Distance Distribution in Reed-Solomon Codes

Jiyou Li and Daqing Wan, *Member, IEEE,*

***Abstract*—Let $\mathbb{F}_q$ be the finite field of q elements. In this paper we obtain bounds on the following counting problem: given a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k+m$ and a non-negative integer r, count the number of polynomials $g(x) \in \mathbb{F}_q[x]$ of degree at most $k-1$ such that $f(x)+g(x)$ has exactly r roots in $\mathbb{F}_q$. Previously, explicit formulas were known only for the cases $m=0,1,2$. As an application, we obtain an asymptotic formula on the list size of the standard Reed-Solomon code $[q,k,q-k+1]_q$.**

***Index Terms*—IEEE, IEEEtran, journal, LATEX, paper, template.**

I. Introduction

A. Motivations

This paper is motivated by the following fundamental coding theory problem:

Problem 1.1: Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. Given a received word u, determine the distance distribution having u as the center. That is, for integer $i \geq 0$, compute the number $N_i(u)$ of codewords in $\mathcal{C}$ whose distance to u is exactly i.

When the received word u is a codeword, this is the classical weight distribution problem, which is generally **NP**-hard and only well understood for certain special codes such as MDS codes and some special families of cyclic codes. When the received word is not a codeword, it is equivalent to the coset weight distribution problem. The coset weight distribution was determined for a few very special classes of linear codes including t-error-correcting BCH codes for $t \leq 3$ (cf. [4], [5], [6]), external self-dual binary codes of length n for $n \leq 20, n = 28, 40, 46, 56$ (cf. [12], [13], [20], [21]) and the second-order Reed-Muller code of length 64 (cf. [1], [22]).

The distance distribution problem can be viewed as the counting version of list decoding and is much harder and widely open even for standard Reed-Solomon codes. In this paper, we make the first attempt to study this problem and obtain an asymptotic formula for standard Reed-Solomon codes.

A special case of our problem is computing the error distance from a received word u, that is, finding the smallest non-negative integer i such that $N_i(u) > 0$. This can be reduced to the decision version of the maximal likelihood decoding problem in coding theory. As Reed Solomon codes are constructed using polynomials, all such problems on Reed-Solomon codes can be reduced to polynomial factorization problems. Details will be explained in Section 2. To be more precise in this introduction, we now introduce some notations.

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let $1 \leq n \leq q$ be a positive integer, $D = \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$ be a subset of cardinality $|D| = n > 0$. For $1 \leq k \leq n$, the Reed-Solomon code $\mathcal{RS}_{n,k}$ has the codewords of the form

$$(f(x_1), \ldots, f(x_n)) \in \mathbb{F}_q^n,$$

where f runs over all polynomials in $\mathbb{F}_q[x]$ of degree at most $k-1$. It is well-known that the minimum distance of the Reed-Solomon code is $n-k+1$. If $D = \mathbb{F}_q$ (resp., $\mathbb{F}_q^*$), then the code $\mathcal{RS}_{q,k}$(resp., $\mathcal{RS}_{q-1,k}$) is called the standard (respectively the primitive) Reed-Solomon codes. All our results for standard Reed-Solomon codes extend to primitive Reed-Solomon codes with minor modification. For this reason, we shall focus on the standard Reed-Solomon codes in this paper.

For any word $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, one can efficiently compute a unique polynomial $u(x) \in \mathbb{F}_q[x]$ of degree at most $n-1$ such that

$$u(x_i) = u_i, \text{ for all } 1 \leq i \leq n.$$

Explicitly, the polynomial $u(x)$ is given by the Lagrange interpolation formula

$$u(x) = \sum_{i=1}^{n} u_i \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

The degree $\deg(u)$ of u is then defined as the degree of the associated polynomial $u(x)$. It is easy to see that u is a codeword if and only if $\deg(u) < k$.

For a given word $u \in \mathbb{F}_q^n$, the distance from u to $\mathcal{RS}_{n,k}$ is defined by

$$d(u, \mathcal{RS}_{n,k}) := \min_{v \in \mathcal{RS}_{n,k}} d(u, v).$$

The maximum likelihood decoding of u is to find a codeword $v \in \mathcal{RS}_{n,k}$ such that $d(u,v) = d(u, \mathcal{RS}_{n,k})$. Thus, computing $d(u, \mathcal{RS}_{n,k})$ is essentially the decision version for the maximum likelihood decoding problem, which is **NP**-complete for general subset $D \subset \mathbb{F}_q$, see Guruswami-Vardy [11] and Cheng-Murray [7]. For standard Reed-Solomon code with $D = \mathbb{F}_q$, the complexity of the maximum likelihood decoding is unknown to be **NP**-complete. This is an important open problem. It was shown by Cheng-Wan [9], [10] that decoding the standard Reed-Solomon code is at least as hard as the discrete logarithm problem in a large extension of the finite field $\mathbb{F}_q$.

If $\deg(u) \leq k-1$, then u is a codeword and thus $d(u, \mathcal{RS}_{n,k}) = 0$. We shall assume that $k \leq \deg(u) \leq n-1$. The following simple result gives an elementary bound for $d(u, \mathcal{RS}_{n,k})$.

J. Li was supported by the National Natural Science Foundation of China under Grant 11771280 and the National Science Foundation of Shanghai Municipal under Grant 17ZR1415400. D. Wan was partially supported by NSF.

J. Li is with the School of Mathematical Sciences, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: lijiyou@sjtu.edu.cn).

D. Wan is with the department of Mathematics, University of California Irvine, CA 92697-3875 USA (e-mail: dwan@math.uci.edu).

Manuscript received February 8, 2019; revised July 26, 2019.

Theorem 1.2: [16] Let $u \in \mathbf{F}_q^n$ be a word such that $k \leq \deg(u) \leq n-1$. Then,

$$n - \deg(u) \leq d(u, \mathcal{RS}_{n,k}) \leq n-k.$$

The word u is called a deep hole if $d(u, \mathcal{RS}_{n,k}) = n-k$, that is, it achieves the covering radius. When $\deg(u) = k$, the upper bound and the lower bound agree and hence u is a deep hole. This gives $(q-1)q^k$ deep holes. For a general Reed-Solomon code $\mathcal{RS}_{n,k}$, it is already difficult to determine if a given word u is a deep hole. Even for the special case that $\deg(u) = k+1$, the deep hole problem is equivalent to the $(k+1)$-subset sum problem over $\mathbb{F}_q$ which is **NP**-complete [7].

