GROUP CODES OVER FIELDS ARE ASYMPTOTICALLY GOOD

MARTINO BORELLO AND WOLFGANG WILLEMS

Keywords. Group algebra, group code, asymptotically good, p-ary entropy function, weight distribution
MSC classification. 94A17, 94B05, 20C05

Abstract. Group codes are right or left ideals in a group algebra of a finite group over a finite field. Following ideas of Bazzi and Mitter on group codes over the binary field [3], we prove that group codes over finite fields of any characteristic are asymptotically good. On the way we extend a result of Massey on the fractional weight of distinct binary n-tuples [13] and a result of Piret on an upper bound on the weight distribution of a binary code [16] to any finite field.

1. Introduction

Let $\mathbb{F}$ be a finite field of characteristic p and let G be a finite group. By a *group code* or, more precisely, a G*-code* we denote a right or left ideal in the group algebra $\mathbb{F}G$. Many interesting linear codes are group codes. For example, cyclic codes of length n are group codes for a cyclic group C_n; Reed-Muller codes are group codes for an elementary abelian p-group [4, 7]; the binary extended self-dual $[24, 12, 8]$ Golay code is a group code for the symmetric group S_4 on 4 letters [5] and the dihedral group D_{24} of order 24 [14]. Many best known codes are group codes as well. For instance, $\mathbb{F}_5(C_6 \times C_6)$ contains a $[32, 28, 6]$ and $\mathbb{F}_5(C_{12} \times C_6)$ a $[72, 62, 6]$ group code [12]. Both codes improved earlier examples in Grassl's list [10].

Already in 1965, Assmus, Mattson and Tyrun [2] asked the question whether the class of cyclic codes, i.e., the class of group codes over cyclic groups, is asymptotically good. The answer is still open. In [3], Bazzi and Mitter proved that the class of group codes over the binary field is asymptotically good. Using the trivial fact that by field extensions neither the dimension nor the minimum distance changes, group codes are asymptotically good in characteristic 2. In this note we use the ideas of Bazzi and Mitter to prove in the last section our main result.

Theorem. Group codes over fields are asymptotically good in any characteristic.

Following the lines of [3], we need to generalize results of Massey [13] and Piret [16] to characteristic p, which we do in section 2 and 3. These results are of interest in their own right. Section 4, in which we analyze the structure of a particular group algebra, heavily depends on methods from representation theory. For the background we refer the reader to [1] and Chapter VII of [11].

M. Borello is with LAGA, UMR 7539, CNRS, Université Paris 13 - Sorbonne Paris Cité, Université Paris 8, F-93526, Saint-Denis, France.

W. Willems is with Otto-von-Guericke Universität, Magdeburg, Germany, and Universidad del Norte, Barranquilla, Colombia.

2. On the fractional weight of distinct p-ary regular k-tuples

In this section we extend a result of Massey [13] about the fractional weight of distinct binary k-tuples to an arbitrary finite field $\mathbb{F}_p$ (here p is a prime power). To do so, we need to add an hypothesis of regularity on the set of k-tuples, which is automatically satisfied if $p = 2$.

Let M be a set of distinct k-tuples with entries in $\mathbb{F}_p$. Furthermore, let $\mathfrak{p}$ be the fraction of the Mk positions of k-tuples in M which contain an element different from 0, and let $\mathfrak{p}_i$ be the fraction of those k-tuples whose i-th component is an element different from 0. Clearly,

$$\mathfrak{p} = \frac{\mathfrak{p}_1 + \cdots + \mathfrak{p}_k}{k}.$$

Let $X = X_1 \cdots X_k$ be a random variable which takes on each of the M given distinct k-tuples values with probability $\frac{1}{M}$. Then the entropy of this random k-tuple is

$$H(X_1 \cdots X_k) = \log_2(M).$$

By ([17], 1.2.6), we have

$$H(X_1 \cdots X_k) \le H(X_1) + \cdots + H(X_k).$$

Let $\mathbb{F}_p = \{\alpha_0, \alpha_1, \dots, \alpha_{p-1}\}$ with $\alpha_0 = 0$. For $j \in \{0, \dots, p-1\}$, let us call $\mathfrak{p}_{i,j}$ the fraction of those k-tuples whose i-th component is equal to j, so that

$$\mathfrak{p}_i = \mathfrak{p}_{i,1} + \cdots + \mathfrak{p}_{i,p-1}.$$

Finally, we define $\mathfrak{p}_{\#j}$ by

$$\mathfrak{p}_{\#j} := \frac{1}{k} \cdot \sum_{i=1}^{k} \mathfrak{p}_{i,j}.$$

Definition 2.1. *The set M is called* regular *if $\mathfrak{p}_{i,1} = \mathfrak{p}_{i,2} = \cdots = \mathfrak{p}_{i,p-1}$ for all $i \in \{1, \dots k\}$.*

Remark 2.2. If the k-tuples in M form a linear code, then obviously M is regular. Actually, we even can relax the hypothesis of linearity: it is enough to assume that the set of k-tuples in M is stable under multiplication by elements in $\mathbb{F}_p^\times$.

