



Towards Communication-Efficient and Personalized Federated Learning

Wojciech Samek

Dept. of Artificial Intelligence, Fraunhofer HHI



2021 IEEE SPS Cycle 2 Virtual School on Networked FL: Theory, Algorithms and Applications

31st March 2022

Distributed Data







Distributed Data

Centralized Learning







Federated Learning - Challenges

Fraunhofer

Heinrich Hertz Institute





Reducing Communication Overhead







Communication Overhead

Total Communication = [#Communication Rounds] x [#Parameters] x [#Avg. Codeword length]

Communication Overhead (1 client): VGG16 on ImageNet

- Number of Iterations until Convergence: 900.000
- Number of Parameters: 138.000.000
- Bits per Parameters: 32

raunhofer

--> Total Communication = **496.8 Terabyte**



Federated Learning - Compression Methods

Total Communication = [#Communication Rounds] x [#Parameters] x [#Avg. Codeword length]

Compression Methods

- Communication Delay
- Lossy Compression: Unbiased
- Lossy Compression: Biased
- Efficient Encoding

🚿 Fraunhofer



Communication Delay

Distributed SGD:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:

<u>Client does:</u>

$$g_i \leftarrow \nabla_{\theta} l(\theta_t, D_i^b)$$

Server does:

$$\theta_{t+1} = \theta_t - \eta \frac{1}{M} \sum_i g_i$$

濍 Fraunhofer

Heinrich Hertz Institute

Federated Averaging:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:

Client does:

$$\theta_i = \mathrm{SGD}_K(\theta_t, D_i)$$

 $\frac{\text{Server does:}}{\theta_{t+1} = \frac{1}{M} \sum_{i} \Delta \theta_i}$



Communication Delay

Advantages:

• Simple

🖉 Fraunhofer

einrich Hertz Institute

- Reduces Communication *Frequency* (advantageous in on-device FL)
- Reduces both Upstream and Downstream communication
- Easy to integrate with Privacy mechanisms



Statistical Heterogeneity

Convergence speed drastically decreases with increasing heterogeneity in the data

→ This effect aggravates if the number of participating clients ("reporting fraction") is low

濍 Fraunhofer



Hsu, Tzu-Ming Harry, Hang Qi, and Matthew Brown. "Measuring the effects of nonidentical data distribution for federated visual classification."



Communication Delay

Advantages:

• Simple

🖉 Fraunhofer

ainrich Hartz Institute

- Reduces Communication *Frequency* (more practical in on-device FL)
- Reduces Upstream + Downstream communication
- Easy to integrate with Privacy mechanisms

Disadvantages:

- Bad performance on non-iid data
- Low sample efficiency



Federated Learning - Compression Methods

Total Communication = [#Communication Rounds] x [#Parameters] x [#Avg. Codeword length]

Compression Methods

- Communication Delay
- Lossy Compression: Unbiased
- Lossy Compression: Biased
- Efficient Encoding

🚿 Fraunhofer



Update Compression

Distributed SGD:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:

Client does:

$$g_i \leftarrow \nabla_{\theta} l(\theta_t, D_i^b)$$

Server does:

$$\theta_{t+1} = \theta_t - \eta \frac{1}{M} \sum_i g_i$$

Distributed SGD with Compression:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:

<u>Client does:</u>

$$g_i \leftarrow \nabla_\theta l(\theta_t, D_i^b)$$
$$\tilde{g_i} \leftarrow \text{comp}(g_i)$$

Server does:

$$heta_{t+1} = heta_t - \eta rac{1}{M} \sum_i ilde{g_i}$$





Update Compression







Update Compression

濍 Fraunhofer

Heinrich Hertz Institute

Algorithm	Test accuracy	Data/epoch	Time per batch		
SGD	94.3% — –	1023 MB	312 ms	+0%	
Atomo	92.6% H	113 MB	948 ms	+204%	
Signum	93.6% — H —	32 MB	301 ms	-3%	
Rank 2	94.4% ——н	8 MB	239 ms	-23%	

- Pros: "Straight forward" Convergence Analysis (Stochastic Gradients, increased variance)
- Cons: Variance blow-up leads to poor empirical performance



Biased Compression

🚿 Fraunhofer

Definition: A compression operator $\operatorname{comp} : \mathbb{R}^d \to \mathbb{R}^d$ is called **biased** iff,

$$E[\operatorname{comp}(x)] \neq x \quad \forall x \in \mathbb{R}^d$$

Biased compression methods do not necessarily converge!

