Matt Keti[1], Daqing Wan[1], and Guizhen Zhu[2]

[1]Department of Mathematics, University of California Irvine, CA 92697-3875, USA,
mketi@uci.edu, dwan@math.uci.edu

[2]Institute for Advanced Study, Tsinghua University, Beijing, 100084, P.R. China,
zhugz08@mails.tsinghua.edu.cn

1 Introduction

In many areas of consumer and scientific technology, a message must be relayed to some remote receiver. Often times, the message is sent over a noisy channel, potentially introducing errors for the receiver. To combat this, the concept of an error-correcting code is employed: the message sender adds some redundant information to the message so that the receiver can attempt to detect and correct errors in the transmission. One of the most popular codes is called the Reed-Solomon code, which has enjoyed remarkable successes in compact disc playback, satellite communications, QR code reading,... There are still open problems regarding the nature of the Reed-Solomon code, particularly in its error-correcting capability. Because of the widespread usage of the code, these problems are very important; we would like to study one of them here.

To set up a Reed-Solomon code, take a finite field $\mathbb{F}_q$ and fix a message block length k. Associate a message string $(m_0, m_1, m_2, \ldots, m_{k-1})$ to the polynomial $m(x) = m_0 + m_1 x + m_2 x^2 + \ldots + m_{k-1} x^{k-1}$. To add the redundant information, first choose $n > k$ points from $\mathbb{F}_q$ to form the set $D = \{x_1, x_2, \ldots, x_n\}$, the evaluation set. Then, pass the message $m(x)$ through the function ϕ, called the encoder, which outputs the string $(m(x_1), m(x_2), \ldots, m(x_n))$, called a codeword. (It is the codeword that is then sent across the channel.) The collection of all codewords from all possible message strings is called the code (or codebook) and is denoted by $\mathcal{C}$. Typical choices for D are $\mathbb{F}_q$ and $\mathbb{F}_q^*$, which are called the standard and primitive Reed-Solomon codes (respectively), and the former can be denoted by $\mathcal{C}_q$. For a general choice $D \subseteq \mathbb{F}_q$, $\mathcal{C}$ is called a generalised Reed-Solomon code.

Next, to get an idea of the error-correcting capacity of the code, we need the concept of the Hamming distance between two words: if $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$

are two words, then the Hamming distance $d(a, b)$ is the number of coordinates in which they differ. For example, if $a = (1, 2, 3)$ and $b = (2, 2, 2)$, then $d(a, b) = 2$. Now for our Reed-Solomon code $\mathcal{C}$, we have the concept of minimum distance: it is the smallest distance between any two distinct codewords and is denoted $d(\mathcal{C})$. It is well-known and easily checked that $d(\mathcal{C}) = n - k + 1$.

The distance result has a very important consequence: if the number of errors in a received word is less than $d(\mathcal{C})/2 = (n - k + 1)/2$ (i.e. half of the minimum distance), then it can be corrected to a unique codeword and then decoded to recover the original message. There are several fast algorithms that do this - the Berlekamp-Massey algorithm is one example [1] [14]. A new question can then be raised: is it possible to decode efficiently past half of the minimum distance? Guruswami and Sudan [7] [8] gave an algorithm that can decode a word with up to $n - \sqrt{nk}$ errors, at the cost of dropping uniqueness. Instead, the algorithm outputs a list of possible decodings and the receiver can select the one that makes the most sense.

At this point, it is unknown whether or not it is possible to quickly decode past $n - \sqrt{nk}$ errors. There are several ways to formulate this question. Define the quantity $d(u, \mathcal{C})$ to be the shortest distance between the received word u and each codeword in $\mathcal{C}$. One problem is the maximum-likelihood decoding: given a received word u, to find a closest codeword v to u. Or in other words, to find an explict codeword v such that $d(u, v) = d(u, \mathcal{C})$. Another formulation is the bounded distance decoding: given a received word u and a bound B, to find one codeword v such that $d(u, v) \leq B$. Both problems are computationally difficult in nature. Guruswami and Vardy in [9] showed that the maximum-likelihood decoding for certain Reed-Solomon codes over $\mathbb{F}_{2^s}$ with small evaluation set D is NP-hard. Cheng and Wan in [5] and [6] showed that maximum-likelihood and bounded distance decoding for the standard and primitive Reed-Solomon codes are at least as hard as computing discrete logarithm over large extensions of the finite field $\mathbb{F}_q$, which is believed to be difficult in cryptographic applications.

Studying these decoding problems brings up a new problem. It is well-known that for any received word u, its distance to $\mathcal{C}$ satisfies $d(u, \mathcal{C}) \leq \max_{u \in \mathbb{F}_q} d(u, \mathcal{C}) = n - k$. The latter quantity is called the covering radius. Any word u for which $d(u, \mathcal{C}) = n - k$ is called a deep hole. The deep hole problem states: given a received word u, to determine whether or not u is a deep hole. Guruswami and Vardy also showed in [9] that making this determination for their family of codes is NP-hard. However, they suggested that it might be easier when the evaluation set is very large or even all of $\mathbb{F}_q$.

