# On Distributed Methods for Variational Inequalities and Beyond 

Aleksandr Beznosikov

MIPT
17 January 2024

## Variational Inequality

## Definition (Stampacchia VIs)

Find $z^{*} \in \mathcal{Z}$ such that $\left\langle F\left(z^{*}\right), z-z^{*}\right\rangle+g(z)-g\left(z^{*}\right) \geq 0, \forall z \in \mathcal{Z}$, where $F: \mathbb{R}^{d} \rightarrow \mathbb{R}^{d}$ is some operator and $g$ is a proper convex lower semicontinuous function.

## Definition (Minty VIs)

Find $z^{*} \in \mathcal{Z}$ such that $\left\langle F(z), z-z^{*}\right\rangle+g(z)-g\left(z^{*}\right) \geq 0, \forall z \in \mathcal{Z}$, where $F: \mathbb{R}^{d} \rightarrow \mathbb{R}^{d}$ is some operator and $g$ is a proper convex lower semicontinuous function.

## Variational Inequality: facts

- Two formulations are equivariant for smooth monotone operators.
- In the case when $g \equiv 0$ and $\mathcal{Z}=\mathbb{R}^{d}$, then VI is equal to

Find $z^{*} \in \mathcal{Z}$ such that $F(z)=0$.

## Variational Inequality: examples

- Minimization:

$$
\min _{z \in \mathbb{R}^{d}} f(z)
$$

We take $F(z) \stackrel{\text { def }}{=} \nabla f(z)$.

- Saddle point problem:

$$
\min _{x \in \mathbb{R}^{d_{x}}} \min _{y \in \mathbb{R}^{d_{y}}} g(x, y)
$$

Here $F(z) \stackrel{\text { def }}{=} F(x, y)=\left[\nabla_{x} g(x, y),-\nabla_{y} g(x, y)\right]$.

- Fixed point problem:

Find $z^{*} \in \mathbb{R}^{d}$ such that $T\left(z^{*}\right)=z^{*}$,
where $T: \mathbb{R}^{d} \rightarrow \mathbb{R}^{d}$ is an operator. We take $F(z)=z-T(z)$.

## Variational Inequality: classical examples

- Game theory and economy (comes from von Neumann). Simple example - matrix game (bilinear sadddle point problem on simplexes):

$$
\min _{x \in \Delta^{d_{x}}} \max _{y \in \Delta^{d_{y}}} x^{T} A y
$$

where $A$ - cost matrix, х и $y$ - probability of actions.

- Constrained optimization and Lagrange multipliers.


## Variational Inequality: ML example

- From classical minimization problem:

$$
\min _{z \in \mathbb{R}^{d}} \frac{1}{n} \sum_{i=1}^{n} l\left(f\left(x_{i}, z\right), y_{i}\right)
$$

where $\left\{x_{i}, y_{i}\right\}_{i=1}^{n}$ - data, $f$ - model $z, l$ - loss.

- To robust formulation via saddle point problem:

$$
\min _{z \in \mathbb{R}^{d}} \max _{\left\|\delta_{i}\right\| \leq e} \frac{1}{n} \sum_{i=1}^{n} I\left(f\left(x_{i}+\delta_{i}, z\right), y_{i}\right)
$$

where $\delta_{i}$ - adversarial noise.

## Variational Inequality: GANs

- GAN represents two models generator $G$ and discriminator $D$.
- $D$ takes an element $x$ as input and determines whether this element is real (from a data sample) or artificially generated by the generator.
- The generator is given some random vector $z$ as input, from which the generator constructs a "fake" instance similar to the real sample.
- Formally, the GAN training problem is formulated as a saddle point problem:

$$
\min _{G} \max _{D} V(D, G)=\mathbb{E}_{\boldsymbol{x} \sim p_{\text {data }}(\boldsymbol{x})}[\log D(\boldsymbol{x})]+\mathbb{E}_{\mathbf{z} \sim p_{\mathbf{z}}(\boldsymbol{z})}[\log (1-D(G(\boldsymbol{z})))]
$$

## Variational Inequality: method

- We know what to do with:

$$
\min _{z \in \mathbb{R}^{d}} f(z)
$$

Gradient descent:

$$
z^{k+1}=z^{k}-\gamma \nabla f\left(z^{k}\right)
$$

- What to do with VIs and saddle point problems? The same idea -descent-ascent:

$$
z^{k+1}=z^{k}-\gamma F\left(z^{k}\right)
$$

## Variational Inequality: method

- The idea of descent-ascent isn't bad and often works, but physical intuition tells that it has some not-so-pleasant aspects.


## Variational Inequality: method

- The idea of descent-ascent isn't bad and often works, but physical intuition tells that it has some not-so-pleasant aspects.
- Consider $\min _{x \in R} \max _{y \in \mathbb{R}} x y$. With starting point $(1,1)$. Where is the solution? Point $(0,0)$.
- Vector: $\binom{\nabla_{x} g\left(x^{k}, y^{k}\right)}{-\nabla_{y} g\left(x^{k}, y^{k}\right)}$ is always orthogonal to $\binom{x^{k}-x^{*}}{y^{k}-y^{*}}$. What does it means? Method diverges.
- Intuition is not strict, but it can tell us to try something a little different.


## Variational Inequality: Extragradient method

```
Algorithm Extragradient method
Вход: stepsize \(\gamma>0\), staring \(z^{0} \in \mathbb{R}^{d}\), number of iterations \(K\)
    1: for \(k=0,1, \ldots, K-1\) do
    2: \(\quad z^{k+1 / 2}=z^{k}-\gamma F\left(z^{k}\right)\)
    3: \(\quad z^{k+1}=z^{k}-\gamma F\left(z^{k+1 / 2}\right)\)
    4: end for
```

It is easy to check that for this method on the problem $\min _{x \in R} \max _{y \in R} x y$, the directions of the final step in the scalar product with the direction to the solution gives a number greater than 0 , hence an acute angle.

## Contemporary challenges

- Exponential growth in model sizes and data volumes.


