Supplementary Document for SQuaFL: Sketched-Quantization based Communication Efficient Federated Learning

We provide the theoretical results of the convergence of SQuaFL for non-convex and convex objectives. First, we state the standard assumptions and definitions commonly used in the context of analyzing stochastic algorithms satisfied by our compressors $\mathcal{S}(\mathcal{Q}(.))$, weight matrix w and objective function f. Here, $\|.\|$ denotes the l_2-norm of a vector v.

Assumption 1. *The local objective function f_n is differentiable and L-smooth such that, $\|\nabla f_n(u) - \nabla f_n(v)\| \leq L\|u - v\|$, $\forall u, v \in \mathbb{R}^d$, for a constant $L > 0$ and is lower-bounded, i.e., $f^* = \min_{w\in\mathbb{R}^d} f(w) > -\infty$.*

Assumption 2. *For all devices n, the stochastic gradients $g_n = \nabla f_n(v)$ are unbiased and variance bounded i.e., $\mathbb{E}[g] = \bar{g}$ and $\mathbb{E}[\|g - \bar{g}\|^2] \leq \sigma^2$, where $\bar{g}$ is the full batch gradient.*

Assumption 3. *A function f is λ-strongly convex if for all $u, v \in \mathbb{R}^d$ we have, $f(u) \geq f(v) + \langle \nabla f(v), u - v\rangle + \frac{\lambda}{2}\|u - v\|^2$.*

We state the following lemma in [1] about the important properties Count Sketches possess, useful in our analysis.

Lemma 1. *For a Count Sketch $\mathcal{S}$ with r hash tables of b bins into $r \times b$ array of counters, for any input element $v_i \in v$ with probability $1 - \delta$, the following relations of unbiasedness and bounded estimation error of Count Sketches hold,*

$$\begin{aligned} &\mathbb{E}[\mathcal{S}(v)] = v, \\ &\mathbb{E}[\|\mathcal{S}(v) - v\|^2] \leq \mu^2 d\|v\|^2, \end{aligned} \tag{1}$$

where $a = \mathcal{O}(\ln(d/\delta))$ and $b = \mathcal{O}(e/\mu^2)$.

Proof. Proof can be found in [1]. ☐

We introduce our following main lemma to show this by stating the properties of our sketched-quantized compressor $\mathcal{S}(\mathcal{Q}(.))$.

Lemma 2. *For a Count Sketch estimate $\mathcal{S}(\cdot)$ with $r = \mathcal{O}(\ln(d/\delta))$ hash tables and $b = \mathcal{O}(e/\mu^2)$ bins over quantized values $\mathcal{Q}(\cdot)$ of any vector v with quantization noise q, to achieve μL_2 additive errors with probability $(1-\delta)$, the following respective relations of unbiasedness and bounded estimation error of our compression hold,*

$$\begin{aligned} &\mathbb{E}[\tilde{v}] = v, \\ &\mathbb{E}[\|\tilde{v} - v\|^2] \leq \Delta\|v\|^2, \end{aligned} \tag{2}$$

where $\tilde{v} = \mathcal{S}(\mathcal{Q}(v))$ and $\Delta = (2\mu^2 d(1 + q) + 2q)$.

Proof.

$$\mathbb{E}[\mathcal{S}(\mathcal{Q}(v))] = \mathbb{E}_{\mathcal{Q}}[\mathbb{E}_{\mathcal{S}}[\mathcal{S}(\mathcal{Q}(v))|\mathcal{Q}(v)]] = \mathbb{E}_{\mathcal{Q}}[\mathcal{Q}(v)] = v,$$

where the first equality follows from the tower property and the second and third from unbiasedness of sketch and quantization respectively. Bounded variance can be shown as,

$$\begin{aligned} &\mathbb{E}[\|\mathcal{S}(\mathcal{Q}(v)) - v\|^2] = \mathbb{E}_{\mathcal{Q}}[\mathbb{E}_{\mathcal{S}}[\|\mathcal{S}(\mathcal{Q}(v)) - v\|^2|\mathcal{Q}(v)]] \\ &= \mathbb{E}_{\mathcal{Q}}[\mathbb{E}_{\mathcal{S}}[\|\mathcal{S}(\mathcal{Q}(v)) - \mathcal{Q}(v) + \mathcal{Q}(v) - v\|^2|\mathcal{Q}(v)]] \\ &\leq 2\mu^2 d\mathbb{E}_{\mathcal{Q}}[\|\mathcal{Q}(v)\|^2] + 2\mathbb{E}_{\mathcal{Q}}[\|\mathcal{Q}(v) - v\|^2] \\ &\leq (2\mu^2 d(1 + q) + 2q)\|v\|^2, \end{aligned}$$

where the first inequality follows from $\mathbb{E}[\|a + b\|^2] \leq 2\mathbb{E}\|a\|^2 + 2\mathbb{E}\|b\|^2$, and the final inequality follows from the bounded variances of sketch and quantization. ☐

