Acta Mathematica et Informatica Universitatis Ostraviensis

Ute Vellbinger

On the minimum distance of ideals in group algebras

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 4 (1996), No. 1, 97--103

Persistent URL: `http://dml.cz/dmlcz/120508`

Terms of use:

© University of Ostrava, 1996

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://project.dml.cz`

On the minimumdistance of ideals in group algebras

UTE VELLBINGER

Abstract. Ideals, which are generated by idempotent elements in a group algebra $\mathbb{F}G$, where $\mathbb{F}$ is a finite field and G is a finite group, are considered as a special kind of codes. For $\mathbb{F} = \mathbb{F}_2$ we give an algorithm which only uses multiplication in the group G, that decides whether the minimumdistance of C is at least 3 or not.

1991 Mathematics Subject Classification: 94B05, 94B60

1 Introduction

Let $\mathbb{F}$ be a finite field, G a finite group with n elements and $\mathbb{F}G$ the corresponding group algebra. In generalization of cyclic codes which are ideals in group algebras corresponding to cyclic groups we want to look at ideals in any finite group algebra from the point of view of coding theory. If $G = \{g_1, \ldots, g_n\}$ than

$$\mathbb{F}G \to \mathbb{F}^n, \quad \sum_{i=1}^{n} x_i g_i \mapsto (x_1, \ldots, x_n)$$

is a vectorspace-isomorphism, so the ideas of length, dimension and minimumdistance stay the same. Thus the *length* n of an ideal C in $\mathbb{F}G$ is exactly the order of G, the *dimension* of the subspace C and for the *minimumdistance* d of C we get as usual:

$$d = \min\{\mathrm{wt}(c) | c \in C \setminus \{0\}\};$$

$\mathrm{wt}(c) = |\{i \mid 1 \leq i \leq n, c_i \neq 0\}|$ for $c = \sum_{i=1}^{n} c_i g_i \in \mathbb{F}G$ is called the *weight* of c.

We will restrict our attention to those ideals which are principal ideals generated by an idempotent element $e \in \mathbb{F}G$, i. e. $e * e = e$, where $*$ denotes the multiplication in $\mathbb{F}G$.

In the case that the characteristic p of $\mathbb{F}$ is prime to the order n of G this is no restriction at all, which follows from the theorem of Maschke [4].

We will use the extra structure of an ideal to get more information on the minimumdistance and we will give a criterion on the coefficients of a generating idempotent that helps to decide whether an ideal has minimumdistance at least 3 or not.

2 Preliminary results

2.1 Lemma. *Let $0 \neq C \subsetneq \mathbb{F}G$ be an (left-) ideal and let d denote the minimumdistance of C. Then $d \geq 2$.*

PROOF: Let us assume that C contains a word of weight 1. Then there exists an element $g \in G$ such that $g \in C$. But g is a unit in $\mathbb{F}G$, so $C = \mathbb{F}G$. □

The following Lemma shows that the information about dimension and minimumdistance is stored up in an idempotent generator.

2.2 Lemma. *Let $e \in \mathbb{F}G$ be an idempotent and let $C = \langle e \rangle$ be the (left-) ideal generated by e. For $i = 1, \ldots, n$ consider $g_i * e$ as an element of $\mathbb{F}^n$ and define the matrix*

$$M_e := \begin{pmatrix} g_1 * e \\ g_2 * e \\ \vdots \\ g_n * e \end{pmatrix} \in \mathbb{F}^{n \times n}$$

Then C is isomorphic to the image of M_e, i. e.

$$C = \{(x_1, \ldots, x_n) \cdot M_e \,|\, (x_1, \ldots, x_n) \in \mathbb{F}^n\}$$

and

$$H_e := (I_n - M_e)^t \in \mathbb{F}^{n \times n}$$

is a parity-check-matrix for the code C, i. e.
$C = \{(z_1, \ldots, z_n) \in \mathbb{F}^n \,|\, H_e(z_1, \ldots, z_n)^t = 0\}$.

