Nonbinary Delsarte-Goethals codes and finite semifields

I.F. Rúa*

Abstract

Symplectic finite semifields can be used to construct nonlinear binary codes of Kerdock type (i.e., with the same parameters of the Kerdock codes, a subclass of Delsarte-Goethals codes). In this paper we introduce nonbinary Delsarte-Goethals codes of parameters $(q^{m+1}\ ,\ q^{m(r+2)+2}\ ,\ \frac{q-1}{q}(q^{m+1}-q^{\frac{m+1}{2}+r})\ )$ over a Galois field of order $q=2^l$, for all $0 \leq r \leq \frac{m-1}{2}$, with $m \geq 3$ odd, and show the connection of this construction to finite semifields.

Keywords: Delsarte-Goethals code, finite semifield, Galois ring, quadratic form, bilinear form.
MSC2010: 11T71, 11E08, 17D99.

1 Introduction

Some classical constructions of nonlinear (binary) codes, such as Kerdock [13], Preparata [30] or Delsarte-Goethals [7] codes, were introduced around 1970. All of them share the common property that they can be seen as the union of cosets of a linear code in a Reed-Muller code [26, 31]. This is the way they are described in the contemporary classic book [23, Chapter 15].

A better understanding of these codes and the relations amongst them came from the introduction of quaternary codes (i.e., codes over the alphabet $\mathbb{Z}/4\mathbb{Z}$) in their study. A pioneer work in this direction is the $\mathbb{Z}/4\mathbb{Z}-$cyclic version of the (punctured) Kerdock code provided by Nechaev in [28] (and announced as early as in 1982 [27]). A key contribution came from the seminal work of Hammons, Kumar, Calderbank, Sloane and Solé [9], where the $\mathbb{Z}/4\mathbb{Z}-$duality of the Kerdock and Preparata codes was shown. In these papers Galois rings $GR(2^{2m}, 2^2)$ of cardinality 2^{2m} and characteristic 2^2 appeared naturally as ring extensions of the alphabet $\mathbb{Z}/4\mathbb{Z}$. The quaternary version of these codes connects them to low-correlation sequences [2, 15], in particular to the sequence family $S(2)$ appearing in the W-CDMA component of the IMT-2000 standard for 3G mobile communication [16].

Later authors exploited other Galois rings with quotient finite field of characteristic 2 to obtain new families of codes. For instance, Kuzmin and Nechaev constructed nonbinary versions (over the alphabet $\mathbb{F}_{2^l}$) of the classical Kerdock code (*Generalized Kerdock codes*) by using Galois rings of the form $GR(2^{2lm}, 2^2)$, i.e., of cardinality 2^{2lm} and characteristic 2^2 $(l > 1)$ [18]. Carlet introduced generalized (binary) versions of Kerdock and Delsarte-Goethals codes, constructed from Galois rings $GR(2^{km}, 2^k)$, i.e., of cardinality 2^{km} and characteristic $2^k > 4$ [5]. Also, a nonbinary generalization (over the alphabet $\mathbb{F}_{2^l}$) of the Preparata code was proposed by Kuzmin, Markov, Nechaev and Neljubin, again with the use of the Galois ring $GR(2^{2lm}, 2^2)$ $(l > 1)$[20].

On a different direction, nonequivalent codes with the same parameters of the binary Kerdock code were introduced by Calderbank, Cameron, Kantor and Seidel [4] using orthogonal and symplectic spreads [11]. This construction is closely related to symplectic finite semifields, a particular

*Departamento de Matemáticas, Universidad de Oviedo, rua@uniovi.es (+34)985103344 (Fax: 3354) Partially supported by MTM - 2017 - 83506 - C2 - 2 - P and FC-GRUPIN-IDI/2018/000193.

class of finite nonassociative division rings in the Knuth orbit of a commutative semifield [12]. The $\mathbb{Z}/4\mathbb{Z}-$valued quadratic forms introduced by Brown [3], proved to be useful in this context. These forms have also been fruitful in the study of quaternary sequence families (see, for instance, [33]), where properties of sets of bilinear forms over the binary field arise naturally. Notice that these sets appeared already in the original description of some of the codes mentioned above [7, 23].

In this paper we introduce a nonbinary version (over the alphabet $\mathbb{F}_{2^l}$) of the Delsarte-Goethals codes. The construction is based on Galois rings of the form $GR(2^{2lm}, 2^2)$ $(l > 1)$, and on the quadratic forms valued in them [22]. These forms were first used to introduce a framework for the construction of nonequivalent Generalized Kerdock codes from symplectic semifield spreads [8], as a generalization of the binary methods in [4]. Sets of ordinary bilinear forms over an arbitrary finite field of characteristic 2 [34] have been naturally considered in our construction. Namely, the construction is related to the set of alternating bilinear forms over the finite field $\mathbb{F}_{2^l}$ originally considered by Delsarte and Goethals [7, Theorem 9]. The construction is also connected to finite semifields.

The structure of the paper is as follows. §2 is devoted to preliminaries: the properties of bilinear and quadratic forms over finite fields and Galois rings needed in the paper are collected there. In §3, we introduce the Generalized Delsarte-Goethals codes and obtain their minimum distance by explicitly computing the ideal weight enumerator of the Galois ring linear codes they are derived from. Finally, in §4 we show the connection of this construction to finite semifields.

2 Preliminaries

In this section we collect all the preliminary results on bilinear and quadratic forms over finite fields and Galois rings required in the rest of the paper.

2.1 Finite fields

Through this paper q will always be a prime power 2^l, and $\mathbb{F}_{q^m}$ will denote the finite field with q^m elements ($m \in \mathbb{N}$). The new construction of Delsarte-Goethals codes will be obtained for $l > 1$ and $m \geq 3$ odd. Notice that the map $\sqrt{\cdot} : \mathbb{F}_q \to \mathbb{F}_q$ given by $x \to \sqrt{x} = x^{\frac{q}{2}}$ is a field automorphism. The trace function of the field extension $\mathbb{F}_{q^m}|\mathbb{F}_q$ will be written as $\mathrm{tr}_q^{q^m}$ or simply as tr. It is an $\mathbb{F}_q-$linear map and so we will denote its kernel by $\ker(\mathrm{tr})$. The absolute trace is the trace function of the field extension $\mathbb{F}_{q^k}|\mathbb{F}_2$. It will be denoted as Abstr [21].

2.1.1 Quadratic and bilinear forms over finite fields

Classical quadratic forms over finite fields (and in particular in characteristic 2) are well-known and we refer to [21, Chapter 5, Section 2] or [25, Section 7.2] for definitions and properties.

Let $Q : \mathbb{F}_q^m \to \mathbb{F}_q$ be a quadratic form (i.e., a homogeneous polynomial of degree 2). Then the associated bilinear form $B_Q : \mathbb{F}_q^m \times \mathbb{F}_q^m \to \mathbb{F}_q$ (the *polarisation* of Q) given by $B_Q(x, y) = Q(x + y) + Q(x) + Q(y)$ is symplectic and it has even rank $2s \in \{0, \ldots, m\}$. Moreover, Q is equivalent (under an invertible linear change of variables) to exactly one of the following quadratic forms:

- H_{2s}: $x_1x_2 + \ldots + x_{2s-1}x_{2s}$;
- E_{2s}: $x_1x_2 + \ldots + x_{2s-3}x_{2s-2} + x_{2s-1}^2 + x_{2s-1}x_{2s} + \beta x_{2s}^2$, where $\mathrm{Abstr}(\beta) = 1$;
- P_{2s}: $x_1x_2 + \ldots + x_{2s-1}x_{2s} + x_{2s+1}^2$

Following [10, Chapter 5] we will call these forms *hyperbolic*, *elliptic* and *parabolic*, respectively. The radical of Q is defined as the radical of B_Q, i.e, the set $\mathrm{rad}(Q) = \mathrm{rad}(B_Q) = \{x \in \mathbb{F}_q \mid B_Q(x, y) = 0, \forall y \in \mathbb{F}_q\}$, and it has dimension $m - 2s$. A well-known example of polarisation is the following:

$$B_Q(x, y) = \mathrm{tr}\left(\sum_{i=1}^{r} a_i(x^{q^i}y + xy^{q^i})\right), \text{ where } Q(x) = \mathrm{tr}\left(\sum_{i=1}^{r} a_i x^{q^i+1}\right), \text{ with } a_i \in \mathbb{F}_{q^m} \tag{1}$$

Proposition 1. *For all $b \in \mathbb{F}_q$, denote $\nu(b) = q(1 - b^{q-1}) - 1$ ($\nu(0) = q - 1, \nu(b) = -1$ otherwise). Let $Q : \mathbb{F}_q^m \to \mathbb{F}_q$ be a quadratic form which polarises to a bilinear form of rank $0 \le 2s \le m$. Then:*

1. *The number of solutions to the equation $Q(x_1, \dots, x_m) = b$ is:*
   - *(a) $q^{m-1} + \nu(b)q^{m-s-1}$, if Q is of hyperbolic type H_{2s};*
   - *(b) $q^{m-1} - \nu(b)q^{m-s-1}$, if Q is of elliptic type E_{2s};*
   - *(c) q^{m-1}, if Q is of parabolic type P_{2s};*
2. *Let $H : \mathbb{F}_q^m \to \mathbb{F}_q$ be a nonzero linear form $H(x_1, \dots, x_m) = \sum_{i=1}^m a_i x_i$, and let $u, v \in \mathbb{F}_q$. Then, the number of solutions to the system of equations $\{\ H(x_1, \dots, x_m) = u\ ,\ Q(x_1, \dots, x_m) = v$ is:*
   - *(a) $q^{m-2} \pm \nu(v)q^{m-s-2}$, if Q is of hyperbolic$(+)$/elliptic$(-)$ type H_{2s}/E_{2s}, and there exists $i > 2s$ such that $a_i \neq 0$;*
   - *(b) q^{m-2}, if Q is of parabolic type P_{2s}, and there exists $i > 2s + 1$ such that $a_i \neq 0$;*
   - *(c) $q^{m-2} \pm \nu(v)q^{m-s-1}$, if Q is of hyperbolic$(+)$/elliptic$(-)$ type H_{2s}/E_{2s}, $a_{2s+1} = \ldots = a_m = 0$, and $Q(a_1, \dots, a_m) = u = 0$;*
   - *(d) $q^{m-2} \pm (-1)^{\mathrm{Abstr}(vQ(a_1,\dots,a_m)/u^2)}q^{m-s-1}$, if Q is of hyperbolic$(+)$/elliptic$(-)$ type H_{2s}/E_{2s}, $a_{2s+1} = \ldots = a_m = 0$, and $Q(a_1, \dots, a_m) \neq 0 \neq u$;*
   - *(e) q^{m-2}, if Q is of hyperbolic$(+)$/elliptic$(-)$ type H_{2s}/E_{2s}, $a_{2s+1} = \ldots = a_m = 0$, and $Q(a_1, \dots, a_m) \neq 0 = u$ or $Q(a_1, \dots, a_m) = 0 \neq u$;*
   - *(f) q^{m-2}, if Q is of parabolic type P_{2s}, and $a_{2s+1} = \ldots = a_m = 0$;*
   - *(g) $q^{m-2} + (-1)^{\mathrm{Abstr}((Q(a_1,\dots,a_m) - a_{2s+1}^2)/a_{2s+1}^2)}\nu(v + (u/a_{2s+1})^2)q^{m-s-2}$, if Q is of parabolic type P_{2s}, and $a_{2s+1} \neq 0 = a_{2s+2} = \ldots = a_m$.*

Proof. The first part is [21, Theorem 6.32], where as the second part consists of particular cases of [14, Propositions 3.3 and 3.4]. Namely, items $2(a)(b)$ fall into Proposition 3.3 (taking $c_l = s = d_l = R(\overline{d}) = d_m = 0$ there). On the other hand, items $2(c)(d)(e)$ are particular cases of Proposition 3.4 $1.a.b$ (observe that $D(\overline{a}, \overline{c}) = R(\overline{c}) = 0$ there). Also, item $2(f)$ corresponds to Proposition 3.4 $2.a$. Finally, item $2(g)$ is Proposition 3.4 case $2.c$ (because $\overline{c} = \overline{0}, D(\overline{a}, \overline{c}) = 0$ there).

