Improved Error Bounds for the Distance Distribution of Reed-Solomon Codes

Zhicheng Gao and Jiyou Li, Member, IEEE

Abstract—We use the generating function approach to derive simple expressions for the factorial moments of the distance distribution over Reed-Solomon codes. We obtain better upper bounds for the error term of a counting formula given by Li and Wan, which gives nontrivial estimates on the number of polynomials over finite fields with prescribed leading coefficients and a given number of linear factors. This improvement leads to new results on the classification of deep holes of Reed-Solomon codes.

Index Terms—Reed-Solomon codes, distance distributions, deep holes, polynomials with prescribed leading coefficients.

I. INTRODUCTION

The theory of error-correcting codes plays an important role in modern communications. One particular and important class is the Reed-Solomon code, which is defined by polynomials evaluations on a given subset in a finite field. Since the invention by Reed and Solomon in 1960s, Reed-Solomon codes are by far the most fundamental examples of evaluation codes and the most widely studied linear codes.

Let \( F_q \) be the finite field with \( q \) elements of characteristic \( p \). Let \( D = \{ x_1, \cdots, x_n \} \) be a subset in \( F_q \) of cardinality \( n \). For \( 1 \leq k \leq n \), the Reed-Solomon code \( R_S_{n,k} \) has the codewords of the form

\[
(f(x_1), \cdots, f(x_n)) \in F_q^n,
\]

where \( f(x) \) runs over all polynomials in \( F_q[x] \) of degree bounded by \( k-1 \). The (Hamming) distance between two words \( u, v \), denoted by \( d(u,v) \), is the number of non-zero entries in \( u - v \). For the Reed-Solomon code, the distance between two codewords represented by polynomials \( f(x) \) and \( g(x) \) is \( n \) minus the number of distinct roots of \( f(x) - g(x) \) in \( D \), or equivalently the number of distinct linear factors \( x - \alpha \) with \( \alpha \in D \). The minimum distance of the Reed-Solomon code is \( n - k + 1 \) since a non-zero polynomial of degree no more than \( k-1 \) has at most \( k-1 \) zeroes. For \( u = (u_1, u_2, \cdots, u_n) \in F_q^n \), one associates a unique polynomial \( u(x) \in F_q[x] \) of degree at most \( n-1 \) such that \( u(x_i) = u_i \), given by the Lagrange interpolation formula

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

Define \( \deg(u) \) to be the degree of the associated polynomial \( u(x) \) of \( u \). Note that \( u \) is a codeword if and only if \( \deg(u) \leq k - 1 \).

For a given word \( u \in F_q^n \), define its distance to the code by

\[
d(u, R_S_{n,k}) := \min\{d(u, v) : v \in R_S_{n,k}\}.
\]

The maximum likelihood decoding of \( u \) is to find a codeword \( v \in R_S_{n,k} \) such that \( d(u, v) = d(u, R_S_{n,k}) \). Thus, the computation of \( d(u, R_S_{n,k}) \) is essentially the decision version for the maximum likelihood decoding problem, which is NP-complete for general subset \( D \subset F_q \) [7]. For standard Reed-Solomon code, i.e., \( D = F_q \), the complexity of the maximum likelihood decoding is unknown to be NP-complete. This is an important open problem. It has been shown by Cheng-Wan [4] to be at least as hard as the discrete logarithm problem in a large finite extension of \( F_q \).

When \( \deg(u) \leq k - 1 \), then \( u \) is a codeword and thus \( d(u, R_S_{n,k}) = 0 \). We shall assume that \( k \leq \deg(u) \leq n - 1 \). The following result given by Li and Wan [9] gives an elementary bound for \( d(u, R_S_{n,k}) \).

Theorem 1: Let \( u \in F_q^n \) be a word such that \( k \leq \deg(u) \leq n - 1 \). Then,

\[
n - \deg(u) \leq d(u, R_S_{n,k}) \leq n - k.
\]

A. The Deep Hole Conjecture

A received word \( u \) is called a deep hole if \( d(u, R_S_{n,k}) = n-k \), that is, \( u \) realizes the covering radius. When \( \deg(u) = k \), the upper bound in Theorem 1 agrees with the lower bound and thus \( u \) must be a deep hole. This gives \((q-1)q^k\) deep holes. For a Reed-Solomon code \( R_S_{n,k} \), it is very difficult to determine if a given word \( u \) is a deep hole. In the special case that \( \deg(u) = k + 1 \), the deep hole problem is equivalent to the subset sum problem over \( F_q \) which is NP-complete if \( p > 2 \).

For the standard Reed-Solomon code, that is, \( D = F_q \), and thus \( n = q \), there is the following interesting conjecture studied by Cheng-Murray [3].

Conjecture 1 (Deep Hole Conjecture): For the standard Reed-Solomon code with \( D = F_q \), the set \( \{ u \in F_q^n | \deg(u) = k \} \) gives the set of all deep holes.

0018-9448 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
To state some of the progresses we need the following definition.

**Definition 1:** Given a monic polynomial \( f(x) \in \mathbb{F}_q[x] \) of degree \( k + \ell \) and an integer \( 0 \leq r \leq k + \ell \), let \( N(f(x), r) \) be 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 \( \mathbb{F}_q \). Then the deep hole conjecture is equivalent to the statement that the inequality

\[
N(f(x), r) > 0, \quad \text{for some } r > k
\]

holds for any \( f(x) \) of degree \( k + \ell \) and any \( \ell \geq 1 \). In particular, studying when the special case \( N(f(x), k + 1) > 0 \) holds for a wider range of parameters will providing sufficient conditions for \( f(x) \) not to be a deep hole.

