

This is the peer reviewed version of the following article:

On ideals in group algebras: An uncertainty principle and the Schur product / Borello, M.; Willems, W.; Zini, G.. - In: FORUM MATHEMATICUM. - ISSN 0933-7741. - 34:5(2022), pp. 1345-1354. [10.1515/forum-2022-0064]

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

25/04/2024 18:03

(Article begins on next page)

On ideals in group algebras: an uncertainty principle and the Schur product

Martino Borello¹, Wolfgang Willems², and Giovanni Zini³

¹Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA,
Université Sorbonne Paris Nord, CNRS, UMR 7539, France

²Otto-von-Guericke Universität, Magdeburg, Germany and Universidad del Norte,
Barranquilla, Colombia

³Università degli Studi di Modena e Reggio Emilia, Modena, Italy

Abstract

In this paper we investigate some properties of ideals in group algebras of finite groups over fields. First, we highlight an important link between their dimension, their minimal Hamming distance and the group order. This is a generalized version of an uncertainty principle shown in 1992 by Meshulam. Secondly, we introduce the notion of the Schur product of ideals in group algebras and investigate the module structure and the dimension of the Schur square. We give a structural result on ideals that coincide with their Schur square, and we provide conditions for an ideal to be such that its Schur square has the projective cover of the trivial module as a direct summand. This has particularly interesting consequences for group algebras of p -groups over fields of characteristic p .

Keywords: group algebra; Hamming distance; uncertainty principle; Schur product.

MSC2020 classification: 20C05, 94B60.

Introduction

Studying the algebraic structure of group algebras KG in positive characteristic p (which reflects many p -local properties of the underlying group G) means to a large extent studying its ideals. In this pure representation theoretical context the Hamming metric, which is naturally given on KG and has a coding theoretical meaning, is not often considered. In this paper we consider ideals in group algebras KG of finite groups G over fields K , endowed with the Hamming metric of KG . Such ideals are classically named group codes, and more specifically G -codes; see [17]. From a coding theoretical point of view, it is meaningful to look for G -codes \mathcal{C} with a large K -dimension $\dim \mathcal{C}$ and a large minimum (Hamming) distance $d(\mathcal{C})$. Several remarkable codes can be detected as ideals in group algebras; for instance, this holds for the extended binary Golay code [5] - which is related to the Leech lattice, to the sporadic simple group M_{24} and to various design-theoretic objects - and for binary Reed-Muller codes [3] - which have strong connections to geometry. Moreover, G -codes over K have been proved to be asymptotically good for any finite field K , see [2, 9]: there exist infinitely many groups G (of growing order) and ideals $\mathcal{C} \leq KG$ with both large dimension and large minimum distance (where “large” means linear in the order of G). The algebraic structure of G -codes has been intensively studied; see e.g. [4, 6, 8, 14] and the references therein. Yet, there are still many open questions about their coding theoretical properties. After recalling some notations and preliminary results in Section 1, the aim of this paper is twofold: Section 2 deals with a bound on the coding-theoretical parameters of a G -code, while Section 3 investigate the structure of

G -codes in relation to their Schur product. We now give some more details on Sections 2 and 3.

In Section 2, we generalize in Theorem 2.4 an uncertainty principle proved by Meshulam [18] to K -valued functions over G for any field K and finite group G , and we put it in the context of coding theory. Uncertainty principles for functions f over abelian groups are classical harmonic analytic results assuring that either f or its Fourier transform \hat{f} has large support; see [13, 23]. Recently, Evra, Kowalski and Lubotzky [11] have started to build a bridge between some uncertainty principles and the goodness of cyclic codes, which are indeed ideals in the group algebra over a cyclic group. The paper [7] pushed forward with this link in relation to MDS codes and the BCH bound, while Feng, Hollmann and Xiang [12] extended the investigation to abelian groups. As a consequence of an uncertainty principle, we prove in Corollary 2.6 the bound

$$d(\mathcal{C}) \cdot \dim \mathcal{C} \geq |G| \tag{1}$$

for any G -code \mathcal{C} . Up to our knowledge, this is the first bound of this shape on the parameters of a general G -code. Note that, for certain families of linear codes in K^n , interesting results on the product of the minimum distance and the dimension have been recently obtained in [1]. The rest of Section 2 thoroughly describes the structure of G -codes attaining equality in (1).

In Section 3, we define the Schur product in a group algebra KG componentwise, in analogy with the Schur - or Hadamard - product of matrices, which is object of the celebrated Schur product theorem on positive definite matrices [21]. We then define the Schur product of G -codes \mathcal{C} as the K -linear subspace spanned by the Schur product of their elements, and investigate it as a G -code itself. In particular we focus on the dimension of the Schur square $\mathcal{C} * \mathcal{C}$, boosted by two main reasons. At first, as highlighted in [20], the dimension of $\mathcal{C} * \mathcal{C}$ is related to the Hilbert sequence and the Castelnuovo-Mumford regularity of \mathcal{C} , which are defined via the classical correspondence between k -dimensional linear codes over K and point multisets in the $(k - 1)$ -dimensional projective space over K . Secondly, as noticed in [10], the dimension of the Schur square of structured codes \mathcal{C} can be quite small, in contrast to random codes, and this has relevant consequences for the security of code-based cryptosystems related to \mathcal{C} . Section 3 considers the module structure of the Schur square $\mathcal{C} * \mathcal{C}$ of G -codes \mathcal{C} . Theorem 3.5 is a structure result in the case $\mathcal{C} * \mathcal{C} = \mathcal{C}$. Then we show in Theorem 3.7 that the projective cover of the trivial module is a direct summand of $\mathcal{C} * \mathcal{C}$ whenever \mathcal{C} is not self-orthogonal. Finally, we explore some consequences of Theorem 3.7, with a particular attention on the case of p -groups in characteristic p , when non-self-orthogonal G -codes have Schur square of maximum dimension.

