Rational points on complete symmetric hypersurfaces over finite fields

Jun Zhang* Daqing Wan †

Abstract

For any affine hypersurface defined by a complete symmetric polynomial in $k \geq 3$ variables of degree m over the finite field $\mathbb{F}_q$ of q elements, a special case of our theorem says that this hypersurface has many, at least $6q^{k-3}$, rational points over $\mathbb{F}_q$ if $1 \leq m \leq q-3$ and q is odd. This result is proved using Segre's classical theorem on ovals in finite projective planes.

1 Introdution

Let $\mathbb{F}_q$ denote the finite field of q elements with characteristic p. The study of $\mathbb{F}_q$-rational points on a hypersurface defined by a symmetric polynomial over $\mathbb{F}_q$ has many important applications. The classical three classes of symmetric polynomials introduced by Newton are power sum symmetric polynomials (Fermat hypersurfaces), elementary symmetric polynomials and complete symmetric polynomials. In this paper, motivated by applications in coding theory, we investigate the class of complete symmetric polynomials as defined below.

Definition 1.1. *The homogeneous complete symmetric polynomial of degree m in the k-variables $\{x_1, x_2, \cdots, x_k\}$ is defined by*

$$h_m(x_1, x_2, \cdots, x_k) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_m \leq k} x_{i_1} x_{i_2} \cdots x_{i_m} = \sum_{j_1 + \cdots + j_k = m, j_i \geq 0} x_1^{j_1} \cdots x_k^{j_k}.$$

By definition, we have $h_0(x_1, x_2, \cdots, x_k) = 1$,

$$h_1(x_1, x_2, \cdots, x_k) = x_1 + x_2 + \cdots + x_k,$$

$$h_2(x_1, x_2, \cdots, x_k) = \sum_{i=1}^{k} x_i^2 + \sum_{1 \leq i < j \leq k} x_i x_j,$$

*Jun Zhang, School of Mathematical Sciences, Capital Normal University, Beijing 100048, P.R. China. The research of Jun Zhang was supported by the National Natural Science Foundation of China under Grant No. 11971321 and No. 11601350. E-mail: junz@cnu.edu.cn

†Daqing Wan is with the Department of Mathematics, University of California, Irvine, CA 92697, USA. Email: dwan@math.uci.edu

etc. Just like the elementary symmetric polynomials, the complete symmetric polynomials $h_m(x_1, ..., x_k)$ $(0 \leq m \leq k)$ generate the ring of all symmetric polynomials in k variables over $\mathbb{Z}$. In characteristic zero, the projective hypersurface defined by $h_m(x_1, ..., x_k) = 0$ is smooth for all $k \geq 2$. In characteristic $p > 0$, the singular locus (even its size) of the projective hypersurface defined by $h_m(x_1, ..., x_k) = 0$ is unknown.

Definition 1.2. *A general complete symmetric polynomial of degree m over $\mathbb{F}_q$ in the k-variables $\{x_1, x_2, \cdots, x_k\}$ is defined as*

$$h(x_1, ..., x_k) := \sum_{e=0}^{m} a_e h_e(x_1, x_2, \cdots, x_k) = \sum_{e=0}^{m} a_e \sum_{j_1+j_2+\cdots+j_k=e, j_i \geq 0} x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k},$$

where $a_e \in \mathbb{F}_q$ and $a_m \neq 0$. Thus, a complete symmetric polynomial in k variables is simply a linear combination of the homogeneous complete symmetric polynomials in k-variables.

Thus, a complete symmetric polynomial $h(x_1, ..., x_k)$ is simply a polynomial in k variables where all terms of the same total degree have the same coefficients. We stress that such polynomials are not homogenous in general. We are interested in the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined by a complete symmetric polynomial $h(x_1, ..., x_k)$ over $\mathbb{F}_q$. As noted above, the singular locus (even its size) of the affine hypersurface defined by $h(x_1, ..., x_n) = 0$ can be quite complicated, especially in characteristic p.

Definition 1.3. *Let $h(x_1, ..., x_k)$ be a complete symmetric polynomial of degree m in k-variables over $\mathbb{F}_q$. Let*

$$N_q(h) := \#\{(x_1, ..., x_k) \in \mathbb{F}_q^k | h(x_1, ..., x_k) = 0\},$$

denote the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined by $h(x_1, ..., x_k) = 0$.

Our basic problem is to study when $N_q(h) > 0$ and to give a good lower bound when it is positive. The problem is trivial if $m = 0$ and thus h is a constant. We shall assume that $m > 0$ and so h is not a constant. A consequence of our main result is the following

Theorem 1.4. *Let $h(x_1, ..., x_k)$ be a complete symmetric polynomial in $k \geq 3$ variables over $\mathbb{F}_q$ of degree m with $1 \leq m \leq q - 3$. If q is odd, then*

$$N_q(h) \geq 6q^{k-3}.$$

Remarks. A classical result of Warning [11] implies that if $N_q(h) > 0$, then $N_q(h) \geq q^{k-m}$, which is apparently weaker than $6q^{k-3}$ if $m \geq 3$, and trivial if $k \leq m$. The condition $N_q(h) > 0$ itself is highly non-trivial to check unless h has no constant term. If one applies Deligne's theorem on the Weil conjecture, even in the sufficiently smooth case (the size of singular locus is already unknown),

one would need to assume that the degree m is small compared to q in order to prove a non-trivial lower bound for $N_q(h)$. One would at least need something like $m = O(q^{\frac{1}{2}-\epsilon_k})$, where ϵ_k is a positive constant depending on k. If $k > m$, the classical Chevally-Warning-Ax-Katz type theorem implies $N_q(h)$ is divisible by $q^{\lceil \frac{k-m}{m} \rceil}$, see [10] for simple proofs of various such divisibility results. Again, one needs to assume $N_q(h) > 0$ and $k > m$ in order to derive a non-trivial lower bound for $N_q(h)$. The above theorem has several new features. It does not assume that the degree m is small compared to q. It does not assume that $N_q(h) > 0$. The lower bound $6q^{k-3}$ works for all degree $1 \leq m \leq q-3$. When $m \geq q-2$, the problem becomes more complicated as m grows. But as we shall see, a stronger version of the problem (with distinct coordinate rational points) in the large degree m case can be reduced to the smaller degree $m < q$ case.