Using tools from finite geometry and additive combinatorics, Zhang, Li and Cheng proved that the deep hole conjecture holds for \( k \leq p - 1 \) or \( q = p + 1 \leq k \leq q - 2 \). In particular, the conjecture holds when \( q = p \) is prime. Kaipa [8] improved this result and he proved that the deep hole conjecture holds for \( k \geq \frac{q - 1}{2} \).

Using tools from number theory and algebraic geometry, Cheng and Murray [3] proved that their conjecture is true if for any positive constant \( \epsilon, 1 < k < q^{1/\epsilon} \) and \( 1 < q^{1/\epsilon} - \epsilon \). There are a series of results on this problem along this direction. Li and Wan [13] proved that the conjecture is true if \( k \leq q^{3/8} \) and \( \ell = o(q^{3/8}) \). A different proof was given by Cafure, Matera and Privitelli [2] with tools from algebraic geometry. A refined result was given by Liao [14].

A received word \( u \) is called **ordinary** if \( d(u, RS_{n,k}) = n - \deg u \), that is, \( u \) realizes the lower bound in Theorem 1. Thus a degree \( k + \ell \) word \( u \) is ordinary if and only if

\[
N(u(x), k + \ell) > 0.
\]

The first result holds for Reed-Solomon codes of positive information rate is the following theorem [15].

**Proposition 1 (Zhu-Wan):** Let \( u \in \mathbb{F}_q^n \) be a received word. Suppose \( \deg u = k + \ell \) and \( 1 \leq \ell \leq q - k - 1 \). Then there are constants \( c_1, c_2 \) such that \( d(u, RS_{n,k}) \leq q - k - r \) for \( \ell < c_1 q^2 \) and \( \left( \frac{3 + \ell}{2} + 1 \right) \log_2 q < k < c_2 q \).

In particular, there are constants \( c_1, c_2 \) such that the Conjecture 1 holds for \( \ell < c_1 q^2 \) and \( \left( \frac{3 + \ell}{2} + 1 \right) \log_2 q < k < c_2 q \). In fact, here \( c_1 + c_2 < \frac{1}{2} \) (See the formula at the bottom of page 222, [15]).

In this paper, we improve Zhu-Wan’s above result by allowing the information rate \( k/q \) to be any constant in \((0,1)\). Our main results are the following two theorems. Theorem 2(a) gives a sufficient condition for a received word \( f \) to be ordinary, and Theorem 2(b) gives a sufficient condition for \( f \) not to be a deep hole. We note that the RHS of (2) is smaller than that of (1).

**Theorem 2:** Let \( q \) be a power of a prime \( p \) and \( f \) be a monic polynomial of degree \( k + \ell \).

(a) Let \( c = (k + \ell)/q \). We have \( d(f, RS_{n,k}) = q - k - \ell \) provided that

\[
\frac{(p-1)c}{p} \ln \frac{1}{c} + (1-c) \ln \frac{1}{1-c} - \frac{1+c}{p} \ln (1+c) 
\geq (\ell - 1) \left( \ln \frac{q}{q} + \frac{\ln (2p)}{\sqrt{q}} \right) + \frac{2}{3q} + \frac{3 \ln q}{2q}.
\]

(b) Let \( c = (k + 1)/q \). We have \( d(f, RS_{n,k}) \leq q - k - 1 \) provided that

\[
\frac{(p-1)c}{p} \ln \frac{1}{c} + (1-c) \ln \frac{1}{1-c} - \frac{1+c}{p} \ln (1+c) 
\geq (\ell - 1) \left( \ln \frac{q}{q} + \ln (2p) \right) + \frac{2}{3q} + \frac{3 \ln q}{2q}.
\]

**Theorem 3:** Let \( q \) be a power of a prime \( p \) and \( f \) be a monic polynomial of degree \( k + \ell \).

(a) For any constant \( c \in (0,1) \), there are positive constants \( p_0, q_0, \gamma_0 \) (depending on \( c \)) such that \( d(f, RS_{n,k}) = q - k - \ell \), provided that \( p \geq p_0, q \geq q_0, \) and \( \ell \leq 1 + \gamma_0 \sqrt{q} \).

(b) For each prime \( p \), there are positive constants \( q_0, \gamma_0 \) (depending on \( p \)) such that \( d(f, RS_{n,k}) = q - k - \ell \), provided that \( 3 \leq k + \ell \leq 0.7q, q \geq q_0, \) and \( \ell \leq 1 + \gamma_0 \sqrt{q} \).

Note that in the above theorem, the asymptotic information rate \( c \) can be any positive constant in \((0,1)\). This is much stronger than the result of Proposition 1 in most cases.

More details about the numerical values of these parameters including the cases for \( p \in \{2,3,5,7\} \) can be found in Corollaries 1 and 2 in Section 4.

**B. Preliminaries and Notations**

Our approach follows that of [6] using generating functions. The coefficients of the generating functions are from the group algebra generated by equivalence classes consisting of polynomials with prescribed leading coefficients.

Throughout the paper, we shall use the notations from [6], which are summarized below.