1 Preliminary results

Throughout the paper, the following notations are used:

- K is a field, and in particular \mathbb{F}_q is the finite field of order q .
- n is a positive integer, K^n is the n -dimensional coordinate K -vector space, and we write $V \leq K^n$ for K -linear subspaces V of K^n .
- G is a finite group, p is a prime number, $|G|_p \geq 1$ is the largest power of p dividing $|G|$, and we write $H \leq G$ for subgroups H of G .
- $KG = \left\{ \sum_{g \in G} a_g g \mid a_g \in K \right\}$ is the group algebra of G over K , and we write $\mathcal{C} \leq KG$ for *right* ideals \mathcal{C} of KG .
- Functions from G to K are identified with elements of KG via the correspondence between $f : G \rightarrow K$ and $\sum_{g \in G} f(g)g$.
- K_G is the trivial KG -module.

- If $H \leq G$ and M is a KH -module, then M^G is the *induced* KG -module, which is defined up to isomorphism as $M^G = \bigoplus_{i=1}^s M g_i$, where $\{g_1, \dots, g_s\} \subseteq G$ is a right transversal of H in G .
- When considering trivial KH -modules with $H \leq G$, or KG -modules induced by KH -modules, or projective covers of KH -modules, we always identify them with the corresponding isomorphic right ideals of KG .

For other classical results on group algebras and its ideals, we refer the reader to [16] or [15, Chapter 16].

1.1 Linear codes in K^n

We recall some basic notions on linear codes in K^n , i.e. on linear subspaces endowed with the Hamming metric; see [15, Chapter 1].

The *support* and the *weight* of an element $v = (v_1, \dots, v_n) \in K^n$ are defined as

$$\text{supp}(v) := \{i \in \{1, \dots, n\} \mid v_i \neq 0\} \subseteq \{1, \dots, n\} \text{ and } \text{wt}(v) := |\text{supp}(v)| \in \{0, \dots, n\}$$

respectively, and the *Hamming distance* on K^n as

$$d(v, v') := |\text{supp}(v - v')|, \quad \text{for any } v, v' \in K^n.$$

A *linear code* \mathcal{C} of length n over the alphabet K is a K -linear subspace of K^n , endowed with the Hamming metric, and the elements of \mathcal{C} are called *codewords*. The *minimum distance* $d(\mathcal{C})$ of \mathcal{C} is defined as the minimum Hamming distance between two distinct codewords, and coincides with the minimum weight of a nonzero codeword:

$$d(\mathcal{C}) := \min\{d(c, c') \mid c, c' \in \mathcal{C}, c \neq c'\} = \min\{\text{wt}(c) \mid c \in \mathcal{C}, c \neq 0\}.$$

If $d = d(\mathcal{C})$ and $k = \dim(\mathcal{C})$, we denote the parameters of \mathcal{C} by $[n, k, d]$. A *generator matrix* of \mathcal{C} is a $k \times n$ matrix M over K whose rows form a basis of \mathcal{C} . An *information set* for \mathcal{C} is a k -subset S of $\{1, \dots, n\}$ such that the columns of M indexed by S are linearly independent (note that the property of being an information set does not depend on M).

An $[n, k, d]$ -linear code \mathcal{C}' over K is *permutation equivalent* to \mathcal{C} if there exists an $n \times n$ permutation matrix P such that $M \cdot P$ is a generator matrix of \mathcal{C}' ; equivalently, if there exists a permutation σ in the symmetric group S_n such that

$$\mathcal{C}' = \sigma(\mathcal{C}) := \{(c_{\sigma(1)}, \dots, c_{\sigma(n)}) \in K^n \mid (c_1, \dots, c_n) \in \mathcal{C}\}.$$

Notice that permutation equivalence preserves the parameters of a code. The *permutation automorphism group* $\text{PAut}(\mathcal{C})$ of \mathcal{C} is the stabilizer of \mathcal{C} in the action of S_n by permutation equivalence, i.e. $\text{PAut}(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}$.

With respect to the standard inner product $\langle (v_1, \dots, v_n), (v'_1, \dots, v'_n) \rangle := \sum_{i=1}^n v_i v'_i$ on K^n we consider the *dual code* $\mathcal{C}^\perp = \{v \in K^n \mid \langle v, c \rangle = 0 \text{ for all } c \in \mathcal{C}\}$ of \mathcal{C} . The code \mathcal{C} is called *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

Definition 1.1. The *Schur product* in K^n is the bilinear map $K^n \times K^n \rightarrow K^n$ defined by

$$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n) \in K^n, \quad \text{for any } a_i, b_i \in K,$$

and the Schur product of two linear codes $\mathcal{C}, \mathcal{C}' \leq K^n$ is defined as the linear code

$$\mathcal{C} * \mathcal{C}' = \langle c * c' \mid c \in \mathcal{C}, c' \in \mathcal{C}' \rangle_K \leq K^n.$$

Since $\mathcal{C} * \mathcal{C}' = \langle c * c' \mid c \in \mathcal{C}, c' \in \mathcal{C}' \rangle_K$ whenever $\mathcal{C} = \langle B \rangle_K$ and $\mathcal{C}' = \langle B' \rangle_K$, we have

$$\dim \mathcal{C} * \mathcal{C}' \leq \min \left\{ n, \dim \mathcal{C} \cdot \dim \mathcal{C}' - \binom{\dim \mathcal{C} \cap \mathcal{C}'}{2} \right\},$$

and in particular

$$\dim \mathcal{C} * \mathcal{C} \leq \min \left\{ n, \binom{\dim \mathcal{C} + 1}{2} \right\}. \quad (2)$$

By [19, Proposition 5.2], if \mathcal{C} is chosen at random and $n > \binom{\dim \mathcal{C} + 1}{2}$, then $\dim \mathcal{C} * \mathcal{C} = \binom{\dim \mathcal{C} + 1}{2}$ almost surely. This is not the case for other algebraically structured codes, such as Reed-Solomon codes; see [24, Section 5].

1.2 G -codes in KG

In analogy to K^n , we endow also the group algebra KG with the Hamming metric as follows. The *support* and the *weight* of an element $f = \sum_{g \in G} a_g g \in KG$ ($a_g \in K$) are defined as $\text{supp}(f) := \{g \in G \mid a_g \neq 0\} \subseteq G$ and $\text{wt}(f) := |\text{supp}(f)| \in \{0, \dots, |G|\}$ respectively. The *Hamming distance* between two elements $f, f' \in KG$ is $d(f, f') := |\text{supp}(f - f')|$.

