INTERNATIONAL COMPUTER SCIENCE INSTITUTE

1947 Center St. • Suite 600 • Berkeley, California 94704-1198 • (510) 643-9153 • FAX (510) 643-7684

On Interpolating Polynomials over Finite Fields

M.A. Shokrollahi

TR-96-010

February 1996

Abstract

A set of monomials $x^{a_0}, \ldots, x^{a_r}$ is called interpolating with respect to a subset S of the finite field $\mathbb{F}_q$, if it has the property that given any pairwise different elements $x_0, \ldots, x_r$ in S and any set of elements $y_0, \ldots, y_r$ in $\mathbb{F}_q$ there are elements $c_0, \ldots, c_r$ in $\mathbb{F}_q$ such that $y_h = \sum_{j=0}^{r} c_j x_h^{a_j}$ for $0 \leq h \leq r$. In this paper we address the question of determining interpolating sets with respect to $S = \mathbb{F}_q$ and $S = \mathbb{F}_q^{\times}$. For q a prime and $S = \mathbb{F}_q$ this is a problem of N. Reingold and D. Spielman posed by A. Odlyzko in [10, p. 399]. We call the interpolating set $\{x^{a_0}, \ldots, x^{a_r}\}$ trivial if its exponent set coincides with $\{0, b, 2b, \ldots, rb\}$ mod $(q-1)$ for some b coprime to $q-1$. The question is whether all interpolating sets with respect to $\mathbb{F}_q$ are trivial.

We start by relating this to a problem on cyclic MDS codes. We then show that for $r = 2$ and $S = \mathbb{F}_q^{\times}$ the problem is equivalent to whether or not for some m the polynomial $(x^m - 1)/(x - 1)$ is a permutation polynomial over $\mathbb{F}_q$. The latter problem has been investigated by R. Matthews [9]. Using Bézout's Theorem and results on arcs in projective spaces, we show that in a certain range for r (depending on q and the maximum of the a_i) the only interpolating sets with respect to $\mathbb{F}_q^{\times}$ are trivial. We then proceed to sharpen this result for the special exponent set $0, 1, 2, \ldots, r-1, m$ where m satisfies $r \leq m \leq q-2$. Finally, we exhibit an example of a nontrivial interpolating set with respect to $\mathbb{F}_q^{\times}$ for even $q \geq 8$. In the language of finite geometries this is an example of a complete q-arc over $\mathbb{F}_q$, and in the language of coding theory this is an example of a cyclic MDS-code which is not equivalent to a generalized Reed-Solomon code.

1 Introduction

A set of monomials $x^{a_0}, \ldots, x^{a_r}$ is called interpolating with respect to a subset S of the finite field $\mathbb{F}_q$, if it has the property that given any pairwise different elements $x_0, \ldots, x_r$ in S and any set of elements $y_0, \ldots, y_r$ in $\mathbb{F}_q$ there are elements $c_0, \ldots, c_r$ in $\mathbb{F}_q$ such that $y_h = \sum_{j=0}^{r} c_j x_h^{a_j}$ for $0 \leq h \leq r$. In the sequel an "interpolating exponent set" denotes a set of pairwise different non-negative integers $a_0, \ldots, a_r$ smaller than q such that the corresponding set of monomials $x^{a_0}, \ldots, x^{a_r}$ is interpolating.

It is obvious that $\{a_0, \ldots, a_r\}$ is interpolating with respect to S if and only if every $(r+1) \times (r+1)$ submatrix of

$$G_S := (P_{\xi_1} | P_{\xi_2} | \cdots | P_{\xi_s}) \tag{1}$$

is nonsingular, where $\xi_1, \ldots, \xi_s$ are the elements of S and $P_\xi := (\xi^{a_0}, \ldots, \xi^{a_r})^\mathsf{T}$. This is equivalent to the statement that the polynomial

$$\det(X_h^{j a_h})_{0 \leq h,j \leq r} \in \mathbb{F}_q[X_0, \ldots, X_r]$$

has no zeros in $S^{r+1} \setminus \Delta$, where $\Delta \subset \mathbb{F}_q^{r+1}$ is the diagonal embedding of $\mathbb{F}_q$. It follows that all exponent sets of the form $\{0, b, 2b, \ldots, rb\}$ mod $(q-1)$, for some b coprime to $q-1$, are interpolating. Indeed, for these sets the above determinant is essentially Vandermonde. In the sequel we call these sets "trivial." A problem of Nick Reingold and Dan Spielman posed by Andrew Odlyzko in [10, p. 399] asks whether for q a prime all interpolating sets with respect to $\mathbb{F}_q$ are trivial. In this paper we investigate this problem for general prime powers q.

