On the Ingleton-Violating Finite Groups and Group Network Codes

Wei Mao, Matthew Thill, and Babak Hassibi, Member, IEEE

Abstract

It is well known that there is a one-to-one correspondence between the entropy vector of a collection of \( n \) random variables and a certain group-characterizable vector obtained from a finite group and \( n \) of its subgroups [1]. However, if one restricts attention to abelian groups then not all entropy vectors can be obtained. This is an explanation for the fact shown by Dougherty et al [2] that linear network codes cannot achieve capacity in general network coding problems (since linear network codes form an abelian group). All abelian group-characterizable vectors, and by fiat all entropy vectors generated by linear network codes, satisfy a linear inequality called the Ingleton inequality. In this paper, we study the problem of finding nonabelian finite groups that yield characterizable vectors which violate the Ingleton inequality. Using a refined computer search, we find the symmetric group \( S_5 \) to be the smallest group that violates the Ingleton inequality. Careful study of the structure of this group, and its subgroups, reveals that it belongs to the Ingleton-violating family \( PGL(2, p) \) with primes \( p \geq 5 \), i.e., the projective group of \( 2 \times 2 \) nonsingular matrices with entries in \( \mathbb{F}_p \). This family of groups is therefore a good candidate for constructing network codes more powerful than linear network codes.

Index Terms

Finite groups, entropy vectors, Ingleton inequality, network coding, network information theory.

Portions of this work were presented at the Forty-Seventh Annual Allerton Conference on Communication, Control, and Computing, 2009 and the 2010 IEEE International Symposium on Information Theory.

The authors are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 USA (email: wmao@caltech.edu, mthill@caltech.edu, hassibi@caltech.edu).

This work was supported in part by the National Science Foundation under grants CCF-0729203, CNS-0932428 and CCF-1018927, by the Office of Naval Research under the MURI grant N00014-08-1-0747, and by Caltech’s Lee Center for Advanced Networking.
I. INTRODUCTION

Let $\mathcal{N} = \{1, 2, \ldots, n\}$, and let $X_1, X_2, \ldots, X_n$ be $n$ jointly distributed discrete random variables. For any nonempty set $\alpha \subseteq \mathcal{N}$, let $X_\alpha$ denote the collection of random variables $\{X_i : i \in \alpha\}$, with joint entropy $h_\alpha \triangleq H(X_\alpha) = H(X_i; i \in \alpha)$. We call the ordered real $(2^n - 1)$-tuple $(h_\alpha : \emptyset \neq \alpha \subseteq \mathcal{N}) \in \mathbb{R}^{2^n - 1}$ an entropy vector. The set of all entropy vectors derived from $n$ jointly distributed discrete random variables is denoted by $\Gamma_n^*$. It is not too difficult to show that the closure of this set, i.e., $\overline{\Gamma_n^*}$, is a convex cone.

The set $\overline{\Gamma_n^*}$ figures prominently in information theory since it describes the possible values that the joint entropies of a collection of $n$ discrete random variables can obtain. From a practical point of view, it is of importance since it can be shown that the capacity region of any arbitrary multi-source multi-sink wired network, whose graph is acyclic and whose links are discrete memoryless channels, can be obtained by optimizing a linear function of the entropy vector over the convex cone $\overline{\Gamma_n^*}$ and a set of linear constraints (defined by the network) [3], [4]. Despite this importance, the entropy region $\overline{\Gamma_n^*}$ is only known for $n = 2, 3$ random variables and remains unknown for $n \geq 4$ random variables. Nonetheless, there are important connections known between $\overline{\Gamma_n^*}$ and matroid theory (since entropy is a submodular function and therefore somehow defines a matroid) [5], determinantal inequalities (through the connection with Gaussian random variables) [6], and quasi-uniform arrays [7]. However, perhaps most intriguing is the connection to finite groups which we briefly elaborate below.

A. Groups and Entropy

Let $G$ be a finite group, and let $G_1, G_2, \ldots, G_n$ be $n$ of its subgroups. For any nonempty set $\alpha \subseteq \mathcal{N}$, the group $G_\alpha \triangleq \bigcap_{i \in \alpha} G_i$ is a subgroup of $G$. Let $|K|$ be the order (cardinality) of a group $K$, and define $g_\alpha \triangleq \log \frac{|G|}{|G_\alpha|}$. We call the ordered real $(2^n - 1)$-tuple $(g_\alpha : \emptyset \neq \alpha \subseteq \mathcal{N}) \in \mathbb{R}^{2^n - 1}$ a (finite) group characterizable vector. Let $\Upsilon_n$ be the set of all group characterizable vectors derived from $n$ subgroups of a finite group.

The major result shown by Chan and Yeung in [1] is that $\overline{\Gamma_n^*} = \text{cone}(\Upsilon_n)$, i.e., the closure of $\Gamma_n^*$ is the same as the closure of the cone generated by $\Upsilon_n$. In other words, every group characterizable vector is an entropy vector, whereas every entropy vector is arbitrarily close to a scaled version of some group characterizable vector.

To show the first part of this statement, let $\Lambda$ be a random variable uniformly distributed on the
elements of $G$. Define $X_i = \Lambda G_i$ for $i = 1, \ldots, n$, then $X_i$ is uniformly distributed on $G/G_i$ and $H(X_i) = \log \frac{|G_i|}{|G|}$. To calculate the joint entropy $h_\alpha = H(X_\alpha)$ for a nonempty subset $\alpha \subseteq \mathcal{N}$, let $\mathcal{X}_\alpha$ denote the set of all coset tuples $\{(xG_i : i \in \alpha) \mid x \in G\}$. Consider the intersection mapping $\Theta_\alpha : \mathcal{X}_\alpha \to G/G_\alpha$, where

$$\Theta_\alpha(xG_i : i \in \alpha) = \bigcap_{i \in \alpha} xG_i = xG_\alpha. \quad (1)$$

$\Theta_\alpha$ is a well defined onto function on $\mathcal{X}_\alpha$, and it is one-to-one since if $(xG_i : i \in \alpha)$ and $(x'G_i : i \in \alpha)$ are mapped to the same coset $xG_\alpha = x'G_\alpha$, then $x^{-1}x' \in G_\alpha$ and so $x^{-1}x' \in G_i$ for all $i$, which implies $(xG_i : i \in \alpha) = (x'G_i : i \in \alpha)$. So $H(X_\alpha) = H(\Theta_\alpha(X_\alpha))$, and as $\Theta_\alpha(X_\alpha) = \Lambda G_\alpha$, we have

$$h_\alpha = H(\Theta_\alpha(X_\alpha)) = \log \frac{|G|}{|G_\alpha|} = g_\alpha.$$ 

Thus indeed every group-characterizable vector is an entropy vector. Showing the other direction, i.e., that every entropy vector can be approximated by a scaled group-characterizable vector is more tricky (the interested reader may consult [1] for the details). Here we shall briefly describe the intuition.

Consider a random variable $X_1$ with alphabet size $N$ and probability mass function $\{p_i, i = 1, \ldots, N\}$. Now if we make $T$ copies of this random variable to make sequences of length $T$, the entropy of $X_1$ is roughly equal to the logarithm of the number of typical sequences. These are sequences where $X_1$ takes its first value roughly $T_{p_1}$ times, its second value roughly $T_{p_2}$ times and so on. Therefore assuming that $T$ is large enough so that the $T_{p_i}$ are close to integers (otherwise, we have to round things) we may roughly write

$$H(X_1) \approx \frac{1}{T} \log \left( \begin{array}{c} T \\ T_{p_1} & T_{p_2} & \ldots & T_{p_{N-1}} & T_{p_N} \end{array} \right),$$

where the argument inside the log is the usual multinomial coefficient. Written in terms of factorials this is

$$H(X_1) \approx \frac{1}{T} \log \frac{T!}{(T_{p_1})!(T_{p_2})! \ldots (T_{p_N})!}. \quad (2)$$

If we consider the group $G$ to be the symmetric group $S_T$, i.e., the group of permutations among $T$ objects, then clearly $|G| = T!$. Now partition the $T$ objects into $N$ sets each with $T_{p_1}$ to $T_{p_N}$ elements, respectively, and define the group $G_1$ to be the subgroup of $S_T$ that permutes these objects while respecting the partition. Clearly, $|G_1| = (T_{p_1})!(T_{p_2})! \ldots (T_{p_N})!$, which is the denominator in (2). Thus, $H(X_1) \approx \frac{1}{T} \log \frac{|G|}{|G_1|}$, so that the entropy $h_{\{1\}}$ is a scaled version of the group-characterizable $g_{\{1\}}$. This argument can be made more precise and can be extended to $n$ random variables—see [1] for the

\(^{1}\)The left coset of $G_i$ in $G$ with representative $\Lambda$. See section [1] for the group theory notations used in this paper.
details. We note, in passing, that this construction often needs \( T \) to be very large, so that the group \( G \) and the subgroups \( G_i \) are huge.

**B. The Ingleton Inequality**

As mentioned earlier, entropy satisfies submodularity and therefore, with some care, defines a matroid. Matroids are defined by a ground set and a rank function, defined over subsets of the ground set, that satisfies submodularity. They were defined in a way to extend the notion of a collection of vectors (in some vector space) along with the usual definition of the rank. A matroid is called *representable* if its ground set can be represented as a collection of vectors (defined over some finite field) along with the usual rank function. Determining whether a matroid is representable or not is, in general, an open problem.

Let \( n = 4 \), \( \mathcal{N} = \{1, 2, 3, 4\} \). In 1971 Ingleton showed that the rank function \( r_{\{\cdot\}} \) of any representable matroid must satisfy the inequality \( [8] \)

\[
  r_{12} + r_{13} + r_{14} + r_{23} + r_{24} \geq r_1 + r_2 + r_{34} + r_{123} + r_{124},
\]

where for simplicity we write \( r_{ij} \) and \( r_{ijk} \) for \( r_{\{i,j\}} \) and \( r_{\{i,j,k\}} \), respectively. However, it turns out that there are entropy vectors that violate the Ingleton inequality \( [9] \), so that entropy is generally not a representable matroid. Using non-representable matroids, \([2]\) constructs network coding problems that cannot be solved by linear network codes (since linear network codes are, by definition, representable).

As \( \Gamma_n^{\mathcal{N}} = \text{cone}(\Upsilon_n) \), we know there must exist finite groups, and corresponding subgroups, such that their induced group-characterizable vectors violate the Ingleton inequality. In \([10]\) it was shown that abelian groups cannot violate the Ingleton inequality, thereby giving an alternative proof as to why linear network codes cannot achieve capacity on arbitrary networks—they form an abelian group. So we need to focus on non-abelian groups and their connections to nonlinear codes.

Finally, we write down the Ingleton inequality for entropy vectors, and translate it to the context of finite groups as follows:

\[
  h_{12} + h_{13} + h_{14} + h_{23} + h_{24} \geq h_1 + h_2 + h_{34} + h_{123} + h_{124},
\]

\[
  |G_1||G_2||G_{34}||G_{123}||G_{124}| \geq |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|.
\]

**C. Group Network Codes**

A communication network is usually represented by a directed acyclic graph \( \mathcal{G} = (\mathcal{V}, \mathcal{E}) \), where the node set \( \mathcal{V} \) and the edge set \( \mathcal{E} \) model the communication nodes and channels respectively. Let \( \mathcal{S} \subset \mathcal{V} \) be
the set of source nodes, \( D(s) \) be the set of sink nodes demanding source \( s \in S \). For any node \( v \) and any edge \( e \), \( \mathcal{I}(v) \) and \( \mathcal{I}(e) \) denote the sets of incoming edges to \( v \) and to the tail node of \( e \), respectively.

A network code should include

1) the assignment of a symbol \( Y_s \) from some alphabet \( Y_s \) at each source node \( s \);
2) the encoding of a symbol \( Y_e \) in some alphabet \( Y_e \) at each edge \( e \), from the symbols on \( \mathcal{I}(e) \).

Namely, \( Y_e = \phi_e(Y_f : f \in \mathcal{I}(e)) \) for some deterministic encoding function \( \phi_e \);
3) the decoding of the symbol \( Y_s \) at each \( u \in D(s) \) for all sources \( s \), i.e. \( Y_s \) is uniquely determined from the symbols on \( \mathcal{I}(u) \): \( Y_s = \phi_{u,s}(Y_f : f \in \mathcal{I}(u)) \) for some decoding function \( \phi_{u,s} \).

It is clear that at each edge \( e \) the symbol \( Y_e \) is a deterministic function of the source symbols \( \{Y_s : s \in S\} \), which is denoted by \( \varphi_e \) and is called the global mapping at \( e \). Also the source random variables \( \{Y_s : s \in S\} \) are usually assumed to be independent and uniform on their respective alphabets.

For example, a linear network code is defined as follows: 1) for each \( t \in S \cup E \), the alphabet \( Y_t \) is a vector space \( F^{d_t} \) over a finite field \( F \) with some finite dimension \( d_t \); 2) all encoding/decoding functions are linear: if \( t \) is an edge or a sink node, then the encoding/decoding function \( \phi_t \) at \( t \) can be written as \( \phi_t(Y_f : f \in \mathcal{I}(t)) = \sum_{f \in \mathcal{I}(t)} M_{t,f}Y_f \) for some matrices \( M_{t,f} \). Thus the global mappings at the edges are also linear.

Group network codes were first proposed by Chan in [11], [12] by considering the fact that finite groups can generate the whole entropy region, and noting that linear network codes are simply a special case. Suppose \( G \) is a finite group, and that \( \{G_e : e \in E\} \) and \( \{G_s : s \in S\} \) are some of its subgroups. One can construct a network code with \( Y_t = G/G_t \) for each \( t \in S \cup E \), such that the entropy vector for \( \{Y_t : t \in S \cup E\} \) is characterizable by the group \( G \) and its subgroups \( \{G_t : t \in S \cup E\} \), if the following requirements are met.

(\textbf{R1}) \textit{Source independence}: the cardinalities of \( G/G_S \) and \( \prod_{s \in S} Y_s \) (the Cartesian product of the source alphabets) are equal, where \( G_S \triangleq \bigcap_{s \in S} G_s \). This is equivalent to \( \prod_{s \in S} |G_s| = |G|^{|S|-1}|G_S| \).

(\textbf{R2}) \textit{Encoding}: \( \forall e \in E, \bigcap_{f \in \mathcal{I}(e)} G_f \leq G_e \).

(\textbf{R3}) \textit{Decoding}: \( \forall s \in S, \bigcap_{f \in \mathcal{I}(u)} G_f \leq G_s \) for each \( u \in D(s) \).

To establish the encoding and decoding process, we need an auxiliary lemma.

\textbf{Lemma 1}: Let \( K_1, K_2 \) be two subgroups of \( G \) with \( K_1 \leq K_2 \). Then the coset mapping

\[ \pi : G/K_1 \to G/K_2 \]

\[ xK_1 \mapsto xK_2 \]
is a well defined onto function, where \( xK_1 \) is mapped to the unique coset in \( G/K_2 \) that contains it. Furthermore, if \( \Lambda_1 \) is a uniform random variable on \( G/K_1 \), then \( \pi(\Lambda_1) \) is uniform on \( G/K_2 \).

Proof: \( \pi \) is well defined since \( xK_2 = x'K_2 \) whenever \( xK_1 = x'K_1 \). Note that \( K_2 \) is partitioned by the \( m \) distinct cosets \( \{y_iK_1 : 1 \leq i \leq m \} \), where \( m = |K_2/K_1| \) and \( y_i \in K_2 \) for \( i = 1, 2, \ldots, m \). Therefore, each \( xK_2 \in G/K_2 \) is also partitioned by the \( m \) cosets \( \{(xy_i)K_1 : 1 \leq i \leq m \} \), which are precisely the \( m \) preimages of \( xK_2 \) under \( \pi \). Thus \( \pi(\Lambda_1) \) is uniform on \( G/K_2 \). \( \blacksquare \)

For any collection \( \alpha \) of subgroups of \( G \), the intersection mapping \( (I) \) is a bijection. Consider the collection of all source subgroups. Let \( \mathcal{X}_S = \{(xG_s : s \in S) \mid x \in G\} \), then we have the bijective intersection mapping \( \Theta_S : \mathcal{X}_S \to G/G_S \). But with (R1), \( |\prod_{s \in S} \mathcal{Y}_s| = |G/G_S| = |\mathcal{X}_S| \) and so \( \mathcal{X}_S = \prod_{s \in S} \mathcal{Y}_s \). This means that any coset tuple \( (xG_s : s \in S) \) in \( \prod_{s \in S} \mathcal{Y}_s \) can be represented in the form \( (xG_s : s \in S) \) for a common \( x \in G \), and the intersection of \( \{xG_s : s \in S\} \) is equal to \( xG_S \). Therefore, we can rewrite the bijection \( \Theta_S \) as

\[
\Theta_S : \prod_{s \in S} \mathcal{Y}_s \to G/G_S,
\]

which maps a tuple to the intersection of all its cosets.

Moreover, let \( t \) be an edge or a sink node, define \( \mathcal{X}_{I(t)} = \{(xG_f : f \in I(t)) \mid x \in G\} \) and \( G_{I(t)} = \bigcap_{f \in I(t)} G_f \). Then the intersection mapping

\[
\Theta_{I(t)} : \mathcal{X}_{I(t)} \to G/G_{I(t)}
\]

is a bijection. With (R2) and (R3), we can also define coset mappings for edges and source/sink pairs as follows. For each edge \( e \), since \( G_{I(e)} \leq G_e \) by (R2), define the coset mapping \( \pi_e \) as with \( K_1 = G_{I(e)} \) and \( K_2 = G_e \). While for each source \( s \) with \( u \in \mathcal{D}(s) \), since \( G_{I(u)} \leq G_s \) by (R3), similarly define \( \pi_{u,s} \) with \( K_1 = G_{I(u)} \) and \( K_2 = G_s \).

Now we can define the encoding and decoding functions. At each edge \( e \), let the encoding function be \( \phi_e = \pi_e \circ \Theta_{I(e)} \). For each source \( s \) with \( u \in \mathcal{D}(s) \), let the decoding function be \( \phi_{u,s} = \pi_{u,s} \circ \Theta_{I(u)} \). In other words, at an edge or a sink node \( t \), the encoding/decoding function takes an input coset tuple \( (Y_f : f \in I(t)) \) and first forms the intersection of all its cosets, which is a coset of \( G_{I(t)} \), then maps this coset to the unique coset of \( G_e \) (or \( G_s \), whichever is appropriate) that contains it. Such network operations define a proper network code, since by the proposition below the decoding functions always yield correct source symbols at each sink node.

**Proposition 1:** Assume (R1) holds, and let the encoding and decoding functions be defined as above. Then for some common \( x \in G \), \( \forall s \in S \), \( Y_s = xG_s \) and \( \forall e \in E \), \( Y_e = xG_e \). Also for each source \( s \) with \( u \in \mathcal{D}(s) \), \( Y_s \) is recovered by the decoding function \( \phi_{u,s} \).
Proof: Let the source symbols \((Y_s : s \in \mathcal{S})\) be an arbitrary tuple from \(\prod_{s \in \mathcal{S}} \mathcal{Y}_s\). Since (R1) is true, as discussed above, for all \(s \in \mathcal{S}, Y_s = xG_s\) with a common \(x \in G\). As \(G\) is directed and acyclic, we can define the “depth” of each node \(v\) as the length of the longest path from a source node to \(v\), and define the depth of an edge to be the depth of its tail node. Note that \(e\) is always “deeper” than \(f\) if \(f \in \mathcal{I}(e)\). Also if \(Y_f = xG_f\) for all \(f \in \mathcal{I}(e)\), then \(Y_e = \phi_e(Y_f : f \in \mathcal{I}(e)) = xG_e\). So by induction on the depths of the edges, \(Y_e = xG_e\) for all \(e \in \mathcal{E}\).

