Cyclically Symmetric Entropy Inequalities

Jun Chen*, Hao Ye†, Chao Tian†, Tie Liu‡, and Zhiqing Xiao§
*McMaster University, Hamilton, ON L8S 4K1, Canada
†The University of Tennessee Knoxville, Knoxville TN 37996, USA
‡Texas A&M University, College Station, TX 77843, USA
§Tsinghua University, Beijing 100084, China

***Abstract*—A cyclically symmetric entropy inequality is of the form $\hbar_{\mathcal{O}} \geq \bar{c}\hbar_{\mathcal{O}'}$, where $\hbar_{\mathcal{O}}$ and $\hbar_{\mathcal{O}'}$ are two cyclic orbit entropy terms. A computational approach is formulated for bounding the extremal value of $\bar{c}$, which is denoted by $\bar{c}_{\mathcal{O},\mathcal{O}'}$. For two non-empty orbits $\mathcal{O}$ and $\mathcal{O}'$ of a cyclic group, it is said that $\mathcal{O}$ dominates $\mathcal{O}'$ if $\bar{c}_{\mathcal{O},\mathcal{O}'} = 1$. Special attention is paid to characterizing such dominance relationship, and a graphical method is developed for that purpose.**

I. Introduction

Let $X_0, X_1, \cdots, X_{n-1}$ be n jointly distributed discrete random variables. The celebrated Han's subset entropy inequality [1] states that

$$\frac{1}{i\binom{n}{i}} \sum_{\mathcal{A}\subseteq\mathcal{Z}_n:|\mathcal{A}|=i} H(X_{\mathcal{A}}) \geq \frac{1}{j\binom{n}{j}} \sum_{\mathcal{A}'\subseteq\mathcal{Z}_n:|\mathcal{A}'|=j} H(X_{\mathcal{A}'}) \quad (1)$$

for any $i, j \in \mathcal{N}_n$ with $i \leq j$, where $\mathcal{Z}_n = \{0, 1, \cdots, n-1\}$ and $\mathcal{N}_n = \{1, 2, \cdots, n\}$. Note that Han's inequality treats different subsets of the same cardinality on an equal footing; as a consequence, it finds natural applications in the converse argument for problems with this symmetric structure (such as symmetric multilevel diversity coding [2]–[5] and symmetric multiple description coding [6]–[8]). For any $\mathcal{A} \subseteq \mathcal{Z}_n$ and any $k \in \mathcal{Z}_n$, define

$$(\mathcal{A} + k)_n = \{(a + k)_n : a \in \mathcal{A}\},$$

where $(\cdot)_n$ denotes the modulo-n operation. It was shown in [4] that (1) is implied by the following sliding-window subset entropy inequality:

$$\frac{1}{i}\sum_{k=0}^{n-1} H(X_{(\mathcal{Z}_i+k)_n}) \geq \frac{1}{j}\sum_{k=0}^{n-1} H(X_{(\mathcal{Z}_j+k)_n}) \quad (2)$$

for any $i, j \in \mathcal{N}_n$ with $i \leq j$. Note that, among the subsets of the same cardinality, only those consisting of cyclically consecutive integers are relevant in (2). As such, the sliding-window subset entropy inequality can be used in lieu of Han's subset entropy inequality to handle problems with more relaxed symmetric structures.

Following [9], we shall interpret (1) and (2) as certain orbit entropy inequalities. Let G be a permutation group over $\mathcal{Z}_n$. For any $\mathcal{A} \subseteq \mathcal{Z}_n$, the collection of distinct sets $g(\mathcal{A}) \triangleq \{g(a) : a \in \mathcal{A}\}$, $g \in G$, is referred to as an orbit of G and is denoted by $\mathcal{O}(\mathcal{A})$. For an orbit $\mathcal{O}$, all its elements have the same cardinality, which is denoted by $\ell_{\mathcal{O}}$; the cardinality of $\mathcal{O}$ itself is denoted by $|\mathcal{O}|$. For each non-empty[1] orbit $\mathcal{O}$ of G, we define the corresponding (normalized) orbit entropy as

$$\hbar_{\mathcal{O}} = \frac{1}{\ell_{\mathcal{O}}|\mathcal{O}|}\sum_{\mathcal{A}\in\mathcal{O}} H(X_{\mathcal{A}}).$$

An orbit entropy inequality is of the form

$$\hbar_{\mathcal{O}} \geq \bar{c}\hbar_{\mathcal{O}'},$$

where $\mathcal{O}$ and $\mathcal{O}'$ are two non-empty orbits of G. Of particular importance is the extremal value of $\bar{c}$, which is defined as

$$\bar{c}_{\mathcal{O},\mathcal{O}'} = \max\{\bar{c} : \hbar_{\mathcal{O}} \geq \bar{c}\hbar_{\mathcal{O}'} \text{ for all } (X_1, \cdots, X_n)\}.$$

We shall refer to $\bar{c}_{\mathcal{O},\mathcal{O}'}$ as the extremal coefficient and the associated inequality $\hbar_{\mathcal{O}} \geq \bar{c}_{\mathcal{O},\mathcal{O}'}\hbar_{\mathcal{O}'}$ as the extremal orbit entropy inequality.

