Self-dual Extended Group Codes

Conchita Martínez-Pérez
Departamento de Matemáticas
Universidad de Zaragoza, 50009 Zaragoza

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

A group code is an ideal in a group algebra KG where K is a finite field and G a finite group. In this context many interesting codes turn out to be group codes, and those which are self-dual are of particular interest. As shown in [14], a group algebra contains a self-dual group code if and only if $|K|$ is a power of 2 and $2 \mid |G|$.

This talk deals with self-dual extended group codes C. As in [14], representation theory of finite groups will serve as the main tool used in the proofs. Strictly speaking we exploit the connection between the two duality functors $C \to C^{\perp}$ and $C \to C^* = \mathrm{Hom}_K(C, K)$ where C^* is considered as a KG-module via the action

$$(fg)(c) = f(cg^{-1}) \text{ for } f \in C^*, g \in G \text{ and } c \in C.$$

C is called a self-dual code if $C = C^{\perp}$ and a self-dual module if $C \cong C^*$.

Throughout, for reasons of simplicity, K is a field with two elements, i. e., all codes which we consider are binary. Furthermore, G always denotes a finite group of order $n = |G|$ and H a subgroup of G.

Definition a) A (H, G)-group code is a K-linear H-invariant subspace of KG where $\{g \mid g \in G\}$ serves as a natural basis. In other words, it is a KH-submodule of the regular module KG.
b) An extended (H, G)-group code is a K-linear H-invariant subspace of $K \oplus KG$ where the additional component K, on which G acts trivially, represents the parity check component.

A (G, G)-group code is briefly called a group code. It is a cyclic code if G is cyclic. A $(1, G)$- group code is nothing else than a linear code of length $|G|$.

Examples a) The binary $[24, 12, 8]$ Golay code is a group code for the symmetric group S_4 (see [4]).
b) Binary Reed-Muller codes are group codes for elementary abelian 2-groups (see [3]). They are also extended cyclic group codes for the Singer cycle of an appropriate general linear group (see [2], Corollary 5.4.1).

In order to state the first result we need further notations. For an odd $n \in \mathbb{N}$ let $s(n) \in \mathbb{N}$ denote the smallest number such that

$$n \mid 2^{s(n)} - 1.$$

In other words, $s(n)$ is the order of 2 in the unit group of $\mathbb{Z}_n$. Furthermore, let

$$s(H) = \operatorname{lcm}\{s(p) |\ 2 \neq p \text{ a prime}, p \mid |H|\}.$$

Finally, for $m \in \mathbb{N}$, let m_2 denote the 2-part of m. With these notations we have

Theorem 1 If G is of odd order then the following conditions are equivalent.

a) There exists a self-dual extended (H, G)-group code.

b) The trivial module is the only irreducible self-dual KH-module.

c) All irreducible KH-modules are of odd dimension.

d) $s(H)$ is odd.

The proof heavily depends on modular representation theory and Galois theory and will appear elsewhere, [10]. Note that the equivalence of b) and c) is quite of interest. It says that a non-trivial irreducible self-dual KH-module exists if and only if there exists an irreducible KH-module of even dimension. Clearly, any non-trivial irreducible self-dual KH-module is of even dimension by Fong's lemma (see [7], VII, 8.13), but the converse does not hold true in general.

We would also like to mention that part c) of Theorem 1 can easily be checked. For primes p with $p \equiv \pm 3 \bmod 8$ the number $s(p)$ is even. For all $p \equiv -1 \bmod 8$ we have $s(p)$ odd. Thus only for $p \equiv 1 \bmod 8$ and $p \mid |H|$ the order of 2 mod p has to be checked.

Example For a prime p with $p \equiv -1 \bmod 8$ we consider a binary extended code of length $p+1$. Note that $p \mid 2^{\frac{p-1}{2}} - 1$ since 2 is a square mod p. As $\frac{p-1}{2}$ is odd part d) of Theorem 1 holds true with H cyclic of order p. Thus there exists a binary self-dual extended cyclic group code of length $p+1$. Note that an extended QR-code is such a code.

A quasi-cyclic code is a (H, G)-group code where G is a cyclic group. If l denotes the cycle length then $|H| = \frac{|G|}{l} = \frac{n}{l}$. We call such codes l-qc codes. As an immediate consequence of Theorem 1 we have

Corollary If $l \mid n = 2m - 1$ then there exists a binary self-dual extended l-qc code of length $2m$ if and only if

$$\prod_{p \text{ a prime},\ 2 \neq p \mid \frac{n}{l}} s(p)$$

is odd.

Examples a) Let $1 < m \in \mathbb{N}$ be odd. Then for all primes p with $p \mid n = 2^m - 1$ we have $s(p) \mid m$. Thus $s(p)$ is odd and by the Corollary there exists a binary self-dual extended cyclic

group code of length 2^m. As an example a binary Reed-Muller code of odd rank m and order $\frac{m+1}{2}$ may serve. The group in question is generated by the Singer cycle of $\mathrm{GL}(m,2)$.
b) Let $m \in \mathbb{N}$ be even. Then $3 \mid 2^m - 1$ and $s(3) = 2$. Thus there is no binary self-dual extended cyclic group code of lenght 2^m. This result is also contained in [5].
If we specialize $m = 6$ and $l = 9$ we get $s(\frac{63}{9}) = s(7) = 3$. Thus there exists a binary self-dual extended 9-qc code of length 64.

