Weight Erosion: A novel personalized FL method

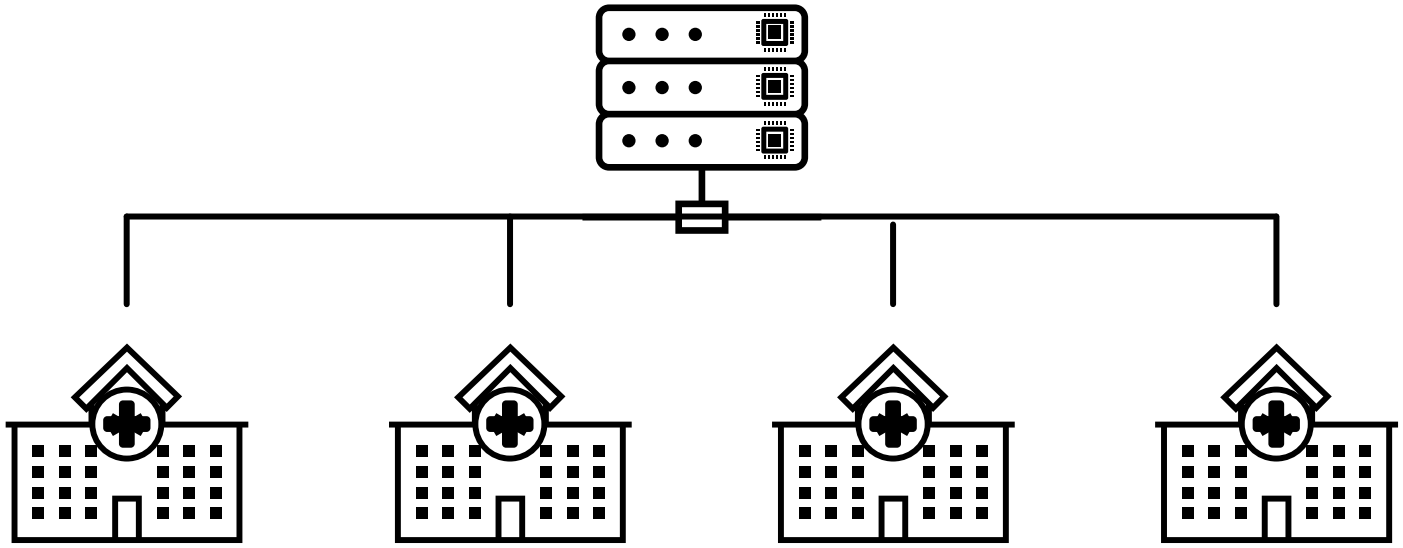
Felix Grimberg, CSE master student

Supervisors: Mary-Anne Hartley, Martin Jaggi, Sai Karimireddy, Andres Colubri

---

June 19th, 2020

Federated Learning & personalization



- Data can’t be shared (private)
- IID?
- Individual data sets too small

- Local fine-tuning, MAML
- Featurization
- Multi-task learning

My contribution

Theory

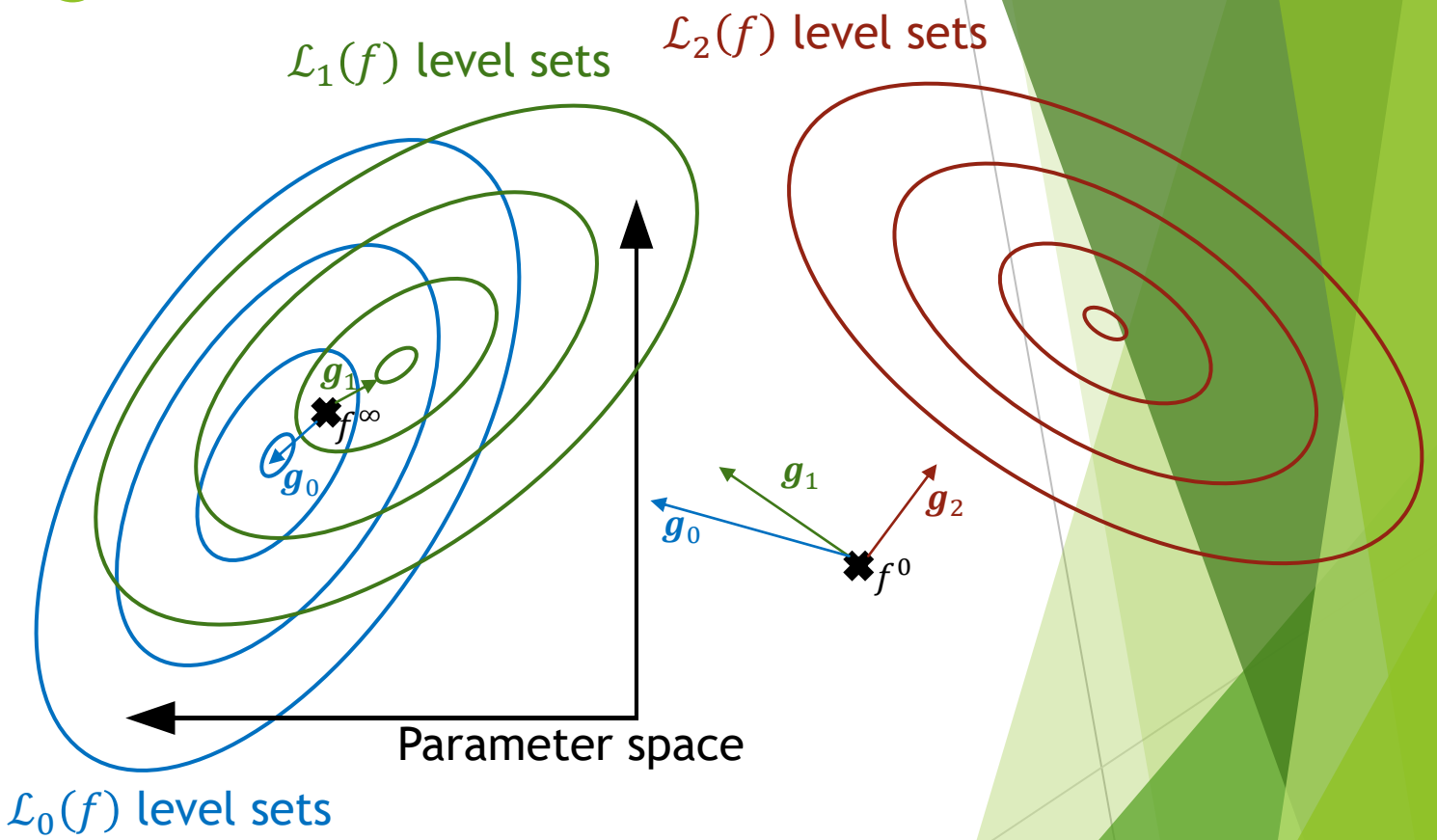
- Adapted Ndoye factor
  - Rank agents *before* training
- Weight Erosion

Application

- Medical data set
- Titanic data set

Weight Erosion aggregation scheme

- Based on distances between gradients
  - He et al., 2020: Compute them securely with MPC, then pick byzantine-robust subset
- Intuition:
  - $\mathcal{D}_0 \approx \mathcal{D}_1 \Rightarrow \boldsymbol{g}_0 \approx \boldsymbol{g}_1$
- Distance depends on
  - minibatch
  - how well the model is already performing



$$\alpha_i^0 = 1$$

$$\alpha_i^r = \alpha_i^{r-1} - \Delta\alpha_i^{r-1} \qquad \Delta\alpha_i^{r-1} \propto \frac{\|\boldsymbol{g}_0 - \boldsymbol{g}_i\|}{\|\boldsymbol{g}_0\|}$$