PROOF: The first assumption follows immediately because $C = \{x * e \,|\, x \in \mathbb{F}G\}$. Using the fact that e is an idempotent yields:

$$\begin{aligned} C &= \{z \in \mathbb{F}G \,|\, z * e = z\} = \\ &= \{z \in \mathbb{F}^n \,|\, z \cdot M_e = z\} = \\ &= \{z \in \mathbb{F}^n \,|\, (I_n - M_e)^t z^t = 0\}. \end{aligned}$$

□

2.3 Remark. It is a wellknown result that $\dim C = n\text{-rank } H_e$ and that the minimumdistance of C is d iff every $d-1$ columns of H_e are linearly independent and there are d columns of H which are linearly dependent. Although the special structure of this parity-check-matrix gives some facilitation, this criterion is somewhat unhandy.

2.4 Remarks.

a) For $x = \sum_{i=1}^{n} x_i g_i \in \mathbb{F}G$ define $\overline{x} := \sum_{i=1}^{n} x_i g_i^{-1}$.
The mapping $\overline{} : \mathbb{F}G \to \mathbb{F}G$, $x \mapsto \overline{x}$, is a (vectorspace-) isomorphism with $\overline{\overline{x}} = x$ and $\overline{x * y} = \bar{y} * \bar{x}$ for all $x, y \in \mathbb{F}G$.

b) If $e \in \mathbb{F}G$ is idempotent, then so are $\bar{e}$, $1 - e$, $1 - \bar{e}$.

c) If $e \in \mathbb{F}G$ is central, i.e. $e * x = x * e$ for all $x \in \mathbb{F}G$, then so are $\bar{e}$, $1 - e$, $1 - \bar{e}$.

In the following we are not interested in C itself but also in the annihilator $\mathrm{Ann}(C) := \{x \in \mathbb{F}G \mid x * c = 0 \text{ for all } c \in C\}$ and the dual code $C^{\perp} = \{x \in \mathbb{F}G \mid \langle x, c\rangle = 0 \text{ for all } c \in C\}$, where $\langle x, c\rangle = \langle \sum_{i=1}^{n} x_i g_i, \sum_{i=1}^{n} c_i g_i\rangle := \sum_{i=1}^{n} x_i c_i$.

2.5 Lemma. *Let $e \in \mathbb{F}G$ e a central idempotent. For $C = \langle e\rangle$ we get:*

$$\mathrm{Ann}(C) = \langle 1 - e\rangle \textit{ and } C^{\perp} = \langle 1 - \bar{e}\rangle.$$

These are wellknown results, see for example [6] and [7].

3 Some estimations for the minimumdistance of ideals

3.1 Definition.

a) Let $C \subset \mathbb{F}G$ be a (left-) ideal. Then C is called *dividing* if
$K(C) := \{g \in G \mid \text{there is } \alpha_g \in \mathbb{F} : c * g = \alpha_g c \text{ for all } c \in C\} \neq \{1\}$.

b) Let $e \in \mathbb{F}G$. Then e is called *dividing*, if the corresponding principal (left-) ideal $C = \langle e\rangle$ is dividing.

3.2 Remarks.

i) If $C \subset \mathbb{F}G$ is dividing, then C defines an equivalence-relation on G ($g \sim h \Leftrightarrow c * g = c * h$ for all $c \in C$) that divides G into non-trivial equivalence-classes.

ii) If $e \in \mathbb{F}G$ is dividing and $C = \langle e \rangle$ then

$$K(C) = \{g \in G \,|\, \text{there is } \alpha_g \in \mathbb{F} : e * g = \alpha_g e\}.$$

The subgroup $K(C)$ is also called monomial kernel [2] and we have the following result:

3.3 Theorem. *(Damgård, Landrock) Let $C \subset \mathbb{F}G$ be an ideal, $0 \neq C \neq \mathbb{F}G$. Then the minimumdistance d of C is at least 3 if and only if $K(\mathrm{Ann}(C)) = \{1\}$.*

PROOF: See [2]. □

3.4 Corollary. *Let $\mathbb{F} = \mathbb{F}_2$ and let $e \in \mathbb{F}_2G$ be a central idempotent, $C = \langle e \rangle$ with minimumdistance d. Then $d \geq 3$ if and only if $1 - e$ is not dividing, i. e. $\{g \in G \,|\, (1-e) * g = 1 - e\} = \{1\}$.*

3.5 Theorem. *Let G be a group whose order is a prime number $p > 2$. Then*

$$e_G := \sum_{g \in G} g \in \mathbb{F}_2 G$$

is the only dividing element in $\mathbb{F}_2G \setminus \{0\}$. e_G is also idempotent and central. So every ideal $0 \neq C \subsetneq \mathbb{F}_2G$, $C \neq \langle 1 + e_G \rangle$, has minimumdistance at least 3.

