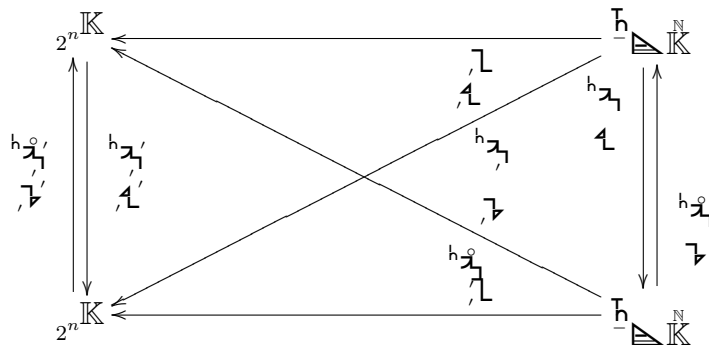


$$2^n \mathbb{K} \xleftarrow{\quad \mathcal{L} \quad} \mathbb{H}^N \mathbb{K}$$

$$\mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}}$$

$$\mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}}$$



$$\mathbf{1} = \begin{cases} h_{2^n}' h_{2^n}' \mathbf{1} \\ \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\mathbf{1} = \begin{cases} h_{2^n}' h_{2^n}' \mathbf{1} \\ \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\mathcal{L} \mathbf{1} = \begin{cases} = h_{2^n}' h_{2^n}' \mathbf{1} & h_{2^n}' h_{2^n}' \mathbf{1} \\ = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} & \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

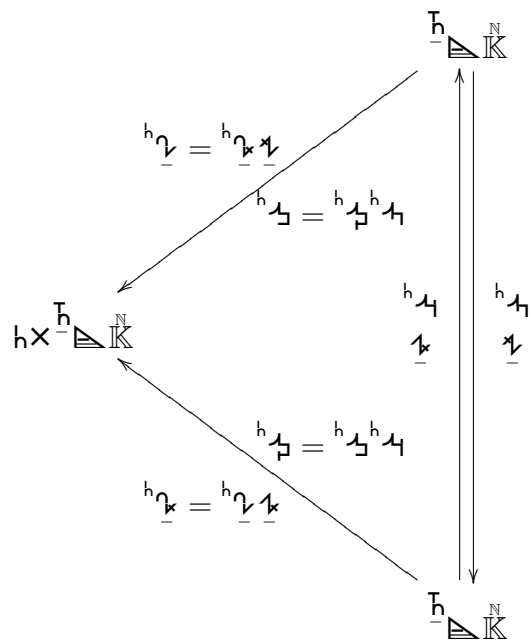
$$\mathcal{L} \mathbf{1} = \begin{cases} = h_{2^n}' h_{2^n}' \mathbf{1} & = h_{2^n}' h_{2^n}' \mathbf{1} \\ = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} & = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\begin{cases} h_{2^n}' \mathbf{1} = \mathcal{L}' h_{2^n}' \mathbf{1} = h_{2^n}' \underline{\mathcal{L} \mathbf{1}} \\ \mathcal{L} \mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\begin{cases} h_{2^n}' \mathbf{1} = \mathcal{L}' h_{2^n}' \mathbf{1} = h_{2^n}' \underline{\mathcal{L} \mathbf{1}} \\ \mathcal{L} \mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\begin{cases} h_{2^n}' \mathbf{1} = \mathcal{L}' h_{2^n}' \mathbf{1} = h_{2^n}' \underline{\mathcal{L} \mathbf{1}} \\ \mathcal{L} \mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$

$$\begin{cases} h_{2^n}' \mathbf{1} = \mathcal{L}' h_{2^n}' \mathbf{1} = h_{2^n}' \underline{\mathcal{L} \mathbf{1}} \\ \mathcal{L} \mathbf{1} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} = \mathcal{L}' \underline{\mathcal{L} \mathbf{1}} \end{cases}$$



$$1 = \underbrace{1}_{\beta} \underbrace{h_{\gamma}}_{\alpha}$$

$$\begin{cases} h_{31} = h_{21} h_{21} \\ h_{41} = h_{21} h_{21} \end{cases}$$

$$h_{21} = \begin{cases} h_{31} h_{31} \\ h_{41} h_{41} \end{cases}$$