□

Next, we introduce a technical lemma on bilinear forms that will be used in the proof of some results of the paper (see Proposition 2 and Theorem 1 below).

Lemma 1. *Let f be a nonzero linear form over $\mathbb{F}_q^m$, and let $B : \mathbb{F}_q^m \times \mathbb{F}_q^m \to \mathbb{F}_q$ be a symplectic bilinear form of rank $0 \le 2s < m$. Then, there exists a symplectic basis $\mathcal{E} = \{e_1, \dots, e_m\}$ for the metric space $(\mathbb{F}_q^m, B)$ (i.e., $B(e_{2i-1}, e_{2i}) = 1$ for all $1 \le i \le s$, and $B(e_i, e_j) = 0$ otherwise) such that exactly one of the following two alternatives holds:*

1. *$f(e_i) = \delta_{im}$, when $\mathrm{rad}(B) \nsubseteq \ker f$. In this case $\mathrm{rank}(B|_{\ker f}) = 2s = \mathrm{rank}(B)$ ($B|_{\ker f}$ is the restriction of the bilinear form B to the subspace $\ker f$), and the rank of the bilinear form $B + f^2$ given by $B(x, y) + f(x)f(y)$ is $\mathrm{rank}(B) + 1$;*

2. *$f(e_i) = \delta_{i1}$, when $\mathrm{rad}(B) \subseteq \ker f$. In this case $\mathrm{rank}(B|_{\ker f}) = 2(s - 1) = \mathrm{rank}(B) - 2$, and $\mathrm{rank}(B + f^2) = \mathrm{rank}(B)$.*

Proof. Since f is nonzero there exists $v \in \mathbb{F}_q^m$ such that $f(v) = 1$, and so $\mathbb{F}_q^m = \ker f \oslash \langle v\rangle$. If $v \in \mathrm{rad}(B)$, then the direct sum of subspaces is also an orthogonal direct sum of subspaces $\mathbb{F}_q^m = \ker f \boxplus \langle v\rangle$ (where the symbol $\boxplus$ means orthogonal direct sum). We can add v to a symplectic basis $\{e_1, \ldots, e_{m-1}\}$ of the restricted form $B|_{\ker f}$ to construct the desired basis $\mathcal{E} = \{e_1, \ldots, e_{m-1}, e_m = v\}$. Moreover, in this situation $\mathrm{rank}(B|_{\ker f}) = \mathrm{rank}(B)$. Also, $B(e_m, e_m) + f(e_m)f(e_m) = 1$ and, for all $1 \le i \ne j \le m$, $B(e_i, e_j) + f(e_i)f(e_j) = 0$, i.e., $\mathrm{rank}(B + f^2) = \mathrm{rank}(B) + 1$.

On the other hand, if $\mathrm{rad}(B) \subseteq \ker f$, then choose a basis $\{v_1, \ldots, v_{m-2s}\}$ of $\mathrm{rad}(B)$, and complete it to a basis of $\ker f$: $\{v_1, \ldots, v_{m-2s}, v_{m-2s+1}, \ldots, v_{m-1}\}$. Take $v \in \mathbb{F}_q^m$ such that $f(v) \ne 0$, and consider the orthogonal direct sum of subspaces $\mathbb{F}_q^m = \mathrm{rad}(B) \boxplus S$, where $S = \langle v_{m-2s+1}, \ldots, v_{m-1}, v\rangle$. The restriction $B|_S$ is nonsingular [32, Theorem 11.7] and so the dimension of the orthogonal complement $T^{\perp_S}$ of $T = \langle v_{m-2s+1}, \ldots, v_{m-1}\rangle$ in S is one [32, Theorem 11.8]. Take $0 \ne w \in T^{\perp_S}$, and observe that $w \in T$ (otherwise, since B is alternating, $w \in (\mathrm{rad}(B) \boxplus T \boxplus \langle w\rangle)^\perp = (\mathbb{F}_q^m)^\perp = \{0\}$, a contradiction). Therefore, we can complete w to a basis $\{w, w_{m-2s+2}, \ldots, w_{m-1}\}$ of T. Because $B|_S$ is nonsingular, the dimension of the orthogonal complement $U^{\perp_S}$ of $U = \langle w_{m-2s+2}, \ldots, w_{m-1}\rangle$ in S is two. Since $U \subseteq T$, we have $w \in T^{\perp_S} \subseteq U^{\perp_S}$, and so we can take a basis $\{w, z\}$ of $U^{\perp_S} \subseteq S$. We claim that $z \notin T$. This is because $w \in T^{\perp_S}$, and if $z \in T$, then $z \in S \cap (\langle w\rangle + U)^\perp = S \cap T^\perp = T^{\perp_S} = \langle w\rangle$, a contradiction. So, $z \notin T$ and $\mathbb{F}_q^m = \langle z, w\rangle \boxplus U \boxplus \mathrm{rad}(B)$. Because $\langle w\rangle \boxplus U \boxplus \mathrm{rad}(B) = T \boxplus \mathrm{rad}(B) = \ker f$, we must have $\mu = f(z) \ne 0$. Clearly, the restriction $B|_{\langle z,w\rangle}$ has rank two (otherwise $\mathrm{rad}(B) = \langle z, w\rangle \boxplus \mathrm{rad}(B)$, a contradiction), and so $B(\mu^{-1}z, w) = \lambda \ne 0$. The hyperbolic pair $\{e_1 = \mu^{-1}z, e_2 = \lambda^{-1}w\}$ can be completed with elements of $U \boxplus \mathrm{rad}(B)$ to the desired symplectic basis $\mathcal{E} = \{e_1, \ldots, e_m\}$ (observe that $f(e_1) = 1$).

In this case the restriction $B|_{\ker f}$ has a symplectic basis $\{e_2, \ldots, e_m\}$ with hyperbolic pairs $(e_3, e_4), \ldots, (e_{2s-1}, e_{2s})$, i.e., $\mathrm{rank}(B|_{\ker f}) = \mathrm{rank}(B) - 2$. Finally, $B(e_m, e_m) + f(e_m)f(e_m) = 0$ and, for all $1 \le i \ne j \le m$, $B(e_i, e_j) + f(e_i)f(e_j) = 0$. Since $B(e_1, e_1) + f(e_1)f(e_1) = B(e_1 + e_2, e_1 + e_2) + f(e_1 + e_2)f(e_1 + e_2) = 1$, we have $\mathrm{rank}(B + f^2) = \mathrm{rank}(B)$. □

2.1.2 Sets of bilinear and quadratic forms over finite fields

Since classical Delsarte-Goethals codes are related to sets of binary bilinear forms [23, Chapter 15], one would expect that the study of nonbinary Delsarte-Goethals codes depend on properties sets of bilinear forms over finite fields of characteristic two. In this subsection we introduce the results on sets of bilinear (and also quadratic) forms needed for such a study. We refer the reader to [7, 33] for details.

Proposition 2. *Let m be an odd integer, $n = \frac{m-1}{2}$, and $0 \le r \le \frac{m-1}{2}$. Denote by $\begin{bmatrix} a \\ b \end{bmatrix}$ the q^2-ary Gaussian binomial coefficient [7]. For all $a_0^0 \in \mathbb{F}_{q^m}$, let*

$$\mathcal{A}_r^{a_0^0} = \left\{ \mathrm{tr}\left(a_0^0 xy\right) + \mathrm{tr}\left(\sum_{i=1}^{r} a_i(x^{q^i}y + xy^{q^i})\right) \mid a_i \in \mathbb{F}_{q^m} \right\}, \mathcal{B}_r^{a_0^0} = \left\{ B(x, y) + \mathrm{tr}\left(\sqrt{a_0^0}x\right) \mathrm{tr}\left(\sqrt{a_0^0}y\right) \mid B \in \mathcal{A}_r^{a_0^0} \right\}$$

Then:

1. *The number of forms of rank i in the set $\mathcal{B}_r^0$ is:*

$$B_r(m-2k-1) = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{r} (-1)^{j-k} (q^2)^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} (q^{m(r-j)} - 1)$$

   for all $0 \leq k \leq \frac{m-3}{2}$, $B_r(0) = 1$, and $B_r(i) = 0$ for other values of i.

2. *The number $B'_r(i)$ of forms of rank i in the multiset $\mathcal{B}'_r = \cup_{a_0^0 \in \mathbb{F}_{q^m}} \mathcal{B}_r^{a_0^0}$ is:*
   - *(a) $B_{r+1}(i)$, for all $i \geq 0$, when $r < \frac{m-1}{2}$;*
   - *(b) $q^m \cdot B_{\frac{m-1}{2}}(i)$, for all $i \geq 0$, when $r = \frac{m-1}{2}$. Moreover, every form appears exactly once in each of the q^m subsets $\mathcal{B}_{\frac{m-1}{2}}^{a_0^0}$ (for all $a_0^0 \in \mathbb{F}_{q^m}$).*

3. *The number $B_r^1(i)$ of forms of rank i in the set $\mathcal{B}_r^1$ is:*
   - *(a) $\frac{B_{r+1}(i) - B_r(i)}{q^m - 1}$, for all $i \geq 0$, when $r < \frac{m-1}{2}$;*
   - *(b) $B_{\frac{m-1}{2}}(i)$, for all $i \geq 0$, when $r = \frac{m-1}{2}$.*

4. *The number of forms of rank i in the set $\mathcal{A}'_r = \cup_{a_0^0 \in \mathbb{F}_{q^m}} \mathcal{A}_r^{a_0^0}$ is:*

$$A_r(m-2k) = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{r} (-1)^{j-k} (q^2)^{\binom{j-k}{2}} \begin{bmatrix} n+1-k \\ n+1-j \end{bmatrix} (q^{m(r-j+1)} - 1)$$

$$A_r(m-2l+1) = (q^2)^{n-l+1} \begin{bmatrix} n \\ l-1 \end{bmatrix} \sum_{j=l}^{r} (-1)^{j-l} (q^2)^{\binom{j-l}{2}} \begin{bmatrix} n+1-l \\ n+1-j \end{bmatrix} (q^{m(r-j+1)} - 1)$$

   for all $0 \leq k \leq \frac{m-1}{2}$, $1 \leq l \leq \frac{m-1}{2}$, $A_r(0) = 1$, and $A_r(i) = 0$ for other values of i.

5. *The number $A_r^1(i)$ of forms of rank i in the set $\mathcal{A}_r^1$ is $\frac{A_r(i) - B_r(i)}{q^m - 1}$, for all $i \geq 0$.*

6. *The number $D_r(i)$ of forms of rank i in $\mathcal{B}_r^1$ for which the restriction to* $\ker \mathrm{tr}$ *has different rank is $D_r(i) = A_r^1(i)$, if i is even, and $D_r(i) = 0$, if i is odd.*

Proof. 1. [34, Theorems 14 and 9][33, Result 6].

