Some Randomized Code Constructions From Group Actions

Louay M. J. Bazzi and Sanjoy K. Mitter, *Fellow, IEEE*

***Abstract*—We study in this paper randomized constructions of binary linear codes that are invariant under the action of some group on the bits of the codewords. We study a non-Abelian randomized construction corresponding to the action of the dihedral group on a single copy of itself as well as a randomized Abelian construction based on the action of an Abelian group on a number of disjoint copies of itself. Cyclic codes have been extensively studied over the last 40 years. However, it is still an open question as to whether there exist asymptotically good binary cyclic codes. We argue that by using a slightly more complex group than a cyclic group, namely, the dihedral group, the existence of asymptotically good codes that are invariant under the action of the group on itself can be guaranteed. In particular, we show that, for infinitely many block lengths, a random ideal in the binary group algebra of the dihedral group is an asymptotically good rate-half code with a high probability. We argue also that a random code that is invariant under the action of an Abelian group G of odd order on k disjoint copies of itself satisfies the binary Gilbert–Varshamov (GV) bound with a high probability for rate $1/k$ under a condition on the family of groups. The underlying condition is in terms of the growth of the smallest dimension of a nontrivial $\mathbb{F}_2$-representation of the group and is satisfied by roughly most Abelian groups of odd order, and specifically by almost all cyclic groups of prime order.**

***Index Terms*—Abelian codes, dihedral group, group actions, group algebra, probabilistic method, quasi-cyclic codes.**

I. Introduction

LINEAR codes that are symmetric in the sense of being invariant under the action of some group on the bits of the codewords have been studied extensively before. However, we still know very little about how the group structure can be exploited in order to establish bounds on the minimum distance or to come up with decoding algorithms.

One example of such codes are codes that are invariant under the action of some group on itself. When the group is cyclic these are cyclic codes. Another example is when we have a group acting on more than one copy of itself. When the group is cyclic these are quasi-cyclic codes.

A. Preliminaries

1) Binary Linear Codes: Unless otherwise specified, by a code, we mean a binary linear code. The *minimum distance* of a binary code is the minimum Hamming distance between two distinct codewords or equivalently the minimum weight of a nonzero codeword since the code is linear. Its *minimum relative distance* is its minimum distance normalized by the block length. Its *rate* is the binary logarithm of the code size normalized by the block length. By a binary code we mean implicitly an *infinite family of binary codes* indexed by the block length. We do not require that each positive integer be a block length, we simply require that there are codes in the family of codes of arbitrarily large block length. The *rate* (*minimum relative distance*, respectively) of the family of codes means the lim-inf of the rate (minimum relative distance, respectively) of a code in the family as the block length tends to infinity. An infinite family of codes is called *asymptotically good* if both its rate and its minimum distance are strictly positive. This is equivalent to saying that the fraction of redundancy added is bounded by a constant, and the minimum distance of the code grows linearly with the block length. We say that a family of codes of rate r and minimum relative distance δ *satisfies or achieves the binary GV (Gilbert–Varshamov) bound* if $r \geq 1 - h(\delta)$, where h is the *binary entropy function*, i.e., $h(x) = -x \log x - (1 - x) \log(1 - x)$. By abuse of notation, when asymptotic statements are made, a code means implicitly an infinite family of codes. For instance, "an asymptotically good code" means "an asymptotically good infinite family of codes," and "a code satisfying the GV bound" means "an infinite family of codes satisfying the GV bound." See [7] and [12] for a general background.

2) Finite Semisimple Rings and Group Algebras: We assemble in this section some basic properties of finite rings with identity and group algebras that we are going to use later. See [1]–[9].

Let R be a finite ring with identity.

A nonzero left ideal of R is called *irreducible* or *minimal* if it is not the direct sum of two nonzero left ideals of R.

The ring R is called *simple* if it has no proper two-sided ideal. Every simple ring R is isomorphic to a matrix algebra $M_d(K)$ over some finite field K, where the *matrix algebra* $M_d(K)$ is the K-algebra consisting of all the $d \times d$ matrices over K. In a simple ring, all the nonzero irreducible left ideals are isomorphic. Moreover, if R is a simple ring isomorphic to $M_d(K)$, then R can be expressed as a direct sum $R = \oplus_{j=1}^{d} R_j$, where the R_j are irreducible left ideals. The decomposition is not unique unless $d = 1$.

The *radical* of R is the intersection of all the maximal left (or, equivalently, right) ideals of R. The radical of R is a two-sided

Manuscript received October 15, 2005. This work was supported by the National Science Foundation under Grant CCR-0112487, by ARO under Grant DAAD19-00-1-0466, by NSF:KDI under Grant ECS-9873451, and by ARO under Grant to Brown University Subcontract 654-21256.

L. M. J. Bazzi is with the Department of Electrical and Computer Engineering, American University of Beirut (AUB), Beirut 1107 2020, Lebanon (e-mail: Louay.Bazzi@aub.edu.lb).

S. K. Mitter is with the Laboratory for Information and Decision Systems, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139-4307 USA (e-mail: mitter@mit.edu).

Communicated by R. J. McEliece, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.876244

ideal. A (left or right) ideal I is called *nilpotent* if $I^n = (0)$ for some integer n. The radical of R contains all the nilpotent (left and right) ideals of R, and it is the largest nilpotent ideal of R.

The ring R is called *semisimple* if its radical is zero. A simple ring is semisimple. Every semisimple ring R is the direct sum $R = \oplus_i R_i$ of two-sided ideals that are simple as rings. Moreover the decomposition is unique, and $R_i R_j = 0$ for all $i \neq j$.

Let G be a finite group and F a finite field. The *group algebra* $F[G]$ of G over F is the F-algebra consisting of formal sums of the form $\sum_{g \in G} f(g)g$ over F, where $f : G \to F$.

The group algebra $F[G]$ is semisimple if and only if the characteristic of F does not divide the order of G.

3) Group Action Codes: A binary linear code invariant under the action of a group is defined as follows. Consider an action ρ of a finite group G on a finite set S, and say that a (binary $\mathbb{F}_2$-linear) code C is ρ-invariant if it satisfies the following. Let M be the $|S|$-dimensional $\mathbb{F}_2$-vector space written as the set of formal sums $\sum_{s \in S} f(s)s, f : S \to \mathbb{F}_2$. Consider the induced action of G on M by (say left) translation $g : f(x) \mapsto f(gx)$. Then we say that C is ρ-invariant if C is a subset of M closed under addition and under translation by the elements of G. In other words, C is ρ-invariant if C is an $\mathbb{F}_2[G]$-submodule of M (again with the left multiplication convention). Note that if $\sum_{s \in S} f(s)s$ is an element of C, then the vector representation of the corresponding codeword is $(f(s))_{s \in S}$. Note also that when talking about the asymptotic properties of a group action code, we implicitly mean that we have an infinite family of group actions $\{\rho_n\}_{n \in I}$, with the group G_n acting on the set S_n via ρ_n. The family is indexed by the block length $n = |S_n|$ of the ρ_n-invariant code C_n.

B. Literature on Group Action Codes

1) Cyclic and Abelian Codes: Binary Abelian codes are invariant under the action of an Abelian group G on a single copy of itself, i.e., they are ideals in the binary group algebra $\mathbb{F}_2[G]$. Cyclic codes correspond to the special case when G is cyclic. These codes, and specifically cyclic codes, have been extensively studied over the last 40 years. See, for instance, [14]. However, the existence of asymptotically good binary cyclic or Abelian codes in general is still an open question.

2) Codes in the Binary Group Algebra of the Dihedral Group: These codes are invariant under the action of the dihedral group D_m on itself, i.e., they are ideals in the binary group algebra $\mathbb{F}_2[D_m]$. The Dihedral group D_m contains 2 m element. It is generated by α and β subject to the relations $\alpha^2 = 1, \beta^m = 1$, and $\alpha\beta = \beta^{-1}\alpha$.

