A note on quasi-uniform distributions and Abelian group representability

Thomas, Eldho K.; Oggier, Frederique

2012

Thomas, E. K., & Oggier, F. (2012). A note on quasi-uniform distributions and Abelian group representability. 2012 International Conference on Signal Processing and Communications (SPCOM), pp.1-5.

https://hdl.handle.net/10356/94135

https://doi.org/10.1109/SPCOM.2012.6290020

A Note on Quasi-Uniform Distributions and Abelian Group Representability

Eldho K. Thomas and Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore.
Email: eldho1@e.ntu.edu.sg, frederique@ntu.edu.sg

***Abstract*—In this note, we study quasi-uniform distributions that are obtained from finite groups. We derive a few simple properties of entropic vectors obtained from Abelian groups, and consider the problem of determining when non-Abelian groups can provide richer entropic vectors than Abelian groups. We focus in particular on the family of dihedral groups D_{2n}, and show that when $2n$ is not a power of 2, the induced entropic vectors for two variables cannot be obtained from Abelian groups, contrarily to the case of D_8 which does not provide more than Abelian groups.**

I. Introduction

Quasi-uniform distributions have attracted increasing interest over the past years because of their connections to information theory. It was shown in [1] that the closure $\bar{\Gamma}_n^*$ of the set of all entropic vectors for n random variables is equivalent to the minimal closed cone containing the set of all n-dimensional quasi-uniform functions, while understanding entropy vectors is a key to determine the capacity regions of many network information theory problems. It was further proven in [3] that one way to obtain quasi-uniform random variables is, surprisingly, through groups. By associating a collection of random variables to subgroups of a given group, one obtains a set of quasi-uniform random variables, whose correlation depends on the subgroup structure of the chosen group. In fact, it was established in [3] that $\bar{\Gamma}_n^*$ is equivalent to the minimal closed cone containing the set of all entropic vectors that can be "characterized" by groups. Finally considering only Abelian groups yields a non-trivial inner bound of $\bar{\Gamma}_n^*$.

Apart their applications to the problem of entropic vectors, quasi-uniform distributions appear in coding theory. Codes can be constructed from quasi-uniform distributions [5], and the resulting so-called quasi-uniform codes are shown to generalize linear codes and almost affine codes [7]. In particular, they can serve as network codes [6] for non-multicast networks.

The connection between groups and quasi-uniform distributions has been studied again in [4], where the authors identified the symmetric group S_5 of order 120 as being the smallest group which violates the Ingleton inequality [8]. Identifying such groups is hoped to both help to approach the problem of entropic vectors, as well as provide possible non-linear network codes. These groups however must be non-Abelian, since it is known from [2] that Abelian groups never violate the inequality.

Determining entropic vectors is a notoriously difficult problem, which we will not tackle here. Instead, we will focus on trying to understand better the connection between quasi-uniform random variables and groups, starting from group theory. The type of questions we are interesting in are:

(1) Given a finite group, how does its subgroup structure determines the correlation of the random variables? In other words, is there some classification of finite groups in terms of the type of entropic vectors they induce? It is too ambitious to consider every finite group, considering the current classification of simple groups, but this makes sense for Abelian groups, whose classification is well known, as well as for some well known studied non-Abelian groups. Though Abelian groups are not improving on linear network codes, they are a starting point to understand more general groups, and to figure out how to design explicit code constructions out of groups.

(2) It is clear that non-Abelian groups are needed, since Abelian groups are not sufficient to bring interesting examples of neither entropic vectors nor codes. However, whether every non-Abelian group can provide new entropic vectors that could not be obtained from Abelian groups is less obvious (and in fact not true). This question also depends on the number n of random variables considered.

This note is organized as follows. We start with providing some background to define our framework. In Section III, we present a few immediate properties of Abelian groups, while we discuss non-Abelian groups and whether they provide new entropic vectors in Section IV, where we mainly focus on the family of dihedral groups. Since this is a preliminary work, numerous open questions are addressed in the conclusion.

II. Preliminaries

Let $X_1, \ldots, X_n$ be a collection of n jointly distributed random variables over some alphabet of size N. We denote by $\mathcal{A}$ a subset of indices from $\mathcal{N} = \{1, \ldots, n\}$, and $X_\mathcal{A} = \{X_i,\ i \in \mathcal{A}\}$.

