{O}}(\sqrt{d}/(\sqrt{n}\epsilon))$ for nonsmooth convex losses. The work [39] showed that private gradient descent using all possible pairs can achieve a utility bound $\tilde{\mathcal{O}}(1/\sqrt{n} + \sqrt{d}/(n\epsilon))$ for strongly smooth and convex losses.

3 Proposed Algorithms for Pairwise Learning

In this section, we describe the proposed algorithms in two common learning settings for pairwise learning: offline and online learning settings. Let ρ be a probability measure defined on $\mathcal{Z} := \mathcal{X} \times \mathcal{Y}$, where \mathcal{X} is an input space and \mathcal{Y} is an output space. In pairwise learning, the performance of \mathbf{w} is measured on a pair of instances (z, z') by a nonnegative loss function $f(\mathbf{w}; z, z')$. Denote by $[n] := \{1, 2, \dots, n\}$ for any $n \in \mathbb{N}$.

Algorithm 1 SGD for Pairwise Learning	Algorithm 2 OGD for Pairwise Learning
<pre> 1: Inputs: $S = \{z_i : i \in [n]\}$ and step sizes $\{\eta_t\}$ 2: Initialize: $\mathbf{w}_0 \in \mathcal{W}$, let $\mathbf{w}_{-1} = \mathbf{w}_0$ and randomly select $i_0 \in [n]$ 3: for $t = 1, 2, \dots, T$ do 4: Randomly select $i_t \in [n]$ 5: $\mathbf{w}_t = \Pi_{\mathcal{W}}(\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}))$ 6: Outputs: $\bar{\mathbf{w}}_T = \sum_{j=1}^T \eta_j \mathbf{w}_{j-2} / \sum_{j=1}^T \eta_j$ </pre>	<pre> 1: Inputs: learning rates $\{\eta_t\}$ 2: Initialize: $\mathbf{w}_0 \in \mathcal{W}$, let $\mathbf{w}_{-1} = \mathbf{w}_0$ and receiving datum z_0. 3: for $t = 1, 2, \dots, T$ do 4: Receive a data point z_t 5: $\mathbf{w}_t = \Pi_{\mathcal{W}}(\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_t, z_{t-1}))$ 6: Outputs: $\tilde{\mathbf{w}}_T = \sum_{j=1}^T \eta_j \mathbf{w}_{j-2} / \sum_{j=1}^T \eta_j$ </pre>

Offline Learning (Finite-Sum) Setting. The first is the finite-sum setting where the training data $S = \{z_i = (x_i, y_i) \in \mathcal{Z} : i \in [n]\}$ are drawn independently according to ρ . In this context, one aims to solve the following empirical risk minimization (ERM):

$$\mathbf{w}_S^* = \underset{\mathbf{w} \in \mathcal{W}}{\operatorname{argmin}} \left[F_S(\mathbf{w}) := \frac{1}{n(n-1)} \sum_{i,j \in [n], i \neq j} f(\mathbf{w}; z_i, z_j) \right]. \quad (1)$$

Our proposed algorithm to solve (1) is described in Algorithm 1. The notation $\Pi_{\mathcal{W}}(\cdot)$ there denotes the projection operator to \mathcal{W} . In particular, at iteration t , it randomly selects one instance z_{i_t} from the uniform distribution over $[n]$ and pairs it only with the previous instance $z_{i_{t-1}}$, and then do the gradient descent based on $\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}})$. This is in contrast to the classical SGD for pairwise learning in [22, 35, 45] where the present instance z_{i_t} is paired with all previous instances $\{z_{i_1}, z_{i_2}, \dots, z_{i_{t-1}}\}$. Note \mathbf{w}_{t-1} depends on $z_{i_{t-1}}$ and then $\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}})$ is not an unbiased estimate of $\nabla F_S(\mathbf{w}_{t-1})$. Therefore, the standard analysis of SGD does not apply. We introduce novel techniques to handle this dependency in our analysis (see more details in Section 4).

Online Learning Setting. In the online learning setting where the data $\{z_0, z_1, z_2, \dots\}$ is assumed i.i.d. from an unknown distribution ρ on \mathcal{Z} , the number of iterations of an online algorithm is identical to the size of available data. In the same spirit to Algorithm 1, the pseudo code is given in Algorithm 2. Specifically, upon receiving a datum z_t at the current time t , we pair it with z_{t-1} which was revealed at the previous time $t-1$ and then perform gradient descent based on the gradient $\nabla f(\mathbf{w}_{t-1}; z_t, z_{t-1})$. It aims to minimize the population risk which is defined as $F(\mathbf{w}) = \mathbb{E}_{Z, Z'}[f(\mathbf{w}; Z, Z')]$. Here $\mathbb{E}_{Z, Z'}$ denotes the expectation with respect to (w.r.t.) $Z, Z' \sim \rho$.

It is worth pointing out that online learning [17, 30, 31] in general does not require the i.i.d. assumption on the data and study the regret bounds. In this paper, we mainly consider the statistical performance, measured by excess generalization bounds, of the output $\tilde{\mathbf{w}}_T$ of Algorithm 2 where the streaming data $\{z_0, z_1, z_2, \dots\}$ is i.i.d. from the population distribution ρ .

Remark 1. As discussed above, OGD for pairwise learning was proposed and studied in [22, 35] where the current instance z_t is paired with a buffering set $B_t \subseteq \{z_1, \dots, z_{t-1}\}$. However, the resultant excess generalization bound is in the form of $\mathcal{O}(\frac{1}{\sqrt{s}} + \frac{1}{\sqrt{n}})$ which indicated that the buffer size s needs to be large enough in order to achieve good generalization. Their analysis does not apply to our case since the buffering set $B_t = \{z_{t-1}\}$ with size $s = 1$ for Algorithm 2. As we show soon in Section 4, we can prove that Algorithm 2, which pairs the current instance z_t with the previous instance z_{t-1} , still enjoys optimal statistical performance $\mathcal{O}(1/\sqrt{n})$.

Remark 2. The work [27] studied the stability and generalization of an SGD-type algorithm for pairwise learning by randomly generating pairs of instances. Specifically, at time t , randomly generating a pair (z_{i_t}, z_{j_t}) from a given set of training data $S = \{z_i : i \in [n]\}$ and the subsequent update is given by $\mathbf{w}_t = \mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{j_t})$. In contrast, our algorithm, i.e. Algorithm 1, updates the model parameter based on the pair of the current random instance and the random one generated at the previous time $t-1$, i.e. $(z_{i_t}, z_{i_{t-1}})$. Furthermore, our work here significantly

differs from [27] in the following aspects. Firstly, the algorithm there by randomly selecting pairs of instances does not work in the online learning setting while ours can seamlessly deal with the streaming data as stated in Algorithm 2. Secondly, regarding the technical analysis, our algorithms are more challenging to analyze than the algorithm in [27]. Indeed, $\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{j_t})$ is not an unbiased estimate of $\nabla F_S(\mathbf{w}_{t-1})$ due to the independency between \mathbf{w}_{t-1} and (i_t, j_t) . Therefore, the optimization error analysis of the algorithm in [27] is the same as the SGD for pointwise learning. As a comparison, $\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}})$ is a biased estimate of $\nabla F_S(\mathbf{w}_{t-1})$ due to the coupling between \mathbf{w}_{t-1} and i_{t-1} . We introduce novel techniques to handle this coupling for both the optimization and generalization analyses. Thirdly, we will soon see below that we provide generalization results for nonsmooth, nonconvex losses and also use Algorithm 1 to develop novel differentially private pairwise learning algorithms while [27] focused on the smooth convex losses in the non-private setting.

Remark 3. If we let $\xi_t = (i_t, i_{t-1})$ in Algorithm 1, then $\{\xi_t : t \in \mathbb{N}\}$ forms a Markov Chain as ξ_t only depends on ξ_{t-1} but not on $\{\xi_1, \dots, \xi_{t-2}\}$. Hence, Algorithm 2 can be regarded as a Markov Chain SGD which was studied in [34]. Despite this similarity, our results differ from [34] in two important aspects. Firstly, we are mainly interested in stability and generalization of Algorithm 1 while [34] focused on the convergence analysis of the Markov Chain SGD. One cannot apply the results in [34] to obtain excess generalization bounds for Algorithm 1 in terms of the population risk as we will show soon in the next section. Secondly, directly applying Theorem 1 in [34] only yields a convergence rate of $\mathcal{O}(1/t^{1-q})$ with some $1/2 < q < 1$ in the convex setting. Our proof for the convergence analysis of Algorithm 1 is much simpler and direct which can yield a faster convergence rate $\mathcal{O}(1/\sqrt{t})$ as shown in Section 4.3.

4 Generalization Analysis

The aim for the generalization analysis of Algorithm 1 and Algorithm 2 is the same, i.e. to analyze the excess generalization error $F(\mathbf{w}) - F(\mathbf{w}^*)$ of a model \mathbf{w} measuring its relative behavior w.r.t. the best model $\mathbf{w}^* = \arg \min_{\mathbf{w} \in \mathcal{W}} F(\mathbf{w})$.

For Algorithm 1 where the training data S with n datum is given beforehand, the excess generalization involves the generalization error and optimization error. Specifically, one has the following error decomposition for $\bar{\mathbf{w}}_T$

$$\mathbb{E}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathbb{E}[F(\bar{\mathbf{w}}_T) - F_S(\bar{\mathbf{w}}_T)] + \mathbb{E}[F_S(\bar{\mathbf{w}}_T) - F_S(\mathbf{w}^*)]. \quad (2)$$

Here, the expectation is taken w.r.t. the randomness of Algorithm 1, i.e., $\{i_t\}$ and the randomness of data S which is i.i.d. from ρ on \mathcal{Z} . We refer to the first term $\mathbb{E}[F(\bar{\mathbf{w}}_T) - F_S(\bar{\mathbf{w}}_T)]$ as the generalization error and $\mathbb{E}[F_S(\bar{\mathbf{w}}_T) - F_S(\mathbf{w}^*)]$ as the optimization error. We will use algorithmic stability to handle its generalization error in Subsection 4.2 for smooth and nonsmooth losses. The estimation of the optimization error is given in Subsection 4.3 for both convex and nonconvex losses. For Algorithm 2, there is no generalization error as the data $\{z_1, z_2, \dots, z_T\}$ is arriving in a sequential manner with T increasing all the time which does not involve the training data. The randomness of Algorithm 2 is only from the i.i.d. data. Therefore, the optimization error in this setting is exactly the excess generalization error $F(\bar{\mathbf{w}}_T) - F(\mathbf{w}^*)$ which is estimated in Subsection 4.3.

4.1 Excess Generalization Error

In this subsection, we present excess generalization error bounds of Algorithm 1 in terms of the sample size, iteration number and step size, which shows how to tune these parameters to get a model with good generalization. Our analysis requires the following assumptions.

Assumption. Let $f : \mathcal{W} \times \mathcal{Z} \times \mathcal{Z} \rightarrow \mathbb{R}^+$ and let $\|\cdot\|_2$ denote the Euclidean norm.

- (A1) Assume, for any z, z' and $\mathbf{w} \in \mathcal{W}$, that $f(\cdot; z, z')$ is G -Lipschitz continuous, i.e. $|f(\mathbf{w}; z, z') - f(\mathbf{w}'; z, z')| \leq G\|\mathbf{w} - \mathbf{w}'\|_2$.
- (A2) Assume, for any $z, z' \in \mathcal{Z}$, the map $\mathbf{w} \mapsto f(\mathbf{w}; z, z')$ is L -strongly smooth, i.e. $f(\mathbf{w}; z, z') - f(\mathbf{w}'; z, z') - \langle \nabla f(\mathbf{w}'; z, z'), \mathbf{w} - \mathbf{w}' \rangle \leq \frac{L}{2}\|\mathbf{w} - \mathbf{w}'\|_2^2$.
- (A3) Assume, for any $z, z' \in \mathcal{Z}$, $f(\cdot; z, z')$ is α -strongly convex, i.e. $f(\mathbf{w}; z, z') - f(\mathbf{w}'; z, z') - \langle \nabla f(\mathbf{w}'; z, z'), \mathbf{w} - \mathbf{w}' \rangle \geq \frac{\alpha}{2}\|\mathbf{w} - \mathbf{w}'\|_2^2$. The case of $\alpha = 0$ is identical to convexity.

(A4) Assume F_S satisfies the Polyak-Łojasiewicz (PL) condition with parameter $\mu > 0$, i.e., for $\mathbf{w}_S \in \arg \min_{\mathbf{w} \in \mathcal{W}} F_S(\mathbf{w})$, there holds $2\mu(F_S(\mathbf{w}) - F_S(\mathbf{w}_S)) \leq \|\nabla F_S(\mathbf{w})\|_2^2$ for all $\mathbf{w} \in \mathcal{W}$.

The PL condition **(A4)** means that the suboptimality in terms of function values can be bounded by gradients [23]. Functions under the PL condition have found various applications including neural networks, matrix factorization, generalized linear models and robust regression (see, e.g., [23]). In particular, AUC maximization problem with the classifier given by a one hidden layer network satisfies the PL condition as shown in [29].

We first study smooth and non-smooth problems for the convex case, and derive the excess generalization bounds of the order $\mathcal{O}(1/\sqrt{n})$ in both cases. We use the notation $B \asymp \tilde{B}$ if there exist constants $c_1, c_2 > 0$ such that $c_1 \tilde{B} \leq B \leq c_2 \tilde{B}$. The proofs are given in Section C.

Theorem 1 (Nonsmooth Problems). *Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_t : t \in [T]\}$ be produced by Algorithm 1 with $\eta_t = \eta > 0$. Let $\bar{\mathbf{w}}_T = \sum_{t=1}^T \eta_t \mathbf{w}_{t-2} / \sum_{t=1}^T \eta_t$. Let (A1) and (A3) hold true with $\alpha = 0$. Then, we have*

$$\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}\left(\sqrt{T}\eta + \frac{T\eta}{n} + \frac{1+T\eta^2}{T\eta}\right). \quad (3)$$

Furthermore, selecting $T \asymp n^2$ and $\eta \asymp T^{-\frac{3}{4}}$ yields that $\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}(1/\sqrt{n})$.

Theorem 2 (Smooth Problems). *Let (A1), (A2) and (A3) hold true with $\alpha = 0$. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_t : t \in [T]\}$ be produced by Algorithm 1 with $\eta_t = \eta \leq 2/L$. Let $\bar{\mathbf{w}}_T = \sum_{t=1}^T \eta_t \mathbf{w}_{t-2} / \sum_{t=1}^T \eta_t$. Then, there holds*

$$\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}\left(\frac{T\eta}{n} + \frac{1+T\eta^2}{T\eta}\right). \quad (4)$$

Furthermore, choosing $T \asymp n$ and $\eta \asymp T^{-\frac{1}{2}}$ implies that $\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}(1/\sqrt{n})$.

Remark 4. Notice that the gradient complexity (i.e. the number of computing gradients) of Algorithm 1 is identical to the number of iterations T . The above results show, to get excess generalization bounds $\mathcal{O}(1/\sqrt{n})$, that Algorithm 1 requires a gradient complexity $\mathcal{O}(n^2)$ for nonsmooth problems, and $\mathcal{O}(n)$ for smooth problems. This matches the existing generalization analysis for pointwise learning [3, 16, 25]. In Appendix E, additional results are provided where we propose Algorithm 4 based on the iterative localization technique [12] in order to reduce the gradient complexity $\mathcal{O}(n^2)$ required in Theorem 1 to $\mathcal{O}(n)$ for nonsmooth problems.

Remark 5. As stated in the introduction, Algorithm 1 can be considered as a specific case of the classic pairwise learning algorithm [22] with a FIFO buffering set B_{t-1} of size $s = 1$. A key difficulty in the generalization analysis is that \mathbf{w}_{t-1} depends on B_{t-1} , which renders the standard martingale analysis not applicable. Kar et al. [22] proposed to remove this coupling effect by considering $\sup_{\mathbf{w}} [f(\mathbf{w}; B_{t-1}) - F_S(\mathbf{w})]$, which is why they only derived the excess generalization error bound $\mathcal{O}(1/\sqrt{s})$. We introduce novel techniques to handle the coupling in both generalization analysis and optimization error analysis. For the generalization analysis, our strategy is to write the stability as a deterministic function of several indicator functions on whether we select the different point in neighboring datasets, and then finally consider the randomness of these indicator functions. This delay of considering expectation successfully decouples the coupling between \mathbf{w}_{t-1} and B_{t-1} . For the optimization error analysis, our novelty is to observe that $f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) = f(\mathbf{w}_{t-2}; z_{i_t}, z_{i_{t-1}}) + \mathcal{O}(\eta_{t-1})$, which removes the decoupling since \mathbf{w}_{t-2} is now independent of both i_t and i_{t-1} . Since the additional term $\mathcal{O}(\eta_{t-1})$ here is a term of smaller magnitude, the coupling effect is removed without incurring any additional cost.