Codes in the binary group algebra of the dihedral group were introduced by MacWilliams [11] in the setting of self dual codes. As far as we know, nothing was known before our work about their asymptotic distance properties.

3) Quasi-Cyclic Codes: Quasi-cyclic codes are invariant under the action of a cyclic group on k disjoint copies of itself, i.e., they are $\mathbb{F}_2[\mathbb{Z}/m\mathbb{Z}]$-submodules of $\mathbb{F}_2[\mathbb{Z}/m\mathbb{Z}]^k$.

Quasi-cyclic codes were first studied by Chen, Peterson, and Weldon [2] in the setting when $m = p$ is prime. The result in [2] says that if 2 is a primitive root of p (i.e., 2 generates $\mathbb{F}_p^\times$), a random quasi-cyclic code, i.e., an $\mathbb{F}_2[\mathbb{Z}p\mathbb{Z}]$-submodule of $\mathbb{F}_2[\mathbb{Z}p\mathbb{Z}]^k$ generated by a random element of $\mathbb{F}_2[\mathbb{Z}p\mathbb{Z}]^k$, achieves the GV bound with a high probability. Without assuming the ERH (Extended Riemann Hypothesis), it is not known whether there are infinitely many primes with the above property. A later result by Kasami [5] shows that if instead of working in $\mathbb{Z}m\mathbb{Z}$, we work in $\mathbb{Z}/p_0^l\mathbb{Z}$, where l can vary and p_0 is fixed to the largest known prime such that 2 is a primitive root of p_0, a random quasi-cyclic code achieves a slightly weaker bound than the GV bound.

A subsequent work by Chepyzhov [3] shows that in the cyclic prime case the condition in [2] that requires 2 to be a primitive root of p can be relaxed to requiring that the size of the multiplicative group generated by 2 in $\mathbb{F}_p^\times$ grows faster than $\log p$, and hence the ERH can be avoided as it is not hard to show that there are infinitely many such primes.

4) Quadratic Residue Codes: Let p be a prime such that 2 is a quadratic residue, i.e., $p = \pm 1 \pmod 8$. Consider the decomposition $x^p - 1 = (x-1)q(x)\bar{q}(x)$ over $\mathbb{F}_2$, where $q(x) = \prod_{i \in Q}(x - \beta^i)$, $q(x) = \prod_{i \in \bar{Q}}(x - \beta^i)$, Q is the set of quadratic residues modulo $p, \bar{Q} = \mathbb{F}_p^\times \backslash Q$, and β is a primitive pth root of 1 in an extension field of $\mathbb{F}_2$. Binary quadratic residues codes are the ideals of $\mathbb{F}_2[\mathbb{Z}/p\mathbb{Z}] = \mathbb{F}_2[x]/(x^p - 1)$ generated by one the polynomial $q(x), \bar{q}(x)$ or one of their products with the polynomial $x - 1$.

Other than being cyclic codes, these codes are invariant under the action of the subgroup

$$\{\left(\begin{smallmatrix} a & * \\ 0 & a^{-1} \end{smallmatrix}\right)\}_{a \neq 0}$$

of $\mathrm{PSL}_2(\mathbb{F}_p)$ on $\mathbb{F}_p$ by affine transformations. They are also extendible from $\mathbb{F}_p$ to $\mathbb{F}_p \cup \{\infty\}$ in such a way they are invariant under the action of $\mathrm{PSL}_2(\mathbb{F}_p)$ by fractional linear transformations on $\mathbb{F}_p \cup \{\infty\}$. See [7], [14], and [17]. It is not known if binary quadratic residue codes can be asymptotically good.

5) Cayley Graphs Codes: Sipser and Spielman [16] constructed explicit binary asymptotically good low density parity check codes based on the explicit constructions of Cayley graphs expanders of Lubotzky, Phillips, and Sarnak [10], and Margulis [8]. The underlying Cayley graph group is $\mathrm{PSL}_2(\mathbb{F}_p), p$ prime. These codes are realized as unbalanced bipartite graphs in such a way that the codewords are defined on the edges of the Cayley graph. They are invariant under the action of $\mathrm{PSL}_2(\mathbb{F}_p)$ on more than one copy of itself.

C. Summary of Results

1) Asymptotically Good Codes in the Group Algebra of the Dihedral Group: The most natural class of group action codes are those that are invariant under the action of a group G on itself, i.e., those that are ideals in the binary group algebra $\mathbb{F}_2[G]$ of a group G. The case when G is cyclic (respectively, Abelian) corresponds to the case of cyclic (respectively, Abelian) codes. Such codes are very well studied. As mentioned before, yet it is still an open question whether there exist asymptotically good cyclic or Abelian codes. The case when G is non-Abelian was studied and introduced by MacWilliams [11] in the setting of the dihedral group D_m. However, it was not noted that this group algebra contains asymptotically good codes.

Our result in Section III says that if we use a slightly stronger group than a cyclic group, and namely the dihedral group, the existence of asymptotically good codes can be guaranteed in the group algebra. In particular, we show that for infinitely many m, a random ideal in $\mathbb{F}_2[D_m]$ is an asymptotically good rate $1/2$ binary code. The first condition we need on m is that the smallest size of the multiplicative group generated by 2 in $\mathbb{F}_p^\times$ as p runs over the prime divisors of m (or equivalently the smallest dimension of a nontrivial $\mathbb{F}_2$-representation of $\mathbb{Z}/m\mathbb{Z}$) grows asymptotically faster than $\log m$. We require also for simplicity another condition and we argue that it is satisfied by all the primes $p = \pm 5 \pmod 8$. By random here, we mean according to some specific distribution, based on the $\mathbb{F}_2$-representations of D_m, which we specify later. The implicit bound on the relative minimum distance is $h^{-1}(1/4)$, where h is the binary entropy function.

As far as we know, this is the first provably good randomized construction of codes that are ideals in the group algebra of a group. We do not know if it was previously known that there exists asymptotically good codes that are ideals in the group algebra of a group.

We leave the corresponding analysis till the end since it is based on the analysis of the quasi-Abelian case that we overview next.

2) Quasi-Abelian Codes Up To the GV Bound: Rather than considering the action of a group G on itself, one can consider the action of G on k disjoint copy of itself. This means looking at codes that are $\mathbb{F}_2[G]$-submodules of $\mathbb{F}_2[G]^k$. When G is cyclic, these are quasi-cyclic codes.

We consider the case when G is an Abelian group of odd order. Our result in Section II is that if the dimension $L(G)$ of the smallest irreducible $\mathbb{F}_2$-representation of G grows faster than logarithmically in the order of the G, then an $\mathbb{F}_2[G]$-submodule of $\mathbb{F}_2[G]^k$ generated by a random element of $\mathbb{F}_2[G]^k$ achieves the GV bound at rate $1/k$ with a high probability. Here, random means almost uniformly in a suitable sense that we specify later. Roughly, almost all Abelian groups of odd order satisfy the above condition. This includes almost all cyclic groups of prime order. Since G is Abelian, $L(G)$ depends only on the order of G, and it is the smallest size of the multiplicative group generated by 2 in $\mathbb{F}_p^\times$, where p runs over the prime divisors of m.

Comparing our result with the existing literature on quasi-cyclic codes surveyed in Section I-B-3), we see that the innovation in our result is in the fact that it holds for Abelian groups that are not necessarily cyclic of prime order which has the advantage of supplying more block lengths. Our condition on the order of the group is a generalization of the condition of Chepyzhov [3] from cyclic groups of prime order to arbitrary Abelian groups of odd order.