Definition 1.2. [15, Chapter 16] A G -code \mathcal{C} over the alphabet K is a *right* ideal of KG , endowed with the Hamming metric. The *length* of \mathcal{C} is $|G|$, the *dimension* of \mathcal{C} is its dimension as a K -linear subspace of KG , and its *minimum distance* is

$$d(\mathcal{C}) := \min\{d(c, c') \mid c, c' \in \mathcal{C}, c \neq c'\} = \min\{\text{wt}(c) \mid c \in \mathcal{C}, c \neq 0\}.$$

We remark here that the choice of *right* ideals as G -codes is a convention that does not affect the validity of the correspondent results for left ideals.

By choosing an ordering on G , say $G = \{g_1, \dots, g_n\}$ with $n = |G|$, we may define a *standard* K -linear isomorphism $\varphi : KG \rightarrow K^n$ by $\sum_{i=1}^n a_i g_i \mapsto (a_1, \dots, a_n)$. We stress that such a standard isomorphism is unique up to the choice of the ordering. The following characterization holds, and allows us to identify those linear codes in K^n that correspond to G -codes.

Proposition 1.3 ([4]). A K -linear subspace \mathcal{C} of KG is a G -code if and only if the permutation automorphism group $\text{PAut}(\varphi(\mathcal{C})) \leq S_n$ of the linear code $\varphi(\mathcal{C}) \leq K^n$ contains a subgroup isomorphic to G acting regularly in its induced natural action on the n positions.

Via a standard isomorphism φ , we may (uniquely) define the standard inner product and the Schur product on KG through the corresponding products on K^n , as

$$\langle f, f' \rangle := \langle \varphi(f), \varphi(f') \rangle \quad \text{and} \quad f * f' = \varphi(f) * \varphi(f'), \quad \text{for any } f, f' \in KG.$$

Therefore, we can also define the Schur product of G -codes $\mathcal{C}, \mathcal{C}' \leq KG$ as the following K -linear subspace of KG :

$$\mathcal{C} * \mathcal{C}' := \langle c * c' \mid c \in \mathcal{C}, c' \in \mathcal{C}' \rangle_K. \quad (3)$$

2 An uncertainty principle for G -codes

In this section, we give an uncertainty principle for field-valued functions over G and the corresponding bound on the parameters of a G -code, also investigating equality in this bound.

Following [12, Section V], we first introduce the following definition for any finite group G .

Definition 2.1. Let S be a nonempty subset of G . A sequence g_1, \dots, g_t in G has *right S -rank t* if $Sg_i = \{sg_i \mid s \in S\}$ is not contained in $\bigcup_{j < i} Sg_j$ for all $i \in \{2, \dots, t\}$.

For any $f \in KG$, we denote by $T_f : KG \rightarrow KG$ the map $v \mapsto fv$.

Lemma 2.2. Let $0 \neq f \in KG$ and $S = \text{supp}(f)$. If there exists a sequence in G with right S -rank t , then $\dim fKG = \text{rank}_K(T_f) \geq t$.

Proof. Let g_1, \dots, g_t be a sequence in G of S -rank t . We aim to show that $T_f(g_1), \dots, T_f(g_t) \in KG$ are linearly independent over K . Suppose by contradiction that there exists $(\lambda_1, \dots, \lambda_t) \in K^t \setminus \{0\}$ such that $\sum_{i=1}^t \lambda_i T_f(g_i) = 0$. Let $r := \max\{i \in \{1, \dots, t\} : \lambda_i \neq 0\}$, so that $\sum_{i=1}^t \lambda_i T_f(g_i)$ is a linear combination of $\bigcup_{i=1}^r Sg_i$. Let $h \in Sg_r \setminus \bigcup_{j < r} Sg_j$. Then the coefficient of h in $\sum_{i=1}^t \lambda_i T_f(g_i) \in KG$ is $\lambda_r \neq 0$, a contradiction. \square

Remark 2.3. We highlight the fact that the lower bound on $\dim fKG$ in Lemma 2.2 is an intrinsic property of G and does not depend on K . More precisely, the bound depends on $\text{supp}(f) \subseteq G$ but not on the nonzero coefficients in f of the elements in $\text{supp}(f)$.

Following the arguments of [18, Theorem 1.(a)] we prove Theorem 2.4, that holds for any field K and any finite group G .

Theorem 2.4. For any $f \in KG$, define $T_f : KG \rightarrow KG$ by $v \mapsto fv$. Then

$$|\text{supp}(f)| \cdot \text{rank}_K(T_f) \geq |G|.$$

Proof. Let $S := \text{supp}(f) \subseteq G$. Let $t \geq 1$ be the maximum size of a sequence $g_1, \dots, g_t \in G$ with right S -rank t . By the maximality of t , we have $\bigcup_{i=1}^t Sg_i = G$ and hence $t \geq |G|/|S|$. We may then conclude by Lemma 2.2. \square

Remark 2.5. Suppose that $\text{char}K$ does not divide the order of G . Given a representation ρ of G over K , the Fourier transform of $f \in KG$ at ρ is

$$\hat{f}(\rho) := \sum_{g \in G} f(g)\rho(g).$$

Let $\text{Irr}(G) = \{\rho_1, \dots, \rho_t\}$ be the set of irreducible representations of G over K . Let $\text{supp}(\hat{f}) := \{\rho \in \text{Irr}(G) \mid \hat{f}(\rho) \neq 0\}$. Since KG is semisimple, the map

$$\varphi : h \rightarrow (\hat{h}(\rho_1), \dots, \hat{h}(\rho_t))$$

is an isomorphism [22, Proposition 10]. Define $S := \varphi \circ T_f \circ \varphi^{-1}$. Then, after the notation of [18],

$$\mu(f) := \sum_{i=1}^t \deg \rho_i \cdot \text{rank}_K \hat{f}(\rho_i) = \text{rank}_K S = \text{rank}_K T_f.$$

So Theorem 2.4 reads

$$|\text{supp}(f)| \cdot \mu(f) \geq |G|,$$

and hence $\mu(f)$ is a measure of $\text{supp}(\hat{f})$. For this reason, Theorem 2.4 is a kind of uncertainty principle for the function $f : G \rightarrow K$.