- For the finite field \( \mathbb{F}_q \), let \( q = p^k \) for some prime \( p \) and \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \).
- For \( f \in \mathbb{F}_q[x] \), \( [x^d]f \) denotes the coefficient of \( x^d \) in \( f \).
- \( M \) denotes the set of monic polynomials in \( \mathbb{F}_q[x] \), \( M_d \) denotes the set of polynomials of degree \( d \) in \( M \).
- Fix a positive integer \( \ell \). Two polynomials \( f, g \in M \) are **equivalent** if they have the same \( \ell \) leading coefficients, that is

\[
x^{\deg(f) - j} f(x) = x^{\deg(g) - j} g(x), \quad 1 \leq j \leq \ell,
\]

or (in a more compact form)

\[
x^{\deg(f)} f(1/x) \equiv x^{\deg(g)} g(1/x) \pmod{x^{\ell+1}}.
\]

This defines an equivalence relation, and we use \( \langle f \rangle \) to denote the equivalence class represented by \( f \). We also use \( E \) to denote the set of all equivalence classes, and \( M_d(\varepsilon) \) denotes the set of polynomials in \( M_d \) in the equivalence class \( \varepsilon \).

The remaining paper is organized as follows. In Section 2 we recall the generating functions obtained in [6] for \( N(f, r) \) for general \( D \subseteq \mathbb{F}_q \). Simple expressions are derived for the factorial moments of the distance between a given received word and a random codeword in \( RS_{n,k} \). In Section 3 we focus on the standard Reed-Solomon code \( RS_{n,k} \) and use the character sum bounds from [12] to derive a sharper error bound for the factorial moments. Proofs of our main results are given in Section 4. Section 5 concludes our paper.
II. GENERATING FUNCTIONS AND MOMENTS OF DISTANCE DISTRIBUTION OVER REED-SOLOMON CODES

For \( \varepsilon \in \mathcal{E} \), let \( N_d(\varepsilon, r) \) denote the number of polynomials in \( \mathcal{M}_d(\varepsilon) \) which contain exactly \( r \) distinct zeros in the given set \( D \). Define generating functions

\[
F(z) = \sum_{f \in \mathcal{M}} \langle f \rangle z^{|\text{deg}(f)|},
\]

\[
G(z, u) = \sum_{\varepsilon \in \mathcal{E}} \sum_{d, r \geq 0} N_d(\varepsilon, r) z^d u^r.
\]

It is convenient to introduce the following element in the group algebra \( \mathbb{C}E \):

\[
E = \frac{1}{q^1} \sum_{\varepsilon \in \mathcal{E}} \varepsilon.
\]

It is easy to see that (see, e.g., [6])

\[
E \varepsilon = E, \quad E^2 = E, \quad \forall \varepsilon \in \mathcal{E}.
\]

We shall use the following result [6]:

**Proposition 2:** Let \( E \) be defined by (3). Then

\[
F(z) = \sum_{d=0}^{\ell-1} \sum_{f \in \mathcal{M}_d} \langle f \rangle z^d + \frac{(qz)^\ell}{1 - qz} E,
\]

\[
G(z, u) = F(z) \prod_{\alpha \in D} ((1 + (u - 1)z)(x + \alpha)).
\]

In the rest of the paper, we shall use the Iverson bracket \( \lfloor P \rfloor \), which has value 1 if the predicate \( P \) is true and 0 otherwise. Let \( D_j \) denote the set of all \( j \)-subsets of \( D \). The following result can be found in [6], we include a short proof here for self completeness.

**Theorem 4:** The number of polynomials in \( \mathcal{M}_d(\varepsilon) \) containing exactly \( r \) linear factors is given by

\[
N_d(\varepsilon, r) = \binom{n}{r} q^{d-r} \sum_{j=0}^{d-r} \binom{n-r}{j} (-q)^{-j}
\]

\[
+ \sum_{j=d-\ell+1}^d \binom{j}{r} (-1)^{j-r} W_j(\varepsilon),
\]

where

\[
W_j(\varepsilon) = \sum_{\eta \in \mathcal{E}_{d-j}} \sum_{S \in D_j} \left\lfloor \eta \prod_{\alpha \in S} (x + \alpha) = \varepsilon \right\rfloor.
\]

**Proof:** For \( \varepsilon \in \mathcal{E} \), let \( [\varepsilon^d] G(z, u) \) denote the coefficient of \( z^d \varepsilon \) in the generating function \( G(z, u) \). Using (4) and (6), we obtain

\[
G(z, u) = \frac{(qz)^\ell}{1 - qz} (1 + (u - 1)z)^n E
\]

\[
+ \left( \sum_{j=0}^{\ell-1} \sum_{j \in \mathcal{M}_d} \langle f \rangle \prod_{\alpha \in D} ((1 + (u - 1)z)(x + \alpha)))
\]

\[
\left[ z^d \varepsilon \right] G(z, u) = \frac{(z^d - e)}{1 - qz} (1 + (u - 1)z)^n
\]

\[
+ \sum_{j=d-\ell+1}^d (u - 1)^j [\varepsilon] \sum_{\eta \in \mathcal{E}_{d-j}} \left\lfloor \eta \prod_{\alpha \in S} (x + \alpha) = \varepsilon \right\rfloor.
\]

It follows that

\[
N_d(\varepsilon, r) = \sum_{j=0}^{d-\ell} \binom{n}{j} q^{d-r-j} \binom{u}{r}(u - 1)^j
\]

\[
+ \sum_{j=d-\ell+1}^d W_j(\varepsilon)(u - 1)^j.
\]

Changing the summation index \( j := j + r \) in the first sum in (11) and using

\[
\binom{n}{j} \binom{j}{r} = \binom{n}{r} \binom{n-r}{j-r},
\]

we complete the proof.

