



HAL
open science

A note on linear complementary pairs of group codes

Martino Borello, Javier de la Cruz, Wolfgang Willems

► **To cite this version:**

Martino Borello, Javier de la Cruz, Wolfgang Willems. A note on linear complementary pairs of group codes. *Discrete Mathematics*, 2020, 343 (8), pp.111905. 10.1016/j.disc.2020.111905 . hal-03852292

HAL Id: hal-03852292

<https://hal.science/hal-03852292>

Submitted on 14 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Note on Linear Complementary Pairs of Group Codes

Martino Borello,

LAGA, UMR 7539, CNRS, Université Paris 13 - Sorbonne Paris Cité,
Université Paris 8, F-93526, Saint-Denis, France.

and

Javier de la Cruz

Universidad del Norte, Barranquilla, Colombia

and

Wolfgang Willems

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

Keywords. Group code, linear complementary pair (LCP)

MSC classification. 94B05, 94B99, 20C05

Abstract

We give a short and elementary proof of the fact that for a linear complementary pair (C, D) , where C and D are 2-sided ideals in a group algebra, D is uniquely determined by C and the dual code D^\perp is permutation equivalent to C . This includes earlier results of [3] and [6] on nD cyclic codes which have been proved by subtle and lengthy calculations in the space of polynomials.

Throughout this note let K be a finite field. A pair (C, D) of linear codes over K of length n is called a *linear complementary pair* (LCP) if $C \cap D = \{0\}$ and $C + D = K^n$, or equivalently if $C \oplus D = K^n$. In the special case that $D = C^\perp$ where the dual is taken with respect to the Euclidean inner product the code C is referred to a *linear complementary dual* (LCD) code. LCD codes have first been considered by Massey in [7]. The nowadays interest of LCP codes aroused from the fact that they can be used in protection against side channel and fault injection attacks [1], [2], [4]. In this context the security of a linear complementary pair (C, D) can be measured by the *security parameter* $\min\{d(C), d(D^\perp)\}$. Clearly, if $D = C^\perp$, then the security parameter for (C, D) is $d(C)$.

Just recently, it has been shown in [3] that for linear complementary pairs (C, D) the codes C and D^\perp are equivalent if C and D are both cyclic or 2D cyclic codes under the assumption that the characteristic of K does not divide the length. In [6], this result has

been extended to the case that both C and D are n D cyclic for $n \in \mathbb{N}$. In both papers the proof is rather complicated and formulated in the world of polynomials.

Recall that an n D cyclic code is an ideal in the algebra

$$R_n = K[x_1, \dots, x_n] / \langle x^{m_1} - 1, \dots, x^{m_n} - 1 \rangle,$$

and that R_n is isomorphic to the group algebra KG where $G = C_{m_1} \times \dots \times C_{m_n}$ with cyclic groups C_{m_i} of order m_i . Thus the above mentioned results are results on ideals in abelian group algebras.

A linear code C is called a *group code*, or G -code, if C is a right ideal in a group algebra

$$KG = \left\{ a = \sum_{g \in G} a_g g \mid a_g \in K \right\}$$

where G is a finite group. The vector space $KG \cong K^{|G|}$ with basis $g \in G$ serves as the ambient space and the weight function is defined by $\text{wt}(a) = |\{g \in G \mid a_g \neq 0\}|$ (which corresponds to the classical weight function via the isomorphism $KG \cong K^{|G|}$). Note that KG carries a K -algebra structure via the multiplication in G . More precisely, if $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g$ are given, then

$$ab = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) g.$$

In this sense n D cyclic codes are group codes for abelian groups G and vice versa since a finite abelian group is the direct product of cyclic groups.

There is a natural K -linear anti-algebra automorphism $\hat{\cdot} : KG \rightarrow KG$ which is given by $g \mapsto g^{-1}$ for $g \in G$ (in the isomorphism $KG \cong K^{|G|}$, the automorphism $\hat{\cdot}$ corresponds to a permutation of the coordinates). Thus we may associate to each $a = \sum_{g \in G} a_g g \in KG$ the *adjoint* $\hat{a} = \sum_{g \in G} a_g g^{-1}$ and call a self-adjoint if $a = \hat{a}$.

