Computing Error Distance of Reed-Solomon Codes

Guizhen Zhu*

Institute For Advanced Study

Tsinghua University, Beijing, 100084, P.R. China

Email:zhugz08@mails.tsinghua.edu.cn

Daqing Wan

Department of Mathematics

University of California, Irvine, CA 92697-3875, USA

Email:dwan@math.uci.edu

Abstract

Under polynomial time reduction, the maximun likelihood decoding of a linear code is equivalent to computing the error distance of a received word. It is known that the decoding complexity of standard Reed-Solomon codes at certain radius is at least as hard as the discrete logarithm problem over certain large finite fields. This implies that computing the error distance is hard for standard Reed-Solomon codes. Using the Weil bound and a new sieve for distinct coordinates counting, we are able to compute the error distance for a large class of received words. This significantly improves previous results in this direction. As a corollary, we also improve the existing results on the Cheng-Murray conjecture about the complete classification of deep holes for standard Reed-Solomon codes.

Keywords: Reed-Solomon code, deep hole, character sum, distinct coordinates counting.

1 Introduction

There is always a possibility that a signal is corrupted when transferred over a long distance. Error-detecting and error-correcting codes alleviate the problem and make the modern communication possible. The Reed-Solomon codes are very popular in engineering a reliable channel due to their simplicity, burst error correction capabilities, and the powerful decoding algorithms within small error distance they admit.

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. For positive integers $k < n \leq q$, the generalized Reed-Solomon code, denoted by C, can be thought of as a map from

*This work is partially supported by NSF of the USA and by the National Natural Science Foundation of China (Grant No.60910118, and 61133013)

$\mathbb{F}_q^k \to \mathbb{F}_q^n$, in which a message $(a_1, a_2, \ldots, a_k)$ is mapped to a vector $(f(x_1), f(x_2), \ldots, f(x_n))$, where $f(x) = a_k x^{k-1} + a_{k-1} x^{k-2} + \cdots + a_1 \in \mathbb{F}_q[x]$ and $\{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{F}_q$ is called the evaluation set. It is obvious that C is a linear subspace of $\mathbb{F}_q^n$ with dimension k. When the evaluation set is the whole field $\mathbb{F}_q$, the resulting code is called the standard Reed-Solomon code, denoted by C_q. In the literature, the standard Reed-Solomon code is often called the extended Reed-Solomon code. This name can be confused (to us) to the generalized Reed-Solomon code.

The *Hamming distance* between two codewords is the number of coordinates in which they differ. The *error distance* of a received word $u \in \mathbb{F}_q^n$ to the code is the minimum Hamming distance of u to codewords. A *Hamming ball* of radius m is the set of vectors within Hamming distance m to some vector in $\mathbb{F}_q^n$. The *minimum distance* of a code is the smallest distance between any two distinct codewords, and is a measure of how many errors the code can correct or detect. The *covering radius* of a code is the maximum possible distance from any vector in $\mathbb{F}_q^n$ to the closest codeword. A deep hole is a vector which achieves this maximum. The minimum distance of generalized Reed-Solomon codes is $n - k + 1$. The covering radius of generalized Reed-Solomon codes is $n - k$.

1.1 Related Work

The pursuit of efficient decoding algorithms for Reed-Solomon codes has yielded intriguing results. If the radius of a Hamming ball centered at a received word is less than half the minimum distance, there can be at most one codeword in the Hamming ball. Finding this unique codeword (if it exists) is called *unambiguous decoding*. It can be efficiently solved by the classical Berlekamp-Massey algorithm [1]. If the radius is somewhat larger, but less than $n - \sqrt{n(k-1)}$, the number of codewords is of polynomial size. In this case, the decoding problem can be efficiently solved by the Guruswami-Sudan list decoding algorithm [6], which outputs all the codewords inside a Hamming ball. If the radius is stretched further, the number of codewords in a Hamming ball may be exponential. We then study the bounded distance decoding problem, which outputs just one codeword in a Hamming ball of certain radius. More importantly, we can remove the restriction on radius and investigate the maximum likelihood decoding problem, which is the problem of computing a closest codeword to a given vector in $\mathbb{F}_q^n$.