 \rightarrow Can be turned into convergent methods via error accumulation.

Karimireddy, et al. "Error feedback fixes signsgd and other gradient compression schemes."

Stich, Cordonnier, Jaggi. "Sparsified SGD with memory."



Error Accumulation

Distributed SGD:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:



Distributed SGD with

Error Accumulation:

For t=1,..,[Communication Rounds]:

For i=1,..,[Participating Clients]:





Federated Learning - Recap Compression

	Unbiased	Biased
Methods	TernGrad, QSGD, Atomo	Gradient Dropping, Deep Gradient Compression, signSGD, PowerSGD,
Convergence Proofs	Bounded Variance Assumption	k-contraction Framework (Stich et al. 2018)





Combination of Methods: Sparse Binary Compression

Total Communication = [#Communication Rounds] x [#Parameters] x [#Avg. Codeword length]



[Sattler et al. 2019]

Heinrich Hertz Institute

濍 Fraunhofer



Combination of Methods: Sparse Binary Compression

Comm.
delay:
$$\Delta \mathcal{W}_i = \text{SGD}_n(\mathcal{W}_i, D_i) - \mathcal{W}_i = [1, -2, 4, 2, 1, -1]^T$$
Sparsify &
binarize: $v^+ = \text{top}_{k\%}(\Delta \mathcal{W}_i) = [4, 2]$ $v^- = \text{top}_{k\%}(-\Delta W) = [2, 1]$ $\mu^+ = \text{mean}(v^+) = 3$ $\mu^- = \text{mean}(v^-) = 1.5$ $\Delta \mathcal{W}_i^* = [0, 0, 3, 3, 0, 0]$ \rightarrow send 1 value, 2 positionsGolomb
encoding:Encode distances between nonzero elements (geom. distr.)
dist = [2, 0] $\bar{b}_{pos} = \mathbf{b}^* + 1/(1-p)^{2^{b^*}}$ Residual
accum.: $R_{\tau} = R_{\tau-1} + \Delta \mathcal{W}_{\tau} - \Delta \mathcal{W}_{\tau}^* = [1, -2, 1, -1, 1, -1]^T$

Towards Communication-Efficient and Personalized Federated Learning

🜌 Fraunhofer

Heinrich Hertz Institute



Results

Compression Method \longrightarrow		Baseline	DGC ¹	FedAvg ²	SBC (1)	SBC (2)	SBC (3)
ResNet50	Accuracy	0.737	0.739	0.724	0.735	0.737	0.728
@ImageNet	Compression	$\times 1$	$\times 601$	$\times 1000$	×2569	×3531	×37208
ResNet18	Accuracy	0.946	0.9383	0.9279	0.9422	0.9435	0.9219
@CIFAR10	Compression	imes1	$\times 768$	$\times 1000$	×2369	×3491	×31664





SBC Challenges

Heterogeneous Data
 → No communication delay



• Bi-directional Communication

 \rightarrow Upstream and Downstream compression

$$\underbrace{\tilde{\text{Global Update:}}}_{\tilde{\Delta \theta}^{(t+1)} = \operatorname{sparse}_{k} \left(\frac{1}{n} \sum_{i=1}^{n} \underbrace{\operatorname{sparse}_{k} \left(\Delta \theta_{i}^{(t+1)} + \mathcal{R}_{i}^{(t)} \right)}_{\tilde{\Delta \theta}_{i}^{(t+1)}} + \mathcal{R}^{(t)} \right) \\
= \operatorname{Partial Participation}_{\theta^{t} \xrightarrow{\tilde{\Delta \theta}^{t+1}} \cdots \xrightarrow{\tilde{\Delta \theta}^{T-1}} \theta^{T}} \underbrace{\text{Update Cache:}}_{P(\tau)} = \left\{ \sum_{t=1}^{s} \Delta \tilde{\theta}^{(T-t)} | s = 1, ..., \tau \right\}$$

