Codes Over Non-Abelian Groups: Point-to-Point Communications and Computation Over MAC

Aria G. Sahebi and S. Sandeep Pradhan
Department of Electrical Engineering and Computer Science,
University of Michigan, Ann Arbor, MI 48109, USA.
Email: ariaghs@umich.edu, pradhanv@umich.edu

***Abstract*—In this paper, we show that good structured codes over non-Abelian groups do exist. Specifically, we construct codes over the smallest non-Abelian group $\mathbb{D}_6$ and show that the performance of these codes is superior to the performance of Abelian group codes of the same alphabet size. This promises the possibility of using non-Abelian codes for multi-terminal settings where the structure of the code can be exploited to gain performance. We also show that for the problem of computation over MAC, these codes are superior to random codes in certain cases.**

I. Introduction

Algebraically structured codes are an important class of codes in coding/information theory and communications and evaluating the information-theoretic performance limits of such codes has been an area of significance [2], [5], [6], [10], [12], [16]. It is well-known that linear codes achieve the symmetric capacity of q-ary channels where q is a prime [7] [6]. Linear codes can also be used to compress a binary source losslessly down to its entropy [11]. Optimality of linear codes for certain communication problems motivates the study of algebraic-structured codes including Abelian and non-Abelian group codes.

In [11] it has been shown that for some multi-terminal communication settings, the average asymptotic performance of the ensemble of structured codes can be better than that of random codes. In recent years, such gains have been shown for a wide class of multi-termianl problems [12], [14], [15]. Thus, characterization of the information theoretic performance limits of these codes became important. However, the structure of the code restricts the encoder to abide by certain algebraic rules. This causes the performance of such codes to be inferior to random codes in some communication settings. Linear codes are highly structured and for some problems in information theory they cannot be optimal. Moreover, these codes can only be defined over alphabets of size a power of a prime.

Group codes are a generalization of linear codes which are algebraically structured and can be defined for any alphabet. These codes can outperform unstructured codes in certain communication problems [12]. Group codes were first studied by Slepian [19] for the Gaussian channel. In [1], the capacity of group codes for certain classes of channels has been computed. Further results on the capacity of group codes were established in [2], [3], [17].

This work was supported by NSF grants CCF-0915619 and CCF-1116021.

In summary, for the point-to-point communication, Abelian group codes are, in general, inferior to linear codes. But for certain multiuser communication, they can outperform the latter.

The next logical step is to characterize the performance limits of codes over non-abelian groups. It has been conjectured by several authors that non-Abelian group codes are inferior to Abelian group codes [8] [9] [13]. Moreover, they suggest that asymptotically good group codes over non-abelian groups may not exist. This motivates a loosening of the structure of the code yet further.

In this work, we define a class of structured codes which includes the class of group codes and has less structure compared to group codes. We evaluate the performance of such codes over the smallest non-Abelian group $\mathbb{D}_6$ and show that these codes have a strictly better performance compared to Abelian group codes for the point-to-point problem. We then use these codes for the problem of computation over MAC and show that these codes are superior to random codes in certain cases. We use a combination of algebraic and information-theoretic tools for this task. This observation broadens our view to structured codes for possible use in multi-terminal settings.

The paper is organized as follows: In Section II, we introduce our notation. In Section III, we define the ensemble of codes and in Section IV, we analyze the performance of these codes for the point-to-point problem. We then simplify this ensemble in Section V and evaluate their performance for the problem of computation over MAC in Section VI. We compare the performance of the constructed codes to the performance of Abelian group codes and random codes in Section VII and we conclude in Section VIII.

II. Preliminaries

1) Groups: A group is a set G equipped with a binary operation "$\cdot$" to form an algebraic structure. The group operation "$\cdot$" must satisfy the group axioms (closure, associativity, identity and invertibility). A group is called *Abelian* if its operation is commutative and *non-Abelian* otherwise.