To try to deal with the deep hole problem, we can start with a simple way to measure $d(u, \mathcal{C})$. We run Lagrange Interpolation on the word $u = (u_1, \cdots, u_n)$ to get a fitted polynomial $u(x)$ satisfying $u(x_i) = u_i$ for all $1 \leq i \leq n$. Then, if $\deg u(x) \leq k-1$, then u is a codeword and $d(u, \mathcal{C}) = 0$. Otherwise, $k \leq \deg u(x) \leq n-1$, and we have the bound [11]

$$n - \deg u(x) \leq d(u, \mathcal{C}) \leq n - k$$

We can see here that if $\deg u(x) = k$, then u is automatically a deep hole.

1.1 Previous Results

1.1.1 Results on Standard Reed-Solomon Codes

Cheng and Murray in [4] searched for deep holes for standard Reed-Solomon codes, and conjectured that the only deep holes were those satisfying $\deg u(x) = k$. More precisely,

Conjecture (Cheng-Murray)**.** All deep holes for standard Reed-Solomon codes are those words satisfying $\deg u(x) = k$. In other words, a received word u is a deep hole for $\mathcal{C}_q$ if and only if $\deg u(x) = k$.

Though they could not prove this, they were able to reduce the problem to finding a rational point on an algebraic hypersurface and derive the following result:

Theorem 1 (Cheng-Murray)**.** Let p be a prime and $1 < k < p^{1/4-\varepsilon}$ be a positive integer. Consider the standard Reed-Solomon code $\mathcal{C}_p$, and let u be a received word and $u(x)$ be its interpolated polynomial. If the degree of $u(x)$ satisfies

$$k < \deg u(x) < k + p^{3/13-\varepsilon}$$

then u is not a deep hole.

Roughly, if u can be represented by a polynomial whose degree is close to k but different from k (i.e. a low-degree polynomial of degree greater than k), then it is not a deep hole.

Several other results in this direction have appeared. Li and Wan viewed the problem in terms of finding solutions to polynomial congruences and used character sums to obtain the following result for $\mathcal{C}_q$:

Theorem 2. Let u be a received word and $u(x)$ be its interpolated polynomial. Suppose $1 \leq d := \deg u(x) - k \leq q - 1 - k$. If

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

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}_q) < q - k$. In other words, u is not a deep hole. Furthermore, if

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

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}_q) = q - (k + d)$.

Not only do these statements give new explicit families of non deep holes; the second statement shows that under the right conditions, the error distance of a received word can be measured exactly.

Liao extended this result using similar techniques in [10] and came up with a bound on the error distance under certain conditions.

Theorem 3. Let $r \geq 1$ be an integer. Let u be a received word and $u(x)$ be is interpolated polynomial of degree m. If $m \geq k + r$,

$$q > \max\left\{2\binom{k+r}{2} + (m-k), (m-k)^{2+\varepsilon}\right\} \text{ and } k > \frac{1}{1+\varepsilon}\left(r + (2+\varepsilon)\left(\frac{m}{2} + 1\right)\right)$$

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}_q) \leq q - k - r$.

Using some techniques from algebraic geometry, Cafure, Matera, and Privitelli in [3] slightly improved on one of Li-Wan's previous results with

Theorem 4. Let u be a received word and $u(x)$ be is interpolated polynomial with $1 \leq d := \deg(u(x)) - k \leq q - 1 - k$. Assume that

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

for some constant $\varepsilon > 0$. Then u is not a deep hole.

Recently, Zhu and Wan [19] used the idea that some high degree polynomials could be represented by low-degree rational functions and proved:

Theorem 5. Let $r \geq 1$ be an integer and u a received word. Suppose we can write

$$\left(\frac{w(x_1)}{h(x_1)}, \frac{w(x_2)}{h(x_2)}, \ldots, \frac{w(x_q)}{h(x_q)}\right) = u$$

for some $h(x) \in \mathbb{F}_q[x]$, with $\gcd(h(x), x^q - x) = 1$, and $\deg h(x) + k \leq \deg w(x) \leq q - 1$. Let m be the smallest such degree of $w(x)$, and set $r \leq d := m - k \leq q - 1 - k$. There are positive constants c_1 and c_2 such that if

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

then $d(u, \mathcal{C}) \leq q - k - r$.

The proof converted the distance problem to finding solutions to a polynomial congruence. Sufficient conditions for when a solution exists were given by a combination of character sums, Weil's bound, and Li-Wan's new sieve.

1.1.2 New Deep Holes on Primitive and Generalised Reed-Solomon Codes

There are many recent studies that search for deep holes for primitive or generalised codes. Wu and Hong in [17] showed that words represented by certain polynomials of degree $q-2$ are deep holes for primitive codes. Their method involved converting the code into a BCH code by way of the Discrete Fourier Transform.