Furthermore, for each \(s \in \mathcal{S}\) with \(u \in \mathcal{D}(s)\), since \(Y_f = xG_f\) for all \(f \in \mathcal{I}(u)\), \(\phi_{u,s}(Y_f : f \in \mathcal{I}(u)) = xG_s = Y_s\). Thus the source symbol \(Y_s\) is successfully recovered at \(u\).

Remark 1: Note that the encoding/decoding function for an edge or a sink node \(t\) is only defined on \(\mathcal{X}_{\mathcal{I}(t)}\), but not on the entire Cartesian product \(\prod_{f \in \mathcal{I}(t)} \mathcal{Y}_f\). This is because for an arbitrary tuple in \(\prod_{f \in \mathcal{I}(t)} \mathcal{Y}_f\), it is possible that the intersection of all cosets is the empty set, which is not a coset of \(G_{\mathcal{I}(t)}\). However, with (R1) this is not a problem, as Proposition 1 guarantees that \((Y_f : f \in \mathcal{I}(t))\) is always a tuple in \(\mathcal{X}_{\mathcal{I}(t)}\).

Remark 2: From the proof above, even without (R1) these encoding and decoding functions still constitute a valid network code, if the sources cooperate in such a way that the transmit tuples are always from \(\mathcal{X}_S\). But in this case the source random variables are dependent.

Next we analyze the global mappings of this group network code, and show that the entropy vector is characterizable by the group \(G\) and its subgroups \(\{G_i : t \in \mathcal{S} \cup \mathcal{E}\}\) when the sources are independent and uniform. First we give another auxiliary lemma.

Lemma 2: Let \(K \leq G\) and let \(G_i, i = 1, \ldots, n,\) be subgroups of \(G\) containing \(K\). For each \(i\) let \(\pi_i\) be the coset mapping defined as \(5\) with \(K_1 = K\) and \(K_2 = G_i\). Let \(\Lambda_K\) be a uniform random variable on \(G/K\), and define \(X_i = \pi_i(\Lambda_K)\) for each \(i\). Then the entropy vector of \(\{X_1, X_2, \ldots, X_n\}\) is exactly the group characterizable vector induced by \(G\) and \(\{G_1, G_2, \ldots, G_n\}\).

Proof: For each nonempty subset \(\alpha \subseteq \mathcal{N}\), since \(K \leq G_\alpha\), we can define the coset mapping \(\pi_\alpha\) with \(K\) and \(G_\alpha\). As in Section 1-A, the alphabet of \(X_\alpha\) is still \(X_\alpha = \{xG_i : i \in \alpha\} \mid x \in G\}\), and the intersection mapping \(\Theta_\alpha\) is a bijection. Also \(\Theta_\alpha(X_\alpha) = \pi_\alpha(\Lambda_K)\), which is uniform on \(G/G_\alpha\) by Lemma 1. So the joint entropy \(H(X_\alpha) = H(\Theta_\alpha(X_\alpha)) = \log \frac{|G|}{|G_\alpha|}\) and the lemma follows.

For each \(s \in \mathcal{S}\) define the coset mapping \(\pi_s\) as \(5\) with \(K_1 = G_S\) and \(K_2 = G_s\). For every edge \(e\) we can similarly define a new coset mapping \(\pi_e\) with \(K_1 = G_S\) and \(K_2 = G_e\), since according to the following proposition, \(G_S \leq G_e\).

Proposition 2: If (R2) is satisfied, then \(\forall e \in \mathcal{E}, G_S \leq G_e\).

Proof: The proposition is trivially true if \(e\) is emitted from a source node. Also if \(G_S \leq G_f\) for all
if \( f \in \mathcal{I}(e) \), then by (R2) we have \( G_S \leq G_e \). Similar to Proposition 1 by induction on the depths of the edges the proof follows.

**Proposition 3:** \( \forall e \in \mathcal{E} \), the global mapping at \( e \) for the above group network code is \( \varphi_e = \pi'_e \circ \Theta_S \). In other words, \( \varphi_e \) first forms the intersection of all the source cosets to obtain a coset of \( G_{\mathcal{I}(e)} \), and then maps this coset to the unique coset of \( G_e \) containing it.

**Proof:** Assume the source symbols \( (Y_s : s \in S) \) are transmitted and let \( \Lambda_S = \Theta_S(Y_s : s \in S) \). Then \( \Lambda_S = xG_S \) for some \( x \in G \), and \( Y_s = xG_s = \pi'_s(\Lambda_S) \) for all \( s \in S \). By Proposition 1 \( Y_e = xG_e = \pi'_e(\Lambda_S) \), so \( \varphi_e = \pi'_e \circ \Theta_S \).

Let the source random variables \( \{Y_s : s \in S\} \) be independent and uniformly distributed, so the joint distribution is uniform on \( \prod_{s \in S} Y_s \). Let \( \Lambda_S = \Theta_S(Y_s : s \in S) \), then \( \Lambda_S \) is uniform on \( G/G_S \) as \( \Theta_S \) is bijective. From Proposition 3 \( \forall t \in S \cup \mathcal{E} \), \( Y_t = \pi'_t(\Lambda_S) \), and so by Lemma 2 the entropy vector for \( \{Y_t : t \in S \cup \mathcal{E}\} \) is characterizable by the group \( G \) and its subgroups \( \{G_t : t \in S \cup \mathcal{E}\} \).

**Remark 3:** For linear network codes, the global mappings are linear functions on the direct sum \( V \) of all source vector spaces. As the underlying field is finite, \( V \) is a finite abelian group. Let \( G = V \), \( G_s \) be the subspace spanned by all source vectors from \( S \setminus \{s\} \), \( G_e \) be the null space of the global mapping at \( e \). Then the linear network code is indeed realized as a group network code. We shall elaborate on this point in Section VII-A.

### D. Discussion

Since we know of distributions whose entropy vector violates the Ingleton inequality, we can, in principle, construct finite groups whose group-characterizable vectors violate Ingleton. Two such distributions are Example 1 in [13], where the underlying distribution is uniform over 7 points and the random variables correspond to different partitions of these seven points, and the example on page 1445 of [14], constructed from finite projective geometry and where the underlying distribution is uniform over \( 12 \times 13 = 156 \) points. Unfortunately, constructing groups and subgroups for these distributions using the recipe of Section I-A results in \( T = 29 \times 7 = 203 \) and \( T = 23 \times 156 = 3588 \), which results in groups of size \( 203! \) and \( 3588! \), which are too huge to give us any insight whatsoever.

These discussions lead us to the following questions.

1) Could the connection between entropy and groups be a red herring? Are the interesting groups too large to give any insight into the problem (e.g., the conditions for the Ingleton inequality to be violated)?
2) What is the smallest group with subgroups that violates the Ingleton inequality? Does it have any special structure?

3) Can one construct network codes from such Ingleton-violating groups?

In this paper we address the first two questions. We identify the smallest group that violates the Ingleton inequality—it is the symmetric group $S_5$, with 120 elements. Through a thorough investigation of the structure of its subgroups we conclude that it belongs to the family of groups $PGL(2, p)$, with $p$ a prime greater than or equal to 5. ($PGL(2, 5)$ is isomorphic to $S_5$.) We therefore believe that the connection to groups is not a red herring and that there may be some benefit to it.

The explicit nature of $PGL(2, p)$ may lend itself to effective network codes. We only mention that non-abelian groups allow for much more flexibility in the design of codes. For example, if the incoming messages to a node in the network, $a$ and $b$, say, are elements from a nonabelian group then the operations $a^2b, aba, ba^2$, say, can potentially all correspond to different elements in the group, whereas in the abelian case they all coincide with $a^2b$. Therefore nodes in a network will have much more choices in terms of what to transmit on their outgoing edges—and this should, ostensibly, be what allows one to achieve capacity. The drawback is, of course, that decoding becomes more complicated than solving a system of linear equations.

We shall not say anymore about codes. What we will do in the remainder of the paper is to describe how we found the smallest Ingleton-violating group and how we uncovered its structure. This required the identification of conditions beyond being abelian that force a group to respect Ingleton. It also required a deep study of the 120 element group that we found via computer search. We now present the details.

II. Notation

We use the following abstract algebra notations throughout this paper:

$|G|$ the order of group $G$.

$G \cong H$ the group $G$ is isomorphic to the group $H$.

$H \leq G$ $H$ is a subgroup of $G$.

$H \trianglelefteq G$ $H$ is a normal subgroup of $G$.

$gH$ the left coset of the subgroup $H$ in $G$ with representative $g$.

$G/H$ the set of all left cosets of subgroup $H$ in $G$. When $H \trianglelefteq G$, $G/H$ is a group. (Factor or quotient group)

$|g|$ the order of element $g = \text{smallest positive integer } m \text{ s.t. } g^m = 1$. 

the conjugate of element $x$ by element $g$ in $G$: $x^g = g^{-1} x g$. (No confusion with
the powers of $x$ as $g$ is an element of $G$.)

$X^g$ the conjugate of subset $X$ by element $g$ in $G$: $X^g = \{x^g : x \in X\}$.

$HK$ or $H \cdot K$ the “set product” of $H, K \subseteq G$: $HK = \{hk : h \in H, k \in K\}$.

$H \times K$ the direct product of groups $H$ and $K$.

$G^n$ the direct product of $n$ copies of the group $G$.

$H \rtimes K$ the semidirect product of groups $H$ and $K$.

$\langle g_1, \ldots, g_m \rangle, \langle S \rangle$ the group generated by the elements $g_1, \ldots, g_m$, and by the set $S$.

$G = \langle S | R \rangle$ $\langle S | R \rangle$ is a presentation of $G$. $S$ is a set of generators of $G$, while $R$ is a set of
relations $G$ should satisfy.

1 the natural number “1”, identity element of a group, or the trivial group. The
meaning should be clear in different contexts with no confusion.

$\mathbb{Z}_n$ the integers modulo $n \cong$ the cyclic group of order $n$.

$S_n$ the symmetric group of degree $n$ = all permutations on $n$ points.

$D_{2n}$ the dihedral group of order $2n$.

$\mathbb{F}_q$ the finite field of $q$ elements.

$\mathbb{Z}_n^\times, \mathbb{F}_q^\times$ the multiplicative group of units of $\mathbb{Z}_n$, and of $\mathbb{F}_q$. $\mathbb{F}_q^\times$ = all nonzero elements of
$\mathbb{F}_q$.

$GL(n, q)$ the general linear group of all invertible $n \times n$ matrices with entries from $\mathbb{F}_q$.

The identity element for $GL(n, q)$ is usually denoted by $I$ = identity matrix.

$|GL(n, q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.

$V_q$ the center of $GL(n, q)$ = all nonzero scalar matrices = $\{\alpha I : \alpha \in \mathbb{F}_q^\times\}$.

$PGL(n, q)$ the projective general linear group = $GL(n, q)/V_q$. $|PGL(n, q)| = |GL(n, q)|/|V_q| =
|GL(n, q)|/(q - 1)$.

$SL(2, q)$ the special linear group = all matrices in $GL(2, q)$ with determinant 1. $|SL(2, q)| =
|PGL(2, q)|$.

$PSL(2, q)$ the projective special linear group = $SL(2, q)/\langle -I \rangle$. $|PSL(2, q)| = |SL(2, q)|/2$.

To simplify expressions in later sections, let $\mathcal{K}_n \triangleq \{0, 1, \ldots, n - 2\}$ for integers $n \geq 2$.

III. COMPUTER SEARCH AND SOME NEGATIVE CONDITIONS

Designing a small admissible structure for an Ingleton-vio-
lating group $G$ and its subgroups is very
difficult without an existing example, so we use computer programs to search for a small instance. We
use the GAP system \cite{15} to search its “Small Group” library, which contains all finite groups of order less than or equal to 2000, except those of 1024. We pick a group in this library, find all its subgroups, then test the Ingleton inequality for all 4-combinations of these subgroups. This is a tremendous task, as there are already more than 1000 groups of order less than or equal to 100, up to isomorphism, each of which might have hundreds of subgroups (some even have more than 1000).

It was therefore extremely critical to prune our search. In fact, we used the following negative conditions, each of which guarantees that Ingleton is not violated.

**Condition 1:** $G$ is abelian. \cite{10}

**Condition 2:** $G_i \trianglelefteq G$, $\forall i$. \cite{16}

**Condition 3:** $G_1G_2 = G_2G_1$, or equivalently $G_1G_2 \leq G$.

**Condition 4:** $G_i = 1$ or $G$, for some $i$.

**Condition 5:** $G_i = G_j$ for some distinct $i$ and $j$.

**Condition 6:** $G_{12} = 1$.

**Condition 7:** $G_i \leq G_j$ for some distinct $i$ and $j$.

**Remark 4:** Condition 2 subsumes Condition 1, while Condition 3 subsumes Condition 2. Also Conditions 4 and 5 are contained in Condition 7.

The proofs for Conditions 3, 6 and 7 are listed below:

**Proof 3** Construct random variables $X_i$'s from uniformly distributed $\Lambda$ on $G$ as in Section I-A. As $G_{1;2} \trianglelefteq G_1G_2 \leq G$, we can similarly construct random variable $X_{1;2} = \Lambda G_{1;2}$. Note that $|G_{1;2}| = |G_1||G_2|/|G_{12}|$, $H(X_{1;2}|X_1) = H(X_{1;2}|X_2) = 0$ as $G_1, G_2 \leq G_{1;2}$. Similar to the proof of Condition 2 in \cite{16}, we use the following information inequality in \cite{17}:

$$2H(E|A) + 2H(E|B) + I(A;B|C) + I(A;B|D) + I(C;D) \geq H(E).$$

Plugging in $A = X_1$, $B = X_2$, $C = X_3$, $D = X_4$ and $E = X_{1;2}$ we can easily deduce Ingleton inequality.

**Remark 5:** In the proof above we used the aforementioned group-entropy correspondence to translate the problem to the entropy domain. Henceforth, in order to show that a group satisfies Ingleton, we shall either prove \ref{4} directly, or equivalently prove \ref{3} using this correspondence.

Observe that the Ingleton inequality has symmetries between subscripts 1 and 2 and between 3 and 4, i.e. if we interchange the subscripts 1 and 2, or 3 and 4, the inequality stays the same. Thus if we prove conditions for some $i \in \{1, 2\}$ and $j \in \{3, 4\}$, we automatically get conditions for all $(i, j) \in$...
\{1, 2\} \times \{3, 4\}. So without loss of generality, we will just prove conditions for the case \((i, j) = (1, 3)\) when these symmetries apply.

**Proof 6:** Realize that (3) can be rewritten as

\[ \delta_{13,14} + \delta_{23,24} + \delta_{134,234} - \delta_{123,124} \geq 0, \]  

(6)

where \(\delta_{\alpha,\beta} \triangleq h_{\alpha} + h_{\beta} - h_{\alpha \cap \beta} - h_{\alpha \cup \beta}\) for \(\emptyset \neq \alpha, \beta \subseteq \mathcal{N}\). (e.g., \(\delta_{134,234} = h_{134} + h_{234} - h_{34} - h_{1234}\).)

By submodularity, all \(\delta_{\alpha,\beta} \geq 0\). If \(G_{12} = 1\), then \(\delta_{123,124} = 0\) and (6) holds.

**Proof 7:** \((i, j) = (1, 2)\) implies Condition 3 \((1, 3)\) implies \(\delta_{123,124} = 0\) in (6). \((3, 1)\) implies \(\delta_{123,234} = 0\) and so \(\delta_{123,234} \leq \delta_{12,24}\), which further implies \(\delta_{123,124} \leq \delta_{23,24}\), thus (6) holds. For \((3, 4)\), (4) becomes \(|G_1||G_2||G_3||G_{124}| \geq |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|\), which follows from \(|G_1||G_{124}| \geq |G_{12}||G_{14}||G_{23}||G_{24}|\) and \(G_2 \geq G_{24}\). 

**Remark 6:** Conditions 6 and 7 were first pointed out to us by Prof. M. Aschbacher using group theoretic techniques. The proofs presented above are based on the submodularity property of entropy.

**Remark 7:** Conditions 1, 3 and 6 are crucial in our searching program, as they appear in the outer searching loops and can reduce a large amount of work.

**IV. THE SMALLEST VIOLATION INSTANCE AND ITS STRUCTURE**

Using GAP we found the smallest group that violates Ingleton is \(G = S_5\). There are 60 sets of violating subgroups up to subscript symmetries. Furthermore, these 60 sets of subgroups are all conjugates of each other. Thus in terms of group structure, these instances are virtually the same. We list below some
information from GAP about one representative:

\[ G_1 = \langle (3, 4, 5), (1, 2)(4, 5) \rangle \cong S_3 \cong D_6 \mid |G_1| = 6 \]
\[ G_2 = \langle (1, 2, 3, 4, 5), (1, 4, 3, 5) \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \mid |G_2| = 20 \]
\[ G_3 = \langle (2, 3), (1, 3, 4, 2) \rangle \cong D_8 \mid |G_3| = 8 \]
\[ G_4 = \langle (2, 4), (1, 2, 5, 4) \rangle \cong D_8 \mid |G_4| = 8 \]
\[ G_{12} = \langle (1, 2)(3, 5) \rangle \cong \mathbb{Z}_2 \mid |G_{12}| = 2 \]
\[ G_{13} = \langle (1, 2)(3, 4) \rangle \cong \mathbb{Z}_2 \mid |G_{13}| = 2 \]
\[ G_{14} = \langle (1, 2)(4, 5) \rangle \cong \mathbb{Z}_2 \mid |G_{14}| = 2 \]
\[ G_{23} = \langle (1, 3, 4, 2) \rangle \cong \mathbb{Z}_4 \mid |G_{23}| = 4 \]
\[ G_{24} = \langle (1, 2, 5, 4) \rangle \cong \mathbb{Z}_4 \mid |G_{24}| = 4 \]
\[ G_{34} = 1 \mid |G_{34}| = 1 \]
\[ G_{123} = 1 \mid |G_{123}| = 1 \]
\[ G_{124} = 1 \mid |G_{124}| = 1 \]

As \( |G_1||G_2||G_{34}||G_{123}||G_{124}| = 120 < 128 = |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}| \), Ingleton is violated. Also, \( G_1 \cdots G_4 \) generate \( G = S_5 \).

To illustrate the structure of these subgroups, we use the group cycle graph. See Fig. II where the dash-dotted lines denote the pairwise intersections of subgroups excluding identity. From the cycle graph we can obtain more structural information which GAP does not show us directly. First, not only is \( G_2 \) a semidirect product of two cyclic groups \( \langle (1, 2, 3, 4, 5) \rangle \cong \mathbb{Z}_5 \) and \( \langle (1, 4, 3, 5) \rangle \cong \mathbb{Z}_4 \) (in particular, it’s metacyclic), but also \( (G_2 \setminus \langle (1, 2, 3, 4, 5) \rangle) \cup \{1\} \) is the union of subgroups which are all isomorphic to \( \langle (1, 4, 3, 5) \rangle \) (actually they are all conjugates of \( \langle (1, 4, 3, 5) \rangle \)) and have trivial pairwise intersections. (In this case we say \( G_2 \) has a “flower” structure.) Second, \( G_4 \) is the conjugate of \( G_3 \) by \( (3, 4, 5) \). In particular, \( (1, 3, 4, 2)^{(3, 4, 5)} = (1, 4, 5, 2) = (1, 2, 5, 4)^{-1} \).

