



HAL
open science

On checkable codes in group algebras

Martino Borello, Javier de la Cruz, Wolfgang Willems

► **To cite this version:**

Martino Borello, Javier de la Cruz, Wolfgang Willems. On checkable codes in group algebras. *Journal of Algebra and Its Applications*, 2022, 21 (06), 10.1142/S0219498822501250 . hal-03852305

HAL Id: hal-03852305

<https://hal.science/hal-03852305>

Submitted on 14 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On checkable codes in group algebras

Martino Borello,

Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA,
Université Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France

and

Javier de la Cruz

Universidad del Norte, Barranquilla, Colombia

and

Wolfgang Willems

Otto-von-Guericke Universität, Magdeburg, Germany
and Universidad del Norte, Barranquilla, Colombia

Keywords. Group algebra; group code; principal ideal algebras.

MSC classification. 94B05, 20C05

Abstract

We classify, in terms of the structure of the finite group G , all group algebras KG for which all right ideals are right annihilators of principal left ideals. This means in the language of coding theory that we classify code-checkable group algebras KG which have been considered so far only for abelian groups G . Optimality of checkable codes and asymptotic results are discussed.

1 Introduction

Block codes were invented in the forties to correct errors in the communication through noisy channels (see [20] for more details). In their most general sense, they are just subsets of (code)words of a fixed length n over an alphabet K , such that the Hamming distance between the words (i.e. the number of distinct letters) is large enough. One of the main practical problems of coding theory is how to store a given code, which can be, without an additional structure, quite expensive (we may have to store the whole list of codewords). This is one of the main reasons why, since the beginning, linear codes were introduced: a linear code of length n over a finite field K is a subspace of the vector space K^n . Such algebraic structure allows to describe a linear code in a more compact way: a linear code C of length n and dimension k can be defined by its parity check matrix, which is a $n \times (n-k)$ matrix H such that $c \in C$ if and only if $cH = 0$, i.e., it is a matrix which gives $n-k$ check equations which determine the code. Such a description reduces exponentially the size of the data to be stored and it has made linear codes so much used. However, in the

context of McEliece cryptosystem [21] and its dual version by Niederreiter [24], in which the public key is given by the parity check matrix, a code of large length and dimension, the size of the matrix constitutes one of the main disadvantages. McEliece cryptosystem and its variants, which are part of the so-called code-based cryptography, are now subjects of intense research, due to their probable resistance to quantum computer's attacks. One of the central problems is to reduce the size of the public key (see for example [3]). In order to do it, one usually adds more algebraic structure. A classical family of more structured linear codes is that of cyclic codes, which are linear codes invariant under a cyclic shift. It is well-known that they can be seen as (principal) ideals inside the polynomial ring $A = K[x]/(x^n - 1)$. If a linear code C is cyclic, we have $C = gA$ with $g \in A$ and C is determined by only one check equation, given by the so-called check polynomial $f = (x^n - 1)/g$. In this note we focus on more general examples in K -algebras in which codes are determined by just one check equation.

A natural generalization of cyclic codes is given by the family of group codes: a linear code C is called a G -code (or a *group code*) if C is a right ideal in the group algebra $KG = \{a = \sum_{g \in G} a_g g \mid a_g \in K\}$ for G a finite group. Here the vector space KG with basis $\{g \in G\}$ serves as the ambient space with the weight function $\text{wt}(a) = |\{g \in G \mid a_g \neq 0\}|$ and the non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ which is defined by

$$\langle g, h \rangle = \delta_{g,h} \quad \text{for } g, h \in G.$$

Note that KG carries a K -algebra structure via the multiplication in G . More precisely, if $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g$ are given, then

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

In this sense cyclic codes are group codes for a cyclic group G . Reed Muller codes over prime fields \mathbb{F}_p are group codes for an elementary abelian p -group G [4, 9], and there are many other remarkable optimal codes which have been detected as group codes [5, 10, 14, 22].