Suppose now that M is regular. Then

$$\mathfrak{p}_{i,1} = \mathfrak{p}_{i,2} = \cdots = \mathfrak{p}_{i,p-1} = \frac{\mathfrak{p}_i}{p-1} \quad \text{and} \quad \mathfrak{p}_{\#1} = \mathfrak{p}_{\#2} = \cdots = \mathfrak{p}_{\#(p-1)} = \frac{\mathfrak{p}}{p-1}.$$

Note also that $\mathfrak{p}_{i,0} = 1 - \mathfrak{p}_i$ and $\mathfrak{p}_{\#0} = 1 - \mathfrak{p}$.
Because of our probabilistic assignment

$$H(X_i) = -\sum_{j=0}^{p-1} \mathfrak{p}_{i,j} \log_2(\mathfrak{p}_{i,j}) = -(1-\mathfrak{p}_i)\log_2(1-\mathfrak{p}_i) - \mathfrak{p}_i \log_2\left(\frac{\mathfrak{p}_i}{p-1}\right)$$

we get

$$H(X_i) = \log_2(p) \cdot h_p(\mathfrak{p}_i),$$

where $h_p(x) = -(1-x)\log_p(1-x) - x\log_p\left(\frac{x}{p-1}\right)$ is the p-ary entropy function. Thus

$$\log_p(M) \le \sum_{i=1}^{k} h_p(\mathfrak{p}_i),$$

and due to the convexity of $h_p(x)$ ([17], Theorem 1.2.9), we have

$$k \cdot \sum_{i=1}^{k} \frac{1}{k} h_p(\mathfrak{p}_i) \le k \cdot h_p\left(\frac{1}{k}\sum_{i=1}^{k} \mathfrak{p}_i\right) = h_p(\mathfrak{p}).$$

It follows

$$\log_p(M) \le k \cdot h_p(\mathfrak{p}).$$

Thus we have proved the following p-ary version of ([13], Theorem).

Theorem 2.3. *Let M be a regular set of distinct k-tuples of elements of $\mathbb{F}_p$. The fraction $\mathfrak{p}$ of elements different from zero in the Mk positions of the k-tuples in M satisfies*

$$h_p(\mathfrak{p}) \geq \frac{1}{k} \cdot \log_p(M),$$

where $h_p(x) = -(1-x)\log_p(1-x) - x\log_p\left(\frac{x}{p-1}\right)$.

We would like to mention here that the bound is sharp. For instance, we may take the vector space $\mathbb{F}_p^k$ for M.

3. An upper bound on the weight distribution of some linear p-ary codes

Let C be an $[n,k]_p$ code (here p is a prime power). Recall that

$$I = \{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$$

of size k is called an information set for C if the restriction of I to these positions leads to all vectors in $\mathbb{F}_p^k$. Now let $I(C)$ denote the set of all information sets. To $I(C)$ we associate a matrix $M(I(C))$ with n columns and $\#I(C)$ rows in the following way. Each row has a 0 outside the corresponding information set and a 1 inside. We are interested in codes C for which the matrix $M(I(C))$ contains a submatrix $M(U(C))$, corresponding to a subset $U(C)$ of $I(C)$ and having a constant number $r \geq 1$ of 1's in each of its n columns. If a subset $U(C)$ of $I(C)$ has this property, we say that C has a *balanced* set of information k-tuples. By counting the 1's, we immediately see that

$$\#U(C)k = rn.$$

Furthermore, for $w \in \{0, \dots, n\}$, let $A_w(C) := \#\{c \in C \mid \mathrm{wt}(c) = w\}$ denote the number of code words of weight w in C. Finally, for $\mathbf{i} \in I(C)$, we define $W(\mathbf{i}, w)$ by

$$W(\mathbf{i}, w) = \sum_{c \in C, \mathrm{wt(c)=w}} \mathrm{wt}(\pi_{\mathbf{i}}(\mathrm{c})),$$

where $\pi_{\mathbf{i}} : \mathbb{F}_p^n \to \mathbb{F}_p^k$ denotes the projection to the coordinates in $\mathbf{i}$.

Let $M := \{\pi_{\mathbf{i}}(c) \mid c \in C, \mathrm{wt}(c) = w\}$. This is a set of $A_w(C)$ distinct k-tuples over $\mathbb{F}_p$ and it is regular, since C is linear, so that the k-tuples in M are stable under multiplication by elements in $\mathbb{F}_p^\times$. Clearly, the fraction of the Mk positions of these k-tuples which contain an element different from 0 is $W(\mathbf{i}, w)/kA_w(C)$. Thus, by Theorem 2.3, we have

$$h_p(W(\mathbf{i}, w)/kA_w(C)) \geq \frac{1}{k} \cdot \log_p(A_w(C)).$$

With this we obtain the p-ary version of Piret's result ([16], Theorem 2).

Theorem 3.1. *Let C be an $[n,k]_p$ code admitting a balanced set $U(C)$ of information k-tuples. Then*

$$A_w(C) \leq p^{k \cdot h_p(w/n)}$$

for all $0 \leq w \leq \frac{p-1}{p} \cdot n$.

Proof. Recall that for $x = \frac{p-1}{p}$ the function $h_p(x)$ has its maximum value. Assume that

$$\frac{1}{k} \cdot \log_p(A_w(C)) > h_p(w/n),$$

hence

$$h_p(W(\mathbf{i}, w)/kA_w(C)) > h_p(w/n).$$

For $w \le \frac{p-1}{p} \cdot n$ this implies

$$W(\mathbf{i}, w) > kwA_w(C)/n$$

for all information sets $\mathbf{i}$.