Figure: Dynamics of growth of modern language models


Figure: Dynamics of dataset growth

## Varieties of distributed learning

- Cluster learning (large players): we train within one large and powerful computing cluster
- Collaborative learning (all players): pooling computing resources over the Internet
- Federated learning (another paradigm): learn on users' local data using their computational power


Figure: Federated learning

## The most popular distributed setup

- Formulation (horizontal):

$$
F(z):=\frac{1}{M} \sum_{m=1}^{M} F_{m}(z):=\frac{1}{M} \sum_{m=1}^{M} \mathbb{E}_{\xi \sim \mathcal{D}_{m}}\left[F_{m}(z, \xi)\right]
$$

- The problem is shared among $M$ computing devices, each device $m$ has access only to its own operator $F_{m}$ or its stochastic realization.


## Communication setups



Figure: Centralized and decentralized connections

## Communicating through the server

- Let us look at an example of how Extragradient becomes centralized.


## Algorithm Centralized Extragradient

Вход: Stepsize $\gamma>0$, starting point $z_{0} \in \mathbb{R}^{d}$, number of iterations $K$
1: for $k=0,1, \ldots, K-1$ do
2: Send $z^{k}$ to all workers $\quad \triangleright$ by server
3: for $m=1, \ldots, M$ in parallel do
4: $\quad$ Recieve $z^{k}$ from server
$\triangleright$ by workers
Compute $F_{m}\left(z^{k}\right)$ in $z^{k} \quad \triangleright$ by workers
Send $F_{m}\left(z^{k}\right)$ to server
$\triangleright$ by workers
7: end for
8: Recieve $F_{m}\left(z^{k}\right)$ from all workers $\quad \triangleright$ by server
9: Compute $F\left(z^{k}\right)=\frac{1}{M} \sum_{m=1}^{M} F_{m}\left(z^{k}\right)$
$\triangleright$ by server
10: $\quad z^{k+1 / 2}=z^{k}-\gamma F\left(z^{k}\right)$
$\triangleright$ by server
11: $\quad$ Similarly for $z^{k+1}$
12: end for

- In the decentralized setting, it does not work, there is no server.


## Assumptions

- Assumption 1. $F_{m}$ is Lipschitz with constant $L$, i.e. for all $z_{1}, z_{2} \in \mathcal{Z}$

$$
\left\|F_{m}\left(z_{1}\right)-F_{m}\left(z_{2}\right)\right\| \leq L\left\|z_{1}-z_{2}\right\| .
$$

(smoothness)

- Assumption 2. $F_{m}$ is strongly monotone with constant $\mu$, i.e. for all $z_{1}, z_{2} \in \mathcal{Z}$

$$
\left\langle F_{m}\left(z_{1}\right)-F_{m}\left(z_{2}\right), z_{1}-z_{2}\right\rangle \geq \mu\left\|z_{1}-z_{2}\right\|^{2}
$$

(strong convexity and strong-convexity-strong-concavity)

- Assumption 3. (for decentralized setting) $F_{m}$ is stored locally on its own device. All devices are connected in a network (undirected may be time-varying graph $G_{k}\left(\mathcal{V}_{k}, \mathcal{E}_{k}\right)$ with max diameter $\Delta$ and max condition number $\chi$ of Laplace matrix).


## Plan

- Deterministic case
- Stochastic: bounded variance
- Stochastic: finite sum
- Compression
- Similarity
- Similarity + compression


## Deterministic case

- We can compute full $F_{m}$ on each device:

$$
F(z):=\frac{1}{M} \sum_{m=1}^{M} F_{m}(z)
$$

## Lower bounds

Lower bounds for distributed algorithms with $K$ communications.

## centralized

| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{32 \mu K}{L}\right)\right)$ |
| :---: | :---: |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L}}\right)\right)$ |
| decentralized (fixed network) |  |
| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L \sqrt{\chi}}\right)\right)$ |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L} \sqrt{\chi}}\right)\right)$ |
| decentralized (time-varying network) |  |
| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L \chi}\right)\right)$ |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L} \chi}\right)\right)$ |

Table: Lower bounds for distributed VI s,

## Lower bounds

- No "problem" acceleration (unlike minimization) since VIs is a broader class of problems
- No "network" acceleration in the time-varying setting


## Lower bounds: idea

- Problem:

$$
f_{m}(x, y)= \begin{cases}f_{1}(x, y)=\frac{M}{2\left|B_{d}\right|} \cdot \frac{L}{2} x^{T} A_{1} y+\frac{\mu}{2}\|x\|^{2}-\frac{\mu}{2}\|y\|^{2}+\frac{M}{2\left|B_{d}\right|} \cdot \frac{L^{2}}{2 \mu} e_{1}^{T} y, & m \in B_{d} \\ f_{2}(x, y)=\frac{M}{2|B|} \cdot \frac{L}{2} x^{T} A_{2} y+\frac{\mu}{2}\|x\|^{2}-\frac{\mu}{2}\|y\|^{2}, & m \in B \\ f_{3}(x, y)=\frac{\mu}{2}\|x\|^{2}-\frac{\mu}{2}\|y\|^{2}, & \text { otherwise }\end{cases}
$$

where $e_{1}=(1,0 \ldots, 0)$ and

$$
A_{1}=\left(\begin{array}{cccccccc}
1 & 0 & & & & & & \\
& 1 & -2 & & & & & \\
& & 1 & 0 & & & & \\
& & & 1 & -2 & & & \\
& & & & \cdots & \cdots & & \\
& & & & & 1 & -2 & \\
& & & & & & 1 & 0 \\
& & & & & & & 1
\end{array}\right), A_{2}=\text { analogically }
$$

- Network - chain


## Optimal algorithms

- In the centralized case, just Centralized Extragradient
- In the decentralized case, we can simulate server communication via gossip procedures.


## Algorithm FastMix

Parameters: Vectors $z_{1}, \ldots, z_{M}$, communic. rounds $P$.
Initialization: Construct matrix $\mathbf{z}$ with rows $z_{1}^{T}, \ldots, z_{M}^{T}$,
choose $\mathbf{z}^{-1}=\mathbf{z}, \mathbf{z}^{0}=\mathbf{z}, \eta=\frac{1-\sqrt{1-\lambda_{2}^{2}(\tilde{W})}}{1+\sqrt{1-\lambda_{2}^{2}(\tilde{W})}}$.
for $h=0,1,2, \ldots, P-1$ do

$$
\mathbf{z}^{h+1}=(1+\eta) \tilde{W} \mathbf{z}^{h}-\eta \mathbf{z}^{h-1}
$$

end for
Output: rows $z_{1}, \ldots, z_{M}$ of $z^{P}$.