We would like to mention here that choosing right ideals as group codes is just done by convention. Everything what we will prove holds equally true for group codes which are left ideals.

If G is cyclic, then all right ideals of KG afford only one check equation as we have seen above. In case G is a general finite group there are only particular right ideals which satisfy this property. Such codes are called *checkable* and these are the subject of this paper. To our knowledge, such codes were first defined in [17] and investigated for abelian group algebras (most of the results of [17] are now published in [18]).

In §2, we characterize checkable codes in terms of their duals, proving that a right ideal $C \leq KG$ is checkable if and only if its dual is a principal right ideal (Theorem 2.6).

This result provides an easy way to construct random checkable codes and we use it to find optimal codes (see Remark 2.9). Moreover, two of the consequences are the following: maximal ideals in group algebras are checkable and two-sided ideals C such that KG/C is a Frobenius algebra are checkable. In particular, the Jacobson radical of every group algebra is checkable.

In §3 we classify, in terms of the structure of the finite group G , all group algebras KG for which all right ideals are checkable, that is *code-checkable group algebras*. This is done in terms of the p -blocks of KG , with p the characteristic of the field K (see Theorem 3.1). As a consequence we get the following (see Corollary 3.2): KG is a code-checkable group algebra if and only if G is p -nilpotent with a cyclic Sylow p -subgroup, which happens if and only if all right ideals in the principal p -block of KG are checkable.

In §4 we shortly present the asymptotic performance of checkable codes. Together with the explicit construction of optimal codes in Remark 2.9, they seem to suggest that the family of checkable codes is worth further investigation. In particular, it is desirable to prove some bounds on the minimum distance for checkable codes and to introduce families of checkable codes with prescribed minimum distance (in analogy to BCH codes). Some results in this direction for dihedral codes have been given recently in [6]. Moreover, it would be extremely interesting to develop some fast decoding algorithms. These would be the minimum requirements for an effective use of these codes in cryptography and this will be the subject of further investigation.

2 Checkable ideals

Let A be a finite dimensional algebra over a field K . For any subset $C \subseteq A$, the *right annihilator* $\text{Ann}_r(C)$ is defined by

$$\text{Ann}_r(C) = \{a \mid a \in A, ca = 0 \text{ for all } c \in C\}.$$

Analogously, the *left annihilator* of C is given by

$$\text{Ann}_l(C) = \{a \mid a \in A, ac = 0 \text{ for all } c \in C\}.$$

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

Definition 2.1 A right ideal $I \leq A$ is called *checkable* if there exists an element $v \in A$ such that

$$I = \{a \mid a \in A, va = 0\} = \text{Ann}_r(v) = \text{Ann}_r(Av).$$

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.

Recall that a finite dimensional K -algebra A is called a *Frobenius algebra* if there exists a K -linear function $\lambda \in \text{Hom}_K(A, K)$ whose kernel contains no left or right ideal other than zero. In case $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$, we say that A is a *symmetric algebra*. Note that group algebras are Frobenius algebras; even more, they are symmetric algebras. In such algebras the annihilators of ideals satisfy the double annihilator property (see [16, Chap. VII]).

Proposition 2.2 (Double Annihilator Property) *Let A be a Frobenius algebra. If $I \leq A$ is a right ideal in A , then*

$$I = \text{Ann}_r(\text{Ann}_l(I)).$$

A similar equation holds for left ideals.

Corollary 2.3 *In a Frobenius algebra A a right (left) ideal I is checkable if and only if $\text{Ann}_l(I)$ ($\text{Ann}_r(I)$) is a principal left (right) ideal.*

Examples 2.4 a) Let $e = e^2$ be an idempotent in A . Then the ideal eA is checkable. This can be seen as follows. Obviously, $eA \leq \text{Ann}_r(A(1-e))$. Since any $0 \neq (1-e)b \in (1-e)A$ is not in $\text{Ann}_r(A(1-e))$ we have $eA = \text{Ann}_r(A(1-e))$.

b) If A is a semisimple algebra, then all right and left ideals are generated by idempotents. Thus all right and left ideals are checkable.