PROOF: Let $e \in \mathbb{F}_2G$ be dividing and $C = \langle e \rangle$. Then $K(C) \neq \{1\}$ is a subgroup of G hence $K(C) = G$, since the order of G is a prime. So for every $g \in G$

$$e = \sum_{h \in G} e_h h = e * g^{-1} = \sum_{h \in G} e_h h g^{-1} = \sum_{j \in G} e_{jg} j$$

and therefore

$$e_1 = e_g \text{ for all } g \in G \text{ and this yields } e = 0 \text{ or } e = e_G.$$

That e_G is dividing, idempotent and central follows immediately and the last assumption is a consequence of Corollary 3.4 and of the theorem of Maschke, since the order of G is an odd number. □

3.6 Lemma. *Let $e = \sum_{j \in G} e_j j \in \mathbb{F}_2G$ be idempotent and central and let $\mathrm{supp}(e) := \{j \in G \,|\, e_j \neq 0\}$ be the support of e.*

First case: $e_1 = 1$. *Then we have for* $g \in G$*:*

$$(1-e)*g = 1-e \quad \Leftrightarrow \quad g, g^{-1} \notin \operatorname{supp}(e) \text{ and } \{jg \mid j \in \operatorname{supp}(e) \setminus \{1\}\} = \operatorname{supp}(e) \setminus \{1\}$$

Second case: $e_1 = 0$. *Then we have for* $g \in G$*:*

$$(1-e)*g = 1-e \quad \Leftrightarrow \quad g, g^{-1} \notin \operatorname{supp}(e) \text{ and } \{jg \mid j \in \operatorname{supp}(e) \setminus \{g^{-1}\}\} = \operatorname{supp}(e) \setminus \{g\}$$

PROOF: $(1-e)*g = 1-e \Leftrightarrow (1-e)*g^{-1} = 1-e \Leftrightarrow e_g 1 - (1-e_1)g^{-1} - \sum_{j\in G\setminus\{1,g^{-1}\}} e_{jg} j = (1-e_1)1 - e_{g^{-1}}g^{-1} - \sum_{j\in G\setminus\{1,g^{-1}\}} e_j j$. If $e_1 = 1$ this is equivalent to $e_g = e_{g^{-1}} = 0$ and $e_{jg} = e_j$ for all $j \in G \setminus \{1, g^{-1}\}$. If $e_1 = 0$ this is equivalent to $e_g = e_{g^{-1}} = 1$ and $e_{jg} = e_j$ for all $j \in G \setminus \{1, g^{-1}\}$. □

Lemma 3.6 gives rise to the following algorithms, which only uses the multiplication of the group G:

3.7 Algorithm I. Let $e = \sum_{j\in G} e_j j \in \mathbb{F}_2 G$ be idempotent and central with $e_1 = 1$. Let $C := \langle e \rangle$ and let d denote the minimumdistance of C.

First step:

$$\begin{aligned} G_1 &:= G \setminus \operatorname{supp}(e). \\ G_2 &:= \{g \in G_1 \mid g^{-1} \in G_1\}. \end{aligned}$$

If $G_2 = \emptyset$, then $d \geq 3$ END
If $G_2 \neq \emptyset$, then:
Second step: $\operatorname{supp}(e) \setminus \{1\} =: \{j_1, \dots, j_b\}$
For $g \in G_2$ and $\beta = 1$ compute $j_\beta g$.
If $j_\beta g \notin \operatorname{supp}(e) \setminus \{1\}$, then start second step for next $g \in G_2$.
If $j_\beta g \in \operatorname{supp}(e) \setminus \{1\}$, the compute $j_{\beta+1} g$.

$$G_3 := \{g \in G_2 \mid j_\beta g \in \operatorname{supp}(e) \setminus \{1\} \text{ for all } \beta = 1, \dots, b\}$$

If $G_3 = \emptyset$, then $d \geq 3$.
If $G_3 \neq \emptyset$, then $d \leq 2$. END

3.8 Algorithm II. Let element $e = \sum_{j\in G} e_j j \in \mathbb{F}_2 G$ be idempotent and central with $e_1 = 0$. Let $C := \langle e \rangle$ and denote the minimumdistance of C by d.