## Stochastic setting: bounded variance

- We can compute only stochastic realizations $F_{m}(z, \xi)$ for each device:

$$
F(z):=\frac{1}{M} \sum_{m=1}^{M} F_{m}(z)=\frac{1}{M} \sum_{m=1}^{M} \mathbb{E}_{\xi \sim \mathcal{D}_{m}}\left[F_{m}(z, \xi)\right]
$$

- Assumption. $F_{m}(z, \xi)$ is unbiased and has bounded variance, i.e. for all $z \in \mathcal{Z}$

$$
\mathbb{E}\left[F_{m}(z, \xi)\right]=F_{m}(z), \mathbb{E}\left[\left\|F_{m}(z, \xi)-F_{m}(z)\right\|^{2}\right] \leq \sigma^{2}
$$

## Lower bounds

Lower bounds for distributed algorithms with $K$ communications and $T$ local computations $(T>K)$.
centralized

| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{32 \mu K}{L}\right)+\frac{\sigma^{2}}{\mu^{2} M T}\right)$ |
| :---: | :--- |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L}}\right)+\frac{\sigma^{2}}{\mu^{2} M T}\right)$ | decentralized (fixed network)


| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L_{\bar{\chi}}}\right)+\frac{\sigma^{2}}{\mu^{2} M T}\right)$ |
| :---: | :--- |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L} \sqrt{\chi}}+\frac{\sigma^{2}}{\mu^{2} M T}\right)\right)$ |

decentralized (time-varying network)

| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L_{\chi}}\right)+\frac{\sigma^{2}}{\mu^{2} M T}\right)$ |
| :---: | :---: |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L}}\right)+\frac{\sigma^{2}}{\mu^{2} M \underline{\underline{\underline{I}}}}\right)$ |

## Lower bounds: idea

- Consider

$$
\min _{x \in \mathbb{R}} f(x)=\frac{\mu}{2}\left(x-x_{0}\right)^{2}
$$

where we do not know the constant $x_{0} \neq 0$.

- Using stochastic first order oracle

$$
\nabla f(x, \xi)=\mu\left(x+\xi-x_{0}\right), \text { where } \xi \in \mathcal{N}\left(0, \frac{\sigma^{2}}{\mu^{2}}\right)
$$

## Optimal algorithms: centralized

Batching as additional idea to the deterministic algorithm

```
Algorithm 1 Centralized Extra Step Method
    Parameters: Stepsize \(\gamma \leq \frac{1}{4 L}\); Communication rounds \(K\), number of local steps \(T\).
    Initialization: Choose \(\left(x^{0}, y^{0}\right)=z^{0} \in \mathcal{Z}, k=\left\lfloor\frac{K}{r}\right\rfloor\) and batch size \(b=\left\lfloor\frac{T}{2 k}\right\rfloor\).
    for \(t=0,1,2, \ldots, k\) do
        for each machine \(m\) do
        \(g_{m}^{t}=\frac{1}{b} \sum_{i=1}^{b} F_{m}\left(z^{t}, \xi_{m}^{t, i}\right)\), send \(g_{m}^{t}\),
        on server:
            \(z^{t+1 / 2}=\operatorname{proj}_{\mathcal{Z}}\left(z^{t}-\frac{\gamma}{M} \sum_{m=1}^{M} g_{m}^{t}\right)\), send \(z^{t+1 / 2}\),
        for each machine \(m\) do
        \(g_{m}^{t+1 / 2}=\frac{1}{b} \sum_{i=1}^{b} F_{m}\left(z^{t+1 / 2}, \xi_{m}^{t+1 / 2, i}\right)\), send \(g_{m}^{t+1 / 2}\),
        on server:
        \(z^{t+1}=\operatorname{proj}_{\mathcal{Z}}\left(z^{t}-\frac{\gamma}{M} \sum_{m=1}^{M} g_{m}^{t+1 / 2}\right), \quad\) send \(z^{t+1}\),
    end for
    Output: \(z^{k+1}\) or \(z_{\text {avg }}^{k+1}\).
```


## Optimal algorithms: decentralized

```
Algorithm 2 Decentralized Extra Step Method
    Parameters: Stepsize \(\gamma \leq \frac{1}{4 L}\); Communication rounds \(K\), number of local calls \(T\).
    Initialization: Choose \(\left(x^{0}, y^{0}\right)=z^{0} \in \mathcal{Z}, z_{m}^{0}=z^{0}, k=\left\lfloor\frac{K}{H}\right\rfloor\) and batch size \(b=\left\lfloor\frac{T}{2 k}\right\rfloor\).
    for \(t=0,1,2, \ldots, k\) do
        for each machine \(m\) do
        \(g_{m}^{t}=\frac{1}{b} \sum_{i=1}^{b} F_{m}\left(z_{m}^{t}, \xi_{m}^{t, i}\right), \quad \hat{z}_{m}^{t+1 / 2}=z_{m}^{t}-\gamma g_{m}^{t}\),
        communication
            \(\tilde{z}_{1}^{t+1 / 2}, \ldots, \tilde{z}_{M}^{t+1 / 2}=\operatorname{FastMix}\left(\hat{z}_{1}^{t+1 / 2}, \ldots, \hat{z}_{M}^{t+1 / 2}, H\right)\),
        for each machine \(m\) do
            \(z_{m}^{t+1 / 2}=\operatorname{proj}_{\mathcal{Z}}\left(\tilde{z}_{m}^{t+1 / 2}\right)\),
            \(g_{m}^{t+1 / 2}=\frac{1}{b} \sum_{i=1}^{b} F_{m}\left(z_{m}^{t+1 / 2}, \xi_{m}^{t+1 / 2, i}\right)\),
            \(\hat{z}_{m}^{t+1}=z_{m}^{t}-\gamma g_{m}^{t+1 / 2}\),
        communication
            \(\tilde{z}_{1}^{t+1}, \ldots, \tilde{z}_{M}^{t+1}=\operatorname{FastMix}\left(\tilde{z}_{1}^{t+1}, \ldots, \hat{z}_{M}^{t+1}, H\right)\),
        for each machine \(m\) do
            \(z_{m}^{t+1}=\operatorname{proj}_{\mathcal{Z}}\left(\tilde{z}_{m}^{t+1}\right)\),
    end for
    Output: \(\bar{z}^{k+1}\) or \(\bar{z}_{\text {avg }}^{k+1}\).
```


## Stochastic case: finite-sum

- We can compute full $F_{m}$ on each device:

$$
F(z):=\frac{1}{M} \sum_{m=1}^{M} F_{m}(z)=\frac{1}{M} \sum_{m=1}^{M} \frac{1}{n} \sum_{i=1}^{n} F_{m, i}(z)
$$

- But we don't want to do it since expensive, we compute only random part $F_{m, i}$.


