Chapter 6

LIMITS TO LIST DECODING REED-SOLOMON CODES

6.1 Introduction

In Chapters 3 and 4 we were interested in the following question: Can one construct explicit codes along with efficient list-decoding algorithms that can correct errors up to the list-decoding capacity ? Note that in the question above, we have the freedom to pick the code. In this chapter, we will turn around the question by focusing on a fixed code and then asking what is the best possible tradeoff between rate and fraction of errors (that can be corrected via efficient list decoding) for the given code.

In this chapter, we will primarily focus on Reed-Solomon codes. Reed-Solomon codes are an important and extensively studied family of error-correcting codes. The codewords of a Reed-Solomon code (henceforth, RS code) over a field $\mathbb{F}$ are obtained by evaluating low degree polynomials at distinct elements of $\mathbb{F}$. The rate versus distance tradeoff for Reed-Solomon codes meets the Singleton bound, which along with the code's nice algebraic properties, give RS codes a prominent place in coding theory. As a result the problem of decoding RS codes has received much attention.

As we already saw in Section 3.1, in terms of fraction of errors corrected, the best known polynomial time list algorithm today can, for Reed-Solomon codes of rate R, correct up to a $1 - \sqrt{R}$ ([97, 63]) fraction of errors. The performance of the algorithm in [63] matches the so-called Johnson bound (cf. [64]) which gives a general lower bound on the number of errors one can correct using small lists in *any* code, as a function of the distance of the code. As we saw in Chapter 3, there are explicit codes known that have better list decodable properties than Reed-Solomon codes. However, Reed-Solomon codes have been instrumental in all the algorithmic progress in list decoding (see Section 3.1 for more details on these developments). In addition, Reed-Solomon codes have important practical applications. Thus, given the significance (both theoretical and practical) of Reed-Solomon codes, it is an important question to pin down the optimal tradeoff between the rate and list decodability of Reed-Solomon codes.

This chapter is motivated by the question of whether the Guruswami-Sudan result is the best possible (i.e., whether the Johnson bound is "tight" for Reed-Solomon codes). By this we mean whether attempting to decode with a larger error parameter might lead to super-polynomially large lists as output, which of course will preclude a polynomial time algorithm. While we don't quite show this to be the case, we give evidence in this direction by demonstrating that in the more general setting of list recovery (to which also the algorithm of Guruswami and Sudan [63] applies) its performance is indeed the best possible.

We also present constructions of explicit “bad list-decoding configurations” for Reed-Solomon codes. The details follow.

6.2 Overview of the Results

6.2.1 Limitations to List Recovery

The algorithm in [63] in fact solves the following more general *polynomial reconstruction* problem in polynomial time: Given n' distinct pairs $(\beta_i, \gamma_i) \in \mathbb{F}^2$ output a list of all polynomials p of degree k that satisfy $p(\beta_i) = \gamma_i$ for more than $\sqrt{kn'}$ values of $i \in \{1, 2, \ldots, n'\}$ (we stress that the β_i's need **not** be distinct). In particular, the algorithm can solve the list recovery problem (see Definition 2.4). As a special case, it can solve the following “error-free” or “noiseless” version of the list recovery problem.

Definition 6.1 (Noiseless List Recovery). *For a q-ary code C of block length n, the noiseless list recovery problem is the following. We are given a set $S_i \subseteq \mathbb{F}_q$ of possible symbols for the i'th symbol for each position i, $1 \leqslant i \leqslant n$, and the goal is to output all codewords $c = \langle c_1, \ldots, c_n \rangle$ such that $c_i \in S_i$ for every i. When each S_i has at most ℓ elements, we refer to the problem as noiseless list recovery with input lists of size ℓ.*

Note that if a code C is $(0, \ell, L)$-list recoverable then L is the worst case output list size when one solves the noiseless list recovery problem on C with input lists of size ℓ.