The complexity for decoding Reed-Solomon codes has also attracted attention recently. Guruswami and Vardy [7] proved that the maximum likelihood decoding of generalized Reed-Solomon codes is NP-hard. In fact, the weaker problem of deciding deep holes for generalized Reed-Solomon codes is already co-NP-complete, see [3]. In the much more interesting case of standard Reed-Solomon codes, it is unknown if decoding remains NP-hard. This is still an open problem. Cheng and Wan [4] [5] managed to prove that the decoding problem of standard Reed-Solomon codes at certain radius is at least as hard as the discrete logarithm problem over a large extension of a finite field. This is the only complexity result that is known for decoding the standard Reed-Solomon code.

Our aim of this paper is to study the problem of computing the error distance of the standard Reed-Solomon code. We shall use algebraic methods. For this purpose, we first define the notion

of the degree of a received word. For $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, let

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

That is, $u(x)$ is the unique (Lagrange interpolation) polynomial of degree at most $n-1$ such that $u(x_i) = u_i$ for $1 \leq i \leq n$. For $u \in \mathbb{F}_q^n$, we define $\deg(u) = \deg(u(x))$, called the degree of u. It is clear that $d(u, C) = 0$ if $\deg(u) \leq k-1$. Without loss of generality, we can assume that $k \leq \deg(u) \leq n-1$ and $u(x)$ is monic. We have the following simple bound.

Proposition 1.1 *[3] For $k \leq \deg(u) \leq n-1$, we have the inequality*

$$n - \deg(u) \leq d(u, C) \leq n - k.$$

This result shows that if $\deg(u) = k$, then $d(u, C) = n - k$ and thus u is a deep hole. As mentioned before, it is NP-hard to determine when $d(u, C) = n - k$ (the deep hole problem) for generalized Reed-Solomon codes. Thus, we will restrict our attention to the most natural and important case, namely the standard Reed-Solomon code C_q. Even in this restricted case, we cannot expect a complete solution to the problem of computing the error distance, as it is at least as hard as the discrete logarithm in a large finite field. However, we expect that a lot more can be said for standard Reed-Solomon codes. For instance, Cheng and Murray [3] conjectured the following complete classification of deep holes for standard Reed-Solomon codes.

Conjecture 1.2 (Cheng-Murray) *All deep holes for standard Reed-Solomon codes are those words satisfying* $\deg(u) = k$. *In other words, a received word u is a deep hole for C_q iff* $\deg(u) = k$.

The deep hole problem for generalized Reed-Solomon codes is NP-hard. In contrast, the Cheng-Murray conjecture implies that the deep hole problem for the standard Reed-Solomon code can be solved in polynomial time. A complete proof of this conjecture (if correct) seems rather difficult at present. As a theoretical evidence, they proved that their conjecture is true if $d := deg(u) - k$ is small and q is sufficiently large compared to $d + k$. More precisely, they showed

Proposition 1.3 *[3] Let $u \in \mathbb{F}_q^q$ such that $1 \leq d := \deg(u) - k \leq q - 1 - k$. Assume that $q \geq \max(k^{7+\epsilon}, d^{\frac{13}{3}+\epsilon})$ for some constant $\epsilon > 0$. Then $d(u, C_q) < q - k$, that is, u is not a deep hole.*

The method of Cheng-Murray is to reduce the problem to the existence of a rational point on a hypersurface over $\mathbb{F}_q$. They showed that the resulting hypersurface is absolutely irreducible and then applied an explicit version of the Lang-Weil theorem. However, they did not obtain the exact value of $d(u, C_q)$, only the weaker inequality $d(u, C_q) < q - k$. Li and Wan [11] improved their results using Weil's character sum estimate and the approach of Cheng-Wan [4] as follows.

Proposition 1.4 *[11] Let $u \in \mathbb{F}_q^q$ such that $1 \leq d := \deg(u) - k \leq q - 1 - k$. If*

$$q > \max((k+1)^2, d^{2+\epsilon}),\ k > \left(\frac{2}{\epsilon} + 1\right) d + \frac{8}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $d(u, C_q) < q - k$, that is, u is not a deep hole. If

$$q > \max\left((k+1)^2, (d-1)^{2+\epsilon}\right),\ k > \left(\frac{4}{\epsilon} + 1\right)d + \frac{4}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $d(u, C_q) = q - (k + d)$.