## Lower bounds

Lower bounds for distributed algorithms with $K$ communications and $T$ local computations.
centralized

| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{32 \mu K}{L}\right)+R_{0}^{2} \exp \left(-\frac{16 \mu K}{\sqrt{n} L}\right)\right)$ |
| :---: | :---: |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L}}\right)+R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{n} \sqrt{L}}\right)\right)$ |
| decentralized (fixed network) |  |
| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L \sqrt{\chi}}\right)+R_{0}^{2} \exp \left(-\frac{16 \mu K}{\sqrt{n} L}\right)\right)$ |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L} \sqrt{\chi}}\right)+R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{n} \sqrt{L}}\right)\right)$ |
| decentralized (time-varying network) |  |
| VIs | $\Omega\left(R_{0}^{2} \exp \left(-\frac{128 \mu K}{L \chi}\right)+R_{0}^{2} \exp \left(-\frac{16 \mu K}{\sqrt{n} L}\right)\right)$ |
| Minimization (exists) | $\Omega\left(R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{L} \chi}\right)+R_{0}^{2} \exp \left(-\frac{\sqrt{\mu} K}{\sqrt{n} \sqrt{L} \mathrm{~L}}\right)\right)_{2 c}$ |

## Lower bounds: idea

- Double separation
- Random choice of batch


## Optimal algorithms: non-distributed with bathching

- New variance reduction algorithm

```
Algorithm 4
    Parameters: Stepsizes \(\eta>0\), momentums \(\alpha, \gamma\), batchsize \(b \in\{1, \ldots, n\}\), probability \(p \in(0,1)\)
    Initialization: Choose \(z^{0}=w^{0} \in \operatorname{dom} g\). Put \(z^{-1}=z^{0}, w^{-1}=w^{0}\)
    for \(k=0,1,2 \ldots\) do
    Sample \(j_{1}^{k}, \ldots, j_{b}^{k}\) independently from \(\{1, \ldots, m\}\) uniformly at random
        \(S^{k}=\left\{j_{1}^{k}, \ldots, j_{b}^{k}\right\}\)
        \(\Delta^{k}=\frac{1}{b} \sum_{j \in S^{k}}\left(F_{j}\left(x^{k}\right)-F_{j}\left(w^{k-1}\right)+\alpha\left(F_{j}\left(x^{k}\right)-F_{j}\left(x^{k-1}\right)\right)\right)+F\left(w^{k-1}\right)\)
        \(x^{k+1}=\operatorname{prox}_{\eta g}\left(x^{k}+\gamma\left(w^{k}-x^{k}\right)-\eta \Delta^{k}\right)\)
        \(w^{k+1}= \begin{cases}x^{k+1}, & \text { with probability } p \\ w^{k}, & \text { with probability } 1-p\end{cases}\)
    end for
```


## Optimal algorithms: fixed network

## Algorithm 1

1: Parameters: Stepsizes $\eta, \theta>0$, momentums $\alpha, \beta, \gamma$,
batchsize $b \in\{1, \ldots, n\}$, probability $p \in(0,1)$
2: Initialization: Choose $\mathbf{z}^{0}=\mathbf{w}^{0} \in(\operatorname{dom} g)^{M}, \mathbf{y}^{0} \in$
$\mathcal{L}^{\perp}$. Put $\mathbf{z}^{-1}=\mathbf{z}^{0}, \mathbf{w}^{-1}=\mathbf{w}^{0}, \mathbf{y}^{-1}=\mathbf{y}^{0}$
3: for $k=0,1,2 \ldots$ do
4: $\quad$ Sample $j_{m, 1}^{k}, \ldots, j_{m, b}^{k}$ independently from $[n]$
5: $\quad S^{k}=\left\{j_{m, 1}^{k}, \ldots, j_{m, b}^{k}\right\}$
6: Sample $j_{m, 1}^{k+1 / 2}, \ldots, j_{m, b}^{k+1 / 2}$ independently from [n]
7: $\quad S^{k+1 / 2}=\left\{j_{m, 1}^{k+1 / 2}, \ldots, j_{m, b}^{k+1 / 2}\right\}$
8: $\quad \delta^{k}=\frac{1}{b} \sum_{j \in S^{k}}\left(\mathbf{F}_{j}\left(\mathbf{z}^{k}\right)-\mathbf{F}_{j}\left(\mathbf{w}^{k-1}\right)\right.$

$$
\left.+\alpha\left[\mathbf{F}_{j}\left(\mathbf{z}^{k}\right)-\mathbf{F}_{j}\left(\mathbf{z}^{k-1}\right)\right]\right)+\mathbf{F}\left(\mathbf{w}^{k-1}\right)
$$

9: $\quad \Delta^{k}=\delta^{k}-\left(\mathbf{y}^{k}+\alpha\left(\mathbf{y}^{k}-\mathbf{y}^{k-1}\right)\right)$
10: $\quad \mathbf{z}^{k+1}=\operatorname{prox}_{\eta \mathbf{g}}\left(\mathbf{z}^{k}+\gamma\left(\mathbf{w}^{k}-\mathbf{z}^{k}\right)-\eta \Delta^{k}\right)$
11: $\quad \Delta^{k+1 / 2}=\frac{1}{b} \sum_{j \in S^{k+1 / 2}}\left(\mathbf{F}_{j}\left(\mathbf{z}^{k+1}\right)-\mathbf{F}_{j}\left(\mathbf{w}^{k}\right)\right)$

$$
+\mathbf{F}\left(\mathbf{w}^{k}\right)
$$

12: $\quad \mathbf{y}^{k+1}=\mathbf{y}^{k}-\theta\left(\mathbf{W} \otimes \mathbf{I}_{d}\right)\left(\mathbf{z}^{k+1}-\beta\left(\Delta^{k+1 / 2}-\mathbf{y}^{k}\right)\right)$
13: $\quad \mathbf{w}^{k+1}= \begin{cases}\mathbf{z}^{k}, & \text { with probability } p \\ \mathbf{w}^{k}, & \text { with probability } 1-p\end{cases}$
14: end for