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

d) LCD group codes C (that is, codes for which $C \cap C^\perp = \{0\}$) are checkable since $C = eKG$ with a self-adjoint idempotent e , by [11].

As mentioned in the introduction, the group algebra KG carries a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. Thus, for any subset $C \subseteq KG$ the orthogonal space $C^\perp \leq KG$ is well defined. Observe that C^\perp is always a K -linear vector space.

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

Lemma 2.5 ([19]) *If C is a right ideal in KG , then $C^\perp = \widehat{\text{Ann}_l(C)}$. Similarly, for a left ideal C we have $C^\perp = \widehat{\text{Ann}_r(C)}$.*

Proof: We have $a = \sum_{g \in G} a_g g \in \widehat{\text{Ann}_l(C)}$ if and only if $\hat{a}ch = 0$, for all $c \in C$ 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 2.6 *For any right ideal $C \leq KG$ the following are equivalent.*

- a) C is checkable.
- b) C^\perp is a principal right ideal.

Proof: According to Corollary 2.3, C is checkable if and only if $\text{Ann}_l(C) = KGv$, for some $v \in KG$. Now Lemma 2.5 implies $C^\perp = \overline{\text{Ann}_l(C)} = \widehat{KGv} = \hat{v}KG$ and the proof is complete. \square

Examples 2.7 a) The binary extended Golay \mathcal{G}_{24} is a group code in \mathbb{F}_2S_4 , with S_4 the symmetric group on 4 letters (see [5]) and a group code in \mathbb{F}_2D_{24} , with D_{24} a dihedral group of order 24 (see [22]). Note that the binary extended Golay code is checkable in both algebras, by Theorem 2.6, since $\mathcal{G}_{24} = \mathcal{G}_{24}^\perp$ is constructed as a principal ideal in both cases. We would like to mention here that the extended ternary Golay code is not a group code according to ([28, Theorem 1.1]).

b) In [4] and [9] it is shown that the Reed-Muller code $\text{RM}_p(r, m)$ of order r and length p^m over the prime field \mathbb{F}_p can be constructed as $\text{RM}_p(r, m) = J^{N-r}$, with J the Jacobson radical of a group algebra \mathbb{F}_pG , for G an elementary abelian p -group of rank m and $N = m(p-1)$. For more details in what follows the reader may inquire [27]. Note that $(J^{N-r})^\perp = \text{RM}_p(r, m)^\perp = \text{RM}_p(N-r-1, m) = J^{r+1}$. Thus in order to check which Reed-Muller codes are checkable, we have to check which powers J^i are principal ideals. Clearly, if $m = 1$, then G is cyclic and therefore all ideals in \mathbb{F}_pG are principal. In case $m > 1$, apart from the full space \mathbb{F}_pG , only $\text{RM}_p(N-1, m) = J$ is checkable. This can be seen as follows. Clearly, $J^\perp = J^N = \text{RM}_p(0, m) = \mathbb{F}_p \sum_{g \in G} g$ is principal. Suppose that J^r is principal, for some $0 < r < N$. Thus J^r/J^{r+1} is principal as well, hence $J^r/J^{r+1} = (a + J^{r+1})\mathbb{F}_pG$. Moreover, J^r/J^{r+1} is a direct sum of trivial \mathbb{F}_pG -modules. Thus $(a + J^{r+1})g = a + J^{r+1}$, for all $g \in G$, which implies $\dim J^r/J^{r+1} = 1$. On the other hand, according to ([27, Proposition 7.2.3]) we have $\dim J^r/J^{r+1} > 1$. Thus only J^N is principal, which means, by Theorem 2.6, that $J = \text{RM}_p(N-1, m)$ is the only checkable Reed-Muller code apart from \mathbb{F}_pG .