2) Group Codes: Given a group G, a group code $\mathbb{C}$ over G with block length n is any subgroup of G^n [4], [10]. A

shifted group code over G, $\mathbb{C}+v$ is a translation of a group code $\mathbb{C}$ by a fixed vector $v \in G^n$.

3) Source and Channel Models: We consider discrete memoryless and stationary channels used without feedback. We associate two finite sets $\mathscr{X}$ and $\mathscr{Y}$ with the channel as the channel input and output alphabets. These channels can be characterized by a conditional probability law $W(y|x)$ for $x \in \mathscr{X}$ and $y \in \mathscr{Y}$. The set $\mathscr{X}$ admits the structure of a finite Abelian group G of the same size. The channel is specified by $(G, \mathscr{Y}, W)$. Assuming a perfect source coding block applied prior to the channel coding, the source of information generates messages over the set $\{1, 2, \ldots, M\}$ uniformly.

4) Achievability and Capacity: A transmission system with parameters (n, M, τ) for reliable communication over a given channel $(G, \mathscr{Y}, W)$ consists of an encoding mapping and a decoding mapping $e : \{1, 2, \ldots, M\} \to G^n$, $f : \mathscr{Y}^n \to \{1, 2, \ldots, M\}$ such that for all $m = 1, 2, \ldots, M$,

$$\frac{1}{M} \sum_{m=1}^{M} W^n \left(f(Y^n) \neq m | X^n = e(m) \right) \leq \tau$$

Given a channel $(G, \mathscr{Y}, W)$, the rate R is said to be achievable if for all $\epsilon > 0$ and for all sufficiently large n, there exists a transmission system for reliable communication with parameters (n, M, τ) such that $\frac{1}{n} \log M \geq R - \epsilon$ and $\tau \leq \epsilon$. The capacity of the channel is defined as the supremum of the set of all achievable rates.

5) Typicality: We use the notion of strong typicality throughout the paper.

6) Dihedral Groups: A dihedral group of order $2p$ is the group of symmetries of a regular p-gon, including reflections and rotations and any combination of these operations. A dihedral group can be represented as a quotient of a free group as follows: $D_{2p} = \langle x, y | x^p = 1, y^2 = 1, xyxy = 1 \rangle$. Dihedral groups are among the simplest non-Abelian groups.

7) Notation: In our notation, $O(\epsilon)$ is any function of ϵ such that $\lim_{\epsilon \to 0} O(\epsilon) = 0$ and for a set A, $|A|$ denotes its size (cardinality).

III. A Class of Structured Codes

Based on Forney's *analysis* of group codes [10], we *construct* a class of structured codes which we call *pseudo-group* codes. The complete description of such codes can be found in a more complete version of this work [18]. For Abelian groups, the definition of pseudo-group codes coincides with the definition of group codes but for non-Abelian groups this class is larger than the class of group codes; i.e. it includes all group codes as well as some non-group codes. In this paper, we use these codes for the smallest non-Abelian group $\mathbb{D}_6$ and show that this loosening of the structure results in a better performance. The generalization of the analysis to dihedral groups $\mathbb{D}_{2p}$ where p is a prime is relatively straight forward. The group $\mathbb{D}_6$ with presentation $\mathbb{D}_6 = \langle x, y | x^3 = 1, y^2 = 1, xyxy = 1 \rangle$ can be characterized by a set $\{1, x, x^2, y, xy, x^2y\}$ with the following table of operations:

$\cdot$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Note that for two elements g, h in $\mathbb{D}_6$, $g \cdot h$ may not be equal to $h \cdot g$. We construct the ensemble of codes over $\mathbb{D}_6$ in a more complete version of this paper [18]. Here we directly present the resulting ensemble of codes. Each code in this ensemble has a rate of $R = \frac{k}{n} \log 6$.

- For $i = 1, \cdots, n$ and $j = 1, \cdots, k$ choose g_{ij} and h_{ij} randomly according to Figure 1. for $(i, j) \neq (i', j')$, (g_{ij}, h_{ij}) is chosen independently from $(g_{i'j'}, h_{i'j'})$.