For the standard Reed-Solomon code, that is, $D = \mathbb{F}_q$ and thus $n = q$, there is the following deep hole conjecture of Cheng-Murray [7].

Conjecture 1.3: For the code $\mathcal{RS}_{q,k}$ with $p > 2$, the set $\{u \in \mathbb{F}_q^n \big| \deg(u) = k\}$ gives the set of all deep holes.
Many results were proved towards this conjecture. Please refer to [2], [14], [19], [26] and the references there.

The deep hole problem is to determine when the upper bound in the above theorem agrees with $d(u, \mathcal{RS}_{n,k})$. One is also interested in the situations when the lower bound $n - \deg(u)$ agrees with $d(u, \mathcal{RS}_{n,k})$. We call u **ordinary** if $d(u, \mathcal{RS}_{n,k}) = n - \deg(u)$. A basic problem is then to determine when a given word u is ordinary. This is equivalent to determining if $N_{n-\deg(u)}(u) > 0$. This problem will be studied in a future paper.

Since $k \leq \deg(u) \leq n-1$, we can write $\deg(u) = k+m$ for some non-negative integer $m \leq n-k-1$. Then, the word u is represented uniquely by a polynomial $u(x) \in \mathbb{F}_q[x]$ of degree $k+m$. For $0 \leq r \leq k+m$, let $N_D(f(x), r)$ denote the number of polynomials $g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) \leq k-1$ such that $f(x)+g(x)$ has exactly r distinct roots in D. It is clear that $N_i(u) = N_D(u(x), n-i)$. Thus, it is enough to study $N_D(f(x), r)$.

From now on, we only work with the standard Reed-Solomon codes $\mathcal{RS}_{q,k}$. Since $D = \mathbb{F}_q$, we can write $N(f(x), r) = N_{\mathbb{F}_q}(f(x), r)$ and $N_i(u) = N(u(x), q-i)$. It is clear that without loss of generality, we can assume that $f(x)$ is monic with no terms of degree less than k. Our distance distribution problem for the standard Reed-Solomon code is reduced to the following number theoretic problem.

Problem 1.4: Let $1 \leq k \leq q$ and $-k \leq m \leq q-k-1$. Given a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k+m$ and an integer $0 \leq r \leq k+m$, count $N(f(x), r)$, the number of polynomials $g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) \leq k-1$ such that $f(x)+g(x)$ has exactly r distinct roots in $\mathbb{F}_q$.

Not much is known about this problem. Elementary explicit formulas for $m \leq 2$ were known before. Exponential lower bounds and asymptotic formula for $N(f(x), r)$ have been studied in [8], [9], [10], [17] in the extreme case $r = m+k$. Our contribution of this paper is to prove results for all $0 \leq r \leq k+m$. If k is very small (say logarithmic in q), one can use the Chebotarev density theorem to derive a good asymptotic formula. However, in coding theory application, k is the code dimension which can be as large as a linear function of q. The problem then becomes more difficult. The main purpose of this paper is to prove nontrivial results for large k and a wide range of r if m is not too large.

B. Known Cases for $m \leq 2$

When $m < 0$, $f(x)$ represents a codeword and thus we may assume $f \equiv 0$, or equivalently $u = 0$. By a famous theorem of Mac Williams, for $0 \leq r \leq k-1$ we have

$$N(0, r) = \binom{q}{r} q^{k-r-1}(q-1)\left(\sum_{j=0}^{k-r-1}(-1)^j \binom{q-r-1}{j} q^{-j}\right).$$

If $m = 0$, then $\deg(f) = k$. In this case, u is a deep hole. An explicit formula for $N(x^k, r)$ was given by A. Knopfmacher and J. Knopfmacher [15].

If $m = 1$, then $\deg(f) = k+1$. We may assume $f(x) = x^{k+1} + ax^k$. It turns out that $N(x^{k+1} + ax^k, r)$ depends on a. An explicit formula for $N(x^{k+1} + ax^k, r)$ was given by Zhou, Wang and Wang [25]. A more complicated explicit counting formula for the case $m = 2$ is also given in the same paper.

When $m > 2$, it is no longer reasonable to expect an explicit formula for $N(f(x), r)$, but we can hope for an asymptotic formula. This is the aim of the present paper.

C. Main Result

For an integer $s \geq 0$, define the alternating sum

$$\mu_s = \sum_{j=0}^{s}(-1)^j \binom{q-r}{j} q^{-j} = 1 - \frac{q-r}{q} + \binom{q-r}{2}\frac{1}{q^2} - \cdots.$$

The absolute value of the j-th term is decreasing in j. It follows that if $r = cq$ for some constant $0 < c < 1$, then

$$0 < c \leq \frac{r}{q} = 1 - \frac{q-r}{q} \leq \mu_s \leq 1.$$

Since μ_s is a truncation of $(1-q^{-1})^{q-r}$, μ_s is close to $(1/e)^{1-c}$ when q and s are both large, and $r \approx cq$. Our main result is the following bound on $N(f(x), r)$, which holds for all k, m, and r.

Theorem 1.5: Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of $\deg(f) = k+m \leq q-1$. For integers $0 \leq r \leq k+m$, we have

$$\left| N(f(x), r) - \mu_{k+m-r}\binom{q}{r} q^{k-r} \right| \leq \sum_{j=k+1}^{k+m} \binom{j}{r}\binom{\frac{q}{p} + m\sqrt{q} + j}{j}\binom{m-1}{k+m-j}\sqrt{q}^{k+m-j}.$$

Our technique to establish Theorem 1.5 is based on a distinct coordinates sieving technique discovered by the authors [17], [18], a weighted inclusion-exclusion sieving formula, and a character sum bound on constant degree polynomials defined over a suitable residue ring.

The number $\sqrt{q}$ in the error term comes from the application of the Riemann hypothesis over finite fields (Weil's bound). The number of non-zero error terms in the error estimate is $k+m-\max\{k+1, r\}$. This means that if either m is small or $k+m-r$ is small, then there are only a few terms in the error estimate. The theorem also becomes stronger in the case

$q = p$ is a prime since then the number $\frac{q}{p}$ becomes 1. We now derive a few corollaries and explain how they are related to previous results.