Finally, we study nonconvex pairwise learning under the PL condition. The proof is in Section C.

Theorem 3. *Let (A1), (A2) and (A4) hold true. Let $\alpha_0, B > 0$. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1 with $\eta_j = 2/(\mu(j+1))$. If $\mathbb{E}_{i_{j+1}, i_{j+2}} [\|\nabla f(\mathbf{w}_j; z_{i_{j+1}}, z_{i_{j+2}})\|_2^2] \leq \alpha_0^2$ and $\sup_{z,z'} f(\mathbf{w}_j; z, z') \leq B$ for any j , then*

$$\mathbb{E}[F(\mathbf{w}_T)] - F(\mathbf{w}^*) = \mathcal{O}\left(\frac{T^{\frac{2L}{2L+\mu}}}{n}\right) + \mathcal{O}(1/(T\mu^2)).$$

Furthermore, choosing $T \asymp n^{\frac{2L+\mu}{4L+\mu}} \mu^{-\frac{4L+2\mu}{4L+\mu}}$ yields that $\mathbb{E}[F(\mathbf{w}_T)] - F(\mathbf{w}^*) = n^{-\frac{2L+\mu}{4L+\mu}} \mu^{-\frac{4L}{4L+\mu}}$.

Remark 6. As pointed out before, there is no generalization error for the OGD algorithm, i.e. Algorithm 2 as the i.i.d. data is given in a streaming manner and the iteration number equals the number of the available data (i.e. $t = n$). In this setting, the optimization error is identical to the excess generalization error, which will be estimated in Subsection 4.3.

4.2 Stability and Generalization Errors

We study generalization errors by algorithmic stability, which measures the sensitivity of the output of an algorithm w.r.t. the perturbation of the dataset. Below we give the definition of uniform argument stability. We say S, S' are neighboring datasets if they differ at most by a single example.

Definition 1. A (randomized) algorithm \mathcal{A} for pairwise learning is called ε -uniformly argument stable if for all neighboring datasets $S, S' \in \mathcal{Z}^n$ we have $\mathbb{E}_{\mathcal{A}}[\|\mathcal{A}(S) - \mathcal{A}(S')\|_2] \leq \varepsilon$.

It is clear ε -uniform argument stability implies $G\varepsilon$ -uniform stability i.e., $\sup_{\mathbf{z}, \mathbf{z}'} \mathbb{E}_{\mathcal{A}}[f(\mathcal{A}(S), \mathbf{z}, \mathbf{z}') - f(\mathcal{A}(S'), \mathbf{z}, \mathbf{z}')] \leq G\varepsilon$ for Lipschitz losses [7]. The connection between the uniform stability for pairwise learning and its generalization has been established in the literature [1, 33].

Lemma 1. If an algorithm \mathcal{A} for pairwise learning is ε -uniformly stable for some $\varepsilon > 0$, then we have $|\mathbb{E}_{S, \mathcal{A}}[F_S(\mathcal{A}(S)) - F(\mathcal{A}(S))]| \leq 2\varepsilon$.

We develop uniform argument stability bound of Algorithm 1 and apply it together with Lemma 1 to establish the following generalization bounds. Theorem 4 handles nonsmooth problems, while Theorem 5 handles smooth problems. The detailed proofs for them can be found in Section A.

Theorem 4. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1 with $\eta_j = \eta$. Let (A1) and (A3) hold with $\alpha = 0$. Then, Algorithm 1 is $2\sqrt{e}G\eta(\sqrt{5t} + \frac{2t}{n})$ -uniformly argument stable and

$$\mathbb{E}_{S, \mathcal{A}}[F(\bar{\mathbf{w}}_t) - F_S(\bar{\mathbf{w}}_t)] \leq 4\sqrt{e}G^2\eta\left(\sqrt{5t} + \frac{2t}{n}\right).$$

Theorem 5. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1 with $\eta_j = \eta \leq 2/L$. Let (A1), (A2) and (A3) hold true with $\alpha = 0$. Then, Algorithm 1 is $\frac{4G}{n} \sum_{j=1}^t \eta_j$ -uniformly argument stable and the generalization error satisfies $\mathbb{E}_{S, \mathcal{A}}[F(\bar{\mathbf{w}}_t) - F_S(\bar{\mathbf{w}}_t)] \leq \frac{8G^2}{n} \sum_{j=1}^t \eta_j$.

For Algorithm 2, there is no generalization error as the data $\{z_1, z_2, \dots, z_T\}$ is assumed to arrive in a sequential manner with T increasing all the time which does not involve the training data.

4.3 Optimization Error

In this subsection, we establish the convergence rate, i.e. optimization error, of Algorithm 1 for convex, nonconvex and strongly convex problems. We consider both bounds in expectation and with high probability. Our analysis is based on the key observation $f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) = f(\mathbf{w}_{t-2}; z_{i_t}, z_{i_{t-1}}) + \mathcal{O}(\eta_{t-1})$. The proofs of results in this subsection are given in Section B.

Below we only present optimization error bounds for Algorithm 1 here in the offline (finite-sum) setting where the training data of size n , denoted by $S = \{z_1, \dots, z_n\}$, is fixed, and the optimization error is measured by $F_S(\bar{\mathbf{w}}_t) - \inf_{\mathbf{w} \in \mathcal{W}} F_S(\mathbf{w})$. We emphasize that all our optimization error bounds hold true for Algorithm 2 in the online learning setting with exactly the same analysis where the streaming data $\{z_1, \dots, z_t, \dots\}$ is assumed to be i.i.d according to the population distribution ρ , and the bounds for the optimization error in this case is given for the excess generalization error (excess population risk), i.e. $F(\tilde{\mathbf{w}}_t) - \inf_{\mathbf{w} \in \mathcal{W}} F(\mathbf{w})$.

Theorem 6. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1. Let (A1) and (A3) hold true with $\alpha \geq 0$. Then, for any \mathbf{w} independent of \mathcal{A} we have the following convergence rates:

(a) Assume f is convex, i.e. $\alpha = 0$. Then, we have

$$\mathbb{E}_{\mathcal{A}}[F_S(\bar{\mathbf{w}}_t)] - F_S(\mathbf{w}) \leq \frac{\|\mathbf{w}_0 - \mathbf{w}\|_2^2 + G^2 \sum_{j=1}^t (2\eta_j \eta_{j-1} + \eta_j^2)}{2 \sum_{j=1}^t \eta_j}. \quad (5)$$

(b) Let f be α -strongly convex with $\alpha > 0$ and $\eta_j = \frac{2}{\alpha(j+1)}$. Then, there holds $\mathbb{E}_{\mathcal{A}}[F_S(\bar{\mathbf{w}}_t)] - F_S(\mathbf{w}) = \mathcal{O}(G^2/(\alpha t))$.

Remark 7. The above convergence rates match those in the pointwise learning [5]. Furthermore, if $\eta_j = \eta$, then Eq. (5) becomes $\mathbb{E}_{\mathcal{A}}[F_S(\bar{\mathbf{w}}_t)] - F_S(\mathbf{w}) = \mathcal{O}(1/(t\eta) + \eta)$ and one can choose $\eta \asymp 1/\sqrt{t}$ to get $\mathbb{E}_{\mathcal{A}}[F_S(\bar{\mathbf{w}}_t)] - F_S(\mathbf{w}) = \mathcal{O}(1/\sqrt{t})$. We can extend our convergence analysis to a more general update as $\mathbf{w}_t = \Pi_{\mathcal{W}}(\mathbf{w}_{t-1} - \frac{\eta_t}{s} \sum_{j=1}^s \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-j}}))$ for $s \in \mathbb{N}$. Indeed, one can use the observation $f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-s}}) = f(\mathbf{w}_{t-s-1}; z_{i_t}, z_{i_{t-s}}) + \mathcal{O}(\sum_{j=1}^s \eta_{t-j})$ to derive the convergence rate $\mathcal{O}(\sqrt{s}/\sqrt{t})$.

Below we present high-probability bounds to understand the variation of the algorithm. We need to take conditional expectation of $f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}})$ w.r.t. (i_{2j}, i_{2j-1}) to get $F_S(\mathbf{w}_{2j-2})$. However, there is a coupling between (i_{2j}, i_{2j-1}) and (i_{2j-1}, i_{2j-2}) . Therefore, one can not directly apply concentration inequalities for martingales to handle $\sum_{j=1}^t (f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}}) - F_S(\mathbf{w}_{2j-2}))$. We introduce a novel decoupling technique to handle this coupling. Note that the high-probability bounds match the bounds in expectation up to a constant factor.

Theorem 7. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1. Let (A1) and (A3) hold true with $\alpha \geq 0$ and $\sup_{\mathbf{w}} f(\mathbf{w}; z, z') \leq B$ for some $B > 0$. Let $\delta \in (0, 1)$.

- (a) Assume f is convex, i.e. $\alpha = 0$ and let $\bar{\mathbf{w}}_t = \sum_{j=1}^t \eta_j \mathbf{w}_{j-2} / \sum_{j=1}^t \eta_j$. Then, for any $\mathbf{w} \in \mathcal{W}$, with probability at least $1 - \delta$ the following inequality holds

$$F_S(\bar{\mathbf{w}}_t) - F_S(\mathbf{w}) \leq \frac{1}{\sum_{j=1}^t \eta_j} \left(2B \left(2 \sum_{j=1}^t \eta_j^2 \log(2/\delta) \right)^{\frac{1}{2}} + \frac{1}{2} \|\mathbf{w}_1 - \mathbf{w}\|_2^2 + G^2 \sum_{j=1}^t (\eta_{j-1} \eta_j + \frac{\eta_j^2}{2}) \right).$$

- (b) Assume f is α -strongly convex with $\alpha > 0$ and $\eta_j = \frac{2}{\alpha(j+1)}$. Let $\bar{\mathbf{w}}_t = \sum_{j=1}^t j \mathbf{w}_{j-2} / \sum_{j=1}^t j$. Then, with probability at least $1 - \delta$, we have $F_S(\bar{\mathbf{w}}_t) - F_S(\mathbf{w}) = \mathcal{O}(G^2 \log(1/\delta) / (\alpha t))$.

Finally, we study the convergence of Algorithm 1 associated with nonconvex functions. We first consider general smooth problems. Since we cannot find a global minimum in this setting, we measure the convergence rate in terms of gradient norms [15]. The following theorem establishes the convergence rate $\mathcal{O}(1/\sqrt{t})$ for $\min_{j=1,\dots,t} \mathbb{E}_{\mathcal{A}}[\|\nabla F_S(\mathbf{w}_j)\|_2^2]$.

Theorem 8. Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1 with $\eta_j = \eta \leq 1/(2\sqrt{L})$. Let (A2) hold true and $\mathbb{E}_{i_{j+1}, i_{j+2}} [\|\nabla f(\mathbf{w}_j; z_{i_{j+1}}, z_{i_{j+2}})\|_2^2] \leq \alpha_0^2$ for some α_0 and any j . Then,

$$\frac{1}{t} \sum_{j=1}^t \mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] \leq \frac{F_S(\mathbf{w}_0)}{t\eta} + 8L\eta\alpha_0^2.$$

Furthermore, choosing $\eta \asymp 1/\sqrt{t}$ implies that $\frac{1}{t} \sum_{j=1}^t \mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] = \mathcal{O}(1/\sqrt{t})$.

We now turn to nonconvex problems under a PL condition. Theorem 9 gives convergence rates of the order $\mathcal{O}(1/t)$, which match the existing results for standard SGD in pointwise learning [23].

Theorem 9. Assume (A2) and (A4) hold true and $\mathbb{E}_{i_{j+1}, i_{j+2}} [\|\nabla f(\mathbf{w}_j; z_{i_{j+1}}, z_{i_{j+2}})\|_2^2] \leq \alpha_0^2$ for some α_0 and any j . Let $\mathbf{w}_{-1} = \mathbf{w}_0$ and $\{\mathbf{w}_j : j \in [t]\}$ be produced by Algorithm 1 with $\eta_j = 2/(\mu(j+1))$. Then

$$\mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_t) - F_S(\mathbf{w}_S)] \leq \frac{32L\alpha_0^2}{\mu^2} \left(\frac{1}{t+1} + \frac{\log(et)}{\mu t(t+1)} \right).$$

5 Application: Differentially Private SGD for Pairwise Learning

We now use Algorithm 1 and our stability analysis (i.e. Theorem 5) to develop a differentially private algorithm for pairwise learning. Let us start with the definition of differential privacy [11].

Definition 2. A (randomized) algorithm \mathcal{A} is called (ϵ, δ) -differentially private (DP) if, for all neighboring datasets S, S' and for all events O in the output space of \mathcal{A} , one has $\mathbb{P}[\mathcal{A}(S) \in O] \leq e^\epsilon \mathbb{P}[\mathcal{A}(S') \in O] + \delta$.

Algorithm 3 Differentially Private Localized SGD for Pairwise Learning

- 1: **Inputs:** Dataset $S = \{\mathbf{z}_i : i \in [n]\}$, parameters $\epsilon, \delta > 0$, and learning rate η , initial point \mathbf{w}_0
- 2: Set $K = \lceil \log_2 n \rceil$ and divide S into K disjoint subsets $\{S_1, \dots, S_K\}$ where $|S_k| = n_k = 2^{-k}n$.
- 3: **for** $k = 1$ to K **do**
- 4: Set $\eta_k = 4^{-k}\eta$
- 5: Compute $\bar{\mathbf{w}}_k$ by Algorithm 1 based on S_k and initiated at \mathbf{w}_{k-1} for $\lceil n_k \log(4/\delta) \rceil$ steps.
- 6: Set $\mathbf{w}_k = \bar{\mathbf{w}}_k + \mathbf{u}_k$ where $\mathbf{u}_k \sim \mathcal{N}(0, \sigma_k^2 I_d)$ with $\sigma_k = 12G\eta_k \log(4/\delta) \sqrt{2 \log(2.5/\delta)} / \epsilon$.
- 7: **Outputs:** \mathbf{w}_K

Our proposed DP algorithm for pairwise learning is described in Algorithm 3 which is inspired by the iterative localization technique [12] for pointwise learning. The privacy and utility guarantees are given by the following theorem. Here D denotes the diameter of \mathcal{W} .

Theorem 10. *Let (A1), (A2), and (A3) hold true with $\sigma = 0$. Let $\{\mathbf{w}_k : k \in [K]\}$ be produced by Algorithm 3 with $\eta = \frac{D}{C} \min\left\{\frac{\log(4/\delta)}{\sqrt{n}}, \frac{\epsilon}{12 \log(4/\delta) \sqrt{2d \log(2.5/\delta)}}\right\} \leq \frac{2}{L}$. Then, Algorithm 3 satisfies (ϵ, δ) -DP and, with gradient complexity $\mathcal{O}(n \log(1/\delta))$, we have the utility bound that*

$$\mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] = \mathcal{O}\left(GD\left(\frac{1}{\sqrt{n}} + \frac{\sqrt{d} \log^{\frac{3}{2}}(1/\delta)}{\epsilon n}\right)\right).$$

The main difference from the pointwise setting in [12] is that Algorithm 3 involves the coupling dependency between $\{i_t, i_{t-1}\}$ at time t in Algorithm 1 and $\{i_{t-1}, i_{t-2}\}$ at time $t-1$, which renders the direct application of the standard concentration inequalities infeasible. We propose a novel decomposition to circumvent this hurdle (see more detailed proof for Theorem 10 in Appendix D).

