A note on data-parallel $\mathbb{T}$estudo

Matteo Campanelli

See figure fig. 1 on next page.

Below are adaptations of some of the equations in Spartan for the data-parallel setting. For further reference on these equations, see Spartan paper, page 20, and our figure.

Below s, u, t are formal (tuples of) variables.

$$\begin{align}
\tilde{F}(s,u) &:= \overbrace{\left(\sum_v \tilde{A}(u,v)\cdot\tilde{Z}(s,v)\right)}\cdot\overbrace{\left(\sum_v \tilde{B}(u,v)\cdot\tilde{Z}(s,v)\right)} - \overbrace{\sum_v \tilde{C}(u,v)\cdot\tilde{Z}(s,v)} \tag{1}\\
&= \bar{A}(s,u)\cdot\bar{B}(s,u) - \bar{C}(s,u) \tag{2}
\end{align}$$

$$Q^*(t) := \sum_{s,u} \chi_t(s||u)\cdot\tilde{\mathcal{F}}(s,u) \tag{3}$$

At the end of the first sumcheck we "fix" (s,u) on a random challenge point $r_x = (\nu, \rho)$. Second sumcheck is on the following claim:

$$y^* = \sum_v \tilde{Z}_{\mathrm{tot}}(\rho, v)\cdot\Big(r_A\cdot\tilde{A}(\nu,v) + r_B\cdot B(\nu,v) + r_C\cdot C(\nu,v)\Big) \tag{4}$$

At the end of the second sumcheck we "fix" v on a random challenge point r_y.

$\underline{\mathsf{Setup}\left(1^{\lambda}, 1^{\ell}, 1^{N_{\text{sub}}}, 1^{K}\right)}$

$\underline{P\left(\left(\vec{x}^{(1)}, \ldots, \vec{x}^{(K)}\right), \left(\vec{w}^{(1)}, \ldots, \vec{w}^{(K)}\right)\right)}$ $\underline{V\left(\left(\vec{x}^{(1)}, \ldots, \vec{x}^{(K)}\right)\right)}$

Let $Z_{\text{tot}} = (\vec{x}^{(1)}, \vec{w}^{(1)}, \ldots, \vec{x}^{(K)}, \vec{w}^{(K)})$

$C_{\text{tot,z}} \leftarrow \mathsf{MippPST.Commit}(\tilde{Z}_{\text{tot}})$

$\xrightarrow{C_{\text{tot,Z}}}$

$\tau \leftarrow\!\!\$\ \mathbb{F}^{\log K + \log N_{\text{sub}}}$

$\xleftarrow{\tau}$

// Claim $Q^*(\tau) = \sum_{s,u} \chi_\tau(s||u) \cdot \tilde{\mathcal{F}}(s,u) = 0$

Invoke SC for $\sum_{s,u} \chi_\tau(s||u) \cdot \tilde{\mathcal{F}}(s,u) = 0$

(Sample SC challenge $r_x = (\nu, \rho) \in \mathbb{F}^{\log K + \log N_{\text{sub}}}$)

[Invoke step 6-11 in Spartan, pg 20,

including SC on eq. (4) and sampling of r_y]

$v \leftarrow \tilde{Z}_{\text{tot}}(\nu||r_y)$

Same final steps as in Spartan, but:

- use $\mathsf{MippPST}$opening for$\tilde{Z}_{\text{tot}}$(on $(\nu||r_y)$)
- each computation commitment $\tilde{M}$ is evaluated on $(\rho||r_y)$

Fig. 1: Interactive version of our protocol for batch relations. Given sub-relation R, above we prove batch relation $R(\vec{x}^{(1)}, \vec{w}^{(1)}) \wedge \cdots \wedge R(\vec{x}^{(K)}, \vec{w}^{(K)})$ $\left(\vec{x}^{(1)}, \ldots, \vec{x}^{(K)}\right)$ are the public inputs, each of size ℓ. $\left(\vec{w}^{(1)}, \ldots, \vec{w}^{(K)}\right)$ are the witnesses, each of size N_{sub}. We define the total witness size N_{tot} as $N_{\text{tot}} := N_{\text{sub}} \cdot K$. Notation $\tilde{v}(\vec{X})$ is the multi-linear extension of vector $\vec{v}$, i.e., $\tilde{v}(\vec{X}) := \sum_i v_i \cdot \chi_{(\vec{X})}(\vec{X})(i)$. "SC" stands for sumcheck. We use commas and concatenation interchangeably. **NB**: The protocol above is not including checks for public input; these checks require more but straightforward formal care; they are being ignored here for simplicity.