A coding theoretical perspective on ideals in group algebras

Martino Borello (Université Paris 8 - LAGA)

June 7th 2021 - ACT21 Zurich

Abstract

Group codes over fields are ideals in the group algebra KG, where K is a finite field and G is a finite group. Introduced by Berman and MacWilliams in the late sixties as a generalization of cyclic codes, they are still the subject of intense research. This short course is intended to be an introduction to their theory, presenting their main properties in relation to classical codes. The last part of the lecture will give an overview of current research perspectives and open problems. A good reference (among the rare ones) for these codes is Chapter 16 of the recent *Concise Encyclopedia of Coding Theory* by Huffman, Kim, and Solé.

Contents

1 Introduction

In the theory of error correcting codes linear codes play a central role due to their algebraic structure which allows, for example, an easy description and storage. Quite early in coding theory it appeared convenient to add additional algebraic structure in order to get more information about the parameters and to speed up the decoding process. In 1957, E. Prange introduced the now well-known class of cyclic codes [23], which are the forefathers of many other families of codes with symmetries discovered thereafter. In particular, abelian codes [2], group codes [19], quasi-cyclic codes [9] and quasi-abelian codes [24] are distinguished descendants of cyclic codes. All of them have nice algebraic structures, and many optimal codes belong to these families.

This short course wants to be an introduction to the theory of group codes, highlighting some basic facts and some more advanced topics. For more details the reader is referred to [14, Chapter 16] and references therein.

2 Background

Throughout these notes, K is a finite field of cardinality q.

A *linear code* $\mathcal{C}$ of *length* n is a K-linear subspace of K^n. An element $c = (c_1, \ldots, c_n) \in \mathcal{C}$ is called a *codeword* and its (Hamming) *weight* is given by

$$\mathrm{wt}(c) := \#\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}.$$

The *minimum distance* of $\mathcal{C}$ is defined by $\mathrm{d}(\mathcal{C}) := \min_{c\in\mathcal{C}\setminus\{0\}} \mathrm{wt}(c)$. An $[n, k, d]_q$ code is a linear code of length n, dimension k and minimum distance d over a field of cardinality q. These are usually called *the parameters* of the code. The dual code $\mathcal{C}^\perp$ is the subspace $\{v \in K^n \mid \langle v, c\rangle = 0, c \in \mathcal{C}\}$, with respect to the standard inner product in K^n.

There are some natural group actions associated to linear codes. The symmetric group S_n acts on the set $\{1, \ldots, n\}$ of coordinates by definition. This action induces an *action on the elements* of K^n, namely for $v \in K^n$ and $\sigma \in S_n$ we have

$$v^\sigma := (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots, v_{\sigma^{-1}(n)}),$$

which induces an *action on subsets* of K^n (and in particular on linear codes). For $\mathcal{C} \subseteq K^n$ we put

$$\mathcal{C}^\sigma := \{c^\sigma \mid c \in \mathcal{C}\}.$$

An element $\sigma \in S_n$ is an *automorphism* of $\mathcal{C}$ if $\mathcal{C}^\sigma = \mathcal{C}$. The stabilizer

$$\mathrm{PAut}(\mathcal{C}) := \{\sigma \in S_n \mid \mathcal{C}^\sigma = \mathcal{C}\}$$

is called the *permutation automorphism group* of $\mathcal{C}$. Moreover, a linear code $\mathcal{C}_1$ is *equivalent* or better *permutation equivalent* to a linear code $\mathcal{C}_2$ if there exists $\sigma \in S_n$ such that $\mathcal{C}_1^\sigma = \mathcal{C}_2$. This is not the most general definition of equivalence but it is sufficient for our purpose. Finally, it is easy to see that $\mathrm{PAut}(\mathcal{C}^\sigma) = \mathrm{PAut}(\mathcal{C})^\sigma$ (*the conjugate of* $\mathrm{PAut}(\mathcal{C})$ *in* S_n *by* σ).

For any other notion in classical coding theory, the reader is referred to [15].

3 Group algebras

Let G be a finite group of cardinality n and let K be a finite field.

Definition 3.1. The *group algebra* KG is the set of formal sums

$$KG := \left\{ a = \sum_{g\in G} a_g g \;\middle|\; a_g \in K \right\},$$

which is a K-vector space in a natural way and which becomes a K-algebra via the multiplication

$$ab := \sum_{g\in G} \left(\sum_{h\in G} a_h b_{h^{-1}g} \right) g,$$

for $a = \sum_{g\in G} a_g g$ and $b = \sum_{g\in G} b_g g$.