Remark 8. The above bound matches the lower bound given in [2] for (ϵ, δ) -differentially private pointwise learning up to a $\log(1/\delta)$ term. Our utility bound improves over the previous work [21] which has the bound $\mathcal{O}(\sqrt{d \log(1/\delta)} \log(n/\delta) / (\sqrt{n}\epsilon))$. During the preparation of this work, we notice a very recent paper [39] also studied the private version of pairwise algorithm by using the localization technique. Their algorithm establishes the optimal rate $\mathcal{O}(1/\sqrt{n} + \sqrt{d \log(1/\delta)} / (\epsilon n))$ which, however, needs an expensive gradient complexity $\mathcal{O}(n^3 \log(1/\delta))$. As a comparison, we achieve nearly optimal utility bound with linear gradient complexity $\mathcal{O}(n \log(1/\delta))$.

Remark 9. In Appendix F, we further remove the smoothness assumption (A2) required in Theorem 10 and propose a private algorithm (stated as Algorithm 5 there) that achieves the optimal rate $\mathcal{O}((1/\sqrt{n} + \sqrt{d \log(1/\delta)} / (\epsilon n)))$ with gradient complexity $\mathcal{O}(n^2 \log(1/\delta))$. Such bound improves over the previous known results with nonsmooth losses [40] where the utility bound was $\mathcal{O}(\sqrt{d \log(1/\delta)} \log(n/\delta) / (\sqrt{n}\epsilon))$.

6 Experimental Validation

We now report some preliminary experiments on AUC maximization with $f(\mathbf{w}; (\mathbf{x}, y), (\mathbf{x}', y')) = \ell(\mathbf{w}^\top (\mathbf{x} - \mathbf{x}')) \mathbb{I}_{[y=1 \wedge y'=-1]}$ where ℓ is a surrogate loss function, e.g., the hinge loss $\ell(t) = (1-t)_+$.

The purpose of our first experiment is to compare our algorithm, i.e. Algorithm 1, against four existing algorithms for pairwise learning in terms of generalization and CPU running time on several datasets available from the LIBSVM website [9]. These algorithms are: 1) OLP [22] uses a buffer B_t updated by a variant of Reservoir sampling with replacement where the buffer size is chosen to be 200 in order to guarantee the maximum AUC score as indicated in [22]; 2) OAM_{gra} [45] is tailored for AUC maximization with the hinge loss which uses buffers by Reservoir sampling. The buffer size is set to be 100 for both positive and negative buffers as suggested in that paper; 3) SGD_{pair} [27] randomly pick a pair from $\binom{n}{2}$ pairs by uniform distribution; 4) SPAUC [26], where AUC maximization problem with the least square loss was reformulated as stochastic saddle point (min-max) problem. Note that SPAUC and OAM_{gra} can only apply to AUC maximization problem with the least square loss and hinge loss, respectively.

To validate the generalization ability, the surrogate loss for Algorithm 1, SGD_{pair} and OLP is chosen to be the hinge loss. Average AUC scores of different algorithms are listed in Table 1 where we

Table 1: Average AUC score \pm standard deviation across multiple datasets. Our best results are highlighted in bold.

Algorithm	diabetes	german	ijcnn1	letter	mnist	usps
Ours	.831 \pm .030	.793 \pm .021	.934 \pm .002	.810 \pm .007	.932 \pm .001	.926 \pm .006
SGD _{pair} [27]	.830 \pm .028	.794 \pm .023	.934 \pm .003	.811 \pm .008	.932 \pm .001	.925 \pm .006
OLP [22]	.825 \pm .028	.787 \pm .028	.916 \pm .003	.808 \pm .010	.927 \pm .003	.917 \pm .006
OAM _{gra} [45]	.828 \pm .026	.785 \pm .029	.930 \pm .003	.806 \pm .008	.898 \pm .002	.916 \pm .005
SPAUC [26]	.828 \pm .031	.799 \pm .026	.932 \pm .002	.809 \pm .008	.927 \pm .002	.923 \pm .005

can see that our algorithm yields competitive generalization performance with OAM and OLP using a large buffering set. Detailed experimental setup, data statistics and more results such as comparison with OLP and OAM with the size of the buffering set $s = 1$ are listed in Appendix G.

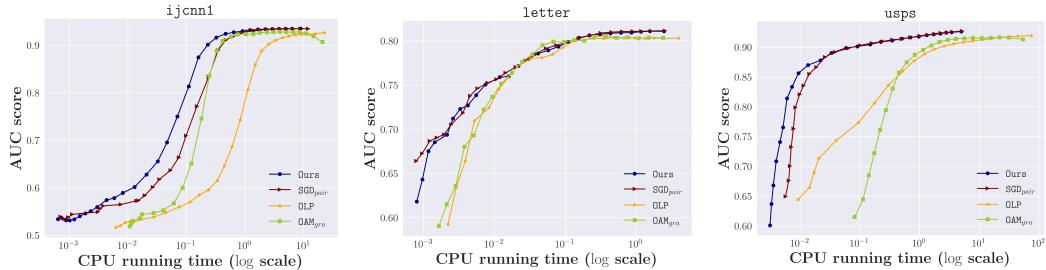


Figure 1: CPU running time (log scale) versus the AUC score

To fairly compare the CPU running time, we apply the following uniform setting across all algorithms: 1) \mathcal{W} is an ℓ_2 ball with the same diameter; 2) the step sizes $\eta_t = \eta$ which is tuned by cross validation. We report the results in Figure 1 for the hinge loss. We can see that CPU running time for our algorithm and SGD_{pair} are similar while OLP and OAM needs more time to converge. The possible reason behind this is that they have a high gradient complexity $\mathcal{O}(s)$ at each iteration while ours is $\mathcal{O}(1)$. More results on comparison for the least square loss and for differentially private algorithms are given in Appendix G.

7 Conclusion

In this paper, we propose simple stochastic and online gradient descent algorithms for pairwise learning. The key idea is to build a gradient estimator by pairing the current instance with the previous instance, which enjoys favorable computation and storage complexity. We leverage the lens of algorithmic stability to study its generalization and apply tools in optimization theory to study its convergence rates for various problems including convex/nonconvex and smooth/nonsmooth settings. We also use our algorithms and stability analysis to develop a new DP algorithm for pairwise learning with differential privacy constraints which significantly improves the existing results. The main difference from pointwise learning in the analysis is the coupling between models and previous instances, which is handled by introducing novel decoupling techniques.

For future work, it would be interesting to see whether the analysis and results still hold true if the current example \mathbf{z}_{i_t} in Algorithm 1 is paired with one arbitrary previous example (e.g., \mathbf{z}_{i_1}). Other future work would be a systematic extension of our algorithms using other acceleration schemes such as momentum and variance reduction techniques.

Acknowledgments

The authors are grateful to the anonymous reviewers for their constructive comments and suggestions. Yiming's work is supported by National Science Foundation (NSF) under grants DMS-2110836, IIS-1816227, IIS-2110546, and IIS-2103450.

References

- [1] S. Agarwal and P. Niyogi. Generalization bounds for ranking algorithms via algorithmic stability. *Journal of Machine Learning Research*, 10(Feb):441–474, 2009.
- [2] R. Bassily, A. Smith, and A. Thakurta. Private empirical risk minimization: Efficient algorithms and tight error bounds. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pages 464–473. IEEE, 2014.
- [3] R. Bassily, V. Feldman, C. Guzmán, and K. Talwar. Stability of stochastic gradient descent on nonsmooth convex losses. *Advances in Neural Information Processing Systems*, 33, 2020.
- [4] A. Bellet, A. Habrard, and M. Sebban. A survey on metric learning for feature vectors and structured data. *arXiv preprint arXiv:1306.6709*, 2013.
- [5] L. Bottou, F. E. Curtis, and J. Nocedal. Optimization methods for large-scale machine learning. *SIAM Review*, 60(2):223–311, 2018.
- [6] S. Boucheron, G. Lugosi, and P. Massart. *Concentration Inequalities: A Nonasymptotic Theory of Independence*. Oxford university press, 2013.
- [7] O. Bousquet and A. Elisseeff. Stability and generalization. *Journal of machine learning research*, 2(Mar):499–526, 2002.
- [8] N. Cesa-Bianchi, A. Conconi, and C. Gentile. On the generalization ability of on-line learning algorithms. *IEEE Transactions on Information Theory*, 50(9):2050–2057, 2004.
- [9] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2:27:1–27:27, 2011. Software available at <http://www.csie.ntu.edu.tw/~cjlin/libsvm>.
- [10] S. Cléménçon, G. Lugosi, and N. Vayatis. Ranking and empirical minimization of U-statistics. *The Annals of Statistics*, pages 844–874, 2008.
- [11] C. Dwork, A. Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.
- [12] V. Feldman, T. Koren, and K. Talwar. Private stochastic convex optimization: optimal rates in linear time. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 439–449, 2020.
- [13] D. J. Foster, A. Sekhari, and K. Sridharan. Uniform convergence of gradients for non-convex learning and optimization. In *Advances in Neural Information Processing Systems*, pages 8759–8770, 2018.
- [14] W. Gao, R. Jin, S. Zhu, and Z.-H. Zhou. One-pass auc optimization. In *International Conference on Machine Learning*, pages 906–914, 2013.
- [15] S. Ghadimi and G. Lan. Stochastic first-and zeroth-order methods for nonconvex stochastic programming. *SIAM Journal on Optimization*, 23(4):2341–2368, 2013.
- [16] M. Hardt, B. Recht, and Y. Singer. Train faster, generalize better: Stability of stochastic gradient descent. In *International Conference on Machine Learning*, pages 1225–1234, 2016.
- [17] E. Hazan. Introduction to online convex optimization. *Foundations and Trends® in Optimization*, 2(3-4):157–325, 2016.
- [18] T. Hu, J. Fan, Q. Wu, and D.-X. Zhou. Learning theory approach to minimum error entropy criterion. *Journal of Machine Learning Research*, 14(2), 2013.
- [19] T. Hu, J. Fan, Q. Wu, and D.-X. Zhou. Regularization schemes for minimum error entropy principle. *Analysis and Applications*, 13(04):437–455, 2015.
- [20] T. Hu, Q. Wu, and D.-X. Zhou. Distributed kernel gradient descent algorithm for minimum error entropy principle. *Applied and Computational Harmonic Analysis*, 49(1):229–256, 2020.
- [21] M. Huai, D. Wang, C. Miao, J. Xu, and A. Zhang. Pairwise learning with differential privacy guarantees. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 694–701, 2020.
- [22] P. Kar, B. Sriperumbudur, P. Jain, and H. Karnick. On the generalization ability of online learning algorithms for pairwise loss functions. In *International Conference on Machine Learning*, pages 441–449, 2013.
- [23] H. Karimi, J. Nutini, and M. Schmidt. Linear convergence of gradient and proximal-gradient methods under the polyak-łojasiewicz condition. In *European Conference on Machine Learning*, pages 795–811, 2016.

- [24] B. Kulis et al. Metric learning: A survey. *Foundations and Trends® in Machine Learning*, 5(4):287–364, 2013.
- [25] Y. Lei and Y. Ying. Fine-grained analysis of stability and generalization for stochastic gradient descent. In *International Conference on Machine Learning*, pages 5809–5819, 2020.
- [26] Y. Lei and Y. Ying. Stochastic proximal auc maximization. *Journal of Machine Learning Research*, 22(61):1–45, 2021.
- [27] Y. Lei, A. Ledent, and M. Kloft. Sharper generalization bounds for pairwise learning. In *Advances in Neural Information Processing Systems*, volume 33, pages 21236–21246, 2020.
- [28] M. Liu, X. Zhang, Z. Chen, X. Wang, and T. Yang. Fast stochastic auc maximization with $O(1/n)$ -convergence rate. In *International Conference on Machine Learning*, pages 3195–3203, 2018.
- [29] M. Liu, Z. Yuan, Y. Ying, and T. Yang. Stochastic auc maximization with deep neural networks. In *International Conference on Learning Representations*, 2020.
- [30] F. Orabona. A modern introduction to online learning. *arXiv preprint arXiv:1912.13213*, 2019.
- [31] S. Shalev-Shwartz. Online learning and online convex optimization. *Foundations and Trends® in Machine Learning*, 4(2):107–194, 2012.
- [32] S. Shalev-Shwartz, O. Shamir, N. Srebro, and K. Sridharan. Stochastic convex optimization. In *COLT*, 2009.
- [33] W. Shen, Z. Yang, Y. Ying, and X. Yuan. Stability and optimization error of stochastic gradient descent for pairwise learning. *Analysis and Applications*, 18(05):887–927, 2020.
- [34] T. Sun, Y. Sun, and W. Yin. On markov chain gradient descent. *Advances in neural information processing systems*, 2018.
- [35] Y. Wang, R. Khadon, D. Pechyony, and R. Jones. Generalization bounds for online learning algorithms with pairwise loss functions. In *Conference on Learning Theory*, volume 23, pages 13–1, 2012.
- [36] Y. Wang, R. Khadon, D. Pechyony, and R. Jones. Online learning with pairwise loss functions. *arXiv preprint arXiv:1301.5332*, 2013.
- [37] K. Q. Weinberger and L. K. Saul. Distance metric learning for large margin nearest neighbor classification. *Journal of Machine Learning Research*, 10:207–244, 2009.
- [38] E. P. Xing, M. I. Jordan, S. J. Russell, and A. Y. Ng. Distance metric learning with application to clustering with side-information. In *Advances in Neural Information Processing Systems*, 2003.
- [39] Z. Xue, S. Yang, M. Huai, and D. Wang. Differentially private pairwise learning revisited, 2021. URL https://shao3wangdi.github.io/papers/IJCAI2021_pairwise.pdf.
- [40] Z. Yang, Y. Lei, S. Lyu, and Y. Ying. Stability and differential privacy of stochastic gradient descent for pairwise learning with non-smooth loss. In *International Conference on Artificial Intelligence and Statistics*, pages 2026–2034. PMLR, 2021.
- [41] Y. Ying and P. Li. Distance metric learning with eigenvalue optimization. *Journal of Machine Learning Research*, 13:1–26, 2012.
- [42] Y. Ying and D.-X. Zhou. Online regularized classification algorithms. *IEEE Transactions on Information Theory*, 52(11):4775–4788, 2006.
- [43] Y. Ying, L. Wen, and S. Lyu. Stochastic online AUC maximization. In *Advances in Neural Information Processing Systems*, pages 451–459, 2016.
- [44] T. Zhang. Data dependent concentration bounds for sequential prediction algorithms. In *Conference on Learning Theory*, pages 173–187, 2005.
- [45] P. Zhao, S. C. Hoi, R. Jin, and T. Yang. Online AUC maximization. In *International Conference on Machine Learning*, pages 233–240, 2011.

A Proofs of Generalization Error (Theorems 4 and 5)

In this section, we present the stability and generalization error bounds for SGD with convex loss functions. We first prove Theorem 4 on smooth problems and then Theorem 5 on nonsmooth problems. Recall $\mathbb{E}_{\mathcal{A}}$ denotes the expectation w.r.t. the internal randomness of \mathcal{A} . For SGD, this means the expectation w.r.t. $\{i_j\}_{j \in [t]}$.

Proof of Theorem 4. We first investigate the uniform stability of Algorithm 1. Let $S' = \{z_1, \dots, z_{n-1}, z'_n\}$, where z'_n is independently drawn from ρ , and $\{\mathbf{w}'_t\}$ be produced by Algorithm 1 w.r.t. data S' . We consider two cases: i.e. the case of $\{i_t \neq n \text{ and } i_{t-1} \neq n\}$ and the case of $\{i_t = n \text{ or } i_{t-1} = n\}$.