Next we estimate

$$\sigma := \sum_{\mathbf{i} \in U(C)} W(\mathbf{i}, w)$$

in two different ways. By the result above,

$$\sigma > \#U(C)kwA_w(C)/n.$$

On the other hand, since any coordinate is counted r times in σ, we also obtain

$$\sigma = rwA_w(C).$$

Thus $r > \#U(C)k/n$, which contradicts the equality $\#U(C)k = rn$. □

Remark 3.2. Note that group codes always admit balanced sets of information tuples. This can be seen as follows. Let $C \le \mathbb{F}_pG$ be a group code and let $S \subseteq G$ be an information set of C. Then $\{Sg\}_{g \in G}$ are information sets as well, because C is invariant under the action of G. Moreover, for all $h \in G$, the number of Sg which contain h is exactly $\#S = \dim C$.

4. The structure of the group algebra $\mathbb{F}_pG_{p,q}$

Let $p \neq 2$ be a fixed prime and let q be a prime such that p divides $q-1$ (there are infinitely many such q, by Dirichlet's Theorem). Note that $q \neq 2$ and let

$$G_{p,q} := \langle \alpha, \beta \mid \alpha^p = \beta^q = 1, \alpha\beta = \beta^{\frac{q-1}{p}}\alpha \rangle = \langle \beta \rangle \rtimes \langle \alpha \rangle. \tag{1}$$

Furthermore, we put $N := \langle \beta \rangle$ and $Q := \mathbb{F}_pN$. Any element r of $\mathbb{F}_pG_{p,q}$ can be written uniquely as

$$r = r_0 + \alpha r_1 + \cdots + \alpha^{p-1} r_{p-1}$$

with $r_0, \ldots, r_{p-1} \in Q$. If $a = \sum_{i=0}^{q-1} a_i \beta^i$ (with $a_i \in \mathbb{F}_p$) is an element of Q, we define $\hat{a}$ by

$$\hat{a} := \sum_{i=0}^{q-1} a_i \beta^{i \cdot \frac{q-1}{p}}$$

Clearly, the map $\hat{\ }: Q \to Q$ is an $\mathbb{F}_p$-algebra automorphism. From the relation $\alpha\beta = \beta^{\frac{q-1}{p}}\alpha$ we get $\alpha\beta^i = \beta^{i \cdot \frac{q-1}{p}}\alpha$ for all $i \in \{0, \ldots, q-1\}$, so that

$$\alpha a = \hat{a}\alpha$$

for all $a \in Q$.

Now we realize Q as $\mathbb{F}_p[x]/\langle x^q - 1 \rangle$. Since Q is a semisimple algebra by Maschke's Theorem ([1], p. 116), we have, due to Wedderburn's Theorem ([1], Chap. 5, Sect. 13, Theorem 16), a unique decomposition

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

into 2-sided ideals Q_i, where each Q_i is a simple algebra over $\mathbb{F}_p$. If

$$x^q - 1 = \prod_{i=0}^{s} f_i$$

is a factorization of $x^q - 1$ into irreducible polynomials $f_i \in \mathbb{F}_p[x]$, then

$$Q_i = \left\langle \frac{x^q - 1}{f_i} \right\rangle \cong \mathbb{F}_p[x]/\langle f_i \rangle \cong \mathbb{F}_{p^{\deg f_i}}.$$

We may suppose that $f_0 = x - 1$, so that $Q_0 = \langle 1 + \ldots + x^{q-1} \rangle \cong \mathbb{F}_p$.
Now let ζ_q be a primitive q-th root of unity in an extension field of $\mathbb{F}_p$. It is well-known by basic Galois theory that, for every $i \in \{1, \ldots, s\}$, there exists exactly one coset A_i in $\mathbb{F}_q^\times / \langle p \rangle$ such that

$$f_i = \prod_{a \in A_i} (x - \zeta_q^a)$$

and the map $f_i \mapsto A_i$ is one-to-one. Furthermore, $\deg f_i = s_p(q)$, which is the multiplicative order of p in $\mathbb{F}_q^\times$. In particular,

$$\dim Q_i \coloneqq l_i = s_p(q)$$

for $i \in \{1, \ldots, s\}$. The automorphism $\hat{}$ maps each Q_i to some Q_j. More precisely, $\hat{Q}_i$ corresponds to the coset $\frac{q-1}{p} A_i$. In particular, $\hat{Q}_i = Q_i$ iff $\frac{q-1}{p} A_i = A_i$, which implies that $\deg f_i = \# A_i$ is divisible by p.

In what follows we need to understand which conditions on q imply $\hat{Q}_i = Q_i$ for all $i \in \{1, \ldots, s\}$. Note that obviously $Q_0 = \hat{Q}_0$.