Application to medical data set

- Ebola data set, 577 patients in 2014 – 2015 (Hartley et al., 2017)
- Classification: predict diagnosis EVD(+) vs. EVD(-)
  - Using features identified in Hartley et al., 2017
  - 1 layer, Log-softmax activation, cross-entropy loss
- Splitting the data set by age:
  - AGE_STRICT: agent 0: 0 – 20 yo / agent 1: 21 – 40 yo / agent 2: 41+ yo
  - AGE_SOME: agents 0 & 1: 0 – 40 yo / agent 2: 41+ yo

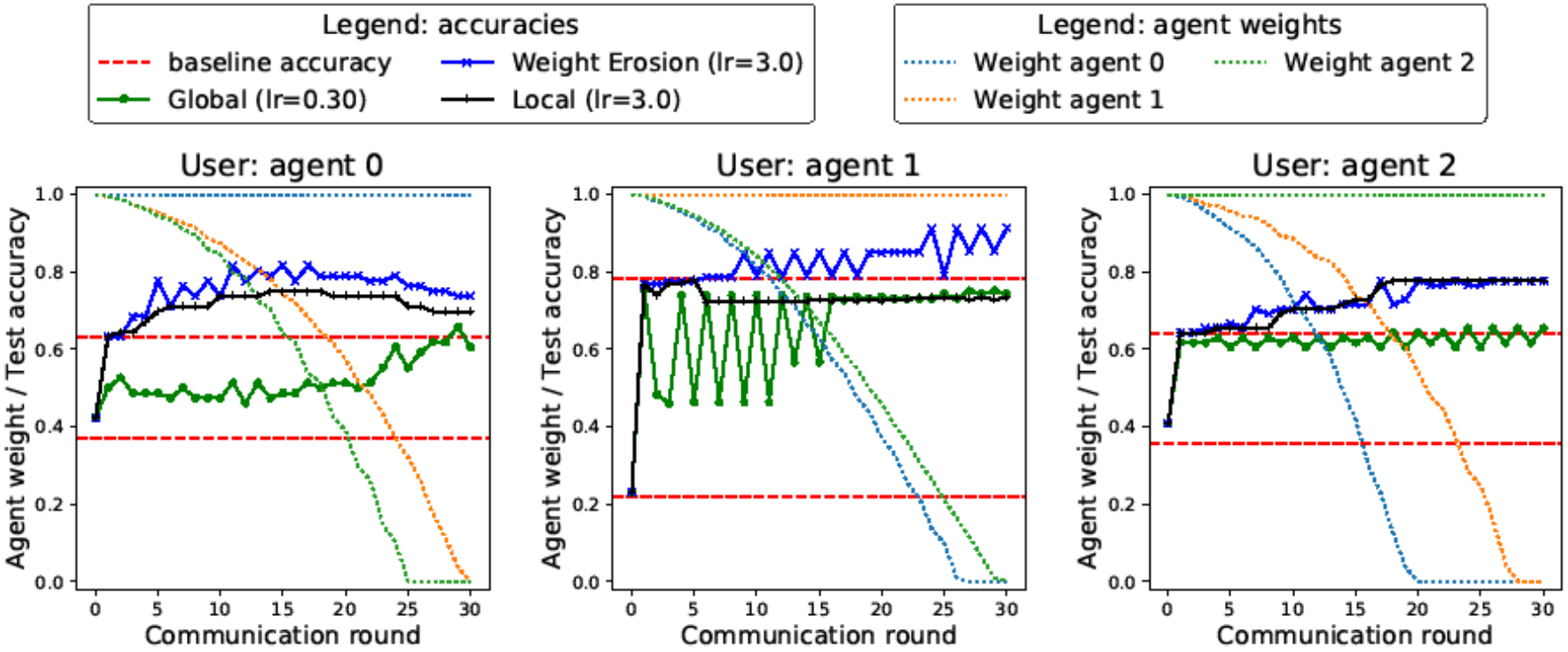


Figure 1: Predicting Ebola infection with AGE_STRICT split.