We note that the condition $k \geq 3$ in the theorem cannot be dropped. For instance, if $k = 2$, one checks that

$$h_m(x_1, x_2) = \frac{x_1^{m+1} - x_2^{m+1}}{x_1 - x_2}.$$

If $(m+1, p(q-1)) = 1$, then the only $\mathbb{F}_q$-rational point of $h_m(x_1, x_2) = 0$ is the origin and so $N_q(h_m) = 1$. Taking $k = 2, q = 5, m = 2$, one finds that $N_q(h_2(x_1, x_2)) = 1 < 6/5 = 6q^{2-3}$.

For even q, the problem is more subtle and we only have the following conjecture giving a slightly weaker bound.

Conjecture 1.5. *Let $h(x_1, ..., x_k)$ be a complete symmetric polynomial in $k \geq 4$ variables over $\mathbb{F}_q$ of degree m with $1 \leq m \leq q-4$. If q is even, then*

$$N_q(h) \geq 24q^{k-4}.$$

For even q, unconditionally, we only have the following significantly weaker result.

Theorem 1.6. *Let $h(x_1, ..., x_k)$ be a complete symmetric polynomial in k variables over $\mathbb{F}_q$ of degree m with $1 \leq m \leq q/2$. If $q \geq 8$ is even and $k \geq q/2$, then*

$$N_q(h) \geq (\frac{q}{2})! \cdot q^{k-\frac{q}{2}}.$$

To prove Theorem 1.4, we will consider the stronger question on the number of $\mathbb{F}_q$-rational points with distinct coordinates. After relating the complete symmetric polynomial $h(x_1, ..., x_k)$ to the determinant of certain generalized Vandermonde determinant, we show that the existence of $\mathbb{F}_q$-rational points with distinct coordinates is related to the vanishing of certain generalized Vandermonde determinant. The latter is then related to the classification of deep holes for Reed-Solomon codes, equivalently possible MDS extension of Reed-Solomon codes. One can then conclude the proof by applying the classical result ($k = 3$, p odd) of Segre [8] on ovals in finite projective planes.

Segre's old result is now a special case of the Cheng-Murray conjecture [3] which classifies deep holes for Reed-Solomon codes, which in turn is a consequence of the normal rational curve conjecture in finite geometry. The Cheng-Murray conjecture remains open in general, but has been proved by Zhuang-Cheng-Li [13] in the case $k \leq p$ and later by Kaipa [5] in the case $k \geq [(q+1)/2]$. These recent works will give us additional results on the number of rational points with distinct coordinates as discussed in next section.

2 Rational points with distinct coordinates

In coding theory, one often requires the additional condition that the coordinates of the rational point are distinct.

Definition 2.1. *Let $h(x_1, ..., x_k)$ be a complete symmetric polynomial of degree m in k-variables over $\mathbb{F}_q$. Let*

$$N_q^*(h) := \#\{(x_1, ..., x_k) \in \mathbb{F}_q^k, x_i \neq x_j \ (i \neq j) | h(x_1, ..., x_k) = 0\}$$

denote the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined by $h(x_1, ..., x_k) = 0$ with the additional condition that the coordinates are distinct.

We are interested in when $N_q^*(h) \geq 1$. Since T is symmetric, $N_q^*(h) \geq 1$ is equivalent to $N_q^*(h) \geq k!$ by permutations of the solutions. We have

Conjecture 2.2. *Let $3 \leq k \leq q-2$ ($4 \leq k \leq q-3$ if q is even). Let*

$$h(x_1, ..., x_k) = \sum_{e=0}^{m} a_e h_e(x_1, ..., x_n) \in \mathbb{F}_q[x_1, ..., x_k]$$

be a complete symmetric polynomial of positive degree m. Then $N_q^*(h) \geq 1$ if and only if the reduction $x^{k-1}(\sum_{e=0}^{m} a_e x^{e)}$ modulo $(x^q - x)$ is not a polynomial of degree equal to $k-1$. If this last condition holds, then $N_q(h) \geq N_q^*(h) \geq k!$.

Remarks. We shall see that the reduction condition modulo $(x^q - x)$ is necessary in order for $N_q^*(h) \geq 1$. The difficulty lies in the sufficient part of the condition. The reduction condition is also simple to check. For $0 \leq j \leq q-2$, let

$$b_j = \sum_{e \equiv j \mod (q-1)} a_e.$$

Then,

$$x^{k-1}(\sum_{e=0}^{m} a_e x^e) \equiv \sum_{j=0}^{q-k} b_j x^{j+k-1} + \sum_{j=q-k+1}^{q-2} b_j x^{j+k-q} \mod (x^q - x)$$

where the second sum on the right is a polynomial of degree at most $k-2$. Thus, the reduction is not a polynomial of degree equal to $k-1$ if and only if

either $b_0 = 0$ or that b_j is not zero for some $1 \le j \le q-k$. As an example, if $1 \le m \le q-k$, then $g(x) = x^{k-1}(\sum_{e=0}^{m} a_e x^e)$ is a polynomial of positive degree $m+k-1 \le q-1$, and so its reduction modulo $(x^q - x)$ has the same positive degree $m+k-1$ which is not equal to $k-1$. As a consequence, we obtain

Conjecture 2.3. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). Let*

$$h(x_1, ..., x_k) = \sum_{e=0}^{m} a_e h_e(x_1, ..., x_n) \in \mathbb{F}_q[x_1, ..., x_k]$$

be a complete symmetric polynomial of positive degree m. If $1 \le m \le q-k$, then $N_q(h) \ge N_q^*(h) \ge k!$.