Definition 1: A set of random variables $X_1, \ldots, X_n$ is quasi-uniform if for any $\mathcal{A} \subset \mathcal{N}$, $X_\mathcal{A}$ is uniformly distributed over its support $\lambda(X_\mathcal{A})$:

$$P(X_\mathcal{A} = x_\mathcal{A}) = \begin{cases} 1/|\lambda(X_\mathcal{A})| & \text{if } x_\mathcal{A} \in \lambda(X_\mathcal{A}), \\ 0 & \text{otherwise.} \end{cases}$$

It is straightforward to compute the entropy of a quasi-uniform distribution. By definition, we have

$$\begin{aligned} H(X_{\mathcal{A}}) &= -\sum_{x_{\mathcal{A}}\in\lambda(X_{\mathcal{A}})} P(X_{\mathcal{A}}=x_{\mathcal{A}})\log P(X_{\mathcal{A}}=x_{\mathcal{A}}) \\ &= \log|\lambda(X_{\mathcal{A}})|. \end{aligned} \quad (1)$$

Surprisingly, one way of obtaining quasi-uniform random variables is through group theory [1]:

Theorem 1: For any finite group G and any subgroups $G_1,\ldots,G_n$ of G, $\exists$ a set of n jointly distributed quasi-uniform discrete random variables $X_1,\ldots,X_n$ such that for all non-empty subsets $\mathcal{A}$ of $\mathcal{N}$, $H(X_{\mathcal{A}})=\log[G:G_{\mathcal{A}}]$, where $G_{\mathcal{A}}=\cap_{i\in\mathcal{A}}G_i$ and $[G:G_{\mathcal{A}}]$ is the index of $G_{\mathcal{A}}$ in G.

Recall that a group G is a set endowed with a binary operation (denoted multiplicatively), satisfying the properties that (1) G is closed under the binary operation, (2) this binary operation is associative, (3) there exists an identity element 1 such that $1g=g1=g$ for every $g\in G$, and (4) every element is invertible, namely there exists g^{-1} such that $gg^{-1}=g^{-1}g=1$ for every $g\in G$. The subgroups G_i, $i=1,\ldots,n$ are subsets of G which form a group. Given a subgroup G_i of G, one can define a left (respectively right) coset of G_i in G by

$$gG_i=\{gh,\ h\in G_i\} \text{ respectively } G_ig=\{hg,\ h\in G_i\}.$$

The number of left (or right) cosets of G_i in G is called the index of G_i in G, denoted by $[G:G_i]$. Lagrange Theorem states that $[G:G_i]=|G|/|G_i|$ where $|G|$ denotes the order (cardinality) of G. The idea of the above theorem is to associate to a random variable X_i whose outcome is some $g\in G$ the left coset gG_i so that $P(X_i=gG_i)=1/[G:G_i]$. We then have that $P(X_i=gG_i,\ i\in\mathcal{A})=1/[G:G_{\mathcal{A}}]$. That the resulting random variables are quasi-uniform follows from coset properties [1].

Let $X_1,\ldots,X_n$ be n jointly distributed discrete random variables with corresponding entropic vector

$$(H(X_1),\ldots,H(X_1,X_2),\ldots H(X_1,\ldots,X_n))$$

which collects all the joint entropies $H(X_{\mathcal{A}})$, $\mathcal{A}\subset\mathcal{N}$. Theorem 1 tells us that given a group G and n subgroups $G_1,\ldots,G_n$, one obtains n quasi-uniform random variables, and the subgroup structure of G determines the correlation among the n random variables, and thus the corresponding entropic vector.

Definition 2: If there exist a group G and subgroups $G_1,\ldots,G_n$ such that $H(X_{\mathcal{A}})=\log[G:G_{\mathcal{A}}]\ \forall\mathcal{A}$, then the entropic vector is said to be *group representable*.

It was already observed in [1] that it is worth distinguishing Abelian groups (with commutative binary operation) from Non-Abelian groups, as mentioned in the introduction. We will start by discussing a few easy properties of Abelian groups, before investigating some well known non-Abelian groups.