The group algebra KG is isomorphic to K^n as a K-vector space, where $n = \#G$. There is a standard way of constructing such an isomorphism, which allows us to transfer many coding theoretical properties from K^n to KG. Once an ordering $g_1, \ldots, g_n$ of the elements of G is chosen, we may define $\varphi : g_i \mapsto e_i$, where $\{e_1, \ldots, e_n\}$ is the standard basis of K^n. Then we extend this map K-linearly so that

$$\varphi : \sum_{i=1}^{n} a_i g_i \mapsto (a_1, \ldots, a_n). \tag{1}$$

The isomorphism φ obtained in this way is not canonical, since it depends on the ordering of the group. But different orderings lead only to a permutation of the coordinates, hence to permutation equivalent codes.

Via the isomorphism φ, we may transfer the Hamming metric from K^n to KG. For $a \in KG$, we define

$$\mathrm{wt}(a) := \mathrm{wt}(\varphi(a)).$$

Moreover, we may define a standard inner product on KG as follows: for $a, b \in KG$,

$$\langle a, b\rangle := \langle \varphi(a), \varphi(b)\rangle,$$

where the last is the standard inner product in K^n. This extends the classical duality to the group algebra context. So, from a coding theoretical point of view, we can consider linear codes either in KG or in K^n without any difference. However, the algebraic structure of KG allows us to consider codes with more structure than linearity.

Definition 3.2 ([2, 19])**.** A *G-code* is a right ideal $\mathcal{C}$ in the group algebra KG. If the group G is cyclic (resp. abelian, resp. dihedral), then the code $\mathcal{C}$ is called a *cyclic* (resp. *abelian,* resp. *dihedral*) *code.* In the case we do not specialize the group G explicitly we briefly speak of a group code.

The restriction to right ideals is only for convention, which means that everything in the following may be stated equally for left ideals.

Remark 3.3. The particular class of cyclic G-codes is nothing else than the family of well known cyclic codes. If G is cyclic, hence generated by a certain $g \in G$, and the isomorphism φ sends $g^i \to e_{i+1}$ for all $i \in \{0, \dots, n-1\}$, then $\varphi(\mathcal{C})$ is *cyclic.* In fact, in this case $KG \cong K[x]/(x^n - 1)$ via the isomorphism $g \mapsto x$. Thus, a cyclic code turns out to be an ideal in the factor algebra $K[x]/(x^n - 1)$, which is the classical definition.

Now let $\mathcal{C}$ be a G-code with $n = \#G$. Observe that the right multiplication on G by one of its elements, say g, induces a permutation $\psi_g \in S_n$ defined by

$$\psi_g(i) = j \;\text{ iff }\; g_i g = g_j. \tag{2}$$

Note that $g \mapsto \psi_g$ is a faithful permutation representation of G, which depends on the chosen ordering of G. If this map coincides with that chosen for φ, then $\psi(G) := \{\psi_g \mid g \in G\}$ is a subgroup of $\mathrm{PAut}(\varphi(\mathcal{C}))$. This is due to the fact that a right ideal is stable by multiplication on the right. Since the action of right multiplication is regular, $\psi(G)$ is a regular subgroup of S_n.

Suppose that $\mathcal{C}$ is a linear code in K^n admitting a regular subgroup G of $\mathrm{PAut}(\mathcal{C})$. Since G is a group of automorphisms, $\mathcal{C}$ becomes a right KG-module via the action

$$c \cdot \left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} a_g c^g \tag{3}$$

for $c \in \mathcal{C}$ and $a_g \in K$, where $c^g \in \mathcal{C}$ is the image of c under the action of g. Moreover, as every regular action of G is isomorphic to the action of G on itself given by right multiplication, there is an ordering of G such that $\varphi^{-1}(\mathcal{C})$ is a G-code in KG. Thus we have proved, in our framework, the known characterization of group codes.

Theorem 3.4 ([3])**.** Let G be a group of order n and let $\mathcal{C}$ be a linear code in K^n. Then $\mathcal{C}$ is a G-code if and only if G is isomorphic to a regular subgroup H of $\mathrm{PAut}(\mathcal{C})$.