Corollary 2.6. For any nonzero G -code \mathcal{C} , we have

$$d(\mathcal{C}) \cdot \dim \mathcal{C} \geq |G|.$$

In particular,

$$2\sqrt{|G|} \leq d(\mathcal{C}) + \dim \mathcal{C} \leq |G| + 1.$$

Proof. Let $f \in \mathcal{C}$ be such that $d(\mathcal{C}) = |\text{supp}(f)|$. Then the subcode fKG has the same minimum distance as \mathcal{C} , but possibly a smaller dimension. Since $\dim(fKG) = \text{rank}_K(T_f)$, the first claim follows by Theorem 2.4. The second claim is a consequence of the AM-GM inequality and the Singleton bound. \square

Remark 2.7. When G is cyclic, the structure of the defining zeros of the cyclic G -code \mathcal{C} is used to prove the BCH bound on the minimum distance. This idea can be extended to prove the so-called shift bound whenever G is abelian of order coprime to $\text{char}K$, by considering the defining zeros of \mathcal{C} as particular elements \hat{f} of the character group \hat{G} ; see [12, Section 3]. Notice that, when $f \in \mathcal{C}$, \hat{f} is related to the dimension of the submodule fKG of \mathcal{C} . We are not able to extend further this strategy to non-abelian groups. Yet one may ask how to define “zeros” of \mathcal{C} in relation to the submodules of \mathcal{C} , and hence to $\dim \mathcal{C}$. In this way, (1) may be read as an analogous bound on the minimum distance.

Remark 2.8. Note that Theorem 2.4 and Corollary 2.6 are a generalization of the Naive uncertainty principle proved in [7, Proposition 2] for cyclic groups G . It is then natural to wonder whether an analogue of [7, Theorem 2] on the asymptotic behavior of cyclic codes holds also for other families of G -codes. For instance, an even stronger result holds for G -codes when G is metacyclic, since metacyclic codes are asymptotically good; see [2, 9]. However, it is likely that results similar to [7, Theorem 2] may hold for different families of groups.

Example 2.9. If \mathcal{C} is the extended binary Golay code, then \mathcal{C} is a self-dual code of length 24 over \mathbb{F}_2 and also an S_4 -code in $\mathbb{F}_2 S_4$; see [5]. In this case $d(\mathcal{C}) \cdot \dim \mathcal{C} = 8 \cdot 12 = 96 > |G|$.

If $\mathcal{C} = \text{RM}(r, m) := \{(f(v))_{v \in \mathbb{F}_2^m} \mid f \in \mathbb{F}_2[x_1, \dots, x_m], \deg f \leq r\}$ is the binary Reed-Muller code of order r in m variables (with $r \leq m$), then \mathcal{C} is a G -code, where G is an elementary abelian 2-group of rank m ; see [3]. In this case,

$$d(\mathcal{C}) \cdot \dim \mathcal{C} = 2^{m-r} \cdot \sum_{i=0}^r \binom{m}{i} \geq 2^{m-r} \cdot \sum_{i=0}^r \binom{r}{i} = 2^m = |G|,$$

and the equality holds if and only if $r = m$.

We characterize the case in which equality in (1) holds, generalizing [18, Theorem 1.(b)].

Theorem 2.10. A G -code \mathcal{C} satisfies $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|$ if and only if there exist $H \leq G$ and $c \in KH$ such that $|H| = d(\mathcal{C})$, cKH has dimension 1 and $\mathcal{C} = cKG$.

Proof. If there exist H and c as in the claim, then \mathcal{C} is induced by the KH -module cKH , with exactly $[G : H]$ direct summands, each of dimension 1. Thus $\dim \mathcal{C} = [G : H]$ and $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|$.

Conversely, suppose that $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|$. Let $c \in \mathcal{C}$ be such that $\text{wt}(c) = d(\mathcal{C})$ and consider $\mathcal{C}_0 := cKG \leq \mathcal{C}$. Clearly $d(\mathcal{C}_0) = d(\mathcal{C})$. Thus, by Corollary 2.6,

$$|G| \leq d(\mathcal{C}_0) \cdot \dim \mathcal{C}_0 = d(\mathcal{C}) \cdot \dim \mathcal{C}_0 \leq d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|.$$

It follows that $\dim \mathcal{C}_0 = \dim \mathcal{C}$, and hence $\mathcal{C} = \mathcal{C}_0 = cKG$. Let $H := \text{supp}(c)$, so that $|H| = d(\mathcal{C})$. Following the arguments and the notations of the proof of Theorem 2.4 with $f = c$, we see that $t = |G|/|H|$ and hence G is the disjoint union

$$G = Hg_1 \sqcup \dots \sqcup Hg_t,$$

for some $g_1, \dots, g_t \in G$. Replacing c by the minimum weight codeword $ch^{-1} \in \mathcal{C}$ with $h \in \text{supp}(c)$, we can assume $1 \in H$. Then, for any $h \in H$, we have $h \in H \cap Hh$, and this implies $H = Hh$ by the following argument from the proof of Theorem 1 in [18]. Suppose by contradiction that $Hh \not\subseteq H$, and choose a maximal sequence $h_1, \dots, h_r \in G$ with $r \geq 2$ such

that $h_1 = 1$, $h_2 = h$ and $Hh_i \not\subseteq \cup_{1 \leq j < i} Hh_j$ for $2 \leq i \leq r$. By maximality $G = \cup_{1 \leq j \leq r} Hh_j = G$, and hence $t \geq r$ by definition of t as in the proof of Theorem 2.4. But $H \cap Hh_1$ implies $r > |G|/|H| = t$, a contradiction. Thus $Hh = H$ for all $h \in H$, whence $H \cdot H \subseteq H$. Since H is finite, this implies that H is a subgroup of G , and $t = [G : H]$. Since

$$\mathcal{C} = cKG = cK \left(\bigsqcup_{i=1}^t Hg_i \right) = \bigoplus_{i=1}^t (cKH)g_i,$$

we have $\dim \mathcal{C} = t \cdot \dim cKH$. By the assumption, $\dim \mathcal{C} = |G|/d(\mathcal{C}) = t$. Therefore $\dim cKH = 1$, and the claim is proved. \square

If H in the claim of Theorem 2.10 is a p -group and $\text{char} K = p$, then the simple KH -module cKH is trivial. Therefore Theorem 2.10 yields immediately the following result.