Guruswami and Sudan algorithm [63] can solve the noiseless list recovery problem for Reed-Solomon codes with input lists of size $\ell < \lceil \frac{n}{k} \rceil$ in polynomial time. That is, Reed-Solomon codes are $(0, \lceil \frac{n}{k} \rceil - 1, L(n))$-list recoverable for some polynomially bounded function $L(n)$. In Section 6.3, we demonstrate that this latter performance is the best possible with surprising accuracy — specifically, we show that when $\ell = \lceil \frac{n}{k} \rceil$, there are settings of parameters for which the list of output polynomials needs to be super-polynomially large in n (Theorem 6.3). In fact, our result also applies to the model considered by Ar et al. [3], where the input lists are “mixtures of codewords.” In particular, in their model the lists at every position take values from a collection of ℓ *fixed* codewords.

As a corollary, this rules out an efficient solution to the polynomial reconstruction algorithm that works even under the slightly weaker condition on the agreement parameter: $t > \sqrt{kn'} - k/2$.[1] In this respect, the “square root” bound achieved by [63] is optimal, and any improvement to their list-decoding algorithm which works with agreement fraction $t/n < \sqrt{R}$ where $R = (k+1)/n$ is the rate of the code, or in other words that works beyond the Johnson bound, must exploit the fact that the evaluation points β_i are distinct (or “almost distinct”).

[1] This in turn rules out, for every $\varepsilon > 0$, a solution to the polynomial reconstruction algorithm that works as long as $t \geqslant \sqrt{(1-\varepsilon)kn'}$.

While this part on tightness of Johnson bound remains speculative at this stage, for the problem of list recovery itself, our work proves that RS codes are indeed sub-optimal, as we describe below. By our work Reed-Solomon codes for list recovery with input lists of size ℓ must have rate at most $1/\ell$. On the other hand, Guruswami and Indyk [52] prove that there exists a fixed $R > 0$ (in fact R can be close to 1) such that for every integer ℓ there are codes of rate R which are list recoverable given input lists of size ℓ (the alphabet size and output list size will necessarily grow with ℓ but the rate itself is independent of ℓ). Note that in Chapter 3, we showed that folded Reed-Solomon codes are explicit list recoverable codes with optimal rate.

6.2.2 Explicit "Bad" List Decoding Configurations

The result mentioned above presents an explicit bad list recovery configuration, i.e., an input instance to the list recovery problem with a super-polynomial number of solutions. To prove results on limitations of list decoding, such as the tightness of the Johnson bound, we need to demonstrate a received word $\mathbf{y}$ with super-polynomially many codewords that agree with $\mathbf{y}$ at t or more places. A simple counting argument establishes the *existence* of such received words that have agreement t with $\binom{n}{t}/q^{t-k}$ many codewords [70, 25]. In particular, this implies the following for $n = q$. For $k = n^{\delta}$ (in which case we say that the Reed-Solomon code has low rate), one can get $t = \frac{k}{2\delta}$ for any $\delta > 0$ and for k in $\Omega(n)$ (in which case we say that the Reed-Solomon code has high rate), one can get $t = k + O\left(\frac{n}{\log n}\right)$. In Section 6.4.2, we demonstrate an *explicit* construction of such a received word with super-polynomial number of codewords with agreement t up to $(2-\varepsilon)k$ (for any $\varepsilon > 0$), where $k = n^{\delta}$ for any $\delta > 0$. Note that such a construction is trivial for $t = k$ since we can interpolate degree k polynomials through any set of k points. In Section 6.4.3, we demonstrate an *explicit* construction of such a received word with super-polynomial number of codewords with agreement t up to $k + \frac{n}{\log^{\omega(1)} n}$, when k is in $\Omega(n)$.