Example 3.5. Let $G = D_{2m} = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma = \sigma^{n-1}\tau\rangle$. If we consider the ordering

$$D_{2m} = \{\underbrace{1}_{b_1}, \underbrace{\tau}_{b_2}, \underbrace{\sigma}_{b_3}, \underbrace{\tau\sigma}_{b_4}, \underbrace{\sigma^2}_{b_5}, \underbrace{\tau\sigma^2}_{b_6}, \dots, \underbrace{\sigma^{m-1}}_{b_{2m-1}}, \underbrace{\tau\sigma^{m-1}}_{b_{2m}}\}, \tag{4}$$

and the K-linear isomorphism $\varphi : KD_{2m} \to K^{2m}$ given by $b_i \mapsto e_i$ (where $\{e_i\}$ is the canonical basis of K^{2m}), a linear code $\mathcal{C} \subseteq K^{2m}$ is a D_{2m}-code if and only if

$$\psi(\sigma) = (1\ 3\ 5\ \dots\ 2m-1)(2\ 4\ 6\ \dots\ 2m)$$

and

$$\psi(\tau) := (1\ 2)(3\ 2m)(4\ 2m-1)(5\ 2m-2)\cdots(m+1\ m+2)$$

are in $\mathrm{PAut}(\mathcal{C})$.

We would like to mention here that a G-code may also be an H-code where H is not isomorphic to G. For instance, the binary extended [24,12,8] Golay code is a G-code for the symmetric group S_4 [4] and the dihedral group D_{24} [20]. Furthermore, there are abelian G-codes which are not group codes for cyclic groups. As an example may serve the binary extended $[8, 4, 4]$ Hamming code. It is a $G = C_2 \times C_4$ code, but it is not equivalent to a cyclic code.

4 Checkable and principal ideals

One of the main feature for which cyclic codes are interesting from a coding theoretical point of view is that they can be described with very few data, namely the length, the base field and a generator or a check polynomial. This happens because every ideal in $K[x]/(x^n - 1)$ is principal. We are interested here in the analogue for group codes. The notion of principal ideal is clear. We need then to explore the notion of "checkability".

For any subset $S \subseteq KG$ the *right annihilator* $\mathrm{Ann}_r(S)$ is defined by

$$\mathrm{Ann}_r(S) = \{a \in KG \mid sa = 0 \text{ for all } s \in S\}.$$

Analogously the *left annihilator* of S is given by

$$\mathrm{Ann}_l(S) = \{a \in KG \mid as = 0 \text{ for all } s \in S\}.$$

Note that the right (resp. left) annihilators are right (resp. left) ideals in KG.

Definition 4.1. A right ideal $\mathcal{C}$ in KG is called *c*heckable if there exists an element $v \in KG$ such that

$$\mathcal{C} = \{a \in KG \mid va = 0\} = \mathrm{Ann}_r(v) = \mathrm{Ann}_r(KGv).$$

Note that checkable left ideals are defined analogously via the left annihilator of a principal right ideal. A group algebra KG is called *code-checkable* if all right ideals of KG are checkable.

Example 4.2. We give here some examples of checkable codes. For the main notions in representation theory, the reader is referred to [16].

a) All cyclic codes are checkable, since the check equation is given by the check polynomial.

b) Let $e = e^2$ be an idempotent in KG. Then the ideal eKG is checkable. This can be seen as follows. Obviously, $eKG \subseteq \mathrm{Ann}_r(KG(1-e))$. Since any $0 \neq (1-e)b \in (1-e)KG$ is not in $\mathrm{Ann}_r(KG(1-e))$ we have $eKG = \mathrm{Ann}_r(KG(1-e))$.

c) If KG is a semisimple algebra (by Maschke's Theorem this happens if $\mathrm{char}K$ does not divide $\#G$), then all right and left ideals are generated by idempotents. Thus all right and left ideals are checkable.

Remark 4.3. In [17] the authors point out that in numerous cases the parameters of checkable group codes for an abelian group G are as good as the best known linear codes mentioned in [13]. Even more, there is a checkable $[36, 28, 6]_5$ group code in $\mathbb{F}_5(C_6 \times C_6)$ and a checkable $[72, 62, 6]_5$ group code in $\mathbb{F}_5(C_6 \times C_{12})$. In both cases the minimum distance is improved by 1 from an earlier lower bound in [13].

The following is a well-known result (see [16, Chap. VII]) that holds for all Frobenius algebras, so in particular for group algebras.