**Theorem 5:** Let \( D' \) denote the set of all \( j \)-tuples of distinct elements of \( D \). We note

\[
W_j(\varepsilon) = \sum_{\eta \in \mathcal{E}_{d-j}} \sum_{S \in D_j} \left\lfloor \eta \prod_{\alpha \in S} (x + \alpha) = \varepsilon \right\rfloor
\]

\[
= \frac{1}{j!} \sum_{\eta \in \mathcal{E}_{d-j}} \sum_{\varepsilon \in \mathcal{E}_{d-j}} \left\lfloor \eta \prod_{\alpha \in S} (x + \alpha) = \varepsilon \right\rfloor.
\]

Theorem 4 was used in [6] to obtain explicit expressions of \( N_f(\varepsilon, r) \) for \( \ell \leq 2 \) and the first two moments of the distance distribution.

Let \( \mathbb{E}(X) \) denote the expected value of a random variable \( X \). We shall use \( n \mathbb{E} \) to denote the falling factorial \( n(n - 1) \cdots (n - m + 1) \). Our next result gives all the factorial moments expressed in terms of \( W_j(\varepsilon) \). This extends the corresponding results in [6] for the first two moments.

**Theorem 5:** Let \( Z := Z(f, g) \) denote the distance between a received word represented by \( f \in \mathcal{M}_{k+\ell} \) and a random codeword \( g \) in \( \mathcal{R}S_{n,k} \) (under uniform distribution, that is, each word in \( \mathcal{R}S_{n,k} \) is chosen with probability \( q^{-k} \)). Let \( Y := n - Z \), and \( \varepsilon \in (f) \). We have

\[
\mathbb{E}(Y^{m}) = \left\lfloor m \leq k \right\rfloor n^m q^{-m}
\]

\[
+\left\lfloor k + 1 \leq m \leq k + \ell \right\rfloor q^{-k} m! W_m(\varepsilon).
\]

**Proof:** Using (9), we obtain the following probability generating function of \( Y \):

\[
p_{k+\ell}(u) = q^{-k} [z^n \varepsilon] G(z, u)
\]

\[
= \sum_{j=0}^{k} q^{-j} \binom{n}{j} (u - 1)^j + q^{-k} \sum_{j=k+1} W_j(\varepsilon)(u - 1)^j.
\]
Hence
\[ 
\mathbb{E}(Y_{\text{var}}) = \left. \frac{d^m}{du^m} p_{k+\ell}(u) \right|_{u=1} \\
= \binom{n}{m} q^{-m} + [k+1 \leq m \leq k+\ell] q^{-k} m! W_m(\varepsilon). 
\]

\[ \square \]

III. STANDARD REED-SOLOMON CODE

In this section we deal with standard Reed-Solomon code, that is, \( D = \mathbb{F}_q \) and hence \( n = q \). We also set \( d = k + \ell \).

In this case \( W_j(\varepsilon) \) can be estimated using Weil bounds on character sums. We first rewrite (13) as

\[ W_j(\varepsilon) = \sum_{\eta \in \mathbb{F}_q^{k+\ell-j}} \sum_{x \in \mathbb{F}_q^j} \eta \prod_{i=1}^j (x + x_i) = \varepsilon. \tag{15} \]

As in [12], \( W_j(\varepsilon) \) can be evaluated using the “coordinate-sieve formula”. And a more detailed combinatorial argument on the distinct coordinates sieving is given in [10], [11] by different methods. The corresponding error terms can be expressed in terms of the following function, which appears in the exponential generating function of permutations with respect to two different types of cycle lengths. Let \( S_m \) denote the set of all permutations of \( 1, 2, \ldots, m \). For \( \tau \in S_m \), define \( l(\tau) \) to be the total number of cycles of \( \tau \) and \( l'(\tau) \) to be the number of cycles of \( \tau \) which are not multiples of \( p \). The standard generating function argument gives [5], [6]

\[ \sum_{m \geq 0} \frac{1}{m!} \sum_{\tau \in S_m} u^{l(\tau)} w^{l'(\tau)} z^m = \exp \left( u \sum_{j \geq 1; 1 \not| j} \frac{z^j}{j} + uw \sum_{j \geq 1; 1 \not| j} \frac{z^j}{j} \right) = (1 - z)^{-uw} (1 - z^p)^{- (u - uw)/p}. \]

As in [6], we define

\[ A_j(u, w) = \frac{1}{j!} \sum_{\tau \in S_j} u^{l(\tau)} w^{l'(\tau)} = [z^j] \left( 1 - z)^{-uw} (1 - z^p)^{- (u - uw)/p} \right) = \sum_{0 \leq i \leq j/p} (uw + j - ip - 1) \binom{(u - uw)/p + i - 1}{i}. \tag{18} \]

Define

\[ q_1 = \min \{ q, (\ell - 1)\sqrt{q} \}. \tag{19} \]

Then we have the following estimate. Proposition 3: Let \( \varepsilon \in \mathcal{E} \). Then

\[ |W_j(\varepsilon) - \binom{q}{j} q^{k-j}| \leq (1 - q^{-\ell}) \binom{\ell - 1}{\ell + k - j} q^{(\ell + k - j)/2} A_j(q, q_1/q). \tag{20} \]

Proof: Let \( \hat{\mathcal{E}} \) denote the set of characters over the group \( \mathcal{E} \). Then by orthogonality of the characters, we have

\[ W_j(\varepsilon) = \sum_{\eta \in \mathbb{F}_q^{k+\ell-j}} \sum_{x \in \mathbb{F}_q^j} \chi(\eta \prod_{i=1}^j (x + x_i)) = \binom{q}{j} q^{k-j} \sum_{\chi \not\equiv 1} \sum_{\eta \in \mathbb{F}_q^{k+\ell-j}} \chi(\eta) \sum_{x \in \mathbb{F}_q^j} \prod_{i=1}^j (x + x_i)). \tag{21} \]