Corollary 2.11. If $\text{char} K = p$ and G is a p -group, then a G -code $\mathcal{C} \leq KG$ satisfies $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|$ if and only if $\mathcal{C} = K_H^G$ for some $H \leq G$.

Remark 2.12. The claim of Corollary 2.11 does not hold if G is not a p -group where $p = \text{char} K$. For instance, if $K = \mathbb{F}_3$, $G = C_2 = \langle r \rangle$, $c = 1 + 2r$ and $\mathcal{C} = cKG$. Then Theorem 2.10 holds with $H = G$, but $\mathcal{C} \neq K_H^G$.

Among the G -codes attaining equality in (1), Proposition 2.13 identifies those which are generated by an idempotent.

Proposition 2.13. Let $\text{char} K = p$ and $\mathcal{C} \leq KG$ be a G -code such that $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G|$. Then $\mathcal{C} = eKG$, for some $e \in KG$ with $e = e^2$, if and only if $p \nmid d(\mathcal{C})$.

Proof. Suppose that $\mathcal{C} = eKG$ with $e = e^2$. Since \mathcal{C} is a projective KG -module, we have $|G|_p \mid \dim \mathcal{C}$ by Dickson's Theorem [16, Chapter 7, Corollary 7.16]. Thus $d(\mathcal{C}) = |G|/\dim \mathcal{C}$ is not divisible by p .

To see the converse we apply Theorem 2.10. Let H and c be as in the claim of Theorem 2.10. Since $p \nmid d(\mathcal{C}) = |H|$, the algebra KH is semisimple, and hence the ideal cKH of KH is generated by an idempotent $e \in KH$, i.e. $cKH = eKH$. It follows that $\mathcal{C} = cKG = eKG$. \square

Let us finally remark that, if $\mathcal{C} < \mathbb{F}_2G$ and G is a 2-group, then $d(\mathcal{C})$ is even, since \mathcal{C} is contained in the Jacobson radical $J(\mathbb{F}_2G)$, which is the subspace of even weight vectors.

3 On the Schur product of G -codes

In this section we deal with the Schur product of G -codes, which is defined in (3).

Lemma 3.1. If $\mathcal{C}, \mathcal{C}' \leq KG$ are G -codes, then $\mathcal{C} * \mathcal{C}' \leq KG$ is a G -code as well.

Proof. Let $c = \sum_{x \in G} c_x x \in \mathcal{C} \leq KG$ and $c' = \sum_{x \in G} c'_x x \in \mathcal{C}' \leq KG$, with c_x, c'_x for all $x \in G$. For any $g \in G$, we have

$$\sum_{x \in G} c_{xg^{-1}} x = \sum_{x \in G} c_x xg = cg \in \mathcal{C}$$

and

$$\sum_{x \in G} c'_{xg^{-1}} x = \sum_{x \in G} c'_x xg = c'g \in \mathcal{C}'$$

since \mathcal{C} and \mathcal{C}' are KG -modules. Hence

$$(c * c')g = \left(\sum_{x \in G} c_x c'_x x \right) g = \sum_{x \in G} c_x c'_x xg = \sum_{x \in G} c_{xg^{-1}} c'_{xg^{-1}} x = cg * c'g \in \mathcal{C} * \mathcal{C}'$$

which proves the claim. \square

By Lemma 3.1, we can investigate KG -linear maps involving the KG -module $\mathcal{C} * \mathcal{C}'$.

Lemma 3.2. Let $\mathcal{C}, \mathcal{C}' \leq KG$ be G -codes of dimension k and k' , respectively. For any $u \in \mathcal{C}'$, let $\varphi_u : \mathcal{C} \rightarrow \mathcal{C} * \mathcal{C}'$ be the map $c \mapsto c * u$. Then the following holds.

- a) For any $u \in \mathcal{C}'$, φ_u is K -linear.
- b) If $k \leq k'$, then there exists $v \in \mathcal{C}'$ such that φ_v is injective.
- c) For any $w \in \mathcal{C}'$, the map φ_w is KG -linear if and only if w belongs to the trivial KG -module K_G . Also, for any nonzero $w \in \mathcal{C}' \cap K_G$, φ_w is injective.

Proof. a) This claim is straightforward.

b) Let S be an information set for \mathcal{C} . Since the existence of v as in the claim is invariant under permutation equivalence for \mathcal{C}' , we can assume that \mathcal{C}' has an information set S' containing S . Let M' be a generator matrix for \mathcal{C}' such that the columns of M' indexed by S' form the identity matrix $I_{k'}$, and choose $v \in \mathcal{C}'$ as the sum of the rows of M' . Then, for any $c \in \mathcal{C}$ and any position i in S , the i -th entries of c and $\varphi_v(c)$ are equal. The claim follows.

c) Let $w = \sum_{x \in G} \lambda_x x \in \mathcal{C}'$. If $w \in K_G$, say $\lambda_x = \lambda \in K$ for any $x \in G$, then

$$\varphi_w(cg) = cg * w = cg * wg = (c * w)g = \varphi_w(c)g$$

for all $c \in \mathcal{C}$ and $g \in G$. Since φ_w is K -linear, this implies that φ_w is KG -linear. Conversely, suppose that φ_w is KG -linear. Then

$$cg * w = \varphi_w(cg) = \varphi_w(c)g = (c * w)g = cg * wg$$

for all $c \in \mathcal{C}$ and $g \in G$. Thus $c * w = c * wg$ and hence $c * (w - wg) = 0$ for all $c \in \mathcal{C}$ and $g \in G$. If there exist $x, g \in G$ such that the component of $w - wg$ at x is nonzero, then we choose $c \in \mathcal{C}$ with nonzero component at x and obtain a contradiction to $c * (w - wg) = 0$. Therefore $w = wg$ for all $g \in G$, implying that $\lambda_x = \lambda \in K$ for all $x \in G$, i.e. $w \in K_G$. Finally, if $w \in \mathcal{C}' \cap K_G$ and $w \neq 0$, then $\text{wt}(w) = |G|$, and therefore φ_w is injective. \square

In general, not all KG -monomorphisms from \mathcal{C} into $\mathcal{C} * \mathcal{C}$ have the shape φ_u .