If $i_t \neq n$ and $i_{t-1} \neq n$, then

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2^2 &\leq \|\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \mathbf{w}'_{t-1} + \eta_t \nabla f(\mathbf{w}'_{t-1}; z'_{i_t}, z'_{i_{t-1}})\|_2^2 \\ &= \|\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \mathbf{w}'_{t-1} + \eta_t \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2^2 \\ &= \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + \eta_t^2 \|\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2^2 \\ &\quad - 2\eta_t \langle \mathbf{w}_{t-1} - \mathbf{w}'_{t-1}, \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}}) \rangle \\ &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + \eta_t^2 \|\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2^2 \\ &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4\eta_t^2 G^2, \end{aligned}$$

where the last second inequality follows from the inequality $\langle \mathbf{w}_{t-1} - \mathbf{w}'_{t-1}, \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}}) \rangle \geq 0$ due to the convexity of f and the last inequality follows from the Lipschitz continuity of f . If $i_t = n$ or $i_{t-1} = n$, it follows from the elementary inequality $(a+b)^2 \leq (1+p)a^2 + (1+1/p)b^2$ and the Lipschitz condition that

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2^2 &\leq (1+p) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 \\ &\quad + (1+1/p)\eta_t^2 \|\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z'_{i_t}, z'_{i_{t-1}})\|_2^2 \\ &\leq (1+p) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4(1+1/p)\eta_t^2 G^2. \end{aligned}$$

We can combine the above two cases together and derive

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2^2 &\leq (\|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4\eta_t^2 G^2) \mathbb{I}_{[i_t \neq n \text{ and } i_{t-1} = n]} \\ &\quad + ((1+p) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4(1+1/p)\eta_t^2 G^2) \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]} \\ &\leq (1+p \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4\eta_t^2 G^2 (1 + \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}/p) \\ &= (1+p)^{\mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}} \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2^2 + 4\eta_t^2 G^2 (1 + \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}/p), \end{aligned}$$

where $\mathbb{I}_{[\cdot]}$ is the indicator function. We can apply the above inequality recursively and get

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2^2 &\leq 4G^2 \sum_{k=1}^t \eta_k^2 (1 + \mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]}/p) \prod_{j=k+1}^t (1+p)^{\mathbb{I}_{[i_j = n \text{ or } i_{j-1} = n]}} \\ &\leq 4G^2 \prod_{j=1}^t (1+p)^{\mathbb{I}_{[i_j = n \text{ or } i_{j-1} = n]}} \sum_{k=1}^t \eta_k^2 (1 + \mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]}/p) \\ &= 4G^2 \eta^2 (1+p)^{\sum_{j=1}^t \mathbb{I}_{[i_j = n \text{ or } i_{j-1} = n]}} (t + \sum_{k=1}^t \mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]}/p), \end{aligned}$$

where the last inequality follows from $\eta_j = \eta$.

Now, we choose $p = 1/(\sum_{j=1}^t \mathbb{I}_{[i_j = n \text{ or } i_{j-1} = n]})$ and use the inequality $(1+x)^{1/x} \leq e$ to derive the following inequality

$$\|\mathbf{w}_t - \mathbf{w}'_t\|_2^2 \leq 4eG^2 \eta^2 \left(t + \left(\sum_{k=1}^t \mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]} \right)^2 \right).$$

By the inequality $\mathbb{I}_{[i_k=n \text{ or } i_{k-1}=n]} \leq \mathbb{I}_{[i_k=n]} + \mathbb{I}_{[i_{k-1}=n]}$ and $(a+b)^2 \leq 2(a^2 + b^2)$ we know

$$\begin{aligned} \mathbb{E}_{\mathcal{A}} \left[\left(\sum_{k=1}^t \mathbb{I}_{[i_k=n \text{ or } i_{k-1}=n]} \right)^2 \right] &\leq 2\mathbb{E}_{\mathcal{A}} \left[\left(\sum_{k=1}^t \mathbb{I}_{[i_k=n]} \right)^2 \right] + 2\mathbb{E}_{\mathcal{A}} \left[\left(\sum_{k=1}^t \mathbb{I}_{[i_{k-1}=n]} \right)^2 \right] \\ &= 4\mathbb{E} \left[\left(\sum_{k=1}^t \mathbb{I}_{[i_k=n]} \right)^2 \right] \leq 4t + 4 \sum_{j,k \in [t]: j \neq k} \mathbb{E} [\mathbb{I}_{[i_j=n]} \mathbb{I}_{[i_k=n]}] \\ &= 4t + 4 \sum_{j,k \in [t]: j \neq k} \frac{1}{n^2} \leq 4t + 4t^2/n^2. \end{aligned}$$

We can combine the above two inequalities together and derive

$$\mathbb{E}_{\mathcal{A}} [\|\mathbf{w}_t - \mathbf{w}'_t\|_2^2] \leq 4eG^2\eta^2 \left(5t + \frac{4t^2}{n^2} \right)$$

and by the convexity of $\|\cdot\|_2^2$ it follows

$$\mathbb{E}_{\mathcal{A}} [\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2^2] \leq \frac{1}{t} \sum_{j=1}^t \mathbb{E}_{\mathcal{A}} [\|\mathbf{w}_j - \mathbf{w}'_j\|_2^2] \leq 4eG^2\eta^2 \left(5t + \frac{4t^2}{n^2} \right).$$

This establishes the uniform stability of Algorithm 1. Furthermore, for any \mathbf{z}, \mathbf{z}' , we have

$$\begin{aligned} \mathbb{E}_{\mathcal{A}} [f(\bar{\mathbf{w}}_t, \mathbf{z}, \mathbf{z}') - f(\bar{\mathbf{w}}'_t, \mathbf{z}, \mathbf{z}')] &\leq G\mathbb{E}_{\mathcal{A}} [\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2] = G\mathbb{E}_{\mathcal{A}} \left[\sqrt{\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2^2} \right] \\ &\leq G\sqrt{\mathbb{E}_{\mathcal{A}} [\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2^2]} \leq 2\sqrt{e}G^2\eta \left(\sqrt{5t} + \frac{2t}{n} \right) \end{aligned}$$

where the first inequality we used the G -Lipschitz continuity of f and the second inequality we used the Jensen's inequality. Therefore, Algorithm 1 is $2\sqrt{e}G^2\eta \left(\sqrt{5t} + \frac{2t}{n} \right)$ -uniformly stable. By Lemma 1 it follows

$$\mathbb{E}_{\mathcal{A}} [F(\bar{\mathbf{w}}_t) - F_S(\bar{\mathbf{w}}_t)] \leq 4\sqrt{e}G^2\eta \left(\sqrt{5t} + \frac{2t}{n} \right),$$

which gives us the desired result. \square

To prove Theorem 5 we require the following lemma on the nonexpansiveness of gradient map $\mathbf{w} \mapsto \mathbf{w} - \eta \nabla f(\mathbf{w}; z, z')$.

Lemma 2 (Hardt et al. 16). *Assume for all $z \in \mathcal{Z}$, the function $\mathbf{w} \mapsto f(\mathbf{w}; z, z')$ is convex and L -smooth. Then for all $\eta \leq 2/L$ and $z, z' \in \mathcal{Z}$ there holds*

$$\|\mathbf{w} - \eta \nabla f(\mathbf{w}; z, z') - \mathbf{w}' + \eta \nabla f(\mathbf{w}'; z, z')\|_2 \leq \|\mathbf{w} - \mathbf{w}'\|_2.$$

Proof of Theorem 5. Let $S' = \{z_1, \dots, z_{n-1}, z'_n\}$, where z'_n is independently drawn from ρ . Let $\{\mathbf{w}'_t\}$ be produced by Algorithm 1 w.r.t. S' . We consider two cases. If $i_t \neq n$ and $i_{t-1} \neq n$, then it follows from Lemma 2 that

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2 &\leq \|\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \mathbf{w}'_{t-1} + \eta_t \nabla f(\mathbf{w}'_{t-1}; z'_{i_t}, z'_{i_{t-1}})\|_2 \\ &= \|\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \mathbf{w}'_{t-1} + \eta_t \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2 \\ &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2. \end{aligned}$$

Otherwise, we know

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2 &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + \eta_t \|\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z'_{i_t}, z'_{i_{t-1}})\|_2 \\ &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2\eta_t G. \end{aligned}$$

We can combine the above two cases together and derive the following inequality

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2 &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 \mathbb{I}_{[i_t \neq n \text{ and } i_{t-1} \neq n]} + (\|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2\eta_t G) \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]} \\ &= \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2\eta_t G \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}. \end{aligned}$$

We can apply the above inequality recursively and get

$$\|\mathbf{w}_t - \mathbf{w}'_t\|_2 \leq 2G \sum_{j=1}^t \eta_j \mathbb{I}_{[i_j=n \text{ or } i_{j-1}=n]} \leq 2G \sum_{j=1}^t \eta_j (\mathbb{I}_{[i_j=n]} + \mathbb{I}_{[i_{j-1}=n]}).$$

Taking expectations over both sides gives $\mathbb{E}_{\mathcal{A}}[\|\mathbf{w}_t - \mathbf{w}'_t\|_2] \leq \frac{4G}{n} \sum_{j=1}^t \eta_j$. It then follows from the convexity of $\|\cdot\|_2$ that

$$\mathbb{E}_{\mathcal{A}}[\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2] \leq \frac{4G}{n} \sum_{j=1}^t \eta_j.$$

This establishes the uniform argument stability of Algorithm 1. Furthermore, it follows the Lipschitz condition that

$$\sup_{z,z'} \mathbb{E}_{\mathcal{A}}[f(\bar{\mathbf{w}}_t; z, z') - f(\bar{\mathbf{w}}'_t; z, z')] \leq \frac{4G^2}{n} \sum_{j=1}^t \eta_j.$$

The desired result then follows from Lemma 1. The proof for Theorem 5 is completed. \square

Finally, we consider the generalization analysis for nonconvex problems under the PL condition. To prove Theorem 3, we first introduce a lemma motivated by the arguments in [16].

Lemma 3. *Let $S = \{z_i\}_{i \in [n]}$ and $S' = \{z'_i\}_{i \in [n]}$ be neighboring datasets differing by a single example. Let $\{\mathbf{w}_t\}_t$ and $\{\mathbf{w}'_t\}_t$ be produced by Algorithm 1 w.r.t. S and S' , respectively. Let Assumption (A1) hold and $\sup_{z,z'} f(\mathbf{w}_i, z, z') \leq B$. Let $\Delta_t = \|\mathbf{w}_t - \mathbf{w}'_t\|_2$. Then for every $z, z' \in \mathcal{Z}$ and every $t_0 \in [n]$, there holds*

$$\mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')|] \leq G\mathbb{E}[\Delta_T | \Delta_{t_0} = 0] + \frac{Bt_0}{n}.$$

Proof. Without loss of generality, we assume that S and S' differ by the last example. Let \mathcal{E} denote the event $\Delta_{t_0} = 0$. Then we have

$$\begin{aligned} \mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')|] &= \mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')| | \mathcal{E}] \Pr\{\mathcal{E}\} \\ &\quad + \mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')| | \mathcal{E}^c] \Pr\{\mathcal{E}^c\}, \end{aligned}$$

where \mathcal{E}^c denotes the complement of \mathcal{E} . Furthermore, we know

$$\Pr\{\mathcal{E}^c\} \leq \sum_{t=1}^{t_0} \Pr\{i_t = n\} = \frac{t_0}{n}.$$

We can combine the above two inequalities and the Lipschitz continuity of f to derive the stated bound, which completes the proof. \square

B Proofs of Optimization Error (Theorems 6-9)

In this section, we prove optimization error bounds for SGD. We first consider convex cases, and prove convergence rates in expectation (Theorem 6) and with high probability (Theorem 7). Then, we establish convergence rates for SGD with nonconvex loss functions (Theorem 8 and Theorem 9).

Proof of Theorem 6. Consider $j \geq 1$. Note that $f(\cdot; z, z')$ is α -strongly convex and G -Lipschitz continuous, we have

$$\begin{aligned}
\|\mathbf{w}_j - \mathbf{w}\|_2^2 &\leq \|\mathbf{w}_{j-1} - \eta_j \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}) - \mathbf{w}\|_2^2 \\
&= \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - 2\eta_j \langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}), \mathbf{w}_{j-1} - \mathbf{w} \rangle + \eta_j^2 \|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})\|_2^2 \\
&\leq (1 - \eta_j \alpha) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - 2\eta_j [f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] + G^2 \eta_j^2 \\
&= (1 - \eta_j \alpha) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - 2\eta_j [f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\quad + 2\eta_j [f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})] + G^2 \eta_j^2 \\
&\leq (1 - \eta_j \alpha) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - 2\eta_j [f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\quad + 2\eta_j G \|\mathbf{w}_{j-1} - \mathbf{w}_{j-2}\|_2 + G^2 \eta_j^2 \\
&\leq (1 - \eta_j \alpha) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - 2\eta_j [f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\quad + 2G^2 \eta_j \eta_{j-1} + G^2 \eta_j^2,
\end{aligned} \tag{B.1}$$

where the last inequality used the fact that $\|\mathbf{w}_j - \mathbf{w}_{j-1}\|_2 = \eta_j \|\nabla f(\mathbf{w}_j; z_{i_j}, z_{i_{j-1}})\|_2 \leq G\eta_j$.

For the convex case, i.e. $\alpha = 0$, we know from (B.1) that

$$\begin{aligned}
&\sum_{j=1}^t \eta_j [f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\leq \frac{1}{2} \sum_{j=1}^t [\|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - \|\mathbf{w}_j - \mathbf{w}\|_2^2] + \frac{G^2}{2} \sum_{j=1}^t (2\eta_{j-1} \eta_j + \eta_j^2) \\
&\leq \frac{1}{2} \|\mathbf{w}_0 - \mathbf{w}\|_2^2 + \frac{G^2}{2} \sum_{j=1}^t (2\eta_{j-1} \eta_j + \eta_j^2).
\end{aligned} \tag{B.2}$$

Taking the expectation on both sides of the above inequality and observing that $f(\cdot; z, z')$ is convex, we get the desired estimation (5).

For the strongly-convex case, i.e. $\alpha > 0$, we obtain from (B.1) that

$$f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}}) \leq \frac{\eta_j^{-1} - \alpha}{2} \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - \frac{\eta_j^{-1}}{2} \|\mathbf{w}_j - \mathbf{w}\|_2^2 + G^2 \eta_{j-1} + \frac{G^2 \eta_j}{2}.$$

Now, we choose $\eta_j = \frac{2}{\alpha(j+1)}$ for any j , which implies that

$$\begin{aligned}
&j[f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\leq \frac{j(j-1)\alpha}{4} \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - \frac{j(j+1)\alpha}{4} \|\mathbf{w}_j - \mathbf{w}\|_2^2 + \frac{2G^2}{\alpha} + \frac{G^2 j}{\alpha(j+1)} \\
&\leq \frac{\alpha}{4} [j(j-1) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - j(j+1) \|\mathbf{w}_j - \mathbf{w}\|_2^2] + \frac{3G^2}{\alpha}.
\end{aligned}$$

Taking the summation over j implies that

$$\begin{aligned}
&\sum_{j=1}^t j[f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) - f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})] \\
&\leq \frac{3G^2 t}{\alpha} + \frac{\alpha}{4} \sum_{j=1}^t [j(j-1) \|\mathbf{w}_{j-1} - \mathbf{w}\|_2^2 - j(j+1) \|\mathbf{w}_j - \mathbf{w}\|_2^2] \\
&\leq \frac{3G^2 t}{\alpha} + \frac{\alpha}{4} [0 - t(t+1) \|\mathbf{w}_t - \mathbf{w}\|_2^2] \leq \frac{3G^2 t}{\alpha}.
\end{aligned} \tag{B.3}$$

Dividing both sides of the above inequality by $\sum_{j=1}^t j$ yields the desired estimation in part (b). \square

To prove high-probability bounds, we require the following lemma on concentration inequalities of martingales [6, 44].

Lemma 4. Let $\tilde{z}_1, \dots, \tilde{z}_n$ be a sequence of random variables such that \tilde{z}_k may depend on the previous variables $\tilde{z}_1, \dots, \tilde{z}_{k-1}$ for all $k = 1, \dots, n$. Consider a sequence of functionals $\xi_k(\tilde{z}_1, \dots, \tilde{z}_k), k = 1, \dots, n$. Let $\alpha_n^2 = \sum_{k=1}^n \mathbb{E}_{\tilde{z}_k} [(\xi_k - \mathbb{E}_{\tilde{z}_k}[\xi_k])^2]$ be the conditional variance.

