ISSN 0032-9460, Problems of Information Transmission, 2018, Vol. 54, No. 2, pp. 101–115. © Pleiades Publishing, Inc., 2018.
Original Russian Text © D. Bartoli, A.A. Davydov, S. Marcugini, F. Pambianco, 2018, published in Problemy Peredachi Informatsii, 2018, Vol. 54, No. 2, pp. 3–19.

CODING THEORY

On the Smallest Size of an Almost Complete Subset of a Conic in PG(2, q) and Extendability of Reed–Solomon Codes[1]

D. Bartoli[a,2,*], A. A. Davydov[b,3,], S. Marcugini[a,2,***], and F. Pambianco[a,2,****]**

[a] *Department of Mathematics and Computer Sciences, Università degli Studi di Perugia, Perugia, Italy*
[b] *Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia*
e-mail: *daniele.bartoli@unipg.it, **adav@iitp.ru, ***stefano.marcugini@unipg.it, ****fernanda.pambianco@unipg.it

Received September 6, 2016; in final form, December 25, 2017

Abstract—In the projective plane $\mathrm{PG}(2,q)$, a subset $\mathcal{S}$ of a conic $\mathcal{C}$ is said to be *almost complete* if it can be extended to a larger arc in $\mathrm{PG}(2,q)$ only by the points of $\mathcal{C}\setminus\mathcal{S}$ and by the nucleus of $\mathcal{C}$ when q is even. We obtain new upper bounds on the smallest size $t(q)$ of an almost complete subset of a conic, in particular,

$$t(q) < \sqrt{q(3\ln q + \ln\ln q + \ln 3)} + \sqrt{\frac{q}{3\ln q}} + 4 \sim \sqrt{3q\ln q},$$
$$t(q) < 1.835\sqrt{q\ln q}.$$

The new bounds are used to extend the set of pairs (N,q) for which it is proved that every normal rational curve in the projective space $\mathrm{PG}(N,q)$ is a complete $(q+1)$-arc, or equivalently, that no $[q+1, N+1, q-N+1]_q$ generalized doubly-extended Reed–Solomon code can be extended to a $[q+2, N+1, q-N+2]_q$ maximum distance separable code.

DOI: 10.1134/S0032946018020011

1. INTRODUCTION

Let $\mathrm{PG}(N,q)$ be the N-dimensional projective space over the Galois field $\mathbb{F}_q$ of order q. In $\mathrm{PG}(N,q)$, an n-arc with $n > N+1$ is a set of n points such that no $N+1$ points belong to the same hyperplane of $\mathrm{PG}(N,q)$. An n-arc of $\mathrm{PG}(N,q)$ is complete if it is not contained in an $(n+1)$-arc of $\mathrm{PG}(N,q)$. A *normal rational curve* in $\mathrm{PG}(N,q)$, $2 \le N \le q-2$, is any $(q+1)$-arc projectively equivalent to the arc $\{(1,t,t^2,\ldots,t^N) : t \in \mathbb{F}_q\} \cup \{(0,\ldots,0,1)\}$. For an introduction to projective spaces over finite fields, see [1–3].

[1] The research has been carried out using computing resources of the Federal Collective Usage Center "Complex for Simulation and Data Processing for Mega-science Facilities" at the National Research Center "Kurchatov Institute," http://ckp.nrcki.ru/.

[2] Supported in part by the Ministry of Education, Universities and Research of Italy (MIUR), project "Geometrie di Galois e strutture di incidenza", Italian National Group for Algebraic and Geometric Structures and Their Applications (GNSAGA–INDAM), and University of Perugia, projects "Configurazioni geometriche e superfici altamente simmetriche" and "Codici lineari e strutture geometriche correlate," Base Research Fund 2015.

[3] The research was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences at the expense of the Russian Science Foundation, project no. 14-50-00150.

Let an $[n, k, d]_q$ code be a q-ary linear code of length n, dimension k, and minimum distance d. If $d = n-k+1$, it is a maximum distance separable (MDS) code. The code dual to an $[n, k, n-k+1]_q$ MDS code is an $[n, n-k, k+1]_q$ MDS code.