In order to generalize these subgroups to a family of violations, we seek a group presentation for them. Observe that \( |G_{23}| \) and \( |G_{24}| \) (both equal to 4) contribute most to the right-hand side \( (RHS) \) of (4), so we may try to let the “petals” of \( G_2 \) (conjugates of \( \langle (1, 4, 3, 5) \rangle \)) grow while keeping other structures fixed. (This is a little conservative, but it is the only successful extension according to our GAP trials. For example, one may try to expand \( G_1 \) at the same time, but the structures of \( G_3 \) and \( G_4 \) usually collapse.)

---

2The permutations are written in cycle notation, e.g. \( (1, 2)(3, 4, 5) \) is the permutation on the set \( \{1, 2, 3, 4, 5\} \) that makes the following mapping: \( 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 3 \). Also GAP’s convention for permutations is used throughout this paper, i.e. permutations are applied to an element from the right.
We assume that $G_2$ is generated by two elements $a$ and $b$ with a normal subgroup $N = \langle a \rangle \cong \mathbb{Z}_n$, as well as a subgroup $H = \langle b \rangle \cong \mathbb{Z}_m$, for some integers $m, n$. This gives us a presentation

$$G_2 = \langle a, b | a^n = b^m = 1, a^b = a^s \rangle$$

for some $0 < s < n$. In order to violate Ingleton as much as possible, we may wish for $n$ to be small while $m$ is large. However, the flower structure of $G_2$ may limit the choices of $n$ and $m$. First of all, for this presentation to be a semidirect product, we need $s^m \equiv 1 \pmod{n}$ (see [18 Sec 5.4]), i.e., $s \in \mathbb{Z}_n^\times$ with $|s| | m$. As a consequence, $|G_2| = mn$, $H \cap N = 1$, and $(a^i)^b^k = a^{i^s k}$ for any integers $i$ and $k$. Moreover, we need $(G_2 \setminus N) \cup \{1\}$ to be the union of groups which are all isomorphic to $H$ with trivial pairwise intersections.

One possible way to achieve this is to restrict $H^{g_1} \cap H^{g_2} = 1$, $\forall g_1 \neq g_2 \in N$, as in our original construction. This is equivalent to $H^g \cap H = 1$, $\forall g \in N \setminus \{1\}$. If this is the case, there will be $|N| = n$
“petals” of size $m$ in $G_2$, and the total number of nonidentity elements will equal $n(m - 1) = nm - n = |G_2 \setminus N|$, then indeed the flower structure would be achieved.

Pick two nonidentity elements $h_1 = b^l \in H$, $h_2 = (b^k)^{a^i} \in H^{a^i}$ for some $0 < k, l < m$, $0 < i < n$. Then

$$h_1 = h_2 \iff a^{-i}bka^i = b^l \iff a^{-i}(a^i)b^{-k}b^k = b^l \iff a^{-i}a^{i-s-k} = b^l = b^{-k} \iff a^{(s-k-1)i} = b^{-k}.$$ 

As $H \cap N = 1$, this is equivalent to $a^{(s-k-1)i} = b^{-k} = 1$, i.e. $l = k$ and $n|(s^{-k} - 1)i$. To guarantee that $H^{a^i} \cap H = 1$, we must have $m \leq |s|$. Otherwise if we let $0 < k = |s| < m$, then $s^{-k} \equiv 1 \pmod{n}$ and so $n|(s^{-k} - 1)i$; therefore we can find a nonidentity element $h_1 = b^k = (b^k)^{a^i} = h_2$ in $H^{a^i} \cap H$.

Now, since $m \leq |s|$ and $|s| \mid m$, we must have $m = |s|$. In particular, $m \leq |Z_n^\times| < n$.

For $m$ to be as large as possible, $s$ should be a primitive root modulo $n$, which makes $m = |Z_n^\times|$. Furthermore, since $m \leq n - 1$, we can achieve the upper bound on $m$ (w.r.t. $n$) when $n = p$, for some prime $p > 2$. (We need $p > 2$ for the petals not to collapse.) In this case $m = |Z_p^\times| = p - 1$. Also if $0 < k < m = |s|$, $0 < i < n = p$, then $n|(s^{-k} - 1)i$ requires $p|i$ or $p|(s^{-k} - 1)$. Since $p > i$, the latter must be true, which implies that $|s| \mid k$. But this is a contradiction since $0 < k < |s|$. So actually we have $H^g \cap H = 1, \forall g \in N$, and the flower structure is realized. In this case the presentation of $G_2$ becomes

$$G_2 = \langle a, b \mid a^p = b^{p-1} = 1, a^b = a^s \rangle$$ 

(8)

where $p > 2$ is a prime, $s$ is a primitive root modulo $p$.

The next step is to extend this presentation to the whole group $G$ generated by $G_1$–$G_4$, with the structure in Fig. Consider the dihedral groups $G_3$ and $G_4$. The subgroups of rotations are just $H^{a^3}$ and $H^{a^4}$ respectively, for some $a_3 = a^{k_3}, a_4 = a^{k_4} \in N$. Also $G_3$ and $G_4$ each shares one element of reflection with the dihedral group $G_1$, while the remaining reflection of $G_1$ is just $(b^{n-k_3})^{a^i}$ in $G_2$, for some $a_1 = a^{k_1} \in N$. Thus if we can determine the generator of the subgroup of rotations of $G_1$, then all elements of $G_1$–$G_4$ are determined. In other words, if we introduce an element $c$ as the generator of rotations of $G_1$, then all elements from $G_1$–$G_4$ can be express as products of $a, b, c$ and their inverses. To simplify our expressions, define

$$b_1 = (b^{n-k_3})^{a_1}, \quad b_2 = b^{s^{k_3}}, \quad b_4 = b^{a^{k_4}}$$ 

(9)

for some integers $k_1, k_3, k_4$. If in Fig. we let $a, b, c, b_1, b_3, b_4$ correspond with $(1, 2, 3, 4, 5)$, $(1, 4, 3, 5)$, $(3, 4, 5)$, $(1, 2)(3, 5)$, $(1, 3, 4, 2)$, $(1, 2, 5, 4)$ respectively, then the subgroups and the whole group in our presentation should be

$$G_1 = \langle c, b_1 \rangle, \quad G_2 = \langle a, b \rangle, \quad G_3 = \langle b_1 c^2, b_3 \rangle, \quad G_4 = \langle b_1 c, b_4 \rangle, \quad G = \langle a, b, c \rangle.$$ 

(10)
As \( G_1 \cong D_6 \), we should have the relation \( c^3 = (cb_1)^2 = 1 \). For \( G_3 \) and \( G_4 \) to be dihedral groups, we need \((b_3 \cdot b_1c^2)^2 = (b_4 \cdot b_1c)^2 = 1\).

Observe that in the original violation, \( G_4 \) is the conjugate of \( G_3 \) by \((3, 4, 5)\), and \((1, 3, 4, 2)^{(3,4,5)} = (1, 2, 5, 4)^{-1}\). In our presentation this translates to \( b_3^c = b_4^{-1} \). We claim this relation makes \((b_3 \cdot b_1c^2)^2 = (b_4 \cdot b_1c)^2 = 1\) if and only if \( k_3 - k_1 \equiv k_1 - k_4 \pmod{p} \). As \(|b_1| = 2\), \( e^3 = (cb_1)^2 = 1\), we have \( cb_1 = b_1c^2 \) and \( b_1c = c^2b_1 \). From the new relation we can establish the following equalities:

\[
(b_3 \cdot b_1c^2)^2 = b_3b_1c^{-1}b_3cb_1 = b_3b_1b_4^{-1}b_1, \\
(b_4 \cdot b_1c)^2 = b_4b_1cb_4^{-1}b_1 = b_4b_1b_3^{-1}b_1 = ((b_3b_1b_4^{-1}b_1)^{-1})b_1.
\]

So \((b_3 \cdot b_1c^2)^2 = 1\) if and only if \((b_4 \cdot b_1c)^2 = 1\). Plugging in \( (9) \) and using \((ai)^{b_k} = a^{i s_k}\) we have

\[
(b_3 \cdot b_1c^2)^2 = a^{[(k_3-k_1)+(k_1-k_4)s^{(p-1)/2}](s^{-1}-1)}.
\]

Since \( s \) is a primitive root modulo \( p \), \(|s^{(p-1)/2}| = 2\). As \( \mathbb{Z}_p^\times \) is cyclic of an even order \( p - 1 \), it is clear that there is a unique element of order 2. Also the order of \(-1\) in \( \mathbb{Z}_p^\times \) is 2, so \( s^{(p-1)/2} \equiv -1 \pmod{p} \), and

\[
(b_3 \cdot b_1c^2)^2 = a^{[(k_3-k_1)-(k_1-k_4)](s^{-1}-1)}.
\]

Now \( p \nmid (s^{-1} - 1) \) as \( s \neq 1 \), so

\[
(b_3 \cdot b_1c^2)^2 = 1 \iff p \mid [(k_3-k_1)-(k_1-k_4)] \iff k_3 - k_1 \equiv k_1 - k_4 \pmod{p}.
\]

The above condition tells us that the petals \( G_{23} \) and \( G_{24} \) of \( G_2 \) should be symmetric w.r.t. \( G_{12} \), i.e. \( G_{23}, G_{12} \) and \( G_{24} \) should be equally spaced. (Once this symmetry is respected, it is very easy for GAP to produce the desired structures, even with arbitrary \( k_1 \) and \( k_3 \).)

In sum, our analysis leads to the following presentation:

\[
G = \langle a, b, c \mid a^p = b^{p-1} = c^3 = 1, a^b = a^s, (cb_1)^2 = b_3b_4 = 1 \rangle \tag{11}
\]

where \( p \) is an odd prime, \( s \) is a primitive root modulo \( p \), \( k_3 - k_1 \equiv k_1 - k_4 \pmod{p} \). If our extension of the subgroup structures succeeds, then the orders of subgroups and intersections would be: \(|G_1| = 6\), \(|G_2| = p(p-1)\), \(|G_3| = |G_4| = 2(p-1)\), \(|G_{12}| = |G_{13}| = |G_{14}| = 2\), \(|G_{23}| = |G_{24}| = p - 1\), \(|G_{34}| = |G_{123}| = |G_{124}| = 1\). LHS of \( (4) \) = 6\( p(p-1) \) while RHS = \( 8(p-1)^2 \). So for \( p \geq 5 \), Ingleton should be violated.
V. Explicit Violation Construction with $PGL(2, q)$

Feeding the above presentation into GAP, we find that for $p = 5, 7, \ldots, 23$ the outcome is a finite group, and it violates Ingleton with subgroups in (10). Moreover, with GAP we verified for the first few primes (up to $p = 11$) that this group is isomorphic to $PGL(2, p)$. In fact, we prove that $PGL(2, p)$ is indeed a family of Ingleton-violating groups for primes $p \geq 5$, by explicitly constructing their violating subgroups. Furthermore, once we have the formats of these subgroups, we extend them to the Ingleton-violating family $PGL(2, q)$ for all finite field order $q \geq 5$. In Appendix A in the framework of group actions we show that this family of Ingleton violations has a remarkably nice interpretation: each subgroup is the stabilizer for a special set of points in the projective geometry of $PGL(2, q)$.

A. The Family $PGL(2, p)$

Let $p$ be an odd prime. For $A \in GL(2, p)$, let $\overline{A}$ denote the left coset of $A$ in $GL(2, p)$ with respect to the center $V_p = \{ \alpha I : \alpha \in \mathbb{F}_p^\times \}$. Thus $\overline{A} = \overline{B}$ if and only if each entry of $A$ is a nonzero constant multiple of the corresponding entry of $B$. $A^T$ denotes the transpose of $A$ as usual. We denote the elements of $\mathbb{F}_p$ by ordinary integers, but the addition and multiplication, as well as equality, are modulo $p$. Furthermore, $-k$ and $k^{-1}$ denotes the additive and multiplicative inverses of $k$ in $\mathbb{F}_p$, respectively. If $s \in \mathbb{F}_p$, and $A$ has multiplicative order $p$, then $A^s$ simply indicates the $s$-th power of $A$, where $s$ is viewed as an integer.

We start by identifying the generators in $PGL(2, p)$ that correspond to presentation (11). Consider the following matrices in $GL(2, p)$:

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

where $t$ is a primitive root modulo $p$, i.e. a generator of $\mathbb{F}_p^\times$. Our guess is that $\overline{A}, \overline{B}, \overline{C}$ correspond to the generators $a, b, c$ in (11) respectively. The powers of these matrices are:

$$A^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}, \quad B^k = \begin{bmatrix} 1 & 0 \\ 0 & t^k \end{bmatrix}, \quad C^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \quad C^3 = I$$

for any integer $k$. Thus $|\overline{A}| = p$, $|\overline{B}| = p - 1$, and $|\overline{C}| = 3$. Also,

$$A^B = B^{-1} A B = \begin{bmatrix} 1 & 0 \\ t^{-1} & 1 \end{bmatrix} = A^s,$$

where $s = t^{-1}$ is also a primitive root modulo $p$. So $\overline{A^B} = \overline{A}^s$. Next we let

$$B_1 = (B^{t^{-1}})^A = \begin{bmatrix} 1 & 0 \\ -k & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -2k & -1 \end{bmatrix},$$
where we calculated $t^{-1}B_1 = -1$ as it is the unique element of order 2 in $\mathbb{F}_p^x$. Now check

$$CB_1 = \begin{bmatrix} -2k_1 & -1 \\ 2k_1 - 1 & 1 \end{bmatrix}, \quad (CB_1)^2 = \begin{bmatrix} 4k_1^2 - 2k_1 + 1 & 2k_1 - 1 \\ -(2k_1 - 1)^2 & 2 - 2k_1 \end{bmatrix}.$$  

Thus if we want $(CB_1)^2 = T$, $k_1$ must be $2^{-1} = \frac{p+1}{2}$. In this case,

$$B_1 = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \quad CB_1 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \quad (CB_1)^2 = T.$$

Let $B_3 = B^{A^k}$, $B_4 = B^{A^kj}$. As $k_3 - k_1 = k_1 - k_4$, we have $k_3 = 1 - k_4$.

$$B^{A^k} = \begin{bmatrix} 1 & 0 \\ k(t-1) & t \end{bmatrix}, \quad B_3C \cdot B_4 = \begin{bmatrix} 0 & 1 \\ -t & k_3(t-1) - t \end{bmatrix} \begin{bmatrix} 1 & 0 \\ k_4(t-1) & t \end{bmatrix},$$

whose $(1,1)$-entry is $k_4(t-1)$. If we want $(B_3)^{-1}B_4 = T$, i.e., $B_3CB_4 = T$, $k_4$ must be 0 since the $(1,1)$-entry of $C$ is 0 and $t \neq 1$. So $k_3 = 1 - k_4 = 1$,

$$B_3 = \begin{bmatrix} 1 & 0 \\ t - 1 & t \end{bmatrix}, \quad B_4 = \begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix} = B, \quad B_3CB_4 = \begin{bmatrix} 0 & 1 \\ -t & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} 0 & t \\ -t & -t \end{bmatrix} = C.$$

So far for $\overline{A}, \overline{B}, \overline{C}$ we have verified all the relations in (11). We can also prove that they are actually a set of generators for $PGL(2, p)$. Observe that each matrix in $GL(2, p)$ can be written as a product of some elementary matrices, which are

$$\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & t^j \end{bmatrix}, \quad \begin{bmatrix} t^i & 0 \\ 0 & 1 \end{bmatrix},$$

where $\alpha, \beta \in \mathbb{F}_{p}$ and $i, j \in \mathbb{K}_p$. They are generated by $A, A^T, B$ and $t^{-1}B$ respectively. So $PGL(2, p)$ is generated by $\overline{A}, \overline{A}^T$ and $\overline{B}$. Now check

$$B_1C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad A^{B_1C} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A^T,$$

due to $\overline{A}, \overline{B}$ and $\overline{C}$ generate $PGL(2, p)$. Hence setting $s = t^{-1}$, $k_1 = \frac{p+1}{2}$, $k_3 = 1$, $k_4 = 0$, we see that $PGL(2, p)$ is a quotient of the group $G$ in (11), in which $\overline{A}, \overline{B}$ and $\overline{C}$ correspond precisely to the generators $a, b$ and $c$ of $G$.

Remark 8: Note that we have not proved that (11) is a presentation of $PGL(2, p)$. To do that, one must show that the order of the group generated by $a, b, c$ in (11) is no more than $|PGL(2, p)| = (p - 1)p(p + 1)$. However, identifying possible corresponding generators still gives us a way to explicitly construct the subgroups to violate Ingleton.

Now we can write out the subgroups in $PGL(2, p)$ corresponding to subgroups in (10).
$G_1 = \langle C, B_1 \rangle$. Note that $|C| = 3$, $|B_1| = 2$, and $(C^2 B_1^2)^2 = T$, so $C^2 B_1^2 = B_1^2 C^2$ and $G_1$ has at most 6 elements $\{(B_1^i C^j) : 0 \leq i < 2, 0 \leq j < 3\}$. Calculating these elements we can see $|G_1| = 6$ exactly and thus indeed $G_1 \cong \mathbb{D}_6 \cong S_3$:

$$G_1 = \left\{ T, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \right\}.$$

$G_2 = \langle A, B \rangle$. We claim that $G_2$ is the subgroup of lower triangular matrices in $GL(2, p)$ modulo $V_p$, i.e.

$$G_2 = \left\{ \begin{bmatrix} 1 & 0 \\ \alpha & \beta \end{bmatrix} \mid \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_p^\times \right\}.$$

As $A, B$ are lower triangular, any element in $G_2$ is a lower triangular matrix modulo $V_p$. On the other hand, $\forall \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_p^\times, \beta = t^l$ for some integer $l$. So

$$\begin{bmatrix} 1 & 0 \\ \alpha & \beta \end{bmatrix} = A^\alpha B^l \Rightarrow \begin{bmatrix} 1 & 0 \\ \alpha & \beta \end{bmatrix} = A^\alpha B^l \in G_2.$$

Thus $|G_2| = p(p-1)$ and $G_2$ has presentation $\langle A, T \rangle$. Therefore $G_2 \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$ and achieves the desired flower structure.

$G_3 = \langle B_1^2(C^2), B_3 \rangle = \langle C B_1, B_3 \rangle$. Note that $|CB_1| = 2$, $|B_3| = |B| = p - 1$, also

$$B_3^k = \begin{bmatrix} 1 & 0 \\ t^k & -1 \end{bmatrix}, \quad B_3^{-1} = \begin{bmatrix} 1 & 0 \\ t^{-1} & -1 \end{bmatrix},$$

$$B_3 \cdot CB_1 = \begin{bmatrix} -1 & -1 \\ 1 - t & 1 \end{bmatrix} = \begin{bmatrix} -t^{-1} & -t^{-1} \\ t^{-1} & t^{-1} \end{bmatrix} = CB_1(B_3)^{-1},$$

so $G_3$ has at most $2(p-1)$ elements $\{(CB_1^i)(B_3^j) : 0 \leq i < 2, 0 \leq j < p - 1\}$. Calculating these elements we can see $|G_3| = 2(p-1)$ exactly and so $G_3 \cong D_{2(p-1)}$:

$$G_3 = \left\{ \begin{bmatrix} 1 & 0 \\ t^k & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & -1 \\ 1 - t^k & 1 \end{bmatrix} \mid k \in K_p \right\}.$$

$^3$We would end up with upper triangular matrices for $G_2$ if $A^T$ were used in place of $A$. But the two resulting groups are actually conjugate to each other, e.g. consider $x = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, $y = \begin{bmatrix} z & 0 \\ y & x \end{bmatrix}$ where $W = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. 


