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

Matteo Campanelli

1 A Batching Testudo (data-parallel computations)

See figure on next page. Here are adaptations of some of the equations in Spartan for the batching case.

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

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

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

Let $Z_i, := (\vec{x}^{(i)}, \vec{w}^{(i)})$ for each i

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

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

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

$\tau_{\text{sel}} \leftarrow\!\!\$\ \mathbb{F}^{\log K}$

$\tau_{\text{sub}} \leftarrow\!\!\$\ \mathbb{F}^{\log N_{\text{sub}}}$

$\tau := \tau_{\text{sel}} || \tau_{\text{sub}}$

$\in \mathbb{F}^{\log K + \log N_{\text{sub}}}$

$\xleftarrow{\tau}$

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

Invoke SC for $0 = \sum_{\vec{b}} \chi(\tau, \vec{b}) \cdot Q^*(\tau)$

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

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

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

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 $(\nu || \rho)$

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 $N_{\text{tot}} := N_{\text{sub}} \cdot K$. $\tilde{v} := \mathsf{mle}[\vec{v}] := \sum_i v_i \cdot \chi_i(\vec{X})$. **NB**: The protocol above is dismissing checks for public input; they simply require more formal care and are ignored here.