Points (in homogeneous coordinates) of an n-arc in $\mathrm{PG}(N, q)$ treated as columns define a generator matrix of an $[n, N+1, n-N]_q$ MDS code. If an n-arc in $\mathrm{PG}(N, q)$ is complete, then the corresponding $[n, N+1, n-N]_q$ MDS code cannot be extended to an $[n+1, N+1, n-N+1]_q$ MDS code. Properties of linear MDS codes and their equivalence to arcs are considered, for example, in [1–14].

In a generator matrix of a $[q+1, N+1, q-N+1]_q$ generalized doubly-extended Reed–Solomon (GDRS) code, the jth column is of the form $(v_j, v_j\alpha_j, v_j\alpha_j^2, \ldots, v_j\alpha_j^N)^T$, where $\alpha_1, \ldots, \alpha_q$ are distinct elements of $\mathbb{F}_q$ and $v_1, \ldots, v_q$ are nonzero (not necessarily distinct) elements of $\mathbb{F}_q$, $j = 1, 2, \ldots, q$. Also, this matrix contains one more column $(0, \ldots, 0, v)^T$ with $v \neq 0$. The dual to a GDRS code is a GDRS code too.

Points (in homogeneous coordinates) of a normal rational curve in $\mathrm{PG}(N, q)$ treated as columns define a generator matrix of a $[q+1, N+1, q-N+1]_q$ GDRS code. The following proposition is well known.

Proposition. *Let N and q be fixed integers with $2 \le N \le q-2$. Let q be a prime power. Then the following statements are equivalent*:

- *Every normal rational curve in $\mathrm{PG}(N, q)$ is a complete $(q+1)$-arc*;
- *No $[q+1, N+1, q-N+1]_q$ GDRS code can be extended to a $[q+2, N+1, q-N+2]_q$ MDS code.*

Due to this proposition, all the results on completeness of normal rational curves given below can be reformulated (in the coding theory language) for the extendability of GDRS codes.

Completeness of normal rational curves and related problems are considered in numerous works starting from Segre's paper [15] of 1955 (see, for example, [1–20], where the corresponding overviews and references can be found). In particular, the following conjecture, connected with Segre's famous three problems, is well known.

Conjecture. *Let $2 \le N \le q-2$. In $\mathrm{PG}(N, q)$, every normal rational curve is a complete $(q+1)$-arc except for the cases of q even and $N \in \{2, q-2\}$, in which cases one point can be added to the curve.*

Remark 1. As a comment to the above conjecture for even q, note the following. If $N = 2$, a point that can be added to a normal rational curve is unique. But if $N = q-2$, there are many points in $\mathrm{PG}(q-2, q)$ which extend a normal rational curve to a $(q+2)$-arc (see [13, Theorem 3.10] for a geometric characterization of these points).

Remark 2. If $k \ge q$, then an $[n, k, n-k+1]_q$ MDS code has length $n \le k+1$ (see, e.g., [10,11]). For $2 \le N \le q-2$, the well-known *MDS conjecture* assumes that an $[n, N+1, n-N]_q$ MDS code (or, equivalently, an n-arc in $\mathrm{PG}(N, q)$) has length $n \le q+1$ except for the cases of q even and $N \in \{2, q-2\}$, in which cases $n \le q+2$. The MDS conjecture considers all MDS codes (or all arcs), whereas the above conjecture concerns only normal rational curves (or GDRS codes). If the MDS conjecture holds for some pair (N, q), then the above conjecture holds too, but the converse is not true in general.

For many pairs (N, q) the above conjecture is proved (see [1–11, 14–20] and references therein), but in general, *completeness of normal rational curves is an open problem*. The main known results are given in Table 1, where p and $p_0(h)$ are *prime*. Note that for rows 1–6 of the table the MDS conjecture is proved. In [5] (see row 7 of Table 1), it is proved that in $\mathrm{PG}(N, q)$, q odd, a subset of size $3(N-1)-6$ of a normal rational curve cannot be extended to a $(q+2)$-arc. This means