Definition 1. *(ϵ-differential privacy). A randomized mechanism $\mathcal{A}$ is ϵ-differentially private if for any two neighboring inputs D, D' that differ in at most one single element, and for any possible output s in the output space of $\mathcal{A}$, it holds that*

$$Pr(\mathcal{A}(D) = s) \leq e^{\epsilon} Pr(\mathcal{A}(D') = s)$$

Using Definition 1, we state the following theorem in [1] that provides differential privacy guarantees of Count Sketch.

Theorem 1. *(ϵ-differential privacy of Count Sketch, [1]). For a sketching algorithm using Count Sketch $S_{r\times b}$ with r arrays of b bins, for any input vector with length κ drawn from a Gaussian distribution $\mathcal{N}(0,\sigma^2)$, and is bounded by a constant ϕ with a large probability, achieves $r.\ln\left(1+\frac{\zeta\phi^2 b(b-1)}{\sigma^2(\kappa-2)}(1+\ln(\kappa-b))\right)$-differential privacy with high probability, where ζ is a positive constant satisfying $\frac{\phi^2 b(b-1)}{\sigma^2(\kappa-2)}(1+\ln(\kappa-b))\leq\frac{1}{2}-\frac{1}{\zeta}$.*

Proof. Proof can be found in [1]. □

Next, we present the following intermediate lemmas to analyze the convergence of SQuaFL.

Lemma 3. *The expectation of the inner product of the stochastic gradient and batch gradient can be bounded using the smoothness and lower boundedness assumption of the local objective function, denoted by $\mathbb{E}_{\mathrm{C}}$ as,*

$$-\mathbb{E}_{\xi,\mathrm{C}}[\langle\nabla f(w_t),g_t\rangle]\leq\frac{\eta}{2N}\sum_{n=1}^{N}[-\|\nabla f(w_t)\|^2-\|\nabla f(w_t^n)\|^2+L^2\eta^2[\sigma^2+\|\bar{g}_t^n\|^2]]. \tag{3}$$

Proof. Expectation over our sketched-quantization compressor denoted by $\mathbb{E}_{\mathrm{C}}$ can be applied as,

$$\begin{aligned}
&-\mathbb{E}[\mathbb{E}_{\mathrm{C}}[\langle\nabla f(w_t),\psi_t\rangle]]\\
&=-\mathbb{E}[\langle\nabla f(w_t),\eta\frac{1}{N}\sum_{n=1}^{N}g_t^n\rangle]\\
&=-\langle\nabla f(w_t),\frac{\eta}{N}\sum_{n=1}^{N}\mathbb{E}[g_t^n]\rangle\\
&=-\frac{\eta}{N}\sum_{n=1}^{N}\langle\nabla f(w_t),\bar{g}_t^n\rangle=-\frac{\eta}{N}\sum_{n=1}^{N}\langle\nabla f(w_t),\nabla f(w_t^n)\rangle &(4)\\
&=-\frac{1}{2}\frac{\eta}{N}\sum_{n=1}^{N}[\|\nabla f(w_t)\|^2+\|\nabla f(w_t^n)\|^2-\|\nabla f(w_t)-\nabla f(w_t^n)\|^2] &(5)\\
&\leq\frac{1}{2}\frac{\eta}{N}\sum_{n=1}^{N}[-\|\nabla f(w_t)\|^2-\|\nabla f(w_t^n)\|^2+L^2\|w_t-w_t^n\|^2] &(6)\\
&\leq\frac{\eta}{2N}\sum_{n=1}^{N}\left[-\|\nabla f(w_t)\|^2-\|\nabla f(w_t^n)\|^2+L^2\eta^2[\sigma^2+\|\bar{g}_t^n\|^2]\right], &(7)
\end{aligned}$$

where (4) is from Assumption 2, (5) is due to the property of $2\langle u,v\rangle=\|u\|^2+\|v\|^2+\|u-v\|^2$ and (6) is from the smoothness assumption 1. We use the following Lemma 4 to bound the last term in (6) to hence obtain (7). □