We start our investigation in the next section by relating interpolating exponent sets with respect to $\mathbb{F}_q$ to such sets with respect to $\mathbb{F}_q^\times$. For the rest of the paper we will then solely concentrate on the latter. Such sets have a coding theoretic interpretation as they give rise to cyclic MDS codes and vice versa.

In Section 3 we concentrate on exponent sets of size three. We show that these sets are interpolating 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]. Using his results, we show that for odd q interpolating exponent sets of size three are trivial. In Section 4 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 interpolating iff they are trivial. Section 5 deals with the special exponent set $\{0, 1, \ldots, r-1, m\}$ for some m satisfying $r \leq m \leq q-2$. We show that if r is not large compared to q, then these exponent sets are not interpolating. For large r there are examples of nontrivial interpolating sets. This will be the topic of the last section. These interpolating sets give rise to cyclic MDS-codes which are not equivalent to Reed-Solomon codes, and to complete q-arcs.

2 Interpolating Sets and Cyclic MDS-Codes

An exponent set $\{a_0, \ldots, a_r\}$ is not interpolating with respect to $\mathbb{F}_q$ if all the a_i are positive. (Otherwise the matrix $G_{\mathbb{F}_q}$ would contain a zero column.) We may therefore assume that $a_0 = 0$.

The condition of being an exponent set with respect to $\mathbb{F}_q^\times$ is related to the corresponding condition with respect to $\mathbb{F}_q$ in the following way:

Lemma 1. *$\{0, a_1, \ldots, a_r\}$ is an interpolating exponent set with respect to $\mathbb{F}_q$ if and only if $\{0, a_1, \ldots, a_r\}$ and $\{a_1, \ldots, a_r\}$ are interpolating exponent sets with respect to $\mathbb{F}_q^\times$.*

PROOF. Suppose that $\{0, a_1, \ldots, a_r\}$ is an interpolating exponent set with respect to $\mathbb{F}_q$. Then this set is clearly also an interpolating exponent set with respect to $\mathbb{F}_q^\times$. Furthermore, every $(r+1)\times(r+1)$-submatrix of the matrix $G_{\mathbb{F}_q}$ defined in (1) is nonsingular. In particular, any submatrix of the form $(P_0 \mid H)$ is nonsingular, where H is a $(r+1)\times r$-submatrix of $G_{\mathbb{F}_q^\times}$. The determinant of this matrix equals that of the matrix obtained by deleting the first row of H. But the latter matrix is of the form $(Q_{\eta_1}|\cdots|Q_{\eta_r})$, where $Q_\eta := (\eta^{a_1}|\cdots|\eta^{a_r})$ and η_i are nonzero elements of $\mathbb{F}_q$. It follows that $\{a_1, \ldots, a_r\}$ is an interpolating exponent with respect to $\mathbb{F}_q^\times$. The argument is reversible. □

One advantage of working with interpolating sets with respect to $\mathbb{F}_q^\times$ is their connection with cyclic MDS-codes. In what follows we assume familiarity with the theory of linear error correcting codes, and in particular with the theory of linear cyclic codes. Good references for these topics are Mac Williams and Sloane [8] and van Lint [7]. Recall that a cyclic code of block-length $q-1$ over $\mathbb{F}_q$ is specified by a set of "zeros" $\{\omega^{a_0}, \omega^{a_1}, \ldots, \omega^{a_r}\}$, where the a_i are pairwise different non-negative integers less than $q-1$, and ω is a generator of $\mathbb{F}_q^\times$. The code C is defined as the set of all polynomials f of degree less than $q-1$ such that $f(\omega^{a_j}) = 0$ for all $j = 0, \ldots, r$. We will usually identify elements of C with their $(q-1)$-dimensional vectors of coefficients. C is called MDS (Maximum Distance Separable) if its minimum distance attains the greatest possible value $r+2$. Note that the matrix $G_{\mathbb{F}_q^\times}$ is a parity check matrix for C. Hence, we have the following.

Proposition 2. *$\{a_0, \ldots, a_r\}$ is interpolating with respect to $\mathbb{F}_q^\times$ if and only if the cyclic code with the set of zeros $\{\omega^{a_0}, \ldots, \omega^{a_r}\}$ is MDS.*

It is easily seen that if $\{a_0, \ldots, a_r\}$ is interpolating with respect to $\mathbb{F}_q^\times$, then so is $\{ba_0 + c, \ldots, ba_r + c\}$ for all b coprime to $q-1$ and all c. (All arithmetics is modulo $q-1$.) In other words, if Γ denotes the group of invertible upper triangular 2×2-matrices over $\mathbb{Z}/(q-1)\mathbb{Z}$, then the property of being interpolating is preserved under the action of Γ on the elements of $\mathbb{Z}/(q-1)\mathbb{Z}$, where the action of $\left(\begin{smallmatrix}\alpha & \beta\\ 0 & \gamma\end{smallmatrix}\right)$ on a is given by $(\alpha a + \beta)/\gamma$. We thus call (interpolating) exponent sets in the Γ-orbit of $\{0, 1, \ldots, r\}$ *essentially trivial.* Note that trivial sets are essentially trivial, but not vice versa.

