Finite nilpotent and metacyclic groups never violate the Ingleton inequality

Stancu, Radu; Oggier, Frederique

2012

Stancu, R., & Oggier, F. (2012). Finite nilpotent and metacyclic groups never violate the Ingleton inequality. 2012 International Symposium on Network Coding (NetCod), pp.25- 30.

<https://hdl.handle.net/10356/94796>

<https://doi.org/10.1109/NETCOD.2012.6261879>

© 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [DOI: <http://dx.doi.org/10.1109/NETCOD.2012.6261879>].

Downloaded on 26 Apr 2023 22:05:54 SGT

Finite Nilpotent and Metacyclic Groups never violate the Ingleton Inequality

Radu Stancu
CNRS UMR 6140 - LAMFA
Université de Picardie
Amiens, France
Email: radu.stancu@u-picardie.fr

Frédérique Oggier
Division of Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

Abstract—In [5], Mao and Hassibi started the study of finite groups that violate the Ingleton inequality. They found through computer search that the smallest group that does violate it is the symmetric group of order 120. We give a general condition that proves that a group does not violate the Ingleton inequality, and consequently deduce that finite nilpotent and metacyclic groups never violate the inequality. In particular, out of the groups of order up to 120, we give a proof that about 100 orders cannot provide groups which violate the Ingleton inequality.

I. INTRODUCTION

The work of [1] revealed a surprising connection between two unexpected topics: information theory and group theory.

Set $\mathcal{N} = \{1, \dots, n\}$ and let $X_1, \dots, X_n$ be n jointly distributed discrete random variables. For any non-empty set $\mathcal{A} \subseteq \mathcal{N}$, we denote by $X_{\mathcal{A}}$ the collection of random variables $\{X_i, i \in \mathcal{A}\}$, and by $H(X_{\mathcal{A}})$ its joint entropy. The ordered $2^n - 1$ -dimensional vector $h_{\mathcal{A}}$, where $\mathcal{A}$ runs through every non-empty subset of $\mathcal{N}$, is called an entropy vector. The set of all possible entropy vectors is denoted by Γ_n^* , and its closure by $\bar{\Gamma}_n^*$. Determining $\bar{\Gamma}_n^*$ is of importance in network information theory, since it can be shown [2], [3] that the capacity region of any arbitrary multi-source multi-sink wired acyclic network whose edges are discrete memoryless channels can be obtained through optimizing a linear function of the entropy vector over $\bar{\Gamma}_n^*$. The problem of characterizing entropy vectors is notoriously difficult. In fact, only $\bar{\Gamma}_2^*$ and $\bar{\Gamma}_3^*$ are known. The case of $n = 4$ random variable remains open.

Let now G be a finite group, and let $G_1, \dots, G_n$ be n of its subgroups. For any non-empty set $\mathcal{A} \subseteq \mathcal{N}$, consider the subgroup

$$G_{\mathcal{A}} = \cap_{i \in \mathcal{A}} G_i$$

of G . Define $g_{\mathcal{A}} = \log \frac{|G|}{|G_{\mathcal{A}}|}$, where $|G|$ denotes the order (cardinality) of the group G . The ordered $2^n - 1$ -dimensional vector $g_{\mathcal{A}}$, where $\mathcal{A}$ again runs through every non-empty subset of $\mathcal{N}$ is called a group characterizable vector. Let Υ_n denote the set of all group characterizable vectors derived from n subgroups of a finite group G .

It was shown in [4] that every group characterizable vector is an entropy vector, whereas every entropy vector is arbitrarily close to a scaled version of some group characterizable vector. The proof that every group characterizable is an entropy vector is not difficult: let a be a random variable uniformly distributed

on G . Define the new random variable $X_i = aG_i$, that is the left coset of a with respect to G_i . Then [1] states that $h_{\mathcal{A}} = \log \frac{|G|}{|G_{\mathcal{A}}|} = g_{\mathcal{A}}$.