## Optimal algorithms: fixed network

```
Algorithm 2
    Parameters: Stepsizes \(\eta_{z}, \eta_{y}, \eta_{x}, \theta>0\), momentums
    \(\alpha, \gamma, \omega, \tau\), parameters \(\nu, \beta\), batchsize \(b \in\{1, \ldots, n\}\),
    probability \(p \in(0,1)\)
    2: Initialization: Choose \(\mathbf{z}^{0}=\mathbf{w}^{0} \in(\operatorname{dom} g)^{M}, \mathbf{y}^{0} \in\)
    \(\left(\mathbb{R}^{d}\right)^{M}, \mathbf{x}^{0} \in \mathcal{L}^{\perp}\). Put \(\mathbf{z}^{-1}=\mathbf{z}^{0}, \mathbf{w}^{-1}=\mathbf{w}^{0}, \mathbf{y}_{f}=\)
    \(\mathbf{y}^{-1}=\mathbf{y}^{0}, \mathbf{x}_{f}=\mathbf{x}^{-1}=\mathbf{x}^{0}, m_{0}=\mathbf{0}^{d M}\)
    3: for \(k=0,1,2, \ldots\) do
        Sample \(j_{m, 1}^{k}, \ldots, j_{m, b}^{k}\) independently from \([n]\)
        \(S^{k}=\left\{j_{m, 1}^{k}, \ldots, j_{m, b}^{k}\right\}\)
        Sample \(j_{m, 1}^{k+1 / 2}, \ldots, j_{m, b}^{k+1 / 2}\) independently from [ \(n\) ]
        \(S^{k+1 / 2}=\left\{j_{m, 1}^{k+1 / 2}, \ldots, j_{m, b}^{k+1 / 2}\right\}\)
        \(\delta^{k}=\frac{1}{b} \sum_{j \in S^{k}}\left(\mathbf{F}_{j}\left(\mathbf{z}^{k}\right)-\mathbf{F}_{j}\left(\mathbf{w}^{k-1}\right)\right.\)
        \(\left.+\alpha\left[\mathbf{F}_{j}\left(\mathbf{z}^{k}\right)-\mathbf{F}_{j}\left(\mathbf{z}^{k-1}\right)\right]\right)+\mathbf{F}\left(\mathbf{w}^{k-1}\right)\)
        \(\Delta_{z}^{k}=\delta^{k}-\nu \mathbf{z}^{k}-\mathbf{y}^{k}-\alpha\left(\mathbf{y}^{k}-\mathbf{y}^{k-1}\right)\)
        \(\mathbf{z}^{k+1}=\operatorname{prox}_{\eta_{\mathbf{z}}}\left(\mathbf{z}^{k}+\omega\left(\mathbf{w}^{k}-\mathbf{z}^{k}\right)-\eta_{z} \Delta_{z}^{k}\right)\)
        \(\mathbf{y}_{c}^{k}=\tau \mathbf{y}^{k}+(1-\tau) \mathbf{y}_{f}^{k}\)
        \(\mathbf{x}_{c}^{k}=\tau \mathbf{x}^{k}+(1-\tau) \mathbf{x}_{f}^{k}\)
        \(\Delta_{y}^{k}=\nu^{-1}\left(\mathbf{y}_{c}^{k}+\mathbf{x}_{c}^{k}\right)+\mathbf{z}^{k+1}+\gamma\left(\mathbf{y}^{k}+\mathbf{x}^{k}+\nu \mathbf{z}^{k}\right)\)
        \(\delta^{k+1 / 2}=\frac{1}{b} \sum_{j \in S^{k+1 / 2}}\left(\mathbf{F}_{j}\left(\mathbf{z}^{k+1}\right)-\mathbf{F}_{j}\left(\mathbf{w}^{k}\right)\right)\)
        \(+\mathbf{F}\left(\mathbf{w}^{k}\right)\)
        \(\Delta_{x}^{k}=\nu^{-1}\left(\mathbf{y}_{c}^{k}+\mathbf{x}_{c}^{k}\right)+\beta\left(\mathbf{x}^{k}+\delta^{k+1 / 2}\right)\)
        \(\mathbf{y}^{k+1}=\mathbf{y}^{k}-\eta_{y} \Delta_{y}^{k}\)
        \(\mathbf{x}^{k+1}=\mathbf{x}^{k}-\left(\mathbf{W}_{T}(T k) \otimes \mathbf{I}_{d}\right)\left(\eta_{x} \Delta_{x}^{k}+m^{k}\right)\)
        \(m^{k+1}=\eta_{x} \Delta_{x}^{k}+m^{k}\)
            \(-\left(\mathbf{W}_{T}(T k) \otimes \mathbf{I}_{d}\right)\left(\eta_{x} \Delta_{x}^{k}+m^{k}\right)\)
        \(\mathbf{y}_{f}^{k+1}=\mathbf{y}_{c}^{k}+\tau\left(\mathbf{y}^{k+1}-\mathbf{y}^{k}\right)\)
        \(\mathbf{x}_{f}^{k+1}=\mathbf{x}_{c}^{k}-\theta\left(\mathbf{W}_{T}(T k) \otimes \mathbf{I}_{d}\right)\left(\mathbf{y}_{c}^{k}+\mathbf{x}_{c}^{k}\right)\)
        \(\mathbf{w}^{k+1}= \begin{cases}\mathbf{z}^{k}, & \text { with probability } p \\ \mathbf{w}^{k}, & \text { with probability } 1-p\end{cases}\)
```


## Quantization and compression

## Definition (Quantization)

A stochastic operator $Q: \mathbb{R}^{d} \rightarrow \mathbb{R}^{d}$ is called quantization if there exists a constant $q \geq 1$ such that

$$
Q(z)=z, \quad \mathrm{E}\|Q(z)\|^{2} \leq q\|z\|^{2}, \quad \forall z \in \mathbb{R}^{d} .
$$

Expected/average compression (how much less the compressed vector takes up in memory): $\beta^{-1} \stackrel{\text { def }}{=} \frac{E\|Q(z)\|_{\text {bits }}}{\|z\| \|_{\text {bits }}}$. Note that $\beta \geq 1$.
Examples: random selection of coordinates.