II. Randomized Construction From Abelian Groups Actions

We establish in this section the Claims of Section I-C-2). We consider the case when G is an Abelian group of odd order. We argue in Theorems 2.1 and 2.4 that if the dimension $L(G)$ of the smallest irreducible $\mathbb{F}_2$-representation of G grows faster than logarithmically in the order of the G, then an $\mathbb{F}_2[G]$-submodule of $\mathbb{F}_2[G]^k$ generated by a random element of $\mathbb{F}_2[G]^k$ achieves the GV bound with a high probability. Since G is Abelian, $L(G)$ depends only on the order of G, and it is the smallest size of the multiplicative group generated by 2 in $\mathbb{F}_p^\times$, where p runs over the prime divisors of m. See Lemma 2.5. We note that roughly, almost all Abelian group of odd order satisfy the above condition.

Theorem 2.1: Let G be a finite Abelian group of odd order m, and consider its binary group algebra

$$\mathbb{F}_2[G] \overset{\text{def}}{=} \{\sum_{g\in G} f(g)g | f : G \to \mathbb{F}_2\}.$$

Consider the randomized construction of codes

$$C_{a,b} = \{(fa, fb) | f \in \mathbb{F}_2[G]\},$$

where a, b are selected uniformly at random from $\mathbb{F}_2[G]$.

Let $L(G)$ be the smallest dimension of a nontrivial $\mathbb{F}_2$-representation of G or, equivalently, the smallest dimension of a nontrivial[1] $\mathbb{F}_2[G]$-module, or equivalently the smallest dimension of a nontrivial irreducible ideal in $\mathbb{F}_2[G]$.

If $\delta > 0$ is such that $h(\delta) \leq \frac{1}{2} - \frac{\log m}{2L(G)}$, then the probability that the minimum relative distance of the code $C_{a,b}$ is below δ or the rate of $C_{a,b}$ is below $\frac{1}{2} - \frac{1}{2m}$ is at most $2^{-2L(G)(1/2-h(\delta))+5\log m}$, where h is the binary entropy function.

Therefore, if $L(G)$ grows asymptotically faster than $\log m$, then the code $C_{a,b}$ achieves the GV bound for rate $1/2$ with a high probability.

Proof: Let $R \overset{\text{def}}{=} \mathbb{F}_2[G]$. Let P be the probability that $C_{a,b}$ has dimension below $m-1$ and minimum distance below $2m\delta$, where δ is say below $1/2$ for the moment. P is at most the probability that there is an $f \in R, f \neq 0$ and $f \neq e_0 \overset{\text{def}}{=} \sum_{g\in G} g$, such that the event

$$E(f, a, b) : 0 \leq w(fa) + w(fb) < 2m\delta$$

occurs. This is true since $(e_0 a, e_0 b)$ is either $(e_0, 0), (0, e_0), (e_0, e_0)$, or $(0, 0)$, and thus $w(e_0 a) + w(e_0 b) = m$, $2m$, or 0. The first two values are above $2\delta m$ and the last can only decrease the rank of $C_{a,b}$ by 1. Thus, by the union bound on f

$$\begin{aligned} P &\leq \sum_{f\in R, f\neq 0, e_0} Pr_{a,b}[E(f, a, b)] \\ &\leq \sum_{l=2}^{m} |D_l| \max_{f\in D_l} Pr_{a,b}[E(f, a, b)]. \end{aligned} \tag{1}$$

where

$$D_l = \{f \in R | \dim_{\mathbb{F}_2} fR = l\}$$

and fR is the ideal generated by f in R. Note that we excluded the case $l = 0$ and $l = 1$ since they can only happen when $f = 0$ and $f = e_0$, respectively.

[1] By a trivial $\mathbb{F}_2[G]$-module, we mean a R-module M such that $rm = m, \forall m \in M$ and $r \in \mathbb{F}_2[G]$.

For all $f \neq e_0$, the ideal fR is nontrivial, so $\dim_{\mathbb{F}_2} fR \geq L(G)$. Thus

$$D_l = \emptyset \text{ for all } 2 \leq l < L(G). \tag{2}$$

Let

$$\Omega_l = \{I \text{ an ideal of } R | \dim_{\mathbb{F}_2} I = l\}$$

so we have

$$|D_l| \leq 2^l |\Omega_l|. \tag{3}$$

For any l, and any $f \in D_l$, we have

$$\begin{aligned}\Pr_{a,b}[E(f,a,b)] \leq & \sum_{r_1, r_2 \in fR \text{s.t.} 0 \leq w(r_1)+w(r_2) < 2m\delta} \\ & \times \Pr_{a,b}[fa = r_1 \text{ and } fb = r_2] \\ \leq & 2^{-2l} \sum_{w_1, w_2 \geq 0; w_1 + w_2 < 2\delta m} |I^{(w_1)}||I^{(w_2)}| \end{aligned} \tag{4}$$

where $I = fR$, and if I is an ideal, by $I^{(w)}$ we mean

$$I^{(w)} \overset{\text{def}}{=} \{r \in I | w(r) = w\}.$$

The 2^{-2l} term is the value of $\Pr_{a,b}[fa = r_1 \text{ and } fb = r_2]$. Indeed, for any $r \in fR$

$$\Pr_a[fa = r] = \frac{|Ker \Phi_f|}{|R|} = \frac{1}{|fR|} = 2^{-l}$$

where $\Phi_f : R \twoheadrightarrow fR$ is given by $a \mapsto fa$.

Replacing (2), (3), and (4) in (1), we get

$$P \leq \sum_{l=L(G)}^{m} 2^{-l} |\Omega_l| \max_{I \in \Omega_l} \sum_{w_1, w_2 \geq 0; w_1 + w_2 < 2\delta m} |I^{(w_1)}||I^{(w_1)}|. \tag{5}$$

Note that so far we have not used any property that depends on G being Abelian. Note also that the maximum above can be replaced by an expected value, but we will not need that.

Lemma 2.2: If I is an ideal in R of dimension l, then $|I^{(w)}| \leq 2^{lh(w/m)}$, where h is the binary entropy function.

Proof: This follows from the work of Piret [13] and Shparlinsky [15]. In fact this holds when $R = \mathbb{F}_2[G]$, and G is an arbitrary group of size m. The result in [13] and [15] says the following.

Let J be an index set of size m and let C be a subset of $\{0,1\}^J$ of size 2^l. Call a subset A of J an *information set* of C if the projection map form C to $\{0,1\}^A$ is a bijection (thus $|A| = l$). Call C *balanced* if there exists $r \geq 1$ and information sets $A_1, \ldots, A_u$ of C such that for all i in J, the number of j such that $i \in A_j$ is exactly r (note that the A_i need not be distinct). The result of [13] and [15] asserts that if C is balanced then the number of vectors in C of weight w is at most $2^{lh(w/m)}$. The proof is a double-counting argument. This is directly applicable to the case when C is ideal in $\mathbb{F}_2[G]$. The reason is that since C is linear it must contain an information set $S \subset G$ of size l, and since C is invariant under the action of G, the $\{Sg\}_{g \in G}$ are informations sets also. These information sets make C balanced because for each a in G, the number of g such that $a \in Sg$ is exactly $|S|$. ▼

Lemma 2.3: $|\Omega_l| \leq m^{l/l_0 + 1}$, where $l_0 = L(G)$.