The Ingleton inequality [6] comes from matroid theory, and can be in particular stated in the context of entropy vectors as

$$\begin{aligned} H(X_{12}) + H(X_{13}) + H(X_{14}) + H(X_{23}) + H(X_{24}) \geq \\ H(X_1) + H(X_2) + H(X_{34}) + H(X_{123}) + H(X_{124}). \end{aligned} \quad (1)$$

It is known that there exist entropy vectors which violate this inequality. If G is a finite group, with subgroups G_i, G_j, G_k , recall that $G_{ij} = G_i \cap G_j$ and $G_{ijk} = G_i \cap G_j \cap G_k$ are subgroups of G , and that

$$\begin{aligned} H(X_{ij}) &= H(X_i, X_j) = \log \frac{|G|}{|G_{ij}|}, \\ H(X_{ijk}) &= H(X_i, X_j, X_k) = \log \frac{|G|}{|G_{ijk}|} \end{aligned}$$

allowing to rewrite (1) as

$$|G_1||G_2||G_{34}||G_{123}||G_{124}| \geq |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|. \quad (2)$$

We will say in short that a group violates the Ingleton inequality if it contains subgroups $G_1, \dots, G_4$ such that (2) does not hold, and that it does not violate the Ingleton inequality otherwise. A family of groups is said never to violate the Ingleton inequality when there exist no group in this family which violates the Ingleton inequality. It was shown in [5] through exhaustive search that the smallest group that violates (2) is the symmetric group S_5 , of order $|S_5| = 120$. In fact, S_5 is isomorphic to the projective general linear group $PGL(2, 5)$ and $PGL(2, p)$, $p \geq 5$ is the first family of groups known to violate the Ingleton inequality.

The contribution of this work is to derive a general condition that shows that a finite group does not violate the Ingleton inequality, and as corollary, we show that finite nilpotent and metacyclic groups never violate the inequality. In particular, we give a partial proof of the numerical search of [5], by showing that our method excludes about 100 orders smaller than 120, where all the groups always satisfy the inequality.

We start by discussing some known negative conditions, as well as providing some new ones, before proving our

main result in Section III. The consequences are discussed in Section IV.

II. NEGATIVE CONDITIONS FOR THE INGLETON INEQUALITY

Let G be a finite group with subgroups $G_1, \dots, G_n$. We will use the notation $H \leq G$ to say that H is a subgroup of G , and $|G|$ to denote the cardinality (or order) of the group G .

To help decide whether a group violates the Ingletton inequality, it is useful to have negative conditions, that is conditions under which a group satisfies (2). We summarize below the known negative conditions:

- 1) G is Abelian (or commutative) [1].
- 2) The G_i are normal in G , written $G_i \trianglelefteq G$ for all i [7].
- 3) $G_1 G_2 = G_2 G_1$ or equivalently $G_1 G_2 \leq G$ [5].
- 4) $G_i = 1$ or G for some i [5].
- 5) $G_i = G_j$ for some $i \neq j$ [5].
- 6) $G_{12} = 1$ [5].
- 7) $G_i \leq G_j$ for some $i \neq j$ [5].

Using the following straightforward lemma, we add some more negative conditions and give a group theoretic proof of some of the known conditions. The reader may be more comfortable with either the information theoretic or group theoretic language. In this paper we adopt the latter.

Lemma 1: If G is a finite group and K, H are subgroups of G then $|G||H \cap K| \geq |H||K|$.

Proof: We construct a map $f : H \times K \rightarrow G$ defined by $f(h, k) = hk$. We have that $hk = h'k'$ if and only if $kk'^{-1} = h^{-1}h' \in H \cap K$. Hence $|f(H \times K)| = \frac{|H||K|}{|H \cap K|}$ and the lemma follows. ■

Note that this lemma has an equivalent information theoretic formulation¹. Indeed

$$\begin{aligned}
& |G||H \cap K| \geq |H||K| \\
\iff & \log |G| + \log |H \cap K| \geq \log |H| + \log |K| \\
\iff & \log |H \cap K| - \log |G| \geq \log |H| - \log |G| + \\
& \log |K| - \log |G| \\
\iff & -\log |H \cap K| + \log |G| \leq -\log |H| + \log |G| \\
& -\log |K| + \log |G| \\
\iff & \log \frac{|G|}{|H \cap K|} \leq \log \frac{|G|}{|H|} + \log \frac{|G|}{|K|}
\end{aligned}$$

which can be rewritten as saying that the mutual information $I(X; Y)$ satisfies

$$I(X; Y) = H(X) + H(Y) - H(X, Y) \geq 0$$

by associating to the subgroups the corresponding random variables.