Theorem 6 (Wu-Hong)**.** Consider the primitive Reed-Solomon code $\mathcal{C}$ over $\mathbb{F}_q$ with $q \geq 4$ and $2 \leq k \leq q-2$. Then polynomials of the form $u(x) = ax^{q-2} + v(x)$ with $a \neq 0$, where $\deg v(x) \leq k-1$, represent deep holes for $\mathcal{C}$.

In a new preprint, Zhang, Fu, and Liao in [18] extended this result for any evaluation set $D \neq \mathbb{F}_q$.

Theorem 7 (Zhang-Fu-Liao)**.** Consider the generalised Reed-Solomon code $\mathcal{C}$ over $\mathbb{F}_q$ with evaluation set $D \neq \mathbb{F}_q$. Then for any $a \neq 0$, $b \notin D$, polynomials of the form $u(x) = a(x-b)^{q-2} + v(x)$, where $\deg v(x) \leq k-1$, represent deep holes for $\mathcal{C}$.

Adapting results from Li and Wan [11], they also found another class of deep holes for a code with a specific message length k:

Theorem 8 (Zhang-Fu-Liao)**.** Let $q > 4$ be a power of 2 and let $\mathcal{C}$ be the generalised Reed-Solomon code over $\mathbb{F}_q$ with $D = \mathbb{F}_q^*$ or $D = \mathbb{F}_q^*/\{1\}$ and $k = q-4$. If $a \neq 0$, then polynomials of the form $u(x) = ax^{q-3} + v(x)$, where $\deg v(x) \leq k-1$, are deep holes for $\mathcal{C}$.

Finally, they showed that for primitive codes over $\mathbb{F}_q$ for $q > 5$ and $2 \leq k \leq q-3$, polynomials of the form

$$u(x) = ax^{k+2} + bx^{k+1} + cx^k + v(x)$$

where $a \in \mathbb{F}_q^*$, $b, c \in \mathbb{F}_q$, and $\deg v(x) \leq k-1$, do not represent deep holes.

These results show that the Cheng-Murray conjecture adapted for primitive codes is false. Wu and Hong tried to modify the conjecture in their paper, stating that the only deep holes are certain polynomials of degree k and $q-2$; however, the new counterexample by Zhang, Fu, and Liao leaves the status of deep holes uncertain.

2 New Results

2.1 Main Theorems

Following [19], we will derive another class of words that are not deep holes for generalised Reed-Solomon codes. First, fix an enumeration $D = \{x_1, x_2, \ldots, x_{|D|}\}$. All of our specific results will hinge on

Theorem 9. Let $\mathcal{C}$ be the generalised Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set D. Let u be a received word. Suppose we can write

$$\left(\frac{w(x_1)}{h(x_1)}, \frac{w(x_2)}{h(x_2)}, \ldots, \frac{w(x_{|D|})}{h(x_{|D|})}\right) = u$$

for some $h(x) \in \mathbb{F}_q[x]$, with no roots in $D \cup 0$, and $\deg h(x) + k \leq \deg w(x) \leq |D| - 1$. Let m be the smallest such degree of $w(x)$. Let $1 \leq r \leq d := m - k \leq |D| - k - 1$. If the bound

$$\left|\sum_{a \in D} \chi(1 - ax)\right| \leq K q^{1/2}$$

is true over all nontrivial characters $\chi : (\mathbb{F}[x]/(\bar{h}(x)))^* \to \mathbb{C}^*$ with $\chi(\mathbb{F}_q^*) = 1$ for some $K \geq d$ and $\bar{h}(x) = x^{m-k+1} h(1/x)$, there are positive constants c_1 and c_2 such that if

$$d \leq K < c_1 \frac{|D|}{q^{1/2}}\ , \quad \left(\frac{d + r}{2} + 1\right) \log_2 q < k < c_2 |D|$$

then $d(u, \mathcal{C}) \leq |D| - k - r$.

This statement is quite robust in that it can handle words that can either be represented by low-degree polynomials or low-degree rational functions. (The next section will show some examples.) In addition, it applies to code families with a positive information rate $k/|D|$.

Setting $h(x) = 1$, the theorem reduces to the usual polynomial case, and we receive

Corollary 1. Let $\mathcal{C}$ be the generalised Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set D. Let $r \geq 1$ be an integer and u a received word with interpolated polynomial $u(x)$ such that $r \leq d := \deg(u(x)) - k \leq |D| - k - 1$. If the bound

$$\left|\sum_{a \in D} \chi(1 - ax)\right| \leq K q^{1/2}$$

is true over all nontrivial characters $\chi : (\mathbb{F}[x]/(x^{d+1}))^* \to \mathbb{C}^*$ with $\chi(\mathbb{F}_q^*) = 1$ for some $K \geq d$, then there are positive constants c_1 and c_2 such that if

$$d \leq K < c_1 \frac{|D|}{q^{1/2}} \ , \ \left(\frac{d+r}{2}+1\right)\log_2 q < k < c_2|D|$$

then $d(u, \mathcal{C}) \leq |D| - k - r$.

