On Cyclic MDS-Codes

M. Amin Shokrollahi

Bell Labs, Rm. 2C-353, 700 Mountain Ave, Murray Hill, NJ 07974, USA

Abstract We investigate the question when a cyclic code is maximum distance separable (MDS). For codes of (co-)dimension 3, this question is related to permutation properties of the polynomial $(x^b-1)/(x-1)$ for a certain b. Using results on these polynomials we prove that over fields of odd characteristic the only MDS cyclic codes of dimension 3 are the Reed-Solomon codes. For codes of dimension $O(\sqrt{q})$ we prove the same result using techniques from algebraic geometry and finite geometry. Further, we exhibit a complete q-arc over the field $\mathbb{F}_q$ for even q. In the last section we discuss a connection between modular representations of the general linear group over $\mathbb{F}_q$ and the question of whether a given cyclic code is MDS.

1 Introduction

A linear code C is called **cyclic** if $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is in C whenever $(c_0, c_1, \ldots, c_{n-1})$ is. Let ϕ denote the morphism from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q[x]/(x^n-1)$ sending $(a_0, \ldots, a_{n-1})$ to $\sum_i a_i x^i \bmod (x^n-1)$. Then it is easy to see that a subspace C of $\mathbb{F}_{q^n}$ is a cyclic code if and only if its image under ϕ is an ideal of $\mathbb{F}_q[x]/(x^n-1)$ [7, Chap. 6]. Since every ideal in this ring is principal, the image of C is generated by a polynomial $g(x)$ dividing x^n-1, unique up to scalar multiples. This polynomial is called the **generator polynomial** of C and the image of any codeword under ϕ is divisible by this polynomial. If n and q are co-prime, then $g(x)$ is uniquely determined by the set of its roots, which are also called the **zeros of** C.

It is easily seen that C is of dimension $n - \deg(g)$. The determination of the minimum distance of C from the set of zeros of g is much harder, though exact results on the complexity of this problem are not known. Typically, most of the research on this problem has concentrated on obtaining good lower bounds for the minimum distance in terms of the set of roots [8]. In this paper, we concentrate on aspects of the problem of bounding the minimum distance from above. Specifically, we discuss problems related to $[q-1, k, d]_q$-cyclic codes. (Here and in the following, an $[n, k, d]_q$-code is a code of block-length n, dimension k, and minimum distance d over the field $\mathbb{F}_q$.) Since q and $q-1$ are obviously co-prime, the code is uniquely identified by the set $\{\omega^{a_0}, \ldots, \omega^{a_r}\}$ of its zeros, where ω is a generator of $\mathbb{F}_q^\times$ which we assume to be fixed throughout the paper. We also assume thoughout, except in a brief remark in §2, that $r > 1$. We may hence identify the code with its **exponent set** $\{a_0, \ldots, a_r\}$. The question we want to investigate is whether the code is maximum distance separable, i.e., whether it has the maximum possible

minimum distance $r+2$. If this is the case, then we call the exponent set $\{a_0, \ldots, a_r\}$ q-**MDS**, or **MDS** for short, if q is obvious from the context.

If the exponent set $\{a_0, \ldots, a_r\}$ is not MDS, then there exists a polynomial $f = f_0 x^{i_0} + \cdots + f_r x^{i_r} \in \mathbb{F}_q[x]$ with pairwise different nonnegative integers $i_0, \ldots, i_r$ less than n such that $f(\omega^{a_0}) = \cdots = f(\omega^{a_r}) = 0$. This is equivalent to

$$\begin{pmatrix} \omega^{a_0 i_0} & \cdots & \omega^{a_0 i_r} \\ \vdots & \ddots & \vdots \\ \omega^{a_r i_0} & \cdots & \omega^{a_r i_r} \end{pmatrix} \begin{pmatrix} f_0 \\ \vdots \\ f_r \end{pmatrix} = 0.$$

The existence of a nonzero f with this property is equivalent to the vanishing of the determinant of the above matrix. Let now

$$X := \begin{pmatrix} X_0^{a_0} & \cdots & X_r^{a_0} \\ \vdots & \ddots & \vdots \\ X_0^{a_r} & \cdots & X_r^{a_r} \end{pmatrix},$$

where $X_0, \ldots, X_r$ are indeterminates over $\mathbb{F}_q$. Then it is easily seen that C is MDS if and only if

$$\det(X) \in \mathbb{F}_q[X_0, \ldots, X_r]$$

has no zeros in $(\mathbb{F}_q^\times)^{r+1} \setminus \Delta$, where $\Delta \subset \mathbb{F}_q^{r+1}$ is the zeroset of the discriminant $\prod_{i<j}(X_i - X_j)$. It follows that for any a and b, b co-prime to $q-1$, all exponent sets of the form $\{a, b+a, 2b+a, \ldots, rb+a\}$ mod $(q-1)$ are q-MDS. Indeed, for these sets the above determinant is essentially Vandermonde. The corresponding cyclic codes are equivalent to *Reed-Solomon codes* [7, §6.8]. In the sequel we call these sets "trivial." One of the results of this paper is that in many cases the only q-MDS exponent sets are the trivial ones, i.e., the corresponding cyclic codes are essentially Reed-Solomon codes. We note in passing that our results also solve some cases of a problem of Nick Reingold and Dan Spielman posed by Andrew Odlyzko in [10, p. 399].