(1) Assume $|\xi_k - \mathbb{E}_{\tilde{z}_k}[\xi_k]| \leq b_k$ for each k . Let $\delta \in (0, 1)$. With probability at least $1 - \delta$

$$\sum_{k=1}^n \mathbb{E}_{\tilde{z}_k}[\xi_k] - \sum_{k=1}^n \xi_k \leq \left(2 \sum_{k=1}^n b_k^2 \log \frac{1}{\delta} \right)^{\frac{1}{2}}. \quad (\text{B.4})$$

(2) Assume that $\xi_k - \mathbb{E}_{\tilde{z}_k}[\xi_k] \leq b$ for each k . Let $\rho \in (0, 1]$ and $\delta \in (0, 1)$. With probability at least $1 - \delta$ we have

$$\sum_{k=1}^n \mathbb{E}_{\tilde{z}_k}[\xi_k] - \sum_{k=1}^n \xi_k \leq \frac{\rho \alpha_n^2}{b} + \frac{b \log \frac{1}{\delta}}{\rho}. \quad (\text{B.5})$$

Proof of Theorem 7. For simplicity, we assume t is an even number. We first consider the convex case. Let

$$\xi_j = \eta_{2j}(f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}}) - f(\mathbf{w}; z_{i_{2j}}, z_{i_{2j-1}})), \quad j \in [t/2].$$

It is obvious that $|\xi_j - \mathbb{E}_{i_{2j}, i_{2j-1}}[\xi_j]| \leq 2B\eta_{2j}$. Let $\tilde{z}_j = (i_{2j}, i_{2j-1})$. It is clear that $\tilde{z}_j, j \in [t/2]$ are i.i.d. random variables. Therefore, one can apply Part (a) of Lemma 4 to derive the following inequality with probability at least $1 - \delta/2$

$$\sum_{j=1}^{t/2} \mathbb{E}_{\tilde{z}_j}[\xi_j] - \sum_{j=1}^{t/2} \xi_j \leq 2B \left(2 \sum_{j=1}^{t/2} \eta_{2j}^2 \log(2/\delta) \right)^{\frac{1}{2}}.$$

It is clear that $\mathbb{E}_{\tilde{z}_j}[\xi_j] = \eta_{2j}(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}))$. Therefore, the following inequality holds with probability at least $1 - \delta/2$

$$\sum_{j=1}^{t/2} \eta_{2j}(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}) - f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}}) + f(\mathbf{w}; z_{i_{2j}}, z_{i_{2j-1}})) \leq 2B \left(2 \sum_{j=1}^{t/2} \eta_{2j}^2 \log(2/\delta) \right)^{\frac{1}{2}}.$$

In a similar way, one can derive the following inequality with probability at least $1 - \delta/2$

$$\begin{aligned} & \sum_{j=1}^{t/2} \eta_{2j-1}(F_S(\mathbf{w}_{2j-3}) - F_S(\mathbf{w}) - f(\mathbf{w}_{2j-3}; z_{i_{2j-1}}, z_{i_{2j-2}}) \\ & \quad + f(\mathbf{w}; z_{i_{2j-1}}, z_{i_{2j-2}})) \leq 2B \left(2 \sum_{j=1}^{t/2} \eta_{2j-1}^2 \log(2/\delta) \right)^{\frac{1}{2}}. \end{aligned}$$

We can combine the above two inequalities together and derive the following inequality with probability $1 - \delta$

$$\sum_{j=1}^t \eta_j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}) - f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) + f(\mathbf{w}; z_{i_j}, z_{i_{j-1}})) \leq 2B \left(2 \sum_{j=1}^t \eta_j^2 \log(2/\delta) \right)^{\frac{1}{2}}.$$

We can combine the above inequality and Eq. (B.2) to derive the following inequality with probability at least $1 - \delta$

$$\sum_{j=1}^t \eta_j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w})) \leq 2B \left(2 \sum_{j=1}^t \eta_j^2 \log(2/\delta) \right)^{\frac{1}{2}} + \frac{1}{2} \|\mathbf{w}_0 - \mathbf{w}\|_2^2 + G^2 \sum_{j=1}^t (\eta_{j-1} \eta_j + \frac{\eta_j^2}{2}).$$

The stated bound then follows from the convexity of F_S .

We now turn to the strongly convex case. Let

$$\xi_j = 2j(f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}}) - f(\mathbf{w}_S; z_{i_{2j}}, z_{i_{2j-1}})), \quad j \in [t/2].$$

It is clear that $|\xi_j - \mathbb{E}_{i_{2j}, i_{2j-1}}[\xi_j]| \leq 4jB \leq 2tB$ for $j \in [t/2]$. Furthermore, the conditional variance satisfies

$$\begin{aligned}\mathbb{E}_{\tilde{z}_j}[(\xi_j - \mathbb{E}_{\tilde{z}_j}[\xi_j])^2] &\leq \mathbb{E}_{\tilde{z}_j}[\xi_j^2] \leq 4j^2G^2\|\mathbf{w}_{2j-2} - \mathbf{w}_S\|_2^2 \\ &\leq 8\alpha^{-1}j^2G^2(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}_S)),\end{aligned}$$

where the first inequality follows from f is G -Lipschitz continuous, and the second inequality used the fact $\nabla F_S(\mathbf{w}_S) = 0$ and f is α -strongly convex.

Note \tilde{z}_j are independent random variables and

$$\mathbb{E}_{\tilde{z}_j}[\xi_j] = 2j(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}_S)).$$

Therefore, we can apply Part (b) of Lemma 4 to derive the following inequality with probability at least $1 - \delta/2$

$$\begin{aligned}2\sum_{j=1}^{t/2} j \left(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}_S) - f(\mathbf{w}_{2j-2}; z_{i_{2j}}, z_{i_{2j-1}}) + f(\mathbf{w}_S; z_{i_{2j}}, z_{i_{2j-1}}) \right) \\ \leq \frac{8G^2\rho \sum_{j=1}^{t/2} j^2(F_S(\mathbf{w}_{2j-2}) - F_S(\mathbf{w}_S))}{2tB\alpha} + \frac{2tB \log(2/\delta)}{\rho}.\end{aligned}$$

In a similar way, one can derive the following inequality with probability at least $1 - \delta/2$

$$\begin{aligned}\sum_{j=1}^{t/2} (2j-1) \left(F_S(\mathbf{w}_{2j-3}) - F_S(\mathbf{w}_S) - f(\mathbf{w}_{2j-3}; z_{i_{2j-1}}, z_{i_{2j-2}}) + f(\mathbf{w}_S; z_{i_{2j-1}}, z_{i_{2j-2}}) \right) \\ \leq \frac{2G^2\rho \sum_{j=1}^{t/2} (2j-1)^2(F_S(\mathbf{w}_{2j-3}) - F_S(\mathbf{w}_S))}{2tB\alpha} + \frac{2tB \log(2/\delta)}{\rho}.\end{aligned}$$

We can combine the above two inequalities together and derive the following inequality with probability at least $1 - \delta$

$$\begin{aligned}\sum_{j=1}^t j \left(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S) - f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}) + f(\mathbf{w}_S; z_{i_j}, z_{i_{j-1}}) \right) \\ \leq \frac{2G^2\rho \sum_{j=1}^t j^2(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S))}{2tB\alpha} + \frac{2tB \log(2/\delta)}{\rho}.\end{aligned}$$

We can combine the above inequality and Eq. (B.3) together and derive the following inequality with probability $1 - \delta$

$$\sum_{j=1}^t j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S)) \leq \frac{3G^2t}{\alpha} + \frac{G^2\rho \sum_{j=1}^t j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S))}{B\alpha} + \frac{2tB \log(2/\delta)}{\rho}.$$

Now, we take $\rho = \min\{1, B\alpha/(2G^2)\}$ and get the following inequality with probability at least $1 - \delta$

$$\sum_{j=1}^t j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S)) \leq \frac{3G^2t}{\alpha} + \frac{1}{2} \sum_{j=1}^t j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S)) + 2t \log(2/\delta) \max\{B, 2G^2/\alpha\}$$

and therefore

$$\sum_{j=1}^t j(F_S(\mathbf{w}_{j-2}) - F_S(\mathbf{w}_S)) \leq \frac{14G^2t \log(2/\delta)}{\alpha} + 4Bt \log(2/\delta).$$

The stated bound then follows from the convexity of F_S . The proof is completed. \square

We now turn to nonconvex problems.

Proof of Theorem 8. It is clear that F_S is L -smooth and therefore

$$\begin{aligned} F_S(\mathbf{w}_j) &\leq F_S(\mathbf{w}_{j-1}) + \langle \mathbf{w}_j - \mathbf{w}_{j-1}, \nabla F_S(\mathbf{w}_{j-1}) \rangle + \frac{L}{2} \|\mathbf{w}_j - \mathbf{w}_{j-1}\|_2^2 \\ &= F_S(\mathbf{w}_{j-1}) - \eta_j \langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle + \frac{L\eta_j^2}{2} \|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})\|_2^2 \end{aligned}$$

Taking expectations over both sides gives

$$\begin{aligned} \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_j)] &\leq \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_{j-1})] - \eta_j \mathbb{E}_{\mathcal{A}}[\langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle] + \\ &\quad \frac{L\eta_j^2}{2} \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})\|_2^2]. \quad (\text{B.6}) \end{aligned}$$

According to the elementary inequality $(a+b)^2 \leq 2(a^2 + b^2)$ we know

$$\begin{aligned} &\mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})\|_2^2] \\ &\leq 2\mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}) - \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2^2] + 2\mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2^2] \\ &\leq 2L\mathbb{E}_{\mathcal{A}}[\|\mathbf{w}_{j-1} - \mathbf{w}_{j-2}\|_2^2] + 2\alpha_0^2 = 2L\eta_{j-1}^2 \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_{j-1}}, z_{i_{j-2}})\|_2^2] + 2\alpha_0^2 \\ &\leq \frac{1}{2} \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_{j-1}}, z_{i_{j-2}})\|_2^2] + 2\alpha_0^2, \end{aligned}$$

where we have used the L -smoothness, the assumption $\mathbb{E}_{i_j, i_{j-1}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2^2] \leq \alpha_0^2$ and $4L\eta_{j-1}^2 \leq 1$. It is clear that $\mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_0; z_{i_1}, z_{i_0})\|_2^2] \leq \alpha_0^2$. It is easy to use an induction and the above inequality to show that

$$\mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}})\|_2^2] \leq 4\alpha_0^2, \quad \forall j. \quad (\text{B.7})$$

Furthermore, the smoothness assumption implies that

$$\begin{aligned} &\langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle \\ &= \langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle + \langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}) - \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle \\ &= \langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-2}) \rangle + \langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) - \nabla F_S(\mathbf{w}_{j-2}) \rangle + \\ &\quad + \langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}) - \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle \\ &\geq \langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-2}) \rangle - L\|\mathbf{w}_{j-1} - \mathbf{w}_{j-2}\|_2(\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2 + \|\nabla F_S(\mathbf{w}_{j-1})\|_2). \end{aligned}$$

According to Schwartz inequality, the variance assumption and Eq. (B.7), we know

$$\begin{aligned} &\mathbb{E}_{\mathcal{A}}[\|\mathbf{w}_{j-1} - \mathbf{w}_{j-2}\|_2(\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2 + \|\nabla F_S(\mathbf{w}_{j-1})\|_2)] \\ &\leq \frac{1}{2\eta_{j-1}} \mathbb{E}_{\mathcal{A}}[\|\mathbf{w}_{j-1} - \mathbf{w}_{j-2}\|_2^2] + \eta_{j-1} \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2^2 + \|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \\ &= \frac{\eta_{j-1}}{2} \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_{j-1}}, z_{i_{j-2}})\|_2^2] + \eta_{j-1} \mathbb{E}_{\mathcal{A}}[\|\nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}})\|_2^2 + \|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \\ &\leq 2\alpha_0^2 \eta_{j-1} + 2\alpha_0^2 \eta_{j-1}. \end{aligned}$$

We can combine the above two inequalities together and get

$$\mathbb{E}_{\mathcal{A}}[\langle \nabla f(\mathbf{w}_{j-1}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-1}) \rangle] \geq \mathbb{E}_{\mathcal{A}}[\langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-2}) \rangle] - 4L\alpha_0^2 \eta_{j-1}.$$

We can combine (B.6), (B.7) and the above inequality, and get

$$\begin{aligned} \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_j)] &\leq \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_{j-1})] - \eta_j \mathbb{E}_{\mathcal{A}}[\langle \nabla f(\mathbf{w}_{j-2}; z_{i_j}, z_{i_{j-1}}), \nabla F_S(\mathbf{w}_{j-2}) \rangle] + 4L\alpha_0^2 \eta_j \eta_{j-1} + 2L\eta_j^2 \alpha_0^2 \\ &\leq \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_{j-1})] - \eta_j \mathbb{E}_{\mathcal{A}}[\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] + 4L\alpha_0^2(\eta_j \eta_{j-1} + \eta_j^2), \end{aligned}$$

where the last inequality holds since \mathbf{w}_{j-2} is independent of i_j and i_{j-1} . The above inequality can be reformulated as

$$\eta_j \mathbb{E}_{\mathcal{A}}[\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] \leq \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_{j-1})] - \mathbb{E}_{\mathcal{A}}[F_S(\mathbf{w}_j)] + 4L\alpha_0^2(\eta_j \eta_{j-1} + \eta_j^2). \quad (\text{B.8})$$

We can take a summation of the above inequality and get

$$\sum_{j=1}^t \eta_j \mathbb{E}_{\mathcal{A}}[\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] \leq F_S(\mathbf{w}_0) + 4L\alpha_0^2 \sum_{j=1}^t (\eta_j \eta_{j-1} + \eta_j^2).$$

Since $\eta_j = \eta$, we further get

$$\sum_{j=1}^t \mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] \leq \eta^{-1} F_S(\mathbf{w}_0) + 8L\alpha_0^2 t\eta.$$

The proof is completed. \square

Proof of Theorem 9. According to the elementary inequality $\frac{1}{2}(a+b)^2 \leq a^2 + b^2$ we know

$$\begin{aligned} \mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-2})\|_2^2] &\geq -\mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-2}) - \nabla F_S(\mathbf{w}_{j-1})\|_2^2] + 2^{-1}\mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \\ &\geq -L\mathbb{E}_{\mathcal{A}} [\|\mathbf{w}_{j-2} - \mathbf{w}_{j-1}\|_2^2] + 2^{-1}\mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \\ &= -L\eta_{j-1}^2 \mathbb{E}_{\mathcal{A}} [\|\nabla f(\mathbf{w}_{j-2}; z_{i_{j-1}}, z_{i_{j-2}})\|_2^2] + 2^{-1}\mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \\ &\geq -4L\eta_{j-1}^2 \alpha_0^2 + 2^{-1}\mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-1})\|_2^2], \end{aligned}$$

where we have used (B.7). This together with (B.8) gives

$$2^{-1}\eta_j \mathbb{E}_{\mathcal{A}} [\|\nabla F_S(\mathbf{w}_{j-1})\|_2^2] \leq 4L\eta_j \eta_{j-1}^2 \alpha_0^2 + \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1})] - \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_j)] + 4L\alpha_0^2 (\eta_j \eta_{j-1} + \eta_j^2).$$

It then follows from the PL condition that

$$\mu\eta_j \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1}) - F_S(\mathbf{w}_S)] \leq \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1})] - \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_j)] + 4L\alpha_0^2 (\eta_j \eta_{j-1} + \eta_j^2 + \eta_j \eta_{j-1}^2).$$

We can reformulate the above inequality as

$$\mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_j) - F_S(\mathbf{w}_S)] \leq (1 - \mu\eta_j) \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1}) - F_S(\mathbf{w}_S)] + 4L\alpha_0^2 (\eta_j \eta_{j-1} + \eta_j^2 + \eta_j \eta_{j-1}^2).$$

Now, taking $\eta_j = 2/(\mu(j+1))$, we get

$$\mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_j) - F_S(\mathbf{w}_S)] \leq \frac{j-1}{j+1} \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1}) - F_S(\mathbf{w}_S)] + \frac{4L\alpha_0^2}{\mu^2} \left(\frac{8}{j(j+1)} + \frac{8}{j^2(j+1)\mu} \right).$$

We can multiple both sides by $j(j+1)$ and get

$$j(j+1) \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_j) - F_S(\mathbf{w}_S)] \leq (j-1)j \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_{j-1}) - F_S(\mathbf{w}_S)] + \frac{4L\alpha_0^2}{\mu^2} (8 + 8j^{-1}\mu^{-1}).$$

Taking a summation of the above inequality gives

$$t(t+1) \mathbb{E}_{\mathcal{A}} [F_S(\mathbf{w}_t) - F_S(\mathbf{w}_S)] \leq \frac{32L\alpha_0^2}{\mu^2} \sum_{j=1}^t (1 + j^{-1}\mu^{-1}).$$

The stated bound then follows. The proof is completed. \square

C Proofs of Excess Generalization Error (Theorems 1-3)

In this section, we prove Theorem 1, Theorem 2 and Theorem 3 on excess generalization error bounds.