3 Small Exponent Sets

Exponent sets if size two are easy to handle: obviously, $\{0, a\}$ is interpolating with respect to $\mathbb{F}_q$ iff $\gcd(a, q-1) = 1$ and $\{a, b\}$ is interpolating with respect to $\mathbb{F}_q^\times$ iff $\gcd(a-b, q-1) = 1$.

Exponent sets of size three are 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 $a \le d := \gcd(b, q-1)$. I is interpolating with respect to $\mathbb{F}_q^\times$ 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 interpolating. 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 interpolating. 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 interpolating 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 3. *For odd q exponent sets of size three with respect to $\mathbb{F}_q$ ($\mathbb{F}_q^\times$) are trivial (essentially 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. An easy example is the nontrivial exponent set $\{0, 1, 4\}$ which can be proved to be interpolating with respect to $\mathbb{F}_8$. In general, interpolating 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 employs techniques from the theory of finite geometries and some algebraic geometry.

4 Arcs and Normal Rational Curves

For the rest of this paper 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.) Hence, 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 an interpolating exponent set with respect to $\mathbb{F}_q^\times$.

A standard example of arcs is given by the set of points of a so-called 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, so at least one f_i has degree n. The curve C_n is called normal if it is not a projection of 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

$$(y_0, \ldots, y_r)^\mathsf{T} = A \cdot (x_0, \ldots, x_r)^\mathsf{T}$$

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 4. *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 5. (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 [12]) *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.*

Except for the last section, we will in the following solely consider the case of odd q, as that of even q can be handled similarly. We remark that the the bound in Part (1) of the above theorem can be improved considerably of q is a prime, see [12].

Using the above results and the Bézout Inequality we will be able to prove that certain interpolating 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 6. *Let $a_1, \ldots, a_r$ be pairwise different positive integers, and K be an algebraically closed field. 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 $A := \max_i a_i$ and $d = \gcd(a_1, \ldots, a_r)$.*

PROOF. Obviously X is a rational curve. Further, it 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

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

In particular, $|X \cap H| \le a_r$. We thus need to show that there is some H such that $|X \cap H| = a_r$. Suppose first that $\gcd(\mathrm{char}\, K, a_r) = 1$, and let H be the zeroset of $x_0 - x_r$. Then $X \cap H$ consists of the points $(1 : \zeta^{a_1} : \cdots : \zeta^{a_r})$, 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 $\gcd(\mathrm{char}\, K, a_r) \ne 1$. Then there is some a_i such that $\gcd(\mathrm{char}\, K, a_i) = 1$. 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 $(1 : \tau_i^{a_1} : \cdots : \tau_i^{a_r})$ 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 7. *Let $I := \{0, a_1, \ldots, a_r\}$ be interpolating with respect to $\mathbb{F}_q^\times$, where q is odd, and suppose that a_1 divides $q - 1$. If $r(\max_i a_i) < q - 1$ and $r < \sqrt{q}/4 + 23/16$, then $I = \{0, 1, 2, \ldots, r\}$.*

PROOF. We may suppose that $r \ge 1$. Let $d := \gcd(a_1, \ldots, a_r)$. Since I is interpolating, 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 $d \ne 1$, as this code contains the codeword $x^{(q-1)/d} - 1$ of weight $2 < r + 2$. So $d = 1$. Further, since I is interpolating, $S := \{(1 : \alpha^{a_1} : \cdots : \alpha^{a_r}) \mid \alpha \in \mathbb{F}_q^\times\}$ is a $(q-1)$-arc. By Part (1) of Theorem 5 and the condition on r 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 $X := \{(1 : t^{a_1} : \cdots : t^{a_r}) \mid t \in K^+\}$, K being the algebraic closure of $\mathbb{F}_q$. By the Bézout Inequality and the last lemma we have $\deg(X \cap C_r) \le r(\max_i a_i) < q - 1$, hence $X = C_r$, as C_r is irreducible. We thus obtain $\max_i a_i = r$, which gives $I = \{0, 1, \ldots, r\}$. □

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

The result of Theorem 7 can be sharpened for the special exponent set $\{0, 1, \ldots, r-1, m\}$ in the following way.