Remarks: The simple condition $3 \le k \le q-2$ cannot be improved. Since for $k = 1$, $h(x)$ can be an arbitrary uni-variate polynomial of degree $m \ge 2$ and one can easily find one such $h(x)$ (any irreducible $h(x)$ will do) such that $N_q^*(h) = 0$. If $k = 2$, take $f(x) = \sum_{e=1}^{m+1} a_e x^e$ to be a permutation polynomial of degree $m+1$ over $\mathbb{F}_q$, then $h(x_1, x_2) := (f(x_1) - f(x_2))/(x_1 - x_2)$ is a complete symmetric polynomial of degree m with no $\mathbb{F}_q$-rational points off the diagonal $x_1 = x_2$. The condition $k \le q-2$ is optimal too. For instance, if $k = q$, there is only one possibility (up to permutation) for solutions with distinct coordinates. One can easily modify the constant term of h so that $N_q^*(h) = 0$. If $k = q-1$ ($q > 3$ odd), a solution set $\{\alpha_1, \cdots, \alpha_{q-1}\}$ is equal to $\mathbb{F}_q - \{\alpha\}$ for some $\alpha \in \mathbb{F}_q$, one then checks that

$$\sum_{i=1}^{q-1} \alpha_i = -\alpha, \ \sum_{i=1}^{q-1} \alpha_i^2 = -\alpha^2.$$

Then,

$$2h_2(\alpha_1, \cdots, \alpha_{q-1}) = (\sum_{i=1}^{q-1} \alpha_i)^2 + \sum_{i=1}^{q-1} \alpha_i^2 = \alpha^2 - \alpha^2 = 0$$

for all distinct $\alpha_1, \cdots, \alpha_{q-1}$ in $\mathbb{F}_q$. As a consequence, the complete symmetric polynomial $2h_2(x_1, ..., x_{q-1}) + c$ ($c \in \mathbb{F}_q^*$) has no $\mathbb{F}_q$-rational points with distinct coordinates.

The main result of this paper is to prove that the above conjecture is true if either $k \le p$ (this is always satisfied if $q = p$ is a prime) or if $k \ge \lfloor (q+1)/2 \rfloor$. Namely,

Theorem 2.4. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). Let*

$$h(x_1, ..., x_k) = \sum_{e=0}^{m} a_e h_e(x_1, ..., x_n) \in \mathbb{F}_q[x_1, ..., x_k]$$

be a complete symmetric polynomial of positive degree m. Assume either $k \le p$ or $k \ge \lfloor (q+1)/2 \rfloor$. Then $N_q^*(h) \ge 1$ if and only if the reduction $x^{k-1}(\sum_{e=0}^{m} a_e x^e)$ modulo $(x^q - x)$ is not a polynomial of degree equal to $k-1$.

Taking $k = 3$ and q odd (so $k = 3 \leq p$), we obtain Theorem 1.4 which is the result stated in the abstract. The reason is that we have

$$h_m(x_1, ..., x_k) = \sum_{e=0}^{m} h_e(x_1, x_2, x_3) h_{m-e}(x_4, \cdots, x_k).$$

It follows that if $h(x_1, ..., x_k)$ is a complete symmetric polynomial in k variables of degree m, then for every choice of $(a_4, \cdots, a_k) \in \mathbb{F}_q^{k-3}$, the specialization $h(x_1, x_2, x_3, a_4, \cdots, a_k)$ is a complete symmetric polynomial of the same degree m in the 3 variable $\{x_1, x_2, x_3\}$ and so we can apply the case $k = 3$ of the above theorem which is true when q is odd and $1 \leq m \leq q - 3$. This proves that

$$N_q(h) \geq \sum_{a_4, \cdots, a_k \in \mathbb{F}_q} N_q^*(T(x_1, x_2, x_3, a_4, \cdots, a_k)) \geq 6q^{k-3}.$$

For q even, the case $k = 4$ of the above conjecture implies that $N_q(h) \geq 24q^{k-4}$ if $k \geq 4$ and $1 \leq m \leq q-4$. But the case $k = 4$ (q even) of the above conjecture is still open. For q even, we can use the case $k = [(q + 1)/2] = q/2$ of the above theorem to deduce the weaker Theorem 1.6.

3 Generalized Vandermonde determinant

In this section, we show that Conjecture 2.2 is equivalent to a vanishing conjecture on certain generalized Vandermonde determinant. We shall work in a slightly more general framework.