Note that the last part of the proposition determines the exact error distance $d(u, C_q)$ under a suitable hypothesis. Using a similar character sum approach, Qunying Liao [12] unified the above two results of Li-Wan and proved the following extension.

Proposition 1.5 *[12] Let $r \geq 1$ be an integer. For any received word $u \in \mathbb{F}_q^q$, $r \leq d := \deg u - k \leq q - 1 - k$. If*

$$q > \max\left(2\binom{k+r}{2} + d, d^{2+\epsilon}\right),\ \ k > \left(\frac{2}{\epsilon} + 1\right)d + \frac{2r+4}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $d(u, C_q) \leq q - k - r$.

In a recent preprint, Antonio Cafure etc. [2] uses a much more sophisticated algebraic-geometry approach and obtains a slightly improvement of one of the Li-Wan results.

Proposition 1.6 *[2] Let $u \in \mathbb{F}_q^q$ such that $1 \leq d := \deg(u) - k \leq q - 1 - k$. Assume that*

$$q > \max\left((k+1)^2, 14d^{2+\epsilon}\right),\ k > d\left(\frac{2}{\epsilon} + 1\right),$$

for some constant $\epsilon > 0$. Then $d(u, C_q) < q - k$, that is, u is not a deep hole.

Again, this result gives only the inequality $d(u, C_q) < q - k$, not the exact value of the error distance $d(u, C_q)$.

1.2 Our results

In this paper, we prove the following result.

Theorem 1.7 *Let $r \geq 1$ be an integer and $u \in \mathbb{F}_q^q$ such that $r \leq d := \deg(u) - k \leq q - 1 - k$. There are positive constants c_1 and c_2 such that if*

$$d < c_1 q^{1/2}, (\frac{d+r}{2} + 1)\log_2 q < k < c_2 q,$$

then $d(u, C_q) \leq q - k - r$.

Actually, our results are more general in the sense that it works for words represented by low degree rational functions, not just low degree polynomials, see Theorem 3.2 for details. Under the condition of $k > (\frac{d+r}{2} + 1)\log_2 q$, Theorem 1.7 has significantly improved the result of Proposition 1.5 as we weaken the condition $k < q^{\frac{1}{2}}$ in Proposition 1.5 to $k < c_2 q$ for some constant c_2. Put it in another way, our result now works for codes with positive information rate, while Proposition 1.5 only works for codes with information rate going to zero. Taking $r = 1$ or d in Theorem 1.7, we obtain similar significant improvements of Li-Wan's results as follows.

Corollary 1.8 *Let $u \in \mathbb{F}_q^q$ such that $1 \le d := \deg(u) - k \le q - 1 - k$. There are positive constants c_1 and c_2 such that if*

$$d < c_1 q^{1/2}, (\frac{d+3}{2}) \log_2 q < k < c_2 q,$$

then $d(u, C_q) < q - k$; and if

$$d < c_1 q^{1/2}, (d+1) \log_2 q < k < c_2 q,$$

then $d(u, C_q) = q - k - d$.

Compared with Proposition 1.4, Corollary 1.8 weakened the condition from $k < \sqrt{q}$ to $k < c_2 q$ under the assumption $k > (d+1)\log_2 q$. This result shows that we can determine the exact error distance for a much larger class of received words.

In our proof, we convert the problem of deciding the error distance of a received word to a polynomial congruence equation. Compared with the geometric approach in [2][3], our method is simpler and it gives stronger results. We use Weil's character sum estimate [14] and Li-Wan's new sieve for distinct coordinates counting [9] to estimate the number of solutions of the congreunce. Compared with the classical inclusion-exclusion principle used in [11] and [12], the Li-Wan's new sieve for distinct coordinates counting has more advantages on decreasing the number of error terms and improving the accuracy of estimating. As a result, we are able to deduce a much weaker sufficient condition for determining the error distance of a received word.