The largest permutation group over $\mathcal{Z}_n$ is the symmetric group S_n. Note that two subsets $\mathcal{A}$ and $\mathcal{A}'$ are in the same orbit of S_n if and only if $|\mathcal{A}| = |\mathcal{A}'|$. It can be shown [9] that, for $G = S_n$,

$$\bar{c}_{\mathcal{O},\mathcal{O}'} = \begin{cases} 1, & \ell_{\mathcal{O}} \leq \ell_{\mathcal{O}'}, \\ \frac{\ell_{\mathcal{O}'}}{\ell_{\mathcal{O}}}, & \text{otherwise.} \end{cases} \quad (3)$$

and the case $\ell_{\mathcal{O}} \leq \ell_{\mathcal{O}'}$ corresponds to Han's subset entropy inequality. On the other hand, the smallest permutation group is the one that consists of only the identity mapping. In this case, every subset of $\mathcal{Z}_n$ gives rise to a distinct orbit, and we have [9]

$$\bar{c}_{\mathcal{O},\mathcal{O}'} = \begin{cases} \frac{|\mathcal{A}'|}{|\mathcal{A}|}, & \mathcal{A} \supseteq \mathcal{A}', \\ 0, & \text{otherwise,} \end{cases}$$

for $\mathcal{O} = \{\mathcal{A}\}$ and $\mathcal{O}' = \{\mathcal{A}'\}$, where $\mathcal{A}$ and $\mathcal{A}'$ are two arbitrary non-empty subsets of $\mathcal{Z}_n$.

In this work we focus on the case $G = C_n$ (the cyclic group over $\mathcal{Z}_n$), and the corresponding orbit entropy inequalities will be referred to as cyclically symmetrical entropy inequalities. This choice enables us to strike a balance between the aforementioned two extreme cases. Indeed, the symmetry of C_n is weak enough (as compared to S_n) to induce a rich class of orbit entropy inequalities and is strong enough (as compared to the identity permutation which has no symmetry at all) to make such inequalities interesting. It will be seen that the sliding-window subset entropy inequality is just a member of a big family of cyclically symmetrical entropy inequalities.

[1] An orbit $\mathcal{O}$ is said to be non-empty if $\mathcal{O} \neq \{\emptyset\}$.

Although some progress was made in [9], it appears difficult, if not impossible, to obtain a complete analytical characterization of $\bar{c}_{\mathcal{O},\mathcal{O}'}$ for cyclically symmetrical entropy inequalities. For this reason, a computational approach is developed in the present work. Specifically, we compute a lower bound on $\bar{c}_{\mathcal{O},\mathcal{O}'}$ using Shannon-type inequalities [10] (formulated as a linear program) and an upper bound on $\bar{c}_{\mathcal{O},\mathcal{O}'}$ by searching over a class of constructions based on maximum distance separable (MDS) codes.

A common feature shared by (1) and (2) is that they continue to hold if we replace the entropy function $H(\cdot)$ with an arbitrary submodular function $f(\cdot)$ satisfying $f(\emptyset) = 0$. The fact that the monotonicity of the entropy function is not needed for establishing (1) and (2) deserves special attention. Intuitively, random variables are only re-distributed in a submodular entropy inequality whereas a monotone entropy inequality involves insertion or deletion of random variables, which often leads to a loose bound. In this sense, submodular entropy inequalities like (1) and (2) are particularly desirable in the converse argument. As a consequence, significant effort has been devoted to proving this type of inequalities (see, e.g., [11]). Motivated by this, we place special emphasis on those extremal cyclically symmetrical entropy inequalities for which $\bar{c}_{\mathcal{O},\mathcal{O}'} = 1$ (note that $\bar{c}_{\mathcal{O},\mathcal{O}'} = 1$ if and only if $\hbar_{\mathcal{O}} \geq \bar{c}_{\mathcal{O},\mathcal{O}'}\hbar_{\mathcal{O}'}$ is a balanced inequality [12]); indeed, a moment's thought will reveal that the proof of such inequalities (assuming they are Shannon-type inequalities) cannot hinge on the monotonicity of the entropy function. Furthermore, we introduce the notion of dominance. Specifically, orbit $\mathcal{O}$ is said to dominate orbit $\mathcal{O}'$ if $\bar{c}_{\mathcal{O},\mathcal{O}'} = 1$. It will be seen that the symmetry of C_n enables us to develop a specialized graphical method for (partially) characterizing this dominance relationship,

The rest of this paper is organized as follows. In Section II, we formulate a computational approach for bounding the extremal coefficient, which yields a complete characterization of $\bar{c}_{\mathcal{O},\mathcal{O}'}$ for $n \leq 6$. Section III is devoted to the investigation of the dominance relationship, and a graphical method is developed for that purpose. Section IV concludes the paper.