Let $2 \leq k \leq n \leq q$ be integers. Let $S \subset \mathbb{F}_q$ be a subset of cardinality n. For any polynomial $f(x) \in \mathbb{F}_q[x]$ and $\alpha_1, \cdots, \alpha_k \in S$, let M_f denote the $k \times k$ matrix

$$M_f(\alpha_1, \cdots, \alpha_k) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_k^{k-2} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_k) \end{pmatrix}.$$

Let

$$D_f(\alpha_1, \cdots, \alpha_k) = \det M_f(\alpha_1, \cdots, \alpha_k)$$

denote its determinant. An interesting problem is to decide when the determinant is non-zero. Since $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$, reducing $f(x)$ modulo $(x^q - x)$ if necessary, we can assume that $\deg(f) \leq q - 1$. Remark that

1. $M_{x^{k-1}}(\alpha_1, \cdots, \alpha_k)$ is the standard Vandermonde matrix.
2. If there are $\alpha_i = \alpha_j$ for some $1 \leq i < j \leq k$, then $D_f(\alpha_1, \cdots, \alpha_k) = 0$. So we are only interested in pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$.

If $0 \leq \deg(f) \leq k-2$, then the last row of $M_f(\alpha_1, \cdots, \alpha_k)$ can be written as a linear combination of the first $k-1$ rows of $M_f(\alpha_1, \cdots, \alpha_k)$. So in this case, $D_f(\alpha_1, \cdots, \alpha_k) = 0$. If $\deg(f) = k-1$, saying $f(x) = ax^{k-1} + g(x)$ with $a \neq 0$ and $0 \leq \deg(g) \leq k-2$, then

$$D_f(\alpha_1, \cdots, \alpha_k) = aM_{x^{k-1}}(\alpha_1, \cdots, \alpha_k) = a \prod_{1 \leq i < j \leq k} (\alpha_j - \alpha_i) \neq 0,$$

for any pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$. If $S \subsetneq \mathbb{F}_q$ is a proper subset, then for any $\alpha \in \mathbb{F}_q \setminus S$, we have $(\alpha_i - \alpha)^{q-2} = (\alpha_i - \alpha)^{-1}$ and thus

$$D_{(x-\alpha)^{q-2}}(\alpha_1, \cdots, \alpha_k) = \frac{1}{\prod_{i=1}^{k}(\alpha_i - \alpha)} \prod_{1 \leq i < j \leq k} (\alpha_j - \alpha_i) \neq 0,$$

for any pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$.

Problem 3.1. *For a given subset $S \subset \mathbb{F}_q$ and polynomial $f(x) \in \mathbb{F}_q[x]$ with $\deg(f) \leq q-1$, is there some efficient way (e.g. polynomial time in $\log q$, $|S|$ and $\deg(f)$) to determine if $D_f(\alpha_1, \cdots, \alpha_k) \neq 0$ for all pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$.*

This problem is difficult in such a generality. In fact, we will soon see that this problem is NP-hard for general S. For even q, $k = 3$ and $S = \mathbb{F}_q$, the problem is the classification of hyperovals in finite projective plane $\mathbb{P}^2(\mathbb{F}_q)$, which is still open (see [2, Section 14.1] for the collection of known families of hyperovals).

The brute-force algorithm takes time

$$\binom{|S|}{k} \times \text{time of computing the determinant of } k \times k \text{ matrix},$$

which is exponential in $|S|$ when $k = c|S|$ for any $0 < c < 1$.

Theoretically, there is an explicit formula for the determinant D_f in terms of complete symmetric polynomials.

Proposition 3.2 ([4])**.** *For any polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{F}_q[x]$ with $a_d \neq 0$, define*

$$C_f(x_1, \cdots, x_k) := \sum_{i=k-1}^{d} a_i h_{i-(k-1)}(x_1, \cdots, x_k).$$

This is a complete symmetric polynomial of degree $d-k+1$, which depends only on the degree at least $k-1$ part of $f(x)$. Then, we have

$$D_f(x_1, \cdots, x_k) = C_f(x_1, \cdots, x_k) \prod_{1 \leq i < j \leq k} (x_j - x_i).$$

Corollary 3.3. *For any polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{F}_q[x]$ with $a_d \neq 0$, and any pairwise distinct $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q$, we have*

$$D_f(\alpha_1, \cdots, \alpha_k) = 0 \text{ if and only if } C_f(\alpha_1, \cdots, \alpha_k) = 0.$$

Let $N_q^*(C_f)$ denote the number of $\mathbb{F}_q$-rational points of C_f with distinct coordinates, and let $N_q^*(D_f)$ denote the number of $\mathbb{F}_q$-rational points of D_f with distinct coordinates. The above corollary says that

$$N_q^*(C_f) = N_q^*(D_f)$$

for all polynomial $f(x) \in \mathbb{F}_q[x]$. As noted before, $N_q^*(C_f) = N_q^*(D_f)$ depends only the residue class of $f(x) \mod (x^q - x)$. Conversely, given a complete symmetric polynomial

$$h(x_1, ..., x_k) = \sum_{e=0}^{m} a_e h_e(x_1, ..., x_n) \in \mathbb{F}_q[x_1, ..., x_k],$$

our construction shows that

$$h(x_1, ...x_k) = C_g(x_1, ..., x_k),\ g(x) = x^{k-1}(\sum_{e=0}^{m} a_e x^e).$$

If the reduction of $g(x)$ modulo $(x^q - x)$ is a polynomial of degree equal to $k-1$, by the above Vandermonde determinant discussion, we have $N_q^*(h) = 0$. This proves one direction of Conjecture 2.2. In the rest of the paper, we will focus on the other direction of the conjecture.

Here are some examples of low degrees:

1. In the case $d = k - 1$, $f(x) = \sum_{i=0}^{k-1} a_i x^i$ $(a_{k-1} \neq 0)$, so

   $$C_f(x_1, \cdots, x_k) = a_{k-1} \text{ and } D_f(x_1, \cdots, x_k) = a_{k-1} \prod_{1 \leq i < j \leq k} (x_i - x_j).$$

   Hence, $D_f(\alpha_1, \cdots, \alpha_k) \neq 0$ for any pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$.