2 Preliminaries

2.1 Character sums and the Weil bound

We first review the theory of character sums in the form we need. Let $\mathbb{F}_q[x]$ be the polynomial ring in one variable over $\mathbb{F}_q$ and $h(x)$ be a fixed irreducible polynomial in $\mathbb{F}_q[x]$ of degree $0 \le h < m - k + 1$, where $m > k$. Let $\overline{h}(x) = x^{m-k+1} h(\frac{1}{x})$. Then $\overline{h}(x)$ is a polynomial in $\mathbb{F}_q[x]$ with degree $m - k + 1$, and divisible by x.

Let $\chi : (\mathbb{F}_q[x]/(\overline{h}(x)))^* \longrightarrow \mathbb{C}^*$ be a multiplicative character from the invertible elements of the residue class ring to the non-zero complex numbers. For $g \in \mathbb{F}_q[x]$, define

$$\chi(g) = \begin{cases} \chi(g \mod \overline{h}(x)), & \text{if } \gcd(g, \overline{h}(x)) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

This defines a multiplicative function of the polynomial ring $\mathbb{F}_q[x]$. We need the following form of the Weil bound as given in [14].

Proposition 2.1 *(Weil) If $\chi \ne 1$ but $\chi(\mathbb{F}_q^*) = 1$, then*

$$\left| \sum_{\substack{g \in \mathbb{F}_q[x], g(0)=1 \\ \deg(g) = m-(k+r)}} \Lambda(g)\chi(g) \right| \le (m-k) q^{\frac{m-(k+r)}{2}}.$$

and

$$\left|1+\sum_{\substack{g \text{ monic}\\ \deg(g)=m-k+r}}\Lambda(g)\chi(g)\right| \le (m-k-1)q^{\frac{m-(k+r)}{2}},$$

where $\Lambda(g)$ *is the Von-Mangoldt function on* $\mathbb{F}_q[x]$*, i.e.* $\Lambda(g)$ *is equal to* $\deg P$ *if* g *is a power of an irreducible polynomial* P *and equal to zero otherwise.*

2.2 Li-Wan's new sieve

Let D be a finite set. For a positive integer k, let $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let X be a subset of D^k. Denote

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, i \neq j\}.$$

Let $f(x_1, x_2, \ldots, x_k)$ be a complex valued function defined over X. Denote

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

Let S_k be the symmetric group on $\{1, 2, \ldots, k\}$. Each permutation $\tau \in S_k$ can be uniquely factorized as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. Namely,

$$\tau = (i_1 i_2 \ldots i_{a_1})(j_1 j_2 \ldots j_{a_2}) \ldots (l_1 l_2 \ldots l_s).$$

with $a_i \ge 1, 1 \le i \le s$. Define

$$X_\tau = \{(x_1, \ldots, x_k) \in X \mid x_{i_1} = \cdots = x_{i_{a_1}}, x_{j_1} = \cdots = x_{j_{a_2}}, \ldots, x_{l_1} = \cdots = x_{l_{a_s}}\}.$$

Similarly, we can define

$$F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k).$$

We say that τ is of type $(c_1, c_2, \ldots, c_k)$ if it has exactly c_i cycles of length i. Let $N(c_1, c_2, \ldots, c_k)$ be the number of permutations of type $(c_1, c_2, \ldots, c_k)$. Define

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum i c_i = k} N(c_1, c_2, \ldots, c_k) t_1^{c_1} t_2^{c_2} \ldots t_k^{c_k}.$$

We have the following combinational formula:

Lemma 2.2 *Suppose* $q \ge d$*, if* $t_i = q$ *for* $d|i$ *and* $t_i = s$ *for* $d \nmid i$*, then we have*

$$\begin{aligned} C_k(s, \ldots, s, q, s, \ldots, s, q, \ldots) &= k! \sum_{i=0}^{\lfloor k/d \rfloor} \binom{\frac{q-s}{d} + i - 1}{i} \binom{s + k - di - 1}{k - di} \\ &\le (s + k + (q-s)/d - 1)_k. \end{aligned}$$

where $(x)_k = x(x-1)\ldots(x-k+1)$.