 \rightarrow Update Caching

🖉 Fraunhofer

Heinrich Hertz Institute



Non-IID Settings



[Sattler et al. 2020]

Heinrich Hertz Institute

濍 Fraunhofer



Communication-Efficient Federated Distillation

Federated Averaging vs. Federated Distillation



Towards Communication-Efficient and Personalized Federated Learning

Fraunhofer

Heinrich Hertz Institute



Reducing Communication Overhead in FD

$$\mathbf{b}_{total} = |X^{pub}| imes \dim(\mathcal{Y}) imes 32$$
 bit

(a) reducing the size of the distillation data set,(b) reducing the entropy of the soft-labels, or(c) improving the efficiency of the coding technique.



💹 Fraunhofei



Compressed Federated Distillation



Distillation Dataset Size Soft-Label Quantization

$$q = \mathcal{Q}_b(p) = \arg \min_{\substack{q_i \in \{\frac{l}{2^b - 1}, l \in 0, \dots, 2^b - 1\} \\ \sum_i q_i = 1}} \|q - p\|_1$$

$$\mathcal{Q}_1(p)_i = \begin{cases} 1 & \text{if } i = \arg \max(p) \\ 0 & \text{else} \end{cases}$$

 $\begin{aligned} & \textit{Delta Coding} \\ & (\hat{Y}^t)_l = \begin{cases} (\tilde{Y}^t)_l & \text{if } (\tilde{Y}^t)_l \neq (\tilde{Y}^{t-1})_l \\ 0 & \text{else} \end{cases} \end{aligned}$

Fraunhofer Heinrich Hertz Institute



Results

Model	Target Accuracy	α	Up/Down	FA	FD	CFD-1-32	CFD_{Δ} -1-32	CFD-1-1	CFD_{Δ} -1-1
ResNet-18	0.71	100.0	up	760.35 (17)	44.80 (14)	0.56 (17)	0.40 (17)	1.36 (41)	0.82 (41)
	0.68	1.0	up	1028.71 (23)	44.80 (14) 48.00 (15)	0.37 (13)	0.28 (13)	0.64(22)	0.43 (22)
	0.45		down	1028.71 (23)	48.00 (15)	41.60 (13)	41.60 (13)	0.72 (22)	0.34 (22)
	0.45	0.1	up down	1520.70 (34) 1520.70 (34)	16.00(5) 16.00(5)	0.09 (7) 22.40 (7)	0.08 (7) 22.40 (7)	0.52 (41) 0.99 (41)	0.40 (41) 0.92 (41)
VGG-16	0.8	100.0	up	671.16 (11)	32.00 (10)	0.40 (12)	0.29 (12)	0.76 (23)	0.47 (23)
	0.50	1.0	down	671.16 (11)	32.00 (10)	38.40 (12)	38.40 (12)	0.76 (23)	0.24 (23)
	0.78	1.0	up down	1281.30 (21) 1281.30 (21)	28.80 (9) 28.80 (9)	0.38 (13) 41.60 (13)	0.28 (13) 41.60 (13)	0.56 (19) 0.62 (19)	0.37 (19) 0.27 (19)
	0.48	0.1	up	2928.69 (48)	25.60 (8)	0.11 (9)	0.09 (9)	0.43 (34)	0.35 (34)
			down	2928.69 (48)	25.60 (8)	28.80 (9)	28.80 (9)	0.77 (34)	0.75 (34)
AlexNet	0.68	100.0	up	n.a.	89.60 (28)	0.94 (29)	0.74 (29)	n.a.	n.a.
			down	n.a.	89.60 (28)	92.80 (29)	92.80 (29)	n.a.	n.a.
	0.64	1.0	up	n.a.	38.40 (12)	0.61 (21)	0.49 (21)	0.76 (26)	0.62 (26)
			down	n.a.	38.40 (12)	67.20 (21)	67.20 (21)	0.84 (26)	0.42 (26)
	0.44	0.1	up down	n.a. n.a.	6.40 (2) 6.40 (2)	0.09 (6) 19.20 (6)	0.08 (6) 19.20 (6)	0.11 (7) 0.17 (7)	0.10 (7) 0.15 (7)