Finally, \( G_4 = \langle B_1C, B_4 \rangle \). \( B_1C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \), so \(|B_1C| = 2\), \(|B_4| = |B| = p - 1\). Also

\[
B_4 \cdot B_1C = \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} = \begin{bmatrix} 0 & t^{-1} \\ 1 & 0 \end{bmatrix} = B_1C(B_4)^{-1},
\]

so \( G_4 \) has at most \( 2(p - 1) \) elements \( \{(B_1C)^i(B_4)^j : 0 \leq i < 2, 0 \leq j < p - 1\} \). Calculating these elements we can see \(|G_4| = 2(p - 1)\) exactly and so \( G_4 \cong D_{2(p - 1)} \):

\[
G_4 = \left\{ (B_4)^k = \begin{bmatrix} 1 & 0 \\ 0 & t^k \end{bmatrix}, \ B_1C(B_4)^k = \begin{bmatrix} 0 & t^k \\ 1 & 0 \end{bmatrix} | k \in \mathbb{K}_p \right\}.
\]

These are all diagonal and anti-diagonal matrices in \( GL(2, p) \) modulo \( V_p \). We have already verified that \( (B_3)^2 = B_4^{-1} \), also \( (B_1C)^2 = B_1C \), thus indeed \( G_4 = G_3^C \).

With all four subgroups explicitly written, we can easily write down the intersections:

\[
G_{12} = \langle B_1 \rangle = \left\{ \bar{I}, \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} \right\} \cong \mathbb{Z}_2, \quad G_{13} = \langle CB_1 \rangle = \left\{ \bar{I}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \right\} \cong \mathbb{Z}_2,
\]

\[
G_{14} = \langle B_1C \rangle = \left\{ \bar{I}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \cong \mathbb{Z}_2, \quad G_{23} = \langle B_3 \rangle = \left\{ \begin{bmatrix} 1 & 0 \\ t^k & 1 \end{bmatrix} | k \in \mathbb{K}_p \right\} \cong \mathbb{Z}_{p-1},
\]

\[
G_{24} = \langle B_4 \rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & t^k \end{bmatrix} | k \in \mathbb{K}_p \right\} \cong \mathbb{Z}_{p-1}, \quad G_{34} = G_{123} = G_{124} = 1.
\]

\[
|G_{12}| = |G_{13}| = |G_{14}| = 2, \quad |G_{23}| = |G_{24}| = p - 1.
\]

So in (4), indeed \( \text{LHS} = |G_1||G_2||G_{34}||G_{123}||G_{124}| = 6p(p - 1)\), \( \text{RHS} = |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}| = 8(p - 1)^2\), \( \text{LHS} - \text{RHS} = 2(p - 1)(4 - p)\). Thus Ingleton is violated when \( p \geq 5 \), and the subgroup structures of \( S_5 \cong PGL(2, 5) \) are exactly reproduced.

\[\text{B. The Family } PGL(2, q)\]

With the explicit forms of the Ingleton-violating subgroups, we can extend the above violation to \( PGL(2, q) \), for each finite field order \( q \geq 5 \). Consider the finite field \( \mathbb{F}_q \). We know that \( q = p^m \) for some prime \( p \) (the characteristic of \( \mathbb{F}_q \)) and some integer \( m \). Since \( \mathbb{F}_p \) is the prime subfield of \( \mathbb{F}_q \), \( GL(2, p) \) is a subgroup of \( GL(2, q) \), which induces a copy of \( PGL(2, p) \) as a subgroup of \( PGL(2, q) \). Therefore, using the same subgroups of \( PGL(2, p) \) as in the previous section, we obtain a (trivial) Ingleton violation.
in $PGL(2, q)$ whenever the characteristic $p \geq 5$. Nevertheless, by extending the interpretations of these subgroups to $PGL(2, q)$, we can obtain a more general (nontrivial) violation, for each finite field order $q \geq 5$.

In the field $\mathbb{F}_q$, we continue to use the ordinary integers with modular arithmetic to represent the prime subfield $\mathbb{F}_p$. With this convention, all the matrices and subgroups in Section V-A are well defined, although now the cosets are taken with respect to $V_q$ rather than $V_p$. These subgroups constitute a trivial embedding of our previous violation in $PGL(2, q)$. However, in $PGL(2, q)$, the previous sets of generators do not guarantee that $G_2$ is the full subgroup of all lower triangular matrices, nor that $G_4$ contains all the diagonal and anti-diagonal matrices.

To address this issue, we redefine $t$ to be a primitive element of $\mathbb{F}_q$, i.e. $t$ generates $\mathbb{F}_q^\times$. Then $|B| = q - 1$. Also instead of a single $A$, we need to introduce more matrices to generate the subgroup $N \triangleq \{ \overline{A}_\alpha | \alpha \in \mathbb{F}_q \}$, where for each $\alpha \in \mathbb{F}_q$ we define

$$A_\alpha \triangleq \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}.$$ Clearly $A_\alpha A_\beta = A_{\alpha+\beta}$, and $A_\alpha^k = A_{\alpha k}$ for each integer $k$. Thus $|\overline{A}_\alpha| = p$ for each $\alpha \in \mathbb{F}_q^\times$. Observe that $\mathbb{F}_q$ is an $m$-dimensional vector space over $\mathbb{F}_p$, let $(\xi_1, \xi_2, \ldots, \xi_m)$ be a basis. Then $\forall \alpha \in \mathbb{F}_q$, $\alpha = \sum_{i=1}^m k_i \xi_i$ for some $k_1, k_2, \ldots, k_m \in \mathbb{F}_p$ and $A_\alpha = \prod_{i=1}^m A_{\xi_i}^{k_i}$. Also $\langle A_{\xi_i} \rangle \cap \langle A_{\xi_j} \rangle = 1$ for distinct $i$ and $j$. Thus

$$N = \langle A_{\xi_1}, A_{\xi_2}, \ldots, A_{\xi_m} \rangle \cong \langle A_{\xi_1} \rangle \times \langle A_{\xi_2} \rangle \times \ldots \times \langle A_{\xi_m} \rangle \cong \mathbb{Z}_p^m.$$ Actually, $N$ is isomorphic to the additive group of the vector space of $\mathbb{F}_q$ over $\mathbb{F}_p$ (Also see Section VII-A).

Let $G_2 = \langle A_{\xi_1}, A_{\xi_2}, \ldots, A_{\xi_m}, B \rangle = \langle N, B \rangle$. Similar to the previous section, it is easy to show that now $G_2$ is indeed the subgroup of all lower triangular matrices modulo $V_q$. For any $\alpha \in \mathbb{F}_q$, we have $A_{\alpha^{-1} \xi} = A_{\alpha^{-1}}$, so $N \triangleq G_2$ and $G_2 = NH$, where $H \triangleq \langle B \rangle$. Also $N \cap H = 1$, thus $G_2 \cong N \rtimes H \cong \mathbb{Z}_p^m \rtimes \mathbb{Z}_{q-1}$.

Although in general $G_2$ does not have presentation (7) or (8) anymore since $N$ is not necessarily cyclic, we can prove that it does have a “generalized flower structure” when $q > 2$, i.e. $(G_2 \setminus N) \cup \{T\}$ is the union of groups which are all isomorphic to $H$ with trivial pairwise intersections. Similar to the analysis of the $G_2$ in Section IV it suffices to show that $H^{\overline{A}_\alpha} \cap H = 1$, $\forall \overline{A}_\alpha \in N \setminus \{I\}$. But this is true since

\footnote{The only problem that may arise is when $p = 2$, $B_1 = (B^{\overline{A}_\alpha})^t \overline{A}_\alpha$ is not well defined. But we can circumvent that by directly working with the final matrix form of $B_1$.}
for each $\alpha \in \mathbb{F}_q^\times$ and some integers $k, l \in \mathbb{K}_q$,

$$(B^k)^{A\alpha} = B^l \iff B^k \cdot A_{\alpha} = A_{\alpha} \cdot B^l \iff \begin{bmatrix} 1 & 0 \\ t^k & t^l \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha & \alpha \end{bmatrix} \iff k = l = 0.$$
\[ G_4 = (B_4C, B_4). \] Now \(|B_4| = q-1\) and \(B_4^{-1}B_4C = B_4C(B_4)^{-1}\), so \(G_4 = \{(B_4^k, B_4C(B_4)^k \mid k \in \mathbb{F}_q\}\) = \{all diagonal and anti-diagonal matrices in \(PGL(2, q)\)\} \(\cong D_{2(q-1)}\).

The intersections are: \(G_{12} = (B_1), G_{13} = (CB_1)\), and \(G_{14} = (B_1C)\), which are all isomorphic to \(\mathbb{Z}_2\);
\(G_{23} = (B_3)\) and \(G_{24} = (B_4)\), both of which are isomorphic to \(\mathbb{Z}_q\); and \(G_{34} = G_{123} = G_{124} = 1\).

The orders of these subgroups are: \(|G_1| = 6, |G_2| = q(q-1), |G_3| = |G_4| = 2(q-1)\). For the intersections: \(|G_{12}| = |G_{13}| = |G_{14}| = 2, |G_{23}| = |G_{24}| = q - 1, |G_{34}| = |G_{123}| = |G_{124}| = 1\). So in \((4), LHS = |G_1||G_2||G_{13}||G_{14}| = 6q(q-1), RHS = |G_{12}||G_{13}||G_{14}||G_{23}||G_{24}| = 8(q-1)^2\), and \(LHS - RHS = 2(q-1)(4-q)\). Thus using these subgroups in \(PGL(2, q)\), Ingleton is violated for each finite field order \(q \geq 5\).

Remark 9: Depending on the characteristic \(p\) of \(\mathbb{F}_q\), the intersection \(G_{12} = (B_1)\) might lie in either the petals or the roots of \(G_2\), as depicted by the dashed circles in Fig. 2. If \(p \neq 2\), then \(q\) is odd and \(B_1 = (B_1^{2-1})\mathbb{1}_B\) where \(k_1 = 2^{-1} = \frac{q+1}{2}\), so \(G_{12}\) is on the petal \(H^{A_1}\). Whereas if \(p = 2\), then \(-1 = 1\) and \(B_1 = A = A_1 \in N\), so \(G_{12}\) becomes a root. Note that the patterns of the other intersections are not changed for different \(q\)’s.

Remark 10: We can also show that \(A_{\xi_1}, A_{\xi_2}, \ldots, A_{\xi_m}, B\) and \(C\) generate \(PGL(2, q)\), using the same argument as the previous section. The only difference is that the elementary matrices of \(GL(2, q)\) are now generated by \(A_{\xi_1}, A_{\xi_2}^T, \ldots, A_{\xi_m}, A_{\xi_m}^T, B\) and \(t^{-1}B\). But as \(A_{\alpha}^{B_1C} = A_{\alpha}^T\), \(\forall \alpha \in \mathbb{F}_q\), we see that \(PGL(2, q)\) is indeed generated by the desired elements.

Remark 11: The subgroups \(G_1-G_4\) have nice interpretations in the framework of group actions and groups of Lie type. Please refer to Appendix A for more details.

C. Generalizations of the Violation Family

We will generalize the above family of Ingleton violations in \(PGL(2, q)\) in two directions. On the one hand, \(PGL(2, q)\) is the quotient group of \(GL(2, q)\), so supposedly \(GL(2, q)\) should have a richer choice of subgroups and still keep the capability of violating Ingleton inequality. This approach is explored in the next section.

On the other hand, since the subgroups involved in the \(PGL(2, q)\) family has nice interpretations in terms of group actions, we can generalize this them in this framework. In Appendix A we follow this method to obtain two new families of violations in \(PGL(n, q)\) for general \(n\), and further generalize to an abstract construction using 2-transitive groups. Note that with Lemma 3 below, the families \(PGL(n, q)\) can also be easily extended to families of violations in \(GL(n, q)\).
VI. More Violations in $GL(2, q)$

As $PGL(2, q)$ is the quotient group of $GL(2, q)$ modulo the subgroup $V_q$ of scalar matrices, naturally one may ask if general linear groups also violate Ingleton. In fact, the following lemma shows that there is at least one set of subgroups in $GL(2, q)$ that violates Ingleton for all finite field orders $q \geq 5$:

**Lemma 3:** If $G$ is a finite group with normal subgroup $N$ such that $H \triangleq G/N$ has a set of Ingleton-violating subgroups, then the preimages of these subgroups under the natural homomorphism are subgroups of $G$ that also violate Ingleton.

**Proof:** Let $(H_i : 1 \leq i \leq 4)$ be a set of Ingleton-violating subgroups in $H$. Define $G_i$ to be the preimage of $H_i$ under the natural homomorphism $g \mapsto gN$, then $G_i$ is a group containing $N$ for each $i$. By the Lattice Isomorphism Theorem (see e.g. [19]), for any nonempty subset $\alpha \subseteq \{1, 2, 3, 4\}$, $G_\alpha/N = H_\alpha$, and so $|G_\alpha| = |H_\alpha| \cdot |N|$. Thus by checking the orders in (4), $(G_i : 1 \leq i \leq 4)$ also violate Ingleton.

Searching with GAP, we find $GL(2, 5)$ to be the smallest general linear group that violates Ingleton. Up to subscript symmetries and conjugations, it has 15 sets of Ingleton-violating subgroups. We would like to analyze their structures, generalize them for $q \geq 5$ if possible, and to relate them to the violation in the $PGL(2, q)$ case.

Throughout this section, we always assume $q$ is a finite field order, and $p$ is the characteristic of $\mathbb{F}_q$. We begin our analysis by identifying the preimages of the Ingleton-violating subgroups in the previous section under the natural homomorphism $\pi : GL(2, q) \rightarrow GL(2, q)/V_q = PGL(2, q)$, according to Lemma 3. With no surprise, when $q = 5$ these are conjugate to one of the 15 violation instances in $GL(2, 5)$, and they take on easy matrix structures similar to the subgroups in Section 5. From these subgroups we further deduce 10 other instances, all of which are essentially variants of the preimage subgroups: each instance differs from the preimages at exactly one subgroup (either $G_1$ or $G_2$). These 11 violation instances can be easily extended to families of Ingleton-violating subgroups in $GL(2, q)$ for $q \geq 5$, but when $p \neq 2$ sometimes we need the extra condition that $\frac{q-1}{2}$ be even. The remaining 4 instances cannot be derived directly from the preimages; however, they are interrelated and all their subgroups are equal or conjugate to some known subgroups from the previous 11 instances. They also generalize to Ingleton-violating families in $GL(2, q)$ with similar conditions as above, plus a limitation that $p \neq 3$.

Table I summarizes how the generalization of these instances depends on the values of $p$ and $q$. We can see that when $p = 2$, these 15 instances collapse to only 6 distinct ones; also some instances need
specific conditions on $p$ and $q$ to violate Ingelton.

In Table III the orders of the subgroups for the cases we have explored in $PGL(2, q)$ and $GL(2, q)$ are listed. No. 0 denotes the instance in $PGL(2, q)$, and No. 1–15 denote the generalizations of the 15 violation instances in $GL(2, 5)$ to $GL(2, q)$. Since all instances have the subgroup order symmetries

$$|G_3| = |G_4|, \quad |G_{123}| = |G_{124}|, \quad |G_{13}| = |G_{14}|, \quad |G_{23}| = |G_{24}|,$$

only one of each pair of orders is listed. Note that when $p = 2$, there are only 6 such distinct generalizations, which are Instances 1, 2, 6, 7, 12 and 14. Thus for the order calculation of all other instances in $GL(2, q)$ assume $p \neq 2$. Moreover, No. 8’, 9’, 13’ and 15’ correspond to Instances 8, 9, 13 and 15 when $p \neq 2$ but $\frac{q-1}{2}$ is odd, in which case Ingelton is satisfied. Finally, the order calculation for
Instances 12–15 only works for }p \neq 3{.}

Although in Table [II] we list the difference between the two sides of (4) to demonstrate if and when Ingleton is violated, it is not the correct quantity to measure the extent of violation for a given entropy vector. For that purpose, the difference

\[ h_1 + h_2 + h_{34} + h_{123} + h_{124} - (h_{12} + h_{13} + h_{14} + h_{23} + h_{24}) \]

for the original inequality (3) should be used, which in finite group context equals \( \log \frac{\text{RHS}}{\text{LHS}} \) of (4). Thus for a 4-tuple of subgroups \( \tau = (G_i : 1 \leq i \leq 4) \), we define the “Ingleton ratio”

\[ r(\tau) = \frac{|G_{12}||G_{13}||G_{14}||G_{23}||G_{24}|}{|G_1||G_2||G_{34}||G_{123}||G_{124}|} \]

(12)
to measure the extent to which Ingleton is violated. Clearly Ingleton fails iff \( r > 1 \). From Table [II] all violation instances listed have the same ratio

\[ r = \frac{4(q - 1)}{3q} \]

which approaches 4/3 when \( q \) is large.

In the following, we present all of these extended violation families, with Section [VI-A] being the set of preimage subgroups, Sections [VI-B] and [VI-C] the 10 variants, and Section [VI-D] the remaining 4 instances. We continue to use the notations from Section [V] with \( t \) being a primitive element of \( \mathbb{F}_q \), but we redefine

\[ N \triangleq \{ A_\alpha | \alpha \in \mathbb{F}_q \} = \langle A_{\xi_1}, A_{\xi_2}, \ldots, A_{\xi_m} \rangle \cong \langle A_{\xi_1} \rangle \times \ldots \times \langle A_{\xi_m} \rangle \cong \mathbb{Z}_{p}^{m} \]

In addition, we introduce the following matrices and subgroups in \( \text{GL}(2, q) \) to facilitate our presentation:

\[
B' = \begin{bmatrix} -1 & 0 \\ 0 & t \end{bmatrix}, \quad P = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}, \quad P' = \begin{bmatrix} t & 0 \\ 0 & -1 \end{bmatrix},
\]

\[
M = \langle C, B_1 \rangle = \left\{ I, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \right\},
\]

\[
K = \langle N, B \rangle = \left\{ \begin{bmatrix} 1 & \alpha \\ \alpha & \beta \end{bmatrix} | \alpha, \beta \in \mathbb{F}_q^\times \right\}, \quad K' = \langle N, B' \rangle = \left\{ \begin{bmatrix} (1)^k & 0 \\ \alpha & t^k \end{bmatrix} | \alpha \in \mathbb{F}_q, \right\},
\]

\[
J = \langle N, P \rangle = \left\{ \begin{bmatrix} \beta & 0 \\ \alpha & 1 \end{bmatrix} | \alpha, \beta \in \mathbb{F}_q^\times \right\}, \quad J' = \langle N, P' \rangle = \left\{ \begin{bmatrix} t^k & 0 \\ \alpha & (1)^k \end{bmatrix} | \alpha \in \mathbb{F}_q, \right\}.
\]

Note that when \( p = 2 \), we have \(-1 = 1\), so \( B' = B, P' = P \), and \( K' = K, J' = J \). Also note that \( M \) and \( K \) precisely correspond to the Section [V] groups \( G_1 \) and \( G_2 \) respectively. The group \( M \) is
isomorphic to $D_6 \cong S_3$, while the other four groups are all semidirect products $\mathbb{Z}_p^m \rtimes \mathbb{Z}_{q-1}$, with $K \cong J$ and $K' \cong J'$. Moreover, $K$ and $J$ have generalized flower structures for all $q > 2$. However, if $p \neq 2$, $K'$ and $J'$ only have flower structures when $\frac{q-1}{2}$ is even, in which case they are also isomorphic to $K$. (See Section B-A in Appendices for proofs.) This turns out to be a necessary condition to violate Ingleton in all the instances where $K'$ and $J'$ are involved.