We start our investigation in the next section by studying exponent sets of size three. We show that these sets are MDS if and only if the polynomial $x^{b-1} + \cdots + x + 1$ is a permutation polynomial over $\mathbb{F}_q$, where b is an integer obtained from the exponent set in question. This problem has been investigated by Matthews [9] in case of odd q. Using his results, we show that q-MDS exponent sets of size three are trivial for odd q. In Section 3 we investigate exponent sets whose sizes are "small" relative to q , and use some algebraic geometry as well as results about arcs in projective spaces to show that they are MDS if and only if they are trivial. Section 4 deals with the special exponent set $\{0, 1, \ldots, r-1, m\}$ for some m satisfying $r \le m \le q-2$. We show that if r is not large compared to q, then these exponent sets are MDS only if they are trivial. Then we will proceed by exhibiting an explicit family of complete q-arcs over fields of even characteristic. The last section of the paper deals with an unexpected connection between the minimum distance of cyclic codes and certain modular representations of $\mathrm{GL}_n(\mathbb{F}_p)$.

Many thanks go to E.F. Assmus, D. Spielman, and M. Zieve for pointing out to me the references [12], [10], and [9], respectively.

2 Small Exponent Sets

Exponent sets if size two are easy to handle: obviously, $\{0, a\}$ is q-MDS iff $\gcd(a, q-1) = 1$ and $\{a, b\}$ is q-MDS iff $\gcd(a-b, q-1) = 1$.

Exponent sets of size three are slightly more difficult to investigate. Let $I := \{0, a, b\}$ be an exponent set. We may without loss of generality assume that a divides $q-1$ and that $a \leq d := \gcd(b, q-1)$. I is q-MDS iff for every $x, y \in \mathbb{F}_q^\times \setminus \{1\}$, $x \neq y$ we have

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & x^a & y^a \\ 1 & x^b & y^b \end{pmatrix} = (x^a - 1)(y^b - 1) - (x^b - 1)(y^a - 1) \neq 0.$$

If $a \geq 3$, then we may take for x and y two different ath roots of unity in $\mathbb{F}_q^\times$, both unequal to one, to see that I is not MDS. The same argument works if $d \geq 3$. If $a = 2$, then necessarily $d = 2$ and we may take $x = -1$ to see that I is not MDS. Hence, we are left with the case $a = 1$. We may without loss of generality assume that $b \leq q/2$, since we may replace $\{0, 1, b\}$ by $\{q-0, q-1, q-b\} = \{1, 0, q-b\}$. Hence $\{0, 1, b\}$ is MDS if and only if the polynomial $(x^b - 1)/(x - 1) = x^{b-1} + \ldots + 1$ is injective on $\mathbb{F}_q \setminus \{0, 1\}$. This implies that the size of the image of this polynomial considered as a polynomial function over $\mathbb{F}_q$ is at least $q - 2$ which is larger than $q - (q-1)/(b-1)$. Hence, we deduce by Wan's Theorem [15] that $x^{b-1} + \ldots + 1$ is a permutation polynomial. A result of Matthews' [9] yields that $b = 2$ if q is odd.

Proposition 1. *For odd q, q-MDS exponent sets of size three are trivial. Equivalently, a cyclic code of block length $q-1$ and co-dimension three over $\mathbb{F}_q$ is MDS if and only if it is equivalent to a Reed-Solomon code.*

The above assertion does not hold for even q. For instance, the exponent set $\{0, 1, 8\}$ is not trivial but it is 32-MDS. To see the latter, note that the polynomial $(x^8 + 1)/(x + 1)$ is a permutation polynomial over $\mathbb{F}_{32}$, since the change of variable $y := x + 1$ transforms it into y^7. (Table 1 gives all values of b such that $(x^b + 1)/(x + 1)$ is a permutation polynomial over $\mathbb{F}_q$ for some small values of q.) Further, a small calculation shows that existence of a and b such that $\{0, 1, 8\} = \{a, a + b, a + 2b\}$ leads to a contradiction; hence the exponent set is nontrivial. (Details are left to the reader.) In general, MDS exponent sets of size three over finite fields of characteristic two correspond to certain ovals in finite Desarguesian planes of even order, for which a complete description has not yet appeared. (See [9, Section 4].)

In the next section we will derive similar assertions for other exponent sets of small size. The method is different from the one used in this section, as it

q	b
4	2
8	2, 4, 6
16	2, 8, 14
32	2, 4, 6, 8, 10, 16, 22, 24, 26, 28, 30
64	2, 32, 63
128	2, 4, 6, 8, 16, 20, 22, 32, 42, 52, 64, 76 86, 96, 106, 108, 112, 120, 122, 124, 126
256	2, 8, 32, 74, 128, 182, 224, 248, 254

Table1. Values of b such that $(x^b + 1)/(x + 1)$ is a permutation polynomial over $\mathbb{F}_q$.

employs techniques from the theory of finite geometries and some algebraic geometry.

3 Arcs and Normal Rational Curves

We denote the r-dimensional projective space over a field K by $\mathbb{P}^r(K)$. A point P with projective coordinates $x_0, \ldots, x_r$ is denoted by $P = (x_0 : \cdots : x_r)$. We start by introducing some definitions and recalling some basic facts about projective spaces over finite fields. A good reference for these subjects is Hirschfeld's book [4].