[Sattler et al. 2021]





Personalization in FL

aunhofo

Federated Learning Environments are characterized by a **high degree of statistical heterogeneity** of the client data

 \rightarrow In many situations, learning one single central model is suboptimal or even undesirable



Federated Learning - Personalization

濍 Fraunhofer







Federated Learning - Personalization



A single classifier can not correctly separate the data all clients.

<u>Solution</u>: Use separate model for each cluster

How to identify these clusters ?





Diverging Preferences

濍 Fraunhofer

Heinrich Hertz Institute

 \rightarrow Only k=2 clusters, no intra-cluster variance Assume: $r_i(\theta) \in \{g(\theta), h(\theta)\}$ • local empirical risk <u>Federated Learning Objective:</u> $F(\theta) := \sum_{i=1}^{n} \frac{|D_i|}{|D|} r_i(\theta) = c_1 g(\theta) + (1 - c_1) h(\theta)$ At every stationary solution of the FL objective it holds: $0 = \nabla F(\theta^*) = c_1 \nabla q(\theta^*) + (1 - c_1) \nabla h(\theta^*)$ Same preferences **Divergent** preferences $\nabla g(\theta^*) = -\frac{1-c_1}{c_1} \nabla h(\theta^*)$ $\Rightarrow \alpha_{i,j} := \cos(\nabla r_i(\theta^*), \nabla r_j(\theta^*)) = \frac{\langle \nabla r_i(\theta^*), \nabla r_j(\theta^*) \rangle}{\|\nabla r_i(\theta^*)\| \|\nabla r_j(\theta^*)\|}$ $0 = \nabla q(\theta^*) = \nabla h(\theta^*)$ $= \begin{cases} 1 & I(i) = I(j) \\ -1 & I(i) \neq I(j) \end{cases}$



Cosine Similarity between Gradients

Fraunhofer

Heinrich Hertz Institute





Separation Theorem

濍 Fraunhofer

Heinrich Hertz Institute



[Sattler et al. 2020]



Clustered Federated Learning







Clustered Federated Learning



		Byzantine	Noisy	Label-Flip	Clean
MNIST	FL	9.8%	96.9%	91.3%	97.5
	CFL (ours)	93.19%	97.4%	97.4%	97.4%
Fashion-	FL	9.6%	77.12%	60.6%	79.9
MNIST	CFL (ours)	78.0%	79.7%	79.7%	80.2
CIFAR	FL	10.0%	70.4%	40.1	76.0
	CFL (ours)	61.7%	74.6%	74.7%	75.3%

Byzantine Setting: A subset of clients behaves unpredictably or tries to disturb the joint training effort in an directed or undirected way

[Sattler et al. 2020]

濍 Fraunhofer





New MPEG Standard

MPEG NNC Standard

Fraunhofer



Standard on "Compression of Neural Networks for Multimedia Content Description and Analysis"





MPEG NNC Standard

ISO/IEC 15938-17 (MPEG-7 Part 17) – NNC (Compression of neural networks for multimedia content description and analysis)

NNC is developed as a toolbox

- Inclusion in external neural network formats and frameworks, such as PyTorch, TensorFlow, ONNX or NNEF

- Independent coding method of neural networks (compression of weights, biases, etc. per parameter tensor plus inclusion of format-specific topology)

Compression efficiency of 95% without degrading classification quality, e.g. top-1.