III. Some Observations on Abelian Groups

In what follows, we denote by C_n the cyclic group of order n. Recall that by definition C_n is generated by a single element. If it is denoted by g, we write

$$C_n=\langle g\rangle=\{1,g,\ldots,g^{n-1}\}.$$

The classification of finite Abelian groups is well known.

Theorem 2: Suppose G is a finite Abelian group. Then G is in a unique way a direct product of cyclic groups of order p^k, with p prime.

This suggests to look at quasi-uniform distributions obtained from direct product of cyclic groups (a direct product of groups is given by their cartesian product where the binary operation is defined componentwise), as well as from cyclic groups of order p^k with p prime. Our first observation is that the most trivial example of correlation, that of independence, can be characterized by a direct product of cyclic groups!

Proposition 1: Quasi-uniform independent random variables can be represented as the direct product of cyclic groups.

Proof: Let $X_1,X_2,\ldots,X_n$ be a set of quasi-uniform independent random variables. By definition

$$P(X_i=x_i)=\frac{1}{a_i}$$

for some integer a_i, $i=1,\ldots,n$. Since the X_i are independent, we get

$$P(X_{\mathcal{A}}=x_{\mathcal{A}})=\frac{1}{a_{\mathcal{A}}}$$

for all $\mathcal{A}\subseteq\{1,\ldots,n\}$ and $a_{\mathcal{A}}=\prod_{i\in\mathcal{A}}a_i$. From (1), the corresponding entropies are

$$H(X_i)=\log a_i,\ H(X_{\mathcal{A}})=\log a_{\mathcal{A}}$$

for all $\mathcal{A}$. (This is of course coherent with $H(X_{i_1},\ldots,X_{i_{\mathcal{A}}})=H(X_{i_1})+\ldots+H(X_{i_{\mathcal{A}}})$ since the variables are independent.)

We need to construct a group G and subgroups G_i such that

$$\log[G:G_{\mathcal{A}}]=H(X_{\mathcal{A}})=\log a_{\mathcal{A}}\ \forall\mathcal{A},$$

where $G_{\mathcal{A}}=\bigcap_{i\in\mathcal{A}}G_i$ and $[G:G_i]$ is the index of G_i in G, $i=1,\ldots,n$. Let $G=C_{a_1}\times\ldots\times C_{a_n}$ be the direct product of the cyclic groups C_{a_i}. Note that the order of G is $|G|=\prod_{j=1}^n a_j$. Consider the subgroup G_i of G given by

$$G_i=C_{a_1}\times\ldots\times\{1_i\}\times\ldots\times C_{a_n}$$

where $\{1_i\}$ is the identity of C_{a_i}. Then

$$G_i\cap G_j=C_{a_1}\times\ldots\times\{1_i\}\times\ldots\times\{1_j\}\times\ldots\times C_{a_n}$$

so that

$$[G:G_i]=\frac{|G|}{|G_i|}=\frac{\prod_{j=1}^n a_j}{\prod_{j\neq i}a_j}=a_i$$

and similarly

$$[G:G_{\mathcal{A}}]=|G|/|G_{\mathcal{A}}|=\frac{\prod_{j=1}^n a_j}{\prod_{j\notin\mathcal{A}}a_j}=a_{\mathcal{A}}$$

for all $\mathcal{A}$ and the result follows. ∎

Note that a characterization of independent random variables in terms of subgroups is given in [2].

We next consider cyclic groups of order a prime power, which yield highly correlated entropic vectors. More precisely:

Proposition 2: Let p be a prime and C_{p^k} be a cyclic group of order p^k. Then the random variables $X_1, \ldots, X_n$ induced by n subgroups of C_{p^k} satisfy, up to a change of label, that $H(X_i|X_n) = 0$ for $i = 1, \ldots, n$.

Proof: Let $G = C_{p^k}$. Then its subgroup structure is

$$G \supset C_{p^{k-1}} \supset \ldots \supset C_p \supset \{1\}.$$

Set $G_i = C_{p^{k-i}}$ for $i = 1, \ldots k$. Note that for all i

$$[G : G_i] = |G|/|G_i| = \frac{p^k}{p^{k-i}} = p^i.$$

We know from Theorem 1 that corresponding to a group G and some subgroups $G_1, \ldots, G_n$ there exist jointly distributed random variables X_i such that $H(X_{\mathcal{A}}) = \log[G : G_{\mathcal{A}}]$.