- For $i = 1, \cdots, n$, choose the dither B_i uniformly randomly from $\mathbb{D}_6$.
- Given the input sequence $u = (u_1, \cdots, u_k)$ where $u_i = x^{a_i} y^{b_i}$, $a_i \in \mathbb{Z}_3$, $b_i \in \mathbb{Z}_2$ for $i = 1, \cdots, k$, the output sequence is equal to $c = (c_1, \cdots, c_n)$ where

$$\begin{aligned} c_1 &= g_{11}^{a_1} h_{11}^{b_1} g_{12}^{a_2} h_{12}^{b_2} \cdots g_{1k}^{a_k} h_{1k}^{b_k} \cdot B_1 \\ c_2 &= g_{21}^{a_1} h_{21}^{b_1} g_{22}^{a_2} h_{22}^{b_2} \cdots g_{2k}^{a_k} h_{2k}^{b_k} \cdot B_2 \\ &\vdots \\ c_n &= g_{n1}^{a_1} h_{n1}^{b_1} g_{n2}^{a_2} h_{n2}^{b_2} \cdots g_{nk}^{a_k} h_{nk}^{b_k} \cdot B_n \end{aligned} \tag{1}$$

We denote this by $c = G(u) \cdot B$.

		h_{ij}			
		1	y	xy	x^2y
g_{ij}	1	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{10}$
	x	0	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{10}$
	x^2	0	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{10}$

Fig. 1: g_{ij} is chosen from $\{1, x, x^2\}$ and h_{ij} is chosen from $\{y, xy, x^2y\}$. The number in the table shows the joint probability of (g_{ij}, h_{ij}) being picked.

We evaluate the performance of these codes using a random coding argument in the next section.

IV. Main Result

In this section we show the existence of good structured codes over the non-Abelian group $\mathbb{D}_6$ by proving the following theorem:

Theorem IV.1. *For the channel $(\mathbb{D}_6, \mathscr{Y}, W)$, let X be a uniform random variable over the channel input and let the random variable $[X]$ indicate the coset of $\{1, x, x^2\}$ in $\mathbb{D}_6$ where X belongs to. i.e.*

$$[X] = \begin{cases} \{1, x, x^2\} & \text{if } X \in \{1, x, x^2\} \\ \{y, xy, x^2y\} & \text{if } X \in \{y, xy, x^2y\} \end{cases}$$

Then the rate R^* is achievable using pseudo-group codes over $\mathbb{D}_6$ where

$$R^* = \min\left(\log_2 6 - H(X|Y), \frac{\log_2 6}{\log_2 3}\left[\log_2 3 - H(X|[X]Y)\right]\right)$$

The rest of this section is devoted to give a sketch of the proof of this theorem. A more complete version of this proof can be found in [18].

Consider the class of pseudo-group codes over $\mathbb{D}_6$ of the form (1) used for the channel $(\mathbb{D}_6, \mathscr{Y}, W)$. The set of messages is $\mathbb{D}_6$ and for each message $u \in \mathbb{D}_6^k$ the encoder maps it to $c \in \mathbb{D}_6^n$ where $c = G(u) \cdot B$. At the receiver, after receiving the channel output $y \in \mathscr{Y}^n$, the decoder looks for a message $\hat{u} \in \mathbb{D}_6^k$ such that $\hat{c} = G(\hat{u}) \cdot B$ is jointly ϵ-typical with y with respect to $P_X W_{Y|X}$ where P_X is uniform over $\mathbb{D}_6$ and $\epsilon > 0$ is arbitrary. If it finds a unique such $\hat{c}$, it decodes y to $\hat{u}$, otherwise it declares error.