Remark 2.8 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 [15]. Even more, there is a checkable [36, 28, 6] group code in $\mathbb{F}_5(C_6 \times C_6)$ and a checkable [72, 62, 6] 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 [15].

Remark 2.9 Theorem 2.6 provides an easy way to construct random checkable codes: it is enough to choose a random element in KG and then take the dual of the principal ideal generated by this element. Such a construction allows to do extensive searches for codes with the best known minimum distance (let us call them optimal codes, for simplicity).

Using MAGMA [8], we observed that there exists an optimal checkable code over \mathbb{F}_2 , for every group of order ≤ 100 , and an optimal checkable code over \mathbb{F}_3 and \mathbb{F}_4 , for every group of order ≤ 50 . For some groups we could find only trivial checkable codes, that is, of dimension 1. But in many cases the optimal checkable codes that we found have a higher dimension.

Let us give two examples: a binary and a ternary optimal code.

If

$$G = \langle a, b, c, d \mid a^8 = b^2 = c^2 = d^8 = 1, ab = ba, ac = ca, bc = cb, da = a^7cd, db = bd^5, dc = cd \rangle$$

(this is the 22nd group of order 64 in the library SmallGroups of MAGMA) and

$$u = 1 + a^6c + ad^4 + a^3 + a^7bd^4 + a^7cd^4 + a^7bc + a^7bcd^4 + d + a^6d + acbd + a^7d^5 \in \mathbb{F}_2G,$$

the dual of uKG is a $[64, 32, 12]$ code over \mathbb{F}_2 .

If

$$G = \langle a, b, c \mid a^4 = b^4 = c^3 = 1, ab = ba, ca = a^3b^3c, cb = ac \rangle \simeq (C_4 \times C_4) \rtimes C_3$$

and

$$v = 1 + 2b + a^3b^2 + 2a^3 + 2a^3b^3 + 2c^2b^3 + c^2ab^3 \in \mathbb{F}_3G,$$

the dual of vKG is a $[48, 15, 18]$ code over \mathbb{F}_3 .

Note that we can describe these codes very easily in terms of a check element, which is a generator of the dual. Here we chose a check element of minimum weight.

Recall that for a right KG -module M the dual KG -module M^* is defined by the K -vector space $M^* = \text{Hom}_K(M, K)$ on which G acts from the right by

$$(\varphi g)(m) = \varphi(mg^{-1}), \quad \text{for } \varphi \in M^*, g \in G, m \in M.$$

Remark 2.10 If C is checkable, then $C^* \cong KG/uKG$, for some $u \in KG$. This immediately follows from Theorem 2.6 applying $KG/C^\perp \cong C^*$ which has been proved in ([28, Proposition 2.3]).

Corollary 2.11 *Maximal ideals in KG are checkable.*

Proof: For a KG -module M , let $l(M)$ denote the composition length of M , i.e., the number of irreducible composition factors in a Jordan-Hölder series of M . Let $l(KG) = l$. Thus, if C is a maximal ideal in KG , then $l(C) = l(C^*) = l - 1$. Since $KG/C^\perp \cong C^*$ we get $l(C^\perp) = 1$. Hence C^\perp is a minimal ideal in KG . But minimal ideals in KG are principal. Hence the assertion follows by Theorem 2.6. \square

Minimal ideals are in general not checkable as the following result shows.