We can specialise this result to a code that uses the evaluation set $D = (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}$ or $D = \mathbb{F}_q$. For these cases, we will be able to take $K = d$.

Corollary 2. Let $\mathcal{C}$ be the primitive Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set $D = (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}$ of size ℓ. Let $r \geq 1$ be an integer and u a received word with interpolated polynomial $u(x)$ such that $r \leq d := \deg(u(x)) - k \leq q - 2 - k$. There are positive constants c_1 and c_2 such that if

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

then $d(u, \mathcal{C}) \leq \ell - k - r$.

Note that the first condition $d < c_1 \frac{\ell}{q^{1/2}}$ will implicitly put a minimum on the size of ℓ due to the dependency between c_1 and c_2. This dependency can be seen in the upcoming example.

Corollary 3. Let $\mathcal{C}$ be the standard Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set $D = \mathbb{F}_q$. Let $r \geq 1$ be an integer and u a received word with interpolated polynomial $u(x)$ such that $r \leq d := \deg(u(x)) - k \leq q - k - 1$. There are positive constants c_1 and c_2 such that if

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

then $d(u, \mathcal{C}) \leq q - k - r$.

This corollary recovers what Zhu and Wan proved in [19].

2.2 Examples

To get a better idea of what these theorems mean, take $\mathcal{C}$ to be the primitive Reed-Solomon code over $\mathbb{F}_{2^8}$ (i.e. $D = \mathbb{F}_{2^8}^*$). We will realise this field as $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$, noting that this is formed using a primitive polynomial.

Now if $r \geq 1$, and u is a codeword with $r \leq d \leq 254 - k$, then we can find c_1 and c_2 such that if

$$d < \frac{255}{16}c_1 \ \text{ and } \ 8\left(\frac{d+r}{2}+1\right) < k < 255c_2$$

then $d(u,\mathcal{C}) \leq 255 - k - r$. To be even more concrete, consider $d = r = 1$; in other words, we want to classify codewords whose polynomial (or rational) interpolations are degree $k+1$ (in the numerator). From the proof below, we can explicitly compute c_1 and c_2 using the formulas

$$1 < \frac{255}{16}c_1 \ , \ c_1 + c_2 = 256^{-\frac{1}{k+1}} - \frac{1}{2}$$

To obtain a wide range of k, fix $c_1 = .0628$. Then we have the condition

$$16 < k < 255\left(256^{-\frac{1}{k+1}} - \frac{1}{2} - .0628\right)$$

A computer algebra system shows that this is satisfied when $17 \leq k \leq 97$. Therefore, for codes using this range of message lengths, received words u represented by a polynomial (or rational function) of degree $k+1$ (in the numerator) are not deep holes. More specifically, we can give the estimate $d(u,C) \leq 254 - k$.

Along the same lines, for $r = 1$ and $d = 2$, polynomials (or rational functions) of degree $k+2$ (in the numerator) do not represent deep holes when the message length satisfies $21 \leq k \leq 86$. Again, such words u satisfy the estimate $d(u,C) \leq 254 - k$. Attempting to increase r or d any more does not yield additional information.

Here is a table with a few examples of words covered by our bounds. We will denote α to be a root of $x^8 + x^4 + x^3 + x^2 + 1$, so α will be a multiplicative generator for $\mathbb{F}_{2^8}^*$.

d	k	Polynomial Interpolation	Rational Interpolation
1	17	$x^{18} + 3x^2 + 1$	N/A
1	97	$x^{98} + x^{24} + x^{17} + 1$	N/A
2	30	$(\alpha^6 + \alpha^3 + 1)x^{254} + \ldots + (\alpha^6 + \alpha^5)$	$x^{32}/(x^2 + \alpha x + \alpha^7)$
2	86	$(\alpha^6 + \alpha^5)x^{254} + \ldots + (\alpha^7 + \alpha^6 + \alpha^2)$	$(x^{88} + 1)/(x^2 + x + \alpha^5)$

2.3 Preliminaries

There are a few theorems that we will need to establish our results.