The expected value of the average probability of error for this coding scheme is given by

$$\mathbb{E}\{P_{avg}(err)\} = \sum_{u\in\mathbb{D}_6^k}\frac{1}{6^k}\sum_{c\in\mathbb{D}_6^n}P(G(u)\cdot B = c)\sum_{\tilde{u}\neq u}\sum_{y\in A_\epsilon^n(Y|c)}$$
$$\sum_{\tilde{c}\in A_\epsilon^n(X|y)} P(G(\tilde{u})\cdot B = \tilde{c}|G(u)\cdot B = c)W(y|c) + O(\epsilon)$$

We need to evaluate the conditional probability $P(G(\tilde{u}) \cdot B = \tilde{c}|G(u)\cdot B = c)$ to proceed. For $u, \tilde{u} \in \mathbb{D}_6^k$ and $x, \tilde{x} \in \mathbb{D}_6^n$, let $u = (u_1, \cdots, u_k)$ where $u_i = x^{a_i}y^{b_i}$ for $i = 1, \cdots, k$ and $\tilde{u} = (\tilde{u}_1, \cdots, \tilde{u}_k)$ where $\tilde{u}_i = x^{\tilde{a}_i}y^{\tilde{b}_i}$ for $i = 1, \cdots, k$. Also let $c = (c_1, \cdots, c_n)$ and $\tilde{c} = (\tilde{c}_1, \cdots, \tilde{c}_n)$ and define $\theta = c\tilde{c}^{-1} = (\theta_1, \cdots, \theta_n)$ where $\theta_i = x^{\alpha_i}y^{\beta_i}$. Define the following quantities:

$$n_1(c,\tilde{c}) = |\{i \in [1,\cdots,n] | \beta_i = 1\}|$$
$$n_2(c,\tilde{c}) = |\{i \in [1,\cdots,n] | \beta_i = 0, \alpha_i \neq 0\}|$$
$$n_3(c,\tilde{c}) = |\{i \in [1,\cdots,n] | \beta_i = 0, \alpha_i = 0\}| = n - n_1 - n_2$$
$$m_1(u,\tilde{u}) = \left|\{i \in [1,\cdots,k] | b_i \neq \tilde{b}_i\}\right|$$
$$m_2(u,\tilde{u}) = \left|\{i \in [1,\cdots,k] | b_i = \tilde{b}_i, a_i \neq \tilde{a}_i\}\right|$$
$$m_3(u,\tilde{u}) = \left|\{i \in [1,\cdots,k] | b_i = \tilde{b}_i, a_i = \tilde{a}_i\}\right| = k - m_1 - m_2$$

Lemma IV.1. *For $u, \tilde{u} \in \mathbb{D}_6^k$ and $c, \tilde{c} \in \mathbb{D}_6^n$, we have*

$$P\left(G(\tilde{u})\cdot B = \tilde{c}|G(u)\cdot B = c\right)$$
$$= \frac{1}{10^{kn}}\left[10^{k-m_1}\cdot 3\sum_{\substack{l=1\\ l \text{ odd}}}^{m_1}\binom{m_1}{l}9^{l-1}\right]^{n_1}\cdot$$
$$\left[\frac{10^{k-m_1-m_2}(10^{m_2}+2)}{3} + 10^{k-m_1}\cdot 3\sum_{\substack{l=2\\ l \text{ even}}}^{m_1}\binom{m_1}{l}9^{l-1}\right]^{n_2}\cdot$$
$$\left[\frac{10^{k-m_1-m_2}(10^{m_2}-1)}{3} + 10^{k-m_1}\cdot 3\sum_{\substack{l=2\\ l \text{ even}}}^{m_1}\binom{m_1}{l}9^{l-1}\right]^{n_3}$$

Moreover, for a fixed u, let $T_{m_1,m_2}(u)$ be the set of all $\tilde{u}$ with $m_1(u,\tilde{u}) = m_1$, $m_2(u,\tilde{u}) = m_2$, then

$$|T_{m_1,m_2}(u)| = \binom{k}{m_1, m_2, m_3}\cdot 3^{m_1}\cdot 2^{m_2}$$
$$= \binom{k}{m_1}\binom{k-m_1}{m_2}\cdot 3^{m_1}\cdot 2^{m_2}$$

Proof: The proof involves solving non-commutative linear equations in several cases. It can be found in a more complete version of this work [18]. ∎