Proof: Here we use the fact that G is Abelian. In general, since $|G|$ is odd, R is semisimple. Let $R = R_0 \oplus R_1 \oplus \ldots \oplus R_s$ be the unique decomposition of R into indecomposable two-sided ideals. The R_i are simple rings. Since G is Abelian the R_i are irreducible and they are the only irreducible ideals in R (Each R_i is actually a field with its idempotent as a unit element). Thus, each ideal in R is of the form $\oplus_{i \in A} R_i$ for some subset A of $\{0, 1, \ldots, s\}$. This fact is the reason behind the claimed bound on $|\Omega_l|$; if G were non-Abelian, then $|\Omega_l|$ can be much larger than this because each R_i may contain many irreducible ideals. Without loss of generality, say that R_0 is the trivial one dimensional ideal, i.e., $R_0 = (\sum_{g \in G} g)R$. Thus, for each $i \neq 0$, the dimension of R_i is at least $l_0 = L(G)$. So, $1 + l_0(s-1) \leq m$. If I is an ideal of dimension l, then it is a direct sum of at most $l/l_0 + 1$ of the R_i. There are at most s^{l/l_0+1} such direct sum, so $|\Omega_l| \leq s^{l/l_0+1} \leq m^{l/l_0+1}$. ▼

Note that we can get a sharper bound, but this is sufficient for our purpose.

Replacing the estimates in Lemmas 2.2 and 2.3 in (5), we get

$$\begin{aligned} P &\leq \sum_{l=l_0}^{m} 2^{-l} m^{l/l_0+1} \sum_{w_1, w_2 \geq 0; w_1 + w_2 < 2\delta m} 2^{l(h(w_1/m) + h(w_2/m))} \\ &\leq \sum_{l=l_0}^{m} 2^{-l} m^{l/l_0+1} (2\delta m)^2 2^{2lh(\delta)} \quad \text{(since } h \text{ is convex)} \\ &\leq \sum_{l=l_0}^{m} 2^{-2l\left(\frac{1}{2} - h(\delta) - \frac{\log m}{2l_0}\right) + 3\log m}. \end{aligned}$$

If $\frac{1}{2} - h(\delta) - \frac{\log m}{2l_0} \geq 0$, we get

$$\begin{aligned} P &\leq 2^{-2l_0(\frac{1}{2} - h(\delta) - \frac{\log m}{2l_0}) + 4\log m} \\ &= 2^{-2l_0(\frac{1}{2} - h(\delta)) + 5\log m}. \end{aligned}$$

This completes the proof of Theorem 2.1. ■

Note that the fact that the estimate of Lemma 2.3 fails for non-Abelian groups does not mean that they do not lead to good codes in the setting of this randomized construction. All that it says is that the argument may need some modifications. In any case, however, it will become clear in Section III that the reason why Lemma 2.3 fails for non-Abelian groups makes them subject to a more natural randomized construction.

More generally we have Theorem 2.4.

Theorem 2.4: Let G be an Abelian group of order m, and consider the randomized codes construction

$$C_{a_1,\ldots,a_k} = \{(fa_1,\ldots,fa_k) | f \in \mathbb{F}_2[G]\}$$

where $a_1,\ldots,a_k$ are selected uniformly at random from R^*, and R^* is the set of even weight strings in $R \overset{\text{def}}{=} \mathbb{F}_2[G]$.

If $L(G)$ grows asymptotically faster than $\log m$, then the code $C_{a_1,\ldots,a_k}$ achieves the GV bound for rate $1/k$ with a high probability.

Proof: The proof is by the same argument in Theorem 2.1. We need this even weight technicality in order to avoid the dominance of some bad events when k is large enough. The fact that the a_i have even weight will take care of the case when $f = e_0$ since then $e_0 a_i = 0$ always. ■

Lemma 2.5: Since G is Abelian, $L(G)$ depends only on the order of G and is given by

$$l(m) = \min\{\#\langle 2\rangle_p | p\text{a prime divisor of } m\}$$

where $\langle 2\rangle_p$ is the multiplicative subgroup generated by 2 in $\mathbb{F}_p^\times$.

Proof: Since G is Abelian, decompose G as $G = G_1 \times \ldots \times G_t$, where $G_i \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ and p_i is prime. Thus, $m = \prod_i p_i^{k_i}$. If $\rho : G \to \mathrm{GL}_l(\mathbb{F}_2)$ is a nontrivial $\mathbb{F}_2$-representation of G, then the restriction of ρ to one of the G_i must be nontrivial, thus $L(G) \geq \min_i L(G_i)$. Conversely, given a representation $\rho_i : G_i \to \mathrm{GL}_l(\mathbb{F}_2)$ of G_i, we can extend ρ_i to G via $\rho_i(g_1 \ldots g_t) = \rho_i(g_i)$. Thus, $L(G) = \min_i L(G_i)$. Therefore, we can assume without loss of generality that G is cyclic of order a power of a prime, say $\mathbb{Z}/p^k\mathbb{Z}$. Then, the dimensions of the irreducible $\mathbb{F}_2$-representations of G are precisely the sizes of the equivalence classes in $(\mathbb{Z}/p^k\mathbb{Z})/\sim$, where $a \sim b$ if $a = 2^i b$ (mod p^k) for some i. The trivial representation corresponds to the class consisting of 0. Thus

$$L(\mathbb{Z}/p^k\mathbb{Z}) = \min_{0<a<p^k} h(a,p^k) \text{ where}$$
$$h(a,p^k) = \min_{i\geq 1; a2^i = a(\mathrm{mod} p^k)} i.$$

Now, $h(a,p^k) = h(1,p^i)$, where $p^i = a/\gcd(p^k,a)$, as can be easily checked. Thus

$$L(\mathbb{Z}/m\mathbb{Z}) = \min_{i=1,\ldots,k} h(1,p^i) = h(1,p)$$

because $h(1,p^i) \geq h(1,p)$ for all $i \geq 1$, and hence the claim since $h(1,p) = \#\langle 2\rangle_p$. ■

Now, if $r : \mathbb{Z}_+ \to \mathbb{Z}_+$ is a nondecreasing function, let

$$Z(r) = \{m \in \mathbb{Z}_+ | l(m) \geq r(m)\}.$$

So any family of Abelian groups whose orders is in $Z(r)$ leads to rate $1/2$ codes up to the attainment of the GV bound as long as $r(m) \gg \log m$.

Let $P(r)$ be the set of primes in $Z(r)$.

Lemma 2.6: When $r(m) \ll \sqrt{m/\log m}$, $P(r)$ is infinite and contains almost all the primes.

Proof: This statement appears in Chepyzhov [3], but we include a proof for completeness. Say that a prime is bad if it is not in $P(r)$, and let B_n be the set of bad primes less than n. If p is a bad prime, then there exists integers a and k such that $0 < a < r(p)$ and $2^a - 1 = kp$. Since $r(n)$ is nondecreasing, we have

$$|B_n| \leq \#\{(a,k) | 0 < a < r(n) \text{ and } (2^a - 1)/k \text{ prime}\}$$
$$\leq r(n)\log(2^{r(n)} - 1) \leq r^2(n)$$

and hence the lemma follows from the prime numbers density theorem. ■

So we have many infinite families of Abelian groups that lead to codes up to the GV bound in the sense of Theorem 2.1, such as the following:

- the cyclic groups of prime order, where the primes are in $P(r)$, and $r(m) = \log m \log\log m$;
- any version of the Abelian groups of order pq, where $p, q \in P(r), r(m) = \log m \log\log m$, and $p^k, q^k > pq$ for some prespecified constant k;
- any version of the Abelian groups of order p^k, where $p \in P(r), r(m) = \log m \log\log m$, and k is a prespecified constant.

III. Dihedral Group Randomized Construction

In this section, we establish the claim of Section I-C-1). We argue in Theorem 3.4 that for infinitely many block lengths, a random ideal in the binary group algebra $\mathbb{F}_2[D_m]$ of the dihedral group D_m is an asymptotically good rate $1/2$ binary code. We show that the condition, we require on m is satisfied by almost half the primes, namely all primes p such that 2 is a nonquadratic residue mod p (i.e., $p = \pm 5 \pmod 8$) and such that the size of the multiplicative group generated by 2 in $\mathbb{F}_p^\times$ grows asymptotically faster than $\log p$. By random here, we mean according to some specific distribution based on the $\mathbb{F}_2$-representations of D_m in Theorem 3.3. The implicit bound on the relative minimum distance is $h^{-1}(1/4)$, where h is the binary entropy function.

