A Note on Self-Dual Group Codes

W. Willems

Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg

Abstract- **In this paper we classify group algebras over Galois rings containing self-dual ideals; i.e., ideals C which satisfy $C = C^{\perp}$ with respect to the natural non-degenerate bilinear form given on group algebras.**

Index Terms- **Ideals in group algebras, self-dual codes, self-dual modules, codes over Galois rings**

1 Introduction

We call a linear code C a *group code* if C is an ideal in a group algebra RG where R is a commutative ring and G is a finite group. In this sense cyclic codes are group codes when G is a cyclic group; Reed Muller codes are group codes when G is an elementary abelian p-group [8] and there are many other remarkable record codes which have been detected as group codes [11], [4], [3].

The reader should be warned here that the term 'group code' is being used in different meanings by other authors; in particular for codes defined over an alphabet forming a group or for codes in which the set of codewords are G-orbits on the unit sphere of some Euclidian space $\mathbf{R}^n$.

The group algebra RG carries a natural non-degenerate G-invariant bilinear form $(.,.)$ which is defined by

$$(g,h) = \begin{cases} 1 & \text{if } g = h \\ 0 & \text{otherwise.} \end{cases}$$

Here G-invariance means that $(ag, bg) = (a, b)$ for all $a, b \in RG$ and all $g \in G$. With respect to this form we may define the orthogonal code $C^{\perp}$

of C as usual and call C self-dual if $C^{\perp} = C$. In this note we consider the following natural question:

Under what conditions on G and R are self-dual group codes in RG existent or non-existent?

Using twisted group algebras Hughes recently proved in [7] that self-dual group codes do not exist if $R = K$ is a field of odd characteristic or $R = \mathbf{Z}_t = \mathbf{Z}/t\mathbf{Z}$ (t odd and not a square) and G is a direct product of a 2- and a $2'$-group. This result generalizes Theorem 8 in [10] in which G is assumed to be abelian. However Hughes' assumption on the group structure is still very restrictive, but essential to his proof.

Exploiting methods from representation theory of finite groups we can drop the assumption on the structure of G completely. Since Galois rings have got much attention in coding theory over the last years we shall prove the main result of this paper over such rings. Remember that Galois rings $R = \mathrm{GR}(p^r, k)$ are residue class polynomial rings $\mathbf{Z}_{p^r}[x]/(f)$ where f is a monic irreducible polynomial of degree k in $\mathbf{Z}_p[x]$ and p is a prime number. This class contains in particular the rings $\mathbf{Z}_{p^r}$ and finite fields $\mathbf{F}_{p^r}$.

Theorem 1.1 *Let p be a prime number, let $r, k \in \mathbf{N}$ and let G be a finite group. Then the group algebra $\mathrm{GR}(p^r, k)G$ contains a self-dual group code if and only if one of the following conditions holds true.*

(i) p is odd and r is even

(ii) $p = 2$ and r or $|G|$ is even.

Specializing to $k = 1$, i.e., $\mathrm{GR}(p^r, 1) = \mathbf{Z}_{p^r}$, and using the Chinese Reminder Theorem we get as a consequence

Corollary 1.2 *Let $t = 2^s p_1^{n_1} \dots p_r^{n_r}$ with pairwise different odd primes p_i and let G be a finite group. Then $\mathbf{Z}_t G$ contains a self-dual group code if and only if all the n_i are even and s or $|G|$ is even.*

Specializing to $r = 1$, i.e., $\mathrm{GR}(p, k) = \mathbf{F}_{p^k}$, we obtain

Corollary 1.3 *Let K be a finite field and let G be a finite group. Then KG contains a self-dual group code if and only if the characteristic of K is 2 and the order of $|G|$ is even.*

In [3] the binary extended Golay code was constructed as a self-dual group code over the symmetric group S_4 on four letters. In the same paper the authors recovered the ternary extended Golay code as an ideal in a twisted ternary group algebra over the alternating group A_4 on four letters. The twist is no longer surprising since $\mathbf{F}_3\mathrm{A}_4$ does not contain a self-dual group code by Corollary 1.3.

We should mention here that unfortunately we are not constructing self-dual group codes which from viewpoint of coding theory are of any interest, i.e., the codes which we construct have bad parameters. So the theorem only provides situations in which a search for good self-dual group codes should be worthwhile.

For results in group and representation theory over fields the reader is referred to [1], [6]. A detailed treatment of Galois rings can be found in [9]. Furthermore all modules which we consider are finitely generated and right modules. Finally RG-modules are not assumed to be free as R-modules.