Proposition 4.4 (Double Annihilator Property)**.** Let $\mathcal{C}$ a right ideal in KG, then

$$\mathcal{C} = \mathrm{Ann}_r(\mathrm{Ann}_l(\mathcal{C})).$$

A similar equation holds for left ideals.

Corollary 4.5. A right (resp. left) ideal $\mathcal{C}$ in KG is checkable if and only if $\mathrm{Ann}_l(\mathcal{C})$ (resp. $\mathrm{Ann}_r(\mathcal{C})$) is a principal left (resp. right) ideal.

In order to state an early result of Jessie MacWilliams recall that the K-linear map $\hat{}: KG \longrightarrow KG$ defined by $g \mapsto \hat{g} = g^{-1}$ $(g \in G)$ is an antialgebra automorphism of KG.

Lemma 4.6 ([19])**.** If $\mathcal{C}$ is a right ideal in KG, then $\mathcal{C}^\perp = \widehat{\mathrm{Ann}_l(\mathcal{C})}$. Similarly, for a left ideal $\mathcal{C}$ we have $\mathcal{C}^\perp = \widehat{\mathrm{Ann}_r(\mathcal{C})}$.

Proof. We have $a = \sum_{g\in G} a_g g \in \widehat{\mathrm{Ann}_l(\mathcal{C})}$ if and only if $\hat{a}ch = 0$ for all $c \in \mathcal{C}$ and all $h \in G$. Since the coefficient at h in $\hat{a}ch$ equals

$$\sum_{g\in G} a_g c_g = \langle a, c\rangle,$$

the assertion follows. □

Theorem 4.7 ([7])**.** For any right ideal $\mathcal{C}$ in KG the following are equivalent.

a) $\mathcal{C}$ is checkable.

b) $\mathcal{C}^\perp$ is a principal right ideal.

Proof. According to Corollary 4.5, $\mathcal{C}$ is checkable if and only if $\mathrm{Ann}_l(\mathcal{C}) = KGv$ for some $v \in KG$. Now Lemma 4.6 implies $\mathcal{C}^\perp = \widehat{\mathrm{Ann}_l(\mathcal{C})} = \widehat{KGv} = \hat{v}KG$ and the proof is complete. □

Remember from finite group theory that a group G is called *p-nilpotent* if G has a normal subgroup N with p not dividing $\#N$ such that the factor group G/N is a p-group, i.e., G/N is isomorphic to a Sylow p-subgroup of G.

Theorem 4.8 ([22])**.** Let $\mathrm{char}K = p$. Then KG is a code-checkable group algebra if and only if G is p-nilpotent with a cyclic Sylow p-subgroup.

Example 4.9. KD_{2m} is code-checkable if and only if $(q, m) = 1$.

Example 4.10. The ideal $\langle 1+\sigma, 1+\tau\rangle \subset \mathbb{F}_2 D_8$ is not principal. Its dual is then not checkable.

5 Counting

The following result is well known (see [15]):

Theorem 5.1. Let $n = q^s t$, with $(t, q) = 1$. If

$$x^n - 1 = (x^t - 1)^{q^s} = (f_0 f_1 \cdots f_r)^{q^s}$$

is a factorization of $x^n - 1$ in irreducible factors in $K[x]$ (we choose $f_0 = x - 1$), then the number of cyclic codes of length n over K is

$$(q^s + 1)^{r+1}.$$

If t is prime, we have $\deg f_i = \mathrm{ord}_t(q)$ (the order of q in $\mathbb{F}_t^*$) for every $i \in \{1, \dots, r\}$, then $r = \frac{t-1}{\mathrm{ord}_t(q)}$.

Note that $\mathrm{ord}_t(q)$ is a "difficult number", related to many conjectures (Artin's conjecture on primitive roots - see [21]). However, there are essentially "few" cyclic codes.

Example 5.2 (Group codes of length 6 in even characteristic)**.** Let $G = D_6 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^2\rangle$ and $K = \mathbb{F}_q$ with q even. The group algebra KG has two orthogonal central idempotents:

$$e_0 := 1 + \sigma + \sigma^2 \text{ and } e_1 := \sigma + \sigma^2.$$

Let $B_0 := e_0 KG$ and $B_1 := e_1 KG$, the 2-blocks (which are indecomposable as 2-sided ideals). The first one, B_0, is indecomposable and it contains the trivial module $M := (1 + \sigma + \sigma^2 + \tau + \tau\sigma + \tau\sigma^2)K$, of dimension

1. B_0 is called the principal block of KG. M is the Jacobson radical of KG. B_0 is a non-split extension of M by M (that is B_0/M is isomorphic to M).