When $m = 0$, we may suppose $f(x) = x^k$. In this case, there is no error term in our asymptotic formula and we thus obtain the following explicit formula first proved in [15], as reported in the above known cases.

Corollary 1.6:

$$N(x^k, r) = \binom{q}{r} q^{k-r} \left(\sum_{j=0}^{k-r} (-1)^j \binom{q-r}{j} q^{-j} \right).$$

When $r = k+m$, there is only one term in the error estimate and we obtain the following corollary, which was first proved in [17].

Corollary 1.7: Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of $\deg(f) = k + m \leq q - 1$. Then,

$$\left| N(f(x), k+m) - \frac{1}{q^m} \binom{q}{k+m} \right| \leq \binom{\frac{q}{p} + m\sqrt{q} + k + m}{k+m}.$$

When $r = k + m - 1$, there are two terms in the error estimate. Combining the two terms, we obtain the following corollary, which is already a new result.

Corollary 1.8: Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of $\deg(f) = k + m \leq q - 1$. Then,

$$\left| N(f(x), k+m-1) - \frac{k+m-1}{q^m} \binom{q}{k+m-1} \right|$$
$$\leq \binom{\frac{q}{p} + m\sqrt{q} + k + m}{k+m} ((m-1)\sqrt{q} + k + m).$$

For general r, there will be more terms in the error estimate. This makes it harder to estimate the error term. However, as we shall see, the above j-th error term in the error estimate is sometimes increasing in j and thus we can combine all the error terms into a single error term. This helps in obtaining a much simpler asymptotic formula, as done in next subsection.

The paper is organized as follows. In the end of this introductory section, some asymptotic analysis for some special parameters are given. In section 2, we prove the main result Theorem 1.5 by a key counting formula given in Lemma 2.2. In section 3 and 4, we introduce a sieving technique and a character sum derived by the Weil bound respectively. The proof of Lemma 2.2 will be given in Section 5.

D. Asymptotic Analysis

As an illustration, we show that our bound above can be used to give a nontrivial asymptotic formula. We assume $q = p$ is prime for simplicity. Then we find simple conditions under which the error term can be significantly simplified. Please note that the binomial coefficients for real numbers are defined by

$$\binom{a}{b} = \frac{\Gamma(a+1)}{\Gamma(b+1)\Gamma(a-b+1)}.$$

Corollary 1.9: Let $q = p$ and $f(x)$ be a polynomial of degree $k + m$. Suppose $k = cp, m = p^\delta, r = k + p^\lambda$, where $c \in (0,1), \delta \in (0, 1/4), \lambda \in (0, \delta)$ are constants. As p goes to infinity, we have

$$N(f(x), r) = \mu_{k+m-r} \binom{p}{r} p^{k-r} (1 + o(1)).$$

Proof: By Theorem 1.5, we have

$$\left| N(f(x), r) - \mu_{k+m-r} \binom{p}{r} p^{k-r} \right|$$
$$\leq \sum_{j=r}^{k+m} \binom{j}{r} \binom{m\sqrt{p} + 1 + j}{m\sqrt{p} + 1} \binom{m-1}{k+m-j} p^{\frac{k+m-j}{2}}$$
$$\leq m \cdot \max_{r \leq j \leq k+m} E_j,$$

where

$$E_j = \binom{j}{r} \binom{m\sqrt{p} + 1 + j}{m\sqrt{p} + 1} \binom{m-1}{k+m-j} p^{\frac{k+m-j}{2}}.$$

One computes that for $r \leq j < k + m$,

$$\frac{E_{j+1}}{E_j} = \frac{(j+1)}{(j+1-r)} \cdot \frac{(m\sqrt{p} + j + 2)}{(j+1)} \cdot \frac{(k+m-j)}{(j-k)\sqrt{p}}.$$

Write $j = r + j'$, where $0 \leq j' < k + m - r = p^\delta - p^\lambda$. Then

$$\frac{E_{j+1}}{E_j} = \frac{(m\sqrt{p} + r + j' + 2)}{(j'+1)} \cdot \frac{(p^\delta - p^\lambda - j')}{(p^\lambda + j')\sqrt{p}}.$$

Since $0 \leq j' < p^\delta - p^\lambda$, we deduce

$$\frac{E_{j+1}}{E_j} > \frac{(m\sqrt{p} + r)}{(p^\delta - p^\lambda)} \cdot \frac{1}{p^\delta \sqrt{p}}.$$

Note that $r \geq cp$ and $\lambda < \delta < \frac{1}{4}$. It follows that for p sufficiently large, we have $E_{j+1}/E_j > 1$ for all j, thus E_j is increasing in j and

$$\max_{r \leq j \leq k+m} E_j = \binom{k+m}{r} \binom{m\sqrt{p} + k + m + 1}{m\sqrt{p} + 1}.$$

As noted in the beginning of this section,

$$0 < c \leq \frac{r}{p} = 1 - \frac{p-r}{p} \leq \mu_{k+m-r} \leq 1.$$

To complete the proof of the corollary, it suffices to show

$$\lim_{p \to \infty} \frac{m\binom{k+m}{k+m-r}\binom{m\sqrt{p}+1+k+m}{m\sqrt{p}+1}}{\binom{p}{r} p^{k-r}} = 0.$$

Since $k + m - r \leq m \leq (k+m)/2$ and $1 \leq r - k \leq m$, it is enough to prove

$$\lim_{p \to \infty} \frac{m\binom{k+m}{m} p^m \binom{m\sqrt{p}+1+k+m}{m\sqrt{p}+1}}{\binom{p}{r}} = 0.$$

By the inequalities

$$(\frac{n}{l})^l \leq \binom{n}{l} \leq (\frac{en}{l})^l,$$

it is sufficient to have

$$\lim_{p \to \infty} \frac{m(e(k+m)p)^m (e + e\frac{k+m}{m\sqrt{p}+1})^{m\sqrt{p}+1}}{(\frac{p}{r})^r} = 0.$$

Since $k = cp, m = p^{\delta}, r = cp + p^{\lambda}$ and $c \in (0,1), \delta \in (0, 1/4), \lambda \in (0, \delta)$, by taking logarithm, it is equivalent to have

$$\lim_{p\to\infty} \left(\delta \ln p + 2p^{\delta} \ln p + p^{1/2+\delta} \ln(e + 2cp^{1/2-\delta}) + cp \ln c\right) = -\infty.$$

This is clearly satisfied since $0 < c < 1$. We obtain the desired asymptotic formula

$$N(f(x), r) = \mu_{k+m-r} \binom{p}{r} p^{k-r}(1 + o(1)).$$

■

Note that our asymptotic analysis here only considers the case $q = p$, k is large, m is small and r is large. It is certainly possible to find other range of parameters for which the same asymptotic formula holds. However, note that m must be bounded by $\sqrt{q}$ in order for our estimate gives a non-trivial estimate. To keep this paper focused, such finer analysis together with its applications to list decoding and bounded distance decoding will be discussed in a future work.