Proof of Theorem 1. According to Theorem 4, we know

$$\mathbb{E}_{S,\mathcal{A}} [F(\bar{\mathbf{w}}_T) - F_S(\bar{\mathbf{w}}_T)] = \mathcal{O} \left(\sqrt{T}\eta + \frac{T\eta}{n} \right).$$

Furthermore, according to Part (a) of Theorem 6 with $\mathbf{w} = \mathbf{w}^*$, we know

$$\mathbb{E}_{S,\mathcal{A}} [F_S(\bar{\mathbf{w}}_T) - F_S(\mathbf{w}^*)] = \mathcal{O} \left(\frac{1 + T\eta^2}{T\eta} \right). \quad (\text{C.1})$$

We can plug the above generalization error bound and optimization error bound back into the error decomposition (2), and get (3). Taking $T \asymp n^2$ and $\eta \asymp T^{-\frac{3}{4}}$ in Eq. (3), we immediately get $\mathbb{E}_{S,\mathcal{A}} [F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}(1/\sqrt{n})$. The desired result is proved. \square

Proof of Theorem 2. According to Theorem 5, we know

$$\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T) - F_S(\bar{\mathbf{w}}_T)] = \mathcal{O}\left(\frac{T\eta}{n}\right).$$

We can plug the above generalization error bound and the optimization error bound (C.1) back into the error decomposition (2), and get (4). Taking $T \asymp n^2$ and $\eta \asymp T^{-\frac{3}{4}}$ in Eq. (4), we immediately get $\mathbb{E}_{S,\mathcal{A}}[F(\bar{\mathbf{w}}_T)] - F(\mathbf{w}^*) = \mathcal{O}(1/\sqrt{n})$. The proof is completed. \square

Proof of Theorem 3. Let $S' = \{z_1, \dots, z_{n-1}, z'_n\}$, where z'_n is independently drawn from ρ . Let $\{\mathbf{w}'_t\}$ be produced by Algorithm 1 w.r.t. S' . If $i_t \neq n$ and $i_{t-1} \neq n$, then

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2 &\leq \|\mathbf{w}_{t-1} - \eta_t \nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \mathbf{w}'_{t-1} - \eta_t \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2 \\ &\leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + \eta_t \|\nabla f(\mathbf{w}_{t-1}; z_{i_t}, z_{i_{t-1}}) - \nabla f(\mathbf{w}'_{t-1}; z_{i_t}, z_{i_{t-1}})\|_2 \\ &\leq (1 + L\eta_t) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2, \end{aligned}$$

where in the last inequality we used the smoothness of f .

Otherwise, it follows from the Lipschitz condition that $\|\mathbf{w}_t - \mathbf{w}'_t\|_2 \leq \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2G\eta_t$. Consequently, it follows that

$$\begin{aligned} \|\mathbf{w}_t - \mathbf{w}'_t\|_2 &\leq (1 + L\eta_t) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 \mathbb{I}_{[i_t \neq n \text{ and } i_{t-1} \neq n]} \\ &\quad + (\|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2G\eta_t) \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]} \\ &\leq (1 + L\eta_t) \|\mathbf{w}_{t-1} - \mathbf{w}'_{t-1}\|_2 + 2G\eta_t \mathbb{I}_{[i_t = n \text{ or } i_{t-1} = n]}. \end{aligned}$$

We can apply the above inequality recursively and get

$$\Delta_t \leq 2G \sum_{k=t_0+1}^t \eta_k \mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]} \prod_{k'=k+1}^t (1 + L\eta_{k'}) + \Delta_{t_0} \prod_{k=t_0+1}^t (1 + L\eta_k).$$

Since $\Delta_{t_0} = 0$ implies $i_{t_0} \neq n$, we have

$$\begin{aligned} \mathbb{E}[\Delta_t | \Delta_{t_0} = 0] &\leq 2G \sum_{k=t_0+1}^t \eta_k \mathbb{E}[\mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]} | \Delta_{t_0} = 0] \prod_{k'=k+1}^t (1 + L\eta_{k'}) \\ &= 2G \sum_{k=t_0+2}^t \eta_k \mathbb{E}[\mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]} | \Delta_{t_0} = 0] \prod_{k'=k+1}^t (1 + L\eta_{k'}) \\ &= 2G \sum_{k=t_0+2}^t \eta_k \mathbb{E}[\mathbb{I}_{[i_k = n \text{ or } i_{k-1} = n]}] \prod_{k'=k+1}^t (1 + L\eta_{k'}), \end{aligned}$$

where we have used the independency between Δ_{t_0} and i_t for $t > t_0$. It then follows that

$$\begin{aligned} \mathbb{E}[\Delta_t | \Delta_{t_0} = 0] &\leq 2G \sum_{k=t_0+2}^t \eta_k \mathbb{E}[\mathbb{I}_{[i_k = n]} + \mathbb{I}_{[i_{k-1} = n]}] \prod_{k'=k+1}^t (1 + L\eta_{k'}) \\ &\leq \frac{4G}{n} \sum_{k=t_0+2}^t \eta_k \prod_{k'=k+1}^t \exp(L\eta_{k'}) \leq \frac{8G}{\mu n} \sum_{k=t_0+2}^t \frac{1}{k+1} \exp\left(2L\mu^{-1} \sum_{k'=k+1}^t \frac{1}{k'+1}\right) \\ &\leq \frac{8G}{\mu n} \sum_{k=t_0+2}^t \frac{1}{k+1} \exp\left(2L\mu^{-1} \log(t/k)\right) = \frac{8G}{\mu n} \sum_{k=t_0+2}^t \frac{1}{k+1} \left(\frac{t}{k}\right)^{2L\mu^{-1}} \\ &\leq \frac{8Gt^{2L\mu^{-1}}}{\mu n} \sum_{k=t_0+2}^t k^{-1-2L\mu^{-1}} \leq \frac{8G}{\mu n(2L\mu^{-1})} \left(\frac{t}{t_0}\right)^{2L\mu^{-1}}. \end{aligned}$$

Here we use $1 + x \leq \exp(x)$ and $\eta_j = \frac{2}{\mu(j+1)}$. We can plug the above inequality back into Lemma 3 and derive

$$\mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')|] \leq \frac{4G^2}{nL} \left(\frac{T}{t_0}\right)^{2L\mu^{-1}} + \frac{Bt_0}{n}.$$

We can choose $t_0 \asymp T^{\frac{2L}{2L+\mu}}$ and get the following generalization error bounds

$$\mathbb{E}[|f(\mathbf{w}_T; z, z') - f(\mathbf{w}'_T; z, z')|] = \mathcal{O}\left(\frac{T^{\frac{2L}{2L+\mu}}}{n}\right).$$

Lemma 1 then implies $\mathbb{E}[F(\mathbf{w}_T) - F_S(\mathbf{w}_T)] = \mathcal{O}\left(\frac{T^{\frac{2L}{2L+\mu}}}{n}\right)$. Furthermore, according to Theorem 9 we have the following optimization error bounds

$$\mathbb{E}_{\mathbf{w}}[F_S(\mathbf{w}_T)] - \inf_{\mathbf{w}}[F_S(\mathbf{w})] = \mathcal{O}(1/(T\mu^2)).$$

The desired result follows by combining the above two inequalities together and using the fact $\mathbb{E}[\inf_{\mathbf{w}}[F_S(\mathbf{w})]] \leq \mathbb{E}[F_S(\mathbf{w}^*)] = F(\mathbf{w}^*)$. \square

D Proof of Privacy and Utility Guarantees of Algorithm 3 (Theorem 10)

In this section, we present the proof of Theorem 10 on the privacy guarantee and excess generalization bound of Algorithm 3.

To this end, we need the definition of ℓ_2 -sensitivity in terms of high probability and some lemmas. The ℓ_2 -sensitivity definition given below corresponds to the high probability version of uniform argument stability stated in Definition 1.

Definition 3. For any $\gamma \in (0, 1)$, a (randomized) algorithm \mathcal{A} has ℓ_2 -sensitivity of Δ with probability at least $1 - \gamma$ if for any neighboring datasets $S, S' \in \mathcal{Z}^n$, one has $\|\mathcal{A}(S) - \mathcal{A}(S')\|_2 \leq \Delta$.

The next lemma demonstrates that Gaussian mechanism ensures the privacy of an algorithm with high probability ℓ_2 -sensitivity.

Lemma 5. Let $\mathcal{A} : \mathcal{Z}^n \rightarrow \mathbb{R}^d$ be a randomized algorithm with ℓ_2 -sensitivity of Δ with probability at least $1 - \delta/2$. Then the Gaussian mechanism $\mathcal{M}(S) = \mathcal{A}(S) + \mathbf{u}$ where $\mathbf{u} \sim \mathcal{N}(0, (2\Delta^2 \log(2.5/\delta)/\epsilon^2)I_d)$ satisfies (ϵ, δ) -DP.

Proof. Let S and S' be two neighboring datasets. Denote E as the set when \mathcal{A} satisfies ℓ_2 -sensitivity of Δ , i.e. $E = \{\|\mathcal{A}(S) - \mathcal{A}(S')\|_2 \leq \Delta\}$. Then we know $\mathbb{P}[E] \geq 1 - \delta/2$. In favor of E , by classical results for Gaussian mechanism, we know \mathcal{M} satisfies $(\epsilon, \delta/2)$ -DP with $\sigma = \Delta\sqrt{2\log(2.5/\delta)}/\epsilon$. Therefore, for any $\epsilon > 0$ and any event O in the output space of \mathcal{M} , we have

$$\begin{aligned} \mathbb{P}[\mathcal{M}(S) \in O] &= \mathbb{P}[\mathcal{M}(S) \in O | E]\mathbb{P}[E] + \mathbb{P}[\mathcal{M}(S) \in O | E^c]\mathbb{P}[E^c] \\ &\leq \left(e^\epsilon \mathbb{P}[\mathcal{M}(S') \in O | E] + \frac{\delta}{2}\right)\mathbb{P}[E] + \frac{\delta}{2} \\ &\leq e^\epsilon \mathbb{P}[\mathcal{M}(S') \in O \cap E] + \frac{\delta}{2} + \frac{\delta}{2} \\ &\leq e^\epsilon \mathbb{P}[\mathcal{M}(S') \in O] + \delta \end{aligned}$$

where the first inequality is because \mathcal{M} satisfies $(\epsilon, \delta/2)$ -DP when E occurs and $\mathbb{P}[E^c] \leq \delta/2$, the second and third inequalities are by basic properties of probability. The proof is completed. \square

We need the following Chernoff's bound for a summation of independent Bernoulli random variables [40].

Lemma 6 (Chernoff bound for Bernoulli vector). *Let X_1, \dots, X_t be independent random variables taking values in $\{0, 1\}$. Let $X = \sum_{j=1}^t X_j$ and $\mu = \mathbb{E}[X]$. Then for any $\tilde{\gamma} > 0$, with probability at least $1 - \exp(-\mu\tilde{\gamma}^2/(2 + \tilde{\gamma}))$ we have $X \leq (1 + \tilde{\gamma})\mu$.*

In order to prove the privacy guarantee and excess generalization bound for Algorithm 3, we also need the following high probability ℓ_2 -sensitivity of the output of Algorithm 1.

Lemma 7. *Let $\{\bar{\mathbf{w}}_t\}$ and $\{\bar{\mathbf{w}}'_t\}$ be produced by Algorithm 1 based on the neighboring datasets S and S' , respectively. If f is convex and L -smooth and $\eta_t = \eta \leq 2/L$, then with probability at least $1 - \gamma$ we have*

$$\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2 \leq 4G\eta\left(\frac{t}{n} + \log(2/\gamma) + \sqrt{\frac{t\log(2/\gamma)}{n}}\right).$$

Proof. Without loss of generality, we assume the different example between S and S' is the n -th item. By the proof of Theorem 5, we know

$$\|\mathbf{w}_t - \mathbf{w}'_t\|_2 \leq 2G \sum_{j=1}^t \eta_j \mathbb{I}_{[i_j=n \text{ or } i_{j-1}=n]} \leq 2G \sum_{j=1}^t \eta_j (\mathbb{I}_{[i_j=n]} + \mathbb{I}_{[i_{j-1}=n]}).$$

Applying Lemma 6, with probability at least $1 - \gamma$ there holds

$$\sum_{j=1}^t (\mathbb{I}_{[i_j=n]} + \mathbb{I}_{[i_{j-1}=n]}) \leq \frac{2t}{n} + 2 \log(2/\gamma) + 2\sqrt{\frac{t \log(2/\gamma)}{n}}.$$

It then follows from the convexity of $\|\cdot\|_2$ that

$$\|\bar{\mathbf{w}}_t - \bar{\mathbf{w}}'_t\|_2 \leq 4G\eta \left(\frac{t}{n} + \log(2/\gamma) + \sqrt{\frac{t \log(2/\gamma)}{n}} \right),$$

which implies the desired result. \square

With the above preparations, we are now ready to prove Theorem 10.

Proof of Theorem 10. We first consider the privacy guarantee of Algorithm 3. Since we run Algorithm 1 for $\lceil n_k \log(4/\delta) \rceil$ steps for each k , by Lemma 7, we know with probability $1 - \delta/2$

$$\|\bar{\mathbf{w}}_k - \bar{\mathbf{w}}'_k\|_2 \leq 12G\eta_k \log(4/\delta).$$

Therefore, by Lemma 5, each iteration k of Algorithm 3 is (ϵ, δ) -DP. Since the partition of the dataset S is disjoint, and each iteration k of Algorithm 3 we only use one subset, thus the whole process satisfies (ϵ, δ) -DP.

Next we investigate the utility bound of Algorithm 3. Let $\bar{\mathbf{w}}_0 = \mathbf{w}^*$ and $\mathbf{u}_0 = \mathbf{w}_0 - \mathbf{w}^*$, then

$$\mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] = \sum_{k=1}^K \mathbb{E}[F(\bar{\mathbf{w}}_k) - F(\bar{\mathbf{w}}_{k-1})] + \mathbb{E}[F(\mathbf{w}_K) - F(\bar{\mathbf{w}}_K)] \quad (\text{D.1})$$

Denote F_{S_k} be the empirical objective based on sample S_k . For the first term on the RHS of (D.1), we have

$$\begin{aligned} & \mathbb{E}[F(\bar{\mathbf{w}}_k) - F(\bar{\mathbf{w}}_{k-1})] \\ &= \mathbb{E}[F(\bar{\mathbf{w}}_k) - F_{S_k}(\bar{\mathbf{w}}_k)] + \mathbb{E}[F_{S_k}(\bar{\mathbf{w}}_k) - F_{S_k}(\bar{\mathbf{w}}_{k-1})] + \mathbb{E}[F_{S_k}(\bar{\mathbf{w}}_{k-1}) - F(\bar{\mathbf{w}}_{k-1})] \\ &= \mathbb{E}[F(\bar{\mathbf{w}}_k) - F_{S_k}(\bar{\mathbf{w}}_k)] + \mathbb{E}[F_{S_k}(\bar{\mathbf{w}}_k) - F_{S_k}(\bar{\mathbf{w}}_{k-1})] \\ &\leq 8G^2 \log(4/\delta) \eta_k + \left(\frac{\mathbb{E}[\|\mathbf{u}_{k-1}\|_2^2]}{2\eta_k n_k} + \frac{3G^2 \eta_k}{2} \right) \leq \frac{\mathbb{E}[\|\mathbf{u}_{k-1}\|_2^2]}{2\eta_k n_k} + 18 \log(4/\delta) G^2 \eta_k, \end{aligned}$$

where the second identity is because $\bar{\mathbf{w}}_{k-1}$ is independent of S_k and the inequality follows from Theorem 6 Part (a) and Theorem 5. Recall that by definition $\eta \leq \frac{D\epsilon}{12G \log(4/\delta) \sqrt{2d \log(2.5/\delta)}}$, so that for all $k \geq 0$,

$$\mathbb{E}[\|\mathbf{u}_k\|_2^2] = d\sigma_k^2 = d \left(\frac{4^{-k} G \eta}{\epsilon} \right)^2 \leq 16^{-k} D^2.$$

Plugging the above estimate into (D.1) it follows

$$\begin{aligned} \mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] &\leq \sum_{k=1}^K \frac{8 \cdot 16^{-k} D^2}{4^{-k} 2^{-k} \eta n} + 18 \log(4/\delta) 4^{-k} G^2 \eta + 4^{-K} G D \\ &\leq \sum_{k=1}^K 2^{-k} \left(\frac{8D^2}{\eta n} + 18 \log(4/\delta) G^2 \eta \right) + \frac{GD}{n^2} \\ &= \mathcal{O} \left(GD \left(\frac{1}{\sqrt{n}} + \frac{\sqrt{d} \log^{\frac{3}{2}}(1/\delta)}{\epsilon n} \right) \right), \end{aligned}$$

where in the second inequality used $K = \lceil \log_2 n \rceil$, and the last inequality is due to $\eta = \frac{D}{G} \min\left\{\frac{\log(4/\delta)}{\sqrt{n}}, \frac{\epsilon}{12 \log(4/\delta) \sqrt{2d \log(2.5/\delta)}}\right\}$. The desired excess generalization error bound is proved.