Lemma 4. *For a given communication round t, bound for the distance between the global and local models can be given as,*

$$\mathbb{E}[\|w_t-w_t^n\|^2]\leq\eta^2\sigma^2+\eta^2\|\bar{g}_t^n\|^2. \tag{8}$$

Proof. From the update rule of our algorithm we have,

$$\mathbb{E}[\|w_t-w_t^n\|^2]=\mathbb{E}[\|w_t-(w_t-\eta g_t^n)\|^2]=\mathbb{E}[\|\eta g_t^n\|^2].$$

Using the expression of variance, $\mathrm{var}[u]=\mathbb{E}[u^2]+[\mathbb{E}[u]^2]$,

$$\begin{aligned}
\mathbb{E}[\|\eta g_t\|^2]&=\mathbb{E}[\|\eta\mathrm{var}[g_t^n]\|^2]+[\|\eta\bar{g}_t^n\|^2]\\
&=\eta^2\mathbb{E}[\|g_t^n-\bar{g}_t^n\|^2]+\eta^2\|\bar{g}_t^n\|^2\\
&=\eta^2\sigma^2+\eta^2\|\bar{g}_t^n\|^2, &(9)
\end{aligned}$$

where (9) also uses variance boundedness of the gradient from Assumption 2. □

Lemma 5. *The expectation of quantized and sketched stochastic gradients can be bounded using unbiased compression properties of our compressor and bounded variance assumptions of the gradients as,*

$$\mathbb{E}[\mathbb{E}_{\mathrm{C}}[\|\psi_t\|^2]]\leq[\Delta+1]\frac{\sigma^2}{N}+\left[\frac{\Delta}{N}+1\right]\frac{1}{N}\sum_{n=1}^{N}\|\bar{g}_t^n\|^2. \tag{10}$$

Proof.

$$\begin{aligned}
\mathbb{E}\left[\mathbb{E}_{\mathrm{C}}[\|\psi_t\|^2]\right] &= \mathbb{E}\left[\mathbb{E}_{\mathrm{C}}\left[\left\|\frac{1}{N}\sum_{n=1}^{N} S(Q(g_t^n))\right\|^2\right]\right] \\
&= \mathbb{E}\left[\mathbb{E}_{\mathrm{C}}\left[\left\|\frac{1}{N}\sum_{n=1}^{N} \psi_t^n\right\|^2\right]\right] \\
&= \mathbb{E}\left[\mathbb{E}_{\mathrm{C}}\left[\left\|\frac{1}{N}\sum_{n=1}^{N} \psi_t^n - \frac{1}{N}\sum_{n=1}^{N}\mathbb{E}_{\mathrm{C}}[\psi_t^n]\right\|^2\right] + \left\|\frac{1}{N}\sum_{n=1}^{N}\mathbb{E}_{\mathrm{C}}[\psi_t^n]\right\|^2\right] && (11) \\
&= \mathbb{E}\left[\mathbb{E}_{\mathrm{C}}\left[\frac{1}{N^2}\sum_{n=1}^{N}\|\psi_t^n - g_t^n\|^2\right] + \left\|\frac{1}{N}\sum_{n=1}^{N} g_t^n\right\|^2\right] && (12) \\
&\le \mathbb{E}\left[\frac{1}{N^2}\sum_{n=1}^{N}\Delta\|g_t^n\|^2\right] + \left\|\frac{1}{N}\sum_{n=1}^{N} g_t^n\right\|^2 && (13) \\
&= \sum_{n=1}^{N}\frac{\Delta}{N^2}\left[\mathrm{var}[g_t^n] + \|\bar{g}_t^n\|^2\right] + \left[\mathrm{var}\left(\frac{1}{N}\sum_{n=1}^{N} g_t^n\right) + \left\|\frac{1}{N}\sum_{n=1}^{N}\bar{g}_t^n\right\|^2\right] && (14) \\
&\le \sum_{n=1}^{N}\frac{\Delta}{N^2}[\sigma^2 + \|\bar{g}_t^n\|^2] + \left[\frac{1}{N^2}\sum_{n=1}^{N}\sigma^2 + \frac{1}{N}\sum_{n=1}^{N}\|\bar{g}_t^n\|^2\right] && (15) \\
&\le [\Delta+1]\frac{\sigma^2}{N} + \left[\frac{\Delta}{N}+1\right]\frac{1}{N}\sum_{n=1}^{N}\|\bar{g}_t^n\|^2.
\end{aligned}$$

where (11) and (14) follow from the variance expression, results from Lemma 2 are used in (12) and (13). (15) is obtained using the variance bound of the gradient from Assumption 2. Hence the proof is completed. □