II. Bounding the Extremal Coefficient: A Computational Approach

In this section we present a computational approach that can be used to obtain upper and lower bounds on $\bar{c}_{\mathcal{O},\mathcal{O}'}$.

A. A Linear Programming Lower Bound

For each $\ell \in \{0, 1, n-1, n\}$, let $\mathcal{O}_\ell$ denote the unique orbit $\mathcal{O}$ of C_n with $\ell_{\mathcal{O}} = \ell$. Consider the following optimization problem, which is induced by the Shannon-type inequalities and the symmetry of C_n:

$$\begin{aligned}
\min\ & \frac{\ell_{\mathcal{O}'}}{\ell_{\mathcal{O}}} H_{\mathcal{O}} \\
\text{s.t. } & H_{\mathcal{O}_n} - H_{\mathcal{O}_{n-1}} \geq 0, \\
& H_{\mathcal{O}(\{i\}\cup\mathcal{Q})} + H_{\mathcal{O}(\{j\}\cup\mathcal{Q})} - H_{\mathcal{O}(\mathcal{Q})} - H_{\mathcal{O}(\{i\}\cup\{j\}\cup\mathcal{Q})} \\
& \geq 0, \qquad i \neq j,\ i, j \in \mathcal{Z}_n, \mathcal{Q} \subseteq \mathcal{Z}_n \setminus \{i, j\}, \\
& H_{\mathcal{O}'} = 1.
\end{aligned}$$

TABLE I
$\bar{c}_{\mathcal{O},\mathcal{O}'}$ FOR $n = 4$.

$\mathcal{O}$ \ $\mathcal{O}'$	$\mathcal{O}_1$	$\mathcal{O}_{2,1}$	$\mathcal{O}_{2,2}$	$\mathcal{O}_3$	$\mathcal{O}_4$
$\mathcal{O}_1$	1	1	1	1	1
$\mathcal{O}_{2,1}$	$\frac{1}{2}$	1	$\frac{3}{4}$	1	1
$\mathcal{O}_{2,2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{3}{4}$	1
$\mathcal{O}_3$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	1	1
$\mathcal{O}_4$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	1

TABLE II
$\bar{c}_{\mathcal{O},\mathcal{O}'}$ FOR $n = 5$.

$\mathcal{O}$ \ $\mathcal{O}'$	$\mathcal{O}_1$	$\mathcal{O}_{2,1}$	$\mathcal{O}_{2,2}$	$\mathcal{O}_{3,1}$	$\mathcal{O}_{3,2}$	$\mathcal{O}_4$	$\mathcal{O}_5$
$\mathcal{O}_1$	1	1	1	1	1	1	1
$\mathcal{O}_{2,1}$	$\frac{1}{2}$	1	$\frac{3}{4}$	1	$\frac{9}{10}$	1	1
$\mathcal{O}_{2,2}$	$\frac{1}{2}$	$\frac{3}{4}$	1	$\frac{9}{10}$	1	1	1
$\mathcal{O}_{3,1}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{4}{5}$	1	1
$\mathcal{O}_{3,2}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{4}{5}$	1	1	1
$\mathcal{O}_4$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	1	1
$\mathcal{O}_5$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	1

Denote this linear program by P and its optimal value by (P). We have the following result.

Proposition 1: $(P) \leq \bar{c}_{\mathcal{O},\mathcal{O}'}$.

B. An Upper Bound via MDS Codes

For each n, let us fix a finite field $\mathbb{F}_q$ of size $q \geq n$. We shall first construct $k + r$ random variables $Z_0, Z_1, \ldots, Z_{k+r-1}$ as follows. Let the first k random variables $Z_0, Z_1, ..., Z_{k-1}$ be independent, identically and uniformly distributed on $\mathbb{F}_q$, and let the r additional random variables $Z_k, Z_{k+1}, ..., Z_{k+r-1}$ be generated by encoding the first k random variables with an arbitrary $(k+r, k)$ MDS code, such as a Reed-Solomon code. Next for each $i \in \mathcal{Z}_{k+r}$, we assign Z_i to m_i elements in the set $(X_0, X_1, \ldots, X_{n-1})$. Without loss of generality, we can assume $1 \leq m_0 \leq m_1 \leq \ldots \leq m_{k+r-1}$ and $\sum_{i=0}^{k+r-1} m_i \leq n$. For any subset $X_{\mathcal{A}}$, denote the number of unique random variables Z_i in this set by m, then

$$H(X_{\mathcal{A}}) = \begin{cases} m \log q, & m \leq k, \\ k \log q, & \text{otherwise.} \end{cases}$$

Optimizing the ratio $\frac{\hbar_{\mathcal{O}}}{\hbar_{\mathcal{O}'}}$ among the choices of parameters $(k, r, m_0, m_1, \ldots, m_{k+r-1})$ and the assignments to $(X_0, X_1, \ldots, X_{n-1})$, we can obtain an upper bound on $\bar{c}_{\mathcal{O},\mathcal{O}'}$.