Proposition 2.12 *Let G be a finite p -group and $\text{char } K = p$. Then the minimal ideal $C = K \sum_{g \in G} g$ in KG is checkable if and only if G is cyclic.*

Proof: Let g_1, \dots, g_s be a minimal set of generators of G . Then $C^\perp = J(KG)$, where $J(KG)$ is the Jacobson radical of KG . One easily sees that $J(KG) = \sum_{i=1}^s (g_i - 1)K$ is principal if and only if $s = 1$, i.e., G is cyclic. Now the assertion follows, by Theorem 2.6. \square

Proposition 2.13 *Let C be a two-sided ideal in KG such that KG/C is a Frobenius algebra. Then C is checkable. In particular, in this case $J(KG)$ is checkable.*

Proof: Since KG/C is a Frobenius algebra, a result of Nakayama ([26, Theorem A]) directly implies $\text{Ann}_l(C) = KGa$, for some $a \in A$. Applying the double annihilator property, we get $C = \text{Ann}_r(KGa)$. Finally note that according to Wedderburn's Theorem $KG/J(KG)$ is a direct sum of full matrix algebras over extension fields of K , hence a Frobenius algebra. \square

3 Code-checkable group algebras

Let $KG = B_0 \oplus \dots \oplus B_s$ be a decomposition of KG into p -blocks B_i , with $\text{char } K = p$ and $B_i = f_i KG$ with block idempotents f_i . Recall that the B_i are 2-sided ideals and as such, indecomposable. They are uniquely determined by KG . Furthermore, the f_i are primitive idempotents in the center of KG . For more details the reader is referred to ([16, Chap. VII, Section 12]).

If $C \leq KG$ is a group code, then $C = Cf_0 \oplus \dots \oplus Cf_s$. One easily sees that C is checkable, i.e. $C = \text{Ann}_r(KGa)$, if and only if

$$Cf_i = \text{Ann}_r^{B_i}(KGf_i a) = \text{Ann}_r^{B_i}(B_i f_i a) = \{b \in B_i \mid (f_i a)b = 0\}.$$

This shows that C is checkable if and only if the block components Cf_i are checkable in B_i , for all i .

For an algebra A a right (left) A -module M is called *uniserial* if it has only one Jordan-Hölder series, or in other words M has only one composition series. Furthermore, the *projective cover* $P(M)$ of an irreducible A -module M is an indecomposable projective A -module which has a factor module isomorphic to M (see ([16, Chap.VII])).

Theorem 3.1 *Let $\text{char } K = p$ and let B be a p -block of KG . Then the following are equivalent.*

- a) *All right ideals in B are checkable.*

- b) All left ideals in B are principal.
- c) B contains only one irreducible left module M whose projective cover $P(M)$ is uniserial.
- d) The defect group of B is cyclic and B contains only one irreducible left module.

Proof: First note that B is a symmetric algebra ([16, Chap.VII, Section 11]).

a) \iff b) Let I be a right ideal of B . Then $I = \text{Ann}_r^B(Bv)$, for some $v \in B$, if and only if $\text{Ann}_l^B(I) = Bv$. Since Ann_r^B yields a bijection from the set of left ideals in B onto the set of right ideals in B we are done.

b) \implies c) Clearly, all left ideals are principal if and only if all right ideals are principal, just by applying the antiautomorphism $\hat{}$. Thus B is an artinian principal ideal ring and ([12, Theorem 2.1]) implies that all left B -modules are homogeneous uniserial. In particular all projective indecomposable left B -modules are uniserial.

Next we have to show that B contains only one irreducible left module. Let $J = J(B)$ denote the Jacobson radical of B and M be an irreducible left B -module with projective cover $P = P(M)$. Let X be the largest submodule of $\text{Soc}_l(P/J^k P)$ whose irreducible components are all isomorphic to M . Since the full preimage of this completely irreducible module is a left ideal in B , it is principal, hence a factor module of B . This implies that X is a factor module of B/JB , for all k . Doing this argument for a decomposition of B into a direct sum of projective indecomposable left modules and counting all composition factors in the regular left module B , we see that all composition factors of $P(M)$ are isomorphic to M .

Since the principal indecomposable modules in a block are connected, we get that B contains only one irreducible left module.

c) \implies b) Let I be a left ideal of B . If there exists $a \in B$ such that $I = Ba + JI$, then by Nakayama's Lemma $I = Ba$ and we are done. Thus it is sufficient to show that I/JI is generated by one element as a B -left module.

