

Theoretical Proofs

Xingyu Cao, Yipeng Liu *Senior Member, IEEE*, Jiani Liu, Ce Zhu *Fellow, IEEE*

Abstract

This document contains the proofs of Definition 4, Proposition 1 and Corollary 1 in the main body.

I. DERIVATION OF FHCS FOR GENERAL TENSORS

Given $\mathcal{T} = \mathbf{u}^{(1)} \circ \mathbf{u}^{(2)} \circ \dots \circ \mathbf{u}^{(N)} \in \mathbb{R}^{I_1 \times I_2 \times \dots \times I_N}$, assign $l = \sum_{n=1}^N (i_n - 1) \prod_{j=1}^{n-1} I_j + 1$, we have $\text{vec}(\mathcal{T})_l = \mathbf{u}_{i_1}^{(1)} \dots \mathbf{u}_{i_N}^{(N)}$. By definition of HCS, we have:

$$\begin{aligned} & \sum_{i_1=1}^{I_1} \dots \sum_{i_N=1}^{I_N} \text{vec}(\mathcal{T})_l \mathbf{s}_1(i_1) \dots \mathbf{s}_N(i_N) \mathbf{w}^{\mathbf{h}_1(i_1) + \dots + \mathbf{h}_N(i_N) - N} \\ &= \sum_{i_1=1}^{I_1} \dots \sum_{i_N=1}^{I_N} \mathbf{u}_{i_1}^{(1)} \dots \mathbf{u}_{i_N}^{(N)} \mathbf{s}_1(i_1) \dots \mathbf{s}_N(i_N) \mathbf{w}^{\mathbf{h}_1(i_1) + \dots + \mathbf{h}_N(i_N) - N} \\ &= \sum_{i_1} \mathbf{u}_{i_1}^{(1)} \mathbf{s}_1(i_1) \mathbf{w}^{\mathbf{h}_1(i_1) - 1} \dots \sum_{i_N} \mathbf{u}_{i_N}^{(N)} \mathbf{s}_N(i_N) \mathbf{w}^{\mathbf{h}_N(i_N) - 1} \\ &= \mathcal{P}_{\text{CS}_1(\mathbf{u}^{(1)})}(\mathbf{w}) \dots \mathcal{P}_{\text{CS}_N(\mathbf{u}^{(N)})}(\mathbf{w}), \end{aligned} \quad (1)$$

where $\mathcal{P}_{\text{CS}_n(\mathbf{u}^{(n)})}(\mathbf{w})$ is the polynomial form of $\text{CS}_n(\mathbf{u}^{(n)})$ for $n \in [N]$. Let $\mathbf{s}_{N+1}(l) = \mathbf{s}_1(i_1) \dots \mathbf{s}_N(i_N)$, $\mathbf{h}_{N+1}(l) = \mathbf{h}_1(i_1) + \dots + \mathbf{h}_N(i_N) - N + 1$, we have

$$\begin{aligned} & \sum_{i_1=1}^{I_1} \dots \sum_{i_N=1}^{I_N} \text{vec}(\mathcal{T})_l \mathbf{s}_1(i_1) \dots \mathbf{s}_N(i_N) \mathbf{w}^{\mathbf{h}_1(i_1) + \dots + \mathbf{h}_N(i_N) - N} \\ &= \sum_l \text{vec}(\mathcal{T})_l \mathbf{s}_{N+1}(l) \mathbf{w}^{\mathbf{h}_{N+1}(l) - 1} \\ &= \mathcal{P}_{\text{HCS}(\text{vec}(\mathcal{T}))}(\mathbf{w}) \\ &= \mathcal{P}_{\text{FHCS}(\mathcal{T})}(\mathbf{w}). \end{aligned} \quad (2)$$

Therefore, we have

$$\mathcal{P}_{\text{FHCS}(\mathcal{T})}(\mathbf{w}) = \mathcal{P}_{\text{CS}_1(\mathbf{u}^{(1)})}(\mathbf{w}) \dots \mathcal{P}_{\text{CS}_N(\mathbf{u}^{(N)})}(\mathbf{w}). \quad (3)$$

Due to the fact that polynomial multiplication equals the convolution of their coefficients, we have

$$\begin{aligned} \text{FHCS}(\mathcal{T}) &= \text{CS}_1(\mathbf{u}^{(1)}) \otimes \dots \otimes \text{CS}_N(\mathbf{u}^{(N)}) \\ &= \mathbb{F}^{-1}(\mathbb{F}(\text{CS}_1(\mathbf{u}^{(1)})) * \dots * \mathbb{F}(\text{CS}_N(\mathbf{u}^{(N)}))), \end{aligned} \quad (4)$$

which completes the proof.