2. In the case $d = k$, $f(x) = \sum_{i=0}^{k} a_i x^i$ $(a_k \neq 0)$, so

   $$C_f(x_1, \cdots, x_k) = a_{k-1} + a_k(x_1 + \cdots + x_k)$$

   is linear and

   $$D_f(x_1, \cdots, x_k) = (a_{k-1} + a_k(x_1 + \cdots + x_k)) \prod_{1 \leq i < j \leq k} (x_i - x_j).$$

   Hence, for any pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$, we have $D_f(\alpha_1, \cdots, \alpha_k) = 0$ if and only if $a_{k-1} + a_k(\alpha_1 + \cdots + \alpha_k) = 0$. This is exactly the k-subset sum problem (k-SSP) over S which is known to be **NP-complete** for general S. For special S, e.g. $S = \mathbb{F}_q$ or $\mathbb{F}_q^*$, there is an explicit formula for $N_q^*(C_f)$, see [6], which implies that $N_q^*(C_f) > 0$ for $3 \leq k \leq q - 2$.

3. In the case $d = k + 1$, $f(x) = \sum_{i=0}^{k+1} a_i x^i$ $(a_{k+1} \neq 0)$, so

   $$C_f(x_1, \cdots, x_k) = a_{k-1} + a_k \sum_{i=1}^{k} x_i + a_{k+1} \left(\sum_{i=1}^{k} x_i^2 + \sum_{1 \leq i < j \leq k} x_i x_j \right).$$

is quadratic. It was shown in [12, Theorem 4.2] that $N_q^*(C_f) > 0$ for $3 \le k \le q-2$ ($k \ne q-2$ if q is even).

These examples and the above discussion show that Conjecture 2.2 is equivalent to the following conjecture.

Conjecture 3.4. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). For any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k \le \deg(f) \le q-1$, there exist pairwise distinct $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q$ such that*

$$D_f(\alpha_1, \cdots, \alpha_k) = 0.$$

This conjecture answers Problem 3.1 when $S = \mathbb{F}_q$: $D_f(\alpha_1, \cdots, \alpha_k) \ne 0$ for all pairwise distinct $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q$ if and only if $\deg(f) = k-1$.

Note that the conjecture is false if we restrict $\alpha_1, \cdots, \alpha_k$ in a proper subset S of $\mathbb{F}_q$. Suppose $\alpha \in \mathbb{F}_q \backslash S$, taking $f(x) = (x-\alpha)^{q-2}$, we have $D_f(\alpha_1, \cdots, \alpha_k) \ne 0$ for all pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$. If $|S| = q-1$, by a translation we can assume that $S = \mathbb{F}_q^*$. In this case, we have the following similar conjecture.

Conjecture 3.5. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). For any polynomial $f(x) \in \mathbb{F}_q[x]$ with $k \le \deg(f) \le q-2$, except those of the form $ax^{q-2} + g(x)$ for some $a \ne 0$ and polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $\deg(g) \le k-2$, there exist pairwise distinct $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q^*$ such that*

$$D_f(\alpha_1, \cdots, \alpha_k) = 0.$$

We shall prove that these two conjectures are true if $k \ge (q+1)/2$.

4 Reed-Solomon codes and MDS codes

In this section, we further relate the conjectures in the previous section to the classification of deep holes for Reed-Solomon codes, equivalently MDS extension of Reed-Solomon codes.

We shall work with a general subset $S = \{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subset \mathbb{F}_q$ of the finite field $\mathbb{F}_q$. For any integer $2 \le k \le n$, define the $(k-1) \times n$ Vandermonde matrix

$$M(S,k) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_n^{k-2} \end{pmatrix}.$$

The row vectors of $M(S,k)$ generate the $[n, k-1]_q$ Reed-Solomon code with evaluation set S. It is an MDS code, which is equivalent to saying that every $(k-1) \times (k-1)$ submatrix of $M(S,k)$ has non-zero determinant.

By Lagrange interpolation, any word $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{F}_q^n$ can be written uniquely as

$$\beta = \beta_f := (f(\alpha_1), \cdots, f(\alpha_n)),$$

where $f(x) \in \mathbb{F}_q[x]$ is a polynomial with $\deg(f) \leq n-1$. The word β_f is a deep hole of the above Reed-Solomon code if and only if the row vectors of the following generalized $k \times n$ Vandermonde matrix

$$M_f(S,k) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_n^{k-2} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \end{pmatrix}$$

generate an MDS code, that is, every $k \times k$ submatrix of $M_f(S,k)$ has non-zero determinant. Equivalently, the determinant $D_f(\alpha_{i_1}, \cdots, \alpha_{i_k}) \neq 0$ for all $1 \leq i_1 < \cdots < i_k \leq n$. As noted before, the classification of deep holes is NP-hard for general S, even in the case when $\deg(f) = k$ (this reduces to the k-subset sum problem).

In the case $S = \mathbb{F}_q$ with $3 \leq k \leq q-3$ ($4 \leq k \leq q-4$ for even q), Cheng-Murray [3] conjectured that β_f is a deep hole if and only if $\deg(f) = k-1$. This conjecture immediately implies (and in fact equivalent) to Conjecture 3.4. This conjecture was already proven in the case $k = 3 \leq p$ for odd $q > 5$ by Segre in his classical paper [8]. This special case is all we need to prove Theorem 1.4.

The Cheng-Murray conjecture remains open in general, but has been proved by Zhuang-Cheng-Li [13] in the case $k \leq p$ and later by Kaipa [5] in the case $k \geq [(q+1)/2]$. As a consequence, Conjecture 3.4 is true if either $k \leq p$ or $k \geq [(q+1)/2]$.

