On codes in group algebras

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

In the sixties of the last century group codes came into the game in coding theory. Berman discovered 1967 that binary Reed Muller codes are ideals in a binary group algebra over an elementary abelian 2-group [2]. The same time, suggested by Gleason, Jessy MacWilliams investigated ideals in a binary group algebra over a dihedral group of order $2n$ [12]. Already 1970 she proposed that one should 'look at groups, not cyclic, which produce codes with some desirable properties'.

Since that time many papers dealt with group codes and there are mainly two reasons for that. First of all, there are many optimal codes in the class of group codes. Secondly, methods from representation theory seem to be extremly powerful when dealing with coding theoretical properties.

Throughout this note we always denote by G a finite group and by $\mathbb{F} = \mathbb{F}_q$ a finite field of size q and characteristic p.

1 Group codes

The $\mathbb{F}$-vector space $\mathbb{F}G = \{a = \sum_{g \in G} a_g g \mid a_g \in \mathbb{F}\}$ with basis $\{g \in G\}$ and multiplication

$$ab = (\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1}g}) g$$

defines an $\mathbb{F}$-algebra which is called a group algebra or more presicely the group algebra of G over $\mathbb{F}$.

For $a = \sum_{g \in G} a_g g \in \mathbb{F}G$ ($a_g \in \mathbb{F}$) we denote by $\mathrm{supp}(a) = \{g \in G \mid a_g \neq 0\}$ the support and by $\mathrm{wt}(a) = |\mathrm{supp}(a)|$ the weight of a. Now we define a distance d by $\mathrm{d}(a, b) = \mathrm{wt}(a-b)$ for $a, b \in \mathbb{F}G$. Note that d satisfies the axioms of a metric on $\mathbb{F}G$.

Definition 1.1 A right ideal $C \leq \mathbb{F}G$ in $\mathbb{F}G$ endowed with the distance d is called a group code, or in case we want to refer to the underlying group a G-code.

Let S_n denote the group of permutations on $\{1, \ldots, n\}$. We consider the natural $\mathbb{F}$-linear action of S_n on $\mathbb{F}^n$ defined on the standard basis e_i by $e_i \sigma = e_{i\sigma}$ for $\sigma \in \mathrm{S}_n$ and $i = 1, \ldots, n$. For an $\mathbb{F}$-linear subspace C of $\mathbb{F}^n$ we denote by $\mathrm{PAut}(C) = \{\sigma \in \mathrm{S}_n \mid \sigma \in \mathrm{Aut}(C)\}$ the group of permutation automorphisms of C. Clearly, if $C \leq \mathbb{F}G$ is a group code, then $G \leq \mathrm{PAut}(C)$ and $G \leq \mathrm{S}_n$ is regular, i.e., transitive of order n.

Theorem 1.2 (Bernal, del Río, Simón (2009), [3]) *Let C be a linear code over $\mathbb{F}$ of length n and let G be a group of order $|G| = n$. Then C is a G-code if and only if G is a regular subgroup of* $\mathrm{PAut}(C)$.

Examples 1.3 a) Cyclic codes are G-codes for G cyclic.
b) (Berman [2], Charpin [7]) Reed-Muller codes over the prime $\mathbb{F}_p$ are G-codes where G is an elementary abelian p-group.
c) (Bernhardt, Landrock, Manz [5]; McLaughlin, Hurley [14]) The binary extended self-dual Golay code is a group code for S_4 and D_{24}, the dihedral group of order 24. In particular a group code does not determine the group uniquely.

2 Self-dual group codes

Definition 2.1 Let M be an $\mathbb{F}G$-module and let $\mathbb{F} \cong \mathbb{F}\sum_{g\in G} g$ be the trivial module. The vector space $\mathrm{Hom}_{\mathbb{F}}(M, F)$ of all $\mathbb{F}$-linear maps from M to $\mathbb{F}$ becomes an $\mathbb{F}G$-module by

$$m(\alpha g) = (mg^{-1})\alpha)$$

for $m \in M, g \in G$ and $\alpha \in \mathrm{Hom}_{\mathbb{F}}(M, F)$. This module is denoted by M^* and called the dual module of M. If $M \cong M^*$ we say that M is a self-dual module.

There is a connection between the orthogonal $C^\perp$ of a group code C and its dual module C^*, namely $\mathbb{F}G/C^\perp \cong C^*$ which has the following crucial consequence when studying self-dual group codes.

Corollary 2.2 *If $C^\perp = \mathrm{C} \leq \mathbb{F}G$ is a self-dual group code, then the multiplicity of any irreducible self-dual $\mathbb{F}G$-module in $\mathbb{F}G$ is even.*

Applying this fact and some known results from modular representation theory we obtain the following.