A. Instance 1: The Preimage Subgroups

To obtain the preimage $H_0$ of a subgroup $H \leq \text{PGL}(2,q)$ under $\pi$, we can generate $H_0$ in $\text{GL}(2,q)$ with the generators of $H$ (without overlines) and $tI$, since $V_q = \langle tI \rangle \cong \mathbb{Z}_{q-1}$.

$G_1 = \langle tI, C, B_1 \rangle = \langle V_q, M \rangle$. Since $V_q$ is the center of $\text{GL}(2,q)$ and intersects $M$ trivially, $G_1$ is a direct product: $G_1 = \{ t^kX \mid X \in M, k \in K \} \cong V_q \times M \cong \mathbb{Z}_{q-1} \times S_3$.

$G_2 = \langle tI, A_{\xi_1}, A_{\xi_2}, \ldots, A_{\xi_m}, B \rangle = \langle tI, N, B \rangle = \langle V_q, K \rangle$. $G_2$ is the subgroups of all lower triangular matrices in $\text{GL}(2,q)$, and as $V_q \cap K = 1$, we have $G_2 \cong V_q \times K \cong \mathbb{Z}_{q-1} \times (\mathbb{Z}_p^m \rtimes \mathbb{Z}_{q-1})$.

$G_3 = \langle tI, B_1 C^2, B_3 \rangle = \langle tI, CB_1, B_3 \rangle = \langle CB_1, T \rangle$, where $T = \langle tI, B_3 \rangle$. As $V_q \cap \langle B_3 \rangle = 1$, we have $T = \{ t^k B_3^m \mid k, m \in K \} \cong V_q \times \langle B_3 \rangle \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$. It is easy to check that $(t^k B_3^m)^{CB_1} = t^{k+m} B_3^{-m} \in T$, so $G_3 = \langle CB_1 \rangle \cdot T$ and $T \trianglelefteq G_3$. Furthermore, $|CB_1| = 2$ and $T \cap \langle CB_1 \rangle = 1$, thus $G_3 \cong T \times \langle CB_1 \rangle \cong (\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \rtimes \mathbb{Z}_2$ and

$$G_3 = \left\{ t^k \begin{bmatrix} 1 & 0 \\ t^m & 1 \end{bmatrix}, \ t^{k+m} \begin{bmatrix} -1 & -1 \\ 1 - t^{-m} & 1 \end{bmatrix} \mid k, m \in K \right\}.$$

$G_4 = \langle tI, B_1 C, B_4 \rangle = \langle tI, B_1 C, B \rangle = \langle B_1 C, D \rangle$, where $D = \langle tI, B \rangle$. Since $V_q \cap \langle B \rangle = 1$, we have $D = \{ t^k B^m \mid k, m \in K \} = \{ \text{all diagonal matrices in } \text{GL}(2,q) \} \cong V_q \times \langle B \rangle \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$. Note that

$$
\begin{bmatrix}
\alpha & 0 \\
0 & \beta
\end{bmatrix}^{B_1 C}
= \begin{bmatrix}
\beta & 0 \\
0 & \alpha
\end{bmatrix} \in D,
$$

so $G_4 = \langle B_1 C \rangle \cdot D$ and $D \trianglelefteq G_4$. Since $|B_1 C| = 2$ and $D \cap \langle B_1 C \rangle = 1$, $G_4 \cong D \rtimes \langle B_1 C \rangle \cong (\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \rtimes \mathbb{Z}_2$. Actually $G_4$ is the subgroups of all diagonal and anti-diagonal matrices in $\text{GL}(2,q):

$$
G_4 = \left\{ \begin{bmatrix}
\alpha & 0 \\
0 & \beta
\end{bmatrix}, \begin{bmatrix}
0 & \beta \\
\alpha & 0
\end{bmatrix} \mid \alpha, \beta \in \mathbb{F}_q^\times \right\}.
$$

Calculating the intersections, we have $G_{12} = \langle tI, B_1 \rangle \cong V_q \times \langle B_1 \rangle$, $G_{13} = \langle tI, CB_1 \rangle \cong V_q \times \langle CB_1 \rangle$ and $G_{14} = \langle tI, B_1 C \rangle \cong V_q \times \langle B_1 C \rangle$, all of which are isomorphic to $\mathbb{Z}_{q-1} \times \mathbb{Z}_2$. Also, $G_{23} = T$, $G_{24} = D$ and $G_{34} = G_{123} = G_{124} = \langle tI \rangle = V_q$.

From the calculation in Table II Ingleton is violated when $q \geq 5$. 

TABLE III

<table>
<thead>
<tr>
<th>Ins. No.</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>(G_1 )</td>
<td>( \langle C, B_1 \rangle )</td>
<td>( \langle -C, B_1 \rangle )</td>
<td>( \langle C, -B_1 \rangle )</td>
<td>( \langle C, tB_1 \rangle )</td>
</tr>
</tbody>
</table>

B. Instances 2–5: Variants with Different \( G_1 \)'s

In all the instances in this section, only \( G_1 \) is different from Section [VI-A] it is now a proper subgroup of \( \langle tI, C, B_1 \rangle \) (see Table III where the generator-form for these groups is used to better demonstrate the subgroup relations). When \( p \neq 2 \), these instances are all distinct; however, when \( p = 2 \), clearly Instances 3 and 4 collapse to Instance 2, while Instance 5 becomes Instance 1. From Table III we can see that they all violate Ingleton when \( q \geq 5 \).

1) Instance 2: \( G_1 = M \).

\( G_{12} = \langle B_1 \rangle \), \( G_{13} = \langle CB_1 \rangle \) and \( G_{14} = \langle B_1C \rangle \) are all isomorphic to \( \mathbb{Z}_2 \), and \( G_{123} = G_{124} = 1 \).

2) Instance 3: \( G_1 = \langle -C, B_1 \rangle \).

We only consider the case \( p \neq 2 \), since otherwise this is the same as Instance 2. As \( |C| = 3 \), we have \( (-C)^3 = -I \) and \( (-C)^4 = C \). Thus \( G_1 = \langle -I, C, B_1 \rangle = \langle -I, M \rangle \cong \langle -I \rangle \times M \cong \mathbb{Z}_2 \times S_3 \cong D_{12} \), since \( \langle -I \rangle \) is a subgroup of \( V_q \) and intersects \( M \) trivially. So \( G_1 = \{ \pm X | X \in M \} \).

Now, \( G_{12} = \langle -I, B_1 \rangle \cong \langle -I \rangle \times \langle B_1 \rangle \), \( G_{13} = \langle -I, CB_1 \rangle \cong \langle -I \rangle \times \langle CB_1 \rangle \) and \( G_{14} = \langle -I, B_1C \rangle \cong \langle -I \rangle \times \langle B_1C \rangle \), all of which are isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). Furthermore, \( G_{123} = G_{124} = \langle -I \rangle \cong \mathbb{Z}_2 \).

3) Instance 4: \( G_1 = \langle C, -B_1 \rangle \).

Here we also need only consider the case \( p \neq 2 \). Observe that \( |C| = 3 \), \( |-B_1| = 2 \) and \( (C \cdot (-B_1))^2 = (CB_1)^2 = I \). This gives us \( G_1 = \{ I, C, C^2, -B_1, -B_1C, -CB_1 \} \), so \( G_1 \cong D_6 \cong S_3 \).

For the intersections, we have \( G_{12} = \langle -B_1 \rangle \), \( G_{13} = \langle -CB_1 \rangle \) and \( G_{14} = \langle -B_1C \rangle \) all isomorphic to \( \mathbb{Z}_2 \), and \( G_{123} = G_{124} = 1 \).

4) Instance 5: \( G_1 = \langle C, tB_1 \rangle \).

When \( p = 2 \), \( q \) is even. Since \( |B_1| = 2 \) and \( |t| = q - 1 \), we have \( (tB_1)^q = tI \) and \( (tB_1)^{q-1} = B_1 \). Thus \( G_1 = \langle tI, C, B_1 \rangle \) and this instance is the same as the preimage subgroups.

So assume \( p \neq 2 \). Here \( q \) is odd, so \( |tB_1| = q - 1 \). When \( k \) is even, \( (tB_1)^k = t^kI \) and so \( C^{(tB_1)^k} = C \). Otherwise \( (tB_1)^k = t^kB_1 \), then \( C^{(tB_1)^k} = B_1CB_1 = C^{-1} \) since \( (CB_1)^2 = I \). So \( G_1 = \langle tB_1 \rangle \cdot \langle C \rangle \) and \( \langle C \rangle \leq G_1 \). Furthermore, \( \langle tB_1 \rangle \cap \langle C \rangle = 1 \) and \( |C| = 3 \), thus \( G_1 \cong \langle C \rangle \times \langle tB_1 \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_{q-1} \) and \( G_1 = \{ t^kI, t^kC, t^kC^2 \mid k \in K_q \text{ and is even} \} \cup \{ t^kB_1, t^kB_1C, t^kCB_1 \mid k \in K_q \text{ and is odd} \} \).
The intersections are: $G_{12} = \langle tB_1 \rangle$, $G_{13} = \langle tCB_1 \rangle$ and $G_{14} = \langle tB_1 C \rangle$ are all isomorphic to $\mathbb{Z}_{q-1}$, and $G_{123} = G_{124} = \langle t^2 I \rangle \cong \mathbb{Z}_{q-1}^2$.

C. Instances 6–11: Variants with Different $G_2$’s

In all the instances in this section, only $G_2$ is different from Section VI-A; it is now a proper subgroup of $\langle tI, N, B \rangle$ (see Table IV). It is easy to see that these instances are distinct when $p \neq 2$; otherwise, Instances 8 and 10 collapse to Instance 6, while Instances 9 and 11 become Instance 7. Thus in the analysis of Instances 8–11, we assume $p \neq 2$. From Table II, Instances 6, 7, 10, 11 violate Ingleton whenever $q \geq 5$; however, if $p \neq 2$, Instances 8 and 9 only violate Ingleton when in addition $q-\frac{1}{2}$ is even. Please refer to Section B-B in Appendices for the calculation of subgroup intersections in Instances 8 and 9.

1) Instance 6: $G_2 = K$.

In this case, $G_{12} = \langle B_1 \rangle \cong \mathbb{Z}_2$ and $G_{123} = G_{124} = 1$. Also, $G_{23} = \langle B_3 \rangle$ and $G_{24} = \langle B \rangle$, both of which are isomorphic to $\mathbb{Z}_{q-1}$.

2) Instance 7: $G_2 = J$.

Now, $G_{12} = \langle -B_1 \rangle \cong \mathbb{Z}_2$ and $G_{123} = G_{124} = 1$. Here, $G_{23} = \langle t^{-1}B_3 \rangle$ and $G_{24} = \langle P \rangle$, both isomorphic to $\mathbb{Z}_{q-1}$.

3) Instance 8: $G_2 = K'$.

\[
G_{12} = \begin{cases} \langle B_1 \rangle \cong \mathbb{Z}_2 & \text{if } \frac{q-1}{2} \text{ is even} \\ \langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise} \end{cases}, \quad G_{123} = G_{124} = \begin{cases} 1 & \text{if } \frac{q-1}{2} \text{ is even} \\ \langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise} \end{cases}.
\]

In this case, $G_{23} = \langle -B_3^{q+1} \rangle$ and $G_{24} = \langle B' \rangle$ are both isomorphic to $\mathbb{Z}_{q-1}$.

4) Instance 9: $G_2 = J'$.

\[
G_{12} = \begin{cases} \langle -B_1 \rangle \cong \mathbb{Z}_2 & \text{if } \frac{q-1}{2} \text{ is even} \\ \langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise} \end{cases}, \quad G_{123} = G_{124} = \begin{cases} 1 & \text{if } \frac{q-1}{2} \text{ is even} \\ \langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise} \end{cases}.
\]

Here, $G_{23} = \langle tB_3^{q+3} \rangle$ and $G_{24} = \langle P' \rangle$ are isomorphic to $\mathbb{Z}_{q-1}$.
are as follows. The conjugators \( E, Q, W \) and the elements of new subgroups are as follows.

<table>
<thead>
<tr>
<th>Ins. No.</th>
<th>( G_1 )</th>
<th>( G_2 )</th>
<th>( G_3 )</th>
<th>( G_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>( M )</td>
<td>( \langle N, B \rangle )</td>
<td>( \langle N, P \rangle^E )</td>
<td>( \langle N, P \rangle^Q )</td>
</tr>
<tr>
<td>13</td>
<td>( M )</td>
<td>( \langle N, B' \rangle )</td>
<td>( \langle N, P' \rangle^E )</td>
<td>( \langle N, P' \rangle^Q )</td>
</tr>
<tr>
<td>14</td>
<td>( M )</td>
<td>( \langle N, P' \rangle^E )</td>
<td>( \langle N, B \rangle )</td>
<td>( \langle N, B \rangle^W )</td>
</tr>
<tr>
<td>15</td>
<td>( M )</td>
<td>( \langle N, P' \rangle^E )</td>
<td>( \langle N, B' \rangle )</td>
<td>( \langle N, B' \rangle^W )</td>
</tr>
</tbody>
</table>

5) Instance 10: \( G_2 = \langle -I, N, B \rangle \).

Now we have \( G_2 = \langle -I, K \rangle \cong \langle -I \rangle \times K \cong \mathbb{Z}_2 \times (\mathbb{Z}_p^m \times \mathbb{Z}_{q-1}) \), since \( \langle -I \rangle \cap K = 1 \). Thus \( G_2 = \{ \pm X \mid X \in K \} \).

For the intersections, we have \( G_{12} = \langle -I, B_1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \) and \( G_{123} = G_{124} = \langle -I \rangle \cong \mathbb{Z}_2 \). Also, \( G_{23} = \langle -I, B_3 \rangle \cong \langle -I \rangle \times \langle B_3 \rangle \) and \( G_{24} = \langle -I, B \rangle \cong \langle -I \rangle \times \langle B \rangle \), both of which are isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_{q-1} \).

6) Instance 11: \( G_2 = \langle -I, N, P \rangle \).

Here \( G_2 = \langle -I, J \rangle \cong \langle -I \rangle \times J \cong \mathbb{Z}_2 \times (\mathbb{Z}_p^m \times \mathbb{Z}_{q-1}) \), since \( \langle -I \rangle \cap J = 1 \). Thus \( G_2 = \{ \pm X \mid X \in J \} \).

Moreover, \( G_{12} = \langle -I, B_1 \rangle = \langle -I, B_1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \) and \( G_{123} = G_{124} = \langle -I \rangle \cong \mathbb{Z}_2 \). Also, \( G_{23} = \langle -I, t^{-1}B_3 \rangle \cong \langle -I \rangle \times \langle t^{-1}B_3 \rangle \) and \( G_{24} = \langle -I, P \rangle \cong \langle -I \rangle \times \langle P \rangle \) are both isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_{q-1} \).

D. Instances 12–15

For these last four instances, \( G_1 \) is always \( M \), \( G_2 - G_4 \) are equal or conjugate to one of \( K, K', J, J' \), as listed in Table V. Thus \( G_2 - G_4 \) are all semidirect products \( \mathbb{Z}_p^m \rtimes \mathbb{Z}_{q-1} \), and the structures of \( G_3 \) and \( G_4 \) are different from all previous instances. The conjugators \( E, Q, W \) and the elements of new subgroups are as follows.

\[
E = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \quad W = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.
\]

\[
J^E = \langle N, P \rangle^E = \left\{ \begin{bmatrix} 1 - v & \nu \\ 1 - u - v & u + v \end{bmatrix} \mid u \in \mathbb{F}_q^*, \nu \in \mathbb{F}_q \right\},
\]

\[
(J')^E = \langle N, P' \rangle^E = \left\{ \begin{bmatrix} (-1)^j - \alpha & \alpha \\ (-1)^j - t^j - \alpha & t^j + \alpha \end{bmatrix} \mid \alpha \in \mathbb{F}_q, j \in \mathbb{K}_q \right\}.
\]
\[ J^Q = \langle N, P \rangle^Q = \left\{ \begin{bmatrix} 1 + 2y & y \\ 2(x - 2y - 1) & x - 2y \end{bmatrix} \mid x \in \mathbb{F}_q^x, y \in \mathbb{F}_q \right\}, \]

\[ (J')^Q = \langle N, P' \rangle^Q = \left\{ \begin{bmatrix} (1 + 2\beta) & \beta \\ 2(t^i - 2\beta - (-1)^i) & t^i - 2\beta \end{bmatrix} \mid \beta \in \mathbb{F}_q, i \in K_q \right\}, \]

\[ K^W = \langle N, B \rangle^W = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{F}_q^x, y \in \mathbb{F}_q \right\} = \{ X^T \mid X \in J \}, \]

\[ (K')^W = \langle N, B' \rangle^W = \left\{ \begin{bmatrix} t^i & \beta \\ 0 & (-1)^i \end{bmatrix} \mid \beta \in \mathbb{F}_q, i \in K_q \right\} = \{ X^T \mid X \in J' \}. \]

As mentioned before, Instances 12–15 do not violate Ingleton when \( p = 3 \). In this case, we have \( 2 = -1 \), so \( E = Q \) and \( M \leq J^E \). Thus in Instance 12 we have \( G_3 = G_4 \) and \( G_1 \leq G_3 \), while in Instances 13 and 14 we have \( G_3 = G_4 \) and \( G_1 \leq G_2 \) respectively. So these three instances satisfy Conditions 5 and/or 7. Instance 15, however, satisfies Condition 3 in this case (see Section B-C in Appendices).

Besides \( p \neq 3 \), we also need \( p \neq 2 \) to make Instances 13 and 15 distinct violations: otherwise they collapse to Instances 12 and 14 respectively. Thus in the rest of this section, we always assume \( p \neq 3 \), while for Instances 13 and 15 we assume \( p > 3 \). From Table II, Instances 12 and 14 violate Ingleton when \( q \geq 5 \) (and of course, \( p \neq 3 \)), while if \( p \neq 2 \), Instances 13 and 15 only violate Ingleton when in addition \( \frac{q-1}{2} \) is even. Please refer to Section B-D in Appendices for the intersection calculations.

1) Instance 12: \( G_2 = K, G_3 = J^E, G_4 = J^Q \).

We have \( G_{12} = \langle B_1 \rangle, G_{13} = \langle B_1C \rangle \) and \( G_{14} = \langle CB_1 \rangle \) all isomorphic to \( \mathbb{Z}_2 \), and \( G_{34} = G_{123} = G_{124} = 1 \). Furthermore,

\[ G_{23} = \left\{ \begin{bmatrix} 1 & 0 \\ 1 - t^j & t^j \end{bmatrix} \mid j \in K_q \right\} = \langle P \rangle^E, \quad G_{24} = \left\{ \begin{bmatrix} 1 & 0 \\ 2(t^i - 1) & t^i \end{bmatrix} \mid i \in K_q \right\} = \langle P \rangle^Q \]

both are isomorphic to \( \mathbb{Z}_{q-1} \).

2) Instance 13: \( G_2 = K', G_3 = (J')^E, G_4 = (J')^Q \).