C. Results

Using the approach introduced above, we are able to characterize $\bar{c}_{\mathcal{O},\mathcal{O}'}$ for $n \leq 6$.

1) $n \leq 3$: The orbits of C_n coincide with those of S_n; as a consequence, $\bar{c}_{\mathcal{O},\mathcal{O}'}$ is given by (3).
2) $n = 4$: There are five non-empty orbits $\mathcal{O}_1$, $\mathcal{O}_{2,1}$, $\mathcal{O}_{2,2}$, $\mathcal{O}_3$, and $\mathcal{O}_4$, which are generated by $\{0\}$, $\{0, 1\}$, $\{0, 2\}$, $\{0, 1, 2\}$, and $\{0, 1, 2, 3\}$, respectively. The list of extremal coefficients for all non-empty orbit pairs can be found in Table I.

TABLE III
$\bar{c}_{\mathcal{O},\mathcal{O}'}$ FOR $n = 6$.

$\mathcal{O}$ \ $\mathcal{O}'$	$\mathcal{O}_1$	$\mathcal{O}_{2,1}$	$\mathcal{O}_{2,2}$	$\mathcal{O}_{2,3}$	$\mathcal{O}_{3,1}$	$\mathcal{O}_{3,2}$	$\mathcal{O}_{3,3}$	$\mathcal{O}_{3,4}$	$\mathcal{O}_{4,1}$	$\mathcal{O}_{4,2}$	$\mathcal{O}_{4,3}$	$\mathcal{O}_5$	$\mathcal{O}_6$
$\mathcal{O}_1$	1	1	1	1	1	1	1	1	1	1	1	1	1
$\mathcal{O}_{2,1}$	$\frac{1}{2}$	1	$\frac{3}{4}$	$\frac{2}{3}$	1	$\frac{9}{10}$	$\frac{9}{10}$	$\frac{3}{4}$	1	1	1	1	1
$\mathcal{O}_{2,2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	1	1	1	1	1	1
$\mathcal{O}_{2,3}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{5}{6}$	1
$\mathcal{O}_{3,1}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{9}$	1	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{2}{3}$	1	$\frac{8}{9}$	$\frac{8}{9}$	1	1
$\mathcal{O}_{3,2}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{4}{5}$	$\frac{2}{3}$	$\frac{8}{9}$	$\frac{8}{9}$	1	1	1
$\mathcal{O}_{3,3}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{4}{5}$	1	$\frac{2}{3}$	$\frac{8}{9}$	$\frac{8}{9}$	1	1	1
$\mathcal{O}_{3,4}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{6}$	1
$\mathcal{O}_{4,1}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{5}{8}$	1	$\frac{5}{6}$	$\frac{5}{6}$	1	1
$\mathcal{O}_{4,2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	1	$\frac{3}{4}$	$\frac{15}{16}$	1
$\mathcal{O}_{4,3}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{5}{6}$	1
$\mathcal{O}_5$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	1	1
$\mathcal{O}_6$	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{6}$	1

3) $n = 5$: There are seven non-empty orbits $\mathcal{O}_1$, $\mathcal{O}_{2,1}$, $\mathcal{O}_{2,2}$, $\mathcal{O}_{3,1}$, $\mathcal{O}_{3,2}$, $\mathcal{O}_4$, and $\mathcal{O}_5$, which are generated by $\{0\}$, $\{0,1\}$, $\{0,2\}$, $\{0,1,2\}$, $\{0,1,3\}$, $\{0,1,2,3\}$, and $\{0,1,2,3,4\}$, respectively. The list of extremal coefficients for all non-empty orbit pairs can be found in Table II.
4) $n = 6$: There are thirteen non-empty orbits $\mathcal{O}_1$, $\mathcal{O}_{2,1}$, $\mathcal{O}_{2,2}$, $\mathcal{O}_{2,3}$, $\mathcal{O}_{3,1}$, $\mathcal{O}_{3,2}$, $\mathcal{O}_{3,3}$, $\mathcal{O}_{3,4}$, $\mathcal{O}_{4,1}$, $\mathcal{O}_{4,2}$, $\mathcal{O}_{4,3}$, $\mathcal{O}_5$, and $\mathcal{O}_6$, which are generated by $\{0\}$, $\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{0,1,2\}$, $\{0,1,3\}$, $\{0,1,4\}$, $\{0,2,4\}$, $\{0,1,2,3\}$, $\{0,1,2,4\}$, $\{0,1,3,4\}$, $\{0,1,2,3,4\}$, and $\{0,1,2,3,4,5\}$, respectively. The list of extremal coefficients for all non-empty orbit pairs can be found in Table III.

