A note on data-parallel Testudo

Matteo Campanelli

See figure fig. 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.

$$\tilde{F}(s, u) := \left( \sum_v \tilde{A}(u, v) \cdot \tilde{Z}(s, v) \right) \cdot \left( \sum_v \tilde{B}(u, v) \cdot \tilde{Z}(s, v) \right) - \sum_v \tilde{C}(u, v) \cdot \tilde{Z}(s, v)$$

(1)

$$\tilde{F}(s, u) = \bar{A}(s, u) \cdot \bar{B}(s, u) - \bar{C}(s, u)$$

(2)

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

(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:

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

(4)

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


Fig. 1: Interactive version of our protocol for batch relations. Given sub-relation \( R \), above we prove batch relation \( R(\vec{x}(1), \vec{w}(1)) \land \cdots \land R(\vec{x}(K), \vec{w}(K)) \) are the public inputs, each of size \( \ell \). \( (\vec{w}(1), \ldots, \vec{w}(K)) \) are the witnesses, each of size \( N_{\text{sub}} \). We define the total witness size \( N_{\text{tot}} \) as \( N_{\text{tot}} := N_{\text{sub}} \cdot K \). Notation \( \tilde{v}(X) \) is the multi-linear extension of vector \( \vec{v} \), i.e., \( \tilde{v}(X) := \sum_i v_i \cdot \chi_{\{X\}}(X)(i) \). “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.