Symmetries in the Entropy Space

Jayant Apte, Qi Chen, and John MacLaren Walsh

***Abstract*—This paper investigates when Shannon-type inequalities completely characterize the part of the closure of the entropy region $\overline{\Gamma_n^*}$ that is symmetric under the action of a specified random variable permutation group. This question is answered exhaustively for every group permuting $n = 4$ and $n = 5$ random variables, while multiple examples for arbitrary $n \geq 6$ are provided for both tightness and non-tightness of the Shannon-type inequalities. For instance, a new result shows that non-Shannon-type inequalities are necessary under the action of the cyclic group C_n, the dihedral group D_n, as well as $S_1 \times C_{n-1}$ and $S_1 \times D_{n-1}$, for every $n \geq 6$.**

I. Introduction

Let N be a set with cardinality n and $\mathcal{H}_n = \mathbb{R}^{2^N}$. For any $\mathbf{h} \in \mathcal{H}_n$, we call $\mathbf{h}$ *entropic* if there exits a set of n jointly distributed discrete random variables $X_N \triangleq \{X_i : i \in N\}$ such that $\mathbf{h}(A) = H(X_A)$ for any $A \subseteq N$, where $X_A \triangleq \{X_i : i \in A\}$ and $H(X_\emptyset) = 0$ by convention. The vector $\mathbf{h}$ is called the *entropy function* of X_N and so $\mathcal{H}_n$ is called the *entropy space* of order n. Let Γ_n^* be the set of all entropy functions and $\overline{\Gamma_n^*}$ be the closure of Γ_n^*, the set of *almost entropic* functions.

For all $A, B \subseteq N$, entropy is a non-negative ($\mathbf{h}(A) \geq 0$), non-decreasing ($\mathbf{h}(A) \leq \mathbf{h}(B)$ if $A \subseteq B$), and submodular ($\mathbf{h}(A) + \mathbf{h}(B) \geq \mathbf{h}(A \cap B) + \mathbf{h}(A \cup B)$) function, and thus a *polymatroid* [2]. The set of all polymatroids, i.e. the set of all non-negative, non-decreasing, and submodular set functions on N, is denoted by Γ_n. The inequalities bounding Γ_n are also called Shannon-type information inequalities since they can be derived by the nonnegativity of Shannon measures [1, Chapter 13-15]. Due to the existence of infinitely many linear non-Shannon-type inequalities [3], [6] when $n \geq 4$, $\overline{\Gamma_n^*}$ is a non-polyhedral convex cone with $\overline{\Gamma_n^*} \subsetneq \Gamma_n$ for $n \geq 4$, whose boundaries have yet to be exhaustively characterized. It is thus a fundamental open problem in information theory to characterize Γ_n^* and $\overline{\Gamma_n^*}$ for $n \geq 4$, as they determine all fundamental information inequalities. It has been shown that characterizing the entropy region is equivalent to determining the capacity regions of all networks and information storage systems under coding, determining all fundamental inequalities regarding sizes of subgroups in group theory, as well as several other fundamental problems [1, Chapter 13-16, 21].

All three authors were with the Dept. of ECE, Drexel University, and this work was supported by the National Science Foundation under the award CCF-1421828. Jayant Apte and John MacLaren Walsh are now with the Dept. of ECE, Drexel University (email: jsa46@drexel.edu, and jwalsh@coe.drexel.edu). Qi Chen has now returned to the Institute of Network Coding, The Chinese University of Hong Kong (email: qichen@ie.cuhk.edu.hk), where he has received additional support via a grant from the University Grant Committee of the Hong Kong Special Administrative Region (Project No. AoE/E-02/08) and Shenzhen Key Laboratory of Network Coding Key Technology and Application, Shenzhen, China (ZDSY20120619151314964).

In this paper, we wish to contribute to this problem by studying the part of the entropy region $\overline{\Gamma_n^*}$ consisting of those almost entropic vectors which obey a specified collection of symmetries. As a collection of symmetries must be closed under composition and have inverses that are also symmetries, they naturally admit a group structure. Formally, we focus on symmetries arising from permuting random variables, and consider any $G \leq S_n$, a collection of permutations forming a subgroup of the symmetric group on N, defining the associated group action on $\mathcal{H}_n$ by

$$\sigma(\mathbf{h})(A) = \mathbf{h}(\sigma(A))$$

for any $\sigma \in G$ and $\mathbf{h} \in \mathcal{H}_n$. Let fix_G be the set of all fixed points (the fixed set) of this action, i.e.,

$$\mathrm{fix}_G = \{\mathbf{h} \in \mathcal{H}_n : \mathbf{h}(A) = \mathbf{h}(B) \text{ if } \exists\, \sigma \in G \text{ s.t. } \sigma(A) = B\}. \tag{1}$$

Inspired by groups of random variable symmetries that arise in rate regions for network coding problems, [4] defined the G-symmetric entropy region,

$$\Psi_G^* = \Gamma_n^* \cap \mathrm{fix}_G$$

and its outer bound, the G-symmetric polymatroidal region

$$\Psi_G = \Gamma_n \cap \mathrm{fix}_G,$$

respectively. This definition built upon [5], which considered the special case of $(n_1, \ldots, n_t)$-partition groups $G_p = S_{N_1} \times S_{N_2} \times \cdots \times S_{N_t}$, wherein $p = \{N_1, N_2, \ldots, N_t\}$ is a t-partition of N with $n_i = |N_i|, i \in \{1, \ldots, t\}$, and proved the following important theorem.

