ARTICLE IN PRESS YJABR:16622

Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Exceptional scattered polynomials

Daniele Bartoli[a], Yue Zhou[b,*]

[a] *Department of Mathematics and Computer Science, University of Perugia, 06123 Perugia, Italy*
[b] *College of Liberal Arts and Sciences, National University of Defense Technology, 410073 Changsha, China*

A R T I C L E I N F O

Article history:
Received 24 October 2017
Available online xxxx
Communicated by William M. Kantor

Keywords:
Maximum scattered linear set
MRD code
Algebraic curve
Finite field
Hasse–Weil bound

A B S T R A C T

Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$. If the $\mathbb{F}_q$-subspace $U = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\}$ defines a maximum scattered linear set, then we call f a scattered polynomial of index t. As these polynomials appear to be very rare, it is natural to look for some classification of them. We say a function f is an exceptional scattered polynomial of index t if the subspace U associated with f defines a maximum scattered linear set in $\mathrm{PG}(1, q^{mn})$ for infinitely many m. Our main results are the classifications of exceptional scattered monic polynomials of index 0 (for $q > 5$) and of index 1. The strategy applied here is to convert the original question into a special type of algebraic curves and then to use the intersection theory and the Hasse–Weil theorem to derive contradictions.

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), yue.zhou.ovgu@gmail.com (Y. Zhou).

https://doi.org/10.1016/j.jalgebra.2018.03.010
0021-8693/

Please cite this article in press as: D. Bartoli, Y. Zhou, Exceptional scattered polynomials, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.03.010

1. Introduction

Let q be a prime power and $r, n \in \mathbb{N}$. Let V be a vector space of dimension r over $\mathbb{F}_{q^n}$. For any k-dimensional $\mathbb{F}_q$-vector subspace U of V, the set $L(U)$ defined by the nonzero vectors of U is called an $\mathbb{F}_q$-*linear set* of $\Lambda = \mathrm{PG}(V, q^n)$ of *rank* k, i.e.

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

It is notable that the same linear set can be defined by different vector subspaces. Consequently, we always consider a linear set and the vector subspace defining it in pair.

Let $\Omega = \mathrm{PG}(W, \mathbb{F}_{q^n})$ be a subspace of Λ and $L(U)$ an $\mathbb{F}_q$-linear set of Λ. We say that Ω has *weight* i in $L(U)$ if $\dim_{\mathbb{F}_q}(W \cap U) = i$. Thus a point of Λ belongs to $L(U)$ if and only if it has weight at least 1. Moreover, for any $\mathbb{F}_q$-linear set $L(U)$ of rank k,

$$|L_U| \le \frac{q^k - 1}{q - 1}.$$

When the equality holds, i.e. all the points of $L(U)$ have weight 1, we say $L(U)$ is *scattered*. A scattered $\mathbb{F}_q$-linear set of highest possible rank is called a *maximum scattered* $\mathbb{F}_q$-*linear set*. See [3] for the possible ranks of maximum scattered linear sets.

Maximum scattered linear sets have various applications in Galois geometry, including blocking sets [1,33,35], two-intersection sets [3,4], finite semifields [5,17,34,39], translation caps [2], translation hyperovals [16], etc. For more applications and related topics, see [43] and the references therein. For recent surveys on linear sets and particularly on the theory of scattered spaces, see [30,31].

In this paper, we are interested in maximum scattered linear sets in $\mathrm{PG}(1, q^n)$. Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$ and

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\}. \tag{1}$$

Clearly U is an n-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ and f can be written as a q-polynomial $f(X) = \sum a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$. It is not difficult to show that a necessary and sufficient condition for $L(U)$ to define a maximum scattered linear set in $\mathrm{PG}(1, q^n)$ is

$$\frac{f(x)}{x} = \frac{f(y)}{y} \text{ if and only if } \frac{y}{x} \in \mathbb{F}_q, \quad \text{for } x, y \in \mathbb{F}_{q^n}^*. \tag{2}$$

In [47], such a q-polynomial is called a *scattered polynomial*.

Two linear sets $L(U)$ and $L(U')$ in $\mathrm{PG}(2, q^n)$ are *equivalent* if there exists an element of $\mathrm{P\Gamma L}(2, q^n)$ mapping $L(U)$ to $L(U')$. It is obvious that if U and U' are equivalent as $\mathbb{F}_{q^n}$-spaces, then $L(U)$ and $L(U')$ are equivalent. However, the converse is not true in general. For recent results on the equivalence and classification of linear sets, we refer to [10,12,13].

Please cite this article in press as: D. Bartoli, Y. Zhou, Exceptional scattered polynomials, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.03.010