Finally, we investigate the gradient complexity argument. Since we run Algorithm 1 for n_k at iteration k . Therefore, the total gradient complexity is $\mathcal{O}\left(\sum_{k=1}^K n_k\right) = \mathcal{O}(n \log(1/\delta))$. The proof is completed. \square

E Additional Results: Localization-Based Algorithm to Improve Theorem 1

In this section, we provide additional results on how to reduce the gradient complexity $\mathcal{O}(n^2)$ required in Theorem 1 to $\mathcal{O}(n)$ for nonsmooth problems. This improvement is attained by Algorithm 4 which is motivated by the iterative localization technique [12].

Algorithm 4 Localized SGD for Pairwise Learning

- 1: **Inputs:** Dataset $S = \{\mathbf{z}_i : i = 1, \dots, n\}$, parameter ζ , initial point \mathbf{w}_0
- 2: Set $K = \lceil \log_2 n \rceil$ and divide S into K disjoint subsets $\{S_1, \dots, S_K\}$ such that $|S_k| = n_k = 2^{-k}n$
- 3: **for** $k = 1$ to K **do**
- 4: Set $\zeta_k = 2^{-k}\zeta$
- 5: Compute $\bar{\mathbf{w}}_k \in \mathcal{W}$ by Algorithm 1 with step sizes $\eta_j = \frac{\zeta_k n_k}{j+1}, j \in [T_k]$ and $T_k \asymp n_k$ iterations based on the objective F_k where

$$F_k(\mathbf{w}; S_k) = \frac{1}{n_k(n_k - 1)} \sum_{z, z' \in S_k: z \neq z'} f(\mathbf{w}; \mathbf{z}, \mathbf{z}') + \frac{1}{\zeta_k n_k} \|\mathbf{w} - \bar{\mathbf{w}}_{k-1}\|_2^2$$

- 6: **Outputs:** $\bar{\mathbf{w}}_K$
-

The next theorem shows that the empirical risk minimization can imply models with good excess generalization error by Algorithm 4.

Theorem E.1. *Let (A1) and (A3) hold true with $\alpha = 0$ and let D be the diameter of \mathcal{W} . Let $\{\bar{\mathbf{w}}_k : k \in [K]\}$ be produced by Algorithm 4 with $\zeta = \frac{D}{G\sqrt{n}}$. Then we have the following excess generalization error bounds*

$$\mathbb{E}[F(\bar{\mathbf{w}}_K) - F(\mathbf{w}^*)] = \mathcal{O}\left(\frac{GD}{\sqrt{n}}\right)$$

with gradient complexity $\mathcal{O}(n)$.

We provide two technical lemmas before we present the proof of Theorem E.1.

Lemma 8. *Let (A1) and (A3) hold true with $\alpha = 0$ and let $\hat{\mathbf{w}}_k = \arg \min_{\mathbf{w}} F_k(\mathbf{w}; S_k)$, then*

$$\mathbb{E}[\|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2^2] = \mathcal{O}(G^2 \zeta_k^2 n_k).$$

Proof. Note that F_k is $\alpha_k = \frac{2}{\zeta_k n_k}$ -strongly convex, by the convergence of Algorithm 1 in Theorem 6 Part (b), we know that

$$\frac{\alpha_k}{2} \mathbb{E}[\|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2^2] \leq \mathbb{E}[F_k(\bar{\mathbf{w}}_k; S_k) - F_k(\hat{\mathbf{w}}_k; S_k)] = \mathcal{O}\left(\frac{G^2}{\alpha_k n_k}\right)$$

which implies

$$\mathbb{E}[\|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2^2] = \mathcal{O}(G^2 \zeta_k^2 n_k).$$

The proof is completed. \square

Lemma 9. *Let (A1) and (A3) hold true with $\alpha = 0$. For any $\mathbf{w} \in \mathcal{W}$, we know that*

$$\mathbb{E}[F(\hat{\mathbf{w}}_k) - F(\mathbf{w})] \leq \frac{\mathbb{E}[\|\bar{\mathbf{w}}_{k-1} - \mathbf{w}\|_2^2]}{\zeta_k n_k} + 2G^2 \zeta_k.$$

Proof. Let $r(\mathbf{w}; \mathbf{z}, \mathbf{z}') = f(\mathbf{w}, \mathbf{z}, \mathbf{z}') + \frac{1}{\zeta_k n_k} \|\mathbf{w} - \bar{\mathbf{w}}_{k-1}\|_2^2$, $R(\mathbf{w}) = \mathbb{E}_{\mathbf{z}, \mathbf{z}'}[r(\mathbf{w}; \mathbf{z}, \mathbf{z}')]$ and $\mathbf{w}_R^* = \arg \min_{\mathbf{w} \in \mathcal{W}} R(\mathbf{w})$. By the proof of Theorem 6 in Shalev-Shwartz et al. [32], one has that

$$\begin{aligned} & \mathbb{E}[F(\hat{\mathbf{w}}_k) + \frac{1}{\zeta_k n_k} \|\hat{\mathbf{w}}_k - \bar{\mathbf{w}}_{k-1}\|_2^2 - F(\mathbf{w}) - \frac{1}{\zeta_k n_k} \|\mathbf{w} - \bar{\mathbf{w}}_{k-1}\|_2^2] \\ &= \mathbb{E}[R(\hat{\mathbf{w}}_k) - R(\mathbf{w})] \leq \mathbb{E}[R(\hat{\mathbf{w}}_k) - R(\mathbf{w}_R^*)] \leq 2G^2 \zeta_k, \end{aligned}$$

which implies that

$$\begin{aligned} \mathbb{E}[F(\hat{\mathbf{w}}_k) - F(\mathbf{w})] &\leq 2G^2 \zeta_k - \frac{1}{\zeta_k n_k} \mathbb{E}[\|\hat{\mathbf{w}}_k - \bar{\mathbf{w}}_{k-1}\|_2^2] + \frac{1}{\zeta_k n_k} \mathbb{E}[\|\mathbf{w} - \bar{\mathbf{w}}_{k-1}\|_2^2] \\ &\leq 2G^2 \zeta_k + \frac{1}{\zeta_k n_k} \mathbb{E}[\|\mathbf{w} - \bar{\mathbf{w}}_{k-1}\|_2^2]. \end{aligned}$$

The proof is completed. \square

Proof of Theorem E.1. Let $\hat{\mathbf{w}}_0 = \mathbf{w}^*$, we have

$$\mathbb{E}[F(\bar{\mathbf{w}}_K)] - F(\mathbf{w}^*) = \sum_{k=1}^K \mathbb{E}[F(\hat{\mathbf{w}}_k) - F(\hat{\mathbf{w}}_{k-1})] + \mathbb{E}[F(\bar{\mathbf{w}}_K) - F(\hat{\mathbf{w}}_K)]. \quad (\text{E.1})$$

For the first term we have

$$\begin{aligned} \sum_{k=1}^K \mathbb{E}[F(\hat{\mathbf{w}}_k) - F(\hat{\mathbf{w}}_{k-1})] &\leq \sum_{k=1}^K \left(\frac{\mathbb{E}[\|\bar{\mathbf{w}}_{k-1} - \hat{\mathbf{w}}_{k-1}\|_2^2]}{\zeta_k n_k} + 2G^2 \zeta_k \right) \\ &= \mathcal{O}\left(\frac{D^2}{\zeta n} + \sum_{k=2}^K G^2 \zeta_k + \sum_{k=1}^K 2^{-k} G^2 \zeta\right) \\ &= \mathcal{O}\left(\frac{D^2}{\zeta n} + G^2 \zeta\right) \quad (\text{E.2}) \end{aligned}$$

where the first inequality is by Lemma 9, the second inequality is by Lemma 8 and $\zeta = \frac{D}{G\sqrt{n}}$. For the second term we have

$$\begin{aligned} \mathbb{E}[F(\bar{\mathbf{w}}_K) - F(\hat{\mathbf{w}}_K)] &\leq G \mathbb{E}[\|\bar{\mathbf{w}}_K - \hat{\mathbf{w}}_K\|_2] \leq G \sqrt{\mathbb{E}[\|\bar{\mathbf{w}}_K - \hat{\mathbf{w}}_K\|_2^2]} = \mathcal{O}(G^2 \zeta_K \sqrt{n_K}) \\ &= \mathcal{O}(2^{-2K} G^2 \zeta \sqrt{n}) = \mathcal{O}(G^2 \zeta) \quad (\text{E.3}) \end{aligned}$$

where the first inequality is by G -Lipschitz continuity of F , the second inequality is by Jensen's inequality, the first identity is by Lemma 8 and the second identity is by $n_k = 2^{-k} n$.

Now putting (E.2) and (E.3) back to (E.1) and using $\zeta = \frac{D}{G\sqrt{n}}$, we derive

$$\mathbb{E}[F(\bar{\mathbf{w}}_K)] - F(\mathbf{w}^*) = \mathcal{O}\left(\frac{GD}{\sqrt{n}}\right).$$

Finally we investigate the gradient complexity. Since F_k is $\frac{2}{\zeta_k n_k}$ -strongly convex, by Theorem 6 Part (b), we need to choose $T_k \asymp n_k$ so that Lemma 8 holds. Therefore, in total, we require $\mathcal{O}\left(\sum_{k=1}^K n_k\right) = \mathcal{O}(n)$ gradient complexity, which yields the desired result. \square

F Additional Results: Differentially Private SGD for Pairwise Learning with Non-Smooth Losses

In this section, we propose a differentially private algorithm based on iterative localization [12] for nonsmooth pairwise learning problems. The algorithm is presented as follows.

We are now ready to present the privacy guarantee and utility bound of Algorithm 5 in the following theorem. The proof differs from the iterative localization algorithm in pointwise learning [12] since we employ our high probability convergence results for non-smooth losses in pairwise learning.

Algorithm 5 Differentially Private Localized SGD for Pairwise Learning

- 1: **Inputs:** Dataset $S = \{\mathbf{z}_i : i \in [n]\}$, parameters ϵ, δ , and ζ , initial points \mathbf{w}_0
 - 2: Set $K = \lceil \log_2 n \rceil$ and divide S into K disjoint subsets $\{S_1, \dots, S_K\}$ where $|S_k| = n_k = 2^{-k}n$.
 - 3: **for** $k = 1$ to K **do**
 - 4: Set $\zeta_k = 4^{-k}\zeta$
 - 5: Compute $\bar{\mathbf{w}}_k \in \mathcal{W}$ by Algorithm 1 with step sizes $\eta_j = \frac{\zeta_k n_k}{j+1}$ on objective F_k such that with prob $1 - \delta$,
- $$F_k(\bar{\mathbf{w}}_k; S_k) - \min_{\mathbf{w} \in \mathcal{W}} F_k(\mathbf{w}; S_k) \leq G^2 \zeta_k / n_k$$
- where $F_k(\mathbf{w}; S_k) = \frac{1}{n_k(n_k-1)} \sum_{z, z' \in S_k: z \neq z'} f(\mathbf{w}; z, z') + \frac{1}{\zeta_k n_k} \|\mathbf{w} - \mathbf{w}_{k-1}\|_2^2$
- 6: Set $\mathbf{w}_k = \bar{\mathbf{w}}_k + \mathbf{u}_k$ where $\mathbf{u}_k \sim \mathcal{N}(0, \alpha_k^2 I_d)$ with $\sigma_k = 4G\zeta_k \sqrt{\log(2.5/\delta)} / \epsilon$.
 - 7: **Outputs:** \mathbf{w}_K
-

Theorem F.1. Let (A1) and (A3) hold true with $\alpha = 0$ and let D be the diameter of \mathcal{W} . Let $\{\mathbf{w}_k : k \in [K]\}$ be produced by Algorithm 5 with $\zeta = \frac{D}{G} \min\left\{\frac{4}{\sqrt{n}}, \frac{\epsilon}{4\sqrt{d \log(1/\delta)}}\right\}$. Then Algorithm 5 satisfies (ϵ, δ) -DP. Furthermore we have the following excess generalization error bounds

$$\mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] = \mathcal{O}\left(GD\left(\frac{1}{\sqrt{n}} + \frac{\sqrt{d \log(1/\delta)}}{\epsilon n}\right)\right)$$

with no more than $\mathcal{O}(n^2 \log(1/\delta))$ stochastic gradient computations.

Proof of Theorem F.1. We first consider the privacy guarantee of Algorithm 5. For any neighboring datasets $S = \{S_1, \dots, S_K\}$ and $S' = \{S'_1, \dots, S'_K\}$ differing by one example, where S' follows the same partition as S , and $S_i \cap S_j = \emptyset$ if $i \neq j$. Let $\hat{\mathbf{w}}_k = \arg \min_{\mathbf{w}} F_k(\mathbf{w}; S_k)$ and $\hat{\mathbf{w}}'_k = \arg \min_{\mathbf{w}} F_k(\mathbf{w}; S'_k)$. We first investigate the ℓ_2 -sensitivity of $\hat{\mathbf{w}}_k$. Since F_k is $\alpha_k = \frac{2}{\zeta_k n_k}$ -strongly convex, by Theorem 6 in Shalev-Shwartz et al. [32] we have

$$\|\hat{\mathbf{w}}_k - \hat{\mathbf{w}}'_k\|_2 \leq \frac{4G}{\alpha_k n_k} = 2G\zeta_k,$$

where $\bar{\mathbf{w}}'_k$ is the return from Line 5 in Algorithm 5 based on $F_k(\mathbf{w}; S'_k)$. By the strong convexity of F_k again, we have with probability at least $1 - \delta$

$$\frac{\alpha_k}{2} \|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2^2 \leq F_k(\bar{\mathbf{w}}_k; S_k) - F_k(\hat{\mathbf{w}}_k; S_k) \leq \frac{G^2 \zeta_k}{n_k}$$

which implies $\|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2 \leq G\zeta_k$. This further implies $\bar{\mathbf{w}}_k$ has ℓ_2 -sensitivity of $4G\zeta_k$ with probability $1 - \delta$. Therefore, by Lemma 5, each iteration k of Algorithm 5 is (ϵ, δ) -DP. Since the partition of the dataset S is disjoint, and each iteration k of Algorithm 5 we only use one subset, thus the whole process will still be (ϵ, δ) -DP.