Beside coding theory, our result may have potential applications in number theory and graph theory. In number theory, it is a classical problem to understand the factorization pattern of a family of polynomials. In graph theory, it is related to the spectrum distribution of Wenger type graphs, see [3].

II. Proof of the Main Theorem

In this section we prove the following main result (Theorem 1.5 in Section 1).

Theorem 2.1: Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of $\deg(f) = k + m \le q - 1$. For all integers $0 \le r \le k + m$, we have

$$\left| N(f(x), r) - \mu_{k+m-r} \binom{q}{r} q^{k-r} \right| \le \sum_{j=k+1}^{k+m} \binom{j}{r} \binom{\frac{q}{p} + m\sqrt{q} + j}{j} \binom{m-1}{k+m-j} \sqrt{q}^{k+m-j}.$$

The main technique of the proof is a weighted sieving formula and the following counting lemma, which will be proved in Section 5.

Lemma 2.2: Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree $d = k + m \le q - 1$. Let $M(f, r)$ denote the number of pairs $(D_r, g(x))$ with D_r being a r-subset in $\mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$ of degree at most $k - 1$ satisfying

$$(f(x) + g(x))|_{D_r} \equiv 0.$$

Then for $k + 1 \le r \le d$, we have

$$\left| M(f, r) - \binom{q}{r} q^{k-r} \right| \le \binom{\frac{q}{p} + m\sqrt{q} + r}{r} \binom{m-1}{d-r} \sqrt{q}^{d-r}.$$

Proof of Theorem 2.1: The proof is based on two different kinds of inclusion-exclusion sievings. We shall let $g(x) \in \mathbb{F}_q[x]$ denote a polynomial of degree at most $k - 1$. For $c \in \mathbb{F}_q$, let P_c denote the property that $f(x) + g(x)$ has c as a root. For a subset $C \subseteq \mathbb{F}_q$, let N_C be the number of $g(x)$ such that $f(x) + g(x)$ has property P_c for each $c \in C$. The $|C| \times |C|$ Vandermonde matrix formed using the elements of C is non-singular. It follows by linear algebra that for $|C| \le k$, we have $N_C = q^{k-|C|}$. In the case $r = 0$, the inclusion-exclusion sieving [23] implies that

$$\begin{aligned} N(f, 0) &= q^k - \sum_{c\in\mathbb{F}_q} N_{\{c\}} + \cdots + (-1)^d \sum_{\{c_1,c_2,\ldots,c_d\}\subset\mathbb{F}_q} N_{\{c_1,c_2,\ldots,c_d\}} \\ &= q^k - \binom{q}{1} q^{k-1} + \binom{q}{2} q^{k-2} - \cdots + (-1)^k \binom{q}{k} q^0 \\ &+ \sum_{j=k+1}^{d} (-1)^j N_j, \end{aligned}$$

where N_j is the number of pairs $(D_j, g(x))$ with D_j being a j-subset in $\mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$ of degree at most $k - 1$ satisfying

$$(f(x) + g(x))|_{D_j} \equiv 0.$$

Applying Lemma 2.2, we have

$$\left| N(f, 0) - \sum_{i=0}^{k+m} (-1)^i \binom{q}{i} q^{k-i} \right| \le \sum_{j=k+1}^{d} \binom{\frac{q}{p} + m\sqrt{q} + j}{j} \binom{m-1}{d-j} \sqrt{q}^{d-j}.$$

This proves the theorem in the case $r = 0$. More generally, for $0 \le r \le d$, using the weighted inclusion-exclusion sieving formula, we deduce

$$\begin{aligned} N(f, r) &= \sum_{\{c_1,c_2,\ldots,c_r\}\subset\mathbb{F}_q} N_{\{c_1,c_2,\ldots,c_r\}} \\ &- \binom{r+1}{r} \sum_{\{c_1,c_2,\ldots,c_{r+1}\}\subset\mathbb{F}_q} N_{\{c_1,c_2,\ldots,c_{r+1}\}} + \cdots \\ &= \sum_{j=r}^{k} (-1)^{j-r} \binom{j}{r} \binom{q}{j} q^{k-j} + \sum_{j=k+1}^{d} (-1)^{j-r} \binom{j}{r} N_j. \end{aligned}$$

Applying Lemma 2.2 again, we have

$$\left| N(f, r) - \sum_{j=r}^{d} \binom{j}{r} \binom{q}{j} (-1)^{j-r} q^{k-j} \right| \le \sum_{j=k+1}^{d} \binom{j}{r} \binom{\frac{q}{p} + m\sqrt{q} + j}{j} \binom{m-1}{d-j} \sqrt{q}^{d-j}.$$

By the elementary properties of binomials, the main term can be rewritten and we obtain the following final form

$$\left| N(f, r) - \binom{q}{r} q^{k-r} \left(\sum_{j=0}^{d-r} (-1)^j \binom{q-r}{j} q^{-j} \right) \right| \le \sum_{j=k+1}^{d} \binom{j}{r} \binom{\frac{q}{p} + m\sqrt{q} + j}{j} \binom{m-1}{d-j} \sqrt{q}^{d-j}.$$

The theorem is proved. ■

III. A DISTINCT COORDINATE SIEVING FORMULA

In this section we introduce a sieving formula, which is a main technique for establishing Lemma 2.2 and might have its own interests. Roughly speaking, this formula significantly improves the classical inclusion-exclusion sieve in many distinct coordinates counting problems. We cite it here without proof. For details and related applications please refer to [17], [18].