Corollary 1: If $G_{12}, G_{13}, G_{14}, G_{23}$, or G_{24} is 1, then G does not violate the Ingletton inequality.

Proof: Suppose that $G_{12} = 1$, so that (2) becomes

$$|G_1||G_2||G_{34}| \geq |G_{13}||G_{14}||G_{23}||G_{24}|. \quad (3)$$

¹We would like to thank the reviewer who pointed this out.

Using Lemma 1 with $G = G_1, H = G_{13}$ and $K = G_{14}$, we get $|G_1||G_{134}| \geq |G_{13}||G_{14}|$. The same lemma with $G = G_2, H = G_{23}$ and $K = G_{24}$ gives $|G_2||G_{234}| \geq |G_{23}||G_{24}|$. Hence (3) is implied by $|G_{34}| \geq |G_{134}||G_{234}|$. This last inequality is obtained from Lemma 1 with $G = G_{34}, H = G_{134}, K = G_{234}$ and the fact that $G_{134} \cap G_{234} \leq G_{12} = 1$.

Suppose that $G_{13} = 1$, so that (2) then becomes

$$|G_1||G_2||G_{34}||G_{124}| \geq |G_{12}||G_{14}||G_{23}||G_{24}|. \quad (4)$$

Lemma 1 with $G = G_1, H = G_{12}$ and $K = G_{14}$ yields $|G_1||G_{124}| \geq |G_{12}||G_{14}|$. The same lemma with $G = G_2, H = G_{23}$ and $K = G_{24}$ gives $|G_2||G_{234}| \geq |G_{23}||G_{24}|$. Hence (4) is implied by $|G_{34}| \geq |G_{234}|$, which is straightforward. The cases $G_{14} = 1, G_{23} = 1$ and $G_{24} = 1$ are treated similarly. ■

Note that it is not true that $G_{34} = 1$ implies that G does not violate the Ingletton inequality. In fact, the group S_5 gives such a counter-example [5]. Below can be found some group theoretic proofs of some of the known negative conditions.

Corollary 2: If $G_i = 1$, for some i , then G does not violate the Ingletton inequality.

Proof: If $G_1 = 1$ the Ingletton inequality becomes

$$|G_2||G_{34}| \geq |G_{23}||G_{24}|. \quad (5)$$

Applying Lemma 1 with $G = G_2, H = G_{23}$ and $K = G_{24}$, we get $|G_2||G_{234}| \geq |G_{23}||G_{24}|$, and (5) follows from $|G_{34}| \geq |G_{234}|$. The case $G_2 = 1$ is treated similarly.

Suppose that $G_3 = 1$. The Ingletton inequality is now

$$|G_1||G_2||G_{124}| \geq |G_{12}||G_{14}||G_{24}|. \quad (6)$$

Applying Lemma 1 with $G = G_1, H = G_{12}$ and $K = G_{14}$, we get $|G_1||G_{124}| \geq |G_{12}||G_{14}|$, and (6) follows from $|G_2| \geq |G_{24}|$. The case $G_4 = 1$ is treated similarly. ■

Corollary 3: If $G_i \leq G_j$ for some $i \neq j$, then G does not violate the Ingletton inequality.

Proof: If $G_1 \leq G_2$, then the Ingletton inequality becomes

$$|G_1||G_2||G_{34}||G_{13}||G_{14}| \geq |G_1||G_{13}||G_{14}||G_{23}||G_{24}|,$$

that is $|G_2||G_{34}| \geq |G_{23}||G_{24}|$, already treated in (5). The case $G_2 \leq G_1$ is treated similarly.

If $G_1 \leq G_3$, then the Ingletton inequality is equivalent to

$$|G_1||G_2||G_{34}||G_{12}||G_{124}| \geq |G_{12}||G_1||G_{14}||G_{23}||G_{24}|,$$

that is

$$|G_2||G_{34}||G_{124}| \geq |G_{14}||G_{23}||G_{24}|. \quad (7)$$

Lemma 1 with $G = G_2, H = G_{23}$ and $K = G_{24}$ gives $|G_{14}||G_2||G_{234}| \geq |G_{14}||G_{23}||G_{24}|$, and (7) is implied by

$$|G_{34}||G_{124}| \geq |G_{14}||G_{234}|.$$

This last inequality comes from Lemma 1. The cases $G_1 \leq G_4, G_2 \leq G_3$ and $G_2 \leq G_4$ are treated similarly.