Thm. 1: *For $|N| \geq 4$,*

$$\overline{\Psi_{G_p}^*} = \Psi_{G_p}$$

if and only if $p = \{N\}$ or $\{\{i\}, N \setminus \{i\}\}$ for some $i \in N$.

The theorem states that the closure of G_p-symmetric entropy region can be fully characterized by Shannon-type inequalities if and only if p is the 1-partition or a 2-partition with one of its blocks being singleton. Building on this theorem, in this paper we study when $\Psi_G = \overline{\Psi_G^*}$ and $\overline{\Psi_G^*} \subsetneq \Psi_G$ for arbitrary random variable permutation groups G.

Naturally, the key quantity in determining the regions $\overline{\Psi_G^*}$ and Ψ_G is the orbits in the power set under the group action, denoted as $2^N//G$, and several results are given regarding the structure of these orbits in §II, as well the structure of these orbit structures themselves under the action of different groups in §III. It is shown that Shannon sufficiency is implied under refinement of the associated partition of the power set, and hence to supergroups of a group, while insufficiency of

Shanon-type inequalities is implied to subgroups. This simple implication, in turn, enables one to leverage the main result of [5] to show that unless the group G acts transitively on N or fixes an element of this set while acting transitively on the remaining $n-1$ elements, Shannon-type inequalities will be insufficient and $\overline{\Psi^*_G} \subsetneq \Psi_G$.

Bearing this in mind, we first undertake an exhaustive solution to the Shannon-type sufficiency question for four and five variables. This is easily carried out with computational tools from GAP and ITAP, and the results are detailed in §IV-A and summarized at the top of Fig. 4.

Shifting attention to $n \geq 6$ and the remaining open cases, which are exclusively associated with transitive subgroups of S_n or S_{n-1}, it becomes clear that the priorities for investigation are containment minimal or maximal transitive groups, as the implication of super/subgroup sufficiency/insufficiency of Shannon-type inequalities can be leveraged to solve more tightness questions. One collection of containment minimal transitive groups are the cyclic groups C_n, and Shannon type inequalities were shown in §IV-A to be sufficient for $n = 4, 5$ for these groups, and thus their supergroups, the dihedral groups D_4 and D_5. However, we prove in §IV-B that Shannon type inequalities are insufficient to characterize $\overline{\Psi^*_{C_n}}$ and $\overline{\Psi^*_{D_n}}$, as well as $\overline{\Psi^*_{S_1 \times C_n}}$ and $\overline{\Psi^*_{S_1 \times D_n}}$ for $n \geq 6$. Together with the results from [5], and their implications to subgroups as described in §III, collectively this forms a wealth of examples of both tightness and non-tightness of the Shannon-type inequalities on group symmetric entropy regions summarized in Fig. 4.

II. Orbit Structure

For a given $G \leq S_n$, for any $\sigma \in G$ and $A \subseteq N$,

$$\sigma(A) = \{\sigma(i) : i \in A\} \tag{2}$$

defines an action of G on 2^N. For $A \subseteq N$, let $\mathcal{O}_G(A) = \{\sigma(A) : \sigma \in G\}$ be the orbit of the action that contains A. If there is no ambiguity, we simply call $\mathcal{O}_G(A)$ an orbit of G. Let $\mathfrak{O}_G = \{\mathcal{O}_G(A) : A \subseteq N\} = 2^N//G$ be the set of all orbits of G and we call it the *orbit structure* of G. Then one can easily check that (1) can be rewritten as

$$\mathrm{fix}_G = \{\mathbf{h} \in \mathcal{H}_n : \mathbf{h}(A) = \mathbf{h}(B) \text{ if } A, B \in \mathcal{O}, \mathcal{O} \in \mathfrak{O}_G\}. \tag{3}$$

It can be seen from (3) that $\mathfrak{O}_G$ uniquely determines fix_G, i.e., $\mathrm{fix}_G = \mathbb{R}^{\mathfrak{O}_G}$. So it also determines in some sense $\overline{\Psi^*_G}$ and Ψ_G, and whether they are equal. Therefore, in this section, we study the structure of $\mathfrak{O}_G$.

There exists a partial order in $\mathfrak{O}_G$ defined below.

Definition 1: *For $\mathcal{O}_1, \mathcal{O}_2 \in \mathfrak{O}_G$, $\mathcal{O}_1 \leq \mathcal{O}_2$ if for any $A \in \mathcal{O}_1$, there exists $B \in \mathcal{O}_2$ such that $A \subseteq B$.*

The definition immediately implies the following.