MPEG NNC Standard

Fraunhofer

Heinrich Hertz Institute





MPEG: Incremental Compression of NN

Call for Proposals on ICNN issued

Responses by April 2021

raunhofer

Aim: Technology for the compressed, interpretable and interoperable representation of updates of trained neural networks

Target: Use cases on **federated learning** with solution categories on:

- Network updates after refining/adding more training data, e.g. in federated learning
- Network updates after transfer learning/adapting to specific data (with and without network structure changes
- Network updates with higher precision/less compression



Conclusion

aunhofe

Federated Learning is a powerful training schemes (e.g., privacypreserving, distributed data, ideal for communications applications).

Clustered Federated Learning allows to apply FL in realistic scenarios, where clients have diverging preferences.

Many challenges still exist (complexity, robustness to adversaries etc.)

CFL provides robustness in Byzantine settings, where standard FL fails.

New MPEG standard for FL / NN update compression.





Federated Learning

🖉 Fraunhofer

Heinrich Hertz Institute

- L Witt, U Zafar, K Shen, F Sattler, D Li, W Samek. <u>Reward-Based 1-bit Compressed Federated Distillation on Blockchain</u> arXiv:2106.14265, 2021 [bibtex] [preprint]
- F Sattler, T Korjakow, R Rischke, W Samek. <u>FedAUX: Leveraging Unlabeled Auxiliary Data in Federated Learning</u> IEEE Transactions on Neural Networks and Learning Systems, 2021 [bibtex] [preprint]
- F Sattler, A Marban, R Rischke, W Samek. <u>CFD: Communication-Efficient Federated Distillation via Soft-Label Quantization and Delta</u> <u>Coding</u> IEEE Transactions on Network Science and Engineering, 2021 [bibtex] [preprint]
- F Sattler, T Wiegand, W Samek. <u>Trends and Advancements in Deep Neural Network Communication</u> ITU Journal: ICT Discoveries, 3(1), 2020 [bibtex] [preprint]
- F Sattler, KR Müller, W Samek. <u>Clustered Federated Learning: Model-Agnostic Distributed Multi-Task Optimization under Privacy</u> <u>Constraints</u> IEEE Transactions on Neural Networks and Learning Systems, 32(8):3710-3722, 2021 [bibtex] [preprint] [supplement]



- F Sattler, S Wiedemann, KR Müller, W Samek. <u>Robust and Communication-Efficient Federated Learning from Non-IID Data</u> IEEE Transactions on Neural Networks and Learning Systems, 31(9):3400-3413, 2020 [bibtex] [preprint]
- D Neumann, F Sattler, H Kirchhoffer, S Wiedemann, K Müller, H Schwarz, T Wiegand, D Marpe, and W Samek. <u>DeepCABAC:</u> <u>Plug&Play Compression of Neural Network Weights and Weight Updates</u> Proceedings of the IEEE International Conference on Image Processing (ICIP), 21-25, 2020 [bibtex] [preprint]
- F Sattler, KR Müller, W Samek. <u>Clustered Federated Learning</u> Proceedings of the NeurIPS'19 Workshop on Federated Learning for Data Privacy and Confidentiality, 1-5, 2019 [bibtex] [preprint]
- F Sattler, KR Müller, T Wiegand, W Samek. <u>On the Byzantine Robustness of Clustered Federated Learning</u> Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 8861-8865, 2020 [bibtex] [preprint]
- F Sattler, S Wiedemann, KR Müller, W Samek. <u>Sparse Binary Compression: Towards Distributed Deep Learning with minimal Communication</u> Proceedings of the IEEE International Joint Conference on Neural Networks (IJCNN), 1-8, 2019
 [bibtex] [preprint]