If $G_3 \leq G_1$, then the Ingletton inequality is equivalent to

$$|G_1||G_2||G_{34}||G_{23}||G_{124}| \geq |G_{12}||G_3||G_{14}||G_{23}||G_{24}|,$$

which in turn is equivalent to

$$|G_1||G_2||G_{34}||G_{124}| \geq |G_{12}||G_3||G_{14}||G_{24}|. \quad (8)$$

Using Lemma 1 with $G = G_2$, $H = G_{12}$ and $K = G_{24}$ we get that (8) is then implied by

$$|G_1||G_{34}| \geq |G_3||G_{14}|.$$

Again this last inequality comes from Lemma 1. The cases $G_4 \leq G_1$, $G_3 \leq G_2$ and $G_4 \leq G_2$ are treated similarly.

The last case is $G_3 \leq G_4$ (or, similarly $G_4 \leq G_3$). In this case the Ingleton inequality is equivalent to

$$|G_1||G_2||G_3||G_{123}||G_{124}| \geq |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|. \quad (9)$$

Using Lemma 1 with $G = G_3$, $H = G_{13}$ and $K = G_{23}$ we get that (9) is then implied by

$$|G_1||G_2||G_{124}| \geq |G_{12}||G_{14}||G_{24}|.$$

Using Lemma 1 with $G = G_2$, $H = G_{12}$ and $K = G_{24}$ we get that (9) is in turn implied by $|G_1| \geq |G_{14}|$ and this last inequality is clearly true. ■

III. NILPOTENT AND METACYCLIC GROUPS

Recall that $K \trianglelefteq G$ means that K is a normal subgroup of G , and it implies that the set G/K of cosets of K in G is in fact a group, called quotient group.

Lemma 2: Let G be a finite group, with subgroups H and $K \trianglelefteq G$ with $|K| = p$, p a prime. Let

$$\begin{aligned} \pi : G &\rightarrow G/K \\ g &\mapsto gK \end{aligned}$$

denote the canonical projection. Then $\pi(H)$ is a subgroup of G/K and

$$\pi(H) \simeq H/(K \cap H).$$

Consequently, if K is a subgroup of H , then $|\pi(H)| = |H|/|K|$, else $|\pi(H)| = |H|$.

Proof: The restriction $\pi|_H$ of π to H is a group homomorphism, with kernel $H \cap K$. By the first isomorphism theorem $\pi(H) \simeq H/(K \cap H)$.

Suppose that K is a subgroup of H , then

$$|\pi(H)| = \frac{|H|}{|K|}.$$

Now $K \cap H$ is a subgroup of K whose order is p , thus $|K \cap H|$ is either 1 or p . It cannot be p when K is not a subgroup of H , thus it is one, which concludes the proof. ■

We first prove a general result.

Theorem 1: Let G be a finite group, having a normal subgroup Z of prime order p . Suppose that G/Z does not violate the Ingleton inequality. Then G does not violate the Ingleton inequality either.

Proof: Let Z be a normal subgroup of G of prime order p . Let $\pi : G \rightarrow G/Z$ be the canonical projection. By assumption, we have that

$$|\pi(G_1)||\pi(G_2)||\pi(G_{34})||\pi(G_{123})||\pi(G_{124})| \geq |\pi(G_{12})||\pi(G_{13})||\pi(G_{14})||\pi(G_{23})||\pi(G_{24})| \quad (10)$$

holds. Using this, we prove in the following that the Ingleton inequality (2) holds. We consider five cases.

Case I. Z is contained in none of the subgroups G_{12} , G_{13} , G_{14} , G_{23} , G_{24} : then

$$\begin{aligned} |\pi(G_{12})||\pi(G_{13})||\pi(G_{14})||\pi(G_{23})||\pi(G_{24})| \\ = |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}| \end{aligned}$$

by Lemma 2, while

$$\begin{aligned} |G_1||G_2||G_{34}||G_{123}||G_{124}| \\ \geq |\pi(G_1)||\pi(G_2)||\pi(G_{34})||\pi(G_{123})||\pi(G_{124})| \end{aligned}$$

which combined with (10) shows that the Ingleton inequality holds.