Prop. 1: *For $A \subseteq B \subseteq N$, $\mathcal{O}_G(A) \leq \mathcal{O}_G(B)$.*

Note that $\mathfrak{O}_G$ may not be a lattice, see Fig. 2(b), the orbit structure of cyclic group C_5.

Let $\{N_1, N_2\}$ be a partition of N, and G_1 and G_2 be permutation groups on N_1 and N_2, respectively. We define

$$\mathfrak{O}_{G_1} \times \mathfrak{O}_{G_2} = \{\mathcal{O} \subseteq 2^N : \{A \cap N_1 : A \in \mathcal{O}\} \in \mathfrak{O}_{G_1}, \{A \cap N_2 : A \in \mathcal{O}\} \in \mathfrak{O}_{G_2}\}.$$

Note that $\mathfrak{O}_{G_1} \times \mathfrak{O}_{G_2}$ is just the Cartesian product of $\mathfrak{O}_{G_1}$ and $\mathfrak{O}_{G_2}$. For $A \subseteq N$, it can be checked that $\mathcal{O}_{G_1 \times G_2}(A) = \mathcal{O}_{G_1}(A \cap N_1) \cdot \mathcal{O}_{G_2}(A \cap N_2)$. For $\mathcal{O}_1 = \mathcal{O}^{(1)}_{G_1} \cdot \mathcal{O}^{(1)}_{G_2}$ and $\mathcal{O}_2 = \mathcal{O}^{(2)}_{G_1} \cdot \mathcal{O}^{(1)}_{G_2}$ in $\mathfrak{O}_{G_1} \times \mathfrak{O}_{G_2}$, $\mathcal{O}_1 \leq \mathcal{O}_2$ if and only if both $\mathcal{O}^{(1)}_{G_1} \leq \mathcal{O}^{(2)}_{G_1}$ and $\mathcal{O}^{(1)}_{G_2} \leq \mathcal{O}^{(2)}_{G_2}$.

Prop. 2: $\mathfrak{O}_{G_1 \times G_2} = \mathfrak{O}_{G_1} \times \mathfrak{O}_{G_2}$.

Proof. Let $B \in \mathcal{O}_{G_1 \times G_2}(A)$. Then there exists $\sigma \in G_1 \times G_2$ such that $B = \sigma(A)$. Let $\sigma = \sigma_1 \sigma_2$, where $\sigma_1 \in G_1$ and $\sigma_2 \in G_2$. Then $B \cap N_1 = \sigma_1(A \cap N_2)$ which implies $B \cap N_1 \in \mathcal{O}_{G_1}(A \cap N_1)$. Similarly $B \cap N_2 \in \mathcal{O}_{G_2}(A \cap N_2)$. Therefore, $\mathcal{O}_{G_1 \times G_2}(A) = \mathcal{O}_{G_1}(A \cap N_1) \cdot \mathcal{O}_{G_2}(A \cap N_2) \in \mathfrak{O}_{G_1} \times \mathfrak{O}_{G_2}$. The other inclusion direction can be verified similarly. □

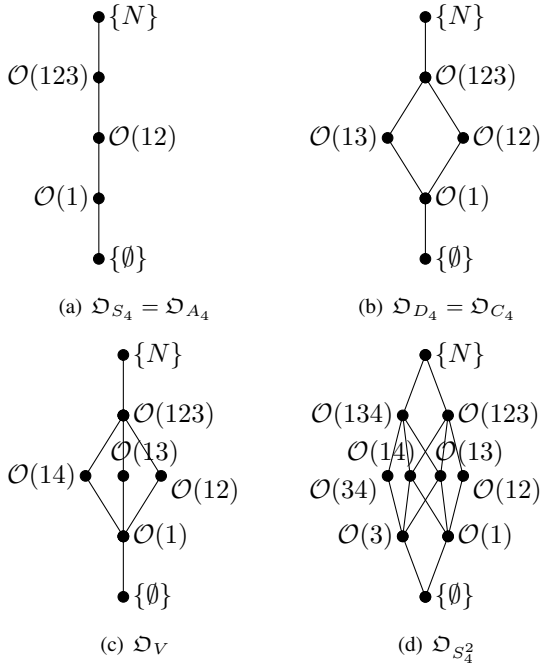
Cor. 1: *Let $p = \{N_1, \cdots, N_t\}$ be a partition of N. Let $G = \prod_{i=1}^t G_i$ be a permutation group on N and G_i be permutation groups on N_i, respectively. Then $\mathfrak{O}_G = \prod_{i=1}^t \mathfrak{O}_{G_i}$.*

According to Corollary 1, if a permutation group G on N can be written as the direct product of G_i on N_i, where N_i is a block of a partition of N, then the orbit structure $\mathfrak{O}_G$ is the direct product of $\mathcal{O}_{G_i}$. We call such groups G *decomposable* if $t \geq 2$ and call other groups *undecomposable*. An orbit structure of a decomposable group is called a *decomposable orbit structure*. An orbit structure which is not equal to the orbit structure of any decomposable group is called an *undecomposable orbit structure*. Note that the orbit structure of an undecomposable group can be decomposable. See Fig. 3, the orbit structure of undecomposable group $S_5^3 \triangleq \langle (12)(45), (345) \rangle$ is decomposable since it is equal to the orbit structure of decomposable group $S_2 \times S_3$.