The sum in (15) can be estimated using Weil bound on character sums as shown in [12]. We note that \( \sum_{\eta \in \mathbb{F}_q} \chi(\eta) \) is the same as \( M_k(\chi) \) in [12], and hence

\[ \left| \sum_{\eta \in \mathbb{F}_q^{k+\ell-j}} \chi(\eta) \right| \leq \left( \frac{\ell - 1}{k + \ell - j} \right) q^{(k + \ell - j)/2} \tag{22} \]

The character sums involving the linear factors are the same as the corresponding ones given in [12], and the estimate of \( G_\tau \) in [12] gives

\[ \left| \sum_{x \in \mathbb{F}_q^j} \chi(\eta \prod_{i=1}^j (x + x_i)) \right| \leq \sum_{\tau \in S_j} q^{l'(\tau)} q_1^{l(\tau)} = j! A_j(q, q_1/q). \tag{23} \]

Substituting (22) and (23) into (21), we complete the proof. \( \square \)

Using Theorem 1 and Proposition 3, we immediately obtain the following.

Theorem 6: Assume \( D = \mathbb{F}_q \). The number \( N_{k+\ell}(\varepsilon, r) \) of monic polynomials of degree \( k + \ell \) containing exactly \( r \) zeros in \( \mathbb{F}_q \) with leading coefficients \( \varepsilon \) satisfies

\[ N_{k+\ell}(\varepsilon, r) - \binom{q}{r} q^{k-r} \sum_{j=0}^{k+\ell-r} \binom{q - r}{j} (-q)^{-j} \leq (1 - q^{-\ell}) \sum_{j=k+1}^{k+\ell} \binom{j}{r} (k - \ell - j) q^{(k + \ell - j)/2} A_j(q, q_1/q). \tag{24} \]

We note that this is essentially [12, Theorem 1.5] except that our \( A_j(q, q_1/q) \) replaces their factor \( \binom{q}{j} q_1^{j-1} \).

\[ \left( \frac{q}{p} + q_1 + j - 1 \right) \tag{25} \]

IV. PROOF OF THE MAIN RESULTS

The following lemma provides a much sharper upper bound for \( A_j(q, q_1/q) \) than the binomial number in (25). It will be used to prove our main results.

Lemma 1: Let \( q_1 = \min \{ q, (\ell - 1)\sqrt{q} \}, \gamma = q_1/q \) and \( c := j/q \). We have

\[ \ln A_j(q, q_1/q) \leq \frac{j}{p} \ln \frac{q + j}{j} + \frac{q - q_1}{q} \ln \left( 1 + \frac{q}{q_1} \right) - q_1 \ln \left( 1 - \frac{j}{q + j} \right)^{1/p}. \tag{26} \]
It follows that, for (16), we have

$$p$$

For example, when (26), we have

$$A_j(q, q_1/q) \geq 0, \quad (j \geq 0).$$

By (16), we have

$$A_j(q, q_1/q) \geq 0, \quad (j \geq 0).$$

It follows that, for $$0 < y < 1$$,

$$A_j(q, q_1/q) \leq y^{-j}(1 - y)^{-q_1} (1 - y^p)^{-q_1 (1 - q_1)/p},$$

$$\ln A_j(q, q_1/q) \leq -j \ln y - q_1 \ln(1 - y) - \frac{q - q_1}{2} \ln (1 - y^p).$$

(28)

To minimize the above upper bound, we choose $$y$$ near the solution to the following saddle point equation

$$\frac{j}{y} + q_1 \frac{1}{1 - y} + (q - q_1) \frac{y^{p-1}}{1 - y^p} = 0,$$

i.e.,

$$q_1 \frac{y}{1 - y} + (q - q_1) \frac{y^{p-1}}{1 - y^p} = j.$$ (29)

When $$q_1$$ is much smaller than $$q$$, we may choose

$$y = \left(\frac{j}{q + j}\right)^{1/p}$$

to be an approximate solution to (29). Substituting this into (28), we obtain (26).

Noting

$$e^{-t} \leq 1 - \frac{3t}{4} (0 \leq t \leq 0.6)$$

(30)

we obtain

$$\left(\frac{j}{q + j}\right)^{1/p} = \exp\left(-\frac{1}{p} \ln \frac{q + j}{j}\right) \leq \exp\left(-\frac{\ln 2}{p}\right) \leq 1 - \frac{3 \ln 2}{4p},$$

$$- \ln \left(1 - \left(\frac{j}{q + j}\right)^{1/p}\right) \leq - \ln \frac{3 \ln 2}{4p} \leq \ln(2p).$$

(31)

Substituting (31) into (26), we obtain (27).

**Remark:** Bound (27) is sufficient for our purpose. One can derive sharper bounds depending on the ranges of $$p, q, \gamma, c$$.

For example, when $$p = 2$$,

$$y(\gamma, c) = \frac{\sqrt{\gamma^2 + 4c^2 + 4\gamma - \gamma}}{2(1 + c)}$$

is the exact solution to the saddle point equation, which can be used to obtain a sharper estimate for $$A_j(q, q_1/q)$$ than (26). When $$\gamma$$ is close to 1, a different choice of $$y$$ gives better estimate for $$A_j(q, q_1/q)$$ than (26).

The following inequality [1, (5)] will be used to estimate binomial numbers.

$$\binom{n}{m} \geq e^{-1/6} \left(\frac{n}{2\pi m(n - m)}\right)^{1/2} \left(\frac{n}{m}\right)^{m} \left(\frac{n}{m - n}\right)^{n - m}.$$ (32)

**Remark:** We may use (32) to show

$$\ln \left(\frac{q/p + q_1 + j - 1}{j}\right) - \ln A_j(q, q_1/q) \to \infty$$

when $$j = cq$$ and $$q_1 = o(q)$$.