When \( \frac{q-1}{2} \) is even, \( G_{12}, G_{13}, G_{14} \) and \( G_{34} \) are the same as in Instance 12. Otherwise \( G_{12} = G_{13} = G_{14} = 1 \) and \( G_{34} = -I \cong \mathbb{Z}_2 \). \( G_{123} \) and \( G_{124} \) are always trivial. Also,

\[ G_{23} = \left\{ \begin{bmatrix} (1)^j & 0 \\ (1)^j - t^j & t^j \end{bmatrix} \mid j \in K_q \right\} = \langle P' \rangle^E, \quad G_{24} = \left\{ \begin{bmatrix} (1)^i & 0 \\ 2(t^i - (1)^i) & t^i \end{bmatrix} \mid i \in K_q \right\} = \langle P' \rangle^Q \]

are both isomorphic to \( \mathbb{Z}_{q-1} \).
3) Instance 14: \( G_2 = J^E, G_3 = K, G_4 = K^W \).

Observe that \( G_2 \) and \( G_3 \) are obtained from swapping the corresponding subgroups from Instance 12. Therefore \( G_{12} \) and \( G_{13} \) are also swapped while \( G_{23} \) remains the same. It turns out that \( G_{14}, G_{34}, G_{123} \) and \( G_{124} \) are also the same as in Instance 12. Furthermore,

\[
G_{24} = \left\{ \begin{bmatrix} t^i & 1 - t^i \\ 0 & 1 \end{bmatrix} \mid i \in K_q \right\} = \langle B \rangle^W \cong \mathbb{Z}_{q-1}.
\]

4) Instance 15: \( G_2 = (J')^E, G_3 = K', G_4 = (K')^W \).

In this case, \( G_2 \) and \( G_3 \) from Instance 13 are swapped to yield the corresponding subgroups here. So \( G_{12} \) and \( G_{13} \) are also swapped while \( G_{23} \) stays the same. Moreover, \( G_{14}, G_{34}, G_{123} \) and \( G_{124} \) are the same as in Instance 13, both when \( \frac{q-1}{2} \) is even and otherwise. Finally,

\[
G_{24} = \left\{ \begin{bmatrix} t^i & (-1)^i - t^i \\ 0 & (-1)^i \end{bmatrix} \mid i \in K_q \right\} = \langle B' \rangle^W \cong \mathbb{Z}_{q-1}.
\]

VII. GROUP NETWORK CODES USING THE (PROJECTIVE) GENERAL LINEAR GROUPS

We can use our Ingleton-violating groups to construct group network codes. From Section I-C, the resulting entropy vectors are characterizable by the subgroups used, thus have the capability of violating the Ingleton inequality. In contrast, the entropy vectors of linear network codes always respect the Ingleton inequality. Furthermore, let \( G \) be any of \( PGL(n, p), PGL(n, q), GL(n, p) \) or \( GL(n, q) \). In the following, we will show that linear network codes can be embedded in the group network codes using direct products of copies of \( G \). Apparently a direct product of any copies of an Ingleton-violating group still violates Ingleton, thus such classes of group network codes are strictly more powerful than linear network codes.

To construct a group network code, the choices of subgroups are not arbitrary: they should meet requirements (R1)–(R3). In particular, (R1) limits what subgroups can be associated with the sources: we need to satisfy

\[
\prod_{s \in S} |G_s| = \frac{|G|^{|S|-1}|G_S|}{|G|}.
\]

When this is the case, we simply say the subgroups \( \{ G_s : s \in S \} \) are independent. We will study the constructions of independent source subgroups in the context of \( PGL(2, q) \) and \( GL(2, q) \) (since they have simpler structures than general \( PGL(n, q) \) and \( GL(n, q) \)), and also provide a universal source subgroup construction for direct products of groups.
A. Embeddings of Linear Network Codes

As remarked in Section I-C, linear network codes are a special type of group network codes. Consider a linear network code $C$ over a finite field $F$. For each $t \in S \cup E$, the alphabet $Y_t$ is a finite dimensional vector space over $F$. Let $v$ denote the concatenation of all the source vectors $(Y_s : s \in S)$, then $v$ is a vector in $V \triangleq \bigoplus_{s \in S} U_s$, where $U_s \triangleq Y_s$. Then for each edge $e$, the global mapping $\varphi_e$ is a linear transformation from $V$ to $Y_e$, whose range is denoted by $U_e$. Also for each source $s$, let $\varphi_s$ be the linear transformation that maps $v \in V$ to its part from $s$, which we call the $s$-th section. Thus for all $t \in S \cup E$, we can write $Y_t = \varphi_t(v)$. Let $W_t$ be the null space of $\varphi_t$, then by the First Isomorphism Theorem, $\psi_t : v + W_t \mapsto \varphi_t(v)$ is a vector space isomorphism between the quotient space $V/W_t$ and $U_t$.

Let $t$ be an edge or a sink node. If $Y_f = 0$ for all $f \in I(t)$, then $Y_t = 0$ as the encoding/decoding functions are linear. Thus $\bigcap_{f \in I(t)} W_f \leq W_t$. Further, for each source $s$

$$W_s = \{v \in V \mid \text{the } s\text{-th section of } v \text{ is 0}\} \cong \bigoplus_{r \in S \setminus \{s\}} U_r,$$

so $\bigcap_{s \in S} W_s = 0$. Since $V/W_s \cong U_s$, we have $\prod_{s \in S} |V/W_s| = |V|$. Let $G = V$, $G_t = W_t$ for all $t \in S \cup E$, then it is straightforward to check that the requirements (R1)–(R3) are all satisfied, so we can define a group network code $C'$ with these groups.

This network code is equivalent to $C$, since $\{\psi_t : t \in S \cup E\}$ provides a set of bijections between their codewords at each source/edge, and these bijections respect the encoding/decoding operations. In particular, assume in $C$ the source vectors yield some $v \in V$. Then $Y_t = \varphi_t(v)$ is transmitted at each source/edge $t$, and with $\psi_t$ the corresponding symbol for $C'$ is $v + W_t^5$. So by Proposition 1 the encoding/decoding result of $C'$ at each edge/sink node is consistent with $C$.

For example, Fig 3 demonstrates a linear network code over $F_q$ for the well-known butterfly network (Fig. 3(a)), and the corresponding group network code (Fig. 3(b),(c)). Here, for the linear network code, we have $V = F_q^2$, $U_1 = U_2 = U_{e_{34}} = F_q$, while $W_1 = \{(0, x) : x \in F_q\}$, $W_2 = \{(y, 0) : y \in F_q\}$, and $W_{e_{34}} = \{(z, -z) : z \in F_q\}$. If we set $G = V$, $G_1 = W_1$, $G_2 = W_2$, and $G_3 = W_{e_{34}}$, then the resulting group network code is equivalent to the original linear one.

From the discussion above, we observe that linear network codes are determined by the underlying additive group structure. The direct sum $V$ can be called the ambient vector space of the linear network.

5Note that cosets are written additively for vector spaces.
code. Let \((V, +)\) denote the additive group of \(V\). If we can find a finite group \(G\) such that \((V, +) \leq G\), then the linear network code is said to be embedded in the group network codes using \(G\), since we can use subgroups of \(G\) to construct an equivalent group network code.

Consider a linear network code with ambient vector space \(V = \mathbb{F}_q^n\) for some \(n\) and \(q\), where \(q = p^m\) for some prime \(p\) and some integer \(m\). Observing that \(\mathbb{F}_q\) is an \(m\)-dimensional vector space over \(\mathbb{F}_p\), we can establish the following facts:

1) \((\mathbb{F}_p, +) \cong \mathbb{Z}_p\),

2) \((\mathbb{F}_q, +) \cong (\mathbb{F}_p, +)^m \cong \mathbb{Z}_p^m\),

3) \((V, +) \cong (\mathbb{F}_q, +)^n \cong \mathbb{Z}_p^{mn}\).

Thus it is fairly easy to see that \((V, +)\) is embedded in the direct product of \(m \cdot n\) copies of a group \(G\), provided that \(G\) contains an element of order \(p\). (By Cauchy’s theorem, this is equivalent to \(p\) divides \(|G|\).) From this fact, we deduce that linear network codes over \(\mathbb{F}_q\) are embedded in the group network codes using direct products of copies of \(G^m\). In particular, let \(G\) be any of the linear groups \(PGL(2, p)\), \(PGL(2, q)\), \(GL(2, p)\) or \(GL(2, q)\). We have the following embeddings in these groups, using properties of the matrix \(A\) and the subgroup \(N\):

1) In \(PGL(2, p)\), \(|A| = p\). So \((V, +) \cong (A)^{mn} \leq PGL(2, p)^{mn}\).

2) In \(GL(2, p)\), \(|A| = p\). So \((V, +) \cong (A)^{mn} \leq GL(2, p)^{mn}\).

3) In \(PGL(2, q)\), \(N = \{\overline{A_0} | \alpha \in \mathbb{F}_q\} \cong \mathbb{Z}_p^m\). So \((V, +) \cong N^n \leq PGL(2, q)^n\).
4) In $GL(2, q)$, $N = \{ A_\alpha | \alpha \in F_q \} \cong \mathbb{Z}_p^n$. So $(V, +) \cong N^n \leq GL(2, q)^n$.

Therefore, linear network codes over $\mathbb{F}_q$ are embedded in the group network codes using direct products of copies of $G$.

It is straightforward to extend these embedding results for the above linear groups from degree 2 to degree $n$, since the former are subgroups of the latter. For example, $GL(2, q)$ is a subgroup of $GL(n, q)$.

**B. Independent Sources Requirement**

If we want to utilize the Ingleton-violating groups $PGL(2, q)$ and $GL(2, q)$ to construct network codes, we need to find their independent subgroups. GAP searching shows that up to conjugation, $PGL(2, 5)$ has 16 independent pairs of subgroups, 1 triple and no quadruple. For $GL(2, 5)$, the numbers are 86, 14 and 0, respectively. It might be desirable to use some of the Ingleton-violating subgroups as sources, but we find no independent pairs in any violation instance in either $PGL(2, 5)$ or $GL(2, 5)$. Furthermore, we have the following negative results:

**Lemma 4:** Let $i, j \in \{1, 2, 3, 4\}$ and $(i, j) \neq (3, 4)$. For four random variables $X_1, X_2, X_3$ and $X_4$, if $X_i$ and $X_j$ are independent, then the Ingleton inequality (3) is satisfied.

**Proof:** By symmetry of (3), we only need to prove the result for when $(i, j) = (1, 2)$ or $(1, 3)$. In the first case, $h_{12} = h_1 + h_2$, so

$$h_{12} + h_{13} + h_{14} + h_{23} + h_{24} \geq h_1 + h_2 + h_3 + h_{123} + h_4 + h_{124}$$

$$\geq h_1 + h_2 + h_{34} + h_{123} + h_{124},$$

where we used $h_{13} + h_{23} \geq h_3 + h_{123}$ and $h_{14} + h_{24} \geq h_4 + h_{124}$ by submodularity of entropy. The second case is similar. 

**Corollary 1:** There is no independent triple or quadruple in a set of four subgroups that violates (4).

On another note, if we want to use the Ingleton-violating subgroups in the network, Proposition 2 tells us that their intersection should contain the intersection of the source subgroups. Since, in $PGL(2, q)$, the intersection of the Ingleton-violating subgroups is trivial, we need to find trivially intersecting independent subgroups to serve as sources. In $PGL(2, 5)$, there are 4 such pairs and no such triples. At least one of these pairs also extends to most general $PGL(2, q)$:

**Proposition 4:** Let $\mathbf{U} = \begin{bmatrix} 0 & -1 \\ t & 0 \end{bmatrix} \in PGL(2, q)$, and let $H$ be the image of $SL(2, q)$ in $PGL(2, q)$ under the natural homomorphism, which is isomorphic to $PSL(2, q)$. When $p \neq 2$, $H$ and $\langle \mathbf{U} \rangle$ are independent in $PGL(2, q)$ with trivial intersection.
**Proof:** It is easy to see $|\mathcal{U}| = 2$, $\det U = t$. The determinant of any matrix representing an element in $H$ takes the form $t^{2k} \in \langle t^2 \rangle$, for some $k$. But $t \not\in \langle t^2 \rangle$ as $q - 1$ is even, so $H \cap \mathcal{U} = \emptyset$. Also $|\mathcal{U}| \cdot |H| = 2 \cdot |SL(2, q)|/2 = |SL(2, q)| = |PGL(2, q)|$, thus (13) holds. \[\square\]

In $GL(2, q)$ there are more Ingleton-violating instances, which have various intersections. So the requirement on the sources is not so strict and we have a richer class of subgroups to work with. As in $PGL(2, q)$, there exist trivially intersecting independent pairs, for example:

**Proposition 5:** In $GL(2, q)$, $SL(2, q)$ and $\langle B \rangle$ (or $\langle P \rangle$) are independent with trivial intersection.

**Proof:** Obviously $\det B^k = 1$ iff $B^k = I$, so $SL(2, q)$ and $\langle B \rangle$ have trivial intersection. Also $|B| \cdot |SL(2, q)| = (q - 1) \cdot |GL(2, q)|/\phi(q - 1) = |GL(2, q)|$, thus (13) is satisfied. The proof for $\langle P \rangle$ is similar. \[\square\]

Generally it is not easy to find many independent subgroups in a group. If the group is a direct product of $n$ of its subgroups, however, it admits a natural construction of $n$ independent subgroups:

**Proposition 6:** If $G = G_1 \times G_2 \times \cdots \times G_n$, then $1 \times G_2 \times \cdots \times G_n$, $G_1 \times 1 \times \cdots \times G_n$, $\ldots$, and $G_1 \times G_2 \times \cdots \times 1$ are $n$ trivially intersecting independent subgroups in $G$.

**Proof:** Trivial intersection is obvious, and it is easy to check that both sides of (13) are equal to $\prod_{i=1}^n |G_i|^{n-1}$. \[\square\]

This construction is the generalization of the source construction for linear network codes, in which case the subgroup at source $s$ is the $W_s$ defined in Section VII-A. Also we see that using direct products we can obtain independent subgroups for an arbitrary number of sources.

If we further require the sources to be of the same alphabet size, then the independent subgroups must have the same order. In the above proposition, this can be achieved by choosing a single subgroup $H$, and setting $G_i = H$ for each $i$. Additionally, for an arbitrary pair of independent subgroups, we can achieve this requirement in the manner described by the following proposition.

**Proposition 7:** If $G_s$ and $G_r$ are independent in $G$, then $G_s \times G_r$ and $G_r \times G_s$ are independent in $G^2$ with the same order.

**Proof:** Since $G_s$ and $G_r$ are independent in $G$, $|G_s||G_r| = |G||G_s \cap G_r|$. The LHS and RHS of (13) are $|G_s|^2|G_r|$ and $|G|^2|G_s \cap G_r|^2$ respectively, which are equal. \[\square\]

**VIII. Conclusion**

Using a refined search we found the smallest group to violate the Ingleton inequality to be the 120 element group $S_5$. Investigating the detailed structure of the subgroups allowed us to determine that this is an instance of the Ingleton-violating family of groups $PGL(2, p)$ for primes $p \geq 5$. We have
begun investigating $PGL(2, p^q)$ groups and conjecture that they violate Ingleton for large enough $p$ and $q$. Computer search verifies that $PGL(2, 2^2)$ does not violate Ingleton, whereas $PGL(2, 2^3)$ and $PGL(2, 3^2)$ do. Finally, investigating the use of these groups to construct network codes more powerful than linear ones may be a fruitful direction for future work.

APPENDIX A

INTERPRETATION AND GENERALIZATIONS OF VIOLATION IN $PGL(2, q)$ USING THEORY OF GROUP ACTIONS

Instead of invertible matrices, we can also regard a general linear group as the group of all invertible linear transformations on a vector space. In this appendix, we take this point of view and consider the actions of linear groups on their corresponding projective geometries. Such actions induce a permutation representation for each general linear group on its projective geometry, and the projective linear groups are naturally defined in this framework. Using the theory of group actions, we show that the Ingleton violation in $PGL(2, q)$ from Section V has a nice interpretation: each subgroup is some sort of stabilizer for a set of points in the projective geometry. Furthermore, based on this understanding, we generalize the construction in $PGL(2, q)$ to two new families of Ingleton violations in $PGL(n, q)$ for a general $n$. Also we provide an abstract construction in 2-transitive groups generalizing these ideas.

Throughout this appendix we assume basic knowledge in the theory of group actions, which can be found in standard group theory textbooks. In particular, we make extensive use of the orbit-stabilizer theorem (see e.g. [19, Sec. 4.1, Prop. 2]), especially when calculating the order of a subgroup. Most notations are standard abstract algebra notations, see e.g. [19]; the rest are introduced when they first appear.

This appendix is mostly based on Prof. M. Aschbacher’s correspondences with us. We have expanded on certain details for clarity.

A. Preliminaries for Linear Groups

Let $V$ be an $n$-dimensional vector space over a field $F$. Recall $GL(V)$ and $SL(V)$ are the general linear group and special linear group on $V$, respectively. They are examples of groups of Lie type, a notion which is not totally well defined.

Each group $G$ of Lie type possesses a building, a simplicial complex on which $G$ is represented as a group of automorphisms. Recall a (abstract) simplicial complex consists of a set $X$ of vertices together
with a set of nonempty subsets of \( X \) called simplices; the only axiom says that each nonempty subset of a simplex is a simplex.

**Example A.1:** Let \( X \) be a partially ordered set. The order complex of \( X \) is the simplicial complex with vertex set \( X \) and with the simplices the nonempty chains in the poset.

**Example A.2:** The projective geometry \( PG(V) \) of \( V \) is the poset of nonzero proper subspaces of \( V \), partially ordered by inclusion. The building of \( GL(V) \) and \( SL(V) \) is the order complex of this poset. Of course \( GL(V) \) permutes the subspaces of \( V \), supplying a representation of \( GL(V) \) on \( PG(V) \) whose kernel is the subgroup of scalar maps. The images of \( GL(V) \) and \( SL(V) \) in \( Aut(PG(V)) \) are the projective general linear group \( PGL(V) \) and projective special linear group \( PSL(V) \). Write \( GL(n, F) \), \( SL(n, F) \), \( PGL(n, F) \), \( PSL(n, F) \) for the corresponding group when \( \dim(V) = n \) and the field is \( F \).

**Example A.3:** Specialize to the case \( n = 2 \). Then \( PG(V) \) consists of the points of \( V \); i.e. the 1-dimensional subspaces of \( V \). This is the so-called projective line. Let \( \mathcal{X} = \{x_1, x_2\} \) be a basis of \( V \). We regard the projective line as \( \Omega = F \cup \{\infty\} \), where \( \infty \) denotes \( F \cdot x_1 \) and for \( e \in F \), \( e \) denotes \( F(e \cdot x_1 + x_2) \). Then given an invertible matrix

\[
M(a, b, c, d) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}
\]

in \( GL(V) \), one can check that, subject to the identification of \( PG(V) \) with \( \Omega \), \( M(a, b, c, d) \) acts on \( \Omega \) via

\[
M(a, b, c, d) : x \mapsto \frac{ax + b}{cx + d},
\]

where arithmetic involving \( \infty \) is suitably interpreted; e.g. \( (a\infty + b)/(c\infty + d) = a/c \) if \( c \neq 0 \) and \( \infty \) if \( c = 0 \). So we can regard \( PGL(V) = PGL(2, F) \) as the group of these projective linear maps \( M(a, b, c, d), ad - bc \neq 0 \) on the projective line \( \Omega \).

The following result is well known and easy to prove:

**Lemma A.1:** \( PGL(2, F) \) is sharply 3-transitive on the projective line \( PG(V) \). That is, \( PGL(V) \) is transitive on ordered 3-tuples of distinct points, and only the identity fixes three points.

Next we introduce several types of subgroups for these linear groups.

A **Borel subgroup** of a group \( G \) of Lie type is the stabilizer of a maximal simplex in its building.