NN Compression

🚿 Fraunhofer

Heinrich Hertz Institute

- H Kirchhoffer, P Haase, W Samek, K Müller, H Rezazadegan-Tavakoli, F Cricri, E Aksu, MM Hannuksela, W Jiang, W Wang, S Liu, S Jain, S Hamidi-Rad, F Racapé, W Bailer. <u>Overview of the Neural Network Compression and Representation (NNR) Standard</u> IEEE Transactions on Circuits and Systems for Video Technology, 2021 [bibtex] [preprint]
- P Haase, D Becking, H Kirchhoffer, K Müller, H Schwarz, W Samek, D Marpe, T Wiegand. <u>Encoder Optimizations for the NNR Standard</u> <u>on Neural Network Compression</u> Proceedings of the IEEE International Conference on Image Processing (ICIP), 2021 [<u>bibtex</u>] [preprint]
- S Wiedemann, S Shivapakashy, P Wiedemanny, D Becking, W Samek, F Gerfers, T Wiegand. <u>FantastIC4: A Hardware-Software Co-Design Approach for Efficiently Running 4bit-Compact Multilayer Perceptrons</u> IEEE Open Journal of Circuits and Systems, 2:407-419, 2021 [bibtex] [preprint]
- S Yeom, P Seegerer, S Lapuschkin, A Binder, S Wiedemann, KR Müller, W Samek. <u>Pruning by Explaining: A Novel Criterion for Deep</u> <u>Neural Network Pruning</u> Pattern Recognition, 115:107899, 2021 [bibtex] [preprint]
- K Müller, W Samek, D Marpe. <u>Ein internationaler KI-Standard zur Kompression Neuronaler Netze</u> FKT- Fachzeitschrift für Fernsehen, Film und Elektronische Medien, 33-36, 2021 [bibtex] [preprint]





- S Wiedemann, H Kirchhoffer, S Matlage, P Haase, A Marban, T Marinc, D Neumann, T Nguyen, A Osman, H Schwarz, D Marpe, T Wiegand, W Samek. <u>DeepCABAC: A Universal Compression Algorithm for Deep Neural Networks</u> IEEE Journal of Selected Topics in Signal Processing, 14(4):700-714, 2020
 [bibtex] [preprint] [code]
- S Wiedemann, KR Müller, W Samek. <u>Compact and Computationally Efficient Representation of Deep Neural Networks</u> IEEE Transactions on Neural Networks and Learning Systems, 31(3):772-785, 2020 [bibtex] [preprint]
- S Wiedemann, T Mehari, K Kepp, W Samek. <u>Dithered backprop: A sparse and quantized backpropagation algorithm for more efficient</u> <u>deep neural network training</u> Proceedings of the CVPR'20 Joint Workshop on Efficient Deep Learning in Computer Vision, 3096-3104, 2020 [bibtex] [preprint]
- A Marban, D Becking, S Wiedemann, W Samek. <u>Learning Sparse & Ternary Neural Networks with Entropy-Constrained Trained</u> <u>Ternarization (EC2T)</u> Proceedings of the CVPR'20 Joint Workshop on Efficient Deep Learning in Computer Vision, 3105-3113, 2020 [bibtex] [preprint]
- S Wiedemann, H Kirchhoffer, S Matlage, P Haase, A Marban, T Marinc, D Neumann, T Nguyen, A Osman, H Schwarz, D Marpe, T Wiegand, W Samek. <u>DeepCABAC: A Universal Compression Algorithm for Deep Neural Networks</u> IEEE Journal of Selected Topics in Signal Processing, 14(4):700-714, 2020
 [bibtex] [preprint] [code]





- P Haase, H Schwarz, H Kirchhoffer, S Wiedemann, T Marinc, A Marban, K Müller, W Samek, D Marpe, T Wiegand. <u>Dependent Scalar</u> <u>Quantization for Neural Network Compression</u> Proceedings of the IEEE International Conference on Image Processing (ICIP), 36-40, 2020 [bibtex] [preprint]
- S Wiedemann, A Marban, KR Müller, W Samek. <u>Entropy-Constrained Training of Deep Neural Networks</u> Proceedings of the IEEE International Joint Conference on Neural Networks (IJCNN), 1-8, 2019 [bibtex] [preprint]
- S Wiedemann, KR Müller, W Samek. <u>Compact and Computationally Efficient Representation of Deep Neural Networks</u> NIPS Workshop on Compact Deep Neural Network Representation with Industrial Applications (CDNNRIA), 1-8, 2018 [bibtex] [preprint]





Thank you for your attention!



Papers

Slides

Software