## Definition (Compression)

(Stochastic) operator $C: \mathbb{R}^{d} \rightarrow \mathbb{R}^{d}$ is called compression if there exists $\delta \geq 1$ such that

$$
\mathrm{E}\|C(z)-z\|^{2} \leq(1-1 / \delta)\|z\|^{2}, \quad \forall z \in \mathbb{R}^{d}
$$

Expected/average compression (how much less the compressed vector occupies in memory): $\beta^{-1} \stackrel{\text { def }}{=} \frac{E\|C(z)\|_{\text {bits }}}{\|z\|_{\text {bits }}}$. Отметим, что $\beta \geq 1$. Examples: Greedy choice of coordinates, low-rank decompositions,

## Ideas

- For example, quantized extragradient method

$$
\begin{aligned}
& z^{k+1 / 2}=z^{k}-\gamma \cdot \frac{1}{M} \sum_{m=1}^{M} Q_{1}\left(F_{m}\left(z^{k}\right)\right) \\
& z^{k+1}=z^{k}-\gamma \cdot \frac{1}{M} \sum_{m=1}^{M} Q_{2}\left(F_{m}\left(z^{k+1 / 2}\right)\right)
\end{aligned}
$$

- Different $Q$ are taken here. In fact it can be the same operator in terms of physics, but with different or the same randomness.


## Ideas

- Good idea: variance reduction.
- Non-distributed problem:

$$
\min _{z \in \mathbb{R}^{d}} \frac{1}{n} \sum_{i=1}^{n} f_{i}(z)
$$

And the next method:

$$
\begin{gathered}
z^{k+1}=z^{k}-\gamma \cdot\left(\nabla f_{i_{k}}\left(z^{k}\right)-\nabla f_{i_{k}}\left(w^{k}\right)+\nabla f\left(w^{k}\right)\right) \\
w^{k+1}=\left\{\begin{array}{lll}
w^{k} & \text { with prob. } & \tau \\
z^{k} & \text { with prob } & 1-\tau
\end{array}\right.
\end{gathered}
$$

## MASHA1

## Algorithm 1 MASHA1

Parameters: Stepsize $\gamma>0$, parameter $\tau \in(0 ; 1)$, number of iterations $K$.
Initialization: Choose $z^{0}=w^{0} \in \mathcal{Z}$.
Devices send $F_{m}\left(w^{0}\right)$ to server and get $F\left(w^{0}\right)$
for $k=0,1,2, \ldots, K-1$ do
for each device $m$ in parallel do
$z^{k+1 / 2}=\tau z^{k}+(1-\tau) w^{k}-\gamma F\left(w^{k}\right)$
Sends $g_{m}^{k}=Q_{m}^{\text {dev }}\left(F_{m}\left(z^{k+1 / 2}\right)-F_{m}\left(w^{k}\right)\right)$ to server
end for
for server do
Sends to devices $g^{k}=Q^{\text {serv }}\left[\frac{1}{M} \sum_{m=1}^{M} g_{m}^{k}\right]$
Sends to devices one bit $b_{k}: 1$ with probability $1-\tau, 0$ with with probability $\tau$ end for
for each device $m$ in parallel do
$z^{k+1}=z^{k+1 / 2}-\gamma g^{k}$
If $b_{k}=1$ then $w^{k+1}=z^{k}$, sends $F_{m}\left(w^{k+1}\right)$ to server and gets $F\left(w^{k+1}\right)$
else $w^{k+1}=w^{k}$
end for
end for

## Convergence MASHA1

- Convergence of MASHA1 in transmitted information:

$$
\mathcal{O}\left(\left[1+\sqrt{\frac{1}{M}+\frac{1}{\beta}} \cdot \frac{L}{\mu}\right] \log \frac{1}{\varepsilon}\right) ;
$$

- Extragradient without quantization:

$$
\mathcal{O}\left(\frac{L}{\mu} \log \frac{1}{\varepsilon}\right)
$$

- Quantization gives boost.


## Compression the same?

- Consider the following distributed problem with $M=3, d=3$ and local functions:

$$
f_{1}(w)=\langle a, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{2}(w)=\langle b, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{3}(w)=\langle c, w\rangle^{2}+\frac{1}{4}\|w\|
$$ where $a=(-3,2,2), b=(2,-3,2)$ и $c=(2,2,-3)$.

## Compression the same?

- Consider the following distributed problem with $M=3, d=3$ and local functions:

$$
f_{1}(w)=\langle a, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{2}(w)=\langle b, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{3}(w)=\langle c, w\rangle^{2}+\frac{1}{4}\|w\|
$$ where $a=(-3,2,2), b=(2,-3,2)$ и $c=(2,2,-3)$.

- Question: where is her optimum?


## Compression the same?

- Consider the following distributed problem with $M=3, d=3$ and local functions:

$$
f_{1}(w)=\langle a, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{2}(w)=\langle b, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{3}(w)=\langle c, w\rangle^{2}+\frac{1}{4}\|w\|
$$ where $a=(-3,2,2), b=(2,-3,2)$ и $c=(2,2,-3)$.

- Question: where is her optimum? $(0,0,0)$.


## Compression the same?

- Consider the following distributed problem with $M=3, d=3$ and local functions:

$$
f_{1}(w)=\langle a, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{2}(w)=\langle b, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{3}(w)=\langle c, w\rangle^{2}+\frac{1}{4}\|w\|
$$ where $a=(-3,2,2), b=(2,-3,2)$ и $c=(2,2,-3)$.