Definition 2.3 *X is called symmetric if for any $x \in X$ and any $g \in S_k$, we have $g \circ x \in X$.*

Definition 2.4 *A complex-valued function f defined on X is called normal on X if X is symmetric and for any two S_k conjugate elements τ and τ' in S_k, we have*

$$\sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k) = \sum_{x \in X_{\tau'}} f(x_1, x_2, \ldots, x_k).$$

Proposition 2.5 *If f is normal on X, then we have*

$$F = \sum_{\sum ic_i = k} (-1)^{k - \sum c_i} N(c_1, c_2, \ldots, c_k) F_\tau.$$

3 Main theorem and its proof

The following lemma is immediate from the definition of the error distance.

Lemma 3.1 *Let $u \in \mathbb{F}_q^q$ be a word with $\deg(u) = k + d$, where $k + 1 \le k + d \le q - 1$. Then, the error distance $d(u, C_q) \le q - k - r$ for some $1 \le r \le d$ iff there exists a subset $\{x_{i_1}, x_{i_2}, \ldots, x_{i_{k+r}}\} \subset \mathbb{F}_q$ and a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $d - r$ such that*

$$u(x) - v(x) = (x - x_{i_1})(x - x_{i_2}) \ldots (x - x_{i_{k+r}}) g(x)$$

for some $v(x) \in \mathbb{F}_q[x]$ with $\deg(v(x)) \le k - 1$.

Fix an ordering $\mathbb{F}_q = \{x_1, \ldots, x_q\}$. Our main result is the following

Theorem 3.2 *Let $r \ge 1$ be an integer and let $u \in \mathbb{F}_q^q$ be a received word. Denote*

$$m = \min \left\{ \deg w(x) \,\middle|\, \begin{array}{l} \left(\frac{w(x_1)}{h(x_1)}, \frac{w(x_2)}{h(x_2)}, \ldots, \frac{w(x_q)}{h(x_q)}\right) = u, \text{for some } h(x) \in \mathbb{F}_q[x], \\ (h(x), x^q - x) = 1, \ \deg h(x) + k \le \deg w(x) \le q - 1. \end{array} \right\}$$

Let $r \le d := m - k \le q - 1 - k$. There are positive constants c_1 and c_2 such that if

$$d < c_1 q^{1/2}, (\frac{d + r}{2} + 1) \log_2 q < k < c_2 q,$$

then $d(u, C_q) \le q - k - r$.

Taking $h(x) = 1$ in the theorem, we have $w(x) = u(x)$ and obtain the simpler polynomial case stated in the introduction section.

Proof of Theorem. Suppose $w(x)$ is the polynomial with degree m, and $h(x)$ is the corresponding irreducible polynomial satisfying the definition of m. Shifting u by a constant codeword if necessary, we may assume that $w(0) \neq 0$. Let $\overline{h}(x) = x^{m-k+1} h(\frac{1}{x})$. This is a polynomial of degree

$m-k+1=d+1$. Let $A=(\mathbb{F}_q[x]/(\overline{h}(x)))^*$ and $\hat{A}$ denote the group of all characters of A. Let $\hat{B}=\{\chi\in\hat{A}\mid\chi(\mathbb{F}_q^*)=1\}$, an abelian subgroup of order $\leq q^d$.

By Lemma 3.1, we know that $d(u,C_q)\leq q-k-r$ if and only if there exists a polynomial $f(x)\in\mathbb{F}_q[x]$ with $\deg f(x)\leq k-1$, such that

$$\frac{w(x)}{h(x)}+f(x)=\frac{w(x)+f(x)h(x)}{h(x)}$$

has at least $k+r$ distinct roots in $\mathbb{F}_q$. i.e. there exists a subset $\{x_1,x_2,\ldots,x_{k+r}\}\subset\mathbb{F}_q$ such that

$$w(x)+f(x)h(x)=(x-x_1)(x-x_2)\ldots(x-x_{k+r})v(x)$$

for some $v(x)\in\mathbb{F}_q[x]$ with $\deg(v(x))=m-(k+r)$. It is sufficient to show that there exists a subset $\{x_1,x_2,\ldots,x_{k+r}\}\subset\mathbb{F}_q$ such that

$$x^m w(\frac{1}{x})+x^m f(\frac{1}{x})h(\frac{1}{x})=(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)x^{m-(k+r)}v(\frac{1}{x}).$$