To study the orbit structure of an arbitrary permutation group, we only need to focus on those undecomposable obit structures and treat them as the building blocks. For symmetric group S_n, the orbit structure is a chain with length $n+1$, i.e., $\mathfrak{O}_{S_n} = \{\mathcal{O}_i = \{A \subseteq N : |A| = i\} : i = 0, \cdots, n\}$ and $\mathcal{O}_i \leq \mathcal{O}_j$ if and only if $i \leq j$. When $n = 1, 2, 3$, all undecomposable orbit structure is orbit structure of symmetric group S_n, while $\mathfrak{O}_{S_3}$ is also equal to $\mathfrak{O}_{A_3}$.

For $n = 4, 5$, the hasse diagrams of all undecomposable orbit structures (up to conjugacy) are listed in Fig.s 1 and 2, respectively. To save space, in the label of the figures, we denote a set by juxtaposing its elements. For example, $\{1, 2\}$ is denoted by 12 and in Fig. 1(c), for group V, $\mathcal{O}(12) = \mathcal{O}_V(\{1, 2\}) = \{\{1, 2\}, \{3, 4\}\}$. In Fig. 3, we give an examples of a decomposable orbit structure $S_2 \times S_3$.

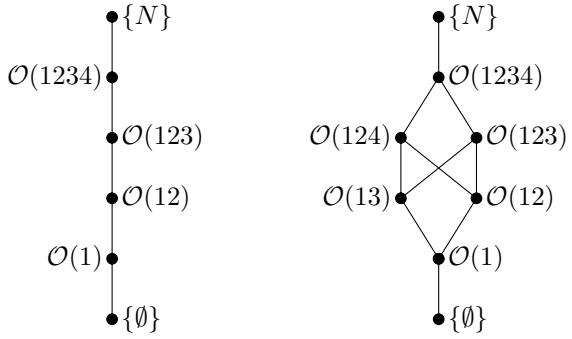
Remark When $G \leq S_n$ is the trivial group, each $A \subseteq N$ forms an orbit of G and $\mathfrak{O}_G$ become isomorphic to the boolean lattice and $\mathrm{fix}_G = \mathcal{H}_n$. Then $\Psi^*_G = \Gamma^*_n$. When $G = S_n$, the symmetric group itself, as we discussed above, $\mathfrak{O}_G$ becomes a chain. When G is a partition group, $\mathfrak{O}_G$ is the direct product of chains, see Fig. 3 for the case of partition group $S_2 \times S_3$.



(a) $\mathfrak{O}_{S_4} = \mathfrak{O}_{A_4}$ (b) $\mathfrak{O}_{D_4} = \mathfrak{O}_{C_4}$

(c) $\mathfrak{O}_V$ (d) $\mathfrak{O}_{S_4^2}$

Fig. 1. Undecomposable orbit structures on $N = \{1, 2, 3, 4\}$



(a) $\mathfrak{O}_{S_5} = \mathfrak{O}_{A_5} = \mathfrak{O}_{GA(1,5)}$ (b) $\mathfrak{O}_{D_5} = \mathfrak{O}_{C_5}$

Fig. 2. Undecomposable orbit structures on $N = \{1, 2, 3, 4, 5\}$

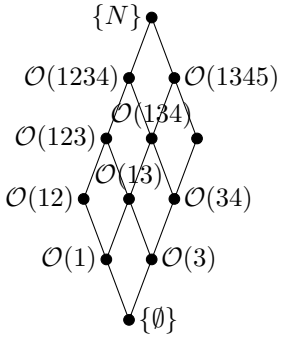


Fig. 3. Orbit structures of $S_2 \times S_3$ and S_5^3

III. Relations Between Orbit Structures

In the previous section, we discussed the orbit structure of a permutation group G. In this section, we discuss the structure among different orbit structures, a partial order defined below.

Definition 2 (Structure of the orbit structures)**:** *For $G_1, G_2 \leq S_n$, $\mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$ if $\mathfrak{O}_{G_1}$ is a refinement of $\mathfrak{O}_{G_2}$.*

For example, by Fig.s 1(b) and 1(c), we see that $\mathfrak{O}_V \leq \mathfrak{O}_{C_4}$.

Prop. 3: *For $G_1 \leq G_2 \leq S_n$, $\mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$.*

Proof. Since $\mathfrak{O}_{G_1}$ and $\mathfrak{O}_{G_2}$ are both partitions of 2^N, to prove $\mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$, it suffices to prove that each orbit of G_2 is the union of the orbits of G_1.

