WHIR (blueprint)

LeastAuthority

April 29, 2025

Definition 1 (3.4)**.** *We define the* ***equality polynomial*** eq *as follows:*

$$\mathsf{eq}((X_0, \dots, X_{m-1}), (Y_0, \dots, Y_{m-1})) = \prod_{i=0}^{m-1} \left(X_i \cdot Y_i + (1 - X_i) \cdot (1 - Y_i)\right).$$

Note that, for every $\widehat{f} \in \mathbb{F}^{<2^{[X_0,\dots,X_{m-1}]}}$ *and* $z \in \mathbb{F}^m$,

$$\widehat{f}(z) = \sum_{b \in \{0,1\}^m} \widehat{f}(b) \cdot \mathsf{eq}(z, b).$$