III. Characterizing the Dominance Relationship: A Graphical Method

Recall that orbit $\mathcal{O}$ is said to dominate orbit $\mathcal{O}'$ (denoted by $\mathcal{O} \succeq \mathcal{O}'$) if $\bar{c}_{\mathcal{O},\mathcal{O}'} = 1$. The relation "$\succeq$" is a partial order over the set of non-empty orbits, namely, it satisfies the following properties:

1) $\mathcal{O} \succeq \mathcal{O}$ (reflexivity);
2) if $\mathcal{O} \succeq \mathcal{O}'$ and $\mathcal{O}' \succeq \mathcal{O}$, then $\mathcal{O} = \mathcal{O}'$ (antisymmetry);
3) if $\mathcal{O} \succeq \mathcal{O}'$ and $\mathcal{O}' \succeq \mathcal{O}''$, then $\mathcal{O} \succeq \mathcal{O}''$ (transitivity).

One can easily infer the dominance relationship from the extremal coefficients for $n \leq 6$ (see Fig. 1).

A. Necessary Conditions for $\mathcal{O} \succeq \mathcal{O}'$

Proposition 2: If $\mathcal{O} \succeq \mathcal{O}'$, then $\ell_{\mathcal{O}} \leq \ell_{\mathcal{O}'}$. Moreover, if $\mathcal{O} \succeq \mathcal{O}'$ and $\mathcal{O} \neq \mathcal{O}'$, then $\ell_{\mathcal{O}} < \ell_{\mathcal{O}'}$.

In fact, we have the following conjecture.

Conjecture: If $\mathcal{O} \succeq \mathcal{O}'$, then there must exist $\mathcal{A} \in \mathcal{O}$ and $\mathcal{A}' \in \mathcal{O}'$ such that $\mathcal{A} \subseteq \mathcal{A}'$.

The conjecture is trivially true when $\ell_{\mathcal{O}} = 1$. We shall show that it is also true when $\ell_{\mathcal{O}} = 2$. In fact, we have the following stronger result.

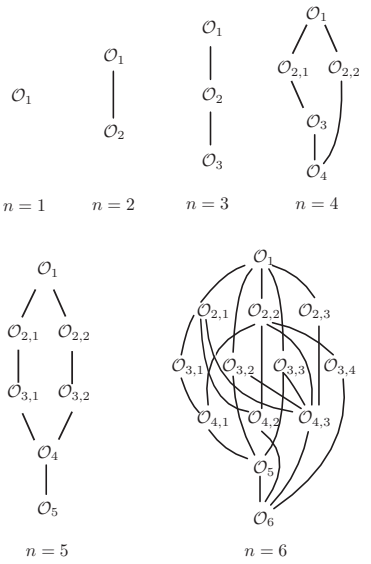

Fig. 1. Hasse diagrams of the dominance relationship for $n \leq 6$.

Proposition 3: Assume $\{0, m\} \in \mathcal{O}$ for some $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$. Then $\mathcal{O} \succeq \mathcal{O}'$ if and only if

$$\frac{\sum_{\mathcal{A} \in \mathcal{O}} \mathbb{I}(\mathcal{A} \cap \{0, m\} \neq \emptyset)}{\sum_{\mathcal{A}' \in \mathcal{O}'} \mathbb{I}(\mathcal{A}' \cap \{0, m\} \neq \emptyset)} \geq \frac{2|\mathcal{O}|}{\ell_{\mathcal{O}'}|\mathcal{O}'|}, \tag{4}$$

where $\mathbb{I}(\cdot)$ is the indicator function.

The proof of Proposition 3 is omitted. Here we explain why (4) implies $\{0, m\} \subseteq \mathcal{A}'$ for some $\mathcal{A}' \in \mathcal{O}'$. Clearly,

$$\begin{aligned} &\frac{1}{|\mathcal{O}|} \sum_{\mathcal{A} \in \mathcal{O}} \mathbb{I}(\mathcal{A} \cap \{0, m\} \neq \emptyset) \\ &= \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{I}(\{k, (m+k)_n\} \cap \{0, m\} \neq \emptyset) \\ &\leq \frac{3}{n}. \end{aligned} \tag{5}$$

On the other hand,

$$\frac{1}{|\mathcal{O}'|}\sum_{\mathcal{A}'\in\mathcal{O}'}\mathbb{I}(\mathcal{A}'\cap\{0,m\}\neq\emptyset)$$
$$=\frac{1}{n}\sum_{k=0}^{n-1}\mathbb{I}((\Lambda(\mathcal{O}')+k)_n\cap\{0,m\}\neq\emptyset), \quad (6)$$

where $\Lambda(\mathcal{O}')$ is an arbitrary element of $\mathcal{O}'$. If $\{0,m\}\nsubseteq(\Lambda(\mathcal{O}')+k)_n$ for any $k\in\mathcal{Z}_n$, then we must have

$$\frac{1}{n}\sum_{k=0}^{n-1}\mathbb{I}((\Lambda(\mathcal{O}')+k)_n\cap\{0,m\}\neq\emptyset)=\frac{2\ell_{\mathcal{O}'}}{n}. \quad (7)$$

Combing (5), (6), and (7) gives

$$\frac{\sum_{\mathcal{A}\in\mathcal{O}}\mathbb{I}(\mathcal{A}\cap\{0,m\}\neq\emptyset)}{\sum_{\mathcal{A}'\in\mathcal{O}'}\mathbb{I}(\mathcal{A}'\cap\{0,m\}\neq\emptyset)}\leq\frac{3|\mathcal{O}|}{2\ell_{\mathcal{O}'}|\mathcal{O}'|},$$

which contradicts (4).