Let m be odd, and consider the dihedral group

$$D_m = \langle \alpha, \beta | \alpha^2 = 1, \beta^m = 1, \alpha\beta = \beta^{-1}\alpha\rangle.$$

D_m has $2m$ elements: $\alpha^i\beta^j$ for $i = 0, 1$ and $j = 0,\ldots,m-1$.

We are interested in the the structure of $\mathbb{F}_2[D_m]$ in terms of its ideals. We will work with left ideals. Note that since the characteristic 2 of $\mathbb{F}_2$ divides the even order of D_m, the ring $\mathbb{F}_2[D_m]$ is not semisimple, i.e., its radical is nonzero.

Let N be the subgroup of D_m generated by β, and H the subgroup generated by α. Note that N is normal. Let

$$Q = \mathbb{F}_2[N].$$

Any element r of $\mathbb{F}_2[D_m]$ can be represented uniquely as $r = q + \alpha q'$, where $q, q' \in Q$. If $q = \sum_{g \in S} g$ is an element of Q, define

$$\tilde{q} \overset{\text{def}}{=} \sum_{g \in S} g^{-1}$$

and note that $\tilde{\ } : Q \rightarrow Q$ is a ring automorphism. From the relation $\alpha\beta = \beta^{-1}\alpha$, we get $\alpha\beta^i = \beta^{-i}\alpha$ for all i, and hence

$$\alpha q = \tilde{q}\alpha$$

for all $q \in Q$.

Since Q is semisimple (because m is odd), let

$$Q = \oplus_{i=0}^{s} Q_i$$

be the unique decomposition of Q into two-sided ideals, where each Q_i is a simple ring. Each Q_i must be a field since Q is commutative and a simple commutative ring is a field (the matrix algebra $M_d(K)$ over the field K is commutative iff $d = 1$).

One of the Q_i is the ideal $(\sum_{g \in N} g)$ generated by $\sum_{g \in N} g$, and it consists of 0 and $\sum_{g \in N} g$. Assume that the Q_i are ordered so that $Q_0 = (\sum_{g \in N} g)$.

The automorphism $\tilde{\ }$ maps each Q_i to some Q_j. We impose a restriction on the order m of D_m. We assume that m is such that

$$\tilde{Q}_i = Q_i, \qquad \text{for } i = 1, \ldots, s. \tag{6}$$

We need this assumption to simplify the analysis.

We argue below that this assumption is satisfied for infinitely many values of m.

Lemma 3.1: Assumption (6) is satisfied for all prime values p of m such that $p = \pm 5$ (mod 8).

Proof: Assume that m is a prime p. Assume further that $p = \pm 5$ (mod 8), or equivalently, 2 is a nonquadratic residue mod p. Realize Q as $Q = \mathbb{F}_2[x]/(x^p - 1)$, and let γ be a primitive pth root of 1 in a extension of $\mathbb{F}_2$; thus, the irreducible decomposition of $x^p - 1$ over $\mathbb{F}_2$ is

$$x^p - 1 = (x-1) \prod_{A \in \mathbb{F}_p^{\times}/\langle 2 \rangle} g_A(x), \text{ where } g_A(x) = \prod_{a \in A} (x - \gamma^a).$$

In these terms, the Q_i, where $i \neq 0$, are in one-to-one correspondence with the cosets $A \in F_2/\langle 2 \rangle$. The ideal Q_i corresponding to A is generated by

$$f_A(x) = (x-1) \prod_{B \in F_2/\langle 2 \rangle : B \neq A} g_B(x).$$

Thus $\tilde{Q}_i$ is generated by $\tilde{f}_A(x) = f_{-A}(x)$. Hence $\tilde{Q}_i = Q_i$ iff $A = -A$. This holds for all $A \in \mathbb{F}_p^{\times}/\langle 2 \rangle$ iff $-1 \in \langle 2 \rangle$, which can be guaranteed when 2 is a nonquadratic-residue since in such a case $2^{(p-1)/2} = -1$ (mod p). ∎

Definition 3.2: If F is a field, by $F^{\times}$ we mean the multiplicative group of F. More generally, if A is a commutative ring with identity, $A^{\times}$ will denote the multiplicative group of the units of A.

Theorem 3.3: Let $R = \mathbb{F}_2[D_m]$, where D_m is the dihedral group, and m is odd. Assume further that (6) holds. Then, the ring R decomposes into a direct sum of two-sided ideals as

$$R = \oplus_{i=0}^{s} R_i,$$

where the structure of the R_i is as follows.

1) $\dim_{\mathbb{F}_2} R_0 = 2$. The ideals of R_0 are $(0) \subset J_0 \subset R_0$ (J_0 is two-sided), where

$$J_0 = \left(\sum_{g \in D_m} g\right) = \left\{0, \sum_{g \in D_m} g\right\}$$
and
$$R_0 = \left(\sum_{g \in N} g\right) = \left\{0, \sum_{g \in N} g, \alpha \sum_{g \in N} g, \sum_{g \in D_m} g\right\}.$$

2) For $i = 1, \ldots, s$, we have

$$R_i = Q_i \oplus \alpha Q_i.$$

Each such R_i is simple as a ring and isomorphic as a ring to $M_2(\mathbb{F}_{2^{l_i/2}})$, where $l_i = \dim_{\mathbb{F}_2} Q_i$. Moreover, R_i contains $2^{l_i/2} + 1$ nonzero irreducible left ideal all isomorphic and each of dimension l_i. They are given by

$$I_{[b]}^i = Q_i(1+\alpha)b = \{q(1+\alpha)b | q \in Q_i\}, \text{for}[b] \in Q_i^{\times}/Z_i^{\times}$$

where $Z_i = \{q \in Q_i | q = \tilde{q}\}$ is a subfield of Q_i.

Note that $(\sum_{g \in D_m} g)^2 = |D_m| \sum_{g \in D_m} g = 0$ because $|D_m|$ is even. Hence, $J_0^2 = (0)$ and, consequently, R_0 is not semisimple. In fact it is not difficult to show that J_0 is the radical of R.

Proof: The representations of D_m are essentially similar to the semisimple case corresponding to the situation when instead of $\mathbb{F}_2$ we have a field F whose characteristic does not divide the order of D_m (see, for instance, [1] and [4]). We need, however, to worry about the fact that the ring is not semisimple and furthermore we need to list all the irreducible left ideals. This is not hard since the group is simple to analyze.

Each R_i is a two-sided ideal since $qR_i = R_i q = R_i$ for each $q \in Q$, and $\alpha R_i = R_i \alpha = R_i$. The claimed structure will essentially follow once we show that for all $i \neq 0$, we have the following:

1) R_i contains no other two-sided ideal, and is thus simple as a ring;
2)
   a) each $I_{[b]}^i$ is an irreducible left ideal;
   b) $I_{[b_1]}^i \neq I_{[b_2]}^i$ iff $[b_1] \neq [b_2]$;
   c) any nonzero left ideal in R_i must contain one of the $I_{[b]}^i$.

To see why it is enough to establish 1) and 2), note first that the fact that R_i is simple implies that all the nonzero irreducible left ideals of R_i are isomorphic and that R_i is isomorphic to $M_d(K)$ for some finite field K, where d is such that $R_i = \oplus_{j=1}^{d} R_{i,j}$ and the $R_{i,j}$ are irreducible (the decomposition is not unique unless $d = 1$). Combining this with 2), which says that each $I_{[b]}^{i}$ is irreducible, we see by dimensional considerations ($\dim_{\mathbb{F}_2} I_{[b]}^{i} = \dim_{\mathbb{F}_2} Q_i = l_i$ and $\dim_{\mathbb{F}_2} R_i = \dim_{\mathbb{F}_2} Q_i + \dim_{\mathbb{F}_2} \alpha Q_i = 2l_i$) that $d = 2$, and hence $|K| = 2^{\frac{1}{4}\dim_{\mathbb{F}_2} R_i} = 2^{l_i/2}$.