Let Ω be a finite set, and let Ω^k be the Cartesian product of k copies of Ω. Let X be a subset of Ω^k. Define $\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, \forall i \neq j\}$. Let $f(x_1, x_2, \ldots, x_k)$ be a complex valued function defined over X and

$$F = \sum_{x \in \overline{X}} f(x_1, x_2, \ldots, x_k).$$

Many problems arising in number theory and coding theory are reduced to evaluate F very carefully. However, the direct inclusion-exclusion sieving has too many terms and thus usually produces too much errors. Roughly speaking, our formula describes what happens for those cancellations and make it possible to compute F explicitly.

Let S_k be the symmetric group on $\{1, 2, \ldots, k\}$. Each permutation $\tau \in S_k$ factorizes uniquely as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. Two permutations in S_k are conjugate if and only if they have the same type of cycle structure (up to the order). For $\tau \in S_k$, define the sign of τ to $\operatorname{sign}(\tau) = (-1)^{k-l(\tau)}$, where $l(\tau)$ is the number of cycles of τ including the trivial cycles. For a permutation $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$ with $1 \leq a_i, 1 \leq i \leq s$, define

$$X_\tau = \left\{(x_1, \ldots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \ldots\right\}. \qquad (1)$$

Similarly, for $\tau \in S_k$, define $F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k)$. Now we can state our sieve formula. We remark that there are many other interesting corollaries of this formula. For interested reader we refer to [17].

Theorem 3.1: Let F and F_τ be defined as above. Then

$$F = \sum_{\tau \in S_k} \operatorname{sign}(\tau) F_\tau. \qquad (2)$$

Note that the symmetric group S_k acts on Ω^k naturally by permuting coordinates. That is, for $\tau \in S_k$ and $x = (x_1, x_2, \ldots, x_k) \in \Omega^k$, $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)})$. A subset X in Ω^k is said to be symmetric if for any $x \in X$ and any $\tau \in S_k$, $\tau \circ x \in X$. For $\tau \in S_k$, denote by $\overline{\tau}$ the conjugacy class determined by τ and it can also be viewed as the set of permutations conjugated to τ. Conversely, for given conjugacy class $\overline{\tau} \in C_k$, denote by τ a representative permutation of this class. For convenience we usually identify these two symbols.

In particular, if X is symmetric and f is a symmetric function under the action of S_k, we then have the following simpler formula than (2).

Corollary 3.2: Let C_k be the set of conjugacy classes of S_k. If X is symmetric and f is symmetric, then

$$F = \sum_{\tau \in C_k} \operatorname{sign}(\tau) C(\tau) F_\tau, \qquad (3)$$

where $C(\tau)$ is the number of permutations conjugated to τ.

IV. BOUNDS ON CHARACTER SUMS

Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree $n > 0$. Let χ be a group homomorphism from $(\mathbb{F}_q[x]/(f(x)))^*$ to $\mathbb{C}^*$. We extend this definition to $\mathbb{F}_q[x]/(f(x))$ by defining $\chi(g) = 0$ for $\gcd(g, f) \neq 1$. Define

$$M_k(\chi) = \sum_{g \in \mathbb{F}_q[x], \text{monic}, \deg(g) = k} \chi(g).$$

Lemma 4.1: Assume that χ is non-trivial. Then for $k \geq 0$,

$$|M_k(\chi)| \leq \binom{n-1}{k} \sqrt{q}^k.$$

Furthermore, if $\chi(\mathbb{F}_q^*) = 1$, then for $n \geq 2$, we have

$$\left| \sum_{g \in \mathbb{F}_q[x], \text{monic}, \deg(g) \leq k} \chi(g) \right| \leq \binom{n-2}{k} \sqrt{q}^k.$$

Proof: The Dirichlet L-function of χ is

$$\begin{aligned} L(\chi, t) &= \sum_{g \in \mathbb{F}_q[x], \text{monic}} \chi(g) t^{\deg(g)} \\ &= \sum_{k=0}^{\infty} M_k(\chi) t^k \in 1 + t\mathbb{C}[[t]]. \end{aligned}$$

If $k \geq n$, for monic g of degree k, we can write uniquely $g = g_1 f + h$, where g_1 is monic in $\mathbb{F}_q[x]$, $\deg(g_1) = k - n$ and $h \in \mathbb{F}_q[x], \deg(h) \leq n - 1$. Thus in this case,

$$\begin{aligned} M_k(\chi) &= \sum_{g_1 \in \mathbb{F}_q[x], \text{monic}, \deg(g_1) = k-n} \ \sum_{\deg(h) \leq n-1} \chi(h) \\ &= q^{k-n} \sum_{h \in \mathbb{F}_q[x]/(f(x))} \chi(h) \\ &= 0. \end{aligned}$$

This implies

$$L(\chi, t) = \prod_{i=1}^{r} (1 - \rho_i t)$$

is a polynomial of degree $\leq n - 1$, i.e., $r \leq n - 1$. By the Weil bound ([24] Theorem 2.1),

$$|\rho_i| \leq \sqrt{q}.$$

It follows that for $0 \leq k \leq n - 1$,

$$|M_k(\chi)| \leq \binom{r}{k} \sqrt{q}^k \leq \binom{n-1}{k} \sqrt{q}^k. \qquad (4)$$

Now, note that $\sum_{g \in \mathbb{F}_q[x], \text{monic}, \deg(g) \leq k} \chi(g)$ is the coefficient of T^k in $L(\chi, T)/(1 - T)$. Let now χ be a non-trivial character but trivial on $\mathbb{F}_q^*$. Then $L(\chi, T)$ has the trivial factor $(1 - T)$ since $L(\chi, 1) = 0$. This means that $L(\chi, T)/(1 - T)$ is a polynomial of degree $n - 2$ [24]. Then by (4) one has

$$\left| \sum_{g \in \mathbb{F}_q[x], \text{monic}, \deg(g) \leq k} \chi(g) \right| \leq \binom{n-2}{k} \sqrt{q}^k.$$

■

V. Proof of Lemma 2.2

In this section we will prove Lemma 2.2. For convenicnec we state it again as the following independent theorem.