A **k-arc** in $\mathbb{P}^r(\mathbb{F}_q)$ is a set S of $k \geq r+1$ points such that no $r+1$ of them lie on a hyperplane. For any point in S we consider a representative in $\mathbb{F}_q^{r+1}$ and form the $(r+1) \times k$-matrix G_S whose columns are these points. Obviously S is an arc if and only if any $(r+1) \times (r+1)$-submatrix of G_S is invertible. (This condition is independent of the choice of the representatives for the points.) So, for $q \geq r+2$ the subset $S(\mathbb{F}_q^\times)$ of $\mathbb{P}^r(\mathbb{F}_q)$ consisting of the points $(1 : \alpha^{a_1} : \cdots : \alpha^{a_r})$, $\alpha \in \mathbb{F}_q^\times$, is a $(q-1)$-arc if and only if $\{0, a_1, \ldots, a_r\}$ is q-MDS.

A standard example of arcs is given by the set of points of a **normal rational curve**. A **rational curve** C_n of order n in $\mathbb{P}^r(\mathbb{F}_q)$ is the set of points $(g_0(t_0, t_1) : \cdots : g_r(t_0, t_1))$ where $t_0, t_1 \in \mathbb{F}_q$ and each g_i is a binary form of degree n and a highest common factor of $g_0, \ldots, g_r$ is 1. The curve C_n may also be written as the set of points $(f_0(t) : \cdots : f_n(t))$, where $f_i(t) := g_i(1, t)$, $t \in \mathbb{F}_q^+ := \mathbb{F}_q \cup \{\infty\}$, and $f_i(\infty)$ is by definition the coefficient of t^n in f_i. As the g_i have no nontrivial common factor, at least one f_i has degree n. The curve C_n is called **normal** if it is not a projection of a rational curve C'_n in $\mathbb{P}^{r+1}(\mathbb{F}_q)$, where C'_n is not contained in any r-dimensional hyperplane of $\mathbb{P}^{r+1}(\mathbb{F}_q)$. A **projective equivalence** in $\mathbb{P}^r(\mathbb{F}_q)$ is a self-mapping of $\mathbb{P}^r(\mathbb{F}_q)$ which associates to a point $(x_0 : \cdots : x_r)$ the point $(y_0 : \cdots : y_r)$ where

$$(y_0, \ldots, y_r)^\top = A \cdot (x_0, \ldots, x_r)^\top$$

for a nonsingular $(r+1) \times (r+1)$-matrix A. The basic facts about normal rational curves can be summarized as follows, see [5, Chapter 21].

Theorem 2. *Let C_n be a normal rational curve in $\mathbb{P}^r(\mathbb{F}_q)$ not contained in a hyperplane. Then*

(i) $q \geq r$;
(ii) $n = r$;
(iii) C_r *is projectively equivalent to*

$$\{(t^r, t^{r-1}, \ldots, t, 1) \mid t \in \mathbb{F}_q^+\};$$

(iv) C_r *consists of $q+1$ points no $r+1$ of which lie on a hyperplane.*
(v) *If $q \geq r+2$ then there is a unique C_r through any $r+3$ points of $\mathbb{P}^r(\mathbb{F}_q)$ no $r+1$ of which lie on a hyperplane.*

Much of the research on arcs has concentrated on the following three problems posed by B. Segre in 1955 [11]: (1) For given r and q what is the maximum value of k for which there exists a k-arc in $\mathbb{P}^r(\mathbb{F}_q)$? (2) For what values of r and q, with $q > r+1$, is every $(q+1)$-arc of $\mathbb{P}^r(\mathbb{F}_q)$ the point set of a normal rational curve? (3) For given r and $q > r+1$, what are the values of k for which every k-arc of $\mathbb{P}^r(\mathbb{F}_q)$ is contained in a normal rational curve of this space?

Theorem 3. (1) (Thas [14]) *For odd q every k-arc in $\mathbb{P}^r(\mathbb{F}_q)$ with $k > q - \sqrt{q}/4 + r - 7/16$ is contained in a unique normal rational curve of this space.*
(2) (Bruen et al. [1], Storme and Thas [13]) *For even $q \geq 4$ and $r \geq 4$ every k-arc of $\mathbb{P}^r(\mathbb{F}_q)$ with $k \geq q + r - \sqrt{q}/2 - 3/4$ is contained in a unique normal rational curve of this space.*

We remark that the the bound in Part (1) of the above theorem can be improved considerably if q is a prime, see [13].

Using the above results and the Bézout Inequality we will be able to prove that certain MDS exponent sets are essentially trivial. For the proof of the following lemma we assume familiarity with the concept of degree of an algebraic variety, see, e.g., [3, Lecture 18].