2.3.1 Weil's Character Sum Bound

As stated in [15]:

Theorem 10 (Weil)**.** Let $h(x)$ be a polynomial of positive degree in the ring $\mathbb{F}_q[x]$, and let $\chi : (\mathbb{F}[x]/(h(x)))^* \to \mathbb{C}^*$ be a multiplicative character. If χ is not trivial, then

$$\left|\sum_{a \in \mathbb{F}_q} \chi(x - a)\right| \leq (\deg h(x) - 1)q^{1/2}$$

Furthermore, if χ is not trivial but $\chi(\mathbb{F}_q^*) = 1$, then

$$\left|1 + \sum_{a \in \mathbb{F}_q} \chi(x-a)\right| \leq (\deg h(x) - 2)q^{1/2}$$

Since we will be dealing with $(\mathbb{F}_q^*)^{(q-1)/\ell}$, these bounds need to be slightly modified:

Lemma 1. Let $h_1(x)$ be a polynomial from $\mathbb{F}_q[x]$ not divisible by x, $h(x) = x^k h_1(x)$ for $k \geq 1$, and $\chi : (\mathbb{F}[x]/(h_1(x)))^* \to \mathbb{C}^*$ with χ nontrivial and $\chi(\mathbb{F}_q^*) = 1$. For a subgroup $(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}$ of $\mathbb{F}_q^*$, we have

$$\left|\sum_{a \in (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a)\right| \leq (\deg h(x) - 1)q^{1/2}$$

Proof. Use the character sum

$$\sum_{a \in (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a) = \sum_{a \in \mathbb{F}_q} \frac{\ell}{q-1} \sum_{(\chi')^{(q-1)/\ell}=1} \chi'(a)\chi(x-a) = \frac{\ell}{q-1} \sum_{(\chi')^{(q-1)/\ell}=1} \sum_{a \in \mathbb{F}_q} \chi'(a)\chi(x-a),$$

where $\chi' : \mathbb{F}_q^* \to \mathbb{C}^*$ denotes a multiplicative character. The two characters χ and χ' can be viewed as characters over the group

$$(\mathbb{F}_q[x]/(h(x)))^* \cong (\mathbb{F}_q[x]/(x^k))^* \times (\mathbb{F}_q[x]/(h_1(x)))^*$$

This is true because we can define the natural reduction map

$$(\mathbb{F}_q[x]/(x^k))^* \times (\mathbb{F}_q[x]/(h_1(x)))^* \to (\mathbb{F}_q[x]/(x))^* \times (\mathbb{F}_q[x]/(h_1(x)))^*$$

just by taking the terms in $(\mathbb{F}_q[x]/(x^k))^*$ modulo x. And since $\mathbb{F}_q^* \cong (\mathbb{F}_q[x]/(x))^*$, χ' lifts to a character over $(\mathbb{F}_q[x]/(x^k))^*$, which therefore extends to a character over $(\mathbb{F}_q[x]/(h(x)))^*$. Because of this, we also have $\chi'(a) = \chi'(-x+a) = \chi'(-1)\chi'(x-a)$. Then,

$$\begin{aligned}\left|\sum_{a \in (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a)\right| &\leq \frac{\ell}{q-1} \sum_{(\chi')^{(q-1)/\ell}=1} \left|\sum_{a \in \mathbb{F}_q} \chi'(a)\chi(x-a)\right| \\ &= \frac{\ell}{q-1} \sum_{(\chi')^{(q-1)/\ell}=1} \left|\sum_{a \in \mathbb{F}_q} (\chi'\chi)(x-a)\right| \\ &\leq \frac{\ell}{q-1} \sum_{(\chi)^{(q-1)/\ell}=1} (\deg h(x) - 1)q^{1/2} \\ &= (\deg h(x) - 1)q^{1/2},\end{aligned}$$

where we used the fact that the product $\chi'\chi$ is a nontrivial character of $(\mathbb{F}_q[x]/(h(x)))^*$. To see this, note that the restriction of $\chi'\chi$ to the second factor $(\mathbb{F}_q[x]/(h_1(x)))^*$ is precisely χ, which is already nontrivial. □

2.3.2 Li-Wan's New Sieve

We also state Li-Wan's new sieve (as in [12] and [19]): let D be a finite set and $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let X be a subset of D^k. Denote

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

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

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

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

$$\tau = (i_1 i_2 \ldots i_{a_1})(j_1 j_2 \ldots j_{a_2}) \cdots (l_1 l_2 \ldots l_{a_s})$$

with $a_i \geq 1$ and $1 \leq i \leq s$. Define

$$X_\tau = \{(x_1, x_2, \ldots, x_k) \mid x_{i_1} = \ldots = x_{i_{a_1}}, x_{j_1} = \ldots = x_{j_{a_2}}, \cdots, x_{l_1} = \ldots = x_{l_{a_s}}\}$$

Similarly define

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

We say that τ is of the 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

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

Now we have the following combinatorial result:

Lemma 2. Suppose $q \geq d$. If $t_i = q$ for $d|i$ and $t_i = s$ for $d \nmid i$, then we have

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

where $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$.