Theorem 8. *Let r be a positive integer less than $\sqrt{q}/4 + 7/16$, and let $r \le m \le q - 2$. Then $\{0, 1, \ldots, r-1, m\}$ is interpolating with respect to $\mathbb{F}_q^\times$, q odd, iff $m = r$ or $m = q - 2$.*

The if-part being clear, we concentrate on 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 iff $m = r$ or $m = q-2$. Obviously $S_{r,m}$ is an arc iff $\mathcal{K} = \mathcal{K}_{r,m} := S_{r,m} \cup \{P\}$ is, where $P = (0: \cdots : 0: 1)$. Below we will show that $\mathcal{K}$ lies on a normal rational curve iff $m = r$ or $m = q-2$. We then use Theorem 5, Part (1), to deduce that if $r < \sqrt{q}/4 + 7/16$, then $\mathcal{K}$ lies on a normal rational curve, i.e., $m = r$ or $m = q-2$.

For the rest of this section we thus concentrate on showing that $\mathcal{K}_{r,m}$ does not lie on a normal rational curve if $r < m < q-2$. For this 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 $\partial_0(g_0(t_0,t_1): \cdots : g_r(t_0,t_1))$ 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 4, Part (v).

Proposition 9. *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* $\deg(\eta) \le r$ *and* $\eta(0) \neq 0$.

Moreover, C is of type γ, $\gamma \in \mathbb{F}_q^+$, iff 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 $\le q-1$. As C is an arc, $\deg(\mu) \ge r$. Hence, $C = \{(1: t: t^2: \cdots : t^{r-1}: \mu(t)) \mid t \in \mathbb{F}_q^+\}$. Since C is normal, $\deg(\mu) = r$.

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

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

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

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

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

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

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 8 is the following result.

Proposition 10. *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 9, C is of type γ for some $\gamma \in \mathbb{F}_q^+$.

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

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

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 $m < q-2$. □

6 Nontrivial Interpolating Exponent Sets for $\mathbb{F}_q^\times$, q Even

In this section we will prove that for even $q \geq 8$ the exponent set $\{0, 1, \ldots, q-5, q-3\}$ is interpolating with respect to $\mathbb{F}_q^\times$. This also shows that the cyclic code with set of roots $\{1, \omega, \ldots, \omega^{q-5}, \omega^{q-3}\}$, ω a generator of $\mathbb{F}_q^\times$, is MDS even though it is not equivalent to a Reed-Solomon code. More strongly, we will prove that the set

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

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 [13] have determined all values for k for which there exists a complete k-arc in $\mathbb{P}^r(\mathbb{F}_q)$, $q-2 \geq r > q - \sqrt{q} - 11/4$.

Theorem 11. *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 $P := (0{:}\,0{:}\,\cdots{:}\,0{:}\,1)$. 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 $\Gamma := (\gamma_0{:}\,\gamma_1{:}\,\cdots{:}\,\gamma_{q-5}{:}\,\gamma_{q-4})$ 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 $P_t := (1{:}\,t{:}\,t^\theta{:}\,tt^\theta)$, θ being an $\mathbb{F}_2$-automorphism of $\mathbb{F}_q$. Hence, there exists $j \in \{1, \ldots, q+1\}$ such that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & \gamma_0 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q-1} & \gamma_1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_1^{q-5} & \alpha_2^{q-5} & \cdots & \alpha_{q-1}^{q-5} & \gamma_{q-5} & 0 \\ \alpha_1^{q-3} & \alpha_2^{q-3} & \cdots & \alpha_{q-1}^{q-3} & \gamma_{q-4} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta_1 & \beta_1^\theta & \beta_1\beta_1^\theta \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_{j-1} & \beta_{j-1}^\theta & \beta_{j-1}\beta_{j-1}^\theta \\ 0 & 0 & 0 & 1 \\ 1 & \beta_{j+1} & \beta_{j+1}^\theta & \beta_{j+1}\beta_{j+1}^\theta \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_q & \beta_q^\theta & \beta_q\beta_q^\theta \\ 1 & \beta_j & \beta_j^\theta & \beta_j\beta_j^\theta \end{pmatrix} = 0^{(q-3)\times 4}, \quad (2)$$

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 (2) 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 (2), $j = 1, \ldots, q-4$, 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, $\Gamma = (1{:}\,0{:}\,\cdots{:}\,0)$. 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. □

7 Acknowledgments

Many thanks go to E.F. Assmus, D. Spielman, and M. Zieve for pointing out to me the references [13], [10], and [9], respectively.

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.* GTM #133, 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.* GTM #86, Springer Verlag, New York, 1982.

[8] F.J. Mac Williams and N.J.A. Sloane: *The Theory of Error Correcting Codes.* North Holland, Amsterdam, 1993.

[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, Ser. **39**, 357–379, 1955.

[12] 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.

[13] L. Storme and J.A. Thas: Complete k-arcs in $PG(n,q)$, q even. *Disc. Math.*, **106/107**, 455–469, 1992.

[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. *Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communication and Computing,* Lecture Notes in Pure and Appl. Math., vol. 141, Marcel Dekker, New York, 1992, pp. 209–216.