2 Preliminaries

In this section we fix R as the Galois ring $R = \mathrm{GR}(p^r, k)$ where p is a prime number and $r, k \in \mathbf{N}$. For reader's convenience we restate some simple facts about R which we freely use throughout this paper (see [9]).

(1) Every ideal of R is generated by p^i for some $0 \leq i \leq r$ and among the ideals we have the inclusion relation

$$0 \subset p^{r-1}R \subset \ldots \subset pR \subset R.$$

In particular R is a local Frobenius ring (see [12], Example 4.22) with the unique simple module R/pR.

(2) R/pR (as a ring) is isomorphic to the field $\mathbf{F}_{p^k}$.

(3) $\mathrm{GR}(p, k) = \mathbf{F}_{p^k}$ and $\mathrm{GR}(p^r, 1) = \mathbf{Z}_{p^r}$.

Definition 2.1 Let M be an R-module. We put

$$M^* = \mathrm{Hom}_R(M, R)$$

and call M^* the *dual module* of M. Clearly, M^* is an R-module if we put

$$(fr)(m) = f(mr)$$

for $f \in \mathrm{Hom}_R(M, R)$, $r \in R$ and $m \in M$. Even more, if M is an RG-module, then the dual M^* becomes an RG-module by

$$(fg)(m) = f(mg^{-1}) \text{ for } f \in \mathrm{Hom}_R(M, R),\ g \in G \text{ and } m \in M,$$

and M is called a *self-dual module* if $M \cong M^*$ as an RG-module.

The next result depends on the fact that over Frobenius rings the map $M \to M^*$ defines a duality in the category of finitely generated R-modules (see for instance [12]).

Proposition 2.2 *If M is a finitely generated R-module, then $|M^*| = |M|$.*

Proof. Since R is a Frobenius ring M and M^* have the same length, i.e., the same number of composition factors. Furthermore, since R/pR is the only simple R-module we obtain $|M^*| = |M|$.

Proposition 2.3 *If C is an ideal in RG then $RG/C^\perp \cong C^*$ as RG-modules.*

Proof. For $a \in RG$ we define the function

$$f_a : RG \to C^*$$

by $f_a(c) = (a, c)$. Clearly f_a is R-linear, hence $f_a \in C^*$. Furthermore, the map $\alpha : RG \to C^*$ defined by $a \mapsto f_a$ is R-linear as well. Even more, α is RG-linear since the G-invariance of the form $(.\,,\,.)$ implies

$$\begin{aligned} \alpha(ag)(c) &= f_{ag}(c) = (ag, c) = (a, cg^{-1}) = f_a(cg^{-1}) = \\ &= \alpha(a)(cg^{-1}) = (\alpha(a)g)(c). \end{aligned}$$

As $C^\perp$ is the kernel of α we obtain an RG-linear monomorphism from $RG/C^\perp$ into C^*. It remains to show that $|RG/C^\perp| = |C^*|$. Now we look at the R-linear map $\beta : C \to (RG/C^\perp)^*$ defined by $c \mapsto h_c$ where $h_c(a + C^\perp) = (c, a)$. Obviously β is well-defined and a monomorphism. With 2.2 we obtain

$$|C| \leq |(RG/C^\perp)^*| = |RG/C^\perp| \leq |C^*| = |C|,$$

which proves the assertion.

Corollary 2.4 *Suppose that RG contains a self-dual group code. If T is a subgroup of G then a simple self-dual RT-module has even multiplicity in RG considered as an RT-module.*

Proof. Let C be a self-dual group code in RG. By 2.3 we have $RG/C \cong C^*$ as RG-modules, hence as RT-modules. If S is a simple self-dual RT-module then the multiplicity of S in C is the same as in C^*. Thus the multiplicity of S in RG considered as an RT-module is even.

Proposition 2.5 *Let H be a subgroup of G. If RH contains a self-dual group code then RG contains a self-dual group code as well.*

Proof. Let $\{x_1, \ldots, x_n\}$ denote a set of right transversals of H in G. For $a, b \in RH$ we have

$$(ax_i, bx_j) = \begin{cases} 0 & \text{if } i \neq j \\ (a,b) & \text{if } i = j. \end{cases}$$

Thus $RG = RH \perp RHx_1 \perp \ldots \perp RHx_n$. Now suppose that $C = C^\perp \leq RH$. Then $\tilde{C} = C \perp Cx_1 \perp \ldots \perp Cx_n$ is an ideal in RG and $\tilde{C} = \tilde{C}^\perp$. In the language of representation theory $\tilde{C}$ is the induced ideal $C^G = C \otimes_{RH} RG$.