2. (a) It is clear that $\mathcal{B}'_r$ is a (multi)set of $q^{m(r+1)}$ alternating forms (since $\mathrm{tr}(x^2) = \mathrm{tr}(x)^2$) containing the zero form ($a_0^0 = a_i = 0$). If we show that it is an $(m, m-(2r+1))-$set (i.e., if $\mathrm{rank}(B_1 - B_2) \geq m - (2r+1)$, for all different $B_1, B_2 \in \mathcal{B}'_r$) then it attains the Singleton bound, and we can use [33, Theorems 6 and 9] to prove the result (see also [7, Theorem 4]). So, consider a difference of two forms $B_1, B_2 \in \mathcal{B}'_r$ ($B_1 \neq B_2$):

$$\mathrm{tr}\left(\left(a_0^0 - b_0^0\right) xy\right) + \mathrm{tr}\left(\sqrt{a_0^0 x}\right) \mathrm{tr}\left(\sqrt{a_0^0 y}\right) - \mathrm{tr}\left(\sqrt{b_0^0 x}\right) \mathrm{tr}\left(\sqrt{b_0^0 y}\right) + \mathrm{tr}\left(\sum_{i=1}^{r} (a_i - b_i)(x^{q^i} y + x y^{q^i})\right)$$

$$= \mathrm{tr}\left(y \left(a_0^0 - b_0^0\right) x\right) + \mathrm{tr}\left(y \left(\sqrt{a_0^0}\,\mathrm{tr}\left(\sqrt{a_0^0 x}\right) - \sqrt{b_0^0}\,\mathrm{tr}\left(\sqrt{b_0^0 x}\right)\right)\right)$$

$$+\mathrm{tr}\left(y\sum_{i=1}^{r}(a_i-b_i)x^{q^i}\right)+\mathrm{tr}\left(y\sum_{i=1}^{r}(a_i-b_i)^{q^{-i}}x^{q^{-i}}\right)$$

$$=\mathrm{tr}\left(y\left(\left(\sum_{i=1}^{r}(a_i-b_i)^{q^{-i}}x^{q^{-i}}+\left(a_0^0-b_0^0\right)x+\sum_{i=1}^{r}(a_i-b_i)x^{q^i}\right)+\sqrt{a_0^0}\mathrm{tr}\left(\sqrt{a_0^0}x\right)-\sqrt{b_0^0}\mathrm{tr}\left(\sqrt{b_0^0}x\right)\right)\right)$$

Such a difference has the form $\mathrm{tr}(y(L(x)+p(x)))$ where $L(x)$ is a $q-$polynomial and $p(x)=\sqrt{a_0^0}\mathrm{tr}\left(\sqrt{a_0^0}x\right)-\sqrt{b_0^0}\mathrm{tr}\left(\sqrt{b_0^0}x\right)$ is a polynomial function in x which can only take $s\leq q^2$ different values $v_1,\ldots,v_s$ (because the trace function is $\mathbb{F}_q-$valued). Therefore, $x\in\mathrm{rad}(B_1-B_2)$ if and only if $\mathrm{tr}(y(L(x)+p(x)))=0$ for all $y\in\mathbb{F}_{q^m}$, i.e., if and only if $L(x)+p(x)=0$, and so:

$$\mathrm{rad}(B_1-B_2)=\bigcup_{i=1}^{s}\{x\in\mathbb{F}_{q^m}\mid L(x)=v_i=p(x)\}\subseteq\bigcup_{i=1}^{s}\{x\in\mathbb{F}_{q^m}\mid L(x)=v_i\}$$

Hence, $\#\mathrm{rad}(B_1-B_2)\leq s\cdot q^{2r}\leq q^{2r+2}$, because the number of solutions to the equation $L(x)=v_i$ is either 0 or the number of solutions to the homogeneous equation $L(x)=0$. This number is at most q^{2r} because $L(x)$ is a $q-$polynomial with exponents ranging from q^{-r} to q^r. Therefore, $\mathrm{rank}(B_1-B_2)\geq m-(2r+2)$. But, since B_1-B_2 is alternating, its rank has to be even, and so $m-(2r+2)$ is not possible (because m is odd). Hence, $\mathrm{rank}(B_1-B_2)\geq m-(2r+1)$, as desired.

(b) When $r=\frac{m-1}{2}$, for all $B\in\mathcal{B}'_{\frac{m-1}{2}}$ we have $B(x,y)=\mathrm{tr}(y\tilde{L}(x))$ with

$$\tilde{L}(x)=\sqrt{a_0^0}\mathrm{tr}\left(\sqrt{a_0^0}x\right)+a_0^0x+\sum_{i=1}^{\frac{m-1}{2}}\left((a_ix)^{q^{-i}}+a_ix^{q^i}\right)$$

For every $a_0^0\in\mathbb{F}_{q^m}$ we can choose $a_i=\sqrt{(a_0^0)^{q^i+1}}$, for all $1\leq i\leq\frac{m-1}{2}$, so that $a_i^{q^{-i}}=\sqrt{((a_0^0)^{q^i+1})^{q^{-i}}}=\sqrt{(a_0^0)^{1+q^{-i}}}$. Therefore:

$$\sum_{i=1}^{\frac{m-1}{2}}\left((a_ix)^{q^{-i}}+a_ix^{q^i}\right)=\sum_{i=1}^{\frac{m-1}{2}}\left(\sqrt{(a_0^0)^{1+q^{-i}}}x^{q^{-i}}+\sqrt{(a_0^0)^{q^i+1}}x^{q^i}\right)$$

$$=\sqrt{a_0^0}\sum_{i=1}^{m-1}\left(\sqrt{a_0^0}x\right)^{q^i}=\sqrt{a_0^0}\left(\mathrm{tr}\left(\sqrt{a_0^0}x\right)-\sqrt{a_0^0}x\right)$$

and so $\tilde{L}(x)=0$.

This means that the zero form appears q^m different times in the multiset $\mathcal{B}'_{\frac{m-1}{2}}$. Let us denote these zero forms by $B_{a_0^0}$, for all $a_0^0\in\mathbb{F}_{q^m}$. Now, the multiset $\mathcal{B}'_{\frac{m-1}{2}}$ can be written as the disjoint union of q^m (multi)cosets: $\mathcal{B}'_{\frac{m-1}{2}}=\left\{B_{a_0^0}+B\mid a_0^0\in\mathbb{F}_{q^m},B\in\mathcal{B}^0_{\frac{m-1}{2}}\right\}$. The first part of the proposition gives us the rank distribution of $\mathcal{B}'_{\frac{m-1}{2}}$.

3. (a) Observe that, for all $a_0^0,a_i\in\mathbb{F}_{q^m}$ ($a_0^0\neq0$), the ranks of the forms $\mathrm{tr}\left(a_0^0xy\right)+\mathrm{tr}\left(\sqrt{a_0^0}x\right)\mathrm{tr}\left(\sqrt{a_0^0}y\right)+\mathrm{tr}\left(\sum_{i=1}^{r}a_i(x^{q^i}y+xy^{q^i})\right)\in\mathcal{B}_r^{a_0^0}$, and $\mathrm{tr}\left(xy\right)+\mathrm{tr}\left(x\right)\mathrm{tr}\left(y\right)+\mathrm{tr}\left(\sum_{i=1}^{r}a_i\sqrt{(a_0^0)^{-q^i-1}}(x^{q^i}y+xy^{q^i})\right)\in$

$\mathcal{B}_r^1$ is the same. Therefore, there is a bijection between the sets $\mathcal{B}_r^1$ and $\mathcal{B}_r^{a_0^0}$ that preserves ranks. Since $\mathcal{B}'_r = \dot{\cup}_{a_0^0 \in \mathbb{F}_{q^m}} \mathcal{B}_r^{a_0^0}$, for all $i \geq 0$ we have $B'_r(i) = B_r(i) + (q^m - 1)B_r^1(i)$, and so item 2 can be used to get the desired result.

(b) The proof of the second part of the proposition shows that the rank distribution of $\mathcal{B}^1_{\frac{m-1}{2}}$ is that of $\mathcal{B}^0_{\frac{m-1}{2}}$, and so $B^1_{\frac{m-1}{2}}(i) = B_{\frac{m-1}{2}}(i)$, for all $i \geq 0$.

4. [34, Theorems 15 and 10][33, Result 7].

5. Like in the proof of item 3, for all $a_0^0 \in \mathbb{F}^*_{q^m}$, there is a bijection between the sets $\mathcal{A}_r^1$ and $\mathcal{A}_r^{a_0^0}$ that preserves ranks. Since $\mathcal{A}_r^0 = \mathcal{B}_r^0$, we deduce the equality $A_r^1 = \frac{A_r(i) - B_r(i)}{q^m - 1}$, for all $i \geq 0$.

6. For all $B \in \mathcal{B}_r^1$, let us apply Lemma 1 with $f = \mathrm{tr}$. Then, $\mathrm{rank}(B|_{\ker \mathrm{tr}}) \neq \mathrm{rank}(B)$ if and only if $\mathrm{rank}(B + \mathrm{tr}^2) = \mathrm{rank}(B) = 2\lfloor \frac{\mathrm{rank}(B + \mathrm{tr}^2)}{2} \rfloor$ [34, Lemma 4], i.e., if and only if $\mathrm{rank}(B + \mathrm{tr}^2)$ is even. So, $D_r(i)$ counts those $B \in \mathcal{B}_r^1$ of rank i such that the rank of $B + \mathrm{tr}^2 \in \mathcal{A}_r^1$ is also i and even.

□

Proposition 3. *Consider a vector-space isomorphism $\mathbb{F}_{q^m} \cong (\mathbb{F}_q)^m$, and let $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be a quadratic form. Then:*

1. *The set of quadratic forms polarising to B_Q is $\mathcal{Q} = \{Q_{(a)}(x) = Q(x) + \mathrm{tr}(ax^2) \mid a \in \mathbb{F}_{q^m}\}$.*

2. *If the rank of B_Q is $2s$ then in the set $\mathcal{Q}$ there are:*

   (a) $H(2s) = \frac{q^{2s} + q^s}{2}$ quadratic forms of hyperbolic type;

   (b) $E(2s) = \frac{q^{2s} - q^s}{2}$ quadratic forms of elliptic type;

   (c) $P(2s) = q^m - q^{2s}$ quadratic forms of parabolic type;

Proof. 1. For all $a \in \mathbb{F}_{q^m}$, the map $\mathrm{tr}(ax^2)$ is a quadratic form with associated zero bilinear form, and so $Q_{(a)}$ polarises to B_Q. Conversely, if $B_{Q'} = B_Q$, then $B_{Q'+Q}$ is zero, and so the form $L(y) = (Q + Q')(\sqrt{y})$ is $\mathbb{F}_q-$linear. Now, [21, Theorem 2.24] gives us the existence of $a \in \mathbb{F}_{q^m}$ such that $L(y) = \mathrm{tr}(ay)$, i.e., $(Q + Q')(x) = \mathrm{tr}(ax^2)$, for all $x \in \mathbb{F}_{q^m}$.

2. Consider a simplectic basis $\mathcal{E} = \{e_1, \dots, e_m\}$ for the metric space $(\mathbb{F}_{q^m}, B_Q)$, i.e., $B_Q(e_{2i-1}, e_{2i}) = 1$ for all $1 \leq i \leq s$, and $B_Q(e_i, e_j) = 0$ otherwise. With respect to such a basis $\mathrm{rad}(B_Q) =< e_{2s+1}, \dots, e_m >$, the coordinate expressions of the quadratic forms $\mathrm{tr}(ax^2)$ is $\sum_{i=1}^m a_i x_i^2$ ($x_1, \dots, x_m$ are the coordinates of x in the basis $\mathcal{E}$, and $a_1, \dots, a_m \in \mathbb{F}_q$). So, w.l.o.g. we can assume that Q is of hyperbolic type H_{2s}, since addition of a term of the form $\sum_{i=1}^m a_i x_i^2$ does not change the set $\mathcal{Q}$.

   Therefore, starting with H_{2s}, let us add a term $\sum_{i=1}^m a_i x_i^2$. If at least one of the $a_{2s+1}, \dots, a_m$ is not zero, then $Q_{(a)}(\mathrm{rad}(Q_{(a)})) \neq 0$ and the corresponding quadratic form is equivalent to P_{2s} [25, 7.2.9 Theorem 4]. Therefore, there are $q^m - q^{2s}$ forms of parabolic type in $\mathcal{Q}$.