Theorem 5.1: Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree $d = k+m \leq q-1$. Let $M(f,r)$ denote the number of pairs $(D_r, g(x))$ with D_r being a r-subset in $\mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$ of degree at most $k-1$ satisfying

$$(f(x)+g(x))|_{D_r} \equiv 0.$$

Then for $k+1 \leq r \leq d$, we have

$$\left|M(f,r) - \binom{q}{r} q^{k-r}\right| \leq \binom{\frac{q}{p} + m\sqrt{q} + r}{r} \binom{m-1}{d-r} \sqrt{q}^{d-r}.$$

We first establish two lemmas which allows us to compute $M(f,r)$ through the method of character sums defined over a residue polynomial ring.

For $k \geq 0$, let P_k denote the set of all polynomials $h(x) \in \mathbb{F}_q[x]$ of degree at most k with $h(0) = 1$. Let χ be a character from $(\mathbb{F}_q[x]/(x^{m+1}))^*$ to $\mathbb{C}^*$. We extend this definition to $\mathbb{F}_q[x]/(x^{m+1})$ by defining $\chi(g) = 0$ for $(g, x^{m+1}) \neq 1$. Let G denote the group of all characters χ such that $\chi(\mathbb{F}_q^*) = 1$. This is an abelian group of order $|G| = q^m$. For any real number x and a positive integer r, define $(x)_r = x(x-1)\cdots(x-r+1)$ and let $(x)_0 = 1$.

Lemma 5.2: Let N_2 be the number of tuples $(x_1, \ldots, x_r, h) \in \mathbb{F}_q^r \times P_{d-r}$ such that $(1-x_1x)\cdots(1-x_rx)h(x) \equiv f(x) (\bmod\ x^{m+1})\}$, where the x_i's are required to be distinct. Assume that $f(0) = 1$. Then

$$\left|N_2 - (q)_r q^{k-r}\right| \leq (\frac{q}{p} + m\sqrt{q} + r - 1)_r \binom{m-1}{d-r} \sqrt{q}^{d-r}.$$

Proof:

$$\begin{aligned} N_2 &= \frac{1}{q^m} \sum_{(x_1,\ldots,x_r)\in\mathbb{F}_q^r, x_i\neq x_j} \sum_{h\in P_{d-r}} \\ &\sum_{\chi\in G} \chi((1-x_1x)\cdots(1-x_rx)h(x)/f(x)) \\ &= (q)_r q^{k-r} + \frac{1}{q^m} \sum_{1\neq\chi\in G} \chi^{-1}(f(x)) W(\chi), \end{aligned}$$

where

$$\begin{aligned} &W(\chi) \\ &= \sum_{(x_1,\ldots,x_r)\in\mathbb{F}_q^r, x_i\neq x_j} \sum_{h\in P_{d-r}} \chi((1-x_1x)\cdots(1-x_rx)h(x)). \end{aligned}$$

For each character χ, the function $\chi((1-x_1x)\cdots(1-x_rx))$ is clearly symmetric in the x_i's. Recall that for a permutation $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$ in the symmetric group S_r with $1 \leq a_i, 1 \leq i \leq s$, the subset X_τ of $X = \mathbb{F}_q^r$ is defined as in 1. Then a complex function $F_\tau(\chi)$ is defined:

$$F_\tau(\chi) = \sum_{(x_1,\ldots,x_r)\in X_\tau} \sum_{h\in P_{d-r}} \chi((1-x_1x)\cdots(1-x_rx)h(x)).$$

Thus by the sieving formula (2), one has

$$N_2 = (q)_r q^{k-r} + \frac{1}{q^m} \sum_{1\neq\chi\in G} \chi^{-1}(f(x)) \sum_{\tau\in S_r} \mathrm{sign}(\tau) F_\tau(\chi).$$

Thus it suffices to estimate $F_\tau(\chi)$ for non-trivial χ, where

$$F_\tau(\chi) = \left(\sum_{(x_1,\ldots,x_r)\in X_\tau} \prod_{i=1}^r \chi(1-x_ix) \right) \cdot \left(\sum_{h\in P_{d-r}} \chi(h(x)) \right).$$

We first estimate the second factor. Since χ is non-trivial, $\chi(\mathbb{F}_q^*) = 1$ and $\chi(x) = 0$, by Lemma 4.1 we deduce

$$\begin{aligned} &|\sum_{h\in P_{d-r}} \chi(h(x))| \\ &= |\sum_{h\in\mathbb{F}_q[x], \mathrm{monic}, \deg(h)\leq d-r} \chi(h(x))| \\ &\leq \binom{m-1}{d-r} \sqrt{q}^{d-r}. \end{aligned}$$

To estimate the first factor, we suppose τ is of type $(c_1, c_2, \ldots, c_r)$, where c_i is the number of i-cycles in τ for $1 \leq i \leq r$. Then the first factor of $F_\tau(\chi)$ is

$$\begin{aligned} G_\tau(\chi) &= \sum_{(x_1,\ldots,x_r)\in X_\tau} \prod_{i=1}^r \chi(1-x_ix) \\ &= (\sum_{a\in\mathbf{F}_q} \chi(1+ax))^{c_1} (\sum_{a\in\mathbf{F}_q} \chi^2(1+ax))^{c_2} \cdots (\sum_{a\in\mathbf{F}_q} \chi^r(1+ax))^{c_r} \\ &= \prod_{i=1}^r (\sum_{a\in\mathbf{F}_q} \chi^i(1+ax))^{c_i}. \end{aligned}$$

Define $m_i(\chi) = 1$ if $\chi^i = 1$ and $m_i(\chi) = 0$ if $\chi^i \neq 1$. By the Weil bound (see [24] Theorem 2.1) we deduce that

$$|G_\tau| \leq q^{\sum_{i=1}^r c_i m_i(\chi)} (m\sqrt{q})^{\sum_{i=1}^r c_i(1-m_i(\chi))}.$$