Case II. Z is contained in exactly one group among G_{12} , G_{13} , G_{14} , G_{23} , G_{24} , i.e., Z is contained in exactly two groups G_i , G_j with $i \neq j$ and $\{i, j\} \neq \{3, 4\}$:

- if $Z \leq G_{12}$, then $Z \leq G_1$ and $Z \leq G_2$, but $Z \not\leq G_3$ and $Z \not\leq G_4$ (otherwise Z would also be contained in G_{13} and G_{14}). By Lemma 2, $|\pi(G_{12})| = |G_{12}|/|Z| = |G_{12}|/p$, repeating this same argument for G_1 and G_2 , we get

$$\begin{aligned} |\pi(G_1)||\pi(G_2)||\pi(G_{34})||\pi(G_{123})||\pi(G_{124})| \\ = \frac{|G_1||G_2||G_{34}||G_{123}||G_{124}|}{p^2} \end{aligned}$$

and

$$\begin{aligned} |\pi(G_{12})||\pi(G_{13})||\pi(G_{14})||\pi(G_{23})||\pi(G_{24})| \\ = \frac{|G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|}{p}. \end{aligned}$$

Together with (10), this shows that Ingleton inequality holds.

- Now it could be that $Z \leq G_{13}$ (or similarly G_{14} , G_{24} , G_{23}), then $Z \leq G_1$ and $Z \leq G_3$, but $Z \not\leq G_2$ and $Z \not\leq G_4$. Repeating the above computation, we have

$$\begin{aligned} |\pi(G_1)||\pi(G_2)||\pi(G_{34})||\pi(G_{123})||\pi(G_{124})| \\ = \frac{|G_1||G_2||G_{34}||G_{123}||G_{124}|}{p} \end{aligned}$$

and

$$\begin{aligned} |\pi(G_{12})||\pi(G_{13})||\pi(G_{14})||\pi(G_{23})||\pi(G_{24})| \\ = \frac{|G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|}{p}, \end{aligned}$$

which yields the same conclusion.

Case III. Z is contained in exactly two groups among G_{12} , G_{13} , G_{14} , G_{23} , G_{24} : there are 10 possibilities of choosing two groups among these four; but there are only two possibilities for Z to be contained in exactly two groups among the above, namely (G_{13}, G_{14}) and (G_{23}, G_{24}) , which can be treated similarly.

Suppose that one of these groups is G_{13} and the other is G_{14} . Then $Z \leq G_1$, $Z \leq G_3$, $Z \leq G_4$, and $Z \not\leq G_2$, so that we have

$$\begin{aligned} |\pi(G_1)||\pi(G_2)||\pi(G_{34})||\pi(G_{123})||\pi(G_{124})| \\ = \frac{|G_1||G_2||G_{34}||G_{123}||G_{124}|}{p^2} \end{aligned}$$

and

$$\begin{aligned} |\pi(G_{12})||\pi(G_{13})||\pi(G_{14})||\pi(G_{23})||\pi(G_{24})| \\ = \frac{|G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|}{p^2}, \end{aligned}$$

with again the same conclusion.

Case IV. If Z is contained in exactly 3 groups among $G_{12}, G_{13}, G_{14}, G_{23}, G_{24}$, we get triples (G_{ij}, G_{ik}, G_{jk}) with $\{i, j, k\} = \{1, 2, 3\}$ or $\{i, j, k\} = \{1, 2, 4\}$.

Suppose that $\{i, j, l\} = \{1, 2, 3\}$. Then $Z \leq G_1$, $Z \leq G_2$, $Z \leq G_3$, and $Z \not\leq G_4$, so that we have

$$\begin{aligned} |\pi(G_1)| |\pi(G_2)| |\pi(G_3)| |\pi(G_{123})| |\pi(G_{124})| \\ = \frac{|G_1| |G_2| |G_3| |G_{123}| |G_{124}|}{p^3} \end{aligned}$$

and

$$\begin{aligned} |\pi(G_{12})| |\pi(G_{13})| |\pi(G_{14})| |\pi(G_{23})| |\pi(G_{24})| \\ = \frac{|G_{12}| |G_{13}| |G_{14}| |G_{23}| |G_{24}|}{p^3}, \end{aligned}$$

bringing us to the same conclusion.