II. PROOFS FOR PROPOSITION 1 AND COROLLARY 1

A. Proof for Proposition 1

First we prove the consistency of FHCS. We proceed by proving that for any 2-order¹ tensors \mathbf{M}, \mathbf{N} with the same size, $\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle$ is a consistent estimator of $\langle \mathbf{M}, \mathbf{N} \rangle$. To this end we prove it is unbiased with bounded variance.

1) *Unbiasedness:*

$$\begin{aligned} \langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle &= \sum_t \text{FHCS}(\mathbf{M})_t \text{FHCS}(\mathbf{N})_t \\ &= \sum_t \left(\sum_{\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) = t} \mathbf{s}_1(i_1) \mathbf{s}_2(i_2) \mathbf{M}_{i_1, i_2} \right) \left(\sum_{\mathbf{h}_1(j_1) + \mathbf{h}_2(j_2) = t} \mathbf{s}_1(j_1) \mathbf{s}_2(j_2) \mathbf{N}_{j_1, j_2} \right), \end{aligned} \quad (5)$$

$$\mathbb{E}_{\mathbf{h}, \mathbf{s}} \langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle = \sum_{\substack{i_1, i_2 \\ j_1, j_2}} \mathbb{E}[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2), \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2))] \mathbb{E}[\mathbf{s}_1(i_1) \mathbf{s}_2(i_2) \mathbf{s}_1(j_1) \mathbf{s}_2(j_2)] \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, j_2}, \quad (6)$$

¹For simplicity we focus on 2-order tensors, i.e. matrices. The conclusion can be easily generalized to tensors with any order.

where E denotes expectation. Given $\mathbf{h}_1, \mathbf{h}_2, \mathbf{s}_1, \mathbf{s}_2$ are 2-wise independent, we have

$$E[\mathbf{s}_1(i_1)\mathbf{s}_2(i_2)\mathbf{s}_1(j_1)\mathbf{s}_2(j_2)] = \begin{cases} 1, & i_1 = j_1, i_2 = j_2 \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

Obviously $E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2), \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2)))]_{i_1=j_1, i_2=j_2} = 1$. Hence

$$E_{\mathbf{h}, \mathbf{s}} \langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle = \sum_{i_1, i_2} \mathbf{M}_{i_1, i_2} \mathbf{N}_{i_1, i_2} = \langle \mathbf{M}, \mathbf{N} \rangle. \quad (8)$$

2) *Variance boundedness:*

$$\begin{aligned} \langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle^2 &= \sum_{\substack{i_1, i_2 \\ j_1, j_2 \\ i'_1, i'_2 \\ j'_1, j'_2}} \delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2), \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2)) \delta(\mathbf{h}_1(i'_1) + \mathbf{h}_2(i'_2), \mathbf{h}_1(j'_1) + \mathbf{h}_2(j'_2)) \\ &\quad \mathbf{s}_1(i_1)\mathbf{s}_2(i_2)\mathbf{s}_1(j_1)\mathbf{s}_2(j_2)\mathbf{s}_1(i'_1)\mathbf{s}_2(i'_2)\mathbf{s}_1(j'_1)\mathbf{s}_2(j'_2) \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, j_2} \mathbf{M}_{i'_1, i'_2} \mathbf{N}_{j'_1, j'_2}. \end{aligned} \quad (9)$$

Denote $\mathfrak{S}_1 := \{i_1, j_1, i'_1, j'_1\}$, $\mathfrak{S}_2 := \{i_2, j_2, i'_2, j'_2\}$, summation variables S_1, S_2, S_3 . We say \mathfrak{S}_k has *best match* if $i_k = j_k, i'_k = j'_k$ for $k \in [2]$. then (9) can be grouped into the following cases:

Case 1 $\mathfrak{S}_1, \mathfrak{S}_2$ both have best matches, then

$$S_1 = \sum_{\substack{i_1, i_2 \\ i'_1, i'_2}} \mathbf{M}_{i_1, i_2} \mathbf{N}_{i_1, i_2} \mathbf{M}_{i'_1, i'_2} \mathbf{N}_{i'_1, i'_2} = \langle \mathbf{M}, \mathbf{N} \rangle^2. \quad (10)$$

Case 2 One out of $\mathfrak{S}_1, \mathfrak{S}_2$ does not have best matches, take \mathfrak{S}_1 for example. Suppose $i_1 = i'_1 \neq j_1 = j'_1$, then

$$\begin{aligned} S_2 &= \binom{2}{1} \binom{2}{1} \sum_{\substack{i_1, i_2 \\ j_1, i'_2}} E[\delta(\mathbf{h}_1(i_1), \mathbf{h}_1(j_1))^2] \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, i_2} \mathbf{M}_{i_1, i'_2} \mathbf{N}_{j_1, i'_2} \\ &= \frac{4}{J} \sum_{\substack{i_1, i_2 \\ j_1, i'_2}} \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, i_2} \mathbf{M}_{i_1, i'_2} \mathbf{N}_{j_1, i'_2} \\ &= \frac{4}{J} \sum_{i_1, j_1} \langle \mathbf{M}(\mathbf{e}_{i_1}, \mathbf{I}), \mathbf{N}(\mathbf{e}_{j_1}, \mathbf{I}) \rangle^2 \\ &\leq \frac{4}{J} \sum_{i_1, j_1} \|\mathbf{M}(\mathbf{e}_{i_1}, \mathbf{I})\|_{\mathbb{F}}^2 \|\mathbf{N}(\mathbf{e}_{j_1}, \mathbf{I})\|_{\mathbb{F}}^2 \\ &= \frac{4}{J} \|\mathbf{M}\|_{\mathbb{F}}^2 \|\mathbf{N}\|_{\mathbb{F}}^2 \end{aligned} \quad (11)$$

holds due to the Cauchy-Schwartz inequality.

Case 3 Neither of $\mathfrak{S}_1, \mathfrak{S}_2$ has best matches. Suppose $i_1 = i'_1 \neq j_1 = j'_1, i_2 = i'_2 \neq j_2 = j'_2$, then

$$S_3 = \binom{2}{1} \binom{2}{1} \sum_{\substack{i_1, i_2 \\ j_1, j_2}} E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2), \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2))] \mathbf{M}_{i_1, i_2}^2 \mathbf{N}_{j_1, j_2}^2 \quad (12)$$

From 2-wise independence of \mathbf{h}_1 and \mathbf{h}_2 , we have

$$P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) = t] = \begin{cases} \sum_{k=0}^t P[\mathbf{h}_1(i_1) = k, \mathbf{h}_2(i_2) = t - k] = \frac{t+1}{J^2}, & t \leq J-1 \\ \sum_{k=t-J+1}^{J-1} P[\mathbf{h}_1(i_1) = k, \mathbf{h}_2(i_2) = t - k] = \frac{2J-1-t}{J^2}, & t \geq J \end{cases}$$

Therefore

$$P[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2), \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2)) = 1] = \left(\frac{1}{J^2}\right)^2 + \left(\frac{2}{J^2}\right)^2 + \cdots + \left(\frac{J}{J^2}\right)^2 + \left(\frac{J-1}{J^2}\right)^2 + \cdots + \left(\frac{1}{J^2}\right)^2 = \frac{2J^2+1}{3J^3}.$$

Then we have

$$S_3 = \binom{2}{1} \binom{2}{1} \frac{2J^2+1}{3J^3} \sum_{\substack{i_1, i_2 \\ j_1, j_2}} \mathbf{M}_{i_1, i_2}^2 \mathbf{N}_{j_1, j_2}^2 = \frac{4(2J^2+1)}{3J^3} \|\mathbf{M}\|_{\mathbb{F}}^2 \|\mathbf{N}\|_{\mathbb{F}}^2. \quad (13)$$