For $i > j$, $H(X_i, X_j) = \log[G : G_i \cap G_j] = \log[G : G_i] = H(X_i)$ which implies $H(X_i|X_j) = H(X_i, X_j) - H(X_i) = 0$.

Now let $G_1, \ldots, G_n$ be a subset of subgroups of G corresponding to $X_1, \ldots, X_n$ and without loss of generality we assume that up to reordering $G_n \subset G_{n-1} \subset \ldots \subset G_1$. Then

$$\begin{aligned} H(X_1, \ldots, X_n) &= \log[G : G_1 \cap \ldots \cap G_n] \\ &= \log[G : G_n] = H(X_n). \end{aligned}$$

By the chain rule of entropy $H(X_n, X_{n-1}, \ldots, X_1) = H(X_n) + H(X_{n-1}|X_n) + \ldots + H(X_1|X_n, \ldots, X_2)$ implying that $H(X_{n-1}|X_n) = \ldots = H(X_1|X_n, \ldots, X_2) = 0$. This tells that given X_n, X_{n-1} is deterministic. By switching the role of X_{n-1} and X_{n-j} in the chain rule, we similarly get

$$H(X_{n-j}|X_n) = 0, \ j = 1, \ldots, n-1,$$

and X_n determines the random variables $X_1, \ldots, X_{n-1}$. ∎

Note that functional dependency is characterized more generally in [2] in terms of subgroups.

Example 1: Consider the cyclic group C_8, whose subgroup structure is shown on Fig. 1. Take $G_1 = C_4$, $G_2 = C_2$. Then

$$H(X_1) = \log 2, \ H(X_2) = \log 4, \ H(X_1, X_2) = \log 4.$$

Thus

$$H(X_1, X_2) = H(X_1|X_2) + H(X_2) = H(X_1|X_2) + \log 4$$

showing that $H(X_1|X_2) = 0$.

IV. Non-Abelian Groups and Abelian Group Representability

We now turn to the case of non-Abelian groups, and wonder whether the entropic vectors they induce could as well be coming from Abelian groups, in which case we refer to them as being *Abelian group representable*. For that, we fix the number n of random variables we are interested in. To show that an Abelian group suffices, we need to explore all possible choices of n, which can be at most the total number of subgroups of G. Note that given a group G, it always contains two trivial subgroups: the identity element $\{1\}$ and the whole group G itself. If a subgroup G_i is chosen to be G, then $\log[G : G] = 0$, that is $H(X_i) = 0$, corresponding to X_i actually taking values deterministically. If on the other hand

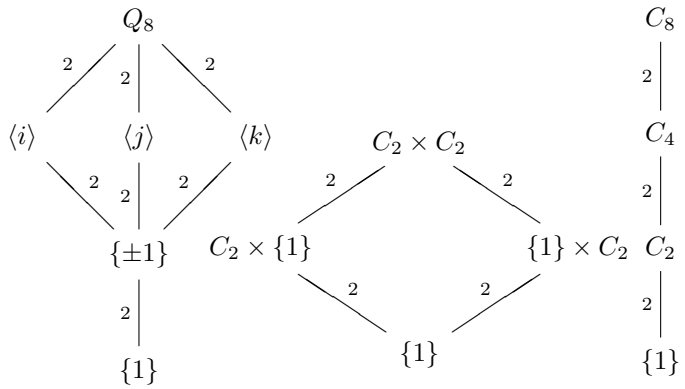

Fig. 1. The quaternion group Q_8 and its lattice of subgroups: when $n = 2$, the Abelian groups $C_2 \times C_2$ and C_8 provide the same entropic vectors. Numbers on the branches refer to the indices of the subgroups.