Examples a) By a result of Sloane and Thompson [12], a binary self-dual group code always has weights congruent 2 mod 4 if the Sylow 2-subgroups are cyclic.
b) Let G be an elementary abelian 2-group. Let a be an element of the Jacobson radical J of KG, but not in J^2. Then, by Corollary 1 of [6], the ideal $C = \langle a \rangle$ generated by a is self-dual. Moreover C is doubly even if and only if the weight of a is divisible by 4.

The examples above indicate that for self-dual group codes the property *doubly even* depends on the structure of the underlying group. For extended group codes the situation is completely different. Here we have

Theorem 2 If C is a binary self-dual extended group code of length n then the following conditions are equivalent.

a) C is doubly even.

b) $n \equiv 0 \bmod 8$.

The implication a) $\Rightarrow$ b) is well known. It holds for any binary self-dual code. The proof is due to Gleason using methods from invariant theory (see [13], 3.3.22).
The converse b) $\Rightarrow$ a) is based on methods of representation theory. To give some flavour we will sketch the crucial parts of the proof.
Let $C = C^\perp \leq K \oplus KG$. By Theorem 1, the trivial module is the only irreducible self-dual KG-module. Thus, by Maschke's Theorem (see [1], p. 116), we have

$$KG = K \sum_{g \in G} g \oplus (W_1 \oplus \ldots \oplus W_t) \oplus (W_1^* \oplus \ldots \oplus W_t^*)$$

with irreducible non-trivial pairwise non-isomorphic KG-modules W_i. This leads to a decomposition of 1 into a sum of central idempotents

$$1 = e_0 + e + e^*$$

where $e_0 = \sum_{g \in G} g$. By a known result of Okuyama and Tsushima (see [11]), we now have $e^* = \bar{e}$ where the map $^- : KG \to KG$ is defined by the antiautomorphism $g \to g^{-1}$. Thus

$$1 = e_0 + e + \bar{e}$$

In particular $\mathrm{supp}(e) \cap \mathrm{supp}(\bar{e}) \subseteq \{1\}$ and $G \backslash \{1\} \subseteq \mathrm{supp}(e) \cup \mathrm{supp}(\bar{e})$. With $v = 1_K + e_0$ one easily gets that

$$C^\perp = C = vK + eKG$$

for some central idempotent e since $KG/C = KG/C^\perp \cong C^*$. Now observe that

$$wt(v) = n \equiv 0 \bmod 8.$$

Furthermore, $1 \in \mathrm{supp}(e)$ since otherwise

$$wt(e) = \frac{n-2}{2} = \frac{n}{2} - 1 \equiv 1 \bmod 2$$

a contradiction to the fact that e is an isotropic vector. Thus

$$wt(e) = \frac{n-2}{2} + 1 = \frac{n}{2} \equiv 0 \bmod 4,$$

since $8 \mid n$. This yields that C has a basis of vectors whose weights are divisible by 4 and by a well-known argument C is doubly even.

Examples a) Theorem 2 proves that the self-dual affine invariant codes of length $2^m (m \geq 3)$ constructed by Charpin and Levy-dit-Vehel in [5] are all doubly even.
b) Binary extended QR-codes of length $p+1$ are doubly even if $p \equiv -1 \bmod 8$, but only even if $p \equiv 1 \bmod 8$.

References

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

[2] E.F. Assmus and J.K. Key, Designs and their codes. Cambridge Universty Press, Cambridge 1992.

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

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

[5] P. Charpin and F. Levy-dit-Vehel, On self-dual affine-invariant codes. J. Comb. Theory Ser. A 67, 223-244 (1994).

[6] P. Charpin, Self-dual codes which are principal ideals of the group algebra $\mathbb{F}_2[\{F_{2^m}, +\}]$. J. Statistical Planning and Interference 56, 79-92 (1996).

[7] B. Huppert and N. Blackburn, Finite groups II, Springer, Berlin/Heidelberg/New York 1982.

[8] J.S. Leon, J.M. Masley and V. Pless, Duadic codes. IEEE Trans. Inform. Theory 30, 709-714 (1984).

[9] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes. North-Holland, Amsterdam 1977.

[10] C. Martínez-Pérez and W. Willems, Self-dual modules and self-dual codes for finite groups. Submitted 2002.
`http://fma2.math.uni-magdeburg.de/~willems/papers/Self_1.ps`

[11] T. Okuyama and T. Tsushima, On a conjecture of P. Landrock. J. Algebra 104, 203-208 (1986).

[12] N.J.A. Sloane and J.G. Thompson, Cyclic self-dual codes. Trans. Inform. Theory 29, 364-366 (1983).

[13] W. Willems, Codierungstheorie. deGruyter, Berlin, New York 1999.

[14] W. Willems, A note on self-dual group code. IEEE Trans. Inform. Theory 48 (12), 3107-3109 (2002).