Protocol 1 `tlookup`

Require: The prover $\mathcal{P}$ knows $\mathbf{S} \in \mathbb{F}^D$. N, D are both powers of 2 such that N divides D.

1: **procedure** TLOOKUP-SETUP($\mathbf{T} \in \mathbb{F}^N$)
2: **return** $[\![\mathbf{T}]\!] \leftarrow \texttt{Commit}(\mathbf{T}; 0)$ ▷ No hiding required
3: **end procedure**
4: **procedure** $\mathcal{P}$.TLOOKUP-PREP($\mathbf{S} \in \mathbb{F}^D, \mathbf{T} \in \mathbb{F}^N$)
5: Compute $\mathbf{m} = \mathbf{m}(\mathbf{S}, \mathbf{T})$ as (10)
6: $\mathcal{P} \to \mathcal{V} : [\![\mathbf{S}]\!] \leftarrow \texttt{Commit}(\mathbf{S})$
7: $\mathcal{P} \to \mathcal{V} : [\![\mathbf{m}]\!] \leftarrow \texttt{Commit}(\mathbf{m})$
8: **end procedure**
9: **procedure** $\langle \mathcal{P}, \mathcal{V} \rangle$.TLOOKUP-PROVE($[\![\mathbf{S}]\!], [\![\mathbf{m}]\!], [\![\mathbf{T}]\!]$)
10: $\mathcal{V} \to \mathcal{P} : \beta \sim \mathbb{F}$
11: $\mathcal{P}$ computes $\mathbf{A}, \mathbf{B}$ as (11)
12: $\mathcal{P} \to \mathcal{V} : [\![\mathbf{A}]\!] \leftarrow \texttt{Commit}(\mathbf{A}), [\![\mathbf{B}]\!] \leftarrow \texttt{Commit}(\mathbf{B})$
13: $\mathcal{P}$ and $\mathcal{V}$ run the sumcheck on (14), followed by the proofs of evaluation on $[\![\mathbf{A}]\!], [\![\mathbf{B}]\!], [\![\mathbf{S}]\!], [\![\mathbf{m}]\!]$ and $[\![\mathbf{T}]\!]$.
14: **end procedure**