The results in [13] and [5] depend crucially on results from finite geometry. To be self-contained, in the rest of this section, we include a simpler and more direct proof of these results motivated by the approach from [5].

Let $v_i = \frac{1}{\prod_{j \neq i}(\alpha_i - \alpha_j)}$ for $1 \leq i \leq n$, which are non-zero in $\mathbb{F}_q$. Define the dual $(n-k+1) \times n$-matrix

$$\begin{aligned} M(S,k)^{\perp} &= \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k} & v_2\alpha_2^{n-k} & \cdots & v_n\alpha_n^{n-k} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k} & \alpha_2^{n-k} & \cdots & \alpha_n^{n-k} \end{pmatrix} \begin{pmatrix} v_1 & 0 & \cdots & 0 \\ 0 & v_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & v_n \end{pmatrix}. \end{aligned}$$

Then

$$M(S,k)(M(S,k)^{\perp})^T = 0. \tag{1}$$

Equation (1) is the well-known relationship between generalized Reed-Solomon codes and their dual codes. We present a proof to make it self-contained. For

any polynomial $a(x) \in \mathbb{F}_q[x]$ of degree $\leq k-2$ and any polynomial $b(x) \in \mathbb{F}_q[x]$ of degree $\leq n-k$, the product $a(x)b(x)$ has degree $\leq n-2$. By the Lagrange interpolation, we have

$$a(x)b(x) = \sum_{i=1}^{n} \frac{\prod_{j\neq i}(x-\alpha_j)}{\prod_{j\neq i}(\alpha_i-\alpha_j)} a(\alpha_i)b(\alpha_i).$$

Comparing the terms of degree $n-1$ of both sides, we get

$$0 = \sum_{i=1}^{n} \frac{1}{\prod_{j\neq i}(\alpha_i-\alpha_j)} a(\alpha_i)b(\alpha_i) = \sum_{i=1}^{n} a(\alpha_i)(v_i b(\alpha_i)). \tag{2}$$

Taking $a(x) = x^{k_1}$ with $0 \leq k_1 \leq k-2$ and $b(x) = x^{k_2}$ with $0 \leq k_2 \leq n-k$, we deduce the orthogonality relation in Equation (1).

Define the extended $k \times (n+1)$ matrix of $M_f(S,k)$ to be

$$M_f^E(S,k) = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_n^{k-2} & 0 \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) & 1 \end{pmatrix}.$$

Lemma 4.1. *Let $w_i = -\sum_{j=1}^{n} v_j \alpha_j^i f(\alpha_j)$ for $i = 0, 1, \cdots, n-k$, and let*

$$M_f^E(S,k)^{\perp} = \begin{pmatrix} v_1 & v_2 & \cdots & v_n & w_0 \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n & w_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1\alpha_1^{n-k} & v_2\alpha_2^{n-k} & \cdots & v_n\alpha_n^{n-k} & w_{n-k} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & \cdots & 1 & w_0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & w_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{n-k} & \alpha_2^{n-k} & \cdots & \alpha_n^{n-k} & w_{n-k} \end{pmatrix} \begin{pmatrix} v_1 & 0 & \cdots & 0 & 0 \\ 0 & v_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & v_n & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then we have

$$M_f^E(S,k)(M_f^E(S,k)^{\perp})^T = 0. \tag{3}$$

Proof. It follows from Equation (1) that the rows of $M_f^E(S,k)^{\perp}$ are orthogonal to the first $k-1$ rows of $M_f^E(S,k)$. From the definition of w_i, we deduce that the rows of $M_f^E(S,k)^{\perp}$ are also orthogonal to the last row of $M_f^E(S,k)$. So we have $M_f^E(S,k)(M_f^E(S,k)^{\perp})^T = 0$. □

The following lemma is well-known as the property of MDS codes: the dual code of an MDS code is still an MDS code (see [7, Chapter 11]).

Lemma 4.2. *Let $A \in \mathbb{F}_q^{k\times n}$ $(1 \le k < n)$ be of rank k and $B \in \mathbb{F}_q^{(n-k)\times n}$ be of rank $n-k$ such that $A \cdot B^T = 0$. Then the following two statements are equivalent:*

1. *every k columns of A are linearly independent,*
2. *every $n-k$ columns of B are linearly independent.*

Remark that if the matrix A satisfies the above condition, the n columns of A are literately called an n-arc in the projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

Definition 4.3. *A set of points in the $(k-1)$-dimensional projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is called an arc if any k points in the set form a basis for the affine space $\mathbb{F}_q^k$.*

An important example for arcs is the following normal rational curve.

Definition 4.4. *For any integer $1 \le k \le q+1$ and $\alpha \in \mathbb{F}_q \cup \infty$, we define vectors (also considered as points in the corresponding projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$)*

$$c_k(\alpha) = \begin{cases} (1, \alpha, \alpha^2, \cdots, \alpha^{k-1})^T & \text{if } \alpha \in \mathbb{F}_q, \\ (0, 0, \cdots, 0, 1)^T & \text{if } \alpha = \infty. \end{cases}$$

For any subset $S \subset \mathbb{F}_q \cup \infty$, the set

$$\mathrm{NRC}_k(S) = \{c_k(\alpha) \,:\, \alpha \in S\}$$

is called a normal rational curve (NRC).

Note that the length of any NRC cannot exceed $q+1$. There are famous conjectures on arcs and NRC.