   If $a_{2s+1} = \dots = a_m = 0$, the type of the form $Q_{(a)}$ depends on its Arf invariant $\Delta(Q_{(a)}) = \sum_{i=1}^s a_{2i-1}a_{2i}$, and so in the parity of summands $a_{2i-1}a_{2i}$ with absolute trace equal to one. If $a_{2i-1} = 0$ or $a_{2i} = 0$, then $\mathrm{Abstr}(a_{2i-1}a_{2i}) = 0$ ($2q - 1$ cases), where as if $a_{2i-1} \neq 0$, then $\{a_{2i-1}a_{2i} \mid a_{2i} \neq 0\} = \mathbb{F}_q^*$, and so $\#\{\mathrm{Abstr}(a_{2i-1}a_{2i}) = 0 \mid a_{2i} \neq 0\} = \frac{q-2}{2}$. Therefore, the number of summands $a_{2i-1}a_{2i}$ with zero (resp. one) absolute trace is $(2q-1)+\frac{q-2}{2}(q-1)=\frac{q^2+q}{2}$ (resp. $q^2-\frac{q-2}{2}=\frac{q^2-q}{2}$) pairs. This proves, as a particular case, the lemma in the case $s=1$. The rest of the cases are proved by induction on s. For $s>1$, $\Delta(Q_{(a)})=0$ if and only if $\mathrm{Abstr}(\sum_{i=1}^{s-1}(a_{2i-1}a_{2i}))=\mathrm{Abstr}(a_{2s-1}a_{2s})$. Using the induction hypothesis this gives a total amount of

$$\frac{q^{2(s-1)}+q^{s-1}}{2}\cdot\frac{q^2+q}{2}+\frac{q^{2(s-1)}-q^{s-1}}{2}\cdot\frac{q^2-q}{2}=\frac{q^{2s}+q^s}{2}$$

hyperbolic forms. The rest of the forms, i.e., $q^m-(q^m-q^{2s})-\frac{q^{2s}+q^s}{2}=\frac{q^{2s}-q^s}{2}$, must be elliptic. □

2.2 Galois rings

In this subsection we include definitions and basic facts on Galois rings (see [28, 24, 1] for details) and the related $R-$valued quadratic forms [22].

Let $R=GR(q^2,2^2)$ be the *Galois Ring of* q^2 *elements (*$q=2^l$*) and characteristic* 2^2. It is an associative commutative local ring with identity $e=1$, maximal ideal $2R$ and quotient field $\overline{R}=R/2R=\mathbb{F}_q$. This ring is uniquely determined by its cardinality and characteristic and it can be constructed as the quotient ring $\mathbb{Z}_4[x]/\left\langle p(x)\right\rangle$, where $p(x)\in\mathbb{Z}_4[x]$ is a *Galois polynomial*, i.e. any monic polynomial of degree l such that $\overline{p}(x)\in\mathbb{Z}_4[x]/2\mathbb{Z}_4[x]\cong\mathbb{Z}_2[x]$ is irreducible. The set of units of R is the multiplicative abelian group $R^*=R\setminus 2R$ and the lattice of ideals of R is the strictly decreasing chain $R\rhd 2R\rhd 0$.

The subset $\Gamma(R)=\{b\in R\mid b^q=b\}$ is called the *Teichmüller coordinate set (TCS)* of R. It is a set of q elements closed under the product and such that any element $b\in R$ can be written uniquely in the form $b=b_0+2b_1$, where $b_i=\gamma_i(b)\in\Gamma(R)$, $i=0,1$. This set is not closed under the addition, though. If we consider the map $\oslash:\Gamma(R)\times\Gamma(R)\to\Gamma(R)$ given by $a\oslash b=\gamma_0(a+b)$, then $(\Gamma(R),\oslash,\cdot)$ is the finite field $\mathbb{F}_q$. Moreover, for any $a,b\in\Gamma(R)$ the following equality holds: $\gamma_1(a+b)=\sqrt{ab}$.

For all $m\in\mathbb{N}$, R is a subring of the Galois ring $S=GR(q^{2m},2^2)$. The group of automorphisms of S fixing R elementwise is cyclic of order l, and it is generated by $\sigma(b)=b_0^q+2b_1^q$, for all $b\in S$. The *trace* of the ring extension $S|R$ is the $R-$linear function $\mathrm{Tr}_R^S(b)=\sum_{i=0}^{m-1}\sigma(b)^i$ (or simply written Tr). It can be checked [29] that

$$\mathrm{Tr}_R^S(b)=\mathrm{tr}_q^{q^m}(b_0)+2\left(\mathrm{tr}_q^{q^m}(b_1)\oslash\varkappa\left(\sqrt{b_0}\right)\right)\tag{2}$$

where $\varkappa(x)=\sum_{0\leq i<j\leq m-1}x^{q^i+q^j}$ is a quadratic form on $\Gamma(S)\cong\mathbb{F}_{q^m}\cong\mathbb{F}_q^m\cong\Gamma(R)^m$ polarising to

$$B_{\varkappa}(x,y)=\mathrm{tr}_q^{q^m}(xy)\oslash\mathrm{tr}_q^{q^m}(x)\mathrm{tr}_q^{q^m}(y)\tag{3}$$

The map $Q:\Gamma(R)^m\to R$ is an *R-valued quadratic form* provided that:

- $Q(\lambda a)=\lambda^2Q(a)$, $\forall\lambda\in R,\forall a\in\Gamma(R)^m$;
- The map $(\cdot,\cdot)_Q:\Gamma(R)^m\times\Gamma(R)^m\to R$ given by $(a,b)_Q=Q(a\oslash b)-Q(a)-Q(b)$, for all $a,b\in\Gamma(R)^m$, is a bilinear form.

2.3 Codes over Galois rings

The general setting of codes over modules can be found in [17]. A linear code over the Galois ring $R=GR(q^2,2^2)$ of length N is a submodule $\mathcal{K}$ of R^N. The *homogeneous weight* (or *Lee weight* in the case $q = 2$ [1]) of a word $\bar{b} = (b^1, \dots, b^N)$ is defined as $w(\bar{b}) = \sum_{i=1}^{N} w_H(b^i)$, where $w_H(b^i) = 0, q, q-1$ if $b^i \in 0R, 2R^*, R^*$, respectively.

Let $\Gamma(R) = \{g_0 = 0, g_1 = 1, \dots, g_{q-1}\}$, and consider $\gamma_* : R \to \Gamma(R)^q$ given by

$$\gamma_*(b_0 + 2b_1) = (b_1, b_1 \oslash b_0, \dots, b_1 \oslash g_{q-1}b_0)$$

for any $b \in R$ ($b_0, b_1 \in \Gamma(R)$). Then $\gamma_*(R)$ is a $[q, 2, q-1]$-Reed-Solomon code over $\Gamma(R) = \mathbb{F}_q$ and so the map γ_* is called the *RS-map* (or *Gray map in the case $q = 2$)*. Moreover, the induced map $\gamma_*^N : R^N \to \Gamma(R)^{Nq}$ is an isometry (taking the usual Hamming weight on the space $\Gamma(R)^{Nq} \cong \mathbb{F}_q^{Nq}$).

Given any word $\bar{b} = (b^1, \dots, b^N)$, let $\nu_0(\bar{b}), \nu_2(\bar{b}), \nu_1(\bar{b})$ be the number of coordinates of $\bar{b}$ in $0R, 2R^*, R^*$, respectively. The *ideal weight enumerator* of a code $\mathcal{K}$ is $W_{\mathcal{K}}(y_0, y_1, y_2) = \sum_{\bar{b} \in \mathcal{K}} y_0^{\nu_0(\bar{b})} y_2^{\nu_2(\bar{b})} y_1^{\nu_1(\bar{b})}$, and it can be used to obtain the homogeneous (Hamming) weight enumerator of the code $\gamma_*^N(\mathcal{K})$ (and so eventually the minimum Hamming distance of such code). Namely, $W^H_{\gamma_*^N(\mathcal{K})}(X, Y) = W_{\mathcal{K}}(Y^q, X^q, YX^{q-1})$.

3 Generalized Delsarte-Goethals codes

In this section we introduce the Generalized Delsarte-Goethals codes, study their combinatorial properties and notice the relation to the original paper of Delsarte-Goethals. Classical (i.e., binary) Delsarte-Goethals codes were introduced with the help of alternating bilinear forms over the finite field $\mathbb{F}_2$ [7, Theorem 9], and as such they are described in [23, Chapter 15]. However, these codes can also be seen as the Gray image of linear quaternary codes, i.e., of linear codes over the alphabet $\mathbb{Z}/4\mathbb{Z}$. This is the way they are described in [9, Section VI] that we recall next.

Let $m \geq 3$, $0 \leq r \leq \frac{m}{2}$. Consider the trace function $\mathrm{Tr} : S \to R$ from $S = GR(2^{2m}, 2^2)$ onto $R = GR(2^2, 2^2) = \mathbb{Z}/4\mathbb{Z}$. Under the identification $\Gamma(S) \cong \mathbb{F}_{2^m}$, the quaternary linear code $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ is defined as:

$$\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r) = \left\{ \left(\mathrm{Tr}\left(a_0 x + 2 \sum_{i=1}^{r} a_i x^{2^i+1} \right) + b \right)_{x \in \mathbb{F}_{2^m}} \mid a_0 \in S, a_1, \dots, a_r \in \mathbb{F}_{2^m}, b \in \mathbb{Z}/4\mathbb{Z} \right\} \quad (4)$$

For m odd it is a code of length $N = 2^m$ over $\mathbb{Z}/4\mathbb{Z}$, cardinality $2^{m(r+2)+2}$ and minimum Lee weight $2^m - 2^{m-\delta}$, where $\delta = \frac{m+1}{2} - r$. Moreover, it is a $\mathbb{Z}/4\mathbb{Z}$-module of type $4^{m+1}2^{rm}$, i.e., it is isomorphic as a $\mathbb{Z}/4\mathbb{Z}-$module to $(\mathbb{Z}/4\mathbb{Z})^{m+1} \times (\mathbb{Z}/2\mathbb{Z})^{rm}$ [9, Section II]. The (binary) *Delsarte-Goethals code* $\mathcal{DG}_2(m+1, \delta)$ is the concatenation of the code $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ and the Reed-Solomon code $\gamma_*(\mathbb{Z}/4\mathbb{Z})$, i.e., $\mathcal{DG}_2(m+1, \delta) = \gamma_*^N(\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r))$. It is a distance-invariant code of length 2^{m+1}, cardinality $2^{m(r+2)+2}$, and minimum Hamming distance $2^m - 2^{\frac{m-1}{2}+r}$.

The quaternary version of the binary Delsarte-Goethals codes connects them to low-correlation sequences [2, 15]. Namely, selected codewords of $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ punctured in the $x = 0$ position provide the family $S(r)$, appearing one of its members ($S(2)$, with $m = 8$) in the W-CDMA component of the IMT-2000 standard for 3G mobile communication [16] (see also [33, Section V]).

This construction can be also regarded from the point of view of $\mathbb{Z}/4\mathbb{Z}-$valued quadratic forms (see [33, Section IV], where $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ is considered in the context of quaternary sequence families). Namely, the quaternary linear code is related to the set of valuations of the $\mathbb{Z}/4\mathbb{Z}-$valued quadratic forms Q_a (with $a = (a_0, a_1, \dots, a_r) \in S \times \Gamma(S)^r$):

$$Q_a : \Gamma(S)(\cong \mathbb{Z}/2\mathbb{Z}^m) \to \mathbb{Z}/4\mathbb{Z} \text{ given by } Q_a(x) = \mathrm{Tr}\left(a_0 x + 2 \sum_{i=1}^{r} a_i x^{2^i+1} \right) \quad (5)$$

We will take into account this approach to introduce a general construction of Delsarte-Goethals codes in arbitrary Galois fields of characteristic 2.

Let $R = GR(q^2, 2^2)$ be the Galois Ring of q^2 elements ($q = 2^l, l \geq 1$) and characteristic 2^2, and let $S = GR(q^{2m}, 2^2)$ be its Galois extension of degree m. We want to define an $R-$linear code in the form of (4) for which the corresponding maps in the form of (5) are $R-$valued quadratic forms. This idea was already considered in [8, Section 4] when constructing nonequivalent Generalized Kerdock codes from symplectic semifield spreads. In particular, the $R-$valued quadratic forms

$$T_s : \Gamma(S)(\cong \Gamma(R)^m) \to R \text{ given by } T_s(x) = \mathrm{Tr}\left(sx^2\right)$$

with $s \in \Gamma(S)$ where used. Therefore, it seems natural to define the Generalized Delsarte-Goethals codes in the following way.

Definition 1. Let $m \geq 3$ odd, $0 \leq r \leq \frac{m-1}{2}$, and $\delta = \frac{m+1}{2} - r$. Consider the trace function $\mathrm{Tr} : S \to R$ from $S = GR(q^{2m}, 2^2)$ onto $R = GR(q^2, 2^2)$ (where $q = 2^l, l \geq 1$), and define the $R-$code:

$$\mathcal{DG}_R(m, r) = \left\{ \left(\mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^{r} a_i x^{q^i+1} \right) + b \right)_{x \in \Gamma(S)} \mid a_0 \in S, a_1, \ldots, a_r \in \Gamma(S), b \in R \right\} \qquad (6)$$

The *Generalized Delsarte-Goethals code* $\mathcal{DG}_q(m+1, \delta)$ is the concatenation of the code $\mathcal{DG}_R(m, r)$ and the Reed-Solomon code $\gamma_*(R)$, i.e., $\mathcal{DG}_q(m+1, \delta) = \gamma_*^{q^m}(\mathcal{DG}_R(m, r))$.