$G_i = \{1\}$, then $\log[G : \{1\}] = \log |G|$. Thus the entropy chain rule yields

$$H(X_i, X_{\mathcal{A}}) = H(X_i) + H(X_{\mathcal{A}}|X_i)$$

for every $\mathcal{A}$ such that $i \notin \mathcal{A}$, but since $H(X_i) = \log |G|$ and $H(X_i, X_{\mathcal{A}}) = \log[G : \{1\} \cap G_{\mathcal{A}}] = \log |G|$, we conclude that

$$H(X_{\mathcal{A}}|X_i) = 0.$$

In words, given X_i, all the $n-1$ other random variables become deterministic, that is, they are actually functions of X_i. We will consequently assume that n is at most the number of non-trivial subgroups of G.

A. Non-Abelian Groups of order 8

We start by looking at groups of small orders. The three smallest non-Abelian groups are the dihedral groups D_6 (of order 6), D_8 (of order 8) and the quaternion group Q_8 (or order 8 as well). The group D_6 will be treated next.

Consider first the quaternion group Q_8:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

If $n = 2$, we can either choose as subgroups two among $\langle i \rangle, \langle j \rangle, \langle k \rangle$, or one among this same list and $\{\pm 1\}$ as the other one. In the first case, we have

$$H(X_1) = \log 2, \ H(X_2) = \log 2, \ H(X_1, X_2) = \log 4.$$

Such an entropic vector can be instead obtained from the Klein group $C_2 \times C_2$ (see Fig. 1) by choosing

$$\begin{aligned} G = C_2 \times C_2, \ G_1 = C_2 \times \{1\}, \\ G_2 = \{1\} \times C_2, \ G_1 \cap G_2 = \{1\}. \end{aligned} \tag{2}$$

In the second case, we have

$$H(X_1) = \log 2, \ H(X_2) = \log 4, \ H(X_1, X_2) = \log 4.$$

It can be obtained from $G = C_8, \ G_1 = C_4, \ G_2 = C_2$.

Consider next the dihedral group D_8 (see Fig. 2), whose description by generators and relations is:

$$D_8 = \langle r, s \mid r^4 = s^2 = 1, \ rs = sr^{-1} \rangle.$$

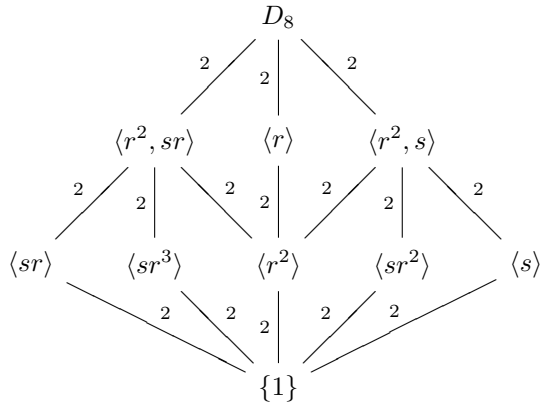

Fig. 2. The dihedral group D_8 and its lattice of subgroups.

If $n = 2$, we have four possible choices of subgroups:
1) Pick for G_1 and G_2 any two subgroups of order 4, then $H(X_1) = \log 2,\ H(X_2) = \log 2,\ H(X_1, X_2) = \log 4$, which can obtained from the Klein group, as in (2).
2) Pick alternatively for G_1 and G_2 any two of the subgroups of order 2, yielding $H(X_1) = \log 4,\ H(X_2) = \log 4,\ H(X_1, X_2) = \log 8$, which corresponds to the Abelian group $C_2 \times C_2 \times C_2$ (see Fig. 3) by choosing $G_1 = C_2 \times \{1\} \times \{1\},\ G_2 = \{1\} \times C_2 \times \{1\},\ G_1 \cap G_2 = \{1\}$.
3) By combining one subgroup G_2 of order 4 with one subgroup G_1 of order 2, with $G_1 \subset G_2$, results in $H(X_1) = \log 4,\ H(X_2) = \log 2,\ H(X_1, X_2) = \log 4$ which can be seen as coming from the Abelian group $C_2 \times C_4$ (see Fig. 3) where $G_1 = \{1\} \times C_2,\ G_2 = \{1\} \times C_4,\ G_1 \cap G_2 = \{1\} \times C_2$.
4) Finally we can have G_2 of order 4, G_1 of order 2, with trivial intersection: $H(X_1) = \log 4,\ H(X_2) = \log 2,\ H(X_1, X_2) = \log 8$, which can again be obtained from $C_2 \times C_4$ with this time $G_1 = \{1\} \times C_2,\ G_2 = C_4 \times \{1\},\ G_1 \cap G_2 = \{1\}$.