**Example A.4:** A maximal simplex in \( PG(V) \) is a flag \( \tau = (0 < V_1 < \cdots < V_{n-1} < V) \), where \( \dim(V_k) = k \). If we pick a basis \( \mathcal{X} = \{x_1, \ldots, x_n\} \) for \( V \) such that \( V_k = \langle x_i : 1 \leq i \leq k \rangle \), then the Borel subgroup stabilizing \( \tau \) is the subgroup whose matrices with respect to \( \mathcal{X} \) are the upper triangular invertible matrices.
Let $G = PGL(2, F)$. By definition, the stabilizers $G_{F_{x_1}} = G_\infty$ and $G_{F_{x_2}} = G_0$ are both Borel subgroups of $G$. The matrices of these subgroups are upper triangular and lower triangular respectively. As $G$ is transitive on $\Omega$, for each of $u = \infty, 0$ we have the bijection $gG_u \mapsto g(u)$ of the coset space $G/G_u$ with $\Omega$.

Buildings have certain special subcomplexes called apartments. For a group $G$ of Lie type, the pointwise stabilizer of an apartment is called a Cartan subgroup of $G$.

Example A.5: In the projective geometry, the apartments are of the form $\Sigma(\mathcal{X})$ for $\mathcal{X} = \{x_1, \cdots, x_n\}$ a basis for $V$, where $\Sigma(\mathcal{X})$ consists of the subspaces spanned by nonempty proper subsets of $\mathcal{X}$. The matrices in the Cartan subgroup stabilizing $\Sigma(\mathcal{X})$ are the diagonal matrices.

Suppose $n = 2$. Then $\Sigma(\mathcal{X}) = \{F_{x_1}, F_{x_2}\} = \{\infty, 0\}$ is just a pair of points. The global stabilizer $G(u, v)$ of a pair of points is the subgroup of $G$ permuting the 2-subset $\{u, v\}$. In $G = PGL(2, F)$ it is (usually) the normalizer of the Cartan subgroup and dihedral. As $G$ is 2-transitive on $\Omega$, the map $gG(0, \infty) \mapsto \{g(0), g(\infty)\}$ is a bijection of the coset space $G/G(0, \infty)$ with the set $\Omega_2$ of 2-subsets of $\Omega$. Further $G_0 \cap G(0, \infty) = G_{0, \infty}$ is a Cartan subgroup isomorphic to the multiplicative group $F^\times$ of $F$.

Let $G$ be $GL(V)$ or $PGL(V)$ in the rest of this section.

An element of $GL(V)$ is unipotent if all its eigenvalues are 1. A subgroup of $GL(V)$ is unipotent if all its elements are unipotent. The unipotent radical $Q(H)$ of a subgroup $H$ of $GL(V)$ is the largest normal unipotent subgroup of $H$. For example if $F$ is finite of characteristic $p$, then $Q(H)$ is the largest normal $p$-subgroup of $H$. Passing to images in $PGL(V)$, we have the corresponding notions in that group also.

A subgroup $H$ of $G$ is a parabolic if $H$ is the stabilizer of a simplex in the projective geometry $PG(V)$. Thus for example Borel subgroups are parabolics, and indeed the parabolics are the overgroups of the Borel subgroups.

For each parabolic $H$, $H = Q(H)L(H)$, where $L(H)$ is a complement to $Q(H)$ in $H$ called a Levi factor of $H$. Thus $H \cong Q(H) \rtimes L(H)$.

Example A.6: Let $F = \mathbb{F}_q$, $U$ an $m$-dimensional subspace of $V$ with $0 < m < n$, $G = GL(V)$, and $H = N_G(U)$ the (global) stabilizer of $U$ in $G$. As $\{U\}$ is a simplex in $PG(V)$, $H$ is a parabolic. For a subspace/quotient space $X$ of $V$, let $C_H(X)$ denote its centralizer in $H$, namely the element-wise stabilizer of $X$. Then $Q(H) = C_H(U) \cap C_H(V/U)$ is of order $q^{m(n-m)}$. Pick a complement $W$ to $U$ in $V$. $L(H) = L_1 \times L_2$ where $L_1 \cong GL(m, q)$ centralizes $W$ and acts faithfully as $GL(U)$ on $U$, and $L_2 \cong GL(n - m, q)$ centralizes $U$ and acts faithfully as $GL(W)$ on $W$. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be bases for $U$

\[\text{Note that } k\text{-transitivity implies } l\text{-transitivity for all } l < k.\]
and $W$ respectively, then the matrices of $Q(H)$, $L_1$ and $L_2$ with respect to $X_1 \cup X_2$ have the forms

\[
\begin{bmatrix}
I & K \\
0 & I
\end{bmatrix}, \quad 
\begin{bmatrix}
K_1 & 0 \\
0 & I
\end{bmatrix} \quad \text{and} \quad 
\begin{bmatrix}
I & 0 \\
0 & K_2
\end{bmatrix}
\]

respectively, where the upper-left block of each matrix above has dimension $m \times m$, with $K_1$ and $K_2$ invertible. Thus $|H| = |Q(H)| \cdot |L(H)| = q_n M M_{n-m}$, where $q_n = q^{n(n-1)/2}$ and for $1 \leq k \leq n$,

\[
M_k = \prod_{i=1}^{k} (q^j - 1).
\]

Note $|GL(k, q)| = q_k M_k$. In $PGL(V)$ the image of $H$ has order $q_n M_{n-m}/(q-1)$.

**B. Interpretation of the Ingleton Violation in $PGL(2, q)$**

Let $F = \mathbb{F}_q$ and $G = PGL(2, q) = PGL(2, \mathbb{F}_q)$. In the Ingleton violation construction in Section V, we have a $4$-tuple of subgroups $\rho = (G_i : 1 \leq i \leq 4)$ of $G$. The group $G_2 = G_{\mathbb{F}x_2} = G_0$ is a Borel subgroup. The subgroups $G_3$ and $G_4$ are isomorphic to the dihedral group $D_2(q-1)$ of order $2(q-1)$, and their intersection $G_{2j}$ with $G_2$ is cyclic of order $q - 1$ and with $G_{34}$ of order $1$. This forces $G_{2j}$, $i = 3, 4$, to be distinct Cartan subgroups of $G_2$, and hence $G_i = G(0, e_i)$ for some $e_i \in F$. In fact from the forms of the matrices in $G_3$ and $G_4$ it is easy to check that $e_3 = -1$ and $e_4 = \infty$.

Finally $G_1 \cong S_3$ with $G_{1i}$ the three subgroups of $G_1$ of order $2$ for $2 \leq i \leq 4$. For $2 \leq i \leq 4$ let $G_{1i} = \langle t_i \rangle$, and for $1 \leq j \leq 4$ let $\Delta_j$ be the orbit of $G_j$ on $\Omega$ containing $0$. Then $|\Delta_j| = |G_j : G_{2j}| = n_j$ where $n_3 = n_4 = 2$ and $n_1 = 3$. Indeed $\Delta_i = \{0, t_i(0)\}$ for $i = 3, 4$, with $\Delta_3 = \{0, -1\}$ and $\Delta_4 = \{0, \infty\}$. Then as $G_1 = \langle t_3, t_4 \rangle$ and $n_1 = 3$, $\Delta = \Delta_1 = \{0, -1, \infty\}$. But as $G$ is sharply $3$-transitive, the global stabilizer $G(\Delta)$ is isomorphic to $S_3$. Hence $G_1 = G(\Delta)$, and is determined by $G_2$, $G_3$, and $G_4$. Again by $3$-transitivity of $G$, the map $gG_1 \mapsto g(\Delta)$ is a bijection of $G/G_1$ with the set $\Omega_3$ of $3$-subsets of $\Omega$.

Hence the $4$-tuple $\rho$ is determined by the ordered triple $(0, -1, \infty)$ with the four subgroups being various (global) stabilizers on it. Furthermore, given an arbitrary ordered triple $(\alpha, \beta, \gamma)$ of distinct points in $\Omega$, we can construct a $4$-tuple $\rho'$ in the same fashion, where $G_2 = G_\alpha$, $G_3 = G(\alpha, \beta)$, $G_4 = G(\alpha, \gamma)$, and $G_1 = G(\alpha, \beta, \gamma)$. Since $G$ is $3$-transitive on $\Omega$, by the same element in $G$ all four subgroups in $\rho'$ are conjugate to their counterparts in $\rho$. In particular, the new tuple $\rho'$ also violates Ingleton. From the observation above we can generalize the Ingleton violation $\rho$ to a broader class of groups, as described in Section [A-D].

With respect to the “flower structure” of $G_2 = G_0$, this follows from the fact that $G_0$ is a Frobenius group on $\Omega' = \Omega - \{0\}$. That is, $G_0$ is a transitive permutation group on $\Omega'$ in which the maximum
number of fixed points of a nonidentity element is 1. (This is guaranteed by the sharp 3-transitivity of \( G \).) Then by a theorem of Frobenius, the identity 1 of \( G_0 \), together with the set of elements with no fixed points, forms a normal subgroup \( K \) called the Frobenius kernel of the Frobenius group. In our case, \( K \) is the subgroup \( N \) in Sections IV and V which is the unipotent radical of the Borel subgroup \( G_0 \) and is isomorphic to the additive group of the field \( F \). Also \( G_0 - K \) is partitioned by the sets \( G_0,a - \{1\}, a \in \Omega^0 \); these are the petals in the flower. The subgroups \( G_0,a \) are the \( q \) Cartan subgroups contained in \( G_0 \), and each is isomorphic to \( F^\times \).

C. Generalizations in \( PGL(n,q) \)

Let \( \tau = (G_i : 1 \leq i \leq 4) \) be a family of subgroups of a finite group \( G \). The Ingleton inequality \( (1) \) fails iff

\[
|G_1G_2| < \frac{|G_{13}G_{23}|G_{14}G_{24}|}{|G_{34}|}.
\]

In all constructions we will consider in this appendix, \( G_i = G_{1i}G_{2i} \) for \( i = 3, 4 \) and \( |G_3| = |G_4| \). Also \( |G_1G_2| = |G_1 : G_{12}|G_2| \). Hence in such constructions Ingleton fails iff

\[
|G_1 : G_{12}|G_2| < \frac{|G_3|^2}{|G_{34}|},
\]

and the Ingleton ratio \( (12) \) becomes

\[
r(\tau) = \frac{|G_3|^2}{|G_1 : G_{12}|G_2||G_{34}|}.
\]

Now we explore three different approaches trying to extend the \( PGL(2,q) \) family of violations \( \rho \) to \( PGL(n,q) \).

Example A.7: Let \( G = PGL(n,q) \) with \( n \geq 3 \). It is easy to see that \( G \) is doubly transitive on the points of \( PG(V) \) and transitive on triples of independent points. Let \( P_i, 2 \leq i \leq 4 \), be independent points in \( V \), \( \Delta_i = \{P_2, P_i\} \) for \( i = 3, 4 \), and \( \Delta = \{P_2, P_3, P_4\} \). Set \( G_2 = N_G(P_2), G_i = N_G(\Delta_i), i = 3, 4, \) and \( G_1 = N_G(\Delta) \). Let \( \tau = (G_i : 1 \leq i \leq 4) \).

Now \( G_2 \) is a parabolic and by Example A.6

\[
|G_2| = qG^{n-1}.
\]

Next \( D = P_2 + P_3 + P_4 \) is a 3-dimensional subspace of \( V \), so by Example A.6 again, \( |N_G(D)| = qG^{n-3}(q-1) \). Further as \( G_1 \) acts as the symmetric group on \( \Delta \) of order 3, through calculation of the preimages in \( GL(n,q) \) we have \( |N_G(D) : G_1| = |GL(3,q)|/(6(q-1)^3) = qG^{3M_3}/(6(q-1)^3) \). So

\[
|G_1| = \frac{|N_G(D)| \cdot 6(q-1)^3}{qG^{3M_3}} = \frac{6qG^{n-3}(q-1)^2}{q^3}.
\]
As $G_1$ is transitive on $\Delta$ of order 3, $|G_1 : G_{12}| = 3$. Therefore

$$|G_1 : G_{12}| |G_2| = 3|G_2| = 3q_n M_{n-1}. \quad (16)$$

Also for $i = 3, 4$, $G_i$ and $G_{1i}$ are both transitive on $\Delta_i$ of order 2, so $|G_i : G_{2i}| = |G_{1i} : G_{12i}| = 2$. Thus $|G_1i_G2i| = |G_1i_G12i||G_{2i}| = |G_i|$ and $G_i = G_{1i}G_{2i}$ for $i = 3, 4$. Since $G$ is doubly transitive on the points, $G_3$ is conjugate to $G_4$ and so $|G_3| = |G_4|$. Further $U = P_2 + P_3$ is a 2-dimensional subspace of $V$, so by Example A.6 $|N_G(U)| = q_n M_2 M_{n-2}/(q - 1)$. Also $|N_G(U) : G_3| = |GL(2, q)|/(2(q - 1)^2) = q M_2/(2(q - 1)^2)$, so

$$|G_3| = \frac{|N_G(U)| \cdot 2(q - 1)^2}{q M_2} = \frac{2q_n M_{n-2}(q - 1)}{q}. \quad (17)$$

Finally $G_{34} = G_\Delta$ is the pointwise stabilizer of $\Delta$. Since $G_1$ is 3-transitive on $\Delta$, $|G_1 : G_{34}| = 3q = 6$. So by (15):

$$|G_{34}| = \frac{q_n M_{n-3}(q - 1)^2}{q^3}. \quad (18)$$

It follows from (16), (17), and (18) that (i) is satisfied iff

$$3q_n M_{n-1} < \frac{4q_n^2 M_{n-2}^2(q - 1)^2 \cdot q^3}{q^2 \cdot q_n M_{n-3}(q - 1)^2} = 4q_n q M_{n-2}(q^{n-2} - 1)$$

which holds iff $3(q^{n-1} - 1) < 4q(q^{n-2} - 1)$ iff

$$q^{n-1} - 4q + 3 > 0. \quad (19)$$

This inequality holds when $n \geq 4$ or $n = 3$ and $q \geq 4$.

Since $G$ is transitive on all triples of independent points, all 4-tuples in this example are conjugate to each other.

The Ingleton ratio is

$$r(\tau) = \frac{4q_n^2 M_{n-2}^2(q - 1)^2 \cdot q^3}{q^2 \cdot 3q_n M_{n-1} \cdot q_n M_{n-3}(q - 1)^2} = \frac{4q(q^{n-2} - 1)}{3(q^{n-1} - 1)},$$

which approaches $4/3$ for large $q$ or $n$. Whereas in the original example $\rho$, $r(\rho) = 4(q - 1)/(3q)$, which also approaches $4/3$ for large $q$. Thus the two families seem to be roughly equally effective in violating Ingleton.

**Example A.8:** As usual let $F = \mathbb{F}_q$ and $G = PGL(n, q)$, with $n \geq 2$. Let $P_i$, $2 \leq i \leq 4$, be distinct but dependent points in $V$. Thus $P_i = Fx_i$, $i = 2, 3$, for two independent vectors $x_2, x_3 \in V$, and $P_4 = F(ex_2 + x_3)$ for some $e \in F$. Let $U$, $\Delta$, $\Delta_i$, $i = 3, 4$, and $G_i$, $1 \leq i \leq 4$, be defined the same as in Example A.7. Note that when $n = 2$ this is our original construction $\rho$. 


From last example, $|G_2| = q_n M_{n-1}$ and $|N_G(U)| = q_n M_2 M_{n-2}/(q - 1)$. Since $U$ is a 2-dimensional subspace of $V$, $PGL(U)$ is sharply 3-transitive on the points of $U$ by Lemma A.1. Now as $\Delta$ is a set of three distinct points in $U$, its global stabilizer in $PGL(U)$ is isomorphic to $S_3$. Thus $G_1$ is 3-transitive on $\Delta$ and $|N_G(U) : G_1| = |GL(2, q)|/(6(q - 1)) = q M_2/(6(q - 1))$. So

$$|G_1| = \frac{|N_G(U)| \cdot 6(q - 1)}{q M_2} = \frac{6q_n M_{n-2}}{q}.$$  \(\text{(20)}\)

$G_1$ is transitive on $\Delta$, while for $i = 3, 4$, $G_i$ and $G_{1i}$ are both transitive on $\Delta$. $G$ is doubly transitive on the points of $PG(V)$. Thus from arguments in Example A.7 we have $|G_1 : G_{12}| |G_2| = 3q_n M_{n-1}$, $G_i = G_{1i} G_{2i}$ for $i = 3, 4$, and $|G_3| = |G_4|$. Also $|G_3| = 2q_n M_{n-2}(q - 1)/q$. Since $G_34 = G_\Delta$ is of index 6 in $G_1$, by (20):

$$|G_{34}| = \frac{q_n M_{n-2}}{q}.$$  

Thus (i) is satisfied iff

$$3q_n M_{n-1} < \frac{4q^2 M^2_{n-2}(q - 1)^2 \cdot q}{q^2 \cdot q_n M_{n-2}} = \frac{4q_n M_{n-2}(q - 1)^2}{q}$$

which holds iff $3q(n^2 - 1) < 4(q - 1)^2$ iff

$$3q \sum_{i=0}^{n-2} q^i - 4q + 4 < 0.$$  \(\text{(21)}\)

When $n = 2$, this inequality holds iff $q \geq 4$. When $n > 2$, however, it always fails because $3q^2 - q + 4 > 0$ for all $q$.

Therefore, the original construction $\rho$ is the only successful case in this example, with Ingleton ratio $r(\rho) = 4(q - 1)/(3q)$.

Example A.9: Again take $G = PGL(n, q)$ with $n \geq 3$. Let $U_2$ be a point of $V$, $U_i$, $i = 3, 4$, distinct 2-dimensional subspaces of $V$ with $U_3 \cap U_4 = U_2$, and $U_1 = U_3 + U_4$ the 3-dimensional subspace of $V$ generated by $U_3$ and $U_4$. Set $G_i = N_G(U_i)$ for $1 \leq i \leq 4$, and $\lambda = (G_i : 1 \leq i \leq 4)$. Then all the $G_i$ are parabolics with $|G_2| = q_n M_{n-1}$ from (14), $|G_3| = |G_4| = q_n M_2 M_{n-2}/(q - 1)$, and $|G_1| = q_n M_3 M_{n-3}/(q - 1)$. As $G_1$ is transitive on the $(q^3 - 1)/(q - 1) = q^2 + q + 1$ points in $U_1$, $|G_1 : G_{12}| = q^2 + q + 1$, so

$$|G_1 : G_{12}| |G_2| = (q^2 + q + 1)q_n M_{n-1}.$$  

For $i = 3, 4$, $G_i$ and $G_{1i}$ are both transitive on the $(q^2 - 1)/(q - 1) = q + 1$ points in $U_i$, so $G_i = G_{1i} G_{2i}$ for $i = 3, 4$. Also $G_{34}$ is the subgroup of $G$ fixing $U_2$ and the points $U_3/U_2$ and $U_4/U_2$ of the quotient space $U_1/U_2$; in particular it is a subgroup of $G_1$. If we pick a basis $\mathcal{X}_1 = \{x_3, x_2, x_4\}$ for $U_1$ such that
U_2 = \langle x_2 \rangle \text{ and } U_i = \langle x_2, x_i \rangle \text{ for } i = 3, 4, \text{ then elements of } G_{34} \text{ correspond to the linear transformations in } GL(U_1) \text{ whose matrices with respect to } \lambda_1 \text{ take the form}

\[
\begin{bmatrix}
a & 0 & 0 \\
x & b & y \\
0 & 0 & c
\end{bmatrix}
\]

where \(a, b\) and \(c\) are nonzero. So \(|G_1 : G_{34}| = |GL(3, q)|/(q^2(q-1)^3) = qM_3/(q-1)^3, \text{ and}

\[
|G_{34}| = \frac{|G_1|}{qM_3/(q-1)^3} = \frac{q_nM_3M_{n-3} \cdot (q-1)^3}{(q-1) \cdot qM_3} = \frac{q_nM_{n-3}(q-1)^2}{q}.
\]

It follows that (2) is satisfied iff

\[
(q^2 + q + 1)q_nM_{n-1} < \frac{q^2M_2^2M_{n-2}^2 \cdot q}{(q-1)^2 \cdot qM_n(q-1)^2} = q_nq(q+1)^2(q^{n-2} - 1)M_{n-2},
\]

which holds iff \((q^2 + q + 1)(q^{n-1} - 1) < q(q+1)^2(q^{n-2} - 1)\) iff

\[
q^n - q^3 - q^2 + 1 > 0,
\]

which holds iff \(n \geq 4\).