- Question: where is her optimum? $(0,0,0)$.
- Let the starting point $w_{0}=(t, t, t)$ for some $t>0$. Then the local gradients are:
$\nabla f_{1}\left(w_{0}\right)=\frac{t}{2}(-11,9,9), \quad \nabla f_{2}\left(w_{0}\right)=\frac{t}{2}(9,-11,9), \quad \nabla f_{3}\left(w_{0}\right)=\frac{t}{2}(9,9,-11)$.
- Question: what will the QGD (gradient descent with compressions) step look like if we use Top1 compression?


## Compression the same?

- Consider the following distributed problem with $M=3, d=3$ and local functions:

$$
f_{1}(w)=\langle a, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{2}(w)=\langle b, w\rangle^{2}+\frac{1}{4}\|w\|^{2}, f_{3}(w)=\langle c, w\rangle^{2}+\frac{1}{4}\|w\|
$$ where $a=(-3,2,2), b=(2,-3,2)$ и $c=(2,2,-3)$.

- Question: where is her optimum? $(0,0,0)$.
- Let the starting point $w_{0}=(t, t, t)$ for some $t>0$. Then the local gradients are:
$\nabla f_{1}\left(w_{0}\right)=\frac{t}{2}(-11,9,9), \quad \nabla f_{2}\left(w_{0}\right)=\frac{t}{2}(9,-11,9), \quad \nabla f_{3}\left(w_{0}\right)=\frac{t}{2}(9,9,-11)$.
- Question: what will the QGD (gradient descent with compressions) step look like if we use Top1 compression?

$$
w_{1}=(t, t, t)+\gamma \cdot \frac{11}{6}(t, t, t)=\left(1+\frac{11 \gamma}{6}\right) w_{0} .
$$

- We move away from the solution geometrically for any $\gamma>0$.


## Error compensation

- Let's try to remember what we didn't pass on in the communication process:

$$
e_{1, m}=0+\gamma F_{m}\left(z_{0}\right)-C\left(0+\gamma F_{m}\left(z_{0}\right)\right) .
$$

- And add this to future parcels:

$$
C\left(e_{1, m}+\gamma F_{m}\left(z_{1}\right)\right)
$$

- In an arbitrary iteration, it is written as follows:

$$
\begin{aligned}
& \text { Parcel: } C\left(e_{k, m}+\gamma F_{m}\left(w_{k}\right)\right), \\
& e_{k+1, m}=e_{k, m}+\gamma F_{m}\left(z_{k}\right)-C\left(e_{k, m}+\gamma F_{m}\left(z_{k}\right)\right)
\end{aligned}
$$

- This technique is called error compensation (error feedback).


## MASHA2 для компрессий

```
Algorithm 2 MASHA2
    Parameters: Stepsize \(\gamma>0\), parameter \(\tau\), number of iterations \(K\).
    Initialization: Choose \(z^{0}=w^{0} \in \mathcal{Z}, e_{m}^{0}=0, e^{0}=0\).
    Devices send \(F_{m}\left(w^{0}\right)\) to server and get \(F\left(w^{0}\right)\)
    for \(k=0,1,2, \ldots, K-1\) do
    for each device \(m\) in parallel do
        \(z^{k+1 / 2}=\tau z^{k}+(1-\tau) w^{k}-\gamma F\left(w^{k}\right)\)
        Sends \(g_{m}^{k}=C_{m}^{\text {dev }}\left(\gamma F_{m}\left(z^{k+1 / 2}\right)-\gamma F_{m}\left(w^{k}\right)+e_{m}^{k}\right)\) to server
        \(e_{m}^{k+1}=e_{m}^{k}+\gamma F_{m}\left(z^{k+1 / 2}\right)-\gamma F_{m}\left(w^{k}\right)-g_{m}^{k}\)
    end for
    for server do
    Sends to devices \(g^{k}=C^{\text {serv }}\left[\frac{1}{M} \sum_{m=1}^{M} g_{m}^{k}+e^{k}\right]\)
        \(e^{k+1}=e^{k}+\frac{1}{M} \sum_{m=1}^{M} g_{m}^{k}-g^{k}\)
        Sends to devices one bit \(b_{k}: 1\) with probability \(1-\tau, 0\) with with probability \(\tau\)
    end for
    for each device \(m\) in parallel do
        \(z^{k+1}=z^{k+1 / 2}-\gamma g^{k}\)
        If \(b_{k}=1\) then \(w^{k+1}=z^{k}\), sends \(F_{m}\left(w^{k+1}\right)\) to server and gets \(F\left(w^{k+1}\right)\)
        else \(w^{k+1}=w^{k}\)
    end for
    end for
```


## Convergence MASHA2

- Convergence of MASHA2 in transmitted information:

$$
\mathcal{O}\left(\left[1+\frac{L}{\mu}\right] \log \frac{1}{\varepsilon}\right)
$$

- Convergence of MASHA1 in transmitted information:

$$
\mathcal{O}\left(\left[1+\sqrt{\frac{1}{M}+\frac{1}{\beta}} \cdot \frac{L}{\mu}\right] \log \frac{1}{\varepsilon}\right) ;
$$

- Extragradient without quantization:

$$
\mathcal{O}\left(\frac{L}{\mu} \log \frac{1}{\varepsilon}\right)
$$

- Compression does not give boost in theory.


## Convergence MASHA2

- Convergence of MASHA2 in transmitted information:

$$
\mathcal{O}\left(\left[1+\frac{L}{\mu}\right] \log \frac{1}{\varepsilon}\right)
$$

- Convergence of MASHA1 in transmitted information:

$$
\mathcal{O}\left(\left[1+\sqrt{\frac{1}{M}+\frac{1}{\beta}} \cdot \frac{L}{\mu}\right] \log \frac{1}{\varepsilon}\right) ;
$$

- Extragradient without quantization:

$$
\mathcal{O}\left(\frac{L}{\mu} \log \frac{1}{\varepsilon}\right)
$$

- Compression does not give boost in theory.