The claimed number of nonzero irreducible left ideals then follows from the fact that, in general, the number of nonzero irreducible left ideals in $M_2(K)$ is $|K| + 1$. To see why this is true, let $\mathcal{I}$ be the set of principal left ideals I of $M_2(K)$ that are not equal to 0 or $M_2(K)$. We will argue below that $\dim_K I = 2$ for all ideals I in $\mathcal{I}$. By dimensional consideration, this implies that any ideal in $\mathcal{I}$ must be irreducible, and the ideals in $\mathcal{I}$ are the only irreducible left ideals. The intersection of two ideals in $\mathcal{I}$ must be the zero ideal because they are irreducible. Moreover, the ideals in $\mathcal{I}$ are generated by rank-one matrices (since $I \neq (0), M_2(K)$ for all $I \in \mathcal{I}$), i.e., elements of $M_2(K) \backslash (\mathrm{GL}_2(K) \cup \{0\})$. Thus, $\cup_{I \in \mathcal{I}} (I \backslash \{0\})$ is a disjoint union equal to $M_2(K) \backslash (\mathrm{GL}_2(K) \cup \{0\})$. It follows that

$$\begin{aligned}
|\mathcal{I}| &= \frac{|\cup_{I \in \mathcal{I}} (I \backslash \{0\})|}{|I \backslash \{0\}|} \\
&= \frac{|M_2(K) \backslash (\mathrm{GL}_2(K) \cup \{0\})|}{|K|^2 - 1} \\
&= \frac{|M_2(K)| - 1 - |\mathrm{GL}_2(K)|}{|K|^2 - 1} \\
&= \frac{|K|^4 - 1 - |K|(|K| - 1)^2(|K| + 1)}{|K|^2 - 1} \\
&= |K|^2 + 1 - |K|(|K| - 1) = |K| + 1.
\end{aligned}$$

We still have to show that $\dim_K I = 2$ for all ideals I in $\mathcal{I}$. Let $I \in \mathcal{I}$. Since $I \neq 0$ or $M_2(K), I$ must be generated by a some rank-one matrix A. Decompose A as $A = B\left(\begin{smallmatrix} \alpha & \beta \\ 0 & 0 \end{smallmatrix}\right)C$, where $\alpha \neq 0$, and B and C are invertible matrices. Thus

$$\begin{aligned}
I = M_2(K)A &= M_2(K)B \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \\
C &= M_2(K) \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \\
C &= M_2(K) \begin{pmatrix} 1 & \beta \\ 0 & 0 \end{pmatrix} C.
\end{aligned}$$

It follows that

$$I = \left\{ \begin{pmatrix} a & a\beta \\ c & c\beta \end{pmatrix} C : a, c \in K \right\}.$$

Therefore, $\dim_K I = 2$.

Proof of 1): Let $r = r_1 + \alpha r_2$, where $r_1, r_2 \in Q_i$, be a nonzero element of R_i, and consider the two-sided ideal I generated by r. It is enough to show that $R_i \subset I$ (and hence $R_i = I$).

First, we show that I must contains an element $q = q_1 + \alpha q_2$, where $q_1, q_2 \in Q_i, q_1 \neq 0$, and $q_1 \neq q_2$. If $r_1 = 0$, use $q = \alpha r$. If $r = r_1 + \alpha r_1$, try $q = gr$ for $g \in N$. Thus, $gr = gr_1 + \alpha g^{-1} r_1$. Assume, for the sake of contradiction, that $gr_1 = g^{-1} r_1$, for all g in N. Hence, $g^2 r_1 = r_1$, for all g in N. Since the square map $N \rightarrow N, x \mapsto x^2$ is subjective (because m is odd), we get $gr_1 = r_1$, for all g in N. This can only happen if $r_1 = \sum_{g \in N} g$. However, then $r_1 \in Q_0$, which is not true.

Thus

$$\begin{aligned}
q + \alpha q q_1^{-1} q_2 &= (q_1 + \alpha q_2) + \left(\alpha q_2 + q_1^{-1} q_2^2\right) \\
&= q_1 + q_1^{-1} q_2^2 = q_1^{-1} \left(q_1^2 + q_2^2\right)
\end{aligned}$$

is a nonzero element Q_i inside I, where inversion is in Q_i as a field. Note that $q_1^{-1}(q_1^2 + q_2^2) \neq 0$ since $q_1 \neq q_2$ and the characteristic of Q_i is 2. Consequently, I contains Q_i, and hence R_i, since the two-sided ideal generated by Q_i is R_i.

Proof of 2):

a) We have $\alpha q(1 + \alpha) = \tilde{q}(1 + \alpha)$, for all $q \in Q$. Thus, $\alpha Q_i (1 + \alpha) b = \tilde{Q}_i (1 + \alpha) = Q_i (1 + \alpha) b$, and $q Q_i (1 + \alpha) b = Q_i (1 + \alpha) b$ for all $q \in Q$, and hence $I_{[b]}^{i}$ is a left ideal. $I_{[b]}^{i}$ is an irreducible left ideal of R since Q_i is an irreducible ideal of Q and $I_{[b]}^{i} = Q_i (1 + \alpha) b$.

b) Let $b \in Q_i^{\times}$. The left ideal $I_{[b]}^{i}$ is generated by $(1 + \alpha) b$ since $(1 + \alpha) b = e_i (1 + \alpha) b$, where e_i is the identity element of the field Q_i. Let $b_1, b_2 \in Q_i^{\times}$. Thus, $I_{[b_1]}^{i} = I_{[b_2]}^{i}$ iff there exists $q \in Q_i^{\times}$ such that $q(1 + \alpha) b_1 = (1 + \alpha) b_2$, i.e., $b_2 = q b_1$ and $b_2 = \tilde{q} b_1$. Combining both equalities, we get $q b_1 = \tilde{q} b_1$. Multiplying by the multiplicative inverse of b_1 in Q_i, we obtain $q = \tilde{q}$. Hence $I_{[b_1]}^{i} = I_{[b_2]}^{i}$ iff there exists $q \in Z_i^{\times}$ such that $b_2 = q b_1$, which is equivalent to saying that $[b_1] = [b_2]$.

c) If I is a nonzero left ideal in Q_i, let $r = b_1 + \alpha b_2$ be any nonzero element of I, where $b_1, b_2 \in Q_i$ are not both zero. If $b_1 = b_2$, i.e., $r = (1+\alpha) b_1$, then $I_{[b_1]} = Q_i (1+\alpha) b_1 = Q_i r \subset I$. If $b_1 \neq b_2$, consider the element $r' = r + \alpha r$ of I. Since $r' = b_1 + \alpha b_2 + \alpha b_1 + b_2 = (1 + \alpha)(b_1 + b_2)$, we get that $I_{[b_1 + b_2]} = Q_i (1 + \alpha)(b_1 + b_2) = Q_i r' \subset I$ (note that $b_1 + b_2 \neq 0$ since $b_1 \neq b_2$).

This completes the proof of Theorem 3.3. ■

Now, we know all the left ideals I of R. They are direct sums of the form $I = \oplus_{i=0}^{n} I^i$, where each I^i is either 0, R_i, one of the $I_{[b]}^{i}$ if $i \neq 0$, or J_0 if $i = 0$.