The Ingleton ratio is

\[
r(\lambda) = \frac{q^2M_2^2M_{n-2} \cdot q}{(q-1)^2 \cdot (q^2 + q + 1)q_nM_{n-1} \cdot qM_n(q-1)^2} = \frac{q(q+1)^2(q^{n-2} - 1)}{(q^2 + q + 1)(q^{n-1} - 1)},
\]

which approaches 1 for large \(q\) and \((q+1)^2/(q^2 + q + 1)\) (which is smaller than 4/3) for large \(n\). So this example seems less effective than the other two.

**D. Generalizations in General 2-transitive Groups**

In the following we generalize the Ingleton violation \(\rho\) in \(PGL(2, q)\) to a more abstract construction, which includes Examples A.7 and A.8 as special cases.

Let \(G\) be a doubly transitive group on a set \(\Omega\) of order \(l \geq 3\), let \(\alpha\) and \(\beta\) be distinct points in \(\Omega\), and assume \(\gamma \in \Omega - \{\alpha, \beta\}\) such that the global stabilizer \(G(\Delta)\) of \(\Delta = \{\alpha, \beta, \gamma\}\) acts as the symmetric group on \(\Delta\) (which is clearly the case when \(G\) is 3-transitive). Let \(G_2 = G_\alpha, G_3 = G(\alpha, \beta), G_4 = G(\alpha, \gamma), \text{ and } G_1 = G(\Delta). \text{ Set } \mu = (G_i : 1 \leq i \leq 4).

Let \(k = |G_{\alpha, \beta}|, d = |G_D|, \Gamma \text{ the orbit of } \gamma \text{ under the action of } G_{\alpha, \beta}, \text{ and } c = |\Gamma|. \text{ Observe that}

\[
c = |G_{\alpha, \beta} : G_\Delta| = k/d \text{ and } c \leq l - 2 \text{ as } \Gamma \subseteq \Omega - \{\alpha, \beta\}. \text{ Further } c = l - 2 \text{ iff } G \text{ is 3-transitive.}
\]

Since \(G\) is 2-transitive on \(\Omega\), \(G_2\) is transitive on \(\Omega - \{\alpha\}\) and so \(|G_2 : G_{\alpha, \beta}| = l - 1\). Also \(|G_1 : G_{12}| = 3\) as \(G_1\) is transitive on \(\Delta\), thus

\[
|G_1 : G_{12}||G_2| = 3|G_2| = 3(l - 1)k.
\]
Next $G_3$ is conjugate to $G_4$ by 2-transitivity of $G$ and for $i = 3, 4$, $G_i$ and $G_{3i}$ are both transitive on $\Delta_i$ of order 2, so $G_{1i}G_{2i} = G_i$ and $|G_i| = 2k$ for $i = 3, 4$. Finally $G_{34} = G_\Delta$ is of order $d$. Thus

$$|G_3|^2/|G_{34}| = 4k^2/d = 4kc,$$

so condition (5) is satisfied iff $3(l - 1)k < 4kc$ iff

$$3(l - 1) < 4c.$$ (22)

Further the Ingleton ratio $r(\mu) = 4c/(3(l - 1))$.

If $G$ is 3-transitive then $c = l - 2$, so $3(l - 1) < 4c = 4(l - 2)$ iff $l > 5$. Further $r(\mu) = 4(l - 2)/(3(l - 1))$.

Both Example A.7 and A.8 fit in this construction, with $\rho$ being the only 3-transitive case. In Example A.7 $l = (q^n - 1)/(q - 1)$ and

$$c = (q^n - 1) - (q^2 - 1) = q^2(q^{n-2} - 1)$$

so by (22), (5) is satisfied iff

$$3(q^n - 1 - q^2 - 1) < 4q^2(q^{n-2} - 1)$$

which gives (19). In Example A.8 $l$ has the same value, but since $GL(U)$ is 3-transitive on the $(q^2 - 1)/(q - 1) = q + 1$ points of $U$, $c = q + 1 - 2 = q - 1$. Then by (22), (5) is satisfied iff

$$3(q^n - 1 - q - 1) < 4(q - 1),$$

which gives (21).

We see that the 3-transitive groups give rise to simple and effective Ingleton violation constructions. This category of groups include the alternating and symmetric groups, the groups $PGL(2, q)$ with $l = q + 1$, the Mathieu groups, the affine groups of degree $2^e$ (which are the semidirect product of an $e$-dimensional vector space $E$ over $F_2$ by $GL(E)$), and the subgroup of the affine group for $e = 4$ where the complement is $A_7$ rather than $GL(4, 2) \cong A_8$.

**APPENDIX B**

**Proofs and Calculations in Section VI**

A. Structures of $M, K, K', J, J'$

When the characteristic $p$ of $\mathbb{F}_q$ equals 2, $K = K'$ and $J = J'$. So for the analysis of $K'$ and $J'$ we only consider the case $p \neq 2$.

Observe that $|A_\alpha| = p$ for each $\alpha \in \mathbb{F}_q^\times$, and

$$|C| = 3, \ |B_1| = 2, \ |B| = |B'| = |P| = |P'| = q - 1.$$
As \((CB_1)^2 = I\), we have \(M \cong D_6 \cong S_3\). It is easy to check that \(\forall \alpha \in \mathbb{F}_q\),

\[ A^B_\alpha = A_{1-t \cdot \alpha}, \quad A_{\alpha}^{B'} = A_{-t \cdot \alpha}, \quad A^P_\alpha = A_{t \cdot \alpha}, \quad A_{\alpha}^{P'} = A_{-t \cdot \alpha}. \]

Therefore, \(N\) is a normal subgroup of all \(K, K', J, J'\) and

\[ K = N \cdot \langle B \rangle, \quad K' = N \cdot \langle B' \rangle, \quad J = N \cdot \langle P \rangle, \quad J' = N \cdot \langle P' \rangle. \]

Also \(N\) trivially intersects each of \(\langle B \rangle, \langle B' \rangle, \langle P \rangle\) and \(\langle P' \rangle\), thus

\[ K \cong N \times \langle B \rangle, \quad K' \cong N \times \langle B' \rangle, \quad J \cong N \times \langle P \rangle, \quad J' \cong N \times \langle P' \rangle, \]

all of which are semidirect products \(\mathbb{Z}_p^m \rtimes \mathbb{Z}_{q-1}\). We claim that \(K \cong J\) and \(K' \cong J'\). Moreover, in the case \(p \neq 2\), all the four groups are isomorphic if and only if \(\frac{q-1}{2}\) is even.

To see this, first consider the bijections \(\sigma : K \to J\) and \(\sigma' : K' \to J'\), where \(\forall \alpha \in \mathbb{F}_q, \forall k \in K_q\),

\[ \sigma \left( A_\alpha B^k \right) = A_{\alpha} P^{-k}, \quad \sigma' \left( A_\alpha (B')^k \right) = A_{\alpha} (P')^{-k}. \]

Observe that \(\forall \alpha, \beta \in \mathbb{F}_q, \forall k, l \in K_q\),

\[ \sigma \left( A_\alpha B^k \cdot A_\beta B^l \right) = \sigma \left( A_{\alpha+t \cdot \beta} B^{k+l} \right) = A_{\alpha+t \cdot \beta} P^{-k-l} = A_{\alpha} P^{-k} \cdot A_{\beta} P^{-l} = \sigma \left( A_\alpha B^k \right) \cdot \sigma \left( A_\beta B^l \right), \]

so \(\sigma\) is indeed an isomorphism. Similarly \(\sigma'\) is also an isomorphism.

Next observe that in the case \(p \neq 2\), when \(\frac{q-1}{2}\) is even, \(\frac{q-1}{4}\) is an integer and so

\[ \left( \frac{q+1}{2} \right)^2 = \left( \frac{q-1}{2} + 1 \right)^2 = \frac{(q-1)^2}{4} + (q-1) + 1 \equiv 1 \pmod{q-1}. \]

Thus \(\left( (B')^{\frac{q+1}{2}} \right)^{\frac{q+1}{2}} = B'\) and \(\langle (B')^{\frac{q+1}{2}} \rangle = \langle B' \rangle\). In addition, since \(\mathbb{F}_q^\times\) is cyclic of an even order \(q-1\), we have \(-1 = t \frac{q+1}{2}\), and thus \((-t)^{\frac{q+1}{2}} = (t^{\frac{q+1}{2}})^{\frac{q+1}{2}} = t\). Consider \(\tau : K \to K'\), where

\[ \tau \left( A_\alpha B^k \right) = A_{\alpha} (B')^{\frac{q+1}{2}k}, \quad \forall \alpha \in \mathbb{F}_q, \forall k \in K_q. \]

Apparently \(\tau\) is a bijection. Also we can show that it is a homomorphism by calculating \(\tau \left( A_\alpha B^k \cdot A_\beta B^l \right)\) with the following fact:

\[ A_\alpha (B')^{\frac{q+1}{2}k} \cdot A_{\alpha} (B')^{\frac{q+1}{2}l} = A_{\alpha + (t \cdot \beta)} (B')^{\frac{q+1}{2}(k+l)} = A_{\alpha+ (t \cdot \beta)} (B')^{\frac{q+1}{2}(k+l)}. \]

Thus when \(\frac{q-1}{2}\) is even, \(K \cong K'\) and the four groups are all isomorphic.

When \(\frac{q-1}{2}\) is odd, however, \(\tau\) is not a bijection anymore, because this time \(B' \notin \langle (B')^{\frac{q+1}{2}} \rangle\) and \(\tau(K) \neq K'\). Furthermore, we can prove that in this case \(K\) and \(J\) are not isomorphic, by showing that \(K\) and \(J\) have generalized flower structures whenever \(q > 2\), whereas if \(p \neq 2\), \(K'\) and \(J'\) only have
flower structures when \( \frac{q-1}{2} \) is even. Since \( K \cong J \) and \( K' \cong J' \), it is enough to only show the analysis of \( K \) and \( K' \). Pick \( \alpha \in \mathbb{F}_q^\times \) and assume \( k, l \in \mathcal{K}_q \). Similar to the \( G_2 \) in Section [VI-B], we have the relation

\[
(B^k)^{A_\alpha} = B^l \iff k = l = 0,
\]

thus \( K \) has a generalized flower structure whenever \( q > 2 \). On the other hand, for \( K' \) we have

\[
(B'^k)^{A_\alpha} = B'^l \iff \begin{bmatrix} (-1)^k & 0 \\ t^k \alpha & t^k \end{bmatrix} = \begin{bmatrix} (-1)^l & 0 \\ (-1)^l \alpha & t^l \end{bmatrix},
\]

which requires \( k = l \) and \( t^l = (-1)^l \). Thus for \( p \neq 2 \), \( l \) can only be 0 or \( \frac{q-1}{2} \). If \( \frac{q-1}{2} \) is even, we have \((-1)^{\frac{q-1}{2}} = 1\) and so \( k = l = 0 \), then \( K' \) also has a generalized flower structure (as expected since here \( K \cong K' \)). If \( \frac{q-1}{2} \) is odd, however, this is not true: in this case \((-1)^{\frac{q-1}{2}} = -1\), so \( k = l = 0 \) or \( \frac{q-1}{2} \) in the above relation. Thus \( \forall \alpha \in \mathbb{F}_q^\times \), \( (B') \cap (B')^{A_\alpha} = \langle -I \rangle \cong \mathbb{Z}_2 \). When \( q = 3 \), \( B' = -I \) and \( K' = \langle A \rangle \times \langle -I \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \); when \( q > 3 \), \( (B') \) and \( (B')^{A_\alpha} \) are distinct groups but have nontrivial intersection. Therefore, in neither case does \( K' \) have a generalized flower structure.

### B. Intersections in Instances 8 and 9

Let \( p \neq 2 \). Observe that \( K' \) and \( J' \) are both subgroups of the \( G_2 \) in Section [VI-A] so all the intersections in both instances are subgroups of their respective counterparts in Section [VI-A]. In instance 8, since \( G_{12} \leq \langle t, B_1 \rangle \) and the (1,1)-entry for every matrix in \( G_2 = K' \) is always \( \pm 1 \), we have \( G_{12} \leq \langle -I, B_1 \rangle \). This further limits the (2,2)-entry to be \( \pm 1 \) for each matrix in \( G_{12} \). As the (2,2)-entry in \( K' \) takes the form \( t^k \) for some \( k \), we see that this \( k \) can only be 0 or \( \frac{q-1}{2} \). By examining the parity of \( \frac{q-1}{2} \), we have

\[
G_{12} = \begin{cases} 
\langle B_1 \rangle \cong \mathbb{Z}_2 & \text{if } \frac{q-1}{2} \text{ is even} \\
\langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise}
\end{cases}, \quad G_{123} = G_{124} = \begin{cases} 
1 & \text{if } \frac{q-1}{2} \text{ is even} \\
\langle -I \rangle \cong \mathbb{Z}_2 & \text{otherwise}
\end{cases}.
\]

Similarly we can calculate \( G_{12}, G_{123} \) and \( G_{124} \) for instance 9.

In both instances, \( G_{24} \) is simply the subgroup of all diagonal matrices in \( G_2 \), and \( G_{23} \leq T \). As matrices in \( K' \) and \( J' \) can be respectively written as

\[
(-1)^k \begin{bmatrix} 1 & 0 \\ \alpha' & (-t)^k \end{bmatrix} = (-1)^k \begin{bmatrix} 1 & 0 \\ \alpha' & (t^{\frac{q+1}{2}})^k \end{bmatrix} \quad \text{and} \quad t^k \begin{bmatrix} 1 & 0 \\ \alpha'' & (-t^{-1})^k \end{bmatrix} = t^k \begin{bmatrix} 1 & 0 \\ \alpha'' & (t^{\frac{q-3}{2}})^k \end{bmatrix}
\]

for some \( \alpha', \alpha'' \in \mathbb{F}_q \) and \( k \in \mathcal{K}_q \), we see that \( G_{23} = \langle -B_{3}^{\frac{q+1}{2}} \rangle \) and \( \langle tB_{3}^{\frac{q-3}{2}} \rangle \) respectively, where

\[
(-B_{3}^{\frac{q+1}{2}})^k = \begin{bmatrix} (-1)^k & 0 \\ t^k & (-1)^k \end{bmatrix}, \quad (tB_{3}^{\frac{q-3}{2}})^k = \begin{bmatrix} t^k & 0 \\ (-1)^k - t^k & (-1)^k \end{bmatrix}
\]

Thus \( G_{23} \cong \mathbb{Z}_{q-1} \) in both cases.
C. The case \( p = 3 \) for Instance 15

In Instance 15, \( G_1 = M = \langle C, B_1 \rangle \) and \( G_2 = (J')^E \). We can show that \( G_1 G_2 = G_2 G_1 \) when \( p = 3 \), thus Ingleton is satisfied by Condition 3. Observe that \( G_2 = \{ X_{\alpha,j} \mid \alpha \in \mathbb{F}_q, j \in \mathcal{K}_q \} \), where

\[
X_{\alpha,j} = \begin{bmatrix}
-1^j - \alpha & \alpha \\
-1^j - t^j - \alpha & t^j + \alpha
\end{bmatrix}.
\]

When \( p = 3 \), we have \( 2 = -1 \). With this relation, it is easy to check that \( C = X_{1,0} \in G_2 \), and for each \( \alpha \) and \( j \)

\[
X^B_{\alpha,j} = \begin{bmatrix}
-1^j + \alpha & -\alpha \\
-1^j - t^j + \alpha & t^j - \alpha
\end{bmatrix} = X_{-\alpha,j} \in G_2.
\]

Thus \( G_1 \) normalizes \( G_2 \). In particular, \( \forall X \in G_2 \) and \( \forall Y \in G_1 \), we have \( X^Y \in G_2 \) and \( X^{Y^{-1}} \in G_2 \), which imply \( YX \in G_1 G_2 \) and \( XY \in G_2 G_1 \) respectively. Therefore, \( G_1 G_2 = G_2 G_1 \).

D. Intersections in Instances 12–15

Most intersections are easily obtained by comparing the formulae of the matrices in the subgroups involved. For the intersection of \( M \) with any of \( J^E, (J')^E, J^Q \) or \( (J')^Q \), we can utilize the properties below to facilitate calculation. Let \( \vec{c}_i(X) \) denote the vector of the \( i \)-th column of a matrix \( X \), we have

\[
\vec{c}_1(X) + \vec{c}_2(X) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ \forall X \in J^E; \quad \vec{c}_1(X) + \vec{c}_2(X) = \pm \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \ \forall X \in (J')^E;
\]

\[
\vec{c}_1(X) - 2\vec{c}_2(X) = \begin{bmatrix} 1 \\ -2 \end{bmatrix}, \ \forall X \in J^Q; \quad \vec{c}_1(X) - 2\vec{c}_2(X) = \pm \begin{bmatrix} 1 \\ -2 \end{bmatrix}, \ \forall X \in (J')^Q.
\]

Thus, we need only seek elements of \( M \) which share these properties.

We also want to mention the calculation of \( G_{34} \) for Instances 13 and 15 when \( p > 3 \). In Instance 13, finding \( G_{34} \) is equivalent to solving the following set of equations:

\[
\begin{align*}
(-1)^i - \alpha &= (-1)^i + 2\beta \\
\alpha &= \beta \\
(-1)^i - t^j - \alpha &= 2(t^i - 2\beta - (-1)^i) \\
t^j + \alpha &= t^i - 2\beta
\end{align*}
\]

\[
\begin{align*}
\alpha &= \beta \\
3\beta &= (-1)^i - (-1)^i \\
t^i &= (-1)^i \\
t^j &= (-1)^i
\end{align*}
\]

From the last two equations, we can see that \( i \) and \( j \) can only be 0 or \( \frac{q-1}{2} \). If \( \frac{q-1}{2} \) is even, then \( (-1)^{\frac{q-1}{2}} = 1 \), so \( i \) and \( j \) must both be 0, which yields that \( G_{34} = 1 \). If \( \frac{q-1}{2} \) is odd, then \( i = 0 \) implies that \( j = 0 \), and \( i = \frac{q-1}{2} \) implies that \( j = \frac{q-1}{2} \). In both cases \( \alpha = \beta = 0 \), therefore \( G_{34} = \langle -I \rangle \). For \( G_{34} \) in Instance 15, we have similar equations and the same discussion also applies.
ACKNOWLEDGMENT

The authors would like to thank Michael Aschbacher and Amin Shokrollahi for very helpful discussions on the conditions and the generalizations of the violations, and on expanding the group structures. They would also like to thank Ryan Kinser for reminding them of the case $PGL(2, q)$.

REFERENCES