In summary:

Proposition 3: Consider $n = 2$ quasi-uniform random variables. The two non-Abelian groups of order 8 induce entropic vectors that can be obtained from Abelian groups.

The above result shows that it should not be taken for granted that any non-Abelian group will provide richer entropic vectors. In order to see if any generality can be derived from these two examples, we now focus on dihedral groups.

B. Dihedral Groups

The dihedral group D_8 of order 8 does not give new entropic vectors for $n = 2$ random variables, as shown above. It is natural to wonder whether this is true for dihedral groups in general. Computations in the case of D_6 (see Fig. 4) show that the answer is no, namely we cannot find an Abelian group yielding the same entropic vectors as D_6. This leads to distinguish the order $2m$ of dihedral groups. It is known that the subgroup structure of a general dihedral group

$$D_{2m} = \langle r, s | r^m = s^2 = 1, rs = sr^{-1}\rangle$$

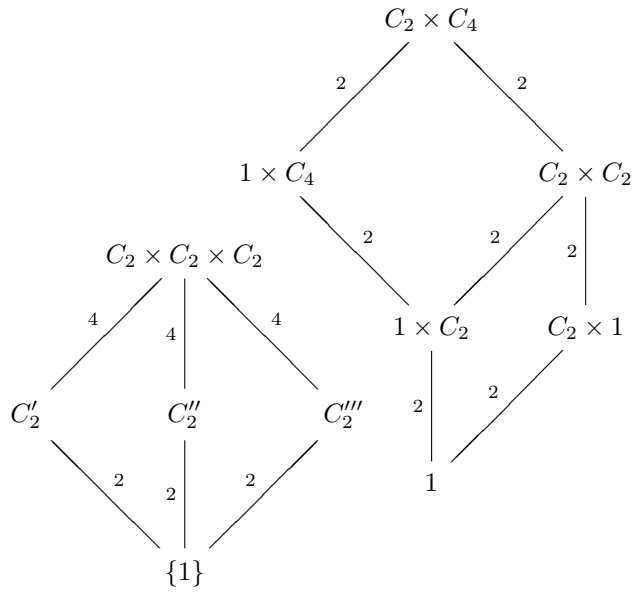

Fig. 3. When $n = 2$, the Abelian groups $C_2 \times C_4$ and $C_2 \times C_2 \times C_2$ provide the same entropic vectors as D_8. The three subgroups of $C_2 \times C_2 \times C_2$ are $C_2' \simeq C_2 \times \{1\} \times \{1\}$, $C_2' \simeq \{1\} \times C_2 \times \{1\}$ and $C_2''' = \{1\} \times \{1\} \times C_2$.

differs depending on the parity of m. We can indeed show the following general result when m is odd:

Proposition 4: Let m be an odd positive integer. The dihedral group D_{2m} induces entropic vectors for $n = 2$ random variables which cannot be obtained from an Abelian group.

Proof: Take $G_1 = \langle s\rangle$ and $G_2 = \langle rs\rangle$ in D_{2m}. Then

$$[G : G_1] = [G : G_2] = m,\ [G : G_1 \cap G_2] = 2m.$$

To prove our claim, we have to show that there does not exist any Abelian group H and subgroups H_1 and H_2 such that

$$[H : H_1] = [H : H_2] = m,\ [H : H_1 \cap H_2] = 2m.$$

If such a group H exists, then $|H| = 2m|H_1 \cap H_2| = 2mk$, where $k = |H_1 \cap H_2| = 2^l k'$, k' odd. This implies that

$$|H_1| = |H_2| = \frac{|H|}{m} = 2k = 2^{l+1}k'$$

and it follows from Theorem 2 that H_1 and H_2 are isomorphic to one of the following groups: $C_{2^{l+1}k'}$, $C_2 \times C_{2^l k'}$, $C_4 \times C_{2^{l-1}k'}$, $C_2 \times C_2 \times C_{2^{l-1}k'}, \ldots$. Without loss of generality suppose that