The next result shows that the conjecture holds for Shannon-type inequalities.

Proposition 4: If $\hbar_{\mathcal{O}}\geq\hbar_{\mathcal{O}'}$ is a Shannon-type inequality, then there must exist $\mathcal{A}\in\mathcal{O}$ and $\mathcal{A}'\in\mathcal{O}'$ such that $\mathcal{A}\subseteq\mathcal{A}'$.

It should be emphasized that the converse of our conjecture is not true since otherwise $\mathcal{O}\succeq\mathcal{O}_{n-1}$ whenever $\ell_{\mathcal{O}}\leq n-1$ (which clearly violates the dominance relationship illustrated in Fig. 1 for $n=4$ and $n=6$).

B. Sufficient Conditions for $\mathcal{O}\succeq\mathcal{O}'$

In this subsection we develop a graphical method that integrates the submodularity of the entropy function with the symmetry of C_n. This method leads to simple derivations of several results on the dominance relationship which would be otherwise difficult to obtain using the general machinery for submodular functions.

Given any $\mathcal{S}\subseteq\mathcal{Z}_n$, define $S'=\mathcal{S}\cap(\mathcal{S}+1)_n$ and $S''=\mathcal{S}\cup(\mathcal{S}+1)_n$. It follows by the submodularity of the entropy function that

$$H(X_{\mathcal{S}})+H(X_{(\mathcal{S}+1)_n})\geq H(X_{\mathcal{S}'})+H(X_{\mathcal{S}''}). \quad (8)$$

Averaging over all cyclically shifted versions of (8) gives

$$\frac{2}{|\mathcal{O}(\mathcal{S})|}\sum_{\mathcal{A}\in\mathcal{O}(\mathcal{S})}H(X_{\mathcal{A}})\geq\frac{1}{|\mathcal{O}(\mathcal{S}')|}\sum_{\mathcal{A}'\in\mathcal{O}(\mathcal{S}')}H(X_{\mathcal{A}'})$$
$$+\frac{1}{|\mathcal{O}(\mathcal{S}'')|}\sum_{\mathcal{A}''\in\mathcal{O}(\mathcal{S}'')}H(X_{\mathcal{A}''}). \quad (9)$$

We shall say that $\mathcal{O}(\mathcal{S}')$ ($\mathcal{O}(\mathcal{S}'')$) can be obtained from $\mathcal{O}$ via the $(+1)$ operation, and connect them with a directed edge from $\mathcal{O}(\mathcal{S})$ to $\mathcal{O}(\mathcal{S}')$ ($\mathcal{O}(\mathcal{S}'')$). Applying this operation to every orbit of C_n yields a directed graph (see those graphs labelled with $(+1)$ in Fig. 2). In such a graph, there are two outgoing edges from each orbit except the two absorbing orbits $\mathcal{O}_0$ and $\mathcal{O}_n$; moreover, from each non-empty orbit, there exists (at least) one directed path to $\mathcal{O}_0$ and one directed path to $\mathcal{O}_n$. For each orbit $\mathcal{O}$, let $\mathcal{D}(\mathcal{O})$ denote the set of orbits that can be obtained from $\mathcal{O}$ via the $(+1)$ operation. Note that $|\mathcal{D}(\mathcal{O})|=2$ if $\mathcal{O}$ is a non-absorbing orbit and $|\mathcal{D}(\mathcal{O})|=1$ if it is an absorbing orbit. Define a Markov process $\{M_t\}_{t=0}^{\infty}$ over this directed graph such that

$$\mathbb{P}(M_{t+1}=\mathcal{O}'|M_t=\mathcal{O})=\frac{1}{|\mathcal{D}(\mathcal{O})|},\quad t\geq 0,$$

for any orbit $\mathcal{O}$ of C_n and any $\mathcal{O}'\in\mathcal{D}(\mathcal{O})$. It follows by (9) that

$$\frac{1}{|\mathcal{O}|}\sum_{\mathcal{A}\in\mathcal{O}}H(X_{\mathcal{A}})$$
$$\geq\sum_{\mathcal{O}'\in\mathcal{D}(O)}\frac{\mathbb{P}(M_1=\mathcal{O}'|M_0=\mathcal{O})}{|\mathcal{O}'|}\sum_{\mathcal{A}'\in\mathcal{O}'}H(X_{\mathcal{A}'}).$$