Furthermore, we say that X is symmetric if for any $x \in X$ and any $g \in S_k$, we have $g \circ x \in X$. Also, if a complex-valued function f is defined on X, we say that it is normal on X if X is symmetric and for any two conjugate elements in S_k, τ and τ', we have

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

Then, we have the result:

Lemma 3. If f is normal on X, then

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

2.3.3 A Rephrasing of Error Distance

For our purposes, it is more convenient to state the error distance in this way:

Lemma 4. Let $\mathcal{C}$ be the generalised Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set D. Let u be a received word and $u(x)$ its interpolated polynomial with $\deg u(x) = k + d$, where $k + 1 \leq k + d \leq q - 1$. The error distance $d(u, \mathcal{C}) \leq |D| - k - r$ for some $1 \leq r \leq d$ if and only if there exists a subset $\{x_{i_1}, x_{i_2}, \ldots, x_{i_{k+r}}\} \subset D$ and a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $d - r$ such that

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

for some $v(x)$ with $\deg v(x) \leq k - 1$.

Proof. First suppose that $d(u, \mathcal{C}) \leq |D| - k - r$. Then, the coordinates of u differ from the coordinates of some codeword v in $|D| - k - r$ places (or less). Then, their interpolated polynomials $u(x)$ and $v(x)$ have (at least) $k + r$ roots in common in D. The result follows.

The converse has a very similar structure, roughly following the above in reverse. □

2.4 The Proof

Suppose $w(x)$ is the polynomial with degree m, and $h(x)$ is the corresponding polynomial with no roots in D. Possibly by shifting u by a constant codeword, we can assume that $w(0) \neq 0$. Also let $\bar{h}(x) = x^{m-k+1} h(1/x)$. This is a polynomial of degree $m - k + 1 = d + 1$ and divisible by x since $h(0) \neq 0$ and $\deg(h(x)) \leq m - k$. Let $A = (\mathbb{F}_q[x]/(\bar{h}(x)))^*$ and $\hat{A}$ denote the group of all characters of A. Let $\hat{B}$ be the set of characters χ in $\hat{A}$ with $\chi(\mathbb{F}_q^*) = 1$. Note that $\hat{B}$ is an abelian subgroup of order $\leq q^d$.

Now, by Lemma 4, $d(u,\mathcal{C}) \leq |D|-k-r$ if and only if there is some 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 D. In other words, there are points $\{x_1, x_2, \ldots, x_{k+r}\} \subset D$ where

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

for some polynomial $v(x)$ with $\deg v(x) = m-(k+r)$. Then replacing x with $1/x$ and multiplying through by x^m, it is enough to find such a subset for the equation

$$\tilde{w}(x) + \tilde{f}(x)\bar{h}(x) = (1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\tilde{v}(x)$$

where $\tilde{w}(x) = x^m w(1/x)$, $\tilde{f}(x) = x^{k-1}f(1/x)$, and $\tilde{v}(x) = x^{m-(k+r)}v(1/x)$. We can now further assume that $\tilde{w}(0)=1$ and $\tilde{v}(0)=1$. Then this equation is equivalent to

$$\frac{(1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)} \equiv 1 \pmod{\bar{h}(x)}$$

Let the number of solutions to this equation be denoted by N_u, noting that the $x_i \in D$ are distinct, $\deg \tilde{v}(x) = m-(k+r) = d-r$, and $\tilde{v}(0)=1$. In other words, N_u gives the number of codewords f in $\mathcal{C}$ where $d(u,f) \leq |D|-k-r$. If N_u is positive, then $d(u,\mathcal{C}) \leq |D|-k-r$. By character sums,

$$N_u = \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \sum_{\chi \in \hat{B}} \chi\left(\frac{(1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right)$$

For ease of notation, define

$$S_\chi(x_1, x_2, \ldots, x_{k+r}, x) = \chi\left(\frac{(1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right)$$

First we will handle the case where $r < d$. To do this, consider the weighted version

$$N = \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) \sum_{\chi \in \hat{B}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x),$$

where Λ denotes the von Mangoldt function. Note that if $N > 0$, then $N_u > 0$. Separating the trivial character from the sum gives

$$\begin{aligned} N &= \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x) \\ &= \frac{1}{|\hat{B}|}(|D|)_{k+r}(q^{d-r}-1) + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x) \end{aligned}$$

Now we have to estimate

$$\left|N - \frac{1}{|\hat{B}|}(|D|)_{k+r}(q^{d-r}-1)\right| = \left|\frac{1}{|\hat{B}|} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\substack{x_i \in D \\ \text{distinct}}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x)\right|$$