Lemma 4. *Let $a_1, \ldots, a_r$ be pairwise different positive integers, and K be an algebraically closed field. Suppose that $d := \gcd(a_1, \ldots, a_r)$ is not divisible by the characteristic of K. The Zariski-closure X of the image of the map $K \to K^r$, $t \mapsto (t^{a_1}, \ldots, t^{a_r})$ is a rational curve of degree A/d, where $A := \max_i a_i$.*

Proof. Obviously X is a rational curve. Further, as d is not divisible by the characteristic of K, X is the closure of the image of the map $t \mapsto (t^{a_1/d}, \ldots, t^{a_r/d})$. So we may suppose that $d = 1$. In addition, we may assume that $a_1 < a_1 < \cdots < a_r$. The degree of X is the maximum of the

numbers $|X \cap H|$, where H runs over all hyperplanes of $\mathbb{P}^r(K)$ such that $X \cap H$ is finite. (For this and other characterizations of degree see, e.g., [3, Lecture 18].) Let $x_0, \ldots, x_r$ be the coordinates of $\mathbb{P}^r(K)$, and let H be the zeroset of $\alpha_0 x_0 + \ldots + \alpha_r x_r$. Then

$$X \cap H = \left\{ (1 \colon \tau^{a_1} \colon \cdots \colon \tau^{a_r}) \;\middle|\; \alpha_0 + \sum_{i=1}^{r} \alpha_i \tau^{a_i} = 0 \right\}.$$

In particular, $|X \cap H| \leq a_r$. We thus need to show that there is some H such that $|X \cap H| = a_r$. Suppose first that $\gcd(\operatorname{char} K, a_r) = 1$, and let H be the zeroset of $x_0 - x_r$. Then $X \cap H$ consists of the points $(1 \colon \zeta^{a_1} \colon \cdots \colon \zeta^{a_r})$, where ζ runs over all the a_rth roots of unity. These points are all different, as $\gcd(a_1, \ldots, a_r) = 1$, so $|X \cap H| = a_r$. Suppose now that $\gcd(\operatorname{char} K, a_r) \neq 1$. Then there is some a_i such that $\operatorname{char} K$ does not divide a_i. The polynomial $X^{a_r} + X^{a_i} + 1$ has $\ell := a_r$ different roots $\tau_1, \ldots, \tau_\ell$ in K, as it is relatively prime to its derivative. Since $\gcd(a_1, \ldots, a_r) = 1$, each of these roots gives rise to a different point $(1 \colon \tau_i^{a_1} \colon \cdots \colon \tau_i^{a_r})$ in $X \cap H$, where H is the zeroset of $x_0 + x_i + x_r$. □

The main theorem of this section is now as follows.

Theorem 5. *Let $I := \{0, a_1, \ldots, a_r\}$ be q-MDS, where the a_i are pairwise different positive integers, and suppose that a_1 divides $q-1$. Further, suppose that $r(\max_i a_i) < q - 1$. If $r < \sqrt{q}/4 + 9/16$ and q is odd, then $I = \{0, 1, 2, \ldots, r\}$. If $4 \leq r \leq \sqrt{q}/2 - 1/4$ and $q \geq 4$ is even, then $I = \{0, 1, 2, \ldots, r\}$.*

Proof. We may suppose that $r \geq 1$. Let $d := \gcd(a_1, \ldots, a_r)$. By assumption, the cyclic code over $\mathbb{F}_q$ with the zeroset $\{1, \omega^{a_1}, \ldots, \omega^{a_r}\}$ is MDS, hence has minimum distance $r + 2$. But this is not possible if $d \neq 1$, as this code contains the codeword $x^{(q-1)/d} - 1$ of weight $2 < r + 2$. So $d = 1$. Further, $S := \{(1 \colon \alpha^{a_1} \colon \cdots \colon \alpha^{a_r}) \mid \alpha \in \mathbb{F}_q^\times\}$ is a $(q-1)$-arc. By Theorem 3 we deduce that S is contained in a normal rational curve C_r of $\mathbb{P}^r(\mathbb{F}_q)$. On the other hand, S is contained in the set of $\mathbb{F}_q$-rational points of the curve $X := \{(1 \colon t^{a_1} \colon \cdots \colon t^{a_r}) \mid t \in K^+\}$, K being the algebraic closure of $\mathbb{F}_q$. By the Bézout Inequality and the last lemma we have $\deg(X \cap C_r) \leq r(\max_i a_i) < q - 1$, hence $X = C_r$, as C_r is irreducible. We thus obtain $\max_i a_i = r$, which gives $I = \{0, 1, \ldots, r\}$. □

4 The Special Exponent Set $\{0, 1, \ldots, r-1, m\}$

Consider a cyclic code with exponent set $\{0, 1, \ldots, r-1, m\}$. Its minimum distance is at least $r + 1$ since it is contained in a Reed-Solomon code of dimension $n - r$. Hence, if the code is not MDS, then its minimum distance is $r + 1$. The result of Theorem 5 can be somewhat sharpened for this special exponent set in the following way.

Theorem 6. *Let r and m be positive integers satisfying $r \leq m \leq q-2$. Further, suppose that $r < \sqrt{q}/4 + 7/16$ if q is odd, and $4 \leq r \leq \sqrt{q}/2 + 3/4$ if $q \geq 4$ is even. Then $\{0, 1, \ldots, r-1, m\}$ is q-MDS if and only if $m = r$ or $m = q-2$.*

The if-part being clear, we continue with the only-if-part. Let

$$S_{r,m} := \{(1 : \alpha : \alpha^2 : \cdots : \alpha^{r-1} : \alpha^m) \mid \alpha \in \mathbb{F}_q^\times\}.$$

We need to show that under the above conditions on r the set $S_{r,m}$ is an arc if and only if $m = r$ or $m = q-2$. Obviously $S_{r,m}$ is an arc if and only if $\mathcal{K} = \mathcal{K}_{r,m} := S_{r,m} \cup \{P\}$ is, where $P = (0 : \cdots : 0 : 1)$. Suppose that $\mathcal{K}$ is an arc. Using Theorem 3 we deduce that $\mathcal{K}$ lies on a normal rational curve. For the rest of this section we concentrate on proving that $m = r$ or $m = q-2$, or, equivalently, that $\mathcal{K}$ does not lie on a normal rational curve if $r < m < q-2$. This would complete the proof of Theorem 6. To proceed with the proof, we need some notation and some auxiliary results.