As a result, we have

$$E_{\mathbf{h},\mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle^2] = S_1 + S_2 + S_3 \leq \langle \mathbf{M}, \mathbf{N} \rangle^2 + \frac{20J^2 + 4}{3J^3} \|\mathbf{M}\|_{\text{F}}^2 \|\mathbf{N}\|_{\text{F}}^2. \quad (14)$$

Therefore

$$\begin{aligned} V_{\mathbf{h},\mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle] &= E_{\mathbf{h},\mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle^2] - E_{\mathbf{h},\mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle]^2 \\ &\leq \frac{20J^2 + 4}{3J^3} \|\mathbf{M}\|_{\text{F}}^2 \|\mathbf{N}\|_{\text{F}}^2. \end{aligned} \quad (15)$$

Combining (8, 15) the consistency is proved.

We further prove FHCS computes a better estimator for tensor inner product than TS.

$$\begin{aligned} \langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle^2 &= \sum_{\substack{i_1, i_2 \\ j_1, j_2 \\ i'_1, i'_2 \\ j'_1, j'_2}} \delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2) \bmod J) \delta(\mathbf{h}_1(i'_1) + \mathbf{h}_2(i'_2) \bmod J, \mathbf{h}_1(j'_1) + \mathbf{h}_2(j'_2) \bmod J) \\ &\quad \mathbf{s}_1(i_1) \mathbf{s}_2(i_2) \mathbf{s}_1(j_1) \mathbf{s}_2(j_2) \mathbf{s}_1(i'_1) \mathbf{s}_2(i'_2) \mathbf{s}_1(j'_1) \mathbf{s}_2(j'_2) \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, j_2} \mathbf{M}_{i'_1, i'_2} \mathbf{N}_{j'_1, j'_2}). \end{aligned} \quad (16)$$

Define $\mathfrak{G}_1, \mathfrak{G}_2$ similarly as mentioned before. Then (16) can be grouped into following cases:

Case 1 $\mathfrak{G}_1, \mathfrak{G}_2$ both have best matches, then

$$S_1 = \sum_{\substack{i_1, i_2 \\ i'_1, i'_2}} \mathbf{M}_{i_1, i_2} \mathbf{N}_{i_1, i_2} \mathbf{M}_{i'_1, i'_2} \mathbf{N}_{i'_1, i'_2} = \langle \mathbf{M}, \mathbf{N} \rangle^2. \quad (17)$$

Case 2 One out of $\mathfrak{G}_1, \mathfrak{G}_2$ does not have best matches, take \mathfrak{G}_1 for example. Suppose $i_1 = i'_1 \neq j_1 = j'_1$, then

$$\begin{aligned} S_2 &= \binom{2}{1} \binom{2}{1} \sum_{\substack{i_1, i_2 \\ j_1, i'_2}} E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(i_2) \bmod J) \delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i'_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(i'_2) \bmod J)] \\ &\quad \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, i_2} \mathbf{M}_{i_1, i'_2} \mathbf{N}_{j_1, i'_2}. \end{aligned} \quad (18)$$

Obviously $E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(i_2) \bmod J)] = 1$ iff $\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J = \mathbf{h}_1(j_1) + \mathbf{h}_2(i_2) \bmod J$. Denote

$$\begin{aligned} \mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J &:= k_1 J + m \\ \mathbf{h}_1(j_1) + \mathbf{h}_2(i_2) \bmod J &:= k_2 J + m, \end{aligned} \quad (19)$$

we have

$$\mathbf{h}_1(i_1) - \mathbf{h}_1(j_1) = (k_1 - k_2)J := kJ. \quad (20)$$

Given $\mathbf{h}_1(i_1), \mathbf{h}_1(j_1) \in [J]$, (20) holds iff $k = 0$, i.e. $\mathbf{h}_1(i_1) = \mathbf{h}_1(j_1)$. Hence

$$\begin{aligned} E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(i_2) \bmod J) \delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i'_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(i'_2) \bmod J)] &= 1 \\ &= P[\mathbf{h}_1(i_1) = \mathbf{h}_1(j_1)] = \frac{1}{J}. \end{aligned} \quad (21)$$