Let $l = |G_2|/|G_1|$ and $G_1\sigma_1, G_1\sigma_2, \cdots, G_1\sigma_l$ be the right cosets of G_1 on G_2, where $\sigma_i \in G_2$ and σ_1 is the identity of G_2 (and also G_1). Then for any $A \subseteq N$,

$$\begin{aligned}\mathcal{O}_{G_2}(A) = \{\sigma(A) : \sigma \in G_2\} &= \bigcup_{i=1}^{l} \{\sigma(\sigma_i(A)) : \sigma \in G_1\} \\ &= \bigcup_{i=1}^{l} \mathcal{O}_{G_1}(\sigma_i(A))\end{aligned}$$

which proves the proposition. □

Lem. 1: *For any $G \leq S_n$, $\overline{\Psi_G^*} = \overline{\Gamma_n^*} \cap \mathrm{fix}_G$.*

Lemma 1 can be proved by a method similar to that of Theorem 4 in [5]. The proof is omitted.

Thm. 2: *For $G_1, G_2 \leq S_n$ with $\mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$,*

1) *if $\overline{\Psi_{G_1}^*} = \Psi_{G_1}$, then $\overline{\Psi_{G_2}^*} = \Psi_{G_2}$;*
2) *if $\overline{\Psi_{G_2}^*} \subsetneq \Psi_{G_2}$, then $\overline{\Psi_{G_1}^*} \subsetneq \Psi_{G_1}$.*

Proof. For $\mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$, by (3), we have $\mathrm{fix}_{G_2} \subseteq \mathrm{fix}_{G_1}$.

Now if $\overline{\Psi_{G_1}^*} = \Psi_{G_1}$, by Lemma 1, we have

$$\begin{aligned}\overline{\Psi_{G_2}^*} &= \overline{\Gamma_n^*} \cap \mathrm{fix}_{G_2} = \overline{\Gamma_n^*} \cap (\mathrm{fix}_{G_1} \cap \mathrm{fix}_{G_2}) \\ &= \overline{\Gamma_n^* \cap \mathrm{fix}_{G_1}} \cap \mathrm{fix}_{G_2} = \overline{\Psi_{G_1}^*} \cap \mathrm{fix}_{G_2} \\ &= \Psi_{G_1} \cap \mathrm{fix}_{G_2} = \Gamma_n \cap \mathrm{fix}_{G_1} \cap \mathrm{fix}_{G_2} \\ &= \Gamma_n \cap \mathrm{fix}_{G_2} = \Psi_{G_2}\end{aligned}$$

which proves the first part of the theorem.

If $\overline{\Psi_{G_2}^*} \subsetneq \Psi_{G_2}$, then there exists $\mathbf{h} \in \Psi_{G_2}$ such that $\mathbf{h} \notin \overline{\Psi_{G_2}^*} = \overline{\Gamma_n^*} \cap \mathrm{fix}_{G_2}$. Since $\mathbf{h} \in \Psi_{G_2} = \Gamma_n \cap \mathrm{fix}_{G_2}$, $\mathbf{h} \in \mathrm{fix}_{G_2}$ which implies that $\mathbf{h} \notin \overline{\Gamma_n^*}$ and so $\mathbf{h} \notin \overline{\Psi_{G_1}} = \overline{\Gamma_n^*} \cap \mathrm{fix}_{G_1}$. One the other hand, since $\Psi_{G_2} \subset \Psi_{G_1}$, $\mathbf{h} \in \Psi_{G_1}$. Therefore $\overline{\Psi_{G_1}^*} \subsetneq \Psi_{G_1}$ which proves the second part of the theorem. □

Proposition 3 and Theorem 2 immediately imply the following Corollary.

Cor. 2: *For $G_1 < G_2 \leq S_n$,*

1) *if $\overline{\Psi_{G_1}^*} = \Psi_{G_1}$, then $\overline{\Psi_{G_2}^*} = \Psi_{G_2}$;*
2) *if $\overline{\Psi_{G_2}^*} \subsetneq \Psi_{G_2}$, then $\overline{\Psi_{G_1}^*} \subsetneq \Psi_{G_1}$.*

The purpose of stating Thm. 2 in terms of orbit structures rather than the subgroups that generate them as presented in corollary 2, and more generally the structure of the orbit structures rather than simply the lattice of subgroups, is that multiple groups can generate the same orbit structure in the

power set, as we shall see multiple examples in the next section and as depicted in Fig. 4. Indeed, as can be seen by Fig.4, which we shall derive in detail in the next section, while $G_1 \leq G_2 \implies \mathfrak{O}_{G_1} \leq \mathfrak{O}_{G_2}$, the converse is not true in general.

Remark According to the the contrapositive of Thm. 1, if $p = N//G \triangleq \{\{\sigma(i) : \sigma \in G\} : i \in N\}$ has three or more blocks, or has two blocks each with more than one element, then $\overline{\Psi_G^*} \subsetneq \Psi_G$. It leaves open only the following remaining cases to determine whether $\overline{\Psi_G^*} = \Psi_G$:

1) G is *transitive*, i.e. $N//G = \{N\}$.
2) G fixes one element of N and acts transitively on the remaining $n-1$ elements, so that $N//G = \{N \setminus i, \{i\}\}$ for some $i \in N$.

Furthermore, we only need to focus on one of these two cases, depending on whether or not we are trying to show sufficiency or insufficiency, as shown by the following theorem.