In addition, the group algebra KG carries a symmetric non-degenerate G -invariant bilinear form $\langle \cdot, \cdot \rangle$ which is defined by

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

Here G -invariance means that $\langle ag, bg \rangle = \langle a, b \rangle$ for all $a, b \in KG$ and all $g \in G$. Via the isomorphism $KG \cong K^{|G|}$, the above form corresponds to the usual Euclidean inner product. With respect to this form we may define the dual code C^\perp of a group code $C \leq KG$ as usual and say that C is self-dual if $C = C^\perp$. Note that for a group code C the dual C^\perp is a right ideal since for all $c \in C$, $c^\perp \in C^\perp$ and $g \in G$ we have

$$\langle c, c^\perp g \rangle = \langle cg^{-1}, c^\perp \rangle = 0.$$

Thus with C the dual C^\perp is a group code as well.

In [9] we classified completely group algebras which contain self-dual ideals. More precisely, a self-dual G -code exists over the field K if and only if $|G|$ and the characteristic of K are even. In [5] we investigated LCD group codes and characterized them via self-adjoint idempotents $e^2 = e = \hat{e}$ in the group algebra KG .

In this short note we prove the following theorem which includes the above mentioned results of [3] and [6]. Observe that we require no assumption on the characteristic of the field K .

Theorem. Let G be a finite group. If $C \oplus D = KG$ where C and D are 2-sided ideals in KG , then D is uniquely determined by C and D^\perp is permutation equivalent to C . In particular $d(D^\perp) = d(C)$.

In order to prove the Theorem we state some elementary facts from representation theory.

Definition. If M is a right KG -module, then the dual vector space $M^* = \text{Hom}_K(M, K)$ becomes a right KG -module via

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

where $m \in M, \alpha \in M^*$ and $g \in G$. With this action M^* is called the *dual module* of M . Clearly, $\dim M^* = \dim M$.

Lemma A. (Okuyama-Tsushima, [8]) If $e = e^2 \in KG$, then $\hat{e}KG \cong eKG^*$. In particular, $\dim \hat{e}KG = \dim eKG$.

Proof: A short proof is given in Lemma 2.3 of [5]. □

Lemma B. If $D = eKG$ with $e^2 = e \in KG$, then $D^\perp = (1 - \hat{e})KG$.

Proof: First observe that $\hat{e}^2 = \hat{e}$ and that $\langle ab, c \rangle = \langle b, \hat{a}c \rangle$ for all $a, b, c \in KG$. Thus

$$\langle ea, (1 - \hat{e})b \rangle = \langle e^2a, (1 - \hat{e})b \rangle = \langle ea, \hat{e}(1 - \hat{e})b \rangle = 0$$

for all $a, b \in KG$. Hence, $(1 - \hat{e})KG \subseteq D^\perp$. As

$$\begin{aligned} \dim (1 - \hat{e})KG &= |G| - \dim \hat{e}KG \\ &= |G| - \dim eKG^* && \text{(by Lemma A)} \\ &= |G| - \dim eKG \\ &= \dim D^\perp \end{aligned}$$

we obtain $(1 - \hat{e})KG = D^\perp$. □

Proof of the Theorem: Since $C \oplus D = KG$ we may write $D = eKG$ and $C = (1-e)KG$ for a suitable central idempotent

$$e = e^2 \in Z(KG) = \{a \mid ab = ba \text{ for all } b \in KG\}$$

(see [5]). Lemma B says that $D^\perp = (1 - \hat{e})KG$. Via the map $\hat{\cdot} : KG \rightarrow KG$ the K -linear code $(1 - \hat{e})KG$ is permutation equivalent to the K -linear code $KG(1 - e)$. But $KG(1 - e) = (1 - e)KG = C$ since e is central, which completes the proof. \square

If C and D are only right ideals, then D is uniquely determined by C , but D^\perp , in general, is not necessarily permutation equivalent to C . It even may happen that $d(D^\perp) \neq d(C)$ as the next example shows.