In general, the quest for *explicit* constructions of this sort (namely small Hamming balls with several codewords) is well motivated. If achieved with appropriate parameters they will lead to a derandomization of the inapproximability result for computing the minimum distance of a linear code [32]. However, for this application it is important to get $2^{n^{\Omega(1)}}$ codewords in a ball of radius ρ times the distance of the code for some constant $\rho < 1$. Unfortunately, neither of our explicit constructions achieve ρ smaller than $1 - o(1)$.

As another motivation, we point out that the current *best* trade-off between rate and relative distance (for a code over constant sized alphabet) is achieved by a non-linear code comprising of precisely a bad list-decoding configuration in certain algebraic-geometric codes [107]. Unfortunately the associated received word is only shown to exist by a counting argument and its explicit specification will be required to get explicit codes with these parameters.

6.2.3 Proof Approach

We show our result on list recovering Reed-Solomon codes by proving a super-polynomial (in $n = q^m$) bound on the number of polynomials over $\mathbb{F}_{q^m}$ of degree k that take values in $\mathbb{F}_q$ at every point in $\mathbb{F}_{q^m}$, for any prime power q where k is roughly q^{m-1}. Note that this implies that there can be a super-polynomial number of solutions to list recovery when input list sizes are $\lceil \frac{n}{k} \rceil$. We establish this bound on the number of such polynomials by exploiting a folklore connection of such polynomials to a classic family of cyclic codes called BCH codes, followed by an (exact) estimation of the size of BCH codes with certain parameters. We also write down an explicit collection of polynomials, obtained by taking $\mathbb{F}_q$-linear combinations of translated norm functions, all of which take values only in $\mathbb{F}_q$. By the BCH bound, we conclude that this in fact is a precise description of the collection of all such polynomials.

Our explicit construction of a received word $\mathbf{y}$ with several RS codewords (for low rate RS codes) with non-trivial agreement with $\mathbf{y}$ is obtained using ideas from [25] relating to representations of elements in an extension finite field by products of distinct linear factors. Our explicit construction for high rate RS codes is obtained by looking at cosets of certain prime fields.

6.3 BCH Codes and List Recovering Reed-Solomon Codes

6.3.1 Main Result

We will work with polynomials over $\mathbb{F}_{q^m}$ of characteristic p where q is a power of p, and $m \geqslant 1$. Our goal in this section is to prove the following result, and in Section 6.3.2 we will use it to state corollaries on limits to list decodability of Reed-Solomon codes. (We will only need a lower bound on the number of polynomials with the stated property but the result below in fact gives an exact estimation, which in turn is used in Section 6.3.4 to give a precise characterization of the concerned polynomials.)

Theorem 6.1. *Let q be a prime power, and $m \geqslant 1$ be an integer. Then, the number of univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $\frac{q^m-1}{q-1}$ which take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$ is exactly q^{2^m}. That is,*

$$\left|\{P(z) \in \mathbb{F}_{q^m}[z] \mid \textit{deg}(P) \leqslant \frac{q^m-1}{q-1} \textit{ and } \forall \alpha \in \mathbb{F}_{q^m}, P(\alpha) \in \mathbb{F}_q\}\right| = q^{2^m}$$

In the rest of this section, we prove Theorem 6.1. The proof is based on a connection of polynomials with the stated property to a family of cyclic codes called BCH codes, followed by an estimation of the size (or dimension) of the associated BCH code. Now, the latter estimation itself uses basic algebra. In particular one can prove Theorem 6.1 using finite field theory and Fourier transform without resorting to coding terminology. However, the connection to BCH codes is well known and we use this body of prior work to modularize our presentation.

We begin with the definition of BCH codes[2]. We point the reader to [80], Ch. 7, Sec. 6, and Ch. 9, Secs. 1-3, for detailed background information on BCH codes.