Thm. 3: $\overline{\Psi^*_{S_1\times G}} = \Psi_{S_1\times G} \implies \overline{\Psi_G^*} = \Psi_G$*, or equivalently,* $\overline{\Psi_G^*} \neq \Psi_G \implies \overline{\Psi^*_{S_1\times G}} \neq \Psi_{S_1\times G}$.

Proof. Observe that the orbits $\mathfrak{O}_{G\times S_1}$ can be found by taking each orbit in $\mathfrak{O}_G$, and repeating it twice, once without the element fixed by S_1, and once with it. Letting $N' = N \cup \{n+1\}$, we see that the projection $\text{proj}_N \Psi_{G\times S_1} = \Psi_G$ (meaning keeping only the elements in the entropy function associated with subsets of the ground set N), since the containment $\subseteq$ holds from the extra variable, inequality, and equalities in the polyhedral cone on the left hand side, and the direction $\supseteq$ holds from the fact that any polymatroid $\mathbf{h} \in \Psi_G$ can trivially be extended to a polymatroid $\mathbf{h}' \in \Psi_{G\times S_1}$ by defining $\mathbf{h}'(A) = \mathbf{h}(A \cap N)$ for all $A \subseteq N'$. A parallel argument shows that $\text{proj}_N \overline{\Psi^*_{G\times S_1}} = \overline{\Psi^*_G}$, since an almost entropic vector can always be extended in this trivial way by making the new random variable deterministic. Thus mapping through the projection operation, $\overline{\Psi^*_{S_1\times G}} = \Psi_{S_1\times G}$ implies $\overline{\Psi_G^*} = \Psi_G$. The other statement is simply the negation of this statement. □

Finally, to best leverage subgroup and supergroup implications set out by Corollary 2, the study should focus on maximal or minimal subgroup, and respect equivalences and the ordering between orbit structures from Thm. 2.

IV. Results: tightness of Polymatroidal region for some symmetrical entropy functions

Bearing the results of the previous section in mind, in this section we exhaustively determine all distinct orbit structures for $n = 4, 5$ random variables, and determine for which ones the Shannon outer bound is tight. Then, we outline several new cases beyond those covered by Thm 1 for which the Shannon outer bound is not tight.

A. Symmetrical entropy functions of 4 or 5 random variables

All subgroups of S_4 and S_5 are easily generated within GAP [7]. When doing so, for each conjugacy class of subgroups, we need to consider only one representative, since the orbit structures of different groups in the same conjugacy class can be obtained from each other by permuting the elements of the ground set. Furthermore, we can consider two representatives of different conjugacy classes with isomorphic orbit structures equivalent for our purpose of determining whether $\Psi_G = \overline{\Psi_G^*}$. Up to conjugacy, there are 11 classes of permutation groups for $n = 4$ and 19 classes of permutation groups for $n = 5$. On the other hand, up to orbit structure isomorphism, there are only 8 and 11 classes of permutation groups respectively for $n = 4$ and 5, and representatives from the conjugacy classes of groups associated with these equivalence classes are listed in the nodes in Fig. 4 under $n = 4$ and $n = 5$, respectively. As described in the previous section, the structure of orbit structures can be partially ordered by partition refinement, and this partial ordering is also depicted via the edges in Fig. 4.

Thm. 4: *Fig. 4 indicates correctly for each node whether* $\Psi_G = \overline{\Psi_G^*}$.

Proof. The orbits in the power set can be found with GAP [7], while the extreme rays of the associated Ψ_G can be calculated by entering the equality constrained regions into lrs [9]. The data located at [10] contains each of these regions Ψ_G and their extreme rays. Paying attention to the structure among the orbits, we can organize the results as follows.

$n = 4$: The only remaining cases not already handled by Thm.s 1 and 2is that of the Normal Klein 4-group $V : \langle (12)(34), (13)(24)\rangle$ and the cyclic/dihedral groups C_4, D_4. We prove $\overline{\Psi_V^*} = \Psi_V$ as this implies, by Theorem 2, $\overline{\Psi_{C_4}^*} = \Psi_{C_4}$. ITAP [8] was used to construct linear polymatroids for all of the rays of Ψ_V, showing that each of them are almost-entropic and thus $\overline{\Psi_V^*} = \Psi_V$ as detailed in [10], [11].