If $$p = q$$ then it follows from (18) that

$$\ln \left(\frac{q/p + q_1 + j - 1}{j}\right) - \ln A_j(q, q_1/q) = \ln \left(\frac{(q_1 + j)^{q_1 + j - 1}}{(q_1 + j - 1)^{q_1 + j - 1}}\right) = \ln \frac{q_1 + j}{q_1} \to \infty.$$ (33)

When $$q \geq p^2$$, we apply (32) to obtain

$$\ln \left(\frac{q/p + q_1 + j - 1}{j}\right) \geq cq \ln \left(\frac{1 + cp}{cp} + \frac{q}{p}\ln(1 + cp)\right).$$

It follows from (27) that, if $$q \geq p^2$$, then

$$\ln \left(\frac{q/p + q_1 + j - 1}{j}\right) - \ln A_j(q, q_1/q) > \frac{q}{p} \ln 1 + c \to \infty.$$ (34)

**Theorem 7:** Let $$q$$ be a power of a prime $$p$$, $$\gamma = (\ell - 1)q^{-1/2} \leq 1$$, and $$f \in M_k + \ell$$.

(a) Let $$c = (k + \ell)/q$$. We have $$d(f, RS_{q,k}) = q - k - \ell$$ provided that

$$\left(\frac{p - 1}{p}\right)^{c} \ln 1 + (1 - c) \ln \frac{1}{1 - c} - \frac{1 + c}{p} \ln(1 + c)$$

$$- \left(\frac{1}{6q} + \frac{\ln q}{q} + \frac{1}{2q} \ln(2q\pi(1 - c))\right)$$

$$\geq \gamma \left(\frac{\ln q}{\sqrt{q}} + \ln(2p) - \frac{1}{p} \ln(1 + c)\right).$$

(b) Let $$c = (k + 1)/q$$. We have $$d(f, RS_{q,k}) \leq q - k - 1$$ provided that

$$\left(\frac{p - 1}{p}\right)^{c} \ln 1 + (1 - c) \ln \frac{1}{1 - c} - \frac{1 + c}{p} \ln(1 + c)$$

$$- \left(\frac{1}{6q} + \frac{\ln q}{q} + \frac{1}{2q} \ln(2q\pi(1 - c))\right)$$

$$\geq \gamma \left(\frac{\ln q}{c\sqrt{c}} + \ln(2p) - \frac{1}{p} \ln(1 + c)\right).$$

(35)

**Proof:** For simplicity, define

$$f(p, c) = \left(\frac{p - 1}{p}\right)^{c} \ln 1 + (1 - c) \ln \frac{1}{1 - c}$$

$$- \frac{1 + c}{p} \ln(1 + c),$$

$$g(q, c) = \frac{1}{6q} + \frac{\ln q}{q} + \frac{1}{2q} \ln(2q\pi(1 - c)).$$
For part (a), we substitute
\[
h_1(p, q, c) = \frac{\ln q}{\sqrt{q}} + \ln(2p) - \frac{1}{p} \ln(1+c),
\]
\[
h_2(p, q, c) = \frac{\ln q}{2\sqrt{q}} + \ln(2p) - \frac{1}{p} \ln(1+c).
\]

For \(k+1 \leq r \leq k+\ell\), we first note
\[r!\mathbb{P}(Y \geq r) \leq \mathbb{E}(Y^r) \leq (k+\ell)^r \mathbb{P}(Y \geq r),\]
and hence \(\mathbb{P}(Y \geq r) > 0\) if and only if \(\mathbb{E}(Y^r) > 0\). It follows from (14) and (20) that \(\mathbb{P}(Y \geq r) > 0\) if
\[
\left(\frac{q}{r}\right) \geq \left(\frac{\ell-1}{\ell + k-r}\right)^{q(r+\ell-k)/2} A_r(q, q, q). \tag{36}
\]

For \(c = r/q\), we use (32) to obtain
\[
\ln \left(\frac{q}{r}\right) \geq q \left( c \ln \frac{1}{c} + (1-c) \ln \frac{1}{1-c} \right) - \frac{1}{2} \ln(2qpc(1-c)) - \frac{1}{6}. \tag{37}
\]

For part (a), we substitute \(r = k + \ell\) into (36) to obtain
\[
\left(\frac{q}{k+\ell}\right) \geq q^{\ell} A_{k+\ell}.
\]

Taking the logarithm on both sides, using (27) and (37), and dividing by \(q\), we obtain the following sufficient condition for \(\mathbb{P}(Y \geq k + \ell) > 0:\)
\[
c \ln \frac{1}{c} + (1-c) \ln \frac{1}{1-c} - \frac{1}{2} \ln(2qpc(1-c)) - \frac{1}{6} q \geq \frac{\ell \ln q}{q} + \frac{c}{p} \ln \frac{1}{c} + \frac{1-c}{q} \ln(1+c) + \gamma \ln(2p).
\]

Now (34) follows by noting \(\mathbb{P}(Y = k + \ell) = \mathbb{P}(Y \geq k + \ell)\) and \(\ell = 1 + \gamma \sqrt{q}\).

For part (b), we substitute \(r = k + 1\) into (36) to obtain
\[
\left(\frac{q}{k+1}\right) \geq q^{\ell+1}/2 A_{k+1}.
\]

Now (35) follows from the same argument as in part (a) with \(h_2\) replacing \(h_1\).