Theorem 4.1. *If q is a prime with $p \mid q - 1$, then the following conditions (i) are equivalent.*

1. *There exists $i \in \{1, \ldots, s\}$ such that $\hat{Q}_i = Q_i$.*
2. *$\hat{Q}_i = Q_i$ for all $i \in \{0, 1, \ldots, s\}$.*
3. *$\frac{q-1}{p} \in \langle p \rangle \leq \mathbb{F}_q^\times$.*
4. *$s_p(q)$ is even.*

Proof. Clearly (2) implies (1). By the discussion above, $\hat{Q}_i = Q_i$ for all $i \in \{1, \ldots, s\}$ iff $\frac{q-1}{p} A_i = A_i$ for all $i \in \{1, \ldots, s\}$, which happens iff $\frac{q-1}{p} \in \langle p \rangle \leq \mathbb{F}_q^\times$. So (2) and (3) are equivalent. Moreover (3) implies (1). Note that $\frac{q-1}{p} \equiv p^m \bmod q$ for some $m \in \mathbb{Z}$ iff $p^{m+1} \equiv -1 \bmod q$. So, $\frac{q-1}{p} \in \langle p \rangle$ iff $s_p(q)$ is even. Hence (4) and (3) are equivalent. $\square$

Now let p be a fixed odd prime and put

$$\mathcal{P} = \{q \mid q \text{ a prime, } p \mid q - 1 \text{ and } s_p(q) \text{ even}\}$$

By ([15], Theorem 2), the set $\mathcal{P}$ of primes is infinite and it has positive density.

Remark 4.2. Actually in case $p \equiv 3 \bmod 4$ one can easily see that $|\mathcal{P}| = \infty$: Suppose that $p \equiv 3 \bmod 4$ and let h, k be integers such that $ph + 4k = 1$. Then, by Dirichlet's Theorem,

$$\mathcal{P}_0 \coloneqq \{q \mid q \equiv 3ph + 4k \bmod 4p \text{ and } q \text{ a prime}\}$$

is infinite. Since for $q \in \mathcal{P}_0$ we have $q \equiv 3 \bmod 4$ and $p \mid q - 1$ we get by the quadratic reciprocity law

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

By Legendre's formula, it follows

$$-1 = \left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \bmod q,$$

so that $2 \mid s_p(q)$. Thus $\mathcal{P}_0 \subseteq \mathcal{P}$.

From now on, we assume that $q \in \mathcal{P}$.

Now let $G = G_{p,q}$ and recall that $Q = \mathbb{F}_p N = Q_0 \oplus \ldots \oplus Q_s$ with $Q_0 = (\sum_{i=0}^{q-1} \beta^i) \mathbb{F}_p$. If we put

$$R_i = Q_i \oplus \alpha Q_i \oplus \ldots \oplus \alpha^{p-1} Q_i$$

for $i \in \{0, \ldots, s\}$, then obviously

$$\mathbb{F}_p G = R_0 \oplus \ldots \oplus R_s.$$

Theorem 4.3. *The structure of R_i is as follows.*

a) *All R_i are 2-sided ideals of $\mathbb{F}_pG$.*
b) *As a left $\mathbb{F}_pG$-module we have $R_0 \cong \mathbb{F}_pG/N$. In particular, R_0 is uniserial of dimension p and all composition factors are isomorphic to the trivial $\mathbb{F}_pG$-module.*
c) *For $i > 0$ all minimal left ideals in R_i are projective $\mathbb{F}_pG$-modules. Thus R_i is a completely reducible left $\mathbb{F}_pG$-module for $i > 0$.*
d) *R_i is indecomposable as a 2-sided ideal, hence a p-*block *of $\mathbb{F}_pG$. In particular, R_i contains up to isomorphism exactly one irreducible left $\mathbb{F}_pG$-module which is of dimension $l_i = s_p(q)$.*
e) *$R_i \cong \mathrm{Mat}_p(\mathbb{F}_{p^{l_i/p}})$ for $i > 0$ and R_i contains up to isomorphism exactly one irreducible left $\mathbb{F}_pG$-module, say M_i, of dimension $l_i = s_p(q)$.*

Proof. a) Clearly, R_i is a left ideal. It is also a right ideal since $Q_i = \hat{Q}_i$ by Theorem 4.1, and $\alpha a = \hat{a}\alpha$ for $a \in Q$.
b) This follows immediately from representation theory (see for instance ([11], Chap. VII, Example 14.10)).
c) Let $\bar{\mathbb{F}}_p \supseteq \mathbb{F}_p$ be a finite splitting field for N ([11], Chap. VII, Theorem 2.6). Thus every irreducible character χ of $\bar{\mathbb{F}}_pN$ is of degree 1. If χ is not the trivial character, then, according to the action of α on β, the induced character χ^G is an irreducible character for G, by Clifford's Theorem. Furthermore χ^G is afforded by an irreducible projective $\bar{\mathbb{F}}_pG$-module ([11], Chap. VII, Theorem 7.17). Thus all non-trivial irreducible $\bar{\mathbb{F}}_pG$-modules are projective. Now, let M be an irreducible non-trivial $\bar{\mathbb{F}}_pG$-module and denote by M_0 the space M regarded as an $\mathbb{F}_pG$ module. Then, by ([11], Chap. VII, Theorem 1.16 a)), $M_0 \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$ is a direct sum of Galois conjugates of M, which are all projective since no one is the trivial module. Finally, by ([11], Chap. VII, Ex. 19 in Sec. 7), the module M_0 is a projective $\mathbb{F}_pG$-module, and by ([11], Chap. VII, Theorem 1.16 d)), $M_0 \cong W \oplus \ldots \oplus W$ for some irreducible $\mathbb{F}_pG$-module W. Thus W is projective. Since obviously all irreducible non-trivial $\mathbb{F}_pG$-modules can be described this way we are done.
d) Note that R_i is not irreducible as a left module since $M_i := Q_i(1 + \alpha + \ldots + \alpha^{p-1})$ is a minimal ideal in R_i. Clearly, $Q_i \cong M_i$ as a left $\mathbb{F}_pN$-module. Thus Q_i has an extension to the irreducible $\mathbb{F}_pG$-module M_i. But all extensions are isomorphic since G/N is a p-group. Thus R_i has up to isomorphism exactly one irreducible F_pG-module and $\mathbb{F}_pG$ has exactly $s+1$ non-isomorphic $\mathbb{F}_pG$-modules. If some R_i is a direct sum of two non-zero 2-sided ideals, then R_i contains at least two non-isomorphic irreducible $\mathbb{F}_pG$-modules, a contradiction.
e) By c) and d), we know that R_i contains up to isomorphism exactly one irreducible left $\mathbb{F}_pG$-module, say M_i, which has dimension l_i. Thus $R_i \cong M_i \oplus \ldots \oplus M_i$ with p components M_i. That R_i has the indicated matrix algebra structure now follows by Wedderburn's Theorem. □