First note that the condition in c) obviously implies that there is also exactly one irreducible right module in B whose projective cover is uniserial. The corresponding irreducible right module is $\hat{M} = \text{Hom}_K(M, K)$ with the right structure

$$(\varphi g)(m) = \varphi(gm) \quad \text{for } \varphi \in \hat{M}, g \in G, m \in M.$$

Thus a result of Nakayama ([23, Theorem 17]) says that all left (and right) B -modules are uniserial. Clearly, I/JI is a B/J -submodule of $\text{Soc}(B/JI)$. Since B/JI is uniserial, we see that I/JI is a submodule of B/J . But all ideals in B/J are principal. Hence I/JI is generated by one element.

c) \implies d). Note that b) is exactly the statement in (1) of ([12, Theorem 2.1]) which is equivalent to (3). Thus all indecomposable left B -modules are submodules of B which means that B is of finite representation type. Now d) follows by ([29], Proposition 2.12.9).

d) \implies c) Again by ([29], Proposition 2.12.9), we know that B is of finite representation type. Following the proof of ([1, Section 18, Proposition 3]), we see that the projective

cover $P(M)$ of the unique irreducible left module M in B is uniserial. \square

As usual the *principal p -block* $B_0(G)$ of G is the block which contains the trivial KG -module. Furthermore, remember from finite group theory that a group G is called *p -nilpotent* if G has a normal p' -subgroup $N = O_{p'}(G)$ such that the factor group G/N is a p -group, i.e., G/N is isomorphic to a Sylow p -subgroup of G .

Corollary 3.2 *Let $\text{char } K = p$ and let $B_0(G)$ be the principal p -block of KG . The following are equivalent.*

- a) G is p -nilpotent with a cyclic Sylow p -subgroup.
- b) KG is a code-checkable group algebra.
- c) All right ideals in $B_0(G)$ are checkable.

Proof: a) \implies b) By ([16, Chap. VII, Theorem 14.9]), each block has exactly one irreducible left module. Since the principal block $B_0(G)$, which contains the trivial module 1_G , is isomorphic to $KG/O_{p'}(G) \cong KT$, with T a Sylow p -subgroup of G , we get that $B_0(G) = P(1_G) \cong KT$ is uniserial. If M is any irreducible KG -module, then $P(M)$ is a factor module of $P(1_G) \otimes M$, which is uniserial. Thus $P(M)$ is uniserial as well. This shows that all blocks of KG satisfy condition c) of Theorem 3.1, hence condition a), which means that KG is code-checkable.

b) \implies c) This is obvious.

c) \implies a). Note that according to Theorem 3.1 the condition in c) implies that $B_0(G)$ contains only one irreducible left module, namely the trivial module 1_G , and $P(1_G)$ is uniserial. Thus again by ([16, Chap. VII, Theorem 14.9]), the group G must be p -nilpotent. In particular, if T is a Sylow p -subgroup of G , then $B_0(G) \cong KG/O_{p'}(G) \cong KT \cong P(1_G)$ forces T to be cyclic. \square

Observe that the equivalence of a) and b) is already contained in an early paper of Passman ([25, Theorem 4.1]).

Remark 3.3 In [18] the authors study group codes in code-checkable group algebras KG , for G abelian, i.e., $G = A \times T$, with A an abelian p' -group and T a cyclic p -group, if $p = \text{char } K$. In particular, a characterization and enumeration of Euclidean self-dual and self-orthogonal group codes is given.

4 Asymptotically good classes

In the literature there are many papers which prove that particular classes of codes are asymptotically good. In [2] the authors investigated binary group codes over dihedral

groups of order $2m$, for m odd. Their results in Section 4 show that the class of group codes over these groups is asymptotically good. Applying field extensions as in ([13], Proposition 12) this result can be extended to any field of characteristic 2. These methods have been generalized to any finite field in odd characteristic [7]. Thus we have the following result.