Since $X = \mathbb{F}_q^r$ is symmetric, by (3) we have

$$\begin{aligned} &N_2 - (q)_r q^{k-r} \\ &= \frac{1}{q^m} \sum_{1\neq\chi\in G} \chi^{-1}(f(x)) \sum_{\tau\in S_r} \mathrm{sign}(\tau) F_\tau(\chi) \\ &= \frac{1}{q^m} \sum_{1\neq\chi\in G} \chi^{-1}(f(x)) \sum_{\tau\in C_r} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) \\ &= \frac{1}{q^m} \sum_{\chi^d\neq 1, \forall 2\leq d\leq r} \chi^{-1}(f(x)) \sum_{\tau\in C_r} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) \\ &+ \frac{1}{q^m} \sum_{\chi\neq 1, \chi^d=1, \text{ for some } 2\leq d\leq r} \chi^{-1}(f(x)) \sum_{\tau\in C_r} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi). \end{aligned}$$

Let $S = \#\{\chi \in G \mid \chi \neq 1, \chi^d = 1 \text{ for some } 2 \leq d \leq r\}$. The last two terms were estimated by a combinatorial counting argument (see [18] page 2361). We thus obtain

$$\left|N_2 - (q)_r q^{k-r}\right| \leq w(S) \binom{m-1}{d-r} \sqrt{q}^{d-r},$$

where

$$w(S) = \frac{q^m - S}{q^m} ((m-1)\sqrt{q}+r-1)_r + \frac{S}{q^m} \cdot (\frac{q}{p} + (m-1)\sqrt{q}+r-1)_r.$$

If S is 0, we have the stronger estimate

$$\left|N_2 - (q)_r q^{k-r}\right| \leq ((m-1)\sqrt{q}+r-1)_r \binom{m-1}{d-r} \sqrt{q}^{d-r}.$$

In general, we have the weaker estimate

$$\left|N_2 - (q)_r q^{k-r}\right| \le \Big(\frac{q}{p}+(m-1)\sqrt{q}+r-1\Big)_r \binom{m-1}{d-r}\sqrt{q}^{d-r}.$$

■

Similarly, if we consider the counting problem in $\mathbb{F}_q^*$, then we will have a slightly different formula.

Lemma 5.3: Let N_2^* be the number of tuples $(x_1, \dots, x_r, h) \in \mathbb{F}_q^{*r} \times P_{d-r}$ such that $(1-x_1x)\cdots(1-x_rx)h(x) \equiv f(x)(\bmod\ x^{m+1})\}$, where we require that the x_i's are distinct. Then for $f(0)=1$, we have

$$\begin{aligned}&\left|N_2^* - (q-1)_r q^{k-r}\right| \\ &\le ((q-1)/p + m\sqrt{q} + r - 1)_r \binom{m-1}{d-r}\sqrt{q}^{d-r}.\end{aligned}$$

Now, we assume that $f(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree d. Suppose the top s coefficients of f are $\alpha = (a_{d-1}, \dots, a_k)$, i.e.,

$$f^\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_k x^k + \cdots .$$

For integer $k \ge 0$, let $\mathbb{F}_q[x]_k$ denote the set of polynomials $g \in \mathbb{F}_q[x]$ of degree at most k.

Proof of Theorem 5.1: Note that $M(f,r)$ equals the number of pairs $(D_r, g(x))$, where $D_r = (x_1, \dots, x_r)$ is an r-subset of $\mathbb{F}_q$ and $g \in \mathbb{F}_q[x]_{k-1}$ such that there is a unique monic $w(x) \in \mathbb{F}_q$ of degree $d-r$ satisfying

$$\begin{aligned}&x^d + a_{d-1}x^{d-1} + \cdots + a_k x^k + g(x) \\ &= (x-x_1)\cdots(x-x_r)w(x). \qquad (5)\end{aligned}$$

Clearly $M(f,r) = N_r^{\alpha,1}(d,m) + N_r^{\alpha,2}(d,m)$, where $N_r^{\alpha,1}(d,m)$ equals the number of such pairs $(D_r, g(x))$ with $D_r \subseteq \mathbb{F}_q^*$ and $N_r^{\alpha,2}$ equals the number of such pairs $(D_r, g(x))$ with D_r containing 0.

Suppose $x_1 = 0$, by dividing x on both sides of (5), it is easy to check $N_r^{\alpha,2}(d,m) = N_{r-1}^{\alpha,1}(d-1,m)$. It then suffices to count $N_r^{\alpha,1}(d,m)$.

Since now we have $x_i \in \mathbb{F}_q^*$, Substitute x by $1/x$ one has

$$\begin{aligned}&\frac{1}{x^d} + a_{d-1}\frac{1}{x^{d-1}} + \cdots + a_k\frac{1}{x^k} + g(\frac{1}{x}) \\ &= (\frac{1}{x}-x_1)(\frac{1}{x}-x_2)\cdots(\frac{1}{x}-x_r)w(\frac{1}{x}).\end{aligned}$$

Multiplying x^d on both sides we then have

$$\begin{aligned}&1 + a_{d-1}x + \cdots + a_k x^s + x^d g(\frac{1}{x}) \\ &= (1-x_1x)(1-x_2x)\cdots(1-x_rx)x^{d-r}w(\frac{1}{x}).\end{aligned}$$

Note that $h(x) = x^{d-r}w(\frac{1}{x})$ is a polynomial of degree $\le d-r$, $x^d g(\frac{1}{x})$ is a polynomial divisible by x^{m+1} and degree bounded by d. It suffices to count the number of pairs $(D_r, h(x))$, where $D_r = (x_1, \dots, x_r)$ is an r subset of $\mathbb{F}_q^*$ and $h(x) \in \mathbb{F}_q[x]$ of degree $\le d-r$ such that

$$\begin{aligned}&1 + a_{d-1}x + \cdots + a_k x^s \\ &\equiv (1-x_1x)(1-x_2x)\cdots(1-x_rx)h(x)(\bmod\ x^{m+1}).\end{aligned}$$

Thus, if we let N_2^* be defined as in Lemma 5.3, then

$$N_r^{\alpha,1}(d,m) = \frac{1}{r!}N_2^*.$$

It follows that

$$\begin{aligned}&\left|N_r^{\alpha,1}(d,m) - \binom{q-1}{r}q^{k-r}\right| \\ &\le \binom{\frac{q-1}{p} + m\sqrt{q} + r - 1}{r}\binom{m-1}{d-r}\sqrt{q}^{d-r}.\end{aligned}$$