Lemma 4.4. *For $i > 0$ we have*

a) *$Z_i := \{a \in Q_i \mid a = \hat{a}\}$ is a subfield of Q_i.*
b) *$\#Z_i = p^{\frac{l_i}{p}} = p^{\frac{s_p(q)}{p}}$.*

Proof. a) This is obviously true.
b) Since α acts fixed point freely on $N \setminus \{1\}$ we get $\dim\{a \in Q^* \mid \hat{a} = a\} = \frac{q-1}{p}$. Now, it is sufficient to show that $\dim Z_1 = \dim Z_j$ for $j \geq 1$, which implies

$$\dim Z_i = \frac{q-1}{sp} = \frac{s_p(q)}{p} = \frac{l_i}{p}.$$

Let $\bar{\mathbb{F}}_p$ be a splitting field for G. To prove that $\dim Z_1 = \dim Z_j$ for $j \geq 1$ first note that $Q_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p = V_1 \oplus \ldots \oplus V_{l_i}$, where $V_j = (\frac{1}{|N|}\sum_{x \in N} \chi_j(x^{-1})x)\bar{\mathbb{F}}_p$ and χ_j is a linear non-trivial character of $\bar{\mathbb{F}}_pN$. Thus α acts regularly on the set $\{V_1, \ldots, V_{l_i}\}$, which proves that the fixed point space of α on $V_1 \oplus \ldots \oplus V_{l_i}$ has dimension $\frac{l_i}{p}$. This implies that the fixed point space on W_i also has dimension $\frac{l_i}{p}$, i.e. $\#Z_i = p^{\frac{l_i}{p}}$. $\square$

In order to determine all minimal left ideals in R_i we need the following notation. For $b \in Q_i^\times$ we denote by $[b]$ the image of b in the factor group $Q_i^\times / Z_i^\times$.

Lemma 4.5. *For $i > 0$ we have the following.*

a) *For $b \in Q_i^\times$, the space $Q_i(1 + \alpha + \ldots \alpha^{p-1})b$ is a minimal left ideal in R_i.*
b) *$Q_i(1 + \alpha + \ldots \alpha^{p-1})b = Q_i(1 + \alpha + \ldots \alpha^{p-1})b'$ iff $[b] = [b']$.*
c) *Each minimal left ideal of R_i is of the form $I^i_{[b]} = Q_i(1 + \alpha + \ldots \alpha^{p-1})b$ with $b \in Q_i^\times$.*

Proof. a) This is clear since $\alpha a = \hat{a}\alpha$ for $a \in Q$ and $\hat{Q}_i = Q_i$.
b) Suppose that $0 \neq a(1 + \alpha + \ldots \alpha^{p-1})b = a'(1 + \alpha + \ldots \alpha^{p-1})b'$ with $a, a', b, b' \in Q_i^\times$. Thus

$$x(1 + \alpha + \ldots \alpha^{p-1})y = (1 + \alpha + \ldots \alpha^{p-1})$$

with $x = a'^{-1}a$ and $y = bb'^{-1}$. Since

$$x(1 + \alpha + \ldots \alpha^{p-1})y = xy + x\hat{y}\alpha + \hat{\hat{y}}\alpha^2 + \ldots$$

we obtain $xy = 1 = x\hat{y}$, hence $y = \hat{y}$. It follows

$$y = bb'^{-1} \in Z_i^\times,$$

hence $[b] = [b']$. Conversely, if $[b] = [b']$, then obviously $Q_i(1+\alpha+\ldots \alpha^{p-1})b = Q_i(1+\alpha+\ldots \alpha^{p-1})b'$.
c) Since $\#Z_i = p^{\frac{l_i}{p}}$ by Lemma 4.4, we have constructed so far exactly $\frac{p^{l_i}-1}{p^{l_i/p}-1}$ minimal left ideals. According to Lemma 4.3 e) we have $R_i \cong \mathrm{Mat}_p(\mathbb{F}_{p^{l_i/p}})$. It is well-known that there is a bijection between the set of minimal left ideals in $\mathrm{Mat}_p(\mathbb{F}_{p^{l_i/p}})$ and the set of 1-dimensional subspaces in a p-dimensional vector space over $\mathbb{F}_{p^{l_i/p}}$, which has cardinality $\frac{p^{l_i}-1}{p^{l_i/p}-1}$. $\square$

5. Asymptotically good group codes

In this section we prove that group codes are asymptotically good in any characteristic. We consider here the group algebra $\mathbb{F}_p G_{p,q}$ and all the notations are as in Section 4.