Definition 6.2. *Let α be a primitive element of $\mathbb{F}_{q^m}$, and let $n = q^m - 1$. The BCH code* $\mathrm{BCH}_{q,m,d,\alpha}$ *of* designed distance d *is a linear code of block length n over $\mathbb{F}_q$ defined as:*

$$\mathrm{BCH}_{q,m,d,\alpha} = \{\langle c_0, c_1, \dots, c_{n-1}\rangle \in \mathbb{F}_q^n \; | c(\alpha^i) = 0 \textit{ for } i = 1, 2, \dots, d-1, \textit{ where } \\ c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]\}.$$

We will omit one or more the subscripts in $\mathrm{BCH}_{q,m,d,\alpha}$ *for notational convenience when they are clear from the context.*

In our proof, we will use the following well-known result. For the sake of completeness, we present its proof here.

Lemma 6.1 (BCH codes are subfield subcodes of RS codes). *Let q be a prime power and $m \geqslant 1$ an integer. Let $n = q^m - 1$, d be an integer in the range $1 < d < n$, and α be a primitive element of $\mathbb{F}_{q^m}$. Then the set of codewords of* $\mathrm{BCH}_{q,m,d,\alpha}$ *maybe written as*

$$\{\langle P(\alpha^0), P(\alpha^1), \dots, P(\alpha^{n-1})\rangle \in \mathbb{F}_q^n \mid P \in \mathbb{F}_{q^m}[z], \deg(P) \leqslant n-d, \\ \textit{and } P(\gamma) \in \mathbb{F}_q \; \forall \gamma \in \mathbb{F}_{q^m}\}.$$

Proof. Our goal is to prove that the two sets

$$S_1 = \{\; \langle c_0, c_1, \dots, c_{n-1}\rangle \; | c(\alpha^i) = 0 \text{ for } i = 1, 2, \dots, d-1, \text{where} \\ c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x] \;\}\,,$$

$$S_2 = \big\{\langle P(\alpha^0), P(\alpha^1), \dots, P(\alpha^{n-1})\rangle \mid P \in \mathbb{F}_{q^m}[z],\ \deg(P) \leqslant n-d, \text{ and } P(\gamma) \in \mathbb{F}_q \\ \forall \gamma \in \mathbb{F}_{q^m}\big\}\,,$$

are identical. We will do so by showing both the inclusions $S_2 \subseteq S_1$ and $S_1 \subseteq S_2$.

We begin with showing $S_2 \subseteq S_1$. Let $P(z) = \sum_{j=0}^{n-d} a_j z^j \in \mathbb{F}_{q^m}[z]$ be a polynomial of degree at most $(n-d)$ that takes values in $\mathbb{F}_q$. Then, for $r = 1, 2, \dots, d-1$, we have

$$\sum_{i=0}^{n-1} P(\alpha^i)(\alpha^r)^i = \sum_{i=0}^{n-1}\Big(\sum_{j=0}^{n-d} a_j \alpha^{ij}\Big)\alpha^{ri} = \sum_{j=0}^{n-d} a_j \sum_{i=0}^{n-1}(\alpha^{r+j})^i = 0\,,$$

where in the last step we use that $\sum_{i=0}^{n-1}\gamma^i = 0$ for every $\gamma \in \mathbb{F}_{q^m} \setminus \{1\}$ and $\alpha^{r+j} \neq 1$ since $1 \leqslant r+j \leqslant n-1$ and α is primitive. Therefore, $\langle P(\alpha^0), P(\alpha^1), \dots, P(\alpha^{n-1})\rangle \in S_1$.

[2] What we define are actually referred to more specifically as *narrow-sense primitive* BCH codes, but we will just use the term BCH codes for them.