3 Proof of Theorem 1.1

Let $R = \mathrm{GR}(p^r, k)$ where p is a prime number and let G be a finite group. First note that RG always contains a self-dual group code if $r = 2m$, namely $C = p^m RG$. Thus we may suppose that r is odd.

The first Proposition is based on the fact that by Wedderburn's Theorem a semi-simple group algebra defined over a field contains the trivial module with multiplicity 1 (see [1], section 13).

Proposition 3.1 *If p and r are odd then no self-dual group codes exist over $R = \mathrm{GR}(p^r, k)$.*

Proof. Let $\{x_1, \ldots, x_t\}$ be a set of left transversals of a Sylow 2-subgroup T of G. Thus G is the disjoint union of the t cosets x_iT and

$$(*) \quad RG = \oplus_{i=1}^{t} \, x_i RT,$$

where $x_iRT \cong RT$ as RT-modules. Next we consider the filtration

$$0 \subset p^{r-1}RT \subset \ldots \subset pRT \subset RT$$

where

$$p^iRT/p^{i+1}RT \cong (R/pR)T$$

as RT- or equivalently $(R/pR)T$-modules. But as a ring R/pR is isomorphic to $\mathbf{F}_{p^k}$. Thus the modules $p^iRT/p^{i+1}RT$ are isomorphic to the regular $\mathbf{F}_{p^k}T$-module. Since p does not divide $|T|$ the group algebra $\mathbf{F}_{p^k}T$ is semi-simple according to Maschke (see [1], Section 12, Corollary 8). Thus $\mathbf{F}_{p^k}T$ contains the trivial module, say $K = \mathbf{F}_{p^k}$, with multiplicity 1. Since r is odd RT contains K with odd multiplicity. By $(*)$ we finally arrive at the fact that the multiplicity of K in RG considered as an RT-module is odd (actually it is rt).

On the other hand if there were a self-dual group code in RG this multiplicity would have to be even by 2.4.

Proposition 3.2 *Let r be odd. Then* $\mathrm{GR}(2^r, k)G$ *contains a self-dual group code if and only if the order of G is even.*

Proof. Let $R = \mathrm{GR}(2^r, k)$ and suppose that RG contains a self-dual ideal. We consider $M = RG$ as an R-module. By 2.4 the multiplicity of the simple self-dual R-module R/pR in M, which obviously is $r|G|$, must be even. This forces $|G|$ to be even since r is odd.

Conversely suppose that $r = 2m + 1$ and that $|G|$ is even. Let t be an involution in G and let H be the subgroup of G generated by t. Now we put

$$C = 2^{m+1}R + 2^{m+1}Rt + 2^mR(1 + t)$$

as an R-module. Clearly, C is an ideal in RH and $C \subseteq C^\perp$. Furthermore

$$|2^{m+1}R + 2^{m+1}Rt| = |2^{m+1}R|^2 = 2^{2mk}$$

and

$$|C/(2^{m+1}R + 2^{m+1}Rt)| = 2^k.$$

Thus $|C| = |R|$ which shows that $C = C^\perp$ is a self-dual group code in RH. An application of 2.5 finishes the proof.

Proposition 3.1 and 3.2 together with the remark at the beginning of this section proves Theorem 1.1.

According to Corollary 1.2 note that there is a natural ring isomorphism

$$\mathbf{Z}_t G \cong \mathbf{Z}_{2^s} G \times \mathbf{Z}_{p_1^{n_1}} G \times \ldots \times \mathbf{Z}_{p_r^{n_r}} G$$

by the Chinese Remainder Theorem. This isomorphism maps

$$\sum_{g\in G} ([a]_t)_g g \mapsto (\sum_{g\in G} ([a]_{2^s})_g g, \ldots, \sum_{g\in G} ([a]_{p_r^{n_r}})_g g)$$

where $[a]_t = a + t\mathbf{Z}$ with $a \in \mathbf{Z}$ and it preserves self-duality (see [5], Theorem 2.1). Thus Corollary 1.2 follows by Theorem 1.1.

Corollary 1.3 is a special case of Theorem 1.1. We only have to put $R = \mathrm{GR}(p, k)$ in case K is a finite field with p^k elements.