Lemma 5.1 (Chepyzhov [8]). *Let $r : \mathbb{N} \longrightarrow \mathbb{N}$ denote a non-decreasing function and let*

$$P(r) = \{t \text{ prime} \mid s_p(t) \geq r(t)\}.$$

If $r(t) << \sqrt{\gamma \cdot t / \log_p t}$, with $\gamma = \log_p(e) \cdot \log_p(2)$, then $P(r)$ is infinite and dense in the set of all primes. In particular, if $\log_p(t) << r(t) << \sqrt{\gamma \cdot t / \log_p t}$, then the set of primes t such that $s_p(t)$ grows faster than $\log_p(t)$ is infinite and dense in the set of all primes.

Proof. Let B_n be the set of primes t less than n which are not in $P(r)$ (i.e., if $\pi(n)$ is the set of primes less than n, then $\pi(n) = B_n \sqcup (P(r) \cap \pi(n))$). Since $s_p(t)$ is the multiplicative order of p modulo t, there exists for every t in B_n integers $a \in \mathbb{N}$ and $k \in \mathbb{N}$ such that

$$0 < a < r(t) \text{ and } p^a - 1 = kt.$$

Thus

$$\#B_n \leq \#\{(a,k) \mid 0 < a < r(t) \text{ and } (p^a - 1)/k \text{ is prime}\} \leq r(t) \cdot \max_{0<a<r(t)} \#\{\text{prime factors of } p^a - 1\}$$

$$\leq r(t) \cdot \log_2(p^{r(t)} - 1) \leq r(t)^2 \cdot \log_2(p) << \frac{t}{\log t}.$$

By the Prime Number Density Theorem, we have $\pi(n) \sim n / \log n$. Thus the set $P(r)$ is infinite, even dense in the set of all primes. $\square$

Remark 5.2. *Since $\mathcal{P}$ has positive density, there are infinitely many $q \in \mathcal{P}$ such that $s_p(q)$ grows faster than $\log_p(q)$.*

Lemma 5.3. *If Ω_l be the set of left ideals in Q of dimension l, then $\#\Omega_l \leq q^{l/s_p(q)+1}$.*

Proof. Recall that $Q_0, Q_1, \ldots, Q_s$ are the irreducible modules in Q where $\dim_{\mathbb{F}_p} Q_0 = 1$ and $\dim_{\mathbb{F}_p} Q_i = s_p(q)$ for $i \in \{1, \ldots, s\}$. An ideal of dimension l is a direct sum of at most $l/s_p(q) + 1$ of these irreducible modules. There are at most $(s+1)^{l/s_p(q)+1}$ such sums and the assertion follows from $s + 1 \leq q = s_p(q) \cdot s + 1$. □

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

Lemma 5.4. *If $f \in Q^*$ such that $\dim fQ = l$ and*

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

then $\#U \geq p^{\frac{2p-1}{p} l}$.

Proof. We may decompose $f = \sum_{i=1}^s f_i$, with $f_i \in Q_i$ and put $S := \{i \mid f_i \neq 0\}$. Since $f_i Q_i^\times = Q_i^\times$ for $i \in S$ (recall that Q_i is isomorphic to a field), we get

$$U = \sum_{i \in S} Q_i^\times (1 + \alpha + \ldots + \alpha^{p-1}) Q_i^\times.$$

By Lemma 4.5, we have

$$Q_i^\times (1 + \alpha + \ldots + \alpha^{p-1}) Q_i^\times = \bigsqcup_{[b] \in Q_i^\times / Z_i^\times} I_{[b]}^i \setminus \{0\},$$

where $\#I_{[b]}^i = p^{l_i}$ and $\#Q_i^\times / Z_i^\times = \#\{\text{irreducible left ideals in } R_i\} = \frac{p^{l_i}-1}{p^{l_i/p}-1}$. It follows

$$\#(Q_i^\times (1 + \alpha + \ldots + \alpha^{p-1}) Q_i^\times) = \frac{p^{l_i} - 1}{p^{l_i/p} - 1} \cdot (p^{l_i} - 1) \geq p^{(p-1)l_i/p} \cdot p^{l_i}.$$

Finally,

$$\#U \leq \sum_{i \in S} p^{(p-1)l_i/p} \cdot p^{l_i} = p^{\frac{2p-1}{p} l},$$

since $l = \sum_{i \in S} l_i$. □

Theorem 5.5. *Let $R := \mathbb{F}_p G_{p,q}$ and consider the unique decomposition $R = \bigoplus_{i=0}^s R_i$ into the p-blocks R_i described in Theorem 4.3.*

Now we choose a left ideal I of R as

$$I = \bigoplus_{i=1}^s I_i$$

where each I_i is taken uniformly at random among the $1 + p^{l_i/p} + \ldots + p^{(p-1)l_i/p}$ non-zero irreducible left ideals of R_i.