Case V. It remains to treat the case Z is contained in all the G_i 's, hence in all subgroups on both sides of 2, and then we have:

$$\begin{aligned} |\pi(G_1)| |\pi(G_2)| |\pi(G_3)| |\pi(G_{123})| |\pi(G_{124})| \\ = \frac{|G_1| |G_2| |G_3| |G_{123}| |G_{124}|}{p^5} \end{aligned}$$

and

$$\begin{aligned} |\pi(G_{12})| |\pi(G_{13})| |\pi(G_{14})| |\pi(G_{23})| |\pi(G_{24})| \\ = \frac{|G_{12}| |G_{13}| |G_{14}| |G_{23}| |G_{24}|}{p^5}, \end{aligned}$$

which concludes the proof of the claim that if (10) holds, then (2) holds for G . ■

As a consequence of the previous theorem we get

Theorem 2: Let G be a finite group, having a normal cyclic subgroup C . Suppose that G/C does not violate the Ingleton inequality. Then G does not violate the Ingleton inequality either.

Proof: We proceed by induction on the order of C . If C is of prime order p then this is Theorem 1. If not, C has a unique subgroup D of order p , for p a prime number dividing $|C|$. Hence, D is a normal subgroup of G . Then G/D has a cyclic normal subgroup which is C/D . Also, $(G/D)/(C/D)$ is isomorphic to G/C and does not violate the Ingleton inequality. By induction, as the order of C/D is strictly smaller than the order of C , we have that G/D does not violate the Ingleton inequality. Now apply Theorem 1 and get that G does not violate the Ingleton inequality either. ■

We now show that nilpotent groups fall into the category of groups described in the previous theorem.

Definition 1: A group G is nilpotent if it has a normal series (called central series)

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1,$$

where

$$G_i/G_{i+1} \leq Z(G/G_{i+1}).$$

Note that $G_{i+1} \trianglelefteq G$ for every i for $Z(G/G_{i+1})$ to make sense, that is for G/G_{i+1} to form a group, where $Z(G)$ denotes the center of G , that is the subgroup of G of elements that commute with every element in the group.

We observe from the definition that nilpotent groups have nontrivial centers since

$$G_{n-1} \leq Z(G).$$

So there exists a prime p such that $p \mid |Z(G)|$. By Cauchy Theorem, there exists a cyclic subgroup C of $Z(G)$ of order $|C| = p$. Then C is in turn a normal subgroup of G , as it is central.

Theorem 3: A finite nilpotent group never violates the Ingleton inequality.

Proof: If G is nilpotent, it has a normal cyclic subgroup C . Again we use induction on the order of G . If $G = C$ then we are in the case on Theorem 1 with $G/C = 1$. So G does not violate the Ingleton inequality. Otherwise, G/C is still nilpotent of order strictly inferior than the order of G . By induction, G/C does not violate the Ingleton inequality, and, by Theorem 1 we have the same for G . ■

Let p be a prime number. Recall that a p -group is a group with the property that the order of any group element is a power of p . The following result follows from well-known facts from group theory, they are recalled here for the sake of completeness.

Corollary 4: Abelian groups and p -groups do not violate the Ingleton inequality.

Proof: A central series for Abelian groups is simply given by

$$G = G_0 \geq G_1 = 1$$

since

$$G_0/G_1 \leq Z(G).$$

Thus they are nilpotent. For a p -group, we can construct a central series $G_{n-k} = Z^k(G)$ as follows. First $1 = Z^0(G) = G_n$, then $Z^1(G) = Z(G) > 1$ since G is a p -group. Given $Z^k(G)$, let $Z^{k+1}(G)$ be the subgroup of G which contains $Z^k(G)$ and corresponds to the center $G/Z^k(G)$, i.e., so that $Z^{k+1}(G)/Z^k(G) = Z(G/Z^k(G))$. Since $G/Z^k(G)$ is a p -group, it has a nontrivial center, making $Z^{k+1}(G) > Z^k(G)$ unless $Z^k(G) = G$. Since G is finite, we must have $Z^n(G) = G$ for some n . Finite p -groups are then nilpotent. We are thus done by Theorem 3. ■

We now consider metacyclic groups.