Conjecture 4.5 (MDS conjecture)**.** *For $3 \le k \le q-2$ ($4 \le k \le q-2$ if q is even), the length of any arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ cannot exceed $q+1$.*

This conjecture is true for prime fields $\mathbb{F}_q$ (see [1]). A much weaker conjecture is the following.

Conjecture 4.6 (Normal Rational Curve Conjecture)**.** *For $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even), $\mathrm{NRC}_k(\mathbb{F}_q \cup \infty)$ cannot be extended to any strictly longer arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.*

See [1, 2] for the extremal structure of $(q+1)$-arcs.

Theorem 4.7 ([1, Theorem 1.10])**.** *For $3 \le q-p+1 \le k \le q-2$, any $(q+1)$-arc is equivalent to $\mathrm{NRC}_k(\mathbb{F}_q \cup \infty)$.*

We also need the following old result on the extension of NRCs.

Theorem 4.8 ([9, Theorem 1])**.** *For $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even), let $\mathrm{NRC}_k(S) \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$ be any NRC with length $|S| \ge k + \lfloor (q-1)/2 \rfloor$. For any $v \in \mathbb{P}^{k-1}(\mathbb{F}_q)$, if $S \cup \{v\}$ forms an arc, then $v = c_k(\beta)$ for some $\beta \in (\mathbb{F}_q \cup \infty) \setminus S$.*

Note that if $f_1(x) \equiv f_2(x) \mod \prod_{\alpha \in S}(x-\alpha)$, then $f_1(\alpha) = f_2(\alpha)$ for all $\alpha \in S$, and it follows that

$$D_{f_1}(\alpha_1, \cdots, \alpha_k) = D_{f_2}(\alpha_1, \cdots, \alpha_k)$$

for all pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$. Reducing $f(x)$ modulo $\prod_{\alpha \in S}(x-\alpha)$ (which is a polynomial of degree n), we can assume that $k \leq \deg(f) \leq n-1$.

The main technical result we need is the following theorem, which was first proved by Zhuang-Cheng-Li [13] in the case $k \leq p$ and later by Kaipa [5] in the case $k \geq [(q+1)/2]$.

Theorem 4.9. *Let $S \subset \mathbb{F}_q$ be a subset of size n and let k be any integer such that $\max(3, n-q+3) \leq k \leq n-2$ ($\max(4, n-q+4) \leq k \leq n-3$ for q even). Assume either $k \leq p$ (and $n = q$) or $k \geq \lfloor \frac{q+1}{2} \rfloor$. Then, for any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k \leq \deg(f) \leq n-1$, except those of the form $a(x-\alpha)^{q-2} + g(x)$ ($\mod \prod_{\beta \in S}(x-\alpha)$) for some $a \neq 0$, $\alpha \in \mathbb{F}_q \setminus S$ and polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $\deg(g) \leq k-2$, there exist pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$ such that $D_f(\alpha_1, \cdots, \alpha_k) = 0$.*

Proof. We consider the opposite side and prove by contradiction. Assume for any pairwise distinct $\alpha_1, \cdots, \alpha_k \in S$, we have

$$D_f(\alpha_1, \cdots, \alpha_k) \neq 0.$$

This condition is equivalent to that any k columns of $M_f(S,k)$ are linearly independent, which is also equivalent to that any k columns of $M_f^E(S,k)$ are linearly independent. By Lemma 4.2, it is equivalent to that any $n+1-k$ columns of $M_f^E(S,k)^\perp$ are linearly independent. That is,

$$\mathrm{NRC}_{n+1-k}(S) \cup \{w = (w_0, w_1, \cdots, w_{n-k})^T\}$$

forms an $n+1$ arc in $\mathbb{P}^{n-k}(\mathbb{F}_q)$, which contains at least n points of $\mathrm{NRC}_k(\mathbb{F}_q \cup \infty)$. In order to apply Theorem 4.8, we need to have the inequality $3 \leq n+1-k \leq q-2$ (and also $4 \leq n+1-k \leq q-3$ for q even) . This translates into the condition $\max(3, n-q+3) \leq k \leq n-2$ (and also $\max(4, n-q+4) \leq k \leq n-3$ for q even), which is satisfied by our assumption. If the condition $k \geq \lfloor (q+1)/2 \rfloor$ holds, then

$$n+1-k+\lfloor \frac{q-1}{2} \rfloor \leq n,$$

and we can apply Theorem 4.8 to conclude that the point w must be contained in $\mathrm{NRC}_k(\mathbb{F}_q \cup \infty)$ as well. That is, as points in $\mathbb{P}^{n-k}(\mathbb{F}_q)$, either $w = (0, 0, \cdots, 1)^T$ or $w = c_{n+1-k}(\alpha)$ for some $\alpha \in \mathbb{F}_q \setminus S$. In the case $|S| = q$ and $k \leq p$ by Theorem 4.7, $w = (0, 0, \cdots, 1)^T$.

- If $w = (0, 0, \cdots, 1)^T$ in $\mathbb{P}^{n-k}(\mathbb{F}_q)$, we get a system of linear equations on variables $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$:

$$\begin{cases} \sum_{j=1}^n v_j \alpha_j^i f(\alpha_j) = 0, & \text{for } i = 0, 1, \cdots, n-k-1, \\ \sum_{j=1}^n v_j \alpha_j^{n-k} f(\alpha_j) = a. \end{cases}$$

for some $a \in \mathbb{F}_q^*$. That is,

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & \cdots & v_n\alpha_n^{n-k-1} \\ v_1\alpha_1^{n-k} & v_2\alpha_2^{n-k} & \cdots & v_n\alpha_n^{n-k} \end{pmatrix} \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_n) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ a \end{pmatrix}. \tag{4}$$

Note that

- by Equality (1), to satisfy the first $n-k$ equations, the vector

  $$(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n))$$

  must belong to the $\mathbb{F}_q$-linear vector space generated by rows of

  $$M(S, k+1) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

  - This means that there is a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree at most $k-1$ such that $f(\alpha_i) = g(\alpha_i)$ for all $1 \le i \le n$. Since $\deg(f) \le n-1$, it forces that $f(x) = g(x)$, which has degree at most $k-1$, contradicting to our assumption $\deg(f) \ge k$.