Theorem 2.3 a) (Willems [21]) *The group algebra $\mathbb{F}G$ contains a self-dual group code if and only if the characteristic of $\mathbb{F}$ is 2 and the order $|G|$ of G is even.*
b) (Sloane, Thompson [19]; Martínez-Pérez, Willems [15]) *In* a) *we even can find doubly-even group codes if and only if the Sylow 2-subgroup is not cyclic nor a Klein four group.*

Note that the ternary extended Golay code is not a group code, but an ideal in a twisted group algebra over $G = \mathrm{A}_4$, the alternating group on 4 letters.

Theorem 2.4 (Günther, Nebe [9]) *If $\mathrm{C} = \mathrm{C}^\perp$ is a binary doubly even G-code, then G is a subgroup of the alternating group $\mathrm{A}_{|G|}$.*

Remark 2.5 The binary extended $[24, 12, 8]$ Golay code and as well, by a result of McLaughlin [13], the $[48, 24, 12]$ Pless symmetry are group codes. Note that a putative binary self-dual $[72, 36, 16]$ code can not be a group code since its automorphism group has oder less or equal 5, a result proved over the years until 2014 by many authors.

3 LCD group codes

Definition 3.1 (J. L. Massey) A linear code $C \leq \mathbb{F}^n$ is called a code with complementary dual, or shortly an LCD code, if $\mathbb{F}^n = \mathrm{C} \oplus \mathrm{C}^{\perp}$.

The condition $\mathbb{F}^n = \mathrm{C} \oplus \mathrm{C}^{\perp}$ is obviously equivalent to $C \cap C^{\perp} = 0$.

LCD codes are of general interest for several reasons. They are asymptotically good (Massey [16]) , achieve the Gilbert-Varshamov bound (Sendrier [18]) and play a crucial role to protect information against side channel or fault injection attacks (Carley and Guilley [6])

Lemma 3.2 LCD *group codes C share the following properties.*

(i) *C is a projective $\mathbb{F}G$-module.*

(ii) $|G|_p \mid \dim \mathrm{C}$ (*Dickson's Theorem*).

(iii) $\mathrm{C} \cong \mathrm{C}^*$ *as $\mathbb{F}G$-modules.*

On $\mathbb{F}G$ there is a natural anti-algebra automorphism defined by $\hat{}$ by $\hat{g} = g^{-1}$ for $g \in G$ and extended linearly. Using this map MacWilliams already described in an early paper that the dual code can be described via the multiplicative structure of $\mathbb{F}G$.

Lemma 3.3 (MacWilliams [12]) *If $\mathrm{C} \leq \mathbb{F}G$ is a group code, then $\mathrm{C}^{\perp} = \widehat{\mathrm{Ann}_l(C)}$.*

This together with properties (i) and (iii) lead to

Theorem 3.4 (de la Cruz, Willems [8]) A group code $C \leq \mathbb{F}G$ is an LCD code if and only if $C = e\mathbb{F}G$ with $e^2 = e = \hat{e} \in \mathbb{F}G$.

As an immediate consequence we get a result of Yang and Massey [22] which says that a cyclic code C if length n is an LCD code if and only if the generator polynomial g is self-reciprocal and the multiplicity of an irreducible polynomial in g is the same as in $x^n - 1$.

Remark 3.5 Let $C = e\mathbb{F}G$ with $e^2 = e = \hat{e} \in \mathbb{F}G$ be an LCD group code. Then
a) $C = \hat{C}$ (C is an adjoint code) if and only if e is in the center of $\mathbb{F}G$.
b) If C is also an MDS code then $\langle \mathrm{supp}(C) \rangle = G$.

Note that according to [6] there are LCD MDS group codes.

Problem 3.6 Does the existence of an LCD MDS group code $C \leq \mathbb{F}G$ imply that char $\mathbb{F}$ does not divide $|G|$? The answer is yes if G is abelian.

4 Checkable group codes

If $\mathrm{C} \leq \mathbb{F}^n$ is a linear code, then testing whether $\mathbf{x} \in \mathbb{F}^n$ belongs to C or not needs in general $n-k$ equations. The definition of checkable codes shows that they require only one test equation.

Definition 4.1 (Jitman, Ling, Liu, Xie [11]) a) Let A be a finite dimensional algebra over the field $\mathbb{F}$. A right ideal $I \leq A$ is called checkable if there exists an $a \in A$ such that $I = \mathrm{Ann}_r(a)$.
b) We say that A is code-checkable if all right ideals of A are checkable.