Let C_r be a normal rational curve of $\mathbb{P}^r(\mathbb{F}_q)$ given by

$$C_r = \{(g_0(t_0, t_1) : \cdots : g_r(t_0, t_1)) \mid t_0, t_1 \in \mathbb{F}_q\}.$$

Let ∂_i denote the differential operator $\partial/\partial T_i$ of the bivariate polynomial ring $\mathbb{F}_q[T_0, T_1]$. The line ℓ_R through the points $R := (g_0(t_0, t_1) : \cdots : g_r(t_0, t_1))$ and $(\partial_0 g_0(t_0, t_1) : \cdots : \partial_0 g_r(t_0, t_1))$ is called **the tangent line** to C_r at R. Let $x_0, \ldots, x_r$ be the coordinates of $\mathbb{P}^r(\mathbb{F}_q)$ and let $\mathbb{P}^{r-1}(\mathbb{F}_q) = \Pi$ be the hyperplane given by $x_r = 0$. The projection of C_r from P onto Π together with the point $R^* := \ell_R \cap \Pi$ is a normal rational curve C_r^* of $\mathbb{P}^{r-1}(\mathbb{F}_q)$, see [6, Lemma 7]. Now let C_r be a normal rational curve containing $\mathcal{K}$. Then $C_r^* = \{(1 : t : \cdots : t^{r-1} : 0) \mid t \in \mathbb{F}_q^+\}$, since the projection of $\mathcal{K}$ is clearly contained in C_r^* and this normal rational curve of Π is uniquely determined by $r + 2 < q$ of its point by Theorem 2, Part (v).

Proposition 7. *Let C be a normal rational curve of $\mathbb{P}^r(\mathbb{F}_q)$ containing $P = (0 : \cdots : 0 : 1)$. Suppose that the projection of C from P onto Π is the curve $C^* = \{(1 : t : \cdots : t^{r-1} : 0) \mid t \in \mathbb{F}_q^+\}$. Then C is one of the following curves:*

- (Type ∞) $C = \{(1 : t : t^2 : \cdots : t^{r-1} : \mu(t)) \mid t \in \mathbb{F}_q^+\}$ *for some* $\mu \in \mathbb{F}_q[X]$ *with* $\deg(\mu) = r$.
- (Type β, $\beta \in \mathbb{F}_q$) $C = \{(t : t(t+\beta) : \cdots : t(t+\beta)^{r-1} : \eta(t)) \mid t \in \mathbb{F}_q^+\}$ *for some* $\eta \in \mathbb{F}_q[X]$ *with* $\deg(\eta) \leq r$ *and* $\eta(0) \neq 0$.

Moreover, C is of type γ, $\gamma \in \mathbb{F}_q^+$, if and only if the tangent line to C at P intersects C^* at the point corresponding to $t = \gamma$.

Proof. Suppose that the tangent line to C at P intersects C^* in the point $(0 : \cdots : 0 : 1 : 0)$. For every $t \in \mathbb{F}_q$ there exists $\tau \in \mathbb{F}_q$ such that $(1 : t : \cdots : t^{r-1} : \tau) \in C$. Hence, $C = \{(1 : t : t^2 : \cdots : t^{r-1} : \mu(t)) \mid t \in$

$\mathbb{F}_q\} \cup \{P\}$, where μ is a polynomial of degree $\leq q-1$. As C is an arc, $\deg(\mu) \geq r$. Hence, $C = \{(1\colon t\colon t^2\colon \cdots\colon t^{r-1}\colon \mu(t)) \mid t \in \mathbb{F}_q^+\}$. Since C is normal, $\deg(\mu) = r$.

Suppose now that the tangent line to C at P intersects C^* at the point $(1\colon \beta\colon \beta^2\colon \cdots\colon \beta^{r-1}\colon 0)$, for some $\beta \in \mathbb{F}_q$. Notice that

$$C^* = \{(\tau^{r-1}\colon (1+\beta\tau)\tau^{r-2}\colon (1+\beta\tau)^2\tau^{r-3}\colon \cdots\colon (1+\beta\tau)^{r-1}\colon 0) \mid \tau \in \mathbb{F}_q^+\}.$$