More generally, we have

$$\frac{1}{|\mathcal{O}|}\sum_{\mathcal{A}\in\mathcal{O}}H(X_{\mathcal{A}})$$
$$\geq\sum_{\mathcal{O}'}\frac{\mathbb{P}(M_t=\mathcal{O}'|M_0=\mathcal{O})}{|\mathcal{O}'|}\sum_{\mathcal{A}'\in\mathcal{O}'}H(X_{\mathcal{A}'}),\quad t\geq 0.$$

For the purpose of proving $\mathcal{O}\succeq\mathcal{O}'$, it suffices to have $\mathbb{P}(M_t=\mathcal{O}_0$ or $\mathcal{O}'|M_0=\mathcal{O})\to 1$ as $n\to\infty$ (with $\mathcal{O}'$ set to be an absorbing state). It is thus clear that $\mathcal{O}\succeq\mathcal{O}'$ if every directed path from $\mathcal{O}$ to $\mathcal{O}_n$ goes through $\mathcal{O}'$.

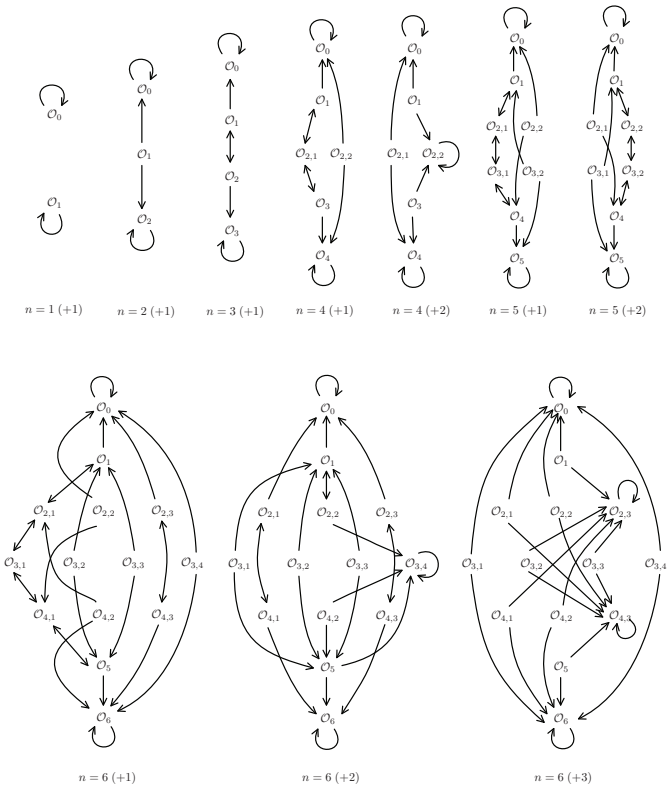

Fig. 2. Directed orbit graphs (with an orbit-independent operation) for $n\leq 6$.

This observation immediately yields the following result, which was first proved in [9] using a subset entropy inequality of Madiman and Tetali [11].

Proposition 5: $\mathcal{O}\succeq\mathcal{O}_n$ for any non-empty orbit $\mathcal{O}$.

The same observation can also be used to establish (2). However, it is apparent that the $(+1)$ operation is just one particular choice. More generally, we can define the $(+m)$ operation for any $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$ and construct the associated directed orbit graph (see Fig. 2). This enables us to establish a generalized sliding-window subset entropy inequality.

For any $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$ and any $i \in \mathcal{N}_s$ (with $s = n/\gcd(n,m)$), let

$$\mathcal{A}_i^{(m)} = \bigcup_{k=0}^{i-1} \{(km)_n\}.$$

The sliding-window subset entropy inequality (2) can be viewed as a special case of the following result with $m = 1$.

Proposition 6: $\mathcal{O}(\mathcal{A}_1^{(m)}) \succeq \mathcal{O}(\mathcal{A}_2^{(m)}) \succeq \cdots \succeq \mathcal{O}(\mathcal{A}_s^{(m)})$ for any $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$.

Proof: This result follows from the simple observation that $\mathcal{O}_0 \leftarrow \mathcal{O}(\mathcal{A}_1^{(m)}) \leftrightarrow \cdots \leftrightarrow \mathcal{O}(\mathcal{A}_{s-1}^{(m)}) \rightarrow \mathcal{O}(\mathcal{A}_s^{(m)})$ is a chain in the directed orbit graph associated with the $(+m)$ operation. ∎

As illustrated in Fig. 1, for $n = 5$, we have $\mathcal{O} \succeq \mathcal{O}_4$ whenever $\ell_{\mathcal{O}} \leq 4$. However, this result cannot be obtained by using the $(+1)$ operation or the $(+2)$ operation alone (see Fig. 2). A possible remedy is to consider directed graphs with orbit-dependent operations. For example, one can modify the directed orbit graph associated with the $(+1)$ operation by applying the $(+2)$ operation to $\mathcal{O}_{3,2}$ and obtain a new graph (see Fig. 3) that has the desired property. This line of thought leads to the following result.