Therefore

$$S_2 = \binom{2}{1} \binom{2}{1} \frac{1}{J} \sum_{\substack{i_1, i_2 \\ j_1, i'_2}} \mathbf{M}_{i_1, i_2} \mathbf{N}_{j_1, i_2} \mathbf{M}_{i_1, i'_2} \mathbf{N}_{j_1, i'_2} \leq \frac{4}{J} \|\mathbf{M}\|_{\text{F}}^2 \|\mathbf{N}\|_{\text{F}}^2. \quad (22)$$

Case 3 Neither of $\mathfrak{G}_1, \mathfrak{G}_2$ has best matches. Suppose $i_1 = i'_1 \neq j_1 = j'_1, i_2 = i'_2 \neq j_2 = j'_2$, then

$$S_3 = \binom{2}{1} \binom{2}{1} \sum_{\substack{i_1, i_2 \\ j_1, j_2}} E[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2) \bmod J)] \mathbf{M}_{i_1, i_2}^2 \mathbf{N}_{j_1, j_2}^2. \quad (23)$$

From 2-wise independence of \mathbf{h}_1 and \mathbf{h}_2 , we have

$$P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J = t] = \begin{cases} P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) = t] + P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) = t + J] = \frac{1}{J}, & t < J - 1 \\ P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) = t] = \frac{1}{J}, & t = J - 1 \end{cases}$$

i.e. $P[\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J = t] = \frac{1}{J}$ for $t = 0, \dots, J-1$. Hence

$$P[\delta(\mathbf{h}_1(i_1) + \mathbf{h}_2(i_2) \bmod J, \mathbf{h}_1(j_1) + \mathbf{h}_2(j_2) \bmod J) = 1] = \left(\frac{1}{J}\right)^2 J = \frac{1}{J}.$$

Therefore

$$S_3 = \binom{2}{1} \binom{2}{1} \frac{1}{J} \sum_{\substack{i_1, i_2 \\ j_1, j_2}} \mathbf{M}_{i_1, i_2}^2 \mathbf{N}_{j_1, j_2}^2 = \frac{4}{J} \|\mathbf{M}\|_F^2 \|\mathbf{N}\|_F^2. \quad (24)$$

As a result, we have

$$E_{\mathbf{h}, \mathbf{s}}[\langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle^2] = S_1 + S_2 + S_3 \leq \langle \mathbf{M}, \mathbf{N} \rangle^2 + \frac{8}{J} \|\mathbf{M}\|_F^2 \|\mathbf{N}\|_F^2. \quad (25)$$

Therefore

$$V_{\mathbf{h}, \mathbf{s}}[\langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle] = E_{\mathbf{h}, \mathbf{s}}[\langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle^2] - E_{\mathbf{h}, \mathbf{s}}[\langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle]^2 \leq \frac{8}{J} \|\mathbf{M}\|_F^2 \|\mathbf{N}\|_F^2. \quad (26)$$

Since the Hash length $J \geq 1$, clearly we have $V_{\mathbf{h}, \mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle] \leq V_{\mathbf{h}, \mathbf{s}}[\langle \text{TS}(\mathbf{M}), \text{TS}(\mathbf{N}) \rangle]$, which means FHCS provides a more accurate estimator than TS for tensor inner product, especially when J is small. It can be proved in a similar way that as the tensor order increases, this inequality becomes more pronounced.

B. Proof for Corollary 1

(15) can be represented as $V_{\mathbf{h}, \mathbf{s}}[\langle \text{FHCS}(\mathbf{M}), \text{FHCS}(\mathbf{N}) \rangle] = O(\frac{\|\mathbf{M}\|_F^2 \|\mathbf{N}\|_F^2}{J})$. By substituting $\mathbf{M} = \mathbf{T}$, $\mathbf{N} = \mathbf{u} \circ \mathbf{u}$, and $\mathbf{M} = \mathbf{T}$, $\mathbf{N} = \mathbf{e}_i \circ \mathbf{u}$, respectively, from Chebychev's inequality we prove the corollary immediately since \mathbf{u} is a unit vector and hence both $\mathbf{u} \circ \mathbf{u}$ and $\mathbf{e}_i \circ \mathbf{u}$ equals 1. The conclusion also generalizes to tensors of any order.