We next proceed to show the inclusion $S_1 \subseteq S_2$. Suppose $\langle c_0, c_1, \ldots, c_{n-1}\rangle \in S_1$. For $0 \leqslant j \leqslant n-1$, define (this is the "inverse Fourier transform")

$$a_j = \frac{1}{n}\sum_{i=0}^{n-1} c_i \alpha^{-ji} \ ,$$

where by $\frac{1}{n}$, we mean the multiplicative inverse of $n \cdot 1$ in the field $\mathbb{F}_{q^m}$. Note that $a_j = \frac{1}{n}c(\alpha^{-j}) = \frac{1}{n}c(\alpha^{n-j})$ where $c(x) = \sum_{i=0}^{n-1} c_i x^i$. So, by the definition of S_1, it follows that $a_j = 0$ for $j > n-d$. Therefore the polynomial $P(z) \in \mathbb{F}_{q^m}$ defined by

$$P(z) = \sum_{j=0}^{n-1} a_j z^j = \sum_{j=0}^{n-d} a_j z^j$$

has degree at most $(n-d)$.

We now claim that for $P(\alpha^s) = c_s$ for $0 \leqslant s \leqslant n-1$. Indeed,

$$\begin{aligned} P(\alpha^s) &= \sum_{j=0}^{n-1} a_j \alpha^{sj} = \sum_{j=0}^{n-1}\left(\frac{1}{n}\sum_{i=0}^{n-1} c_i \alpha^{-ji}\right)\alpha^{sj} \\ &= \sum_{i=0}^{n-1}\frac{c_i}{n}\sum_{j=0}^{n-1}(\alpha^{s-i})^j = c_s \ , \end{aligned}$$

where in the last step we used the fact that $\sum_{j=0}^{n-1}(\alpha^{s-i})^j = 0$ whenever $i \neq s$, and equals n when $i = s$. Therefore, $\langle c_0, c_1, \ldots, c_{n-1}\rangle = \langle P(\alpha^0), \ldots, P(\alpha^{n-1})\rangle$. We are pretty much done, except that we have to check also that $P(0) \in \mathbb{F}_q$ (since we wanted $P(\gamma) \in \mathbb{F}_q$ for all $\gamma \in \mathbb{F}_{q^m}$, including $\gamma = 0$). Note that $P(0) = a_0 = \frac{1}{n} \cdot \sum_{i=0}^{n-1} c_i$. Since $n = q^m - 1$, we have $n + 1 = 0$ in $\mathbb{F}_{q^m}$ and so $\frac{1}{n} = -1 \in \mathbb{F}_q$. This together with the fact that $c_i \in \mathbb{F}_q$ for every i implies that $P(0) \in \mathbb{F}_q$ as well, completing the proof. □

In light of the above lemma, in order to prove Theorem 6.1, we have to prove that $|\mathrm{BCH}_{q,m,d,\alpha}| = q^{2m}$ when $d = (q^m - 1)(1 - \frac{1}{q-1})$. We turn to this task next. We begin with the following bound on the size of BCH codes [15, Ch. 12]. For the sake of completeness, we also give a proof sketch.

Lemma 6.2 (Dimension of BCH Codes). *For integer i, n, let $\lfloor i \rfloor_n$ be a shorthand for i* mod *n. Then $|\mathrm{BCH}_{q,m,d,\alpha}| = q^{|I(q,m,d)|}$ where*

$$I(q,m,d) = \{i \mid 0 \leqslant i \leqslant n-1, \lfloor iq^j \rfloor_n \leqslant n - d \, \textit{for all} \, j, 0 \leqslant j \leqslant m-1\} \qquad (6.1)$$

for $n = q^m - 1$. (Note that for this value of n, if $i = i_0 + i_1 q + \cdots i_{m-1}q^{m-1}$, then $\lfloor iq \rfloor_n = i_{m-1} + i_0 q + i_1 q^2 + \cdots + i_{m-2}q^{m-1}$, and so $\lfloor iq \rfloor_n$ is obtained by a simple cyclic shift of the q-ary representation of i.)

Proof. It follows from Definition 6.2 that the BCH codewords are simply polynomials $c(x)$ over $\mathbb{F}_q$ of degree at most $(n-1)$ that vanish at α^i for $1 \leqslant i < d$. Note that if $c(x), c'(x)$ are two such polynomials, then so is $c(x)+c'(x)$. Moreover, since $\alpha^n = 1$, $xc(x) \mod (x^n-1)$ also vanishes at each designated α^i. It follows that if $c(x)$ is a codeword, then so is $r(x)c(x) \mod (x^n - 1)$ for every polynomial $r(x) \in \mathbb{F}_q[x]$.