Next we investigate the utility bound of Algorithm 5. Firstly, for any fixed \mathbf{w} ,

$$\begin{aligned} \mathbb{E}[F(\bar{\mathbf{w}}_k) - F(\mathbf{w})] &= \mathbb{E}[F(\hat{\mathbf{w}}_k) - F(\mathbf{w})] + \mathbb{E}[F(\bar{\mathbf{w}}_k) - F(\hat{\mathbf{w}}_k)] \\ &\leq \frac{\mathbb{E}[\|\mathbf{w}_{k-1} - \mathbf{w}\|_2^2]}{\zeta_k n_k} + 3G^2 \zeta_k \end{aligned}$$

where we used Lemma 9 and $\|\bar{\mathbf{w}}_k - \hat{\mathbf{w}}_k\|_2 \leq G\zeta_k$. Denote $\bar{\mathbf{w}}_0 = \mathbf{w}^*$ and $\mathbf{u}_0 = \mathbf{w}_0 - \mathbf{w}^*$, we have

$$\begin{aligned} \mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] &= \sum_{k=1}^K \mathbb{E}[F(\bar{\mathbf{w}}_k) - F(\bar{\mathbf{w}}_{k-1})] + \mathbb{E}[F(\mathbf{w}_K) - F(\bar{\mathbf{w}}_K)] \\ &\leq \sum_{k=1}^K \left(\frac{\mathbb{E}[\|\mathbf{u}_{k-1}\|_2^2]}{\zeta_k n_k} + 3G^2 \zeta_k \right) + G\mathbb{E}[\|\mathbf{u}_K\|_2]. \end{aligned} \tag{F.1}$$

Recall that by definition $\zeta \leq \frac{D\epsilon}{4G\sqrt{d \log(2.5/\delta)}}$, so that for all $k \geq 0$, there holds

$$\mathbb{E}[\|\mathbf{u}_k\|_2^2] = d\sigma_k^2 = d\left(\frac{4^{-k}G\zeta}{\epsilon}\right)^2 \leq 16^{-k}D^2.$$

Plugging the above estimate into (F.1) it follows

$$\begin{aligned}
\mathbb{E}[F(\mathbf{w}_K) - F(\mathbf{w}^*)] &\leq \sum_{k=1}^K 2^{-k} \left(\frac{8D^2}{\zeta n} + 3G^2\zeta \right) + 4^{-K} GD \\
&\leq \sum_{k=1}^K 2^{-k} GD \left(\frac{8}{n} \max \left\{ \sqrt{n}, \frac{\sqrt{d \log(1/\delta)}}{\epsilon} \right\} + \frac{1}{2\sqrt{n}} \right) + \frac{GD}{n^2} \\
&\leq 9GD \left(\frac{1}{\sqrt{n}} + \frac{\sqrt{d \log(1/\delta)}}{n\epsilon} \right) + \frac{GD}{n^2}.
\end{aligned}$$

This yields the desired utility bound.

Finally, we investigate the gradient complexity argument. Since F_k is $\frac{2}{\zeta_k n_k}$ -strongly convex. We know from Theorem 7 Part (b), after $T_k \asymp n_k^2 \log(1/\delta)$ iterations, we have with probability $1 - \delta$

$$F_k(\bar{\mathbf{w}}_k; S_k) - \min_{\mathbf{w}} F_k(\mathbf{w}; S_k) = \mathcal{O}\left(\frac{G^2 \zeta_k n_k \log(1/\delta)}{n_k^2 \log(1/\delta)}\right) = \mathcal{O}\left(\frac{G^2 \zeta_k}{n_k}\right)$$

which satisfies the requirement at Line 5 of Algorithm 5. Therefore, in total the gradient complexity is of the form $\mathcal{O}\left(\sum_{k=1}^K n_k^2 \log(1/\delta)\right) = \mathcal{O}(n^2 \log(1/\delta))$. The proof is completed. \square

G Additional Experiments

In this section, we provide the experimental details and additional experiments to support our theoretical findings. The datasets we used are from LIBSVM website [9]. The statistics of the data is included in Table G.1. For data with multiple classes, we convert the first half of class numbers to be the positive class and the second half of class numbers to be the negative class.

Table G.1: Data Statistics. n is the number of samples and d is the number of features.

	diabetes	german	ijcnn1	letter	mnist	usps
n	768	1,000	49,990	15,000	60,000	7,291
d	8	24	22	161	780	256

Table G.2: Average AUC score \pm standard deviation across multiple datasets. Our best results are highlighted in bold.

Algorithm	diabetes	german	ijcnn1	letter	mnist	usps
Our	.831 \pm .030	.793 \pm .021	.934 \pm .002	.810 \pm .007	.932 \pm .001	.926 \pm .006
SGD _{pair} [27]	.830 \pm .028	.794 \pm .023	.934 \pm .003	.811 \pm .008	.932 \pm .001	.925 \pm .006
OLP [22]	.825 \pm .028	.787 \pm .028	.916 \pm .003	.808 \pm .010	.927 \pm .003	.917 \pm .006
OAM _{gra} [45]	.828 \pm .026	.785 \pm .029	.930 \pm .003	.806 \pm .008	.898 \pm .002	.916 \pm .005
OLP-RS1	.736 \pm .074	.630 \pm .065	.668 \pm .026	.683 \pm .033	.749 \pm .045	.737 \pm .056
OAM-RS1	.737 \pm .069	.640 \pm .058	.677 \pm .014	.675 \pm .050	.685 \pm .042	.691 \pm .059
SPAUC [26]	.828 \pm .031	.799 \pm .026	.932 \pm .002	.809 \pm .008	.927 \pm .002	.923 \pm .005

For each dataset, we have used 80% of the data for training and the remaining 20% for testing. The results are based on 25 runs of random shuffling. The generalization performance is reported using the average AUC score and standard deviation on the test data. To determine proper hyper parameters, we conduct 5-fold cross validation on the training sets: 1) for Algorithm 1 and SGD_{pair}, we select step sizes $\eta_t = \eta \in 10^{[-3:3]}$ and \mathcal{W} diameter $D \in 10^{[-3:3]}$; 2) for OLP we select step sizes $\eta_t = \eta/\sqrt{t}$ where $\eta \in 10^{[-3:3]}$ and \mathcal{W} diameter $D \in 10^{[-3:3]}$; 3) for OAM_{gra} we select learning rate parameter $C \in 10^{[-3:3]}$; 4) for SPAUC we select step sizes $\eta_t = \eta/\sqrt{t}$ where $\eta \in 10^{[-3:3]}$.

Firstly, Table G.2 summarizes the generalization performance of different algorithms which contains more comparison results than Table 1. In particular, two additional results are added for comparison, i.e. OLP-RS1 and OAM-RS1 which denote the OLP [22] and OAM_{gra} [45] with Reservoir sampling and the buffering set size $s = 1$, respectively. We can see that OLP-RS1 and OAM-RS1 are inferior to other algorithms. This inferior performance for OLP and OAM with a small buffering set was also observed in the experiments of [22, 45].

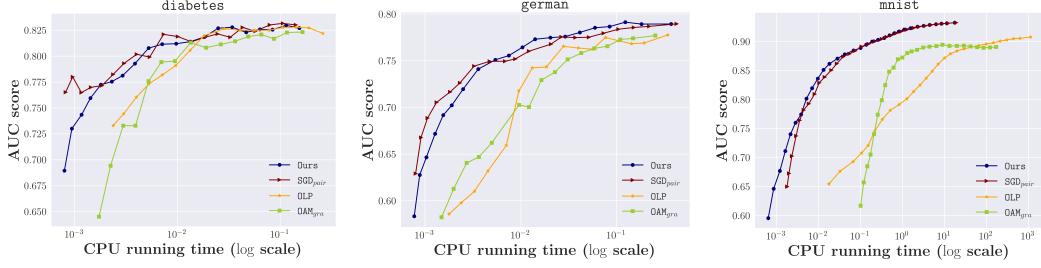


Figure G.1: More CPU running time against AUC score for the hinge loss

Secondly, we also report more plots on CPU running time against the AUC score on different datasets. Figure G.1 contains more convergence plots for the hinge loss. For a fair comparison of Algorithm 1 with SPAUC, the loss function is chosen as the least square loss for Algorithm 1, SGD_{pair} and GLP. The results are shown in Figure G.2. We can see there that SPAUC performs very well among most of the datasets. However, this algorithm was designed very specifically for the AUC maximization problem with the least square loss while our algorithm can handle any loss functions and any pairwise learning problems. We can also observe that our algorithm and SGD_{pair} converge in a similar CPU running time. In fact, Algorithm 1 is slightly faster than SGD_{pair} when the number of samples gets larger. This is partly due to different sampling schemes in Algorithm 1 and SGD_{pair} . Indeed, at each iteration SGD_{pair} picks a random pair of examples from $\binom{n}{2}$ pairs, while Algorithm 1 only needs to randomly pick one example from n individual ones. Figure G.3 depicts the CPU times of these two sampling schemes versus the the number of examples n . We can see that, when the sample size n increases, the sampling scheme used in SGD_{pair} needs significantly more time than our algorithm.

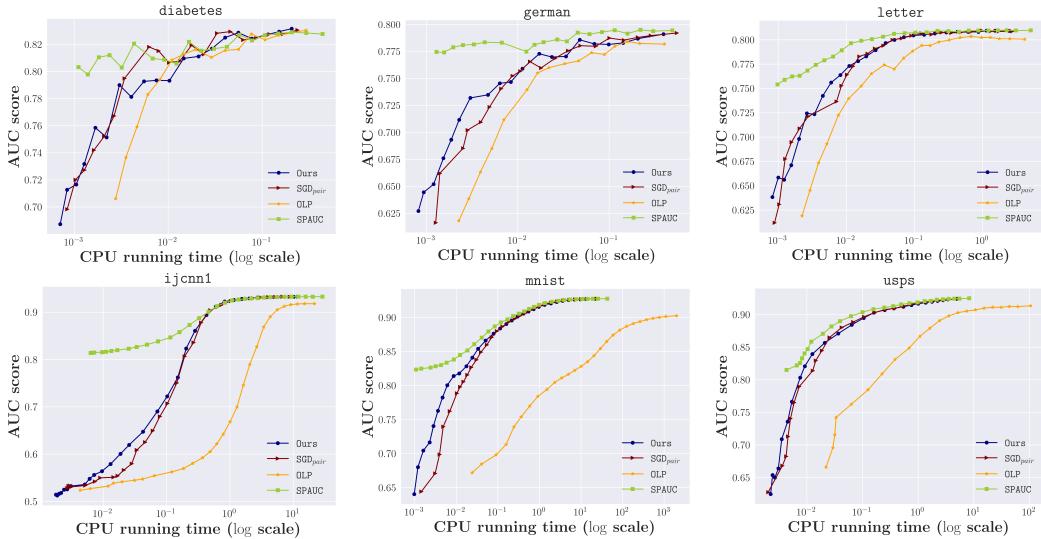


Figure G.2: AUC score against CPU running time for the square loss

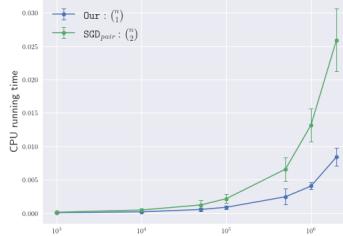


Figure G.3: CPU running time of different sampling schemes against the sample size n

Next, we investigate our Algorithm 1 in the non-convex setting. To this end, we use the logistic link function $\text{logit}(t) = (1 + \exp(-t))^{-1}$ and then the square loss surrogate function $\ell(t) = (1 - t)^2$.

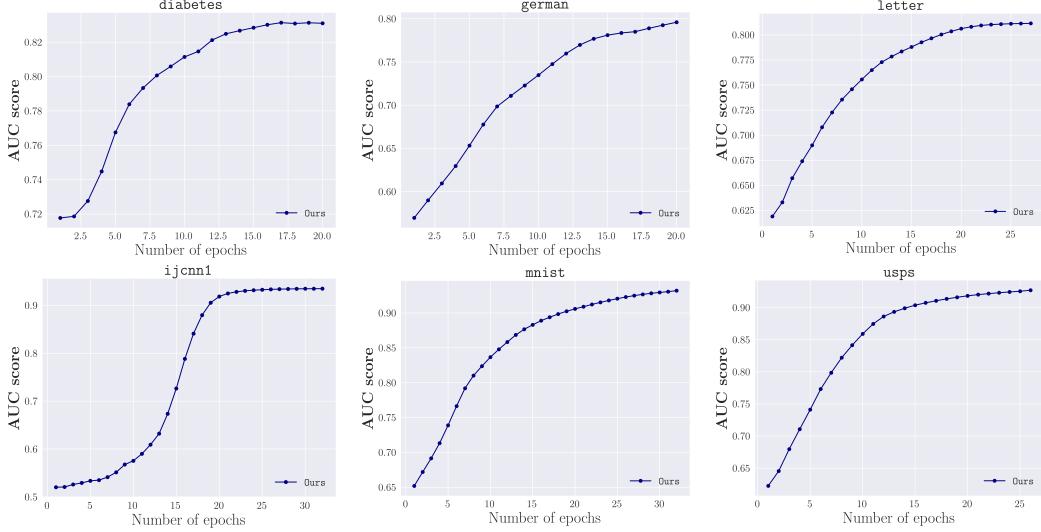


Figure G.4: Convergence of Algorithm 1 for the generalized linear model

That is, the loss function for the problem of AUC maximization becomes $f(\mathbf{w}; (\mathbf{x}, y), (\mathbf{x}', y')) = (1 - \text{logit}(\mathbf{w}^\top (\mathbf{x} - \mathbf{x}')))^2 \mathbb{I}_{[y=1 \wedge y'=-1]}$. Although f is non-convex, it was shown that it satisfies the PL condition [13]. The results are reported in Figure G.4 which shows that Algorithm 1 also converges very quickly in this non-convex setting.

Finally, we compare our differentially private algorithm for AUC maximization (i.e. Algorithm 3) with the logistic loss $\ell(t) = \log(1 + \exp(-t))$ against the state-of-art algorithm DPEGD [39]. DPEGD used gradient descent and the localization technique to guarantee privacy. Algorithm 1 was used as non-private baseline, i.e. $\epsilon = 0$. Here, $\delta = \frac{1}{n}$ as suggested in the previous work [39]. We consider the effect of different privacy budget ϵ 's against the generalization ability. The implementation across all algorithms is based on fixed training size 256. Average AUC scores over 25 times repeated experiments are listed in Table G.3 and G.4 for the datasets of diabetes and german, respectively. These results demonstrate Algorithm 3 achieves competitive performance with DPEGD using full gradient descent.

Table G.3: Average AUC \pm standard deviation on diabetes. Non-Private result is $.813 \pm .016$.

Algorithm	$\epsilon = 0.2$	$\epsilon = 0.5$	$\epsilon = 0.8$	$\epsilon = 1.0$	$\epsilon = 1.5$	$\epsilon = 2.0$
Our	$.690 \pm .094$	$.751 \pm .028$	$.771 \pm .016$	$.783 \pm .024$	$.784 \pm .018$	$.789 \pm .018$
DPEGD [39]	$.624 \pm .109$	$.727 \pm .055$	$.768 \pm .027$	$.796 \pm .011$	$.797 \pm .017$	$.792 \pm .016$

Table G.4: Average AUC \pm standard deviation on german. Non-Private result is $.763 \pm .016$.

Algorithm	$\epsilon = 0.2$	$\epsilon = 0.5$	$\epsilon = 0.8$	$\epsilon = 1.0$	$\epsilon = 1.5$	$\epsilon = 2.0$
Our	$.614 \pm .035$	$.672 \pm .064$	$.721 \pm .024$	$.725 \pm .032$	$.747 \pm .019$	$.749 \pm .021$
DPEGD [39]	$.598 \pm .018$	$.703 \pm .039$	$.723 \pm .029$	$.742 \pm .028$	$.753 \pm .017$	$.757 \pm .018$

We also report the CPU running times of Algorithm 3 and DPEGD. In this setting, we fix the privacy budget $\epsilon = 1$ and vary the training size n . The results are reported in Table G.5. These results shows that Algorithm 3 can arrive competitive performance with DPEGD with less CPU running time.

Table G.5: Average AUC score and average CPU running time \pm standard deviation.

Algorithm		diabetes			german		
		$n = 100$	$n = 200$	$n = 300$	$n = 100$	$n = 200$	$n = 300$
Our	AUC	$.709 \pm .051$	$.788 \pm .019$	$.790 \pm .021$	$.681 \pm .029$	$.692 \pm .032$	$.734 \pm .022$
	Time	$.046 \pm .010$	$.096 \pm .019$	$.135 \pm .026$	$.377 \pm .097$	$.637 \pm .136$	$.767 \pm .151$
DPEGD [39]	AUC	$.705 \pm .070$	$.772 \pm .017$	$.777 \pm .023$	$.687 \pm .033$	$.700 \pm .038$	$.755 \pm .019$
	Time	$.421 \pm .067$	$.885 \pm .158$	$1.41 \pm .248$	$1.00 \pm .185$	$1.88 \pm .273$	$2.57 \pm .421$