To do this, apply Li-Wan's new sieve. Let $X = D^{k+r}$, $\bar{X} = \{(x_1, x_2, \ldots, x_{k+r}) \in D^{k+r} \mid x_i \neq x_j, i \neq j\}$, $f(x) = \chi((1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x))$, and $F = \sum_{x \in \bar{X}} f(x)$. We have that X is symmetric and f is normal, so we can compute F. For our case, we take

$$F_\tau = \sum \chi(1-x_{11}x)\cdots\chi(1-x_{1c_1}x)\cdots\chi^{k+r}(1-x_{(k+r)1}x)\cdots\chi^{k+r}(1-x_{(k+r)c_{k+r}}x)$$

where the sum is over $x_{st_s} \in D$, $1 \leq s \leq k+r$, and $1 \leq t_s \leq c_s$. We will use the Li-Wan sieve estimate and the bounds

$$\left|\sum_{a \in D} \chi(1-ax)\right| \leq Kq^{1/2} \quad \text{and} \quad K \geq d$$

over all nontrivial $\chi \in \hat{B}$ with $\chi(\mathbb{F}_q^*) = 1$. We have that

$$\begin{aligned}
&\left|N - \frac{1}{|\hat{B}|}(|D|)_{k+r}(q^{d-r}-1)\right| \\
&\leq \frac{1}{|\hat{B}|}\left|\sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v})\chi(\tilde{v})\right| \left|\sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi^{-1}(\tilde{w}) \sum_{\substack{x_i \in D \\ \text{distinct}}} \chi\left((1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\right)\right| \\
&\leq \frac{1}{|\hat{B}|} dq^{\frac{d-r}{2}} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\sum ic_i = k+r} N(c_1, c_2, \ldots, c_{k+r})|F_\tau| \\
&\leq \frac{1}{|\hat{B}|} dq^{\frac{3d-r}{2}} C_{k+r}(Kq^{1/2}, |D|, Kq^{1/2}, |D|, \ldots) \\
&\leq \frac{1}{|\hat{B}|} dq^{\frac{3d-r}{2}} \left(Kq^{1/2} + k + r + \frac{|D| - Kq^{1/2}}{2} - 1\right)_{k+r} \\
&\leq \frac{1}{|\hat{B}|} dq^{\frac{3d-r}{2}} \left(Kq^{1/2} + k + r - \frac{Kq^{1/2}}{2} + \frac{|D|}{2}\right)_{k+r} \\
&\leq \frac{1}{|\hat{B}|} dq^{\frac{3d-r}{2}} \left(Kq^{1/2} + k + \frac{|D|}{2}\right)_{k+r}
\end{aligned}$$

Therefore, it is sufficient to prove that

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

And since $d > r$, we have another sufficient condition:

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

If we take $K < c_1 \dfrac{|D|}{q^{1/2}}$ and $k < c_2|D|$, then it suffices to find c_1 and c_2 satisfying

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

which means that it is enough to find

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

By some rearrangement and simplification, we have

$$k > \log_2 d + \left(\frac{d+r+1}{2} \right) \log_2 q - r$$

A simpler condition can be prescribed. Since $r \le d \le K < q^{1/2}$, we can just replace $\log_2 d - r$ with $\frac{1}{2} \log_2 q$ to receive:

$$k > \left(\frac{d+r}{2} + 1 \right) \log_2 q$$

For the case $r = d$, we use the unweighted counting function N_u, noting that $\tilde{v}(x) = 1$. Then we have

$$\begin{aligned} N_u &= \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} 1 + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi \left(\frac{(1 - x_1 x)(1 - x_2 x) \cdots (1 - x_{k+r} x)}{\tilde{w}(x)} \right) \\ &= \frac{1}{|\hat{B}|} (|D|)_{k+d} + \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \chi \left(\frac{(1 - x_1 x)(1 - x_2 x) \cdots (1 - x_{k+d} x)}{\tilde{w}(x)} \right) \end{aligned}$$

Applying the same method as the previous case gives the estimate

$$\left| N_u - \frac{1}{|\hat{B}|} (|D|)_{k+d} \right| \le \frac{q^d}{|\hat{B}|} \left(K q^{1/2} + k + \frac{|D|}{2} \right)_{k+d}$$

and then it is enough to have

$$\frac{1}{|\hat{B}|} (|D|)_{k+d} > \frac{q^d}{|\hat{B}|} \left(K q^{1/2} + k + \frac{|D|}{2} \right)_{k+d}$$

which actually gives a better bound than before. This concludes the proof. □

2.4.1 The Second Corollary

To prove the second corollary, we only need to find a number K satisfying the bounds

$$\left|\sum_{a\in(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(1-ax)\right| \leq Kq^{1/2} \quad \text{and} \quad K \geq d$$

over all characters χ from $\hat{B}$ in the main proof. This is where we can use Lemma 1, noting that $\deg \bar{h}(x) = d+1$:

$$\begin{aligned}\left|\sum_{a\in(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(1-ax)\right| &= \left|\sum_{a\in(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(-a)\chi(x-a^{-1})\right| \\ &= \left|\sum_{a\in(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a^{-1})\right| \\ &= \left|\sum_{a\in(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a)\right| \\ &\leq dq^{1/2}\end{aligned}$$

So we have $K = d$, and the first bound is satisfied. The second bound $K \geq d$ is automatically satisfied. □