Define

$$A(m_1) = \sum_{\substack{l=1\\ l \text{ odd}}}^{m_1}\binom{m_1}{l}9^l$$
$$B(m_1,m_2) = \frac{(10^{m_2}+2)}{10^{m_2}} + \sum_{\substack{l=2\\ l \text{ even}}}^{m_1}\binom{m_1}{l}9^l$$
$$C(m_1,m_2) = \frac{(10^{m_2}-1)}{10^{m_2}} + \sum_{\substack{l=2\\ l \text{ even}}}^{m_1}\binom{m_1}{l}9^l$$

Using the above lemma and definitions, the expected value of the average probability of error can be upper bounded by:

$$\mathbb{E}\{P_{avg}(err)\}$$
$$\leq \sum_{m_1=0}^{k}\sum_{m_2=0}^{k-m_1}\sum_{n_1=0}^{n}\sum_{n_2=0}^{n-n_1}\binom{k}{m_1}\binom{k-m_1}{m_2}\cdot 3^{m_1}\cdot 2^{m_2}\frac{1}{10^{kn}}\cdot$$
$$10^{n(k-m_1)}\cdot\frac{1}{3^n}A(m_1)^{n_1}B(m_1,m_2)^{n-n_1-n_2}C(m_1,m_2)^{n_2}\cdot$$
$$\left|\left(x\cdot\{y,xy,x^2y\}^{n_1}\times\{x,x^2\}^{n_2}\times\{1\}^{n-n_1-n_2}\right)\cap A_\epsilon^n(X|y)\right|$$

Note that the cardinality term in the above expression can be upper bounded by

$$\left|\left(c\cdot\{y,xy,x^2y\}^{n_1}\times\{1,x,x^2\}^{n-n_1}\right)\cap A_\epsilon^n(X|y)\right|$$

and in turn, we have the following lemma:

Lemma IV.2. *Let $y \in \mathscr{Y}^n$ be an arbitrary channel output sequence. For any $x \in A_\epsilon^n(X|y)$, we have*

$$\left|\left(c\cdot\{y,xy,x^2y\}^{n_1}\times\{1,x,x^2\}^{n-n_1}\right)\cap A_\epsilon^n(X|y)\right|$$
$$\leq \binom{n}{n_1}2^{n[H(X|[X]Y)+O(\epsilon)]}$$

Where the random variable $[X]$ takes value from the set of cosets of $\{1, x, x^2\}$ in $\mathbb{D}_6$.

Proof: The complete proof of this lemma can be found in a more complete version [18]. ∎

Using these lemmas we can show that $\forall\delta,\delta' > 0$ if

$$\begin{cases} R < \log_2[6(1-\delta)] - H(X|Y) \\ R < \frac{\log_2 6}{\log_2 3}\left\{\log_2\left[3(1-\delta')\right] - H(X|[X]Y)\right\}\end{cases}$$

then the expected value of the average probability of error vanishes as n increases. This implies that the rate R^* is

achievable.

In the following two sections, we state some recent results in this direction without proofs. These results will be published in due course.

V. A Simpler Construction

In Section III, we defined the class of pseudo-group codes based on Forney's analysis of group codes and in Section IV we showed that these codes have a good performance for the point-to-point communication problem. In this section, we introduce another class of codes over $\mathbb{D}_6$ with similar properties as those of pseudo-group codes defined in Section III. The new class of pseudo-group codes defined in this section have the advantage of a simpler construction. This enables us to use this ensemble in Section VI for the problem of computation over MAC.