Remark 3.3. If $K = \mathbb{F}_2$, then the map $c \mapsto c * c$ is a KG -monomorphism from \mathcal{C} into $\mathcal{C} * \mathcal{C}$.

On the other side, KG -monomorphisms from \mathcal{C} into $\mathcal{C} * \mathcal{C}$ may not exist at all, as Example 3.4 shows.

Example 3.4. Let $K = \mathbb{F}_3$, $G = C_2 = \langle r \rangle$ and $\mathcal{C} = (1 + 2r)KG$. Then \mathcal{C} is a nontrivial irreducible KG -module of dimension 1. By direct computation we have $\mathcal{C} * \mathcal{C} = (1 + r)KG$, which is the trivial KG -module. Therefore a KG -monomorphism from \mathcal{C} into $\mathcal{C} * \mathcal{C}$ does not exist.

Theorem 3.5 provides the structure of those G -codes \mathcal{C} which coincide with $\mathcal{C} * \mathcal{C}$.

Theorem 3.5. Let $\mathcal{C} \leq KG$ be a G -code with $\mathcal{C} \neq \{0\}$. If $\mathcal{C} = \mathcal{C} * \mathcal{C}$, then there exists a subgroup $H \leq G$ such that $\mathcal{C} = K_H^G$. In particular, $d(\mathcal{C}) \cdot \dim(\mathcal{C}) = |G|$.

Proof. Any two codewords $c, c' \in \mathcal{C}$ of minimum weight $\text{wt}(c) = \text{wt}(c') = d(\mathcal{C})$ satisfy

$$\text{supp}(c) \cap \text{supp}(c') = \emptyset \quad \text{or} \quad \text{supp}(c) \cap \text{supp}(c') = \text{supp}(c), \quad (4)$$

because $c * c' \in \mathcal{C}$ and $\text{supp}(c * c') \subseteq \text{supp}(c)$.

Moreover, every element of G is in the support of some minimum weight codeword of \mathcal{C} , because the multiplication action of G on itself is transitive and \mathcal{C} is a KG -module. Therefore, there exist $c_1, \dots, c_s \in \mathcal{C}$ of minimum weight such that G is the disjoint union

$$G = \text{supp}(c_1) \sqcup \dots \sqcup \text{supp}(c_s).$$

Let $O_i = \text{supp}(c_i)$ for $i = 1, \dots, s$, and assume without loss of generality that $1 \in O_1$. Then, for any $g \in O_1$, the set O_1g is the support of the minimum weight codeword c_1g and satisfies $g \in O_1 \cap O_1g$, which implies $O_1 = O_1g$ by (4). Thus $O_1 = O_1O_1$, and hence $H := O_1$ is a subgroup of G .

For any $i = 1, \dots, s$, it follows that $O_i = Hg_i$ for some $g_i \in G$ (indeed, for $g_i \in O_i$).

Write $c_i = \sum_{h \in H} \lambda_h^{(i)} hg_i$, where $\lambda_h^{(i)} \neq 0$ for all $h \in H$. For any $h' \in H$, the codeword $c_i * c_i - \lambda_{h'}^{(i)} c_i \in \mathcal{C}$ has weight $|\{h \in H : \lambda_h^{(i)} \neq \lambda_{h'}^{(i)}\}| < \text{wt}(c_i) = d(\mathcal{C})$, and hence $c_i * c_i - \lambda_{h'}^{(i)} c_i = 0$. Then $\lambda_h^{(i)} = \lambda_{h'}^{(i)}$ is constant for all $h \in H$ and, after scaling by $(\lambda^{(i)})^{-1} \in K$, we can assume that $c_i = \sum_{h \in H} hg_i$. It follows that

$$(K_H)^G = \bigoplus_{i=1}^s \left(K \sum_{h \in H} h \right) g_i = \bigoplus_{i=1}^s K \left(\sum_{h \in H} hg_i \right) = \bigoplus_{i=1}^s K c_i \subseteq \mathcal{C}.$$

Conversely, in order to prove that $\mathcal{C} \subseteq K_H^G$, let $a \in \mathcal{C}$. Then

$$a = a * \sum_{g \in G} g = a * \sum_{i=1}^s c_i = \sum_{i=1}^s a * c_i = \sum_{i=1}^s a_i,$$

where $a_i := a * c_i \in KHg_i$. From $\mathcal{C} * \mathcal{C} \subseteq \mathcal{C}$ it follows $a_i \in \mathcal{C}$. Since $\text{supp}(a_i) \subseteq \text{supp}(c_i)$, this implies that either $a_i = 0$ or $\text{wt}(a_i) = d(\mathcal{C})$. Then, arguing as above, we have $a_i = \mu^{(i)} c_i$ for some $\mu^{(i)} \in K$. Hence $a = \sum_{i=1}^s \mu^{(i)} c_i \in K_H^G$ and the equality $\mathcal{C} = K_H^G$ is proved.

Finally, the claim $d(\mathcal{C}) \cdot \dim(\mathcal{C}) = |G|$ follows immediately from Theorem 2.10. \square

For any G -code $\mathcal{C} \leq KG$, we define recursively $\mathcal{C}^{(1)} = \mathcal{C}$ and $\mathcal{C}^{(t+1)} = \mathcal{C}^{(t)} * \mathcal{C}$. By [20, Theorem 2.32], we know that $\dim \mathcal{C}^{(t+1)} \geq \dim \mathcal{C}^{(t)}$ for any $t \geq 1$. This allows to define the *Castelnuovo-Mumford regularity* of \mathcal{C} as the smallest t such that $\dim \mathcal{C}^{(t+i)} = \dim \mathcal{C}^{(t)}$ for all $i \geq 0$; see [20, Definition 1.5]. The eventual behaviour of $\mathcal{C}^{(t)}$ is easily obtained in the binary case.