Definition 2: A metacyclic group is a group M having a cyclic normal subgroup C , such that the quotient M/C is also cyclic.

Theorem 4: Metacyclic groups do not violate Ingleton inequality.

Proof: We have that M is metacyclic if and only if M has a normal subgroup C such that M/C is cyclic. We conclude using Theorem 2 and the fact that any cyclic group does not violate the Ingleton inequality, by Corollary 4. ■

Remark that Theorem 4 is not a consequence of Theorem 3 as not all metacyclic groups are nilpotent. For example, dihedral groups D_{2n}

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

where n is not a power of 2 are not nilpotent, but they are metacyclic.

Recall that a Sylow p -subgroup is a maximal p -subgroup. The Sylow Theorems tell us that (1) a Sylow p -subgroup always exists if p divides the order n of the group, (2) the

number n_p of Sylow p -subgroups is congruent to 1 modulo p , and (3) n_p divides n' where $n = n'p^r$ for the maximal $r \geq 1$. The Sylow Theorems are explained in about every book that deals with group theory.

Theorem 5: Any group G of order $p_1p_2\dots p_r$, where the p_i 's are distinct prime numbers, and any divisor of $p_1p_2\dots p_i$ is not 1 modulo p_{i+1} , for all $1 \leq i < r$, does not violate Ingleton inequality.

Proof: We use again induction on r . If $r = 1$ then G is cyclic and it does not violate the Ingleton inequality by Corollary 4. Otherwise, let $p = p_r$ and P be a Sylow p -subgroup of G , which is necessarily a cyclic group of order p . Then, by Sylow Theorems, P is a normal subgroup of order p of G , given that divisors of $p_1p_2\dots p_{r-1}$ are not 1 modulo p_r . Also, G/P has order $p_1p_2\dots p_{r-1}$, hence, by induction, it does not violate the Ingleton inequality. Using Theorem 1, we get that G does not violate the Ingleton inequality. ■

IV. CONSEQUENCES

Let us now use the above results to understand which groups of small order (smaller than 120) cannot violate the Ingleton inequality. Remark that numerical computations with GAP show that there are 1236 groups having order ranging from 2 to 120, among which 601 groups are not nilpotent. However we can be more precise.

Groups of some given orders, listed below, will never violate the Ingleton inequality:

- prime order p : these are only cyclic groups, thus Abelian groups.
- order $2p$, p prime: groups of order $2p$ are either cyclic groups or dihedral groups.
- order pq , p, q distinct primes: such a group is either cyclic, or a semi-direct product $C_p \rtimes C_q$.
- order p^m , p prime: these are p -groups.

This actually removes more than half the orders from 1 to 120. In particular the following orders are left:

12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 50, 52, 54, 56, 60
63, 66, 68, 70, 72, 75, 76, 78, 80, 84, 88, 90, 92, 96, 98, 99
100, 102, 104, 105, 108, 110, 112, 114, 116, 117

Consider a finite group of order n . Now suppose that $p|n$ but p^2 does not divide n . In this case, we can look at the Sylow p -subgroups of G , which will be cyclic of order p . If G has a unique Sylow p -subgroup, then it will be normal. The number n_p of Sylow p -subgroups satisfies $n_p \equiv 1 \pmod{p}$, and $n_p|n'$ where $n = n'p$. We compute some values below, for orders smaller than 120 only (and we do not repeat those values already removed earlier). Note in particular:

Lemma 3: If $n = n'p$, where p does not divide n' and any divisor of n' different from 1 is not congruent to 1 modulo p , then $n_p = 1$.

Proof: Indeed, $n_p|n'$ and n_p is congruent to 1 modulo p by Sylow's theorems. Using the hypothesis we get that $n_p = 1$. ■

Hence groups of order $n'p$ with n' and p satisfying the hypothesis in the lemma above never violate the Ingleton

inequality, provided that groups of order n' never violate the Ingleton inequality. Note that these cases are also different from Theorem 5 since they consider powers of the same prime in the decomposition of n .

