WHIR (blueprint)

LeastAuthority

April 29, 2025

inputchapter/error$_c$orrecting$_c$ode

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

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

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

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