Fig. 3. A directed orbit graph (with orbit-dependent operations) for $n = 5$.

Proposition 7: Assume that n is a prime number. We have $\mathcal{O} \succeq \mathcal{O}_{n-1}$ for any non-empty orbit $\mathcal{O}$ with $\ell_{\mathcal{O}} \leq n-1$.

Proof: Given each orbit $\mathcal{O}$ with $\ell_{\mathcal{O}} \leq n-2$, pick $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$ such that $\{0, m\} \subseteq \mathcal{Z}_n \backslash \mathcal{A}$ for some $\mathcal{A} \in \mathcal{O}$ and apply the $(+m)$ operation to this orbit. It can be verified that the resulting orbit graph has the desired property. ∎

It can be readily seen from Fig. 1 that Proposition 7 does not hold for $n = 4$ and $n = 6$. In fact, the following result, which provides a complete characterization of $\bar{c}_{\mathcal{O},\mathcal{O}_{n-1}}$ for the case $\ell_{\mathcal{O}} = n-2$, shows that one can always find a counter-example to Proposition 7 if n is not a prime number.

Proposition 8: For any non-empty orbit $\mathcal{O}$, if $\mathcal{Z}_n \backslash \{0, m\} \in \mathcal{O}$ for some $m \in \mathcal{N}_{\lfloor \frac{n}{2} \rfloor}$, then

$$\bar{c}_{\mathcal{O},\mathcal{O}_{n-1}} = \frac{(n-1)(n-\gcd(n,m)-1)}{(n-2)(n-\gcd(n,m))}.$$

Proof: Let $X_{(km)_n}$, $k \in \mathcal{Z}_{s-1}$, be $s-1$ mutually independent uniformly distributed Bernoulli random variables, and let $X_{((s-1)m)_n}$ be their modulo-2 sum, where $s = n/\gcd(m,n)$; moreover, set $X_i = 0$ for $i \in \mathcal{Z}_n \backslash \bigcup_{k=0}^{s-1} \{(km)_n\}$. It can be verified that

$$\hbar_{\mathcal{O}} = \frac{n(s-1)-s}{n(n-2)},$$
$$\hbar_{\mathcal{O}_{n-1}} = \frac{s-1}{n-1},$$

which implies

$$\bar{c}_{\mathcal{O},\mathcal{O}_{n-1}} \leq \frac{(n-1)(n-\gcd(n,m)-1)}{(n-2)(n-\gcd(n,m))}.$$

The proof of a matching lower bound is omitted. ∎

IV. Conclusion

We have undertaken a detailed study of cyclically symmetric entropy inequalities with an emphasis on those which only require the submodularity of the entropy function. It is worth mentioning that the inequalities unveiled in the present paper can be used to obtain new conclusive results on multilevel diversity coding and multiple description coding.

Acknowledgment

This work was supported in part by the National Science Foundation under Grants CCF-13-20237, CCF-15-24839, and CCF-15-26095.

References

[1] T. S. Han, "Nonnegative entropy measures of multivariate symmetric correlations," *Inf. Control*, vol. 36, no. 2, pp. 133-156, Feb. 1978.

[2] J. R. Roche, R. W. Yeung, and K. P. Hau, "Symmetrical multilevel diversity coding," *IEEE Trans. Information Theory*, vol. 43, no. 5, pp. 1059–1064, May 1997.

[3] R. W. Yeung and Z. Zhang, "On symmetrical multilevel diversity coding," *IEEE Trans. Information Theory*, vol. 45, no. 2, pp. 609–621, Mar. 1999.

[4] J. Jiang, N. Marukala, and T. Liu, "Symmetrical multilevel diversity coding and subset entropy inequalities," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 84–103, Jan. 2014.

[5] Z. Xiao, J. Chen, Y. Li, and J. Wang, "Distributed multilevel diversity coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6368–6384, Nov. 2015.

[6] H. Wang and P. Viswanath, "Vector Gaussian multiple description with two levels of receivers," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 401–410, Jan. 2009.

[7] C. Tian, S. Mohajer, and S. N. Diggavi, "Approximating the Gaussian multiple description rate region under symmetric distortion constraints," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3869–3891, Aug. 2009.

[8] L. Song, S. Shuo, and J. Chen, "A lower bound on the sum rate of multiple description coding with symmetric distortion constraints," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7547–7567, Dec. 2014.

[9] J. Chen, A. Salimi, T. Liu, and C. Tian, "Orbit-entropy cones and extremal pairwise orbit-entropy inequalities," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, to appear.

[10] R. W. Yeung, *Information Theory and Network Coding*. New York: Springer, 2008.

[11] M. Madiman and P. Tetali, "Information inequalities for joint distributions, with interpretations and applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2699-2713, Jun. 2010.

[12] T. Chan, "Balanced information inequalities," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3261-3267, Dec. 2003.