If $0 < \delta \leq \frac{p-1}{p}$ satisfies $h_p(\delta) \leq \frac{p-1}{p^2} - \frac{\log_p(q)}{p \cdot s_p(q)}$, then the probability that the minimum relative distance of I is below δ is at most

$$p^{-p \cdot s_p(q) \cdot \left(\frac{p-1}{p^2} - h_p(\delta)\right) + (2p+1)\log_p(q)}.$$

Proof. Since every irreducible left ideal I_i is of the form given in Lemma 4.5, the above randomized construction is equivalent to consider

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

where $[b]$ is selected uniformly at random from $Q^{*\times}/Z$ with $Z := \{a \in Q^{*\times} \mid \hat{a} = a\}$. Since $Q^{*\times}$ is a group, we have $Q^{*\times} = aQ^{*\times}$ for all $a \in Q^{*\times}$, hence

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

for all $a \in Q^{*\times}$. Let

$$P = \Pr(\mathrm{d}(I_{[b]}) \le pq\delta) = \frac{\#\{I_{[b]} \mid \mathrm{d}(I_{[b]}) \le pq\delta\}}{\#(Q^{*\times}/T)} = \frac{\#\{(a,b) \mid \mathrm{d}(aQ^*(1+\alpha+\ldots+\alpha^{p-1})b) \le pq\delta\}}{\#(Q^{*\times})^2}.$$

By definition of the minimum distance, we have that

$$P \le \sum_{f\in Q^*, f\neq 0} \Pr_{(a,b)\in(Q^{*\times})^2}(0 \le \mathrm{wt}(af(1+\alpha+\ldots+\alpha^{p-1})b) < pq\delta).$$

We can partition Q as

$$Q = \bigsqcup_{l=s_p(q)}^{q} \underbrace{\{f \in Q \mid \dim_{\mathbb{F}_p} fQ = l\}}_{=D_l} \quad \text{and} \quad Q^* = \bigsqcup_{l=s_p(q)}^{q} \underbrace{D_l \cap Q^*}_{=D_l^*},$$

so that

$$P \le \sum_{l=s_p(q)}^{q} \#(D_l^*) \max_{f\in D_l^*} \Pr_{(a,b)\in(Q^{*\times})^2}(0 \le \mathrm{wt}(af(1+\alpha+\ldots+\alpha^{p-1})b) < pq\delta).$$

Let Ω_l be the set of left ideals in Q of dimension l. Then

$$\#(D_l^*) \le \#(D_l) \le p^l \cdot \#(\Omega_l) \le p^l \cdot q^{l/s_p(q)+1}$$

by Lemma 5.3. For any l and any $f \in D_l^*$, we can define

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

as in Lemma 5.4. Using this we get

$$\begin{aligned}
&\Pr_{(a,b)\in(Q^{*\times})^2}(0 \le \mathrm{wt}(af(1+\alpha+\ldots+\alpha^{p-1})b) < pq\delta) = \\
&= \sum_{r\in U, 0\le \mathrm{wt}(r)<pq\delta} \Pr_{(a,b)\in(Q^{*\times})^2}(af(1+\alpha+\ldots+\alpha^{p-1})b = r) \le \\
&\le \max_{r\in U} \Pr_{(a,b)\in(Q^{*\times})^2}(af(1+\alpha+\ldots+\alpha^{p-1})b = r) \cdot \\
&\cdot \sum_{w_1,\ldots,w_p\ge 0, w_1+\ldots+w_p<pq\delta} \#(fQ^{(w_1)}) \cdot \ldots \cdot \#(fQ^{(w_p)}),
\end{aligned}$$

where $fQ^{(w)}$ is the set of elements of weight w in fQ.
It is easy to see that each $r \in U$ can occur with the same probability as $af(1+\alpha+\ldots+\alpha^{p-1})b$, so that the above probability is independent of r. Thus we have

$$\Pr_{(a,b)\in(Q^{*\times})^2}(af(1+\alpha+\ldots+\alpha^{p-1})b = r) = \frac{1}{\#U} \le p^{-\frac{2p-1}{p}l},$$

by Lemma 5.4.
Moreover, fQ is a $[pq,l]_p$ group code, so that, by Remark 3.2 and Theorem 3.1, we have

$$\#(fQ^{(w)}) \le p^{l\cdot h_p(w/pq)}$$

for all $w \le (p-1)\cdot q$ (which is true, since $\delta \le \frac{p-1}{p}$). Putting together all previous inequalities we have

$$P \le \sum_{l=s_p(q)}^{q} p^{-\frac{p-1}{p}l} \cdot q^{l/s_p(q)+1} \cdot \sum_{w_1,\ldots,w_p \ge 0, w_1+\ldots+w_p < pq\delta} p^{l\cdot\sum_{i=1}^{p} h_p(w_i/pq)},$$

so that, by the convexity,

$$P \le \sum_{l=s_p(q)}^{q} p^{-\frac{p-1}{p}l} \cdot q^{l/s_p(q)+1} \cdot (pq\delta)^p \cdot p^{l\cdot p\cdot h_p(\delta)} \le \sum_{l=s_p(q)}^{q} p^{l\cdot p\cdot\left(h_p(\delta)-\frac{p-1}{p^2}+\frac{\log_p(q)}{p\cdot s_p(q)}\right)+p+p\log_p(q)}.$$