- We do the case $p = 5$ in more details, which treats groups of order $n = 5n'$. If $p = 5$, the number n_5 of Sylow 5-subgroups is $n_5 = 5k + 1$ for some positive integer k . For n_5 to be 1, n_5 should not divide n' otherwise, that is n' should not be divisible by $5k + 1$, $k \geq 1$. Also 5 should not divide n' , to make sure that the size of the Sylow 5-subgroup is 5. We can have $n' = 2, 3, 4, 7, 8, 9, 13, 14, 17, 19, 21, 23$, among which primes have already been removed ($n = 5n'$ is then a product of two primes), letting $n' = 4, 8, 9, 14, 21$, for respectively $n = 20, 40, 45, 70, 110$. Now we already know that groups of orders 4, 8, 9, 14, 21 always satisfy the Ingleton inequality, thus we can conclude for groups of order 20, 40, 45, 70, 110 using Theorem 1, and the fact that a unique Sylow 5-subgroup means that it is normal.
- If $p = 7$, we can have $n' = 4, 6, 9, 10, 12$, in which case $n_7 = 1$, for respectively $n = 28, 42, 63, 70, 84$. However we cannot remove 84 now, since $84 = 7 \cdot 12$ and we first need to show that groups of order 12 never violate the Ingleton inequality to remove 84.
- If $p = 11$, we can have $n' = 4, 6, 8, 9, 10$, in which case $n_{11} = 1$, for respectively $n = 44, 66, 88, 99, 110$.
- If $p = 13$, we can have $n' = 4, 6, 8, 9$, in which case $n_{13} = 1$, for respectively $n = 52, 78, 104, 117$.
- If $p = 17$, we can have $n' = 4, 6$, in which case $n_{17} = 1$, for respectively $n = 68, 102$.
- If $p = 19$, we can have $n' = 4, 6$, in which case $n_{19} = 1$, for respectively $n = 76, 114$.
- Similarly $n_{23} = 1$ when $n = 4 \cdot 23 = 92$ and $n_{29} = 1$ when $n = 4 \cdot 29 = 116$.

We can thus update our list of orders where there might be groups which violate the Ingleton inequality:

12, 18, 24, 30, 36, 48, 50, 54, 56, 60
72, 75, 80, 84, 90, 96, 98, 100, 105, 108, 112

Note that we might be able to remove a few more orders by treating them case by case, however our goal was to remove orders systematically using the techniques developed above.

V. CONCLUSION

We considered the problem of finding groups that violate the Ingleton inequality by providing negative conditions, namely a general condition under which a finite group will always satisfy the inequality. We identified families of groups falling into this category, and gave a partial proof that the smallest group which does violate it is of order 120, by showing that about 100 orders have groups which always satisfy the inequality. Current and future work obviously involves completing the proof that no group of order less than 120 violates the inequality, as well as providing either further negative conditions, or new families of groups that do violate the

Ingleton inequality. The next step will then be the construction of codes from these groups.

ACKNOWLEDGMENTS

The research of F. Oggier for this work is supported by Nanyang Technological University under Research Grant M58110049. Part of this work was done while R. Stancu was visiting the Division of Mathematical Sciences, at Nanyang Technological University.

REFERENCES

- [1] T.H. Chan, "Aspects of Information Inequalities and its Applications", PhD thesis, 1998.
- [2] X. Yan, R. Yeung, Z. Zhang, "The capacity for multi-source multi-sink network coding," *ISIT 2007*, France, June 2007.
- [3] B. Hassibi and S. Shadbakht, "Normalized entropy vectors, network information theory and convex optimization," *ITW 2007*, July 2007.
- [4] T. H. Chan and R. W. Yeung, "On a relation between information inequalities and group theory", *IEEE Trans. on Information Theory*, vol. 48, no. 7, July 2002.
- [5] Wei Mao and B. Hassibi, "Violating the Ingleton inequality with finite groups", *47th Annual Allerton Conference on Communication, Control, and Computing*, 2009.
- [6] A. Ingleton, "Representation of matroids," *Combinatorial Mathematics and its Applications*, 1971.
- [7] H. Li and E.K.P. Chong, "On connections between group homomorphisms and the ingleton inequality," *ISIT 2007*.