The new ensemble of codes is constructed as follows:

- For $i = 1, \cdots, n$ and $j = 1, \cdots, k$, let
$$r_{ij}, t_{ij}, d_i \in \mathbb{Z}_3$$
$$s_{ij}, \delta_i \in \mathbb{Z}_2$$
be uniform and independent random variables over their corresponding domains.
- Given the input sequence $\boldsymbol{u} = (u_1, u_2, \cdots, u_k) \in \mathbb{D}_6^k$ where $u_j = x^{a_j^u} y^{b_j^u}$, $a_j^u \in \mathbb{Z}_3$, $b_j^u \in \mathbb{Z}_2$ for $j = 1, \cdots, k$, define
$$\begin{cases} A_i(\boldsymbol{u}) = \sum_{j=1}^k r_{ij} a_j^u + \sum_{j=1}^k t_{ij} b_j^u \\ B_i(\boldsymbol{u}) = \sum_{j=1}^k s_{ij} b_j^u \end{cases}$$
- The output of the encoder is $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{D}_6^n$ where for $i = 1, \cdots, n$,
$$x_i = y^{B_i(u)+\delta_i} x^{A_i(u)+d_i}$$
We denote this by $\boldsymbol{x} = G(\boldsymbol{u})$

It turns out that this ensemble has the same average performance as the ensemble of codes defined in Section III. i.e. it can achieve the rate R^* defined in Theorem IV.1.

VI. Computation Over MAC

In this section, we use the ensemble of codes defined in Section V for the problem of computation over multiple access channels. Consider the two user MAC depicted in Figure 2 where X, Z take values from the Dihedral group $\mathbb{D}_6$ and Y takes values from a finite set $\mathscr{Y}$.

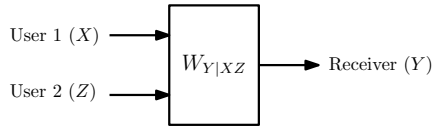

Fig. 2: Two user MAC: Computation of $\mathbb{D}_6$ operation.

When the inputs of the channel are $x, z \in \mathbb{D}_6$, the channel output is $y \in \mathscr{Y}$ with conditional probability $W_{Y|XZ}(y|x,z)$. Let n be the block length and let $\mathbb{C}_1 \subseteq \mathbb{D}_6^n$ and $\mathbb{C}_2 \subseteq \mathbb{D}_6^n$ be codebooks corresponding to Users 1 and 2 respectively. If User 1 sends a message $\boldsymbol{x} \in \mathbb{C}_1$ and User 2 sends a message $\boldsymbol{z} \in \mathbb{C}_2$, the decoder wishes to reconstruct $\boldsymbol{x} \cdot \boldsymbol{z}$ losslessly where the multiplication is the component-wise group operation.
The average probability of error for any code in this ensemble is given by

$$P_{err} = \sum_{\boldsymbol{x} \in \mathbb{C}_1} \sum_{\boldsymbol{z} \in \mathbb{C}_2} \frac{1}{|\mathbb{C}_1| \cdot |\mathbb{C}_2|} \sum_{\boldsymbol{y} \in \mathscr{Y}^n} W_{Y|XZ}^n(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{z}) \sum_{\substack{\tilde{\boldsymbol{w}} \in \mathbb{C}_1 \cdot \mathbb{C}_2 \\ \tilde{\boldsymbol{w}} \neq \boldsymbol{x}\boldsymbol{z}}} \mathbb{1}_{\{\tilde{\boldsymbol{w}} \in A_\epsilon^n(W|\boldsymbol{y})\}}$$

Let X and Z be uniform and independent random variables over $\mathbb{D}_6$ and let Y be the channel output when the inputs are X and Z. Define $W = X \cdot Z$ where $\cdot$ is the group operation. Note that W itself is uniform. It turns out the rate $R = \min(R_1, R_2, R_3)$ is achievable using non-Abelian codes where

$$R_1 = \log_2 6 \, [1 - H^*]$$
$$R_2 = \log_2 3 - H(W|[W]Y)$$
$$R_3 = \frac{\log_2 6}{\log_2 12} \, [\log_2 6 - H(W|Y)]$$

where

$$H^* = \sum_{s \in \mathscr{Y}} P_Y(s) \Bigg[\big(P_{W|Y}(x|s) + P_{W|Y}(x^2|s)\big) \, h\Big(\frac{P_{W|Y}(x|s)}{P_{W|Y}(x|s) + P_{W|Y}(x^2|s)}\Big) + \big(P_{W|Y}(xy|s) + P_{W|Y}(x^2y|s)\big) h\Big(\frac{P_{W|Y}(xy|s)}{P_{W|Y}(xy|s) + P_{W|Y}(x^2y|s)}\Big) + \big(P_{W|Y}(1|s) + P_{W|Y}(y|s)\big) \Bigg]$$