Finally, if $h_p(\delta) \le \frac{p-1}{p^2} - \frac{\log_p(q)}{p\cdot s_p(q)}$, then

$$P \le p^{-p\cdot s_p(q)\cdot\left(\frac{p-1}{p^2}-h_p(\delta)\right)+(p+1)\log_p(q)+p} \le p^{-p\cdot s_p(q)\cdot\left(\frac{p-1}{p^2}-h_p(\delta)\right)+(2p+1)\log_p(q)}.$$

□

Corollary 5.6. *Group codes over finite fields are asymptotically good.*

Proof. We have to prove the assertion only for odd prime fields. The general case then follows by field extension (see ([9], Proposition 12)). According to Lemma 5.1 and Remark 5.2, we may choose a sequence of primes q_i in $\mathcal{P}$ such that $q_1 < q_2 < \ldots$ and $\frac{s_p(q_i)}{\log_p(q_i)} \longrightarrow 0$ for $i \longrightarrow \infty$. Let $0 < \delta \le \frac{p-1}{p}$ with $h_p(\delta) \le \frac{p-1}{p^2} - \frac{\log_p(q_1)}{p\cdot s_p(q_1)}$. Thus the assumption in Theorem 5.5 is satisfied for all q_i and we can find a left ideal I_{q_i} in $\mathbb{F}_p G_{p,q_i}$ with relative minimum distance at least δ. Furthermore, $\dim I_{q_i} = s \cdot s_p(q_i) = q-1$. Thus

$$\frac{\dim I_{q_i}}{pq_i} = \frac{1}{p} - \frac{1}{pq_i} \ge \frac{1}{p} - \frac{1}{pq_1}.$$

This shows that the sequence of the left ideals I_{q_i} is asymptotically good. □

Remark 5.7. Note that the groups $G_{p,q}$ are p-nilpotent with cyclic Sylow p-subgroups. Thus the asymptotically good sequence we constructed in the Corollary is a sequence of group codes in code-checkable group algebras [6]. In such algebras all left and right ideals are principal.

Acknowledgement. The first author was partially supported by PEPS - Jeunes Chercheur-e-s - 2018. The second author likes to thank Université Paris 8 and LAGA for their hospitality and financial support during a stay in October 2018. We are very grateful to Patrick Solé and Pieter Moree who brought to our attention that the set $\mathcal{P}$ is infinite also in case $p \equiv 1 \bmod 4$.

References

[1] J.L. Alperin and R.B. Bell, Groups and representations, *Graduate Text in Math.*, Springer Verlag 1995.
[2] E.F. Assmus, H.F. Mattson and R. Turyn, Cyclic codes, *Report AFCRL-65-332 of the Appl. Res. Lab.*, Sylvania Electronic Systems 1965.
[3] L.M.J. Bazzi and S.K. Mitter, Some randomized code constructions from group actions, *IEEE Trans. Inform. Theory,* vol. 52, pp. 3210-3219, 2006.
[4] S.D. Berman, On the theory of group codes, *Kibernetika,* vol. 3, pp. 31-39, 1967.
[5] F. Bernhardt, P. Landrock and O. Manz, The extended Golay codes considered as ideals, *J. Comb. Theory, Series A,* vol. 55, pp. 235-246, 1990
[6] M. Borello, J. de la Cruz and W. Willems, Checkable codes in group algebras, `arXiv: 1901.10979`, 2018.
[7] P. Charpin, Une généralisation de la construction de Berman des codes de Reed-Muller p-aire, *Comm. Algebra,* vol 16, pp. 2231-2246, 1988.
[8] 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, 1992.
[9] A. Faldum and W. Willems, Codes of small defect, *Designs, Codes and Cryptography,* vol.10, pp. 341-350, 1997.

[10] M. Grassl, Bounds on the minimum distance of linear codes. Online http://www.codetables.de.
[11] B. Huppert and N. Blackburn, Finite Groups II, Springer Verlag 1982.
[12] S. Jitman, S. Ling, H. Liu and X. Xie, Checkable codes from group rings, arXiv: 1012.5498v1, 2010.
[13] J.L. Massey, On the fractional weight of distinct binary n-tuples, *IEEE Trans. Inform. Theory,* vol. 20, pp. 131-131, 1974.
[14] I. McLoughlin and T. Hurley, A group ring construction of the extended binary Golay code, *IEEE Trans. Inform. Theory,* Vol. 54, pp. 4381-4383, 2008.
[15] P. Moree and B. Sury, Primes in a prescribed arithmetic progression dividing the sequence $\{a^k + b^k\}_{k=1}^{\infty}$, *Int. J. Number Theory*, vol. 5, pp. 641-655, 2009.
[16] P. Piret, An upper bound on the weight distribution of some systematic codes, *IEEE Trans. Inform. Theory,* vol. 31, pp. 520-521, 1985.
[17] S. Roman, Coding and Information Theory, Graduate Text in Math. 134, Springer-Verlag 1992.