Theorem 3.6. Let $K = \mathbb{F}_2$ and $\mathcal{C} \leq KG$ be a G -code with $\mathcal{C} \neq \{0\}$. Then there exists a subgroup $H \leq G$ such that $\mathcal{C} \leq K_H^G$ and $\mathcal{C}^{(t)} = K_H^G$ for any t big enough.

Proof. By Remark 3.3, we know that $\mathcal{C}^{(2^i)} \leq \mathcal{C}^{(2^{i+1})}$ for any $i \geq 0$. Since G is finite, there exists $t \in \mathbb{N}$ such that $\mathcal{C}^{(2^t)} * \mathcal{C}^{(2^t)} = \mathcal{C}^{(2^{t+1})} = \mathcal{C}^{(2^t)}$. By Theorem 3.5, this implies that $\mathcal{C}^{(2^t)} = K_H^G$ for some $H \leq G$. Note that the case $\mathcal{C}^{(2^t)} = KG$ corresponds to $H = 1$. \square

In the next results we investigate the KG -module $\mathcal{C} * \mathcal{C}$ in relation with the self-orthogonality of \mathcal{C} . Notice that the standard inner product on $K^n \times K^n$ corresponds via a standard isomorphism $K^n \cong KG$ to the inner product on $KG \times KG$ defined by

$$\langle \cdot, \cdot \rangle : KG \times KG \rightarrow K, \quad (c, c') \mapsto \varepsilon(c * c'),$$

where ε is the KG -linear augmentation defined by

$$\varepsilon : KG \rightarrow K, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g.$$

Therefore, a G -code $\mathcal{C} \leq KG$ is self-orthogonal if and only if $\mathcal{C} * \mathcal{C} \subseteq \ker \varepsilon$.

Theorem 3.7. Let $\mathcal{C} \leq KG$ be a G -code such that $\mathcal{C} \not\subseteq \mathcal{C}^\perp$. Then $\mathcal{C} * \mathcal{C} = \mathcal{P}_0 \oplus \mathcal{M}$, where \mathcal{P}_0 and \mathcal{M} are KG -modules, and \mathcal{P}_0 is a projective cover of the trivial KG -module K_G . In particular, if $\text{char} K = p$, then $|G|_p \leq \dim \mathcal{C} * \mathcal{C}$.

Proof. Write $KG = \mathcal{P}_0 \oplus \mathcal{P}_1$, where \mathcal{P}_0 is a projective cover of KG . For all $a \in KG$ denote by a_0 and a_1 the components of a in \mathcal{P}_0 and \mathcal{P}_1 , respectively, and consider the projection $\pi : \mathcal{C} * \mathcal{C} \rightarrow \mathcal{P}_0$ defined by $a \mapsto a_0$. We prove that π is KG -linear and surjective.

Note that $\ker \varepsilon = \mathcal{P}_0 \mathcal{J}(KG) \oplus \mathcal{P}_1$, where $\mathcal{J}(KG)$ is the Jacobson radical of KG ; see [16, Chapter 7, §10]. Also, since $\mathcal{C} \not\subseteq \mathcal{C}^\perp$, there exists $c \in (\mathcal{C} * \mathcal{C}) \setminus \ker \varepsilon$, which satisfies $c_0 = \pi(c) \in \mathcal{P}_0 \setminus \ker \varepsilon$. Therefore $c_0 \in \mathcal{P}_0 \setminus \mathcal{P}_0 \mathcal{J}(KG)$, and we get $\mathcal{P}_0 = c_0 KG$. Thus π is a KG -epimorphism from $\mathcal{C} * \mathcal{C}$ onto the projective KG -module \mathcal{P}_0 . Hence, up to a KG -isomorphism, \mathcal{P}_0 is a direct summand of $\mathcal{C} * \mathcal{C}$; see [16, Chapter 7, §7].

The claim on $|G|_p$ now follows by $\dim \mathcal{P}_0 \leq \dim \mathcal{C} * \mathcal{C}$ and Dickson's Theorem; see [16, Chapter 7, Corollary 7.16]. \square

Proposition 3.8 gives an application of Theorem 3.7 to G -codes over the binary field.

Proposition 3.8. Let $K = \mathbb{F}_2$ and $\mathcal{C} \leq \mathbb{F}_2 G$ be a G -code such that $\mathcal{C} \not\subseteq \mathcal{C}^\perp$. Suppose that the projective cover \mathcal{P}_0 of the trivial KG -module is K_H^G for some subgroup $H \leq G$; for instance, this holds if H is a normal p -complement of G . Then $\mathcal{C} * \mathcal{C} = \mathcal{P}_0$ if and only if $\mathcal{C} \leq \mathcal{P}_0$.

Proof. By Remark 3.3, \mathcal{C} is a submodule of $\mathcal{C} * \mathcal{C}$. Therefore, $\mathcal{C} * \mathcal{C} = \mathcal{P}_0$ implies $\mathcal{C} \leq \mathcal{P}_0$. If G is 2-nilpotent and H is a normal 2-complement of G , then $\mathcal{P}_0 = K_H^G$ because $\text{char} K = 2$; see [16, Chapter 7, §7]. Therefore we can suppose that $\mathcal{P}_0 = K_H^G$ for some subgroup $H \leq G$. Since $K = \mathbb{F}_2$, it is easy to see that $\mathcal{P}_0 * \mathcal{P}_0 = \mathcal{P}_0$, whenever $\mathcal{P}_0 = K_H^G$ with $H \leq G$. Therefore, from $\mathcal{C} \leq \mathcal{P}_0$ it follows that $\mathcal{C} * \mathcal{C} \leq \mathcal{P}_0 * \mathcal{P}_0 = \mathcal{P}_0$. By Theorem 3.7, $\mathcal{C} * \mathcal{C}$ contains a module isomorphic to \mathcal{P}_0 . Thus, from $\mathcal{C} \leq \mathcal{P}_0$ it follows $\mathcal{C} * \mathcal{C} = \mathcal{P}_0$, and the claim is proved. \square

Example 3.9. Let $K = \mathbb{F}_2$ and G be the Mathieu group M_{11} , of order $2^4 \cdot 3^2 \cdot 5 \cdot 11$. Let \mathcal{C} be the projective cover \mathcal{P}_0 of the trivial KG -module, which satisfies $\dim \mathcal{C} = 2^4 \cdot 7$. Since $\dim \mathcal{C} \nmid |M_{11}|$, \mathcal{C} is not induced by the trivial module of a subgroup. By Theorem 3.5, we get $\mathcal{C} \neq \mathcal{C} * \mathcal{C}$. Also, by direct checking, $\mathcal{C} \not\subseteq \mathcal{C}^\perp$. Therefore, the claim of Proposition 3.8 does not hold for $G = M_{11}$.