Proposition 4. *With the notation of the previous definition:*

1. *$\mathcal{DG}_R(m, r)$ is an $R-$linear code of length $N = q^m$ and cardinality $q^{m(r+2)+2}$. Moreover, as an $R-$module it is isomorphic to $R^{m+1} \times (\mathbb{F}_q)^{rm}$.*

2. *The Generalized Delsarte-Goethals code $\mathcal{DG}_q(m+1, \delta)$ is an $\mathbb{F}_q-$(non-linear)distance-invariant code of length q^{m+1} and cardinality $q^{m(r+2)+2}$.*

Proof. 1. It is clear that $\mathcal{DG}_R(m, r)$ is an $R-$module because of the linearity of the trace function, and so it is an $R-$linear code of length $|\Gamma(S)| = q^m$. If we show that the zero codeword is only obtained when $a_0 = a_1 = \ldots = a_r = b = 0$, then we can conclude that $\mathcal{DG}_R(m, r)$ is an $R-$module isomorphic to $S \times (\Gamma(S))^r \times R \cong R^{m+1} \times (\mathbb{F}_q)^{rm}$ of cardinality $q^{m(r+2)+2}$. But this is easy, as $\mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^r a_i x^{q^i+1}\right) + b = 0$ for all $x \in \Gamma(S)$, makes $\mathrm{tr}(a_0^0x^2) = b_0$, and $\mathrm{tr}(a_0^1x^2 + \sum_{i=1}^r a_i x^{q^i+1}) + \varkappa\left(\sqrt{a_0^0x}\right) = b_1$, for all $x \in \mathbb{F}_{q^m}$ (where $a_0 = a_0^0 + 2a_0^1$ and $b = b_0 + 2b_1$ are the $2-$adic decompositions of the elements a_0 and b). From the first equality we deduce $a_0^0 = b_0 = 0$ (observe that $\mathrm{tr}(a_0^0x^2) = (\mathrm{tr}(\sqrt{a_0^0x}))^2$ and use [21, Theorem 2.24]). If we substitute $a_0^0 = 0$ into the second equality we get $\mathrm{tr}(xL_a(x)) = b_1$, for all $x \in \mathbb{F}_{q^m}$, where $L_a(x) = a_0^1x + \sum_{i=1}^r a_i x^{q^i}$. Clearly this forces $b_1 = 0$ (take $x = 0$) and $a_0^1 = a_1 = \ldots = a_r = 0$, because $\mathrm{tr}(xL_a(x))$ is a trace form equal to zero with $\deg L_a \leq \frac{m-1}{2}$ [25, 7.2.20 Remark].

2. Apply [19, Theorem 2].

□

Observe that, as particular cases, we recover both the classical Delsarte-Goethals codes and the Generalized Kerdock codes.

Remark 1. 1. If $l = 1$, i.e., $q = 2$, then $\mathcal{DG}_R(m, r)$ is equivalent to the code $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ of equation (4), and so the Generalized Delsarte-Goethals code $\mathcal{DG}_q(m + 1, \delta)$ is equivalent to the original binary Delsarte-Goethals code $\mathcal{DG}_2(m + 1, \delta)$. Namely, the map $\varphi : \Gamma(S)^{q^m} \to \Gamma(S)^{q^m}$, given by $\varphi((c_x)_{x\in\Gamma(S)}) = ((c_{x^2})_{x\in\Gamma(S)})$ induces a permutation equivalence between $\mathcal{DG}_{\mathbb{Z}/4\mathbb{Z}}(m, r)$ and $\mathcal{DG}_R(m, r)$ because

$$\mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^{r} a_i(x^2)^{2^i+1}\right) + b = \mathrm{Tr}(a_0x^2) + 2\mathrm{Tr}\left(\sum_{i=1}^{r} a_i(x^{2^i+1})^2\right) + b$$

$$= \mathrm{Tr}(a_0x^2) + 2\mathrm{tr}\left(\left(\bigoplus_{i=1}^{r} \sqrt{a_i}x^{2^i+1}\right)^2\right) + b = \mathrm{Tr}(a_0x^2) + 2\left(\mathrm{tr}\left(\bigoplus_{i=1}^{r} \sqrt{a_i}x^{2^i+1}\right)\right)^2 + b$$

$$= \mathrm{Tr}(a_0x^2) + 2\mathrm{tr}\left(\bigoplus_{i=1}^{r} \sqrt{a_i}x^{2^i+1}\right) + b = \mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^{r} \sqrt{a_i}x^{2^i+1}\right) + b$$

2. If $r = 0$, then [8, Proposition 1] shows that $\mathcal{DG}_R(m, 0)$ is equivalent to the base linear code $\mathcal{K}_R(m)$, and so the Generalized Delsarte-Goethals code $\mathcal{DG}_q(m + 1, \frac{m+1}{2})$ is equivalent to the Generalized Kerdock $\mathcal{K}_q(m + 1)$ code [29].

3. The code $\mathcal{DG}_R(m, r)$ is the set of translates of valuations of the $R-$valued quadratic forms Q_a (with $a = (a_0, a_1, \ldots, a_r) \in S \times \Gamma(S)^r$):

$$Q_a : \Gamma(S)(\cong \Gamma(R)^m) \to R \text{ given by } Q_a(x) = \mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^{r} a_ix^{q^i+1}\right)$$

Namely, if $\lambda \in R, x \in \Gamma(S)$, then

$$Q_a(\lambda x) = \mathrm{Tr}\left(a_0(\lambda x)^2 + 2\sum_{i=1}^{r} a_i(\lambda x)^{q^i+1}\right) = \mathrm{Tr}\left(a_0\lambda^2x^2 + 2\sum_{i=1}^{r} a_i\lambda^{q^i+1}x^{2^i+1}\right)$$

$$= \mathrm{Tr}\left(\lambda^2\left(a_0x^2 + 2\sum_{i=1}^{r} a_ix^{2^i+1}\right)\right) = \lambda^2Q_a(x)$$

because $\lambda^{q^i} \equiv \lambda \bmod 2R$. And also, for all $x, y \in \Gamma(S)$,

$$(x, y)_{Q_a} = Q_a(x \oslash y) - Q_a(x) - Q_a(y)$$

$$= \mathrm{Tr}\left(a_0(x \oslash y)^2 + 2\sum_{i=1}^{r} a_i(x \oslash y)^{q^i+1}\right) - \mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^{r} a_ix^{q^i+1}\right) - \mathrm{Tr}\left(a_0y^2 + 2\sum_{i=1}^{r} a_iy^{q^i+1}\right)$$

$$= \mathrm{Tr}\left(a_0(2xy) + 2\sum_{i=1}^{r} a_i(x^{q^i}y \oslash xy^{q^i})\right) = 2\mathrm{Tr}\left(a_0xy + \sum_{i=1}^{r} a_i(x^{q^i}y \oslash xy^{q^i})\right)$$

because $(x \oslash y)^2 = (x^2 \oslash y^2) = x^2 + y^2 + 2xy$, and $(x \oslash y)^{q^i+1} = (x^{q^i} \oslash y^{q^i})(x \oslash y) = x^{q^i+1} \oslash y^{q^i+1} \oslash (x^{q^i}y \oslash xy^{q^i})$. So, the corresponding bilinear form is $B_{Q_a}(x, y) = \mathrm{tr}\left(a_0xy + \sum_{i=1}^{r} a_i(x^{q^i}y \oslash xy^{q^i})\right)$ (cf. [33, page 5806]).

The main result of this paper is the computation of the ideal weight enumerator of the $R-$linear code $\mathcal{DG}_R(m,r)$. As a consequence we obtain the minimum distance of the Generalized Delsarte-Goethals codes.

Theorem 1. *The ideal weight enumerator of the code $\mathcal{DG}_R(m,r)$ is described with the data contained in Table 1.*

#case	Pair $(\nu_0(a,b), \nu_2(a,b))$ related to the term $y_0^{\nu_0(a,b)} \cdot y_2^{\nu_2(a,b)} \cdot y_1^{q^m-\nu_0(a,b)-\nu_2(a,b)}$	#codewords (coefficient)
1	$(\ 0\ ,\ 0\ )$	$q^{m(r+1)+1}(q-1)$
2	$(\ q^{m-1}\ ,\ q^m - q^{m-1})$	$B_r(m-2k-1)(q^m - q^{2s}\ )q$
3	$(\ q^{m-1} \pm (q-1)q^{m-s-1}\ ,\ q^m - q^{m-1} \mp (q-1)q^{m-s-1}\ )$	$B_r(m-2k-1)\,\frac{q^{2s} \pm q^s}{2}$
4	$(\ q^{m-1} \mp q^{m-s-1}\ ,\ q^m - q^{m-1} \pm q^{m-s-1})\ )$	$B_r(m-2k-1)\,\frac{q^{2s} \pm q^s}{2}(q-1)$
5	$(\ q^{m-2} \pm (q-1)q^{m-s-2}\ ,\ q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-2}\ )$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\,\frac{q^{2s} \pm q^s}{2}(q^m-1)q$
6	$(\ q^{m-2} \mp q^{m-s-2}\ ,\ q^{m-1} - q^{m-2} \pm q^{m-s-2}\ )$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\,\frac{q^{2s} \pm q^s}{2}(q^m-1)(q-1)q$
7	$(\ q^{m-2} \pm (q-1)q^{m-s-2}\ ,\ q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-2})$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\,\frac{q^{2s} \pm q^s}{2}(q^m-1)(q-1)q$
8	$(\ q^{m-2} \mp q^{m-s-2}\ ,\ q^{m-1} - q^{m-2} \pm q^{m-s-2})$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\,\frac{q^{2s} \pm q^s}{2}(q^m-1)(q-1)^2q$
9	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$(B_r^1(m-2k-1) - D_r(m-2k-1))(q^m - q^{2s+1})(q^m-1)q^2$
10	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)(q^m - q^{2s})(q^m-1)q^2$
11	$(\ q^{m-2} \pm (q-1)q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-1}\ )$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)$
12	$(\ q^{m-2} \mp q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \pm q^{m-s-1})$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)$
13	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)q$
14	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)q$
15	$(\ q^{m-2} \pm q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \mp q^{m-s-1})$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)^2\,\frac{q}{2}$
16	$(\ q^{m-2} \pm (q-1)q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-1}\ )$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)$
17	$(\ q^{m-2} \mp q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \pm q^{m-s-1})$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)^2$
18	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)^2q$
19	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)q\,\frac{q-2}{2}$
20	$(\ q^{m-2} \pm q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \mp q^{m-s-1})$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)^2\,\frac{q}{2}\,\frac{q-2}{2}$
21	$(\ q^{m-2}\ ,\ q^{m-1} - q^{m-2}\ )$	$D_r(m-2k-1)q^{2(s-1)}(q^m-1)(q-1)q\,\frac{q}{2}$
22	$(\ q^{m-2} \mp q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \pm q^{m-s-1})$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)\,\frac{(q-1)q}{2}\,\frac{q}{2}$
23	$(\ q^{m-2} \pm q^{m-s-1}\ ,\ q^{m-1} - q^{m-2} \mp q^{m-s-1})$	$D_r(m-2k-1)\,\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)\,\frac{(q-1)q}{2}\,\frac{q}{2}$

Table 1: $0 \le k \le \frac{m-1}{2}$ and $s = \frac{m-2k-1}{2}$ (numbers B_r, B_r^1 and D_r are defined in Proposition 2)

