# WHIR (blueprint)

LeastAuthority

April 29, 2025

**Definition 3.1.** *An error-correcting code* of length $n$ over an alphabet $\Sigma$ is a subset $\mathcal{C} \subseteq \Sigma^n$. The code $\mathcal{C}$ is a *linear code* if $\Sigma = \mathbb{F}$ is a field and $\mathcal{C}$ is a subspace of $\mathbb{F}^n$.

**Definition 1** (3.4)**.** *We define the* ***equality polynomial*** $\mathsf{eq}$ *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* $z \in \mathbb{F}^m$,

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