If we denote $\tilde{w}(x)=x^m w(1/x)$, $\tilde{f}(x)=x^{k-1}f(1/x)$, $\tilde{v}(x)=x^{m-(k+r)}v(1/x)$, then we have

$$\tilde{w}(x)+\tilde{f}(x)\overline{h}(x)=(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x), \tag{3.1}$$

with $\deg\tilde{w}(x)=m$, $\deg\tilde{f}(x)\leq k-1$ and $\deg\tilde{v}(x)=m-(k+r)=d-r$. Equation 3.1 is equivalent to the congruence

$$(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x)\equiv\tilde{w}(x)\pmod{\overline{h}(x)}. \tag{3.2}$$

Since $\tilde{w}(0)\neq 0$, without loss of generality, we can assume that $\tilde{w}(0)=1$ and hence $\tilde{v}(0)=1$. Equation 3.2 is then equivalent to the following congruence

$$\frac{(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\equiv 1\pmod{\overline{h}(x)}. \tag{3.3}$$

The number of solutions in equation 3.3 is

$$N_u=\#\left\{(x_1,\ldots,x_{k+r},\tilde{v}(x))\;\middle|\;\begin{array}{l}\frac{(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\equiv 1\pmod{\overline{h}(x)}\\ x_i\in\mathbb{F}_q,\textit{distinct},\deg\tilde{v}(x)=m-(k+r),\tilde{v}(0)=1\end{array}\right\}.$$

Thus, N_u is the number of codewords $v\in C_q$ with $d(u,v)\leq q-k-r$. If $N_u>0$, then $d(u,C_q)\leq q-k-r$. Using character sums, we find

$$N_u=\frac{1}{|\hat{B}|}\sum_{\substack{x_i\in\mathbb{F}_q,\textit{distinct}\\1\leq i\leq k+r}}\;\sum_{\substack{\tilde{v}(x)\in\mathbb{F}_q[x],\tilde{v}(0)=1\\\deg\tilde{v}(x)=d-r}}\;\sum_{\chi\in\hat{B}}\chi\left(\frac{(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right).$$

We first assume that $r<d$. In this case, to simplify the proof, we consider the following weighted version

$$N=\frac{1}{|\hat{B}|}\sum_{\substack{x_i\in\mathbb{F}_q,\textit{distinct}\\1\leq i\leq k+r}}\;\sum_{\substack{\tilde{v}(x)\in\mathbb{F}_q[x],\tilde{v}(0)=1\\\deg\tilde{v}(x)=d-r}}\Lambda(\tilde{v})\sum_{\chi\in\hat{B}}\chi\left(\frac{(1-x_1x)(1-x_2x)\ldots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right).$$

It is clear that if $N > 0$, then $N_u > 0$. We use Li-Wan's new sieve (Proposition 2.5) to estimate N.

Let $X = \mathbb{F}_q^{k+r}$, $\overline{X} = \{(x_1, x_2, \ldots, x_{k+r}) \in \mathbb{F}_q^{k+r} | \ x_i \neq x_j, i \neq j\}$,

$$f(x) = f(x_1, x_2, \ldots, x_{k+r}) = \chi((1 - x_1x)(1 - x_2x)\ldots(1 - x_{k+r}x)),$$

$$F = \sum_{x \in \overline{X}} \chi((1 - x_1x)(1 - x_2x)\ldots(1 - x_{k+r}x)) = \sum_{x \in \overline{X}} f(x).$$

Obviously, X is symmetric and f is normal on X, we can use Proposition 2.5 directly to compute F. In this case,

$$F_\tau = \sum_{\substack{x_{st_s} \in \mathbb{F}_q \\ 1 \leq s \leq k+r, 1 \leq t_s \leq c_s}} \chi(1 - x_{11}x)\ldots\chi(1 - x_{1c_1}x)\chi^2(1 - x_{21}x)\ldots\chi^{k+r}(1 - x_{(k+r)1}x)\ldots\chi^{k+r}(1 - x_{(k+r)c_{k+r}}x).$$