$$\begin{aligned} H_1 &= C_{2^{i_1}} \times C_{2^{i_2}} \times \ldots \times C_{2^{i_{p-1}}} \times C_{2^{i_p}k'} \\ H_2 &= C_{2^{j_1}} \times C_{2^{j_2}} \times \ldots \times C_{2^{j_{q-1}}} \times C_{2^{j_q}k'}, \end{aligned}$$

where $i_1 + \ldots + i_p = l + 1 = j_1 + \ldots + j_q$ and each i_s, j_r are nonnegative integers. We can add $p - q$ components of $\{1\} \times \ldots \times \{1\}$ at the end of H_2 if $p > q$ and vice-versa.

Now we need to construct an Abelian group H that contains both H_1 and H_2. By looking componentwise at H_1 and H_2, we see that if $C_{2^{i_s}} = C_{2^{j_s}}$, then H must have as sth component a group that contains $C_{2^{i_s}}$, and if $C_{2^{i_s}} \neq C_{2^{j_s}}$, then this time the sth component of H will contain $C_{2^{\max\{i_s, j_s\}}}$.

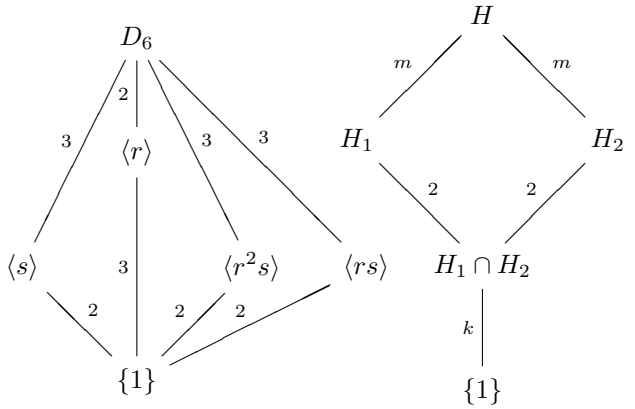

Fig. 4. On the left, the dihedral group D_6 and its lattice of subgroups. On the right, the structure that an Abelian group H should satisfy to give the same entropic vectors as D_{2m}, m odd.

Since $H_1 \neq H_2$, note that there are at least two components say s and r which are different. Indeed, let us assume that there is one such component, say the sth one in H_1, the condition $|H_1| = |H_2|$ forces to have another such component, the rth one in H_2 to compensate. Therefore the sth and rth components of H are of order at least $2^{\max\{i_s,j_s\}} \geq 2$ and $2^{\max\{i_r,j_r\}} \geq 2$ respectively. Hence, for $i = 1, 2$

$$2^t |H_i| \mid |H|,\ t \geq 1 \Rightarrow 2^t \mid m = [H : H_i] = \frac{|H|}{|H_i|},$$

which contradicts the assumption that m is odd. ∎

Corollary 1: If $2m$ is not a power of 2, the dihedral group D_{2m} induces entropic vectors for $n = 2$ random variables which cannot be obtained from an Abelian group.

Proof: The subgroup structure of the dihedral group D_{2m} is well known: it possesses dihedral subgroups $\langle r^d, r^f s \rangle$ with d divides m and $0 \leq f < d$ of order $2m/d$. Thus whenever $2m/d = 2m'$ with m' odd, the dihedral group D_{2m} contains as subgroup the dihedral group $D_{2m'}$, with m' odd. This does not happen only when $2m$ is a power of 2. Note however that the entropic vectors from $D_{2m'}$ which are not Abelian group representable cannot serve for D_{2m} since their indices are different in $D_{2m'}$ and D_{2m}.

Consider the subgroups $G_1 = \langle rs \rangle$ and $G_2 = \langle r^{m'}, s \rangle$ of D_{2m} of indices $[G : G_1] = m = 2^{n-1}m',\ n \geq 2$ and $[G : G_2] = m'$, odd, respectively having trivial intersection, that is $[G : G_1 \cap G_2] = 2m$.