Lemma 3.10. If $\mathcal{C} \leq KG$ is a self-orthogonal G -code, then $\dim \mathcal{C} * \mathcal{C} < |G|$.

Proof. From $\mathcal{C} \subseteq \mathcal{C}^\perp$ it follows that $\mathcal{C} * \mathcal{C} \leq \ker \varepsilon$. With the notations of the proof of Theorem 3.7, we have that $\ker \varepsilon = \mathcal{P}_0 \mathcal{J}(KG) \oplus \mathcal{P}_1$ is strictly contained in KG , and the same holds for $\mathcal{C} * \mathcal{C}$. The claim follows. \square

Example 3.11. Consider again the binary G -codes introduced in Example 2.9.

If \mathcal{C} is the extended binary Golay code, then $\mathcal{C} * \mathcal{C} = \ker \varepsilon$, so that $\dim \mathcal{C} * \mathcal{C} = |G| - 1 = 23$.

If \mathcal{C} is the Reed-Muller code $\text{RM}(r, m)$ of order r in m variables with $r \leq (m - 1)/2$, then \mathcal{C} is self-orthogonal. It is easy to observe that $\mathcal{C} * \mathcal{C} = \text{RM}(2r, m)$. In this case $\mathcal{C} * \mathcal{C} < \ker \varepsilon$ whenever $r < (m - 1)/2$.

In the case of p -groups in characteristic p , the converse of Lemma 3.10 holds.

Proposition 3.12. Let $\text{char} K = p$, let G be a p -group and let $\mathcal{C} \leq KG$ be a G -code. If \mathcal{C} is not self-orthogonal, then $\mathcal{C} * \mathcal{C} = KG$.

Proof. The claim follows immediately from the last part of Theorem 3.7. \square

Using the bound (2) on the dimension of $\mathcal{C} * \mathcal{C}$, Proposition 3.12 yields the following corollary.

Corollary 3.13. Let $\text{char} K = p$, G be a p -group and $\mathcal{C} \leq KG$ be a G -code. If

$$\dim \mathcal{C} < \frac{\sqrt{8|G| + 1} - 1}{2},$$

then \mathcal{C} is self-orthogonal.

Acknowledgments

The first author was partially supported by the ANR-21-CE39-0009 - BARRACUDA (French *Agence Nationale de la Recherche*). The third author was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

- [1] F. Alizadeh, S. Glasby, and C. E. Praeger. Sequences of linear codes where the rate times distance grows rapidly. *arXiv preprint arXiv:2110.01277*, 2021.
- [2] L. M. Bazzi and S. K. Mitter. Some randomized code constructions from group actions. *IEEE Trans. Inform. Theory*, 52(7):3210–3219, 2006.
- [3] S. D. Berman. On the theory of group codes. *Cybernetics*, 3(1):25–31 (1969), 1969.
- [4] J. J. Bernal, Á. del Río, and J. J. Simón. An intrinsical description of group codes. *Des. Codes Cryptogr.*, 51(3):289–300, 2009.
- [5] F. Bernhardt, P. Landrock, and O. Manz. The extended golay codes considered as ideals. *J. Combin. Theory Ser. A*, 55(2):235–246, 1990.
- [6] M. Borello, J. De La Cruz, and W. Willems. On checkable codes in group algebras. *J. Algebra Appl.*, page 2250125, 2021.
- [7] M. Borello and P. Solé. The uncertainty principle over finite fields. *Discrete Math.*, 345(1):Paper No. 112670, 7, 2022.
- [8] M. Borello and W. Willems. On the algebraic structure of quasi group codes. *arXiv preprint arXiv:1912.09167*, 2019.
- [9] M. Borello and W. Willems. Group codes over fields are asymptotically good. *Finite Fields Appl.*, 68:101738, 12, 2020.
- [10] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J.-P. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Des. Codes Cryptogr.*, 73(2):641–666, 2014.
- [11] S. Evra, E. Kowalski, and A. Lubotzky. Good cyclic codes and the uncertainty principle. *Enseign. Math.*, 63(3-4):305–332, 2017.
- [12] T. Feng, H. D. Hollmann, and Q. Xiang. The shift bound for abelian codes and generalizations of the donoho-stark uncertainty principle. *IEEE Trans. Inform. Theory*, 65(8):4673–4682, 2019.
- [13] G. B. Folland and A. Sitaram. The uncertainty principle: a mathematical survey. *J. Fourier Anal. Appl.*, 3(3):207–238, 1997.
- [14] E. J. García-Claro and H. Tapia-Recillas. On the dimension of ideals in group algebras, and group codes. *J. Algebra Appl.*, 21(2):Paper No. 2250024, 16, 2022.
- [15] W. C. Huffman, J.-L. Kim, and P. Solé. *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC, 2021.

- [16] B. Huppert and N. Blackburn. *Finite groups. II*, volume 242 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1982. AMD, 44.
- [17] J. MacWilliams. Codes and ideals in group algebras. In *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)*, pages 317–328. Univ. North Carolina Press, Chapel Hill, N.C., 1969.
- [18] R. Meshulam. An uncertainty inequality for groups of order pq . *European J. Combin.*, 13(5):401–407, 1992.
- [19] R. Pellikaan and I. Márquez-Corbella. Error-correcting pairs for a public-key cryptosystem. *J. Phys.: Conf. Ser.*, 855:012032, 2017.
- [20] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.
- [21] J. Schur. Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen. *J. Reine Angew. Math.*, 140:1–28, 1911.
- [22] J.-P. Serre. *Linear representations of finite groups*, volume 42. Springer, 1977.
- [23] T. Tao. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.*, 12(1):121–128, 2005.
- [24] C. Wieschebrink. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In *Post-quantum cryptography*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 61–72. Springer, Berlin, 2010.