The tangent line at P intersects C^* in the point corresponding to $\tau = \infty$. Hence,

$$C = \{(\tau^{r-1}\colon (1+\beta\tau)\tau^{r-2}\colon \cdots\colon (1+\beta\tau)^{r-1}\colon \mu(\tau)) \mid \tau \in \mathbb{F}_q\} \cup \{P\},$$

for some polynomial $\mu \in \mathbb{F}_q[X]$. As before, we obtain $\deg(\mu) = r$, and hence $C = \{(\tau\colon (1+\beta\tau)\tau^{r-2}\colon \cdots\colon (1+\beta\tau)^{r-1}\colon \mu(\tau)) \mid \tau \in \mathbb{F}_q^+\}$. Thus

$$\begin{aligned} C &= \left\{ \left(\frac{1}{t^{r-1}}\colon \frac{1+\beta/t}{t^{r-2}}\colon \cdots\colon (1+\beta/t)^{r-1}\colon \mu(1/t)\right) \;\middle|\; t \in \mathbb{F}_q^\times \right\} \\ &\quad \cup \{P\} \cup \{(0\colon 0\colon \cdots\colon 1\colon \mu(0))\} \\ &= \left\{ (t\colon (t+\beta)t\colon \cdots\colon (t+\beta)^{r-1}t\colon t^r\mu(1/t)) \;\middle|\; t \in \mathbb{F}_q^\times \right\} \\ &\quad \cup \{P\} \cup \{(0\colon 0\colon \cdots\colon 1\colon \mu(0))\} \\ &= \left\{ (t\colon (t+\beta)t\colon \cdots\colon (t+\beta)^{r-1}t\colon \eta(t)) \;\middle|\; t \in \mathbb{F}_q^+ \right\}, \end{aligned}$$

where $\eta(X) = X^r\mu(1/X)$ is the reversal of μ. Note that $\eta(0) \neq 0$ as $\deg(\mu) = r$, and that $\deg(\eta) \leq r$. □

The last step in the proof of Theorem 6 is the following result.

Proposition 8. *Suppose that $r < m < q-2$. Then the set $\mathcal{K}_{r,m}$ does not lie on a normal rational curve.*

Proof. Suppose that $\mathcal{K} = \mathcal{K}_{r,m}$ lies on a normal rational curve C. By Proposition 7, C is of type γ for some $\gamma \in \mathbb{F}_q^+$.

Assume first that $\gamma = \infty$. Then there exists a polynomial μ of degree r over $\mathbb{F}_q$ such that $C = \{(1\colon t\colon \cdots\colon t^{r-1}\colon \mu(t)) \mid t \in \mathbb{F}_q^+\}$. As $\mathcal{K}$ lies on C, we deduce that the polynomial $X^m - \mu(X)$ has $q-1$ different roots over $\mathbb{F}_q$, hence is zero. But this implies that $X^m = \mu(X)$, hence $m = r$, a contradiction.

Suppose now that $\gamma = \beta$. Then there exists a polynomial η over $\mathbb{F}_q$ of degree $\leq r$, and for all $\tau \in \mathbb{F}_q^\times$ there exists $t \in \mathbb{F}_q^\times$ such that

$$(1\colon \tau\colon \cdots\colon \tau^{r-1}\colon \tau^m) = (1\colon (t+\beta)\colon \cdots\colon (t+\beta)^{r-1}\colon \eta(t)/t).$$

Hence, $\tau = t+\beta$ and $(t+\beta)^m = \eta(t)/t$ for all $t \in \mathbb{F}_q^\times$. Thus, the polynomial $X(X+\beta)^m - \eta(X)$ has $q-1$ zeros in $\mathbb{F}_q$. Since $\deg(\eta) \leq r < m$, this polynomial is not zero, and is of degree $m+1$. Hence, $m+1 \geq q-1$, which is a contradiction to $m < q-2$. This proves the proposition and completes the proof of Theorem 6. □

5 Complete q-Arcs over $\mathbb{F}_q$, q Even

In this section we will prove that the set

$$K_q := \{(1\colon \alpha\colon \cdots\colon \alpha^{q-5}\colon \alpha^{q-3}) \mid \alpha \in \mathbb{F}_q^+ \setminus \{0\}\}$$

is a **complete** q-arc in $\mathbb{P}^{q-4}(\mathbb{F}_q)$, i.e., it is a q-arc which cannot be extended to a $q+1$-arc. We remark that Storme and Thas [12] have determined all values for k for which there exists a complete k-arc in $\mathbb{P}^r(\mathbb{F}_q)$, $q-2 \geq r > q-\sqrt{q}-11/4$.

The exponent set corresponding to this arc is $\{0,1,\ldots,q-5,q-3\}$ which turns out to be the set $\{2j+1 \mid j=0,\ldots,q-3\}$ which is clearly trivial. Hence, the corresponding set of $(q-1)$ points in the projective space lies on a normal rational curve. However, the particular one-point extension of this set given by K_q does not lie on a normal rational curve even though it is an arc.

Theorem 9. *For $q \geq 8$ a power of two the set K_q is a complete q-arc in $\mathbb{P}^{q-4}(\mathbb{F}_q)$.*

Proof. We first prove that $K := K_q$ is a q-arc. Let $P := (0\colon 0\colon \cdots\colon 0\colon 1)$. K is a q-arc iff $K' := K \setminus \{P\}$ is. Suppose that there exist pairwise different $\alpha_1,\ldots,\alpha_{q-3} \in \mathbb{F}_q^\times$ such that the corresponding points in K' lie on a hyperplane, i.e., such that the matrix $M := (\alpha_{ij})$, $\alpha_{ij} := \alpha_i^j$ for $i = 1,\ldots,q-3$, $j = 0,\ldots,q-5$, and $\alpha_{q-3,j} = \alpha_j^{q-3}$, is singular. Let V denote the Vandermonde matrix $V = (\alpha_i^j)$, $i = 1,\ldots,q-3$, $j = 0,\ldots,q-4$. Then $0 = \det M/\det V = \alpha_1 + \cdots + \alpha_{q-3}$, which is a contradiction, as the sum of all the elements of $\mathbb{F}_q$ is zero. Hence, K' and K are arcs.