Example. Let $K = \mathbb{F}_2$ and let

$$G = \langle a, b \mid a^7 = 1 = b^2, a^b = a^{-1} \rangle$$

be a dihedral group of order 14. If we put

$$e = 1 + a + a^2 + a^4 + b + a^2b + a^5b + a^6b,$$

then $e = e^2$. With MAGMA one easily computes $d((1 - e)KG) = 2$ and $d(KG(1 - e)) = 3$.

Now let $C = (1 - e)KG$ and $D = eKG$. By Lemma B, we have $D^\perp = (1 - \hat{e})KG$. Thus

$$d(D^\perp) = d((1 - \hat{e})KG) = d(KG(1 - e)) = 3,$$

but $d(C) = d((1 - e)KG) = 2$. We like to mention here that C and D are quasi-cyclic codes. \square

Remark. Let $|K| = q^2$. In this case we may consider the Hermitian inner product on KG which is defined by

$$\left\langle \sum_{g \in G} a_g g, \sum_{h \in G} b_h h \right\rangle = \sum_{g \in G} a_g b_g^q.$$

For $a = \sum_{g \in G} a_g g$ we put $a^{(q)} = \sum_{g \in G} a_g^q g$. With this notation we have

$$D^\perp = (1 - \widehat{e^{(q)}})KG$$

in Lemma B. Applying the anti-automorphism $\hat{\cdot} : KG \rightarrow KG$ we see that D^\perp is permutation equivalent to $KG(1 - e^{(q)})$. If in addition e is central, then $e^{(q)}$ is central. Thus D^\perp is permutation equivalent to $(1 - e^{(q)})KG = ((1 - e)KG)^{(q)}$.

It follow that

$$d(D^\perp) = d((1 - e)KG)^{(q)} = d((1 - e)KG) = d(C).$$

Thus, in the Hermitian case a linear complementary pair (C, D) of 2-sided group codes C and D also has security parameter $d(C)$.

References

- [1] S. BHASIN, J.-L. DANGER, S. GUILLEY, Z. NAJIM AND X.T. NGO, “Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses.” In *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust (HOST) 2015*, pp. 82-87.
- [2] J. BRINGER, C. CARLET, H. CABANNE, S. GUILLEY AND H. MAGHREBI, “Orthogonal direct sum making: A smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks.” in *Proc. WIST*, Springer 2014, pp. 40-56.
- [3] C. CARLET, C. GÜNERI, F. ÖZBUDAK, B. ÖZKAYA AND P. SOLÉ, “On linear complementary pairs of codes.” *IEEE Trans. Inform. Theory*, vol. 64, pp. 6583-6589, 2018.
- [4] C. CARLET and S. GUILLEY, “Complementary Dual Codes for Counter-measures to Side-Channel Attacks. In “Coding Theory and Applications.” Eds. R. Pinto, P. Rocha Malonek and P. Vettorey, *CIM Series in Math. Sciences*. vol. 3, pp. 97-105, Springer 2015.
- [5] J. DE LA CRUZ AND W. WILLEMS, “ On group codes with complementary duals.” *Des. Codes Cryptogr.*, vol. 86, pp. 2065-2073, 2018.
- [6] C. GÜNERI, B. ÖZKAYA AND S. SAYICI, “On linear complementary pair of nD cyclic codes.” *IEEE Commun. Lett.*, vol. 22, pp. 2404-2406, 2018.
- [7] J.L. MASSEY, “Linear codes with complementary duals.” *Discrete Math.*, vol. 106/107, 337-342, 1992.
- [8] T. OKUYAMA AND Y. TSUSHIMA, “On a conjecture of P. Landrock.” *J. of Algebra*, vol. 104, pp. 203-208, 1986.
- [9] W. WILLEMS, “A note on self-dual group codes.” *IEEE Trans. Inf. Theory*, vol. 48, pp. 3107-3109, 2002.