The block B_1 contains two primitive orthogonal idempotents:

$$f_1 := 1+\sigma+\tau+\tau\sigma \text{ and } f_2 := 1+\sigma+\tau\sigma+\tau\sigma^2.$$

We have that f_1KG and f_2KG are two isomorphic irreducible modules of dimension 2. Call V this irreducible module, up to isomorphism. So this is the decomposition of KG in projective indecomposable modules:

$$KG = \underbrace{\begin{matrix} M \\ M \end{matrix}}_{B_0} \oplus \underbrace{V \oplus V}_{B_1}.$$

The defect group of the 2-block B_1 is trivial and we have that $B_1 \cong \mathrm{Mat}_2(K)$. An explicit isomorphism may be given as follows:

$$f_1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; f_2 \mapsto \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

This implies that B_1 has

$$\frac{\#\mathrm{Mat}_2(K) - \#\mathrm{GL}_2(K) - 1}{\#V - 1} = \frac{q^4-(q^2-1)(q^2-q)-1}{q^2-1} = q+1$$

irreducible modules isomorphic to V. Now, we have all the ingredients to count all right ideals in KG: since every ideal $I = (I\cap B_0)\oplus(I\cap B_1)$, it is enough to count all possible intersections. Now,

$$(I\cap B_0) = \begin{cases} B_0 \\ M \\ \{0\} \end{cases} \quad \text{and} \quad (I\cap B_1) = \begin{cases} B_1 \\ \cong V \\ \{0\} \end{cases}$$

so we have $3\cdot(2+q+1) = 3q+9$ right ideals in KG, which are then q-ary codes of length 6.

We compare to the number of q-ary cyclic codes, with q even, of length 6. Since

$$x^6-1 = (x-1)^2(x^2+x+1)^2$$

and x^2+x+1 is irreducible when q is an odd power of 2 and reducible otherwise, we have 9 cyclic codes when q is an odd power of 2 and 27 otherwise. In general (except for $q=4$) this is (much) less than the number of dihedral codes of length 6.

Up to equivalence: 9 cyclic binary codes and 14 dihedral binary codes of length 6. Note also that it happens that dihedral codes over a certain finite field have better parameters than all cyclic ones: for example, there is no $[6,4,3]_8$ cyclic code, whereas there exists a dihedral codes with those parameters (you can easily verify it with MAGMA).

For some abelian groups we have the following.

Proposition 5.3 ([18]). If $\mathrm{char} K = p$ and $G = A\times C_{p^k}$, where A is an abelian group with $(\#A, p) = 1$ and C_{p^k} is a cyclic group of order p^k, then KG contains exactly $(p^k+1)^t$, where t is the number of irreducible KA-modules.

It would be interesting to have other general results for other groups.

6 Other nice results and outlook

Duality. For a right KG-module $\mathcal{C}$, the *dual module* is $\mathcal{C}^* = \mathrm{Hom}_K(\mathcal{C}, K)$, which is a KG-module by $c(\alpha g) = (cg^{-1})\alpha$, for $c\in\mathcal{C}$, $g\in G$ and $\alpha\in\mathrm{Hom}_K(\mathcal{C},K)$. It is proved in [25] that, if $\mathcal{C}$ is a right ideal in KG, then $KG/\mathcal{C}^\perp \cong \mathcal{C}^*$ as KG-modules. This is the fundamental ingredient to prove.

Theorem 6.1 ([25])**.** The group algebra KG contains a self-dual group code if and only if $\mathrm{char}K = 2$ and $\#G$ is even.

Theorem 6.2 ([10])**.** A group code $\mathcal{C}$ in KG is an LCD code if and only if $\mathcal{C} = eKG$ with $e^2 = e = \hat{e}$. In this case, $\mathcal{C}^\perp = (1 - e)KG$.

Similar results are also proved for LCP [6].

Dimension. The dimension of a group code is determined by the algebraic structure of KG. The next result is contained in [16].

Theorem 6.3 (Dickson)**.** If $\mathrm{char}K = p$, e is an idempotent in KG, and $|G|_p$ is the highest power of p dividing $\#G$, then $|G|_p$ divides $\dim eKG$.