Proof. We need to compute, for all $a_0 \in S, a_1, \ldots, a_r \in \Gamma(S), b \in R$, the number of $x \in \Gamma(S)$ such that $c(a,b) := \mathrm{Tr}\left(a_0x^2 + 2\sum_{i=1}^r a_i x^{q^i+1}\right) + b = 0$ and such that $c(a,b) \in 2R^*$. If

$$\nu_0(a,b) := \#\{x \in \Gamma(S) \mid c(a,b) = 0\}\ ,\ \nu_2(a,b) := \#\{x \in \Gamma(S) \mid c(a,b) \in 2R^*\}$$

then the corresponding codeword contributes with a term $y_0^{\nu_0(a,b)} \cdot y_2^{\nu_2(a,b)} \cdot y_1^{q^m-\nu_0(a,b)-\nu_2(a,b)}$ to the ideal weight enumerator of the code. We can use the $2-$adic decomposition of $c(a,b)$ to express $\nu_0(a,b), \nu_2(a,b)$ in terms of two equations over the finite field $\mathbb{F}_{q^m}$. Namely:

$$\mathrm{tr}(a_0^0x^2) = b_0 \tag{7}$$

$$\varkappa\left(\sqrt{a_0^0}x\right) + \mathrm{tr}\left(a_0^1x^2 + \sum_{i=1}^{r} a_i x^{q^i+1}\right) + \sqrt{b_0}\mathrm{tr}(\sqrt{a_0^0}x) = b_1 \tag{8}$$

where $a_0 = a_0^0 + 2a_0^1$ and $b = b_0 + 2b_1$ are the 2−adic decompositions of the elements a_0 and b. So, $\nu_0(a,b) := \#\{x \in \mathbb{F}_{q^m} \mid (7)(8) \text{ are true}\}$, $\nu_2(a,b) := \#\{x \in \Gamma(S) \mid (7) \text{ is true but } (8) \text{ is not}\}$

1. First, let $a_0^0 = 0$. It is clear that equation (7) is true if and only if $b_0 = 0$. If $b_0 \neq 0$ ($q-1$ choices), then, for all $a_0^1, a_1, \dots, a_r \in \Gamma(S), b_1 \in \Gamma(R)$ ($(q^m)^{r+1} \cdot q$ choices), we have $\nu_0(a,b) = \nu_2(a,b) = 0$, and the first row of the table is obtained. If $b_0 = 0$, then the equation (7) holds and we need to count the solutions to the equation $\mathrm{tr}\left(a_0^1x^2 + \sum_{i=1}^r a_i x^{q^i+1}\right) = b_1$ (as $\nu_2(a,b) = q^m - \nu_0(a,b)$ in this case). Observe that because of Proposition 3, for fixed $a_1, \dots, a_r \in \Gamma(S)$, the left hand side of the equation corresponds to evaluations of the set of quadratic forms polarising to $B_{\mathrm{tr}\left(\sum_{i=1}^r a_i x^{q^i+1}\right)}$. If the rank of this bilinear form is $m - 2k - 1$ (with $0 \leq k \leq \frac{m-1}{2}$), then Proposition 3 gives us the number of quadratic forms of hyperbolic, elliptic and parabolic type in the set. For each of them, Proposition 1 provides the number of solutions to equation (8). So, using Proposition 2 we deduce that there are $B_r(m-2k-1)$ bilinear forms $\mathrm{tr}\left(\sum_{i=1}^r a_i(x^{q^i}y + xy^{q^i})\right)$ of rank $m-2k-1$ (recall equation (1)), associated to $H(m-2k-1), E(m-2k-1), P(m-2k-1)$ quadratic forms of hyperbolic, elliptic or parabolic type, for which the number of solutions to equation (8) depends on whether $b_1 = 0$ or $b_1 \neq 0$ ($q-1$ choices) in the elliptic and hyperbolic cases. This gives us rows #2 (parabolic), #3 (hyperbolic/elliptic $b_1 = 0$) and #4 (hyperbolic/elliptic, $b_1 \neq 0$) in the table.

2. Let us now consider the case $a_0^0 \neq 0$. The change of variable $y = \sqrt{a_0^0}x$, transforms equation (7) into a linear one ($\mathrm{tr}(y) = \sqrt{b_0}$), and equation (8) into

$$\varkappa(y) + \mathrm{tr}\left(c_0y^2 + \sum_{i=1}^{r} c_i y^{q^i+1}\right) + \sqrt{b_0}\mathrm{tr}(y) = b_1$$

with $c_0 = a_0^1(a_0^0)^{-1}$ and $c_i = a_i(\sqrt{(a_0^0)^{-1}})^{q^i+1}$, for all $i = 1, \dots, r$. If we count the number of solutions $\nu_0(a,b)$ to the system of equations (7)(8), then $\nu_2(a,b) = q^{m-1} - \nu_0(a,b)$ (because the number of solutions to equation (7) is always q^{m-1}). If (7) is true, then (8) becomes

$$\varkappa(y) + \mathrm{tr}\left(c_0y^2 + \sum_{i=1}^{r} c_i y^{q^i+1}\right) = \tilde{b}_1$$

with $\tilde{b}_1 = b_1 + b_0$. Again, because of Proposition 3, for fixed $c_1, \dots, c_r \in \Gamma(S)$, as c_0 varies, the left hand side of the latter equation corresponds to evaluations of the set $\mathcal{Q}$ of quadratic forms polarising to $B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}$. Since equations (1) and (3), the ranks of such bilinear forms (for all $c_1, \dots, c_r \in \Gamma(S)$) is given by Proposition 2. Namely, for all values of i, there are $D_r(i)$ bilinear forms $B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}$ of rank i such that $\mathrm{rad}\left(B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}\right) \subseteq \ker \mathrm{tr}$ (see Lemma 1), and there are $B_r^1(i) - D_r(i)$ bilinear forms $B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}$ of rank i such that $\mathrm{rad}\left(B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}\right) \not\subseteq \ker \mathrm{tr}$. Let us now simultaneously compute the number of solutions to (7) and (8) for all Q in $\mathcal{Q}$.

   (a) We begin with the case of those bilinear forms $B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}$ of rank $0 \leq 2s < m$ such that $\mathrm{rad}\left(B_{\mathrm{tr}\left(\sum_{i=1}^r c_i y^{q^i+1}\right)+\varkappa(y)}\right) \not\subseteq \ker \mathrm{tr}$. We consider the symplectic basis $\mathcal{E}$ of

Lemma 1 (taking $B = B_{\mathrm{tr}(\sum_{i=1}^{r} c_i y^{q^i+1})+\varkappa(y)}$ and $f = \mathrm{tr}$). In coordinates with respect to such a basis, the quadratic forms in $\mathcal{Q}$ have the form $\sum_{i=1}^{s} y_{2i-1}y_{2i} + \sum_{i=1}^{m} h_i y_i^2$, where $h_i \in \mathbb{F}_q$ and $y = \sum_{i=1}^{m} y_i e_i$. So, the system of equations (7)(8) becomes $y_m = \sqrt{b_0}$ (7) and $\sum_{i=1}^{s} y_{2i-1}y_{2i} + \sum_{i=1}^{m} h_i y_i^2 = \tilde{b}_1$ (8).

i. If $(h_{2s+1}, \dots, h_m) = (0, \dots, 0)$ then, up to a change of the first $2s$ coordinates, we are in the case 2.(a) of Proposition 1. So, $\nu_0(a, b) = q^{m-2} \pm \nu(\tilde{b}_1)q^{m-s-2}$. We have $(q-1)$ choices for a_0^0, $B_r^1(m-2k-1) - D_r(m-2k-1)$ choices for the a_i, $\frac{q^{2s}+q^s}{2}$ or $\frac{q^{2s}-q^s}{2}$ for the h_i, and q or $q(q-1)$ for b. Rows #5 (hyperbolic/elliptic, $\tilde{b}_1 = 0$) and #6 (hyperbolic/elliptic, $\tilde{b}_1 \neq 0$) collect this information.

ii. On the other hand, when $h_m \neq 0$ and $(h_{2s+1}, \dots, h_{m-1}) = (0, \dots, 0)$, we can change $2s+1$ coordinates (the first $2s$ and the last one) and apply case 2.(g) of Proposition 1. Namely, we can first change the first $2s$ coordinates to get the quadratic form $H_{2s} + h_m y_m^2$ or $E_{2s} + h_m y_m^2$, while preserving the linear one.
In the first case, a second change $\sqrt{h_m} y_m = Y_{2s+1}, y_{2s+1} = Y_m$ (other coordinates remain $y_i = Y_i$) gives us P_{2s} and the linear form $\frac{Y_{2s+1}}{\sqrt{h_m}}$. Therefore, we have $\nu_0(a, b) = q^{m-2} + \nu(\tilde{b}_1 + b_0 h_m)q^{m-s-2}$. There are $(q^m - 1)$ choices for a_0^0, $B_r^1(m-2k-1) - D_r(m-2k-1)$ choices for the a_i, $\frac{q^{2s}+q^s}{2} \cdot (q-1)$ for the h_i, and q or $q(q-1)$ for b, which gives us the upper part of rows #7 ($\tilde{b}_1 + b_0 h_m = 0$) and #8 ($\tilde{b}_1 + b_0 h_m \neq 0$).
In the second case, a further change of coordinates ($y_{2s-1} + y_{2s} = Y_{2s}, \sqrt{\beta} y_{2s} + \sqrt{h_m} y_m = Y_{2s+1}, y_{2s+1} = Y_m$) gives us P_{2s} and the linear form $\frac{\sqrt{\beta}}{\sqrt{h_m}} Y_{2s-1} + \frac{\sqrt{\beta}}{\sqrt{h_m}} Y_{2s} + \frac{1}{\sqrt{h_m}} Y_{2s+1}$, with $\mathrm{Abstr}(\beta) = 1$. Therefore (with the notation of 2.(g) in Proposition 1), $(Q(a_1, \dots, a_m) - a_{2s+1}^2)/a_{2s+1}^2 = \beta$, and so $\nu_0(a, b) = q^{m-2} - \nu(\tilde{b}_1 + b_0 h_m)q^{m-s-2}$. There are $(q^m - 1)$ choices for a_0^0, $B_r^1(m-2k-1) - D_r(m-2k-1)$ choices for the a_i, $\frac{q^{2s}-q^s}{2} \cdot (q-1)$ for the h_i, and q or $q(q-1)$ for b, which gives us the lower part of rows #7 ($\tilde{b}_1 + b_0 h_m = 0$) and #8 ($\tilde{b}_1 + b_0 h_m \neq 0$).

iii. Finally, in the rest of cases, because there exists $h_t \neq 0$ with $2s+1 \leq t < m$, we can change $\sum_{i=2s+1}^{m-1} \sqrt{h_i} y_i = Y_{2s+1}$ together with an independent change of the first $2s$ coordinates to get the quadratic form $H_{2s} + Y_{2s+1}^2 + h_m Y_m^2$ or $E_{2s} + Y_{2s+1}^2 + h_m Y_m^2$, while preserving the linear one. In the first (alt. second) case, a further change $Y_{2s+1} + \sqrt{h_m} Y_m = Z_{2s+1}$ (alt. $Y_{2s-1} + Y_{2s} = Z_{2s-1}, \sqrt{\beta} Y_{2s} + Y_{2s+1} + \sqrt{h_m} Y_m = Z_{2s+1}$) gives us P_{2s} where as the equivalent linear form does not change. Therefore, case 2.(b) of Proposition 1 applies, i.e., $\nu_0(a, b) = q^{m-2}$. There are $(q^m - 1)$ choices for a_0^0, $B_r^1(m-2k-1) - D_r(m-2k-1)$ choices for the a_i, $(q^{m-2s-1} - 1)q^{2s+1} = q^m - q^{2s+1}$ for the h_i, and q^2 for b, which gives us row #9.

