Linear Algebra and its Applications 548 (2018) 203–220

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

A new family of MRD-codes ☆

Bence Csajbók [a], Giuseppe Marino [b,*], Olga Polverino [b], Corrado Zanella [c]

[a] MTA–ELTE Geometric and Algebraic Combinatorics Research Group, ELTE Eötvös Loránd University, Budapest, Hungary, Department of Geometry, 1117 Budapest, Pázmány P. stny. 1/C, Hungary

[b] Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Viale Lincoln 5, I-81100 Caserta, Italy

[c] Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università di Padova, Stradella S. Nicola, 3, I-36100 Vicenza, Italy

A R T I C L E   I N F O

Article history:
Received 7 June 2017
Accepted 28 February 2018
Available online 12 March 2018
Submitted by R. Brualdi

MSC:
51E20
05B25
51E22

Keywords:
Scattered subspace
MRD-code
Linear set

A B S T R A C T

We introduce a family of linear sets of $\mathrm{PG}(1, q^{2n})$ arising from maximum scattered linear sets of pseudoregulus type of $\mathrm{PG}(3, q^n)$. For $n = 3, 4$ and for certain values of the parameters we show that these linear sets of $\mathrm{PG}(1, q^{2n})$ are maximum scattered and they yield new MRD-codes with parameters $(6, 6, q; 5)$ for $q > 2$ and with parameters $(8, 8, q; 7)$ for q odd.

☆ The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA – INdAM). The first author was partially supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by OTKA Grant No. K 124950.

* Corresponding author.

E-mail addresses: csajbokb@cs.elte.hu (B. Csajbók), giuseppe.marino@unicampania.it (G. Marino), olga.polverino@unicampania.it (O. Polverino), corrado.zanella@unipd.it (C. Zanella).

https://doi.org/10.1016/j.laa.2018.02.027
0024-3795/

1. Introduction

Linear sets are natural generalizations of subgeometries. Let $\Lambda = \mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$, where V is a vector space of dimension r over $\mathbb{F}_{q^n}$. A point set L of Λ is said to be an $\mathbb{F}_q$-*linear set* of Λ of rank k if it is defined by the non-zero vectors of a k-dimensional $\mathbb{F}_q$-vector subspace U of V, i.e.

$$L = L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}.$$

The maximum field of linearity of an $\mathbb{F}_q$-linear set L_U is $\mathbb{F}_{q^t}$ if $t \mid n$ is the largest integer such that L_U is an $\mathbb{F}_{q^t}$-linear set.

Two linear sets L_U and L_W of Λ are said to be $\mathrm{P\Gamma L}$-*equivalent* (or simply *equivalent*) if there is an element ϕ in $\mathrm{P\Gamma L}(r, q^n)$, the collineation group of Λ, such that $L_U^\phi = L_W$. It may happen that two $\mathbb{F}_q$-linear sets L_U and L_W of Λ are $\mathrm{P\Gamma L}$-equivalent even if the two $\mathbb{F}_q$-vector subspaces U and W are not in the same orbit of $\Gamma\mathrm{L}(r, q^n)$, the group of invertible $\mathbb{F}_{q^n}$-semilinear transformations of V (see [8] and [5] for further details).

The set of $m \times n$ matrices $\mathbb{F}_q^{m\times n}$ over $\mathbb{F}_q$ is a rank metric $\mathbb{F}_q$-space with rank metric distance defined by $d(A, B) = rk\,(A - B)$ for $A, B \in \mathbb{F}_q^{m\times n}$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is called a *rank distance code* (RD-code for short). The minimum distance of $\mathcal{C}$ is

$$d(C) = \min_{A,B\in\mathcal{C},\ A\neq B} \{d(A, B)\}.$$

In [11] the Singleton bound for an $m\times n$ rank metric code $\mathcal{C}$ with minimum rank distance d was proved:

$$\#\mathcal{C} \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}. \tag{1}$$

If this bound is achieved, then $\mathcal{C}$ is an MRD-code. MRD-codes have various applications in communications and cryptography; see for instance [12,17]. More properties of MRD-codes can be found in [11–13,33]. When $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m\times n}$, we say that $\mathcal{C}$ is an $\mathbb{F}_q$-linear code and the dimension $\dim_q(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. If d is the minimum distance of $\mathcal{C}$ we say that $\mathcal{C}$ has parameters $(m, n, q; d)$.

In [35, Section 4], the author showed that scattered linear sets of $\mathrm{PG}(1, q^m)$ of rank m yield $\mathbb{F}_q$-linear MRD-codes of dimension $2m$ and minimum distance $m - 1$. Also, codes arising in this way have *middle nucleus* of order q^m (which is an invariant with respect to the equivalence on MRD-codes, see Section 6). In Proposition 6.1 we prove that every code with these parameters can be obtained from a suitable scattered linear set of rank m of $\mathrm{PG}(1, q^m)$. The correspondence between MRD codes and linear sets of $\mathrm{PG}(1, q^m)$ has been recently generalized in [6]. The number of non-equivalent MRD-codes obtained from a scattered linear set of $\mathrm{PG}(1, q^m)$ of rank m was studied in [5, Section 5.4]. In [24] the author investigated in detail the relationship between linear sets of $\mathrm{PG}(n-1, q^n)$ of rank n and $\mathbb{F}_q$-linear MRD-codes.