$n = 5$: It suffices to prove $\overline{\Psi^*_{C_5}} = \Psi_{C_5}$ and $\overline{\Psi^*_{S_1\times C_4}} \neq \Psi_{S_1\times C_4}$, as Thm.s 1 and2together with this information handle the other cases via implication. $\overline{\Psi^*_{C_5}} = \Psi_{C_5}$ can be proven by using, e.g. ITAP to construct a linear polymatroid for each of the rays of Ψ_{C_5} as detailed in [10]. Next, among the extreme rays of $\Psi_{S_1\times C_4}$, one finds the polymatroid

$$\mathbf{h}(A) = \begin{cases} 0 & \text{if } A = \emptyset, \\ 2 & \text{if } |A| = 1, \\ 3 & \text{if } |A| = 2 \text{ and } A \neq \{2,4\} \text{ or } \{3,5\}, \\ 4 & \text{if } A = \{2,4\}, \{3,5\} \text{ or } |A| \geq 3. \end{cases}$$

By restricting the polymatroid on $\{1, 2, 3, 4\}$, we have

$$\widetilde{\mathbf{h}}(\mathcal{A}) = \begin{cases} 0 & \text{if } A = \emptyset, \\ 2 & \text{if } |A| = 1, \\ 3 & \text{if } |A| = 2 \text{ and } \mathcal{A} \neq \{2,4\}, \\ 4 & \text{if } A = \{2,4\} \text{ or } |\mathcal{A}| \geq 3, \end{cases} \tag{4}$$

which violates Zhang-Yeung inequality, and is therefore non-entropic. Thus $\overline{\Psi^*_{S_1\times C_4}} \neq \Psi_{S_1\times C_4}$. □

B. Cyclic and dihedral Symmetric Entropy Functions, $n \geq 6$

From the remark at the end of §III, we know that for $G \leq S_n$, to determine whether $\overline{\Psi_G^*} = \Psi_G$, we should consider transitive groups that are either minimal or maximal. In this

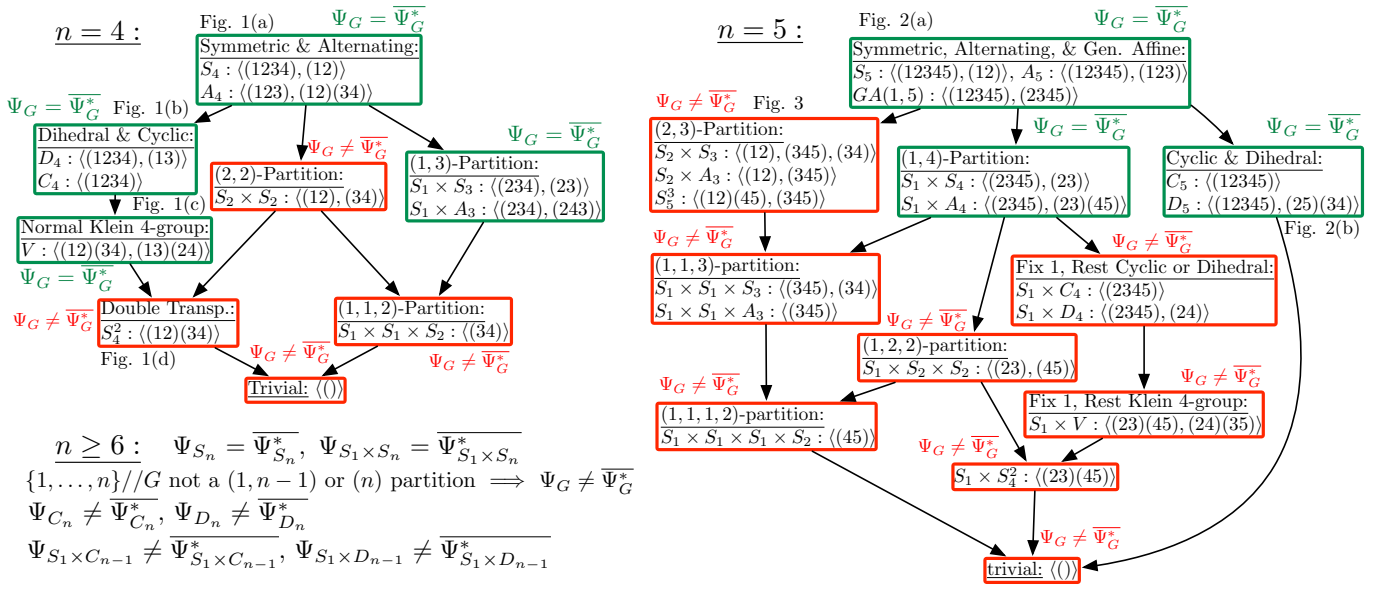


Fig. 4. Summary of results in this paper about the tightness of Shannon outer bounds to group symmetrical entropy regions. Equivalent subgroups of S_n yielding the same orbit structures in the power set are grouped together, and the partial order based on refinement of the associated partition in the power set is displayed. For each subgroup, a sample representation is provided in terms of its generators. When the orbit structure has been depicted elsewhere in the paper, the appropriate figure is also indicated.

vein, we consider the cyclic group C_n and dihedral group D_n, which we have just shown to have Shannon-type inequalities tight for $n = 4, 5$ in the result below.