In [11], an algorithm for computing the dimension of general group codes is given. In a very recent paper [12], several relations and bounds for the dimension of principal ideals in group algebras are determined by analysing minimal polynomials of regular representations.

Minimum distance. There are asymptotic results.

Theorem 6.4 ([1, 8])**.** The class of group codes in checkable group algebras is asymptotically good over every finite field.

However, the question about cyclic or abelian codes is still open.
Not much is known about group codes with prescribed minimum distance. Some results about dihedral codes are contained in [5].

References

[1] L.M.J. Bazzi and S.K. Mitter. *Some randomized code constructions from group actions.* IEEE Trans. Inform. Theory 52 (2006): 3210-3219.

[2] S.D. Berman. *Semisimple cyclic and Abelian codes.* II. Kibernetika (Kiev) no. 3 (1967): 21-30 (Russian).

[3] J.J. Bernal, A. del Río and J.J. Simón. *An intrinsical description of group codes.* Designs, Codes and Cryptography 51.3 (2009): 289-300.

[4] F. Bernhardt, P. Landrock and O. Manz. *The extended Golay codes considered as ideals.* J. Comb. Theory, Series A 55 (1990): 235-246.

[5] M. Borello and A. Jamous. *Dihedral codes with prescribed minimum distance*, In: Bajard J.C., Topuzoglu A. (eds) Arithmetic of Finite Fields. WAIFI 2020. Lecture Notes in Computer Science, vol 12542. Springer, Cham. (2021).

[6] M. Borello, J. de la Cruz and W. Willems. *A note on linear complementary pairs of group codes.* Discrete Mathematics, 343(8) (2020): 111905.

[7] M. Borello, J. de la Cruz and W. Willems. *On checkable codes in group algebras.* to appear in Journal of Algebra and Its Applications.

[8] M. Borello and W. Willems. *Group codes over fields are asymptotically good.* Finite Fields and Their Applications 68 (2020): 101738.

[9] C.L. Chen, W.W. Peterson and E.J. Weldon Jr. *Some results on quasi-cyclic codes.* Information and Control, 15.5 (1969): 407-423.

[10] J. de la Cruz and W. Willems. *On group codes with complementary duals.* Des. Codes Cryptogr., 86 (2018): 2065–2073.

[11] M. Elia and E. Gorla. *Computing the dimension of ideals in group algebras, with an application to coding theory.* Journal of Algebra, Number Theory and Applications 45(1) (2020): 13-28.

[12] E. J. García-Claro and H. Tapia-Recillas. *On the dimension of ideals in group algebras, and group codes.* to appear in Journal of Algebra and its Applications.

[13] M. Grassl. Bounds on the minimum distance of linear codes. Online `http://www.codetables.de`.

[14] W.C. Huffman, J.L. Kim and P. Solé. *Concise Encyclopedia of Coding Theory.* Chapman and Hall/CRC, 2021.

[15] W.C. Huffman and V. Pless. *Fundamentals of error-correcting codes.* Cambridge university press, 2010.

[16] B. Huppert and N. Blackburn. *Finite Groups II.* Springer, Berlin, 1982.

[17] S. Jitman, S. Ling, H. Liu and X. Xie. *Checkable codes from group rings.* `arXiv: 1012.5498v1`, 2010.

[18] S. Jitman, S. Ling, H. Liu and X. Xie. *Abelian codes in principal ideal group algebras.* IEEE Trans. Inform.Theory 59 (2013): 3046-3058.

[19] F.J. MacWilliams. *Codes and ideals in group algebras.* Comb. Math. and its Appl. Proceedings ed. by R.C. Bose and T.A. Dowling, Chap. 18 (1967): 317-328.

[20] I. McLoughlin and T. Hurley. *A group ring construction of the extended binary Golay code.* IEEE Trans. Inform. Theory 54 (2008):4381-4383.

[21] P. Moree. *Artin's primitive root conjecture–a survey.* Integers, 12(6) (2012): 1305-1416.

[22] D.S. Passman. *Observations on group rings.* Comm. Algebra 5 (1977): 1119-1162.

[23] E. Prange. *Cyclic Error-Correcting Codes in Two Symbols.* Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN-57-103 (1957).

[24] S.K. Wasan. *Quasi abelian codes.* Publ. Inst. Math. 35 (1977): 201-206.

[25] W. Willems. *A note on self- group codes.* IEEE Trans. Inform. Theory 48 (2007): 3107-3109.