The following figure shows the intervals where \(f(p, c) \geq 0\) for \(p \in \{2, 3, 5, 7, 17\}\).

The next two corollaries provide some precise ranges of \(c\) for \(p \leq 7\). Since the deep hole conjecture has been verified for \(k \geq \lfloor (p-1)/2 \rfloor\), we focus on \(k \leq (p-2)/2\) in Corollary 1.

**Corollary 1:** Let \(q\) be a power of a prime \(p, c = (k+\ell)/q\) and \(\gamma = (\ell-1)/\sqrt{q}\). Let \(f(p, c), g(q, c), h_2(p, q, c)\) be defined in the proof of Theorem 7. Then \(d(f, R_{S_{q,k}}) = q - k - \ell\) for each of the following cases.

(a) \(p = 2, q \geq 2^5, 3 \leq c \leq \frac{q-2}{2}\), \(\gamma \leq \frac{f(p, c) - g(q, c)}{h_2(p, q, c)}\),

(b) \(p = 3, q \geq 3^3, 1 \leq c \leq \frac{q-2}{2}\), \(\gamma \leq \frac{f(p, c) - g(q, c)}{h_2(p, q, c)}\),

(c) \(p = 5, q \geq 5^2, 1 \leq c \leq \frac{q-2}{2}\), \(\gamma \leq \frac{f(p, c) - g(q, c)}{h_2(p, q, c)}\),

(d) \(p \geq 7, q \geq 1, 1 \leq c \leq \frac{q-2}{2}\), \(\gamma \leq \frac{f(p, c) - g(q, c)}{h_2(p, q, c)}\).

**Proof:** We first note
\[
\frac{\partial^2}{\partial c^2} (f(p, c) - g(q, c)) = \frac{1 + c}{c(c-1)} + \frac{c}{c^p} + \frac{1 - 2c + 2c^2}{2q^c(1-c)^2} \leq \frac{1 + c}{c} + \frac{1 - 2c + 2c^2}{2c^2(1-c)^2} \quad \text{using } p \geq 2, q \geq 1/c
\]
\[
= \frac{2c^2 + 3c^3 - 3}{2(1+c)(1-c)^2} < 0. \quad \text{if } 0 \leq c \leq 0.68.
\]

Hence for given \(p, q,\) each \(f(p, c) - g(q, c)\) is concave down on \([0, 0.5]\). Thus we only need to verify \(f(p, c) - g(q, c) > 0\) at the end points of the respective interval.

For part (a) we have
\[
f(2, 0.5) - g(0.5, 0.5) > 0.041, \quad f(2, 4/4) - g(4/4, 4/4) > 0.0187. \quad (q \geq 32)
\]

For part (b) we have
\[
f(3, 0.5) - g(0.5, 0.5) > 0.1772, \quad f(3, 2/4) - g(2/4, 2/4) > 0.0005. \quad (q \geq 27)
\]

For part (c) we have
\[
f(5, 0.5) - g(0.5, 0.5) > 0.2933, \quad f(5, 2/4) - g(2/4, 2/4) > 0.0373. \quad (q \geq 25)
\]

For part (d) we have \(f(p, c) > f(7, c)\) if \(p > 7\), and
\[
f(7, 0.5) - g(0.5, 0.5) > 0.0837, \quad f(7, 2/4) - g(2/4, 2/4) > 0.0424. \quad (q \geq 7)
\]

**Corollary 2:** Let \(q\) be a power of a prime \(p, c = (k+\ell)/q, \gamma, f(p, c), g(q, c)\) and \(h_1(p, q, c)\) be as defined in the proof of Theorem 7. Then \(d(f, R_{S_{q,k}}) = q - k - \ell\) for each of the following cases.

(a) \(p = 2, q \geq 2^8, 3 \leq c \leq 0.7, \gamma \leq \frac{f(p, c) - g(p, 1/2)}{h_1(p, q, c)}\),

(b) \(p = 3, q \geq 3^4, 3 \leq c \leq 0.8, \gamma \leq \frac{f(p, c) - g(p, 1/2)}{h_1(p, q, c)}\),
(c) \( p = 5, q \geq 5^3, \frac{2}{q} \leq c \leq 0.9, \quad \gamma \leq \frac{f(p,c) - g(q,1/2)}{h_1(p,q,c)} \),
\[ (d) \quad p \geq 7, q \geq 7^4, \frac{2}{q} \leq c \leq 0.95, \quad \gamma \leq \frac{f(p,c) - g(q,1/2)}{h_1(p,q,c)}. \]

**Proof:** The proof is similar to that of Corollary 1. To maximize the range of \( c \), we use the bound \( g(q,c) \leq g(q,1/2) \), and note that \( f(p,c) \) is concave up on \((0,1)\) for each \( p \geq 2 \). Hence for given \( p, q \) we only need to verify \( f(p,c) - g(q,1/2) > 0 \) at the end points of the respective interval.