Theorem 3.4: Let m be an odd integer, and consider the dihedral group D_m. Assume further that (6) holds. Let $R = \mathbb{F}_2[D_m]$, and consider the unique decomposition

$$R = \oplus_{i=0}^{s} R_i,$$

of R into two-sided ideals as in Theorem 3.3.

Consider the following randomized code construction: generate a rate-$(\frac{1}{2} - \frac{1}{2m})$ random left ideal I of $\mathbb{F}_2[D_m]$ as

$$I = \oplus_{i=1}^{s} I^i$$

where each I^i is selected uniformly at random from one of the $2^{l_i/2} - 1$ nonzero irreducible left ideals of R_i.

If $\delta > 0$ is such that $h(\delta) \leq \frac{1}{4} - \frac{\log m}{2l(m)}$, then the probability that the minimum relative distance of I is below δ is at most $2^{-2l(m)(1/4-h(\delta))+5\log m}$, where h is the binary entropy function.

Moreover, there are infinitely many such m such that (6) holds and $l(m)$ grows asymptotically faster than $\log m$, for instance for almost all the primes $p = \pm 5 \pmod 8$.

Therefore, there are infinitely many integers m such that the left ideal I of $\mathbb{F}_2[D_m]$ is an asymptotically good rate $1/2$ binary code with a high probability.

Proof: First, recall that since Q is a direct sum of ideals $Q = \oplus_i Q_i$, each element q of Q has a unique decomposition $q = \sum_i q_i$, where $q_i \in Q_i$. Recall also that since the decomposition is into two sided ideals, we have $Q_iQ_j = (0)$ for all $i \neq j$ (because $Q_iQ_j \subset Q_i \cap Q_j = (0)$). Thus if q decomposes as $q = \sum_i q_i$ and q' as $q' = \sum_i q'_i$, we have $qq' = \sum_i q_iq'_i$. Finally, recall that each Q_i is a field being a simple commutative ring.

Let $Q^* = \oplus_{i=1}^s Q_i$, and let $Q^{*\times}$ be the multiplicative group of units of of Q^*. Thus

$$Q^{*\times} = \left\{ \sum_{i=1}^{s} q_i : q_i \in Q_i^\times \right\}$$

where $Q_i^\times$ is the multiplicative subgroup of the field Q_i. Note that $(\sum_{i=1}^s q_i)^{-1} = \sum_{i=1}^s q_i^{-1}$, where q_i^{-1} is the multiplicative inverse of q_i in the field Q_i. Finally, let T be the subgroup of $Q^{*\times}$ given by $T = \{q \in Q^{*\times} | q = \tilde{q}\}$.

Similarly, since R is a direct sum of ideals $R = \oplus_i R_i$, each element r of R has a unique decomposition $r = \sum_i r_i$, where $r_i \in R_i$. Moreover, since the decomposition is into two sided ideals, we have $R_iR_j = (0)$ for all $i \neq j$. Thus if r decomposes as $r = \sum_i r_i$ and r' as $r' = \sum_i r'_i$, we have $rr' = \sum_i r_ir'_i$.

Therefore, the above randomized construction is equivalent to the following: pick a random left ideal

$$I_{[b]} = Q(1+\alpha)b = Q^*(1+\alpha)b = \{q(1+\alpha)b | q \in Q^*\}$$

where $[b]$ is selected uniformly at random from $Q^{*\times}/T$. From Section II, we know that there are infinitely many m with $l(m) \gg \log m$, and they contain specifically almost all the primes. Combining with Lemma 3.1, we get that there are infinitely many such m such that (6) holds and $l(m)$ grows asymptotically faster than $\log m$, for instance almost all the primes $p = \pm 5 \pmod 8$.

To establish the minimum distance bound, we follow the argument in Theorem 2.1. We will use the structure of the dihedral group representations from Theorem 3.3 at the end in (9), (10), and (11).

Observe the relation between this randomized construction and the rate-half randomized construction in that Theorem 2.1. This ensemble of codes is, in a suitable sense, a subfamily of that ensemble.

Since $Q^{*\times}$ is a group, $Q^{*\times} = aQ^{*\times}$ for all a in $Q^{*\times}$. Thus

$$I_{[b]} = Q^*(1+\alpha)b = aQ^*(1+\alpha)b$$

for all a in $Q^{*\times}$. Hence, the probability P that the minimum distance of $I_{[b]}$ is below $2\delta m$ when $[b]$ is selected uniformly at random from $Q^{*\times}/T$, is the same as the probability that $aQ^*(1+\alpha)b$ has a minimum distance below $2\delta m$, when a and b are selected uniformly at random from $Q^{*\times}$.

Now we proceed as in Theorem 2.1. P is the probability that there is an $f \in Q^*, f \neq 0$, such that $0 \leq w(af(1+\alpha)b) < 2m\delta$. Thus, P is at most

$$\sum_{f \in Q^*; f \neq 0} Pr_{a,b \in Q^{*\times}}[0 \leq w(af(1+\alpha)b) < 2m\delta]$$

and this is at most

$$\sum_{l=l(m)}^{m} |D_l^*| \max_{f \in D_l^*} \Pr_{a,b \in Q^{*\times}}[0 \leq w(af(1+\alpha)b) < 2m\delta]$$

where $D_l^* = D_l \cap Q^*$, and $D_l = \{f \in Q | \dim_{\mathbb{F}_2} fQ = l\}$. As before, we have

$$|D_l^*| \leq |D_l| \leq 2^l |\Omega_l|$$

where Ω_l is the set of left ideals in Q of dimension l.

Consider any l, and any $f \in D_l^*$. We have

$$Pr_{a,b \in Q^{*\times}}[0 \leq w(af(1+\alpha)b) < 2m\delta] = \sum_{r \in U \text{s.t. } 0 \leq w(r) < 2m\delta} \Pr_{a,b \in Q^{*\times}}[af(1+\alpha)b = r]$$

where

$$U = Q^{*\times} f(1+\alpha) Q^{*\times}$$

and this is at most

$$\max_{r \in U} Pr_{a,b \in Q^{*\times}}[fa(1+\alpha)b = r] \times \sum_{w_1,w_2 \geq 0; w_1+w_2 < 2\delta m} |I^{(w_1)}||I^{(w_2)}|$$

where $I = fQ$, and $I^{(v)}$ is the set of elements in I of weight v. Fix $l \geq l(m)$, any f in D_l^*, and any r in U. We will argue at the end that

$$\Pr_{a,b \in Q^{*\times}}[fa(1+\alpha)b = r] \leq 2^{-3l/2}. \tag{7}$$

We have from Lemmas 2.2 and Lemma 2.3 that $|\Omega_l| \leq m^{l/l(m)+1}, |I^{(w_1)}| \leq 2^{lh(w_1/m)}$, and $|I^{(w_2)}| \leq 2^{lh(w_2/m)}$. Thus, modulo (7), we are done since by arguing as in Theorem 2.1, we get

$$\begin{aligned} P &\leq \sum_{l=l(m)}^{m} 2^l m^{l/l(m)+1} 2^{-3l/2} \\ &\quad \times \sum_{w_1,w_2 \geq 0; w_1+w_2 < 2\delta m} 2^{l(h(w_1/m)+h(w_2/m))} \\ &\leq \sum_{l=l(m)}^{m} 2^{-l/2} m^{l/l(m)+1} (2\delta m)^2 2^{2lh(\delta)} (\text{since h is convex}) \\ &\leq 2^{-2l(m)(\frac{1}{4}-h(\delta))+5\log m} \end{aligned}$$

where the last bound holds when $\frac{1}{4} - h(\delta) - \frac{\log m}{2l(m)} \geq 0$. The difference is that now we have $1/4$ instead of $1/2$. The reason is that before we had 2^{-2l} instead of $2^{-3l/2}$.