Let us now show that K is complete. Suppose not, and assume that there is a point $\Gamma := (\gamma_0\colon \gamma_1\colon \cdots\colon \gamma_{q-5}\colon \gamma_{q-4})$ such that $K'' := K \cup \{\Gamma\}$ is a $(q+1)$-arc in $\mathbb{P}^{q-4}(\mathbb{F}_q)$. The dual of K'' is a $(q+1)$-arc in $\mathbb{P}^3(\mathbb{F}_q)$, which by a result of Casse and Glynn [2] is projectively equivalent to $\{P_t \mid t \in \mathbb{F}_q^+\}$, where $P_t := (1\colon t\colon t^\theta\colon tt^\theta)$, θ being an $\mathbb{F}_2$-automorphism of $\mathbb{F}_q$. Hence, there exists $j \in \{1,\ldots,q+1\}$ such that

$$\begin{pmatrix} 1 & 1 & \cdots 1 & \gamma_0 & 0 \\ \alpha_1 & \alpha_2 & \cdots \alpha_{q-1} & \gamma_1 & 0 \\ \vdots & \vdots & \ddots \vdots & \vdots & \vdots \\ \alpha_1^{q-5} & \alpha_2^{q-5} & \cdots \alpha_{q-1}^{q-5} & \gamma_{q-5} & 0 \\ \alpha_1^{q-3} & \alpha_2^{q-3} & \cdots \alpha_{q-1}^{q-3} & \gamma_{q-4} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1\ \beta_1 & \beta_1^\theta & \beta_1\beta_1^\theta \\ \vdots\ \vdots & \vdots & \vdots \\ 1\ \beta_{j-1} & \beta_{j-1}^\theta & \beta_{j-1}\beta_{j-1}^\theta \\ 0\ 0 & 0 & 1 \\ 1\ \beta_{j+1} & \beta_{j+1}^\theta & \beta_{j+1}\beta_{j+1}^\theta \\ \vdots\ \vdots & \vdots & \vdots \\ 1\ \beta_q & \beta_q^\theta & \beta_q\beta_q^\theta \\ 1\ \beta_j & \beta_j^\theta & \beta_j\beta_j^\theta \end{pmatrix} = 0^{(q-3)\times 4}, \tag{1}$$

where $\mathbb{F}_q = \{\alpha_1,\ldots,\alpha_{q-1},0\} = \{\beta_1,\ldots,\beta_q\}$. Considering the $(1,1)$-component of the product in (1) we see that $j \neq q$. Suppose that $j < q$.

Considering the $(1,1)$-component we see that $q-2+\gamma_0=0$, hence $\gamma_0=0$. Considering the $(1,2)$-component we obtain $\sum_{i<q, i\neq j}\beta_i=0$, which is a contradiction, since this yields $\beta_q+\beta_j=0$, i.e., $\beta_q=\beta_j$. Suppose now that $j=q+1$. Considering the $(j,1)$-component of (1), $j=1,\ldots,q-4$, we obtain $\sum_{i=1}^{q-1}\alpha_i^{j-1}+\gamma_{j-1}=0$, which yields $\gamma_0=1$, $\gamma_1=\cdots=\gamma_{q-5}=0$. Considering the $(q-3,1)$-component gives $\sum_{i=1}^{q-1}\alpha_i^{q-3}+\gamma_{q-4}=0$, hence $\gamma_{q-4}=0$. So, $\Gamma=(1\colon 0\colon \cdots\colon 0)$. But the following argument shows that $K\cup\{\Gamma\}$ is not an arc, and this gives us the desired contradiction: choose pairwise different $\alpha_1,\ldots,\alpha_{q-4}\in\mathbb{F}_q^\times$ which sum up to zero, and let V be the Vandermonde determinant of the α_i. Then

$$\det\begin{pmatrix} 1 & 1 & \cdots & 1 & 1\\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q-4} & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_1^{q-5} & \alpha_2^{q-5} & \cdots & \alpha_{q-4}^{q-5} & 0\\ \alpha_1^{q-3} & \alpha_2^{q-3} & \cdots & \alpha_{q-4}^{q-3} & 0 \end{pmatrix} = \Big(\sum_i \alpha_i\Big)\Big(\prod_i \alpha_i\Big)V = 0.$$

This completes the proof. □

6 Relationship to Modular Representations of $\mathrm{GL}_n(\mathbb{F}_q)$

In this section we are going to point out a somewhat unexpected relationship between the classification problem for certain cyclic MDS-codes and certain modular representations of the general linear group over a finite field.