2.4.2 The Third Corollary

To prove the third corollary, we again need to find K satisfying

$$\left|\sum_{a\in\mathbb{F}_q} \chi(1-ax)\right| \leq Kq^{1/2} \quad \text{and} \quad K \geq d$$

As before, $\deg \bar{h}(x) = d+1$. Using Theorem 10 (Weil) and the fact that $\chi(x) = 0$, since $\bar{h}(x)$ is divisible by x, we have

$$\left|\sum_{a\in\mathbb{F}_q} \chi(1-ax)\right| = \left|1 + \sum_{a\in\mathbb{F}_q} \chi(x-a)\right| \leq (d-1)q^{1/2} \leq dq^{1/2}$$

Therefore $K = d$ is the suitable choice. □

3 Summary and Further Problems

In Reed-Solomon codes with large evaluation sets D satisfying some character sum bounds, we were able to measure the error distances for certain families of received words and show that they were not deep holes. We then applied these results to common choices of $D = \mathbb{F}_q$ or (large subgroups of) $\mathbb{F}_q^*$. These results raise some new problems.

1. In the primitive / generalised codes, we required the condition $d < c_1 \frac{\ell}{q^{1/2}}$. If it were possible to relax the condition to $d < c_1 \frac{\ell}{q^{1/2-\varepsilon}}$, we would be able to choose much smaller values of c_1 to get better information rates on our codes.

2. In our codes, the set $D = (\mathbb{F}_q^*)^{(q-1)/\ell}$ can be thought of as the image of the polynomial $f(x) = x^{(q-1)/\ell}$ whose domain is $\mathbb{F}_q^*$. Is it possible to make similar statements when $f(x)$ is replaced with an arbitrary polynomial?

It would be interesting to see the development of these problems, as they could advance the search for deep holes.

References

[1] E.R. Berlekamp. Algebraic Coding Theory. New York: McGraw-Hill, 1968.

[2] V.K. Bhargava, S.B. Wicker, et al. Reed-Solomon Codes and Their Applications. IEEE Press, Piscataway, NJ. 1994.

[3] A. Cafure, G. Matera, and M. Privitelli. Singularities of Symmetric Hypersurfaces and Reed-Solomon Codes. Advances in Mathematics of Communications, Vol. 6(1), 2012, pp.69-94.

[4] Q. Cheng and E. Murray. On deciding deep holes of Reed-Solomon codes. Proceedings of TAMC 2007, LNCS 4484, pp. 296-305

[5] Q. Cheng and D. Wan. On the List and Bounded Distance Decodibility of Reed-Solomon Codes. Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04).

[6] Q. Cheng and D. Wan. Complexity of Decoding Positive-Rate Primitive Reed-Solomon Codes. IEEE Transactions on Information Theory, Vol. 56, No. 10, October 2010: 5217-5222.

[7] V. Guruswami. List Decoding of Error-Correcting Codes. Springer-Verlag Berlin Heidelberg, 2004.

[8] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. IEEE Transactions on Information Theory, Vol. 45, No. 6, September 1999: 1757-1767.

[9] V. Guruswami and A. Vardy. Maximum-Likelihood Decoding of Reed-Solomon Codes is NP-hard. SODA '05 Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms: 470-478. Society for Industrial and Applied Mathematics Philadelphia, PA, USA, 2005.

[10] Q. Liao. On Reed-Solomon Codes. Chinese Annals of Mathematics, 32B(1), 89-98. Springer-Verlag Berlin Heidelberg, 2011.

[11] J. Li and D. Wan. On the subset sum problem over finite fields. Finite Fields and Their Applications, Volume 14, Issue 4, November 2008: 911-929

[12] J. Li and D. Wan. A new sieve for distinct coordinate counting. Science China Mathematics, Vol. 53 No.9: 2351-2362. Science China Press and Springer-Verlag Berlin Heidelberg, 2010.

[13] Y. Li and D. Wan. On error distance of Reed-Solomon codes, Science China Mathematics, Vol. 51, No. 11, 1982-1988. Science China Press and Springer-Verlag Berlin Heidelberg, 2008.

[14] J.L. Massey. Shift-Register Syntehsis and BCH Decoding. IEEE Transactions on Information Theory, Vol. IT-15, No. 1, January 1969.

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

[16] A. Weil. Basic Number Theory. Springer-Verlag, 1973.

[17] R. Wu and S. Hong. On deep holes of generalized Reed-Solomon codes. arXiv:1108.3524v2.

[18] J. Zhang, Fang-Wei Fu, and Qun-Ying Liao. New Deep Holes of Generalized Reed-Solomon Codes. arXiv:1205.6593v1.

[19] G. Zhu and D. Wan. Computing Error Distance of Reed-Solomon Codes. TAMC 2012, LNCS 7287, pp. 214-224, 2012. Springer-Verlag Berlin Heidelberg, 2012.