VII. Comparison With Abelian Group Codes and Random Codes

The only Abelian group of size 6 is $\mathbb{Z}_6 = \{0, 1, \cdots, 5\}$ where the group operation is addition mod-6. The best achievale rate using Abelian group codes over $\mathbb{Z}_6$ is known to be [17]

$$R^* = \min \Bigg(\log_2 6 - H(X|Y), \frac{\log_2 6}{\log_2 3} \, [\log_2 3 - H(X|[X]_3 Y)], \log_2 6 \, [1 - H(X|[X]_2 Y)] \Bigg)$$

where $[X]_3$ takes values from cosets of $\{0, 2, 4\}$ and $[X]_2$ takes values from cosets of $\{0, 3\}$. In the following, we present two examples. In the first example, we show that the achievable rate using the new code can be strictly larger than the rate achievable using Abelian group codes for the point-to-point problem. In the second example, we show that under certain conditions, the achievable rate using non-Abelian codes can be strictly larger than the rate achievable using random codes for the problem of computation over MAC.

A. Example 1: Point-to-Point Problem

We give an example where the capacity of group codes is zero whereas the constructed code achieves a strictly positive rate. Consider the channel depicted in Figure 3 where $\epsilon_1 = 0.1$, $\epsilon_2 = 0.2$ and $\epsilon_3 = 0.15$. If we maximize over all possible la-

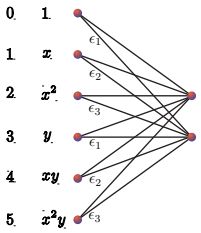

Fig. 3: Point-to-Point Channel: The first column on the left shows the input labels in $\mathbb{Z}_6$ and the second column shows the labels in $\mathbb{D}_6$.

belings of the channel input alphabet, it can be shown that both coding schemes achieve the symmetric capacity of the channel which is equal to 0.0139 bits per channel use. However, if the labels are assumed to be fixed, the achievable rate using pseudo-group codes is equal to $R^* = \min(0.0139, 0.0227) = 0.0139$ and the achievable rate using Abelian group codes is equal to $R = \min(0.0139, 0.0227, 0) = 0$. Indeed using the converse provided in [17] we can show that the capacity of Abelian group codes over this channel is equal to zero. We observe that for this channel, the codes over $\mathbb{D}_6$ outperform the codes over $\mathbb{Z}_6$.

B. Example 2: Computation Over MAC

Consider the channel depicted in Figure 4 where X, Z and W take values form $\mathbb{D}_6$ and Y is binary. The channel $W_{Y|W}$ is characterized the input-output re-

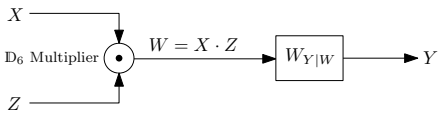

Fig. 4: MAC for computation of $\mathbb{D}_6$ operation.

lation $Y = W \cdot N$ where N is a random noise taking values from $\{1, x, x^2, y, xy, x^2y\}$ with probabilities $[\ 0.1606 \quad 0.1396 \quad 0.3545 \quad 0.0049 \quad 0.0230 \quad 0.3173\ ]$ respectively. Note that the channel $W_{Y|W}$ is symmetric. The achievable rate using non-Abelian codes can be computed as $R_{\text{new}} = \min(R_1, R_2, R_3) = 0.3936$ where $R_1 = 0.5500$, $R_2 = 0.4756$ and $R_3 = 0.3936$. The achievable rate using random codes is equal to

$$R_{\text{random}} = \frac{1}{2} I(XZ; Y) = 0.2729$$

We observe that for this example, non-Abelian codes outperform random codes.