For $m\geq r$ the exponent set $\{0,1,\ldots,r-1,m)$ is q-MDS if and only if the polynomial

$$\frac{\det\begin{pmatrix} X_0^0 & X_1^0 & \cdots & X_{r-1}^0 & X_r^0\\ X_0^1 & X_1^1 & \cdots & X_{r-1}^1 & X_r^1\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ X_0^{r-1} & X_1^{r-1} & \cdots & X_{r-1}^{r-1} & X_r^{r-1}\\ X_0^m & X_1^m & \cdots & X_{r-1}^m & X_r^m \end{pmatrix}}{\det\begin{pmatrix} X_0^0 & X_1^0 & \cdots & X_{r-1}^0 & X_r^0\\ X_0^1 & X_1^1 & \cdots & X_{r-1}^1 & X_r^1\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ X_0^{r-1} & X_1^{r-1} & \cdots & X_{r-1}^{r-1} & X_r^{r-1}\\ X_0^r & X_1^r & \cdots & X_{r-1}^r & X_r^r \end{pmatrix}} \tag{2}$$

does not have any roots outside $(\mathbb{F}_q^\times)^{r+1}\setminus\Delta$ where Δ is the zeroset of the discriminant (see Sect. 1). The above quotient is easily seen to be equal to the sum of all monomials in $r+1$ variables of degree $m-r$. This is a special case of a **Schur-function**. Such functions arise as characters of polynomial representations of GL_n over fields of characteristic 0. This classical result

has a certain analogue in our case: the special Schur function derived as the quotient of the determinants above appear as characters of certain modular representations of $\mathrm{GL}_{r+1}(\mathbb{F}_q)$.

To be more specific, let ρ denote the representation of $\mathrm{GL}_{r+1}(\mathbb{F}_q)$ given by the action of this group on the space of homogeneous $r+1$-variate polynomials of degree $m-r$, and let ϕ be the character of ρ. Suppose that $A \in \mathrm{GL}_{r+1}(\mathbb{F}_q)$ is a diagonal matrix with entries $\alpha_0, \ldots, \alpha_r$. It acts on the space of homogeneous $r+1$-variate polynomials of degree $m-r$ by sending a monomial $\mu = \mu(X_0, \ldots, X_r)$ into $\mu(\alpha_0, \ldots, \alpha_r)\mu$. Hence, the value of $\phi(A)$ is given by $S(\alpha_0, \ldots, \alpha_r)$ where S is the sum of all monomials of degree $m-r$ in $r+1$ variables. In other words, S is equal to the expression given in (2).

Proposition 10. *Assumptions and notation being as above, the exponent set* $\{0, 1, \ldots, r-1, m\}$ *is* q*-MDS if and only if the character* ϕ *has no zeros in the union of those conjugacy classes of* $\mathrm{GL}_{r+1}(\mathbb{F}_q)$ *which have* $r+1$ *different eigenvalues in* $\mathbb{F}_q$.

Proof. The assertion is essentially proved above. If the exponent set is q-MDS, then $S(\alpha_0, \ldots, \alpha_r)$ is nonzero for any setting of pairwise different nonzero α_i in $\mathbb{F}_q$. Hence, since S is the value of ϕ at the conjugacy class of the diagonal matrix having $\alpha_0, \ldots, \alpha_r$ as diagonal entries, the assertion follows. Conversely, if ϕ does not have a zero on the union of the given conjugacy classes, then $S(\alpha_0, \ldots, \alpha_r)$ is nonzero for any setting of pairwise different nonzero α_i in $\mathbb{F}_q$, which implies that the given exponent set is MDS. □

As of yet, we do not know of any methods in modular representation theory which would resolve the question of whether or not the exponent set $\{0, 1, \ldots, r-1, m\}$ is MDS.

References

1. A.A. Bruen, J.A. Thas, and A. Blokhius. On MDS codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre. *Invent. math.*, 92:441–459, 1988.
2. L.R.A. Casse and D.G. Glynn. The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$. *Geom. Ded.*, 13:157–163, 1982.
3. J. Harris. **Algebraic Geometry**. Number 133 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1992.
4. J.W.P. Hirschfeld. **Projective Geometries over Finite Fields**. Clarendon Press, Oxford, 1979.
5. J.W.P. Hirschfeld. **Finite Projective Spaces of Three Dimensions**. Clarendon Press, Oxford, 1985.
6. H. Kaneta and T. Maruta. An elementary proof and an extension of Thas' theorem on k-arcs. *Math. Proc. Camb. Phil. Soc.*, 105:459–462, 1989.
7. J.H. van Lint. **Introduction to Coding Theory**, volume 86 of *Graduate Texts in Mathematics*. Springer Verlag, third edition, 1998.

8. J.H. van Lint and R.M. Wilson. On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory*, 32:23–40, 1986.
9. R. Matthews. Permutation properties of the polynomials $1 + x + \ldots + x^k$ over a finite field. *Proc. Amer. Math. Soc.*, 120:47–51, 1994.
10. G.L. Mullen and P.Jau-Shyong Shiue (editors). **Finite Fields: Theory, Applications, and Algorithms**. American Mathematical Society, Providence, Rhode Island, 1994.
11. B. Segre. Curve razionali normali e k-archi negli spazi finite. *Ann. Mat. Pura Appl. IV*, 39:357–379, 1955.
12. L. Storme and J.A. Thas. Complete k-arcs in $PG(n, q)$, q even. *Disc. Math.*, 106/107:455–469, 1992.
13. L. Storme and J.A. Thas. MDS codes and arcs in $PG(n, q)$ with q even: an improvement on the bounds of Bruen, Thas, and Blokhius. *J. Comb. Theory, Series A*, 62:139–154, 1993.
14. J.A. Thas. Normal rational curves and k-arcs in Galois spaces. *Rend. Mat.*, (6)1:331–334, 1968.
15. D. Wan. A p-adic lifting lemma and its applications to permutation polynomials. In **Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communication and Computing**, volume 141 of *Lecture Notes in Pure and Appl. Math.*, pages 209–216. Marcel Dekker, New York, 1992.