(b) Next, we consider the case when $\mathrm{rad}\left(B_{\mathrm{tr}(\sum_{i=1}^{r} c_i y^{q^i+1})+\varkappa(y)}\right)$, of dimension $1 \leq m - 2s \leq m - 2$, is contained in $\ker \mathrm{tr}$. Let $\mathcal{E}$ be again the symplectic basis of Lemma 1 (taking $B = B_{\mathrm{tr}(\sum_{i=1}^{r} c_i y^{q^i+1})+\varkappa(y)}$ and $f = \mathrm{tr}$). In coordinates with respect to such a basis, the system of equations (7)(8) becomes $y_1 = \sqrt{b_0}$ (7) and $\sum_{i=1}^{s} y_{2i-1}y_{2i} + \sum_{i=1}^{m} h_i y_i^2 = \tilde{b}_1$ (8) (where $h_i \in \mathbb{F}_q$ and $y = \sum_{i=1}^{m} y_i e_i$).

i. If $(h_{2s+1}, \dots, h_m) \neq (0, \dots, 0)$, we can change the last $m-2s$ coordinates ($\sum_{i=2s+1}^{m} \sqrt{h_i} y_i = Y_{2s+1}$) and (independently) the first $2s$ to get either the equivalent form $H_{2s} + Y_{2s+1}^2 = P_{2s}$ or the form $E_{2s} + Y_{2s+1}^2$. Clearly, this transformation leaves the equivalent linear form involving only the first $2s$ coordinates (as the original form involved only

y_1 and the change of the first $2s$ coordinates was made independently of the remaining coordinates). In the second case, another change of coordinates ($Y_{2s-1}+Y_{2s}=Z_{2s}, \sqrt{\beta}Y_{2s}+Y_{2s+1}=Z_{2s+1}$ gives us P_{2s} and an equivalent linear form in the first $2s$ coordinates. Therefore, case 2.(f) of Proposition 1 applies and so $\nu_0(a,b)=q^{m-2}$. There are (q^m-1) choices for a_0^0, $D_r(m-2k-1)$ choices for the a_i, $(q^{m-2s}-1)q^{2s}=q^m-q^{2s}$ for the h_i, and q^2 for b, which gives us row #10.

ii. Therefore, in the rest of the proof we assume $(h_{2s+1},\ldots,h_m)=(0,\ldots,0)$.
If, besides, $h_1=0$, then the change of coordinates $y_1+h_2y_2=Y_1$, together with a suitable (independent) change of the coordinates $y_3,\ldots,y_{2s}$ leaves the quadratic form equal to H_{2s} or E_{2s}, and the linear form $Y_1+h_2Y_2$. So, we can apply cases 2.$(c)(d)(e)$ of Proposition 1, depending on whether $\sqrt{b_0}=0, Q(1,h_2,0,\ldots,0)=h_2=0$ or not. So, we have (q^m-1) choices for a_0^0, $D_r(m-2k-1)$ choices for the a_i, $\frac{q^{2(s-1)}+q^{s-1}}{2}$ or $\frac{q^{2(s-1)}-q^{s-1}}{2}$ for $h_3,\ldots,h_{2s}$. When $h_2=0$, we have row #11 ($b=0$), row #12 ($b_0=0\neq\tilde{b}_1$) or row #13 ($b_0\neq 0$). When $h_2\neq 0$ ($q-1$ possibilities), we have row #14 ($b_0=0$) and row #15 ($b_0\neq 0$ and the $\frac{q}{2}$ possible $\tilde{b}_1$ with Abstr $\left(\frac{\tilde{b}_1h_2}{b_0}\right)=0$ or 1).
Something similar happens when $h_1\neq 0$ but $\mathrm{Abstr}(h_1h_2)=0$, i.e., when there exists $g\in\mathbb{F}_q$ such that $h_1h_2=g+g^2$. The change of coordinates $\sqrt{h_1}y_1+\frac{g}{\sqrt{h_1}}y_2=Y_1, \sqrt{h_1}y_1+\frac{g+1}{\sqrt{h_1}}y_2=Y_2$, together with a suitable (independent) change of the coordinates $y_3,\ldots,y_{2s}$ leaves the quadratic form H_{2s} or E_{2s}, and the linear form equal to $\frac{g+1}{\sqrt{h_1}}Y_1+\frac{g}{\sqrt{h_1}}Y_2$. Since $Q\left(\frac{g+1}{\sqrt{h_1}},\frac{g}{\sqrt{h_1}},0,\ldots,0\right)=h_2$ we are in the same situation as above (with the restriction to just $\frac{q-2}{2}$ possibilities when $h_2\neq 0$, because of the condition on the absolute trace of h_1h_2). This gives us rows #16 to #20.

iii. Finally, we deal with the case $h_1\neq 0$ and $\mathrm{Abstr}(h_1h_2)=1$. We can change coordinates $y_3,\ldots,y_{2s}$ to get either $H_{2(s-1)}$ or $E_{2(s-1)}$. In the first case the quadratic form has type E_{2s} because we can apply the change $\sqrt{h_1}y_1=Y_{2s-1}, \frac{y_2}{\sqrt{h_1}}=Y_{2s}, y_{2s-1}=Y_1, y_{2s}=Y_2$, and so the linear form is equivalent to $\frac{Y_{2s-1}}{\sqrt{h_1}}$. In this situation $Q\left(0,\ldots,0,\frac{1}{\sqrt{h_1}},\overset{(s}{0},\ldots,0\right)=\frac{1}{h_1}\neq 0$. In the second case we can apply the change $y_1=Y_1+h_2Y_2, y_2=Y_2+\sqrt{h_1}Y_{2s}, y_{2s-1}=\sqrt{h_1}Y_1+\sqrt{h_1}h_2Y_2+Y_{2s-1}$ to get H_{2s} and an equivalent linear form $Y_1+h_2Y_2$. Therefore, $Q(1,h_2,0,\ldots,0)=h_2\neq 0$. Therefore, if $b_0=0$, case 2.(e) of Proposition 1 gives us row #21. Observe that in such a case we have (q^m-1) choices for a_0^0, $D_r(m-2k-1)$ choices for the a_i, $q-1$ possible h_1, $\frac{q}{2}$ possible h_2, $q^{2(s-1)}$ choices for the remaining h_i (it does not matter whether we are in the hyperbolic or elliptic case), and q for b_1. If $b_0\neq 0$ ($q-1$ choices), case 2.(d) of Proposition 1 is used to get rows #22 and #23, where we count (q^m-1) choices for a_0^0, $D_r(m-2k-1)$ choices for the a_i, $\frac{(q-1)q}{2}$ pairs (h_1,h_2), $\frac{q^{2(s-1)}\pm q^{s-1}}{2}$ choices for $h_3,\ldots,h_{2s}$, and $q-1$ possible b_0, and $\frac{q}{2}$ different $\tilde{b}_1$, depending on the absolute trace of $\frac{\tilde{b}_1Q(a_1,\ldots,a_m)}{b_0}$ (observe that in these cases the hyperbolic and elliptic roles are inverted).

□

Theorem 2. *The terms of the ideal weight enumerator of the code $\mathcal{DG}_R(m,r)$ are summarized in Table 2. And so the minimum distance of the Generalized Delsarte-Goethals code $\mathcal{DG}_q(m+1,\delta)$ is* $\frac{q-1}{q}\left(q^{m+1}-q^{\frac{m+1}{2}+r}\right)$.

#case	Term	Coefficient
1	$y_1^{q^m}$	$q^{m(r+1)+1}(q-1)$
2	$y_0^{q^{m-1}} y_2^{q^m - q^{m-1}}$	$B_r(m-2k-1)(q^m - q^{2s} \ )q$
3	$y_0^{q^{m-1} \pm (q-1)q^{m-s-1}} y_2^{q^m - q^{m-1} \mp (q-1)q^{m-s-1}}$	$B_r(m-2k-1)\frac{q^{2s} \pm q^s}{2}$
4	$y_0^{q^{m-1} \mp q^{m-s-1}} y_2^{q^m - q^{m-1} \pm q^{m-s-1}}$	$B_r(m-2k-1)\frac{q^{2s} \pm q^s}{2}(q-1)$
5	$y_0^{q^{m-2} \pm (q-1)q^{m-s-2}} y_2^{q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-2}} y_1^{q^m - q^{m-1}}$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\frac{q^{2s} \pm q^s}{2}(q^m-1)q^2$
6	$y_0^{q^{m-2} \mp q^{m-s-2}} y_2^{q^{m-1} - q^{m-2} \pm q^{m-s-2}} y_1^{q^m - q^{m-1}}$	$(B_r^1(m-2k-1) - D_r(m-2k-1))\frac{q^{2s} \pm q^s}{2}(q^m-1)(q-1)q^2$
7	$y_0^{q^{m-2}} y_2^{q^{m-1} - q^{m-2}} y_1^{q^m - q^{m-1}}$	$(B_r^1(m-2k-1) - D_r(m-2k-1))(q^m - q^{2s+1})(q^m-1)q^2$ $+D_r(m-2k-1)(q^m - q^{2s})(q^m-1)q^2$ $+2D_r(m-2k-1)q^{2s}(q^m-1)(q-1)$
8	$y_0^{q^{m-2} \pm (q-1)q^{m-s-1}} y_2^{q^{m-1} - q^{m-2} \mp (q-1)q^{m-s-1}} y_1^{q^m - q^{m-1}}$	$D_r(m-2k-1)\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)q$
9	$y_0^{q^{m-2} \mp q^{m-s-1}} y_2^{q^{m-1} - q^{m-2} \pm q^{m-s-1}} y_1^{q^m - q^{m-1}}$	$D_r(m-2k-1)\frac{q^{2(s-1)} \pm q^{s-1}}{2}(q^m-1)(q-1)q$ $+D_r(m-2k-1)\frac{q^{2(s-1)}}{2}(q^m-1)(q-1)^2q^2$

Table 2: Summary table of terms in the ideal weight enumerator ($0 \leq k \leq \frac{m-1}{2}$ and $s = \frac{m-2k-1}{2}$) (numbers B_r, B_r^1 and D_r are defined in Proposition 2)

Proof. The table is obtained from Table 1 adding the number of codewords associated to the same term. Namely, rows #1 to #4 remain the same, where as rows #5#7 give row #5, rows #6#8 give row #6, rows #9#10#13#14#18#19#21 give row #7, rows #11#16 give row #8 and rows #12#15#17#20#22#23 give row #9.

On the other hand, if for each term we denote by ν_i the exponent of the variable y_i $(i = 0, 1, 2)$, then the cases #1 to #4 give codewords of weight $q\nu_2$, i.e., 0 and $q^{m+1} - q^m - \Delta$ with $\Delta \in \{0, \pm(q-1)q^{m-s}, \pm q^{m-s}\}$, and $\frac{m-1}{2} - r < s \leq \frac{m-1}{2}$, because $B_r(m-2k-1)$ has to be nonzero ($s = 0$ is also possible in some cases). The rest of the cases give codewords of weight $q\nu_2 + (q-1)(q^m - q^{m-1}) = q(q^{m-1} - \nu_0) + (q^{m+1} - 2q^m + q^{m-1}) = q^{m+1} - q^m - q(\nu_0 - q^{m-2})$. For them we have $q(\nu_0 - q^{m-2}) \in \{\pm(q-1)q^{m-s-1}, \pm q^{m-s-1}, 0, \pm(q-1)q^{m-s}, \pm q^{m-s}\}$, with $\frac{m-1}{2} - r < s \leq \frac{m-1}{2}$ (because $B_r^1(m-2k-1) - D_r(m-2k-1)$ or $D_r(m-2k-1)$ can not be zero). Also, $s = \frac{m-1}{2} - r$ is allowed in rows #5#6 and #7, because in such a case $B_r^1(m-2k-1) - D_r(m-2k-1)$ is nonzero too. Therefore, the minimum weight in a nonzero codeword is achieved in row #5 when $s = \frac{m-1}{2} - r$, i.e., $q^{m+1} - q^m - (q-1)q^{m-(\frac{m-1}{2}-r)-1} = (q-1)(q^m - q^{\frac{m+1}{2}+r-1}) = \frac{q-1}{q}\left(q^{m+1} - q^{\frac{m+1}{2}+r}\right)$. □

4 Connection of the construction with nonassociative rings

In this final section we connect the codes introduced in this paper with finite semifields, i.e., with finite nonassociative division rings. The connection is related to the construction of codes of Kerdock type from symplectic finite semifields (a particular class of finite nonassociative division rings in the Knuth orbit of a commutative semifield), and also with the recent observation that binary additive MRD codes with minimum distance $n-1$ are spanned by two binary additive MRD codes with minimum distance n [35].