- If $w = c_{n+1-k}(\alpha)$ for $\alpha \in \mathbb{F}_q \setminus S$, we get a system of linear equations on variables $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$:

  $$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k} & v_2\alpha_2^{n-k} & \cdots & v_n\alpha_n^{n-k} \end{pmatrix} \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_n) \end{pmatrix} = b \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-k} \end{pmatrix}$$

  for some $b \in \mathbb{F}_q^*$.

Operating rows transformations, it is easy to get

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1(\alpha_1-\alpha) & v_2(\alpha_2-\alpha) & \cdots & v_n(\alpha_n-\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k-1}(\alpha_1-\alpha) & v_2\alpha_2^{n-k-1}(\alpha_2-\alpha) & \cdots & v_n\alpha_n^{n-k-1}(\alpha_n-\alpha) \end{pmatrix} \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_n) \end{pmatrix} = \begin{pmatrix} b \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Similar as above, the last $n-k$ equations show that the vector

$$(f(\alpha_1)(\alpha_1-\alpha), \cdots, f(\alpha_n)(\alpha_n-\alpha))$$

is a linear combination of the rows of $M(S, k+1)$. That is, there is a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree at most $k-1$ such that $f(\alpha_i)(\alpha_i - \alpha) = g(\alpha_i)$ for all $1 \le i \le n$. This implies that

$$f(x)(x-\alpha) \equiv g(x) \pmod{\prod_{\beta \in S}(x-\beta)},$$

where $\deg(g) \le k-1$. Write $g(x) = a + (x-\alpha)g_1(x)$ where $a = g(\alpha)$ and $\deg(g_1) \le k-2$. Then,

$$f(x) \equiv \frac{a}{x-\alpha} + g_1(x) \equiv a(x-\alpha)^{q-2} + g_1(x) \pmod{\prod_{\beta \in S}(x-\beta)}.$$

By our assumption that $k \le \deg(f) \le n-1$, we must have $a \neq 0$. The proof is complete. □

Taking $S = \mathbb{F}_q$ in the above theorem, we get

Corollary 4.10. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). For any polynomial $f(x) \in \mathbb{F}_q[x]$ with $k \le \deg(f) \le q-1$, there exist pairwise distinct $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q$ such that*

$$D_f(\alpha_1, \cdots, \alpha_k) = 0$$

if either $k \le p$ or $\lfloor (q+1)/2 \rfloor \le k$.

Remark 4.11. *By Conjecture 22 in [2], saying that for $6 \le k \le q-5$ any $(q+1)$-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is equivalent to $\mathrm{NRC}_k(\mathbb{F}_q \cup \infty)$, and the proof above, Conjecture 3.4 is true, and hence Conjecture 2.2 is true.*

Taking $S = \mathbb{F}_q^*$ in Theorem 4.9, we get

Corollary 4.12. *Let $3 \le k \le q-2$ ($4 \le k \le q-3$ if q is even). Assume that $\lfloor (q+1)/2 \rfloor \le k$. For any polynomial $f(x) \in \mathbb{F}_q[x]$ with $k \le \deg(f) \le q-2$, except those of the form $ax^{q-2} + g(x)$ for some $a \neq 0$ and polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $\deg(g) \le k-2$, there exist pairwise distinct non-zero $\alpha_1, \cdots, \alpha_k \in \mathbb{F}_q^*$ such that*

$$D_f(\alpha_1, \cdots, \alpha_k) = 0.$$

References

[1] Simeon Ball. On large subsets of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 3(1-2):733–748, 2011.

[2] Simeon Ball and Michel Lavrauw. Arcs in finite projective spaces. *e-prints arXiv:1908.10772*, Aug 2019.

[3] Qi Cheng and Elizabeth Murray. On deciding deep holes of Reed-Solomon codes. *Lecture Notes in Computer Science*, 4484:296–305, 2007.

[4] A.M. Fink. Certain determinants related to the Vandermonde. *Proceedings of the American Mathematical Society*, 38(3):483–488, 1973.

[5] Krishna Kaipa. Deep holes and MDS extensions of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 63(8):4940–4948, 2017.

[6] Jiyou Li and Daqing Wan. On the subset sum problem over finite fields. *Finite Fields and Their Applications*, 14(4):911–929, 2008.

[7] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

[8] Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[9] G. Seroussi and R. M. Roth. On MDS extensions of generalized Reed-Solomon codes. *IEEE Transactions on Information Theory*, 32(3):349–354, May 1986.

[10] Daqing Wan. A Chevalley-Warning approach to p-adic estimates of character sums. *Proceedings of the American Mathematical Society*, 123(1):45–54, 1995.

[11] Ewald Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abh. Math. Sem. Univ. Hamburg*, 11(1):76–83, 1935.

[12] Jun Zhang, Fang-Wei Fu, and Qunying Liao. New deep holes of generalized Reed-Solomon codes. *Scientia Sinica*, 43(7):727–740, 2013.

[13] J. Zhuang, Q. Cheng, and J. Li. On determining deep holes of generalized Reed-Solomon codes. *IEEE Transactions on Information Theory*, 62(1):199–207, Jan 2016.