Similarly, by the estimate in Lemma 5.2 one has

$$\begin{aligned}&\left|N_r^{\alpha,2}(d,m) - \binom{q-1}{r-1}q^{k-r}\right| \\ &\le \binom{\frac{q-1}{p} + m\sqrt{q} + r - 2}{r-1}\binom{m-1}{d-r}\sqrt{q}^{d-r}.\end{aligned}$$

Finally we conclude

$$\begin{aligned}&\left|M(f,r) - \left(\binom{q-1}{r} + \binom{q-1}{r-1}\right)q^{k-r}\right| \\ &\le \binom{\frac{q-1}{p} + m\sqrt{q} + r - 1}{r}\binom{m-1}{d-r}\sqrt{q}^{d-r} \\ &+ \binom{\frac{q-1}{p} + m\sqrt{q} + r - 2}{r-1}\binom{m-1}{d-r}\sqrt{q}^{d-r} \\ &\le \binom{\frac{q-1}{p} + m\sqrt{q} + r}{r}\binom{m-1}{d-r}\sqrt{q}^{d-r}.\end{aligned}$$

■

Remark: As we mentioned in the first section, our main results for standard Reed-Solomon codes extend to primitive Reed-Solomon codes with minor modification. In fact, in this case, things are simpler. What we need to count is exactly $\frac{1}{r!}N_2^*$, which is given in Lemma 5.3.

Acknowledgment

The authors would like to thank the anonymous referees and the editor for their constructive and valuable suggestions.

References

[1] Louay Bazzi. Weight distribution of cosets of small codes with good dual properties. *IEEE Trans. Inform. Theory*, 61(12):6493–6504, 2015.

[2] Antonio Cafure, Guillermo Matera, and Melina Privitelli. Singularities of symmetric hypersurfaces and Reed-Solomon codes. *Adv. Math. Commun.*, 6(1):69–94, 2012.

[3] Xiwang Cao, Mei Lu, Daqing Wan, Li-Ping Wang, and Qiang Wang. Linearized Wenger graphs. *Discrete Math.*, 338(9):1595–1602, 2015.

[4] Pascale Charpin. Weight distributions of cosets of two-error-correcting binary BCH codes, extended or not. *IEEE Trans. Inform. Theory*, 40(5):1425–1442, 1994.

[5] Pascale Charpin, Tor Helleseth, and Victor A. Zinoviev. The coset distribution of triple-error-correcting binary primitive BCH codes. *IEEE Trans. Inform. Theory*, 52(4):1727–1732, 2006.

[6] Pascale Charpin and Victor Zinoviev. On coset weight distributions of the 3-error-correcting BCH-codes. *SIAM J. Discrete Math.*, 10(1):128–145, 1997.

[7] Qi Cheng and Elizabeth Murray. On deciding deep holes of Reed-Solomon codes. In *Theory and applications of models of computation*, volume 4484 of *Lecture Notes in Comput. Sci.*, pages 296–305. Springer, Berlin, 2007.

[8] Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM J. Comput.*, 37(1):195–209, 2007.

[9] Qi Cheng and Daqing Wan. Complexity of decoding positive-rate primitive Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 56(10):5217–5222, 2010.

[10] Qi Cheng and Daqing Wan. A deterministic reduction for the gap minimum distance problem. *IEEE Trans. Inform. Theory*, 58(11):6935–6941, 2012.

[11] Venkatesan Guruswami and Alexander Vardy. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. *IEEE Trans. Inform. Theory*, 51(7):2249–2256, 2005.

[12] Masaaki Harada. On the complete coset weight distributions of extremal formally self-dual even codes. *Bull. Yamagata Univ. Natur. Sci.*, 16(3):71–79, 2007.

[13] Masaaki Harada and Takuji Nishimura. On the complete coset weight distribution of the extremal self-dual $[46, 23, 10]$ code. *IEEE Trans. Inform. Theory*, 51(7):2700–2702, 2005.

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

[15] Arnold Knopfmacher and John Knopfmacher. Counting polynomials with a given number of zeros in a finite field. *Linear and Multilinear Algebra*, 26(4):287–292, 1990.

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

[17] Jiyou Li and Daqing Wan. A new sieve for distinct coordinate counting. *Sci. China Math.*, 53(9):2351–2362, 2010.

[18] Jiyou Li and Daqing Wan. Counting subset sums of finite abelian groups. *J. Combin. Theory Ser. A*, 119(1):170–182, 2012.

[19] Qunying Liao. On Reed-Solomon codes. *Chin. Ann. Math. Ser. B*, 32(1):89–98, 2011.

[20] Michio Ozeki. On covering radii and coset weight distributions of extremal binary self-dual codes of length 40. *Theoret. Comput. Sci.*, 235(2):283–308, 2000. Combinatorics and optimization (Okinawa, 1996).

[21] Michio Ozeki. On covering radii and coset weight distributions of extremal binary self-dual codes of length 56. *IEEE Trans. Inform. Theory*, 46(7):2359–2372, 2000.

[22] Michio Ozeki and Katsushi Waki. Complete coset weight distributions of second order Reed-Muller code of length 64. *J. Math-for-Ind.*, 3A:1–20, 2011.

[23] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[24] Daqing Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.

[25] Haiyan Zhou, Li-Ping Wang, and Weiqiong Wang. Counting polynomials with distinct zeros in finite fields. *J. Number Theory*, 174:118–135, 2017.

[26] Jincheng Zhuang, Qi Cheng, and Jiyou Li. On determining deep holes of generalized Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 62(1):199–207, 2016.

Jiyou Li received the B.S. degree in Mathematics from Yunnan University in 2001, the M.S. degree in Mathematics from Beijing Normal University in 2004 and the Ph.D. degree in Mathematics from Peking University in 2008.

He joined the Shanghai Jiao Tong University in 2008, where he is now an Associate Professor of Mathematics. His research interests include number theory, coding theory and combinatorics.

Daqing Wan received the B.S. degree from Chengdu Institute of Geology in 1982, the M.S. degree from Sichuan University in 1986, and the Ph.D. degree from the University of Washington in Seattle in 1991.

He joined the University of California at Irvine in 1997, where he is now a Professor of Mathematics. His research interests include number theory, coding theory, algorithms and complexity.