A finite nonassociative ring S is called presemifield, if the set of nonzero elements S^* is closed under the product. If S is unital, then it is called finite semifield. The characteristic of a finite presemifield S is a prime number p, and S is a finite-dimensional algebra over $\mathbb{F}_q$ $(q = p^c)$ of dimension m, for some $c, m \in \mathbb{N}$, so that $|S| = q^m$.

Given a $\mathbb{F}_q$−basis $B = \{b_1, \ldots, b_m\}$ of S, a unique set of multiplication constants $\lambda_{ijk} \in \mathbb{F}_q$ can be defined by the rule $b_i \cdot b_j = \sum_{k=1}^{m} \lambda_{ijk} b_k$. The finite presemifield S is commutative if and only if $\lambda_{ijk} = \lambda_{jik}$ for all $1 \leq i, j, k \leq m$. Also, S is called symplectic if $\lambda_{ijk} = \lambda_{kji}$ for all $1 \leq i, j, k \leq m$. There is a direct connection between these two types of finite presemifields, as observed in [12], since a commutative presemifield is in the Knuth orbit of a symplectic presemifield and reciprocally.

When S is a symplectic presemifield over $\mathbb{F}_2$ and $s \in S$, the coordinate matrix M_s of the map of right multiplication $R_s(x) = x \cdot s$ can be taken symmetric, and so it defines a $\mathbb{Z}/4\mathbb{Z}-$valued quadratic form Q_s in a straightforward way (namely, $Q_s(x) = xM_sx^{\intercal}$, where $x \in \mathbb{F}_2^m$, $x^{\intercal}$ is its transpose, and operations are carried out mod 4). Moreover, according to [4], when $m \geq 3$ odd, the set $\{Q_s \mid s \in S\}$ induces a $\mathbb{Z}/4\mathbb{Z}-$Kerdock code (namely, $\{(Q_s(x) + 2ax^{\intercal} + \varepsilon)_{x\in\mathbb{F}_2^m} \mid s \in S, a \in \mathbb{F}_2^m, \varepsilon \in \mathbb{Z}/4\mathbb{Z}\}$) which, under the Gray map, produces a nonlinear binary code of Kerdock type (i.e., with the same parameters of the Kerdock code) but not necessarily equivalent.

More generally, any (non necessarily symplectic) finite presemifield over $\mathbb{F}_q$ induces a set of q^m (non necessarily symmetric) bilinear forms $xM_sy^{\intercal}$ satisfying $M_s - M_t$ nonsingular for all $s \neq t$. And reciprocally, any additively closed set of q^m bilinear forms with coordinate matrices M_s ($s \in \mathbb{F}_q^m$) satisfying $M_s - M_t$ nonsingular for all $s \neq t$, induces a presemifield by the multiplication rule $x \bullet s = M_s x^{\intercal}$.

On the other hand, there is a connection between finite presemifields and $m \times m$ maximum rank-distance (MRD) codes, i.e., codes C consisting of $m \times m$ matrix words over $\mathbb{F}_q$ under the rank metric [6] satisfying the following property: $|C| = q^{m(m-e+1)}$, where $\text{rank}(A) \geq e$, for all $0 \neq A \in C$. Additively closed MRD codes of order q^m correspond to presemifields (simply consider the set of coordinate matrices of the maps R_s, for all $s \in S$). Recently, it has been observed that for any additively closed binary MRD code of order 2^{2m} (i.e., with minimum rank distance $m-1$) there exist two presemifields S_1 and S_2 such that $C = \{M_{s_1} - M_{s_2} \mid s_1 \in S_1, s_2 \in S_2\}$, that is, it is spanned by the coordinate matrices of right multiplication of two finite presemifields [35, Main Theorem].

The codes considered in this paper are related to the original work of Delsarte and Goethals [7] in the following way. As mentioned in [34, page 1021] the alternating $(m+1, m+1-2r)-$set of alternating forms constructed in Theorem 9 of such a paper is the set $\phi(Y)$, where $Y = \{B_{Q_a} \mid (a_0, \ldots, a_r) \in \Gamma(S)^{r+1}\}$ (see Remark 1.3) and $\phi(B_{Q_a}) : (\Gamma(S) \times \Gamma(R))^2 \to \Gamma(R)$ is given by

$$\phi(B_{Q_a})((x, \alpha), (y, \beta)) = B_{Q_a}(x, y) + \sqrt{B_{Q_a}(x, x)B_{Q_a}(y, y)} + \beta\sqrt{B_{Q_a}(x, x)} + \alpha\sqrt{B_{Q_a}(y, y)}$$

The set C of coordinate matrices of these $q^{m(r+1)}$ bilinear forms is additively closed and satisfies $\text{rank}(A) \geq m + 1 - 2r$, for all $0 \neq A \in C$. It is clear that C is not a MRD, but it attains the bound $|C| \leq q^{m(r+1)}$ [34, Corollary 7]. So, from this point of view, it is a set of maximum size induced by the bilinear maps B_{Q_a}. In the same line of [35, Main Theorem] we can straightforwardly state that C can be spanned by the ϕ images of coordinate matrices of right multiplication of $r + 1$ finite presemifields. Namely:

$$Y = \left\{ M_{a_0} + \sum_{i=1}^{r} (M_{a_i} + M_{a_i}^t) \mid a_i \in \Gamma(S) \right\}$$

where the presemifields are obtained from the sets of bilinear forms $\{\text{Tr}(a_i x^{q^i} y)\}_{a_i \in \Gamma(S)}$. It is an open problem to determine whether this number of presemifields allowing this description is minimal.

5 Conclusions

Classical binary Delsarte-Goethals codes can be described through quaternary codes (i.e., codes over the alphabet $\mathbb{Z}/4\mathbb{Z}$). This description connects them to low-correlation sequences, in particular to the sequence family $S(2)$ appearing in the W-CDMA component of the IMT-2000 standard for 3G mobile communication. In this paper we have introduced a nonbinary version of the Delsarte-Goethals based on Galois rings of the form $GR(2^{2lm}, 2^2)$, and on the quadratic forms valued in them ($m \geq 3$ odd). The resulting codes over the alphabet $\mathbb{F}_q$ ($q = 2^l$) have length q^{m+1}, cardinality $q^{m(r+2)+2}$ and Hamming distance $\frac{q-1}{q}(q^{m+1} - q^{\frac{m+1}{2}+r})$, where $0 \leq r \leq \frac{m-1}{2}$. Such a minimum distance has been obtained by explicitly computing the ideal weight enumerator of the Galois ring linear codes they are derived from. Binary Delsarte-Goethals codes and the Generalized Kerdock codes of A.A. Nechaev and A.S. Kuzmin are obtained as particular instances, when $l = 1$ or $r = 0$, respectively. A connection of this construction to finite semifields has been also established.

Acknowledgments

This paper is humbly dedicated to the memory of Viktor Timofeevich Markov and Aleksandr Aleksandrovich Nechaev.

References

[1] G. Bini, F. Flamini, Finite commutative rings and their applications, Kluwer Academic Publishers, Boston, MA, (2002).

[2] S. Boztaş, R. Hammons and P.V. Kumar, *4-Phase Sequences with Near-Optimum Correlation Properties*, IEEE Trans. on Inform. Theory, **IT-38 (3)**, (1992), 1101–1113.

[3] E.H. Brown, *Generalizations of the Kervaire invariant*, Ann. of Math. (2) **95 (2)** (1972), 368–383.

[4] A.R. Calderbank, P.J. Cameron, W.M. Kantor and J.J. Seidel, *$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, Proc. London Math. Soc. **75** (1997), 436–480.

[5] C. Carlet, *$\mathbb{Z}_{2^k}$-Linear Codes*, IEEE Trans. Inform. Theory **44 (4)** (1998) 1543–1547.

[6] Ph. Delsarte, *Bilinear Forms over a Finite Field, with Applications to Coding Theory*, Journal of Combinatorial Theory, Series A, **25** (1978), 226–241.

[7] P. Delsarte and J-M. Goethals, *Alternating bilinear forms over $GF(q)$*, Journal of Combinatorial Theory, Series A, **19(1)** (1975), 26–50.

[8] S. González, C. Martínez, I.F. Rúa, *Symplectic Spread based Generalized Kerdock Codes*, Designs, Codes and Cryptography **42 (2)** (2007), 213–226.

[9] A.R. Hammons,Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

[10] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Science Publications, New-York (1979).

[11] W.M. Kantor, *Spreads, translation planes and Kerdock sets. I.*, SIAM J. Algebraic and Discrete Methods **3** (1982), 151–165.

[12] W.M. Kantor, *Commutative semifields and symplectic spreads*, J. Algebra **270** (2003), 96–114.

[13] A.M. Kerdock, *A class of low-rate non-linear binary codes*, Inform. Control **20** (1972), 182–187.

[14] A. Klapper, *Cross-correlations of geometric sequences in characteristic two*, Des. Codes Cryptogr. **3** (1993) 347–377.

[15] P.V. Kumar, T. Helleseth, A.R. Calderbank and A.R. Hammons, Jr., *Large Families of Quaternary Sequences with Low Correlation*, IEEE Trans. Inform. Theory, **42** (1996), 579–592.

[16] P.V. Kumar, H.F. Francis Lu, T. Helleseth and D.-J. Shin, *On the Large Family of Low Correlation Quaternary Sequences* $S(2)$, IEEE Intnl. Conf. Personal Wireless Comm., (ICPWC?2000), Hyderbad, December 17-20, 2000.

[17] V.L. Kurakin, A.S. Kuzmin, V.T. Markov, A.V. Mikhalev and A.A. Nechaev, Linear codes and polylinear recurrences over finite rings and modules (a survey), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 13*, Lect. Notes. in Comput. Sci. **1719** (Springer, Berlin, 1999) 363-391.

[18] A.S. Kuzmin and A.A. Nechaev, *Linearly presented codes and Kerdock code over an arbitrary Galois field of the characteristic* 2, Russian Math. Surveys **49 (5)** (1994), 183–184.

[19] A.S. Kuzmin and A.A. Nechaev, $\mathbb{Z}_4-$*linearity, two approaches*, Vth Int. Workshop on Alg. and Comb. Coding Theory, Proceedings, Sozopol, Bulgaria, (1996), 212–215.

[20] A.S. Kuzmin, V.T. Markov, A.A. Nechaev, A.S. Neljubin *A generalization of the binary Preparata code*, Discrete Applied Mathematics, **154** (2006), 337–345.

[21] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics and its applications 20, Addison-Wesley (1983).

[22] M.C. López-Díaz, I.F. Rúa, *An invariant for quadratic forms valued in Galois rings of characteristic 4*, Finite Fields Appl. **13 (4)** (2007), 946–961.

[23] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam (1977).

[24] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics **28**, Marcel Dekker, New York, (1974).

[25] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC-Press, Boca-Raton (2013).

[26] D.E. Muller, *Application of Boolean algebra to switching circuit design and to error detection* IRE Transactions on Computers, **3** (1954), 6–12.

[27] A.A. Nechaev, *Trace function in Galois ring and noise stable codes*, V All-Union Symp. on theory of rings, algebras and modules (Novosibirsk) (1982), 97.

[28] A.A. Nechaev, *Kerdock's code in a cyclic form*, Diskret. Mat. **1** (1989), 123–139.

[29] A.A. Nechaev and A.S. Kuzmin, *Trace-function on a Galois ring in coding theory*, Lecture Notes Comput. Sci. **1255** (1997), 277–290.

[30] F.P. Preparata, *A class of optimum non-linear double-error correcting codes*, Inform. Control **13** (1968) 378–400.

[31] I.S. Reed, *A class of multiple-error-correcting codes and the decoding scheme* IEEE Transactions on Information Theory, **4** (1954), 38–49.

[32] S. Roman, Advanced Linear Algebra, Graduate Texts in Mathematics 135, Springer-Verlag, New York (1992)

[33] K-U. Schmidt, $\mathbb{Z}_4-$*valued quadratic forms and quaternary sequence families*, IEEE Trans. Inf. Theory **55 (12)** (2009), 5803–5810.

[34] K-U. Schmidt, *Symmetric bilinear forms over finite fields of even characteristic*, J. Comb. Theory Series A**117** (2010), 1011–1026.

[35] J. Sheekey, *Binary additive MRD codes with minimum distance $n-1$ must contain a semifield spread set*, `arXiv:1808.08854` (2018).