We show that there does not exist any Abelian group H and subgroups H_1 and H_2 such that $[H : H_1] = m$, $[H : H_2] = m'$ and $[H : H_1 \cap H_2] = 2m$. If such a group H exists, then $|H| = 2m|H_1 \cap H_2| = 2^n m' k = 2^{n+l} m' k'$, where $k = 2^l k' = |H_1 \cap H_2|, k'$ odd. This implies $|H_1| = 2^{l+1} k'$, $|H_2| = 2^{n+l} k'$. Then H_1 is isomorphic to one of the group $C_{2^{l+1}k'},\ C_2 \times C_{2^l k'},\ C_4 \times C_{2^{l-1}k'},\ C_2 \times C_2 \times C_{2^{l-1}k'}, C_2 \times C_{2k'_1} \times C_{2^{l-1}k'_2} \ldots$; where $k'_1 k'_2 = k'$ and H_2 is isomorphic to one among $C_{2^{n+l}k'},\ C_2 \times C_{2^{n+l-1}k'},\ C_4 \times C_{2^{n+l-2}k'},\ C_2 \times C_2 \times C_{2^{n+l-2}k'}, C_2 \times C_{2k'_1} \times C_{2^{n+l-2}k'_2} \ldots$.

Without loss of generality assume that

$$H_1 = C_{2^{i_1}} \times C_{2^{i_2}} \times \ldots \times C_{2^{i_{p-1}}} \times C_{2^{i_p}k'}$$

and

$$H_2 = C_{2^{j_1}} \times C_{2^{j_2}} \times \ldots \times C_{2^{j_{q-1}}} \times C_{2^{j_q}k'};$$

where $i_1 + \ldots + i_p = l + 1$ and $j_1 + \ldots + j_q = n + l$. Since $n \geq 2$, $|H_2| = 2^f |H_1|, f \geq 1$. This implies that there exists a component t such that $2^{\max\{i_t,j_t\}} = 2^{j_t}$. Since $|H_1 \cap H_2| < |H_1|$, there exists a component u such that $2^{\max\{i_u,j_u\}} = 2^{i_u}$. Then $2^v |H_2| \| |H|,\ v \geq 1$ implies $2^v | m'$, a contradiction using a similar argument as above. ∎

V. Conclusion

In this note, we looked at quasi-uniform distributions from a group theory point of view. After observing a few simple properties of Abelian groups in terms of their corresponding entropic vectors, we studied a few non-Abelian groups of small orders, as well as dihedral groups, to determine when non-Abelian groups induce entropic vectors that cannot be obtained from Abelian groups. This opens a series of questions, for example: (1) since Abelian groups are classified, is there some classification of entropic vectors generated by Abelian groups? (2) the same question can be asked for families of non-Abelian groups, it would be good to at least determine entropic vectors that cannot be obtained from Abelian groups. (3) This works shows a special behaviour for D_8 and Q_8: is there something special related to the structure of 2-groups? or maybe more generally of p-groups? Finally, once these connections will be better understand, an important open question is the design of explicit codes out of groups.

Acknowledgement

The work is supported by the Nanyang Technological University under Research Grant M58110049.

References

[1] T.H. Chan, "Aspects of Information Inequalities and its Applications", M.Phil Thesis, Dept. of Information Enginering, The Chinese University of Hong Kong, September 1998.

[2] T. H. Chan, "Group characterizable entropy functions," *2007 IEEE International Symposium on Information Theory (ISIT 2007)*, Nice, France, 24-29 June 2007.

[3] T. H. Chan and R. W. Yeung, "On a relation between information inequalities and group theory,"*IEEE Trans. on Information Theory*, Vol. 48, pp.1992-1995, July 2002.

[4] Wei Mao and B. Hassibi, "Violating the Ingleton inequality with finite groups", *47th Annual Allerton Conference on Communication, Control, and Computing*, 2009.

[5] T.H. Chan, A. Grant and T. Britz, "Properties of quasi-uniform codes", *2010 IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, 13-18 June 2010.

[6] T. H. Chan and A. Grant, "On Capacity regions of non-multicast networks", *2010 IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, 13-18 June 2010.

[7] J. Simonis and A. Ashikhmin, "Almost affine codes", *Designs, Codes and Cryptography*, vol. 14, no. 2, 1998.

[8] A. Ingleton, "Representation of matroids," *Combinatorial Mathematics and its Applications*, 1971.