Full lines: model's accuracy on the user's test set.
Red (dashed): baseline test accuracy (always EVD(+) or always EVD(-)).
Pointed lines: weight of each agent in the Weight Erosion scheme.

The learning rates are displayed in the legend. Each agent's data set contains two batches of 125 samples each.

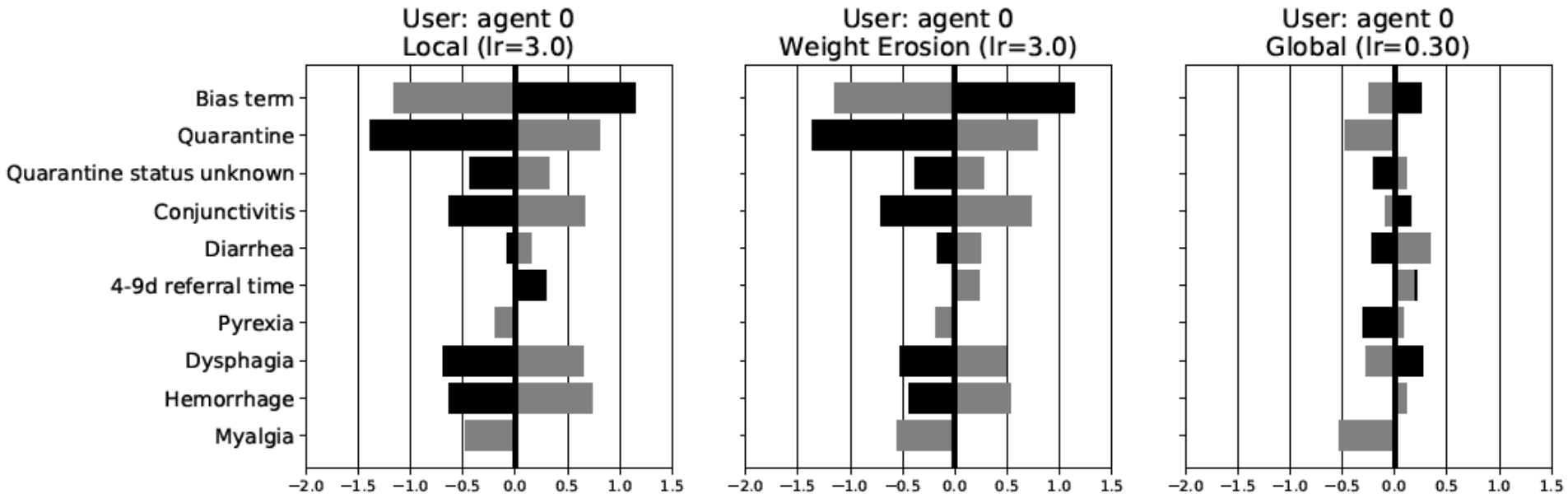


Figure 3: Parameters of the models in Figure 1 (left).

Weight for the 1st output of the linear regression layer.

Weight for the 2nd output of the linear regression layer.

Strong correlation with EVD(-)

Strong correlation with EVD(+)

References

- Hartley et al., 2017:
  - Mary-Anne Hartley et al. “Predicting Ebola infection: A malaria-sensitive triage score for Ebola virus disease”. In: *PLoS neglected tropical diseases* 11.2 (2017).
- Ndoye factor:
  - Mohamed Ndoye et al. “Collaborative privacy”. *Semester project* (2020). url: https://www.mndoye.com/collaborativeprivacy.pdf.
- He et al., 2020:
  - Lie He, Sai Praneeth Karimireddy, and Martin Jaggi. \Secure Byzantine-Robust Machine Learning". In: *arXiv:2006.04747* [cs, stat] (June 8, 2020). url: http://arxiv.org/abs/2006.04747 (visited on 06/16/2020).