If $\chi \in \hat{B}$ is non-trivial and $\chi(\mathbb{F}_q^*) = 1$, by Weil's bound and noting that $\chi(x) = 0$ since $\bar{h}(x)$ is divisible by x, we can see that

$$\left|\sum_{x_i \in \mathbb{F}_q} \chi(1 - x_ix)\right| = \left|1 + \sum_{a \in \mathbb{F}_q} \chi(x - a)\right| \leq (d - 1)q^{\frac{1}{2}}.$$

We know that if $\chi \neq 1$ and $\chi^h = 1$, then $h \geq 2$.

$$\begin{aligned} N &= \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \leq i \leq k+r}} \sum_{\substack{\tilde{v}(x) \in \mathbb{F}_q[x], \tilde{v}(0) = 1 \\ \deg \tilde{v}(x) = d-r}} \Lambda(\tilde{v}) + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \leq i \leq k+r}} \sum_{\substack{\tilde{v}(x) \in \mathbb{F}_q[x], \tilde{v}(0) = 1 \\ \deg \tilde{v}(x) = d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi\left(\frac{(1 - x_1x)\ldots(1 - x_{k+1}x)\tilde{v}(x)}{\tilde{w}(x)}\right) \\ &= \frac{1}{|\hat{B}|}(q)_{k+r}(q^{d-r} - 1) + \frac{1}{|\hat{B}|} \sum_{\substack{\tilde{v}(x) \in \mathbb{F}_q[x], \tilde{v}(0) = 1 \\ \deg \tilde{v}(x) = d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \leq i \leq k+r}} \chi\left(\frac{(1 - x_1x)\ldots(1 - x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right) \end{aligned}$$

Using the analysis above, we can get that

$$\begin{aligned} \left|N - \frac{1}{|\hat{B}|}(q)_{k+r}(q^{d-r} - 1)\right| &\leq \frac{1}{|\hat{B}|} \left| \sum_{\substack{\tilde{v}(x) \in \mathbb{F}_q[x], \tilde{v}(0) = 1 \\ \deg \tilde{v}(x) = d-r}} \Lambda(\tilde{v})\chi(\tilde{v}) \right| \left| \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi^{-1}(\tilde{w}) \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \leq i \leq k+r}} \chi\left((1 - x_1x)\ldots(1 - x_{k+r}x)\right) \right| \\ &\leq \frac{1}{|\hat{B}|} dq^{\frac{d-r}{2}} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\sum ic_i = k+r} N(c_1, c_2, \ldots, c_{k+r})|F_\tau| \\ &\leq \frac{1}{|\hat{B}|} dq^{\frac{3d-r}{2}} C_{k+r}((d - 1)q^{1/2}, q, \ldots, (d - 1)q1/2, q, \ldots) \\ &\leq \frac{dq^{\frac{3d-r}{2}}}{|\hat{B}|} \left(dq^{1/2} + k + \frac{q}{2}\right)_{k+r}. \end{aligned}$$

So, in order to prove $N_u > 0$. It is sufficient to prove

$$(q)_{k+r}(q^{d-r} - 1) > dq^{\frac{3d-r}{2}} \left(dq^{1/2} + k + \frac{q}{2}\right)_{k+r}.$$

Since we assumed that $d > r$, we get the following sufficient condition:

$$\frac{q}{dq^{1/2} + k + \frac{q}{2}} > \left(\frac{dq^{\frac{3d-r}{2}}}{q^{d-r} - 1} \right)^{\frac{1}{k+r}}.$$

With the assumption $d < c_1 q^{1/2}, k < c_2 q$, it is sufficient to prove that there are positive constants c_1, c_2 satisfying

$$c_1 + c_2 < \left(\frac{dq^{\frac{3d-r}{2}}}{q^{d-r} - 1} \right)^{\frac{-1}{k+r}} - \frac{1}{2}.$$

This is possible if $\left(\frac{dq^{\frac{3d-r}{2}}}{q^{d-r}-1} \right)^{\frac{1}{k+r}} < 2$, that is, if $k > (\frac{d+r}{2} + 1) \log_2 q$. This completes the poof in the case $r < d$.