Theorem 2. *(Non-convex). Considering the iterates w_t generated from our SQuaFL algorithm with sketch size $\mathcal{O}\left(b\log\left(\frac{dT}{\delta}\right)\right)$, where the given bins $b = \mathcal{O}\left(\frac{e}{\mu^2}\right)$, suppose that the conditions in Assumptions 1-2 hold and we set the step size as $\eta = \frac{1}{L}\sqrt{\frac{N}{T(\Delta+1)}}$, then the following condition holds,*

$$\frac{1}{T}\sum_{t=0}^{T-1}\|\nabla f(w_t)\|^2 \le \frac{2(f(w_0)-f^*)}{\eta^2 T} + L^2\eta^2\sigma^2 + \frac{L\eta^2\sigma^2(\Delta+1)}{N}. \tag{16}$$

Proof. The sequence of iterates computed from the update step of the SQuaFL algorithm is given by,

$$w_{t+1} = w_t - \eta\psi_t \tag{17}$$

Since we quantize and sketch the local updates, values returned from query used to update the global model can be written as,

$$\begin{aligned}
w_{t+1} &= w_t - \eta\left(\frac{\eta}{N}\sum_{n=1}^{N}\left[S\left(Q\left(\frac{w_t - w_t^n}{\eta}\right)\right)\right]\right) \\
w_{t+1} &= w_t - \eta\left(\frac{\eta}{N}\sum_{n=1}^{N} S\left(Q\left(g_t^n\right)\right)\right) && (18)
\end{aligned}$$

Next, taking expectation over the randomness of quantization and count sketch as $\mathbb{E}_{\mathrm{C}}$ and using the unbiased properties,

$$\begin{aligned}
\mathbb{E}_{\mathrm{C}}[\psi_t] &= \mathbb{E}\left[\frac{\eta}{N}\sum_{n=1}^{N}\left[S\left(Q\left(\frac{w_t - w_t^n}{\eta}\right)\right)\right]\right] \\
&= \frac{1}{N}\sum_{n\in\mathcal{N}}\left[-\eta\mathbb{E}_{\mathrm{C}}\left[S\left(Q\left(g_t^n\right)\right)\right]\right] \triangleq g_t. && (19)
\end{aligned}$$

Using the results from (17), (19) and L-smoothness assumption of the gradient we have,

$$f(w_{t+1}) - f(w_t) \le -\eta\langle\nabla f(w), g_t\rangle + \frac{\eta^2 L}{2}\|g_t\|^2. \tag{20}$$

Taking expectation over sampling on both sides, we obtain:

$$\begin{aligned}\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[f(w_{t+1})-f(w_t)\right]] &\leq -\eta\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[\langle\nabla f(w),\psi_t\rangle\right]]+\frac{\eta^2 L}{2}\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[\|\psi_t\|^2\right] \\ &= -\eta\mathbb{E}[\langle\nabla f(w),g_t\rangle]+\frac{\eta^2 L}{2}\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[\|\psi_t\|^2\right].\end{aligned} \tag{21}$$

Using the results from Lemmas 3, 4 and 5 to bound the terms in (21) we obtain,

$$\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[f(w_{t+1})-f(w_t)\right]] \leq \frac{L\eta^4\sigma^2}{2N}[\Delta+1+LN]-\frac{\eta^2}{2N}\sum_{n=1}^{N}\|\bar{g}_t^n\|^2\left[-L\eta^2\left(\frac{\Delta}{N}+1\right)-L^2\eta^2+1\right]-\frac{\eta^2}{2}\|\nabla f(w_t)\|^2. \tag{22}$$

Suppose the value of $[-L\eta^2\left(\frac{\Delta}{N}+1\right)-L^2\eta^2+1]\leq 1$, we can rewrite (22) as,

$$\mathbb{E}[\mathbb{E}_{\mathrm{C}}\left[f(w_{t+1})-f(w_t)\right]] \leq -\frac{\eta^2}{2}\|\nabla f(w_t)\|^2+\frac{L\eta^2\sigma^2}{2N}[\Delta+1+L\eta N].$$