4 Examples and Remarks

Example 4.1 Let $K = \mathbf{F}_3$ be a field with three elements and let $G = \mathrm{A}_4$ be the alternating group on four letters. The group algebra KG has two simple modules, the trivial one, say K, and a module of dimension 3, say V. (Actually V is the factor module of the permutation module by the trivial one.) The decomposition of KG into a direct sum of indecomposable modules looks like

$$KG = \begin{array}{c} K \\ K \\ K \end{array} \oplus V \oplus V \oplus V$$

(see [6], 3.19 a)). The first summand is the projective cover of the trivial module. It is a uniserial module with composition factors isomorphic to K; the module V itself is projective. Thus by 2.4, the group algebra KG does not contain a self-dual group code, in particular it does not contain the ternary extended Golay code as a self-dual ideal. To some extent this explains the twisted group algebra needed in [3].

Remark 4.2 If C is a self-dual group code in KG (K a field of characteristic 2 as we have shown above) then C is not complemented by an ideal. In particular, a self-dual group code is never generated by an idempotent:

If C were complemented then $KG \cong C \oplus C^*$, by 2.4. This implies that the projective cover of the trivial module occurs in KG with even multiplicity which contradicts the well-known fact that this multiplicity is 1. In [3] the extended binary Golay code is generated as a group code by the sum of two idempotents where the sum itself is not an idempotent - as it must be.

Examples 4.3 a) We consider the self-dual binary Reed-Muller code $C = \mathrm{RM}(1,3)$ which is a group code in $\mathbf{F}_2G$ where G is an elementary abelian 2-group of order 8. By Berman (see [2]), C coincides with J^2 where $J = \langle g-1 \mid g \in G \rangle$ denotes the Jacobson radical of $\mathbf{F}_2G$. The filtration of $\mathbf{F}_2G$ by the radical powers of J (i.e. the Loewy structure of $\mathbf{F}_2G$) is a follows

$$\begin{array}{cccc} & K & & J^0 \\ K & K & K & J^1 \\ K & K & K & J^2 \\ & K & & J^3 \end{array}$$

In particular, $C^\perp = C = J^2 \ncong KG/J^2 \cong C^*$.
b) Let $G = \langle a, b \rangle$ be a Klein four group. Now the group algebra $\mathbf{F}_2G$ does not contain a self-dual Reed-Muller code. However $\mathbf{F}_2G$ contains a self-dual group code, namely $C = \langle 1+a+b+ab, 1+a \rangle$ as an $\mathbf{F}_2$-space. Here the structure of $\mathbf{F}_2G$ is of shape

$$\begin{array}{cccc} & K & & J^0 \\ K & & K & J^1 \\ & K & & J^2 \end{array}$$

In this case we have $C = C^\perp \cong C^*$ which is a nonsplit extension of the trivial module by itself.

Remark 4.4 Let $\bar{}$ denote an involution on the field K and let $[\,.\,,\,.\,]$ be the standard Hermitian form on KG with respect to the given involution; i.e.,

$$[rg, sh] = r\bar{s}\delta_{g,h}$$

for $r, s \in K$ and $g, h \in G$. If we define the K-structure on $M^* = \mathrm{Hom}_K(M, K)$ by

$$(fr)(m) = f(m\bar{r})$$

we get again $KG/C^\perp \cong C^*$. Thus Corollary 1.3 holds also true for Hermitian forms.

References

[1] J.L. Alperin and R.B.Bell, Groups and representations. Graduate Text in Math., Springer, New York, Heidelberg 1995.

[2] S.D. Berman, On the theory of group codes. Kibernetika 3, 31-39 (1967).

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

[4] J.H. Conway, S.J. Lomonaco Jr and N.J.A. Sloane, A $[45, 13]$-code with minimal distance 16. Discrete Math. 83, 213-217 (1990).

[5] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem. Hokkaido Math. J. 28, 253-283 (1999).

[6] R. Gow, B. Huppert, R. Knőrr, O. Manz and W. Willems, Representation theory in arbitrary characteristic. Centro Internationale Per La Ricerca Mathematica, Trento 1993.

[7] G. Hughes, Structure theorems for group ring codes with an application to self-dual codes. Designs, Codes and Cryptoraphy 24, 5-14 (2001).

[8] P. Landrock and O. Manz, Classical codes as ideals in group algebras. Designs, Codes and Cryptography 2, 273-285 (1992).

[9] B.R. McDonald, Finite rings with identity. Marcel Dekker, New York 1974.

[10] B.S. Rajan and M.U. Siddiqi, A generalized DFT for abelian codes over $\mathbf{Z}_m$. IEEE Trans. Inform. Theory 40, 2082-2090 (1994).

[11] A. vom Felde, A new presentation of Cheng-Sloane's $[32, 17, 8]$-code. Arch. Math, 60, 508-511 (1993).

[12] J.A. Wood, Duality for modules over finite rings and applications to coding theory. Am. J. Math. 121, No. 3, 555-575 (1999).