First step:

$$\begin{aligned} G_1 &:= \operatorname{supp}(e). \\ G_2 &:= \{g \in \operatorname{supp}(e) \mid g^{-1} \in G_1\}. \end{aligned}$$

If $G_2 = \emptyset$, then $d \geq 3$. END
If $G_2 \neq \emptyset$, then:
Second step: $\text{supp}(e) \setminus \{g^{-1}\} := \{j_1, \ldots, j_b\}$
For $g \in G_2$ and $\beta = 1$ compute $j_\beta g$.
If $j_\beta g \notin \text{supp}(e) \setminus \{g\}$, then start second step for next $g \in G_2$.
If $j_\beta g \in \text{supp}(e) \setminus \{g\}$, then compute $j_{\beta+1} g$.

$$G_3 := \{g \in G_2 \mid j_\beta g \in \text{supp}(e) \setminus \{g\} \text{ for all } \beta = 1, \ldots, b\}.$$

If $G_3 = \emptyset$, then $d \geq 3$.
If $G_3 \neq \emptyset$, then $d \leq 2$. END

3.9 Lemma. *Let $e \in \mathbb{F}_2 G$ be an idempotent, central and dividing element. Then:*

i) The minimumdistance of $C = \langle e \rangle$ is at least 3.

ii) The minimumdistance of $C^\perp = \langle 1 + \bar{e} \rangle$ is at most 2.

iii) The minimumdistance of $\text{Ann}(C) = \langle 1 + e \rangle$ is at most 2.

This is a consequence of 3.4 and the following Lemma:

3.10 Lemma. *Let $e \in \mathbb{F}_2 G$ be an idempotent, central element. Then*

a) e is dividing iff $\bar{e}$ is dividing.

b) If e is dividing, then $1 + e$ is not dividing.

PROOF:

a)

$$\begin{aligned} e \text{ dividing} &\Leftrightarrow e * g = e \text{ for some } g \in G \setminus \{1\} \\ &\Leftrightarrow \overline{e * g} = \bar{e} \text{ for some } g \in G \setminus \{1\} \\ &\Leftrightarrow \bar{e} * g = \bar{e} \text{ for some } g \in G \setminus \{1\} \\ &\Leftrightarrow \bar{e} \text{ is dividing.} \end{aligned}$$

b) Let e be dividing and assume that $1 - e$ is also dividing. Then there exists some $g \in G \setminus \{1\}$ with $(1 - e) * g = 1 - e$, so $g - 1 = e * (g - 1)$ and that means $g - 1 \in \langle e \rangle$ in contradiction to 3.4.

□

References

[1] Busazi, K., Petho, A., Lakatos, P., *Code distances of one class of group codes*, Probl. Inf. Transm. **17** (1982), 149–156.

[2] Damgård, I., Landrock, P., *Ideals and codes in group algebras*, Aarhus Universitet, Preprint Series 1986/87, No. 12, Oktober 1986.

[3] Karpilovsky, G., *Commutative group algebras*, Marcel Dekker Inc., New York/Basel, 1983.

[4] Kasch, F., *Moduln und Ringe*, Teubner, Stuttgart, 1977.

[5] Landrock, P., *Finite group algebras and their modules*, Cambridge University Press, Cambridge, 1983.

[6] MacWilliams, F. J., *Binary codes which are ideals in the group algebra of an abelian group*, The Bell System Technical Journal (Juli–August 1970), 987–1011.

[7] MacWilliams, F. J., *Codes and ideals in group algebras*, in Bose and Dowling: Combinatorial Math. and its Applications, University of North Carolina Press (1969), 317–328.

[8] MacWilliams, F. J., Sloane, N. J. A., *The theory of error-correcting codes*, North-Holland, Amsterdam/New York/Oxford/Tokyo, 1977.

[9] Vellbinger, U., *Ideale in Gruppenalgebren in der Codierungstheorie*, Thesis, Duisburg, 1995.

Address: Gerhard–Mercator–Universität, Gesamthochschule Duisburg, Fachbereich 11–Mathematik, Lotharstr. 65, 47057 Duisburg, Germany, e-mail: vellbinger@math.uni-duisburg.de