Theorem 4.1 ([2], [7]) *For any finite field K the class of group codes in code-checkable group algebras is asymptotically good.*

References

- [1] J.L. ALPERIN, Local representation theory. Cambridge University Press, Cambridge 1986.
- [2] L.M.J. BAZZI AND S.K. MITTER, Some randomized code constructions from group actions. *IEEE Trans. Inform. Theory* 52 (2006), 3210-3219.
- [3] T.P. BERGER, P.L. CAYREL, P. GABORIT AND A. OTMANI, Reducing key length of the McEliece cryptosystem. In *International Conference on Cryptology in Africa*, Springer, Berlin, Heidelberg (2009), 77–97.
- [4] S.D. BERMAN, On the theory of group codes. *Kibernetika* 3 (1967), 31-39.
- [5] F. BERNHARDT, P. LANDROCK AND O. MANZ, The extended Golay codes considered as ideals. *J. Comb. Theory, Series A* 55 (1990), 235-246.
- [6] M. BORELLO AND A. JAMOUS, Dihedral codes with prescribed minimum distance. To appear in *Lecture Notes in Comput. Sci.*, 2021.
- [7] M. BORELLO AND W. WILLEMS, Group codes are asymptotically good. *Finite Fields Appl.* 68 (2020), 101738.
- [8] W. BOSMA, J. CANNON AND C. PLAYOUST, The Magma algebra system I: The user language. *J. Symbol. Comput.* 24 (1997), 235–265.
- [9] P. CHARPIN, Une généralisation de la construction de Berman des codes de Reed-Muller p -aire, *Comm. Algebra* 16 (1988), 2231-2246.
- [10] J.H. CONWAY, S.J. LOMONACO JR and N.J.A. SLOANE, A $[45, 13]$ code with minimal distance 16. *Discrete Math.* 83 (1990), 213-217.
- [11] J. DE LA CRUZ AND W. WILLEMS, On group codes with complementary duals. *Des. Codes and Cryptogr.* 86 (2018), 2065-2073.
- [12] D. EISENBUD AND P. GRIFFITH, The structure of serial rings. *Pacific J. Math.* 36 (1971), 109-121.

- [13] F. FALDUM AND W. WILLEMS, Codes of small defect. *Des. Codes and Cryptogr.* 10 (1997), 341-350.
- [14] A. VOM FELDE, A new presentation of Cheng-Sloane's $[32, 17, 8]$ -code. *Arch. Math.* 60 (1993), 508-511.
- [15] M. GRASSL, Bounds on the minimum distance of linear codes. Online <http://www.codetables.de>.
- [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](https://arxiv.org/abs/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] F.J. MACWILLIAMS AND N.J.A. SLOANE, The theory of error-correcting codes. (Vol. 16), Elsevier, (1977).
- [21] R. J. MCELIECE, A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report 42-44*, (1978), 114-116.
- [22] I. MCLOUGHLIN AND T. HURLEY, A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory* 54 (2008), 4381-4383.
- [23] T. NAKAYAMA, On Frobeniusean algebras II. *Ann. of Math.* 42 (1941), 1-21.
- [24] H. NIEDERREITER, Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory. Problemy Upravleniya i Teorii Informacii* 15, (1986), 159-166.
- [25] D.S. PASSMAN, Observations on group rings. *Comm. Algebra* 5 (1977), 1119-1162.
- [26] Y. TSUSHIMA, On the annihilator ideals of the radical of a group algebra. *Osaka J. Math.* 8 (1971), 91-97.
- [27] W. WILLEMS, Codierungstheorie. de Gruyter, Berlin 1999.
- [28] W. WILLEMS, A note on self-dual group codes. *IEEE Trans. Inform. Theory* 48 (2007), 3107-3109.
- [29] A. ZIMMERMANN, Representation Theory. Springer, Heidelberg 2014.