Examples 4.2 a) Let $e = e^2$ be an idempotent in A. Then the ideal eA is checkable. This can be seen as follows. Obviously, $eA \leq \mathrm{Ann}_r(A(1-e))$. Since any $0 \neq (1-e)b \in (1-e)A$ is not in $\mathrm{Ann}_r(A(1-e))$ we have $eA = \mathrm{Ann}_r(A(1-e))$.
b) LCD group codes C are checkable since $\mathrm{C} = e\mathbb{F}G$ with $e^2 = e = \hat{e}$.
c) All cyclic codes are checkable via the control polynomial.
d) A semisimple group algebra is code-checkable since all ideals (right or left) are generated by idempotents.

Lemma 4.3 *A group code $C \leq \mathbb{F}G$ is checkable if and only if $C^\perp$ is a principal ideal in $\mathbb{F}G$.*

We may decompose $\mathbb{F}G$ into a direct sum

$$\mathbb{F}G = B_0 \oplus B_1 \oplus \ldots \oplus B_s$$

of 2-sided indecomposable ideals B_i of $\mathbb{F}G$ (indecomposable as 2-sided ideals). Up to the labeling the B_i are uniquely determined by $\mathbb{F}G$ and called the blocks, or more presicely the p-blocks of $\mathbb{F}G$ if the characteristic of $\mathbb{F}$ is p.
The block which contains the trivial module is usually called the principal block.

Theorem 4.4 (Borello, de la Cruz, Willems [4]) *Let* char $\mathbb{F} = p$ *and let B be a p-block of $\mathbb{F}G$. Then the following are equivalent.*

a) *All right ideals in B are checkable, i.e., B is code-checkable.*

b) *All left ideals in B are principal.*

c) *B contains only one irreducible left module, say L, and its projective cover $P(L)$ is uniserial.*

Recall that a group G is p-nilpotent if G has a normal p-subgroup N with $p \nmid |N|$ such that G/N is a p-group. The equivalence of b) and c) has been proved already by Passman in 1977 [17].

Corollary 4.5 *Let* char $\mathbb{F} = p$ *and let B be the principal p-block of $\mathbb{F}G$. Then the following are equivalent.*

a) *B is code-checkable.*

b) *G is p-nilpotent with cyclic Sylow p-subgroups.*

c) *$\mathbb{F}G$ is code-checkable.*

Remark 4.6 In [11] 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 ones from [10]. 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 [10].

5 Asymptotically good classes of group codes

Theorem 5.1 (Stichtenoth [20]) *Group codes are asymptotically good over the field $\mathbb{F}_{q^2}$.*

Problem 5.2 Is the class of group codes asymtotically good over any finite field?

Theorem 5.3 (Bazzi, Mitter [1]) *In characteristic 2 the class of group codes in checkable group algebras is asymptotically good.*

Problem 5.4 Is the class of checkable group codes asymptotically good in odd characteristic?

References

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

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

[3] J.J. Bernal, A. del Río and J.J. Simón, An intrinsic description of group codes, *Des. Codes Cryptogr.* 51 (2009), 289-300.

[4] M. Borello, J. de la Cruz and W. Willems, Checkable codes in group algebras, Preprint 2018.

[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] C. Carlet and S. Guilley, Complementary dual codes for counter measures to side channel attack, in *Coding Theory and Appl.*, Springer 2002, 97-105.

[7] P. Charpin, Une généralisation de la construction de Berman des codes de Reed-Muller p-aire, *Comm. Algebra* 16 (1988), 2231-2246.

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

[9] A. Gúnther and G. Nebe, Automorphisms of doubly even self-dual binary codes, *Bull.London Math. Soc.* 41 (2009), 769-778.

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

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

[12] 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.

[13] I. McLaughlin, A group ring construction of the $[48, 24, 12]$ type II linear block code, *Des. Codes Cryptogr.* 63 (2012), 29-41.

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

[15] C. Martínez-Peréz and W. Willems, Self-dual codes and modules of finite groups in characteristic two, *IEEE Trans. Inform. Theory* 50 (2004), 1798-1803.

[16] J.L. Massey, Linear codes with complementary duals, *Discrete Math* 106/107 (1992), 337-342.

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

[18] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.* 285 (2204), 345-347.

[19] N.J.A. Sloane and J.G. Thompson, Self-dual cyclic codes, *IEEE Trans. Inform. Theory* 29 (1983), 364-366.

[20] H. Stichtenoth, Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound, *Trans. Inform. Theory* 52 (2006), 2218-2224.

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

[22] X. Yang and J.L. Massey, The necessary and sufficient condition for a cyclic code to have a complementary dual, *Discrete Math.* 126 (1994), 391-393.