C. Comparison

If we compare the two achievable rates for the point-to-point problem, we observe that for the case of Abelian group codes there is an additional term in the minimization which can be explained by the additional structure of the Abelian group codes. Indeed, the pseudo-group code over $\mathbb{D}_6$ is additive (homomorphic) with respect to the y generator and is not homomorphic with respect to the x generator whereas Abelian group codes are homomorphic with respect to both of their generators. This means compared to Abelian Group codes, the constructed codes gain a higher rate by reducing the structure.

VIII. Conclusion

We have shown that good structured codes over non-Abelian groups do exist. We constructed codes over the smallest non-Abelian group $\mathbb{D}_6$ and showed that the performance of these codes is superior to the performance of Abelian group codes of the same alphabet size. We also showed that such codes can be used for multi-terminal problems (such as computation over MAC) and can outperform random codes in such settings.

References

[1] R. Ahlswede. "Group codes do not achieve Shannons's channel capacity for general discrete channels". *The annals of Mathematical Statistics*, 42(1):224–240, Feb. 1971.

[2] R. Ahlswede and J. Gemma. "Bounds on algebraic code capacities for noisy channels I". *Information and Control*, 19(2):124–145, 1971.

[3] R. Ahlswede and J. Gemma. "Bounds on algebraic code capacities for noisy channels II". *Information and Control*, 19(2):146–158, 1971.

[4] N. J. Bloch. *"Abstract Algebra With Applications"*. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1987.

[5] G. Como and F. Fagnani. "The capacity of finite abelian group codes over symmetric memoryless channels". *IEEE Transactions on Information Theory*, 55(5):2037–2054, 2009.

[6] R. L. Dobrushin. "Asymptotic optimality of group and systematic codes for some channels". *Theor. Probab. Appl.*, 8:47–59, 1963.

[7] P. Elias. "Coding for noisy channels". *IRE Conv. Record*, part. 4:37–46, 1955.

[8] D. Forney. "On the hamming distance properties of group codes". *IEEE Transactions on Information Theory*, 38:1797–1801, 1992.

[9] J. Interlando, R. Palazzo, and M Elia. "Group block codes over nonabelian groups are asymptotically bad". *IEEE Transactions on Information Theory*, 42:1277–1280, 1996.

[10] G. D. Forney Jr and M. Trott. "The dynamics of group codes: State spaces, trellis diagrams, and canonical encoders". *IEEE Transactions on Information Theory*, 39(9):1491–1513, 1993.

[11] J. Korner and K. Marton. "How to encode the modulo-two sum of binary sources". *IEEE Trans. on Inf. Th.*, IT-25:219–221, Mar. 1979.

[12] D. Krithivasan and S. S. Pradhan. "Distributed source coding using abelian group codes". 2011. IEEE Trans. on Inf. Th.(57)1495-1519.

[13] P. Massey. "Many Non-Abelian Groups Support Only Group Codes That Are Conformant To Abelian Group Codes". *ISIT*, 1997. Ulm. Germany.

[14] B. A. Nazer and M. Gastpar. "Computation over multiple-access channels". *IEEE Trans. on Inf. Th.*, 53, Oct. 2007.

[15] T. Philosof, A. Kishty, U. Erez, and R. Zamir. "Lattice strategies for the dirty multiple access channel". *Proceedings of IEEE International Symposium on Information Theory*, July 2007. Nice, France.

[16] S. S. Pradhan and K. Ramchandran. "Distributed source coding using syndromes (DISCUS): Design and construction". *IEEE Transactions on Information Theory*, 49(3):626–643, 2003.

[17] A. G. Sahebi and S. S. Pradhan. "On the Capacity of Abelian Group Codes Over Discrete Memoryless Channels". July 2011. ISIT, Saint Petersburg, Russia.

[18] A. G. Sahebi and S. Sandeep Pradhan. Asymptotically good codes over non-abelian groups. 2012. Online: http://arxiv.org/submit/410556.

[19] D. Slepian. "Group codes for for the Gaussian channel". *Bell Syst. Tech. Journal*, 1968.