## Similarity

- The operators $\left\{F_{m}\right\}$ is $\delta$-related in mean. It means that for any $j$ operators $\left\{F_{m}-F_{j}\right\}$ is $\delta$-Lipschitz continuous in mean, i.e. for all $u, v$ we have

$$
\frac{1}{M} \sum_{m=1}^{M}\left\|F_{m}(u)-F_{j}(u)-F_{m}(v)+F_{j}(v)\right\|^{2} \leq \delta^{2}\|u-v\|^{2}
$$

- Comes from hessian (second derivatives similarity):

$$
\left\|\nabla^{2} f_{m}(z)-\nabla^{2} f_{j}(z)\right\| \leq \delta
$$

- Natural assumption since from Hoeffding: $\delta=\tilde{\mathcal{O}}(L / \sqrt{b})$ or even $\delta=\tilde{\mathcal{O}}(L / b)$, where $b$ is the number of local data points on each of the devices.


## Method for data similarity

- Mirror descent for minimization problems:

$$
z^{k+1}=\arg \min _{w \in \mathbb{R}^{d}}\left(\gamma\left\langle\nabla f\left(z^{k}\right), w\right\rangle+V\left(w, z^{k}\right)\right)
$$

where $V(x, y)$ is the Bregman divergence generated by the function $\varphi(x)$ (here we need to require that $f_{1}$ is convex):

$$
\varphi(x)=f_{1}(x)+\frac{\delta}{2}\|x\|^{2}
$$

The function $f_{1}$ is stored on the server.

## Method for data similarity

- Mirror descent for minimization problems:

$$
z^{k+1}=\arg \min _{w \in \mathbb{R}^{d}}\left(\gamma\left\langle\nabla f\left(z^{k}\right), w\right\rangle+V\left(w, z^{k}\right)\right)
$$

where $V(x, y)$ is the Bregman divergence generated by the function $\varphi(x)$ (here we need to require that $f_{1}$ is convex):

$$
\varphi(x)=f_{1}(x)+\frac{\delta}{2}\|x\|^{2} .
$$

The function $f_{1}$ is stored on the server.

- What is the number of communications that occur in $K$ iterations of such a mirror descent? $K$ of communications (the number of gradient counts $\nabla f$ ), computing arg min requires only computations on the server.


## Convergence for data similarity: theorem

## Theorem (convergence for data similarity)

Let $f$ be strongly convex, $f_{i}$ be convex, and $\ell$ be smooth, and $\varphi(w)=f_{1}(w)+\delta\|w\| \|^{2}$, then mirror descent with step $\gamma=1$ converges and is satisfied:

$$
V\left(w^{*}, w_{K}\right) \leq\left(1-\frac{\mu}{\mu+2 \delta}\right)^{K} V\left(w^{*}, w_{0}\right)
$$

## Convergence for data similarity: theorem

## Theorem (convergence for data similarity)

Let $f$ be strongly convex, $f_{i}$ be convex, and $\ell$ be smooth, and $\varphi(w)=f_{1}(w)+\delta\|w\| \|^{2}$, then mirror descent with step $\gamma=1$ converges and is satisfied:

$$
V\left(w^{*}, w_{K}\right) \leq\left(1-\frac{\mu}{\mu+2 \delta}\right)^{K} V\left(w^{*}, w_{0}\right)
$$

- It means that if we need to achieve an accuracy $\varepsilon\left(V\left(w^{*}, w_{K}\right) \sim \varepsilon\right)$, then we need to

$$
K=\left(\left[1+\frac{\delta}{\mu}\right] \log \frac{V\left(w^{*}, w_{0}\right)}{\varepsilon}\right) \text { communications. }
$$

## Similarity + compression

## - Double kill of two ideas

```
Algorithm 1 Three Pillars Algorithm
    Parameters: stepsizes \(\gamma\) and \(\eta\), momentum \(\tau\), probability \(p \in(0 ; 1]\), number of local steps \(H\);
    Initialization: Choose \(z^{0}=m^{0}=\left(x^{0}, y^{0}\right) \in \mathcal{Z}\);
    for \(k=0,1, \ldots, K-1\) do
        Server takes \(u_{0}^{k}=z^{k}\);
        for \(t=0,1, \ldots, H-1\) do
            Server computes \(u_{t+1 / 2}^{k}=\operatorname{proj}_{\mathcal{Z}}\left[u_{t}^{k}-\eta\left(F_{1}\left(u_{t}^{k}\right)-F_{1}\left(m^{k}\right)+F\left(m^{k}\right)+\frac{1}{\gamma}\left(u_{t}^{k}-z^{k}-\tau\left(m^{k}-z^{k}\right)\right)\right)\right]\);
            Server updates \(u_{t+1}^{k}=\operatorname{proj}_{\mathcal{Z}}\left[u_{t}^{k}-\eta\left(F_{1}\left(u_{t+1 / 2}^{k}\right)-F_{1}\left(m^{k}\right)+F\left(m^{k}\right)+\frac{1}{\gamma}\left(u_{t+1 / 2}^{k}-z^{k}-\tau\left(m^{k}-z^{k}\right)\right)\right)\right]\);
        end for
        Server broadcasts \(u_{H}^{k}\) and \(F_{1}\left(u_{H}^{k}\right)\) to devices;
        Devices in parallel compute \(Q_{i}\left(F_{i}\left(m^{k}\right)-F_{1}\left(m^{k}\right)-F_{i}\left(u_{H}^{k}\right)+F_{1}\left(u_{H}^{k}\right)\right)\) and send to server;
        Server updates \(z^{k+1}=\operatorname{proj}_{\mathcal{Z}}\left[u_{H}^{k}+\gamma \cdot \frac{1}{n} \sum_{i=1}^{n} Q_{i}\left(F_{i}\left(m^{k}\right)-F_{1}\left(m^{k}\right)-F_{i}\left(u_{H}^{k}\right)+F_{1}\left(u_{H}^{k}\right)\right)\right]\);
        Server updates \(m^{k+1}=\left\{\begin{array}{ll}z^{k}, & \text { with probability } p, \\ m^{k}, & \text { with probability 1-p, }\end{array}\right.\);
        if \(m^{k+1}=z^{k}\) then
            Server broadcasts \(m^{k+1}\) to devices;
            Devices in parallel compute \(F_{i}\left(m^{k}\right)\) and send to server;
            Server computes \(F\left(m^{k+1}\right)=\frac{1}{n} \sum_{i=1}^{n} F_{i}\left(m^{k+1}\right)\);
        end if
    end for
```