For part (a) we have

\[ f(2,0.7) - g(q,0.5) > 0.0009, \]
\[ f(2,3/q) - g(q,1/2) > 0.0069. \quad (q \geq 2^8) \]

For part (b) we have

\[ f(3,0.8) - g(q,1/2) > 0.002, \]
\[ f(3,3/q) - g(q,1/2) > 0.0189. \quad (q \geq 3^4) \]

For part (c) we have

\[ f(5,0.5) - g(q,1/2) > 0.0011, \]
\[ f(5,2/q) - g(q,1/2) > 0.0044. \quad (q \geq 5^3) \]

For part (d) we have \( f(p,c) > f(7,c) \) if \( p > 7 \), and

\[ f(7,0.95) - g(q,1/2) > 0.0004, \]
\[ f(7,2/q) - g(q,1/2) > 0.0007. \quad (q \geq 7^4) \]

**Proof of Theorem 2 and Theorem 3:** Theorem 2 follows immediately from Theorem 7 by noting

\[ g(q,c) \leq g(q,1/2) \leq \frac{2}{3q} + \frac{3 \ln q}{2q}. \]

For Theorem 3(a), we may set \( p_0 = \frac{1+c}{1-c} \). Then, for \( p \geq p_0 \), we have

\[ f(p,c) \geq \frac{c}{2} \ln \left( \frac{1}{c} \right) + \left( 1 - c - \frac{1+c}{p} \right) \ln (1+c) \geq \frac{c}{2} \ln \frac{1}{c}. \]

Choosing a sufficiently large positive \( q_0 \) such that

\[ \frac{2}{3q_0} + \frac{3 \ln q_0}{2q_0} < \frac{c}{2} \ln \frac{1}{c}, \]

and setting \( \gamma_0 = (f(p_0,c) - g(q_0,1/2))/h_1(p_0,q_0,0) \), we obtain Theorem 3(a).

Theorem 3(b) follows from Corollary 2 by setting \( q_0 = 7^4 \) and \( \gamma_0 = (f(p_0,c) - g(q_0,1/2))/h_1(p_0,q_0,0) \).

V. CONCLUSION

In this paper we used the generating function approach to derive simple expressions of the factorial moments of the distance distribution over RS\(_{n,k}\). This recovers the Li-Wan’s counting formula. We also apply the saddle point estimate to derive a sharper bound on the error term. This improves the previous estimate and leads to several new applications on deep hole problem and ordinary words problem.

**ACKNOWLEDGMENT**

The authors would like to thank Prof. Daqing Wan and the anonymous referees for their constructive and valuable suggestions which improve the presentation of the article.

**REFERENCES**

[1] B. Bollobás, *Random Graphs*. New York, NY, USA: Academic, 1985.
[2] M. Privitelli, G. Matera, and A. Cafure, “Singularity of symmetric hypersurfaces and Reed–Solomon codes,” *Adv. Math. Commun.*, vol. 6, no. 1, pp. 69–94, Jan. 2012.
[3] Q. Cheng and E. Murray, “On deciding deep holes of Reed–Solomon codes,” in *Theory and Applications of Models of Computation* (Lecture Notes in Computer Science), vol. 4484. Berlin, Germany: Springer, 2007, pp. 296–305.
[4] Q. Cheng and D. Wan, “On the list and bounded distance decodability of Reed–Solomon codes,” *SIAM J. Comput.*, vol. 37, no. 1, pp. 195–209, Jan. 2007.
[5] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[6] Z. Gao, “Counting polynomials over finite fields with prescribed leading coefficients and linear factors,” *Finite Fields Their Appl.*, vol. 82, Sep. 2022, Art. no. 102052.
[7] V. Guruswami and A. Vardy, “Maximum-likelihood decoding of Reed–Solomon codes is NP-hard,” in *Proc. 16th Annu. ACM-SIAM Symp. Discrete Algorithms*, New York, NY, USA, 2005, pp. 470–478.
[8] K. Kaipa, “Deep holes and MDS extensions of Reed–Solomon codes,” *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4940–4948, Aug. 2017.
[9] J. Li and D. Wan, “On the subset sum problem over finite fields,” *Finite Fields Appl.*, vol. 14, no. 4, pp. 911–929, 2008.
[10] J. Li and D. Wan, “A new sieve for distinct coordinate counting,” *Sci. China Math.*, vol. 53, no. 9, pp. 2351–2362, 2010.
[11] J. Li and D. Wan, “Counting subset sums of finite Abelian groups,” *J. Combinat. Theory, A*, vol. 119, no. 1, pp. 170–182, 2012.
[12] J. Li and D. Wan, “Distance distribution in Reed–Solomon codes,” *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2743–2750, May 2020.
[13] Y. Li and G. Zhu, “On the error distance of extended Reed–Solomon codes,” *Adv. Math. Commun.*, vol. 10, no. 2, pp. 413–427, Apr. 2016.
[14] Q. Liao, “On Reed–Solomon codes,” *Chin. Ann. Math. B*, vol. 32, pp. 89–98, Jan. 2010.
[15] G. Zhu and D. Wan, “Computing error distance of Reed–Solomon codes,” in *Theory and Applications of Models of Computation* (Lecture Notes in Computer Science), vol. 7287. Berlin, Germany: Springer, 2012, pp. 214–224.

Zhicheng Gao received the B.S. degree in mathematics from Nanjing University, China, in 1984, and the Ph.D. degree in mathematics from the University of California at San Diego, USA, in 1989.

He spent two years at the University of Waterloo as a Post-Doctoral Fellow and joined Carleton University, Ottawa, Canada, in 1992. His main research interests include enumerative combinatorics, graph theory, and games of chance.

Jiyou Li (Member, IEEE) received the B.S. degree in mathematics from Yunnan University in 2004, and the Ph.D. degree in mathematics from the University of California at San Diego, USA, in 1989.

He joined Shanghai Jiao Tong University in 2008, where he is currently a Professor in mathematics. He spent half a year (September 2012–February 2013) with the University of Delaware as a Visiting Scholar and one year (March 2015–March 2016) with the Massachusetts Institute of Technology as a Visiting Associate Professor. His research interests include number theory, combinatorics, and algebraic coding theory.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.