Thm. 5: *For $n \geq 6$, $\overline{\Psi^*_{C_n}} \subsetneq \Psi_{C_n}$, $\overline{\Psi^*_{D_n}} \subsetneq \Psi_{D_n}$, $\overline{\Psi^*_{S_1 \times C_{n-1}}} \subsetneq \Psi_{S_1 \times C_{n-1}}$, and $\overline{\Psi^*_{S_1 \times D_{n-1}}} \subsetneq \Psi_{S_1 \times D_{n-1}}$.*

Proof. For $G \leq S_n$, let $\mathfrak{O}_{2,G} = \{\mathcal{O}_G(A) \in \mathfrak{O}_G : \forall A \in \mathcal{O}, |A| = 2\}$. Note that $\mathfrak{O}_{2,C_n} = \{\{\sigma(\{1, 1+i\}) : \sigma \in C_n\}, i = 1, \cdots, \lfloor n/2 \rfloor\}$. We pick $\{\sigma(\{1, 4\}) : \sigma \in C_n\} \in \mathfrak{O}_{2,C_n}$. Let $\mathbf{h} \in \mathcal{H}_n$ be defined by

$$\mathbf{h}(A) = \begin{cases} 0 & \text{if } A = \emptyset, \\ 2 & \text{if } |A| = 1, \\ 3 & \text{if } |A| = 2 \text{ and } A \notin \{\sigma(\{1, 4\}) : \sigma \in C_n\}, \\ 4 & \text{if } A \in \{\sigma(\{1, 4\}) : \sigma \in C_n\} \text{ or } |A| \geq 3. \end{cases}$$

This $\mathbf{h} \in \Gamma_n$ and $\mathbf{h} \in \text{fix}_{C_n}$ which implies $\mathbf{h} \in \Psi_{C_n}$. By restricting $\mathbf{h}$ on $\{1, 2, 3, 4\}$, we have the ray (4) which violates Zhang-Yeung inequality, hence is non-entropic, impling that $\mathbf{h}$ is also non-entropic and $\overline{\Psi^*_{C_n}} \subsetneq \Psi_{C_n}$. For dihedral groups $D_n, n \geq 6$, note that $\mathfrak{O}_{2,D} = \mathfrak{O}_{2,C}$ thus $\overline{\Psi^*_{D_n}} \subsetneq \Psi_{D_n}$. These in turn imply $\overline{\Psi^*_{S_1 \times C_{n-1}}} \subsetneq \Psi_{S_1 \times C_{n-1}}$, and $\overline{\Psi^*_{S_1 \times D_{n-1}}} \subsetneq \Psi_{S_1 \times D_{n-1}}$ for $n \geq 7$ by Thm. 3. All that remains is $\overline{\Psi^*_{S_1 \times C_5}} \subsetneq \Psi_{S_1 \times C_5}$, and $\overline{\Psi^*_{S_1 \times D_5}} \subsetneq \Psi_{S_1 \times D_5}$. Among the extreme rays of Ψ_G for this case, one finds

$$\mathbf{h}(A) = \begin{cases} 0 & \text{if } A = \emptyset, \\ 2 & \text{if } |A| = 1, \\ 3 & \text{if } |A| = 2 \text{ and } A \notin \mathcal{O}_G(\{2, 4\}), \\ 4 & \text{otherwise .} \end{cases}$$

By restricting the polymatroid on $\{1, 4, 5, 6\}$, we obtain a ray isomorphic to the ray (4) which violates Zhang-Yeung inequality, therefore non-entropic, implying $\mathbf{h}$ is also non-entropic and hence $\overline{\Psi^*_G} \subsetneq \Psi_G$ for $G = S_1 \times C_5$ and $G = S_1 \times D_5$. □

V. Conclusion

This paper studied whether or not Shannon-type inequalities fully characterize the part of the entropy region that is symmetric under the action of various permutation groups on the random variables. Several results were outlined regarding implications between different groups of the sufficiency/insufficiency of Shannon-type inequalities. Aside from these implications, the main results of the paper are summarized in Fig. 4.

References

[1] R. W. Yeung, *Information Theory and Network Coding*, Springer, 2008.
[2] S. Fujishige, "Polymatroidal dependence structure of a set of random variables," *Info. Contr.*, 39: pp. 55-72,1978.
[3] Z. Zhang and R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Trans. Info. Theory*, vol. 44, pp. 1440-1452, Nov. 1998.
[4] J. Apte and J. Walsh, "Symmetry in network coding," in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015.
[5] Q. Chen and R. W. Yeung, "Partition-symmetrical entropy functions," accepted by *IEEE Trans. Inform. Theory*.
[6] F. Matúš, "Infinitely many information inequalities," IEEE Int. Symp. Info. Theory, Nice, France, June 2007.
[7] The GAP Group, GAP – Groups, Algorithms, and Programming, http://www.gap-system.org
[8] J. Apte and J. M. Walsh, Information Theoretic Achievability Prover-A GAP4 Package, http://www.ece.drexel.edu/walsh/aspitrg/software.html
[9] D. Avis, "A revised implementation of the reverse search vertex enumeration algorithm,"*Polytopes—Combinatorics and Computation*, pp.177–198, Springer, 2000.
[10] J. Apte, Computer Proofs for Symmetrical entropy functions, https://goo.gl/ViNmVb
[11] J. Apte and J. M, Walsh,"Constrained linear representability of polymatroids and algorithms for computing achievability proofs in network coding ," submitted to *IEEE Trans. Info. Theory*, http://arxiv.org/abs/1605.04598.