Assume now that $r = d$. The above proof breaks down, but the theorem can be proved in a similar way by working with the original un-weighted counting function N_u. Since $r = d$, we have $\tilde{v}(x) = 1$. Thus,

$$\begin{aligned} N_u &= \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \le i \le k+r}} 1 + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \le i \le k+r}} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi \left(\frac{(1 - x_1 x) \dots (1 - x_{k+1} x)}{\tilde{u}(x)} \right) \\ &= \frac{1}{|\hat{B}|} (q)_{k+r} + \frac{1}{|\hat{B}|} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\substack{x_i \in \mathbb{F}_q, distinct \\ 1 \le i \le k+r}} \chi \left(\frac{(1 - x_1 x) \dots (1 - x_{k+r} x)}{\tilde{u}(x)} \right). \end{aligned}$$

Using a similar estimate, we can deduce that

$$\left| N - \frac{1}{|\hat{B}|} (q)_{k+r} \right| \le \frac{q^d}{|\hat{B}|} \left(dq^{1/2} + k + \frac{q}{2} \right)_{k+d}.$$

To get $N > 0$, it is sufficient to have

$$(q)_{k+d} > q^d \left(dq^{1/2} + k + \frac{q}{2} \right)_{k+d}.$$

This actually proves something stronger than what is stated in the theorem if $r = d$. The proof is complete.

4 Conclusions

In this paper, we proved that for those received words represented by a low degree rational function in a suitable sense, the error distance can be explicitly determined for the standard Reed-Solomon codes. It would be very interesting to see if the square root condition $d < c\sqrt{q}$ in our main theorem can be improved to a linear condition $d < cq$ for some positive constant c. A similar problem in different contexts occurs in [5] and [15].

References

[1] E. Berlekamp and L. Welch, *Error correction of algebraic block codes,* U.S. Patent Number 4633470, 1986.

[2] Antonio Cafure, Guillermo Matera and Melina Privitelli, *Singularities of symmetric hypersurfaces and an application to Reed-Solomon codes*, arXiv 1109.2265v1, Sep 10, 2011.

[3] Q. Cheng and E. Murray, *On deciding deep holes of Reed-Solomon codes*, In Proceedings of TAMC 2007, LNCS4484,296-305.

[4] Q. Cheng and D. Wan, *On the list and bounded distance decodability of Reed-Solomon codes*, SIAM J. Comput. **37** (2007), no. 1, 195-209.

[5] Q. Cheng and D. Wan, *Complexity of decoding positive-rate Reed-Solomon codes*, IEEE Trans. Inform Theory, **56** (2010), No. 10, 5217-5222.

[6] V. Guruswami and M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometry codes*, IEEE Trans Inform Theory, 45(6):1757-1767(1995).

[7] V. Guruswami and A. Vardy, *A Maximum-likelihood decoding of Reed-Solomon codes is NP-Hard*, IEEE Trans Inform Theory, 51(7):2249-2256(2005).

[8] J. Y. Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl, 2008, 14, 911-929.

[9] J. Y. Li and D. Wan, *A new sieve for distinct coordinate counting*, Science China Mathematics, 2010, Vol.53, No.9, 2351-2362.

[10] J. Y. Li and D. Wan, *Counting subset sums of finite abelian groups*, Journal of Combinatorial Theory Series A, archive Volume 119 Issue 1, January, 2012.

[11] Yujuan Li and D. Wan, *On error distance of Reed-Solomon codes*, Science in China Mathematics, Vol 51, 11(2008), 1982-1988.

[12] Qunying Liao, *On Reed-Solomon Codes*, Chinese Annals of Mathematics, Series B, 32B(1), 2011, 89-98.

[13] M. Sudan, *Decoding of Reed-Solomon codes beyond the error-correction bound*, J Complexity, 13: 180-193(2007).

[14] D. Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation, 66, 119-1212(1997).

[15] G. Zhu and D. Wan, *An asymptotic formula for counting subset sums over subgroups of finite fields*, Finite Fields Appl. (2011). doi: 10.1016/j.ffa.2011.07.010.