Summing up over communication rounds $t=0,\cdots,T-1$ and rearranging the terms yields the following, hence proving the theorem,

$$\frac{1}{T}\sum_{t=0}^{T-1}\|\nabla f(w_t)\|^2 \leq \frac{2(f(w_0)-f(w_*))}{\eta^2 T}+L^2\eta^2\sigma^2+\frac{L\eta^2\sigma^2(\Delta+1)}{N}. \tag{23}$$

□

Corollary 1. *The number of communication rounds by using the results and step size as indicated in Theorem 2 with* $\eta=\frac{1}{L}\sqrt{\frac{N}{T(\Delta+1)}}$*, can be roughly set as,* $T\geq\mathcal{O}\left(\frac{N}{\Delta+1}\right)$.

Proof. A lower bound can be obtained on the communication rounds by rewriting the step size condition as,

$$\begin{aligned}L^2\eta^2+L\eta^2\left(\frac{\Delta}{N}+1\right) &\leq 1 \\ &= \frac{\sqrt{\left(\frac{\Delta}{N}+1\right)^2+4}-\left(\frac{\Delta}{N}+1\right)}{2L}.\end{aligned} \tag{24}$$

Using the step size value as indicated in Theorem 2 as $\eta=\frac{1}{L}\sqrt{\frac{N}{T(\Delta+1)}}$ in (24) we obtain,

$$T \geq 4N/\left[(\Delta+1)\eta^2\left[\sqrt{\left(\frac{\Delta}{N}+1\right)^2\eta^2+4}-\left(\frac{\Delta}{N}+1\right)\eta^2\right]^2\right] \tag{25}$$

$$\geq \mathcal{O}\left(\frac{N}{(\mu^2 d+q)+1}\right). \tag{26}$$

Hence, for a target accuracy ϵ, we can have $T\geq\mathcal{O}\left(\frac{N}{\Delta+1}\right)$ number of communication rounds. □

Theorem 3. *(Strongly Convex). From the iterates generated from our SQuaFL algorithm for the total number of communication rounds* T*, suppose that the conditions in Assumptions 1-3 hold and we set the step size as* $\eta=\sqrt{\frac{1}{2L\left(\frac{\Delta}{N}+1\right)}}$ *and given bins* $b=\mathcal{O}\left(\frac{e}{\mu^2}\right)$*, then the following holds,*

$$\mathbb{E}[f(w_T)-f^*] \leq (1-\eta^2\lambda)^T(f(w_0)-f^*)+\frac{L\eta^2\sigma^2}{2\lambda}\left[L+(\Delta+1)\frac{1}{N}\right]. \tag{27}$$

Proof. Using the condition stated in (24),

$$L^2\eta^2+L\eta^2\left(\frac{\Delta}{N}+1\right)\leq 1,$$

we can obtain,

$$\begin{aligned}\mathbb{E}[f(w_{t+1})-f(w_t)] &\leq -\frac{\eta^2}{2}\|\nabla f(w_t)\|^2+\frac{L\eta^4\sigma^2}{2N}(LN+(\Delta+1)) \\ &\leq -\lambda\eta^2(f(w_{t+1})-f(w_t))+\frac{L\eta^4\sigma^2}{2N}(LN+(\Delta+1)).\end{aligned} \tag{28}$$

With the optimal solution f^*, we can obtain the following bound,

$$\mathbb{E}[f(w_{t+1}) - f^*] \leq (1 - \eta^2\lambda)(f(w_t) - f^*) + \frac{L\eta^4\sigma^2}{2N}(LN + (\Delta + 1)).$$

Over T communication rounds, we can obtain the following,

$$\begin{aligned}\mathbb{E}[f(w_T) - f^*] &\leq (1 - \eta^2\lambda)^T(f(w_0) - f^*) + \frac{1 - (1 - \eta^2\lambda)^T}{1 - (1 - \eta^2\lambda)}\frac{L\eta^4\sigma^2}{2N}(LN + (\Delta + 1)) \\ &= (1 - \eta^2\lambda)^T(f(w_0) - f^*) + \frac{1}{\eta^2\lambda}\frac{L\eta^4\sigma^2}{2N}(LN + (\Delta + 1)). \qquad (29)\end{aligned}$$

Hence, we obtain the value in (27) proving the theorem. □

REFERENCES

[1] T. Li, Z. Liu, V. Sekar, and V. Smith, "Privacy for free: Communication-efficient learning with differential privacy using sketches," *arXiv preprint arXiv:1911.00972*, 2019.

APPENDIX