We still have to establish (7). The first thing to note is that when a and b are selected uniformly at random from $Q^{*\times}$, each $r \in U$ is equally likely to occur as $fa(1+\alpha)b$. The reason is that if $r = a'f(1+\alpha)b'$, where $a', b' \in Q^{*\times}$, then the event $af(1+\alpha)b = r = a'f(1+\alpha)b'$ can be expressed as

$$a''af(1+\alpha)b''b = e^*f(1+\alpha)e^* = f(1+\alpha)$$

where a'' (respectively, b'') is the inverse of a' (respectively, b') in the multiplicative group $Q^{*\times}$, and where e^* is the identity element of group $Q^{*\times}$ which acts also as an identity element for the ring Q^* ($e^* = \sum_i e_i$, where each e_i is the identity element of the field Q_i. Thus if $f = \sum_i f_i$, where $f_i \in Q_i$, we have $fe^* = \sum_i f_i e_i = \sum_i f_i = f$). Therefore

$$\begin{aligned}\Pr_{a,b \in Q^{*\times}}[fa(1+\alpha)b = r] &= \Pr_{a,b \in Q^{*\times}}[a''af(1+\alpha)b''b \\ &= f(1+\alpha)] \\ &= \Pr_{a,b \in Q^{*\times}}[af(1+\alpha)b = f(1+\alpha)]\end{aligned}$$

since $a''Q^{*\times} = Q^*$ and $b''Q^{*\times} = Q^*$. Since this is independent of choice of $r \in U$, we get

$$\Pr_{a,b \in Q^{*\times}}[fa(1+\alpha)b = r] = \frac{1}{|U|}. \tag{8}$$

Decompose f uniquely as $f = \sum_{i=1}^{s} f_i$, where each $f_i \in Q_i$, and let S be the set of i such that $f_i \neq 0$, thus $l = \sum_{i \in S} l_i$. We can express U as

$$\begin{aligned}U &= Q^{*\times} f(1+\alpha)Q^{*\times} \\ &= \left\{\sum_{i \in S} u_i | u_i \in Q_i^\times f_i(1+\alpha)Q_i^\times\right\} \\ &= \left\{\sum_{i \in S} u_i | u_i \in Q_i^\times(1+\alpha)Q_i^\times\right\}\end{aligned}$$

since, for $i \in S$, we have $f_i Q_i^\times = Q_i^\times$ because f_i is invertible being a nonzero element of the field Q_i. Now

$$\begin{aligned}Q_i^\times(1+\alpha)Q_i^\times &= \bigcup_{b \in Q_i^\times} Q_i^\times(1+\alpha)b \\ &= \bigcup_{b \in Q_i^\times} (Q_i(1+\alpha)b \backslash \{0\}) \\ &= \bigcup_{b \in Q_i^\times} I_{[b]}^i \backslash \{0\}\end{aligned}$$

where we have used in the second equality the fact that $Q_i^\times$ is a group (hence $q_i b \neq 0$ for all $q_i, b \in Q_i^\times$) and the fact that˜is an automorphism of $Q_i^\times$ (hence $\tilde{b} \neq 0$ for all $b \in Q_i^\times$).

We know from Theorem 3.3 that $I_{[b_1]}^i \neq I_{[b_2]}^i$ iff $[b_1] \neq [b_2]$ as elements of $Q_i^\times / Z_i^\times$. Thus

$$Q_i^\times(1+\alpha)Q_i^\times = \bigcup_{[b] \in Q_i^\times / Z_i^\times} I_{[b]}^i \backslash \{0\}. \tag{9}$$

From Theorem 3.3, the $I_{[b]}^i$ are nonzero irreducible left ideals of R_i. Since the intersection of two left ideals is a left ideal, the above union is a disjoint union. Hence

$$|Q_i^\times(1+\alpha)Q_i^\times| = \sum_{[b] \in Q_i^\times / Z_i^\times} |I_{[b]}^i \backslash \{0\}|. \tag{10}$$

Using Theorem 3.3 again, we obtain

$$|Q_i^\times(1+\alpha)Q_i^\times| = (2^{l_i/2}+1)(2^{l_i}-1). \tag{11}$$

Hence

$$|U| = \prod_{i \in S} |Q_i^\times(1+\alpha)Q_i^\times| = \prod_{i \in S}(2^{l_i/2}+1)(2^{l_i}-1).$$

Noting that

$$(2^{l_i/2}+1)(2^{l_i}-1) = 2^{3l_i/2} + 2^{l_i} - 2^{l_i/2} - 1 \geq 2^{3l_i/2},$$

since $l_i \geq 2$ (l_i is divisible by 2), we obtain

$$|U| \geq 2^{3/2 \sum_{i \in S} l_i} = 2^{3l/2},$$

and hence (7) via (8).

This completes the proof of Theorem 3.4. ■

It is important to note that the $h^{-1}(1/4)$ bound we obtained on the minimum relative distance is unlikely to be tight. We ended up with this bound because our argument is based on counting, and the construction does not have enough randomness so that a counting argument can go up to the GV bound, i.e., up to $h^{-1}(1/2)$.

IV. Conclusion

We studied two randomized constructions of binary linear codes that are invariant under the action of some group on the bits of the codewords: a randomized Abelian construction based on the action of an Abelian group on a number of disjoint copies of itself, and a non-Abelian randomized construction corresponding the action of the dihedral group on a single copy of itself. We argued that both ensembles of codes are asymptotically good.

Acknowledgment

The authors would like to thank D. Spielman and M. Sudan for very helpful discussions on this material.

References

[1] M. Burrow, *Representation Theory of Finite Groups*. New York: Academic Press, 1965.

[2] C. L. Chen, W. W. Peterson, and E. J. Weldon Jr., "Some results on quasi-cyclic codes," *Inf. Control*, vol. 15, no. 5, pp. 407–423, Nov. 1969.

[3] V. Chepyzhov, "New lower bounds for minimum distance of linear quasi-cyclic and almost linear cyclic codes," *Probl. Peredachi Inf.*, vol. 28, pp. 33–44, Jan. 1992.

[4] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*. New York: Wiley Interscience, 1962.

[5] T. Kasami, "A gilbert-varshamov bound for quasi-cyclic codes of rate $1/2$," *IEEE Trans. Inf. Theory* , vol. IT-20, p. 679, 1974.

[6] R. Lidl and H. Niederreiter, *Finite Fields. Number 20 in Encyclopedia of Mathematics and its Applications*. Reading, MA: Addison-Wesley, 1983.

[7] x. Lint and J. H. van, *Introduction to Coding Theory*, ser. Graduate texts in mathematics. New York: Springer, 1999.

[8] G. A. Margulis, "Explicit group theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators," *Problems Inf. Transmission*, vol. 24, no. 1, pp. 39–46, Jul. 1988.

[9] McDonald and R. Bernard, *Finite Rings With Identity*. New York: Marcel Dekker, 1974.

[10] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

[11] F. J. MacWilliams, "Codes and ideals in group algebras," in *Combinatorial Mathematics and Its Applications*, R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC: Univ. of North Carolina Press, 1969, pp. 317–328.

[12] J. F. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1992.

[13] P. H. Piret, "An upper bound on the weight distribution of some codes," *IEEE Inf. Theory*, vol. 31, no. 4, pp. 520–521, 1985.

[14] V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds., *Handbook of Coding Theory*. New York: Elsevier, 1998.

[15] I. E. Shparlinsky, "On weight enumerators of some codes," *Probl. Peredechi Inf.*, vol. 22, no. 2, pp. 43–48, 1986.

[16] M. Sipser and D. Spielman, "Expander codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1710–1722, 1996.

[17] H. N. Ward, "Quadratic residue codes and symplectic groups," *J. Algebra*, vol. 29, pp. 150–171, 1974.