In other words $\mathrm{BCH}_{q,m,d}$ is an *ideal* in the quotient ring $R = \mathbb{F}_q[x]/(x^n-1)$. It is well known that R is a principal ideal ring, i.e., a ring in which every ideal is generated by one element [77, Chap. 1, Sec. 3]. Therefore there is a unique monic polynomial $g(x) \in \mathbb{F}_q[x]$ such that

$$\mathrm{BCH}_{q,m,d,\alpha} = \{g(x)h(x) \mid h(x) \in \mathbb{F}_q[x]; \deg(h) \leqslant n-1-\deg(g)\}$$

It follows that $|\mathrm{BCH}_{q,m,d,\alpha}| = q^{n-\deg(g)}$, and so it remains to prove that $\deg(g) = n - |I(q,m,d)|$ where $I(q,m,d)$ is defined as in (6.1).

It is easily argued that the polynomial $g(x)$ is the monic polynomial of lowest degree over $\mathbb{F}_q$ that has α^i for every i, $1 \leqslant i < d$, as roots. It is well known ([80, Chap. 7, Sec. 5]) that $g(x)$ is then given by

$$g(x) = \prod_{\beta \in M(\alpha) \cup M(\alpha^2) \cdots \cup M(\alpha^{d-1})} (x-\beta),$$

where $M(\alpha^i)$ is the *cyclotomic coset*[3]of α^i. Further for the ease of notation, define $M_{d,\alpha} = M(\alpha) \cup M(\alpha^2) \cdots \cup M(\alpha^{d-1})$. To complete the proof we will show that

$$\mid M_{d,\alpha} \mid = n - \mid I(q,m,d) \mid . \tag{6.2}$$

To prove (6.2), we claim that for every $0 \leqslant i \leqslant n-1$, $\alpha^i \in M_{d,\alpha}$ if and only if $(n-i) \notin I(m,q,d)$. To see that this is true note that $(n-i) \notin I(q,m,d)$ if and only if there is a $0 \leqslant j_i < m$ such that $\lfloor (n-i)q^{j_i} \rfloor_n = n - i^* > n-d$. In other words, $\lfloor iq^{j_i} \rfloor_n = i^*$, where $0 \leqslant i^* < d$. This implies that $(n-i) \notin I(q,m,d)$ if and only if $\alpha^i \in M(\alpha^{i^*}) \subseteq M_{d,\alpha}$, which proves the claim. □

Let's now use the above to compute the size of $\mathrm{BCH}_{q,m,d,\alpha}$ where $d = (q^m-1) - \frac{q^m-1}{q-1}$. We need to compute the quantity $|I(q,m,d)|$, i.e., the number of i, $0 \leqslant i < q^m - 1$ such that $\lfloor iq^j \rfloor_{q^m-1} \leqslant \frac{q^m-1}{q-1} = 1 + q + \cdots + q^{m-1}$ for each $j = 0, 1, \ldots, m-1$. This condition is equivalent to saying that if $i = i_0 + i_1 q + \cdots + i_{m-1}q^{m-1}$ is the q-ary expansion of i, then all the m integers whose q-ary representations are cyclic shifts of $(i_0, i_1, \ldots, i_{m-1})$ are $\leqslant 1 + q + \cdots + q^{m-1}$. Clearly, this condition is satisfied if and only if for each $j = 0, 1, \ldots, m-1$, $i_j \in \{0,1\}$. There are 2^m choices for i with this property, and hence we conclude $|I(q,m,d)| = 2^m$ when $d = (q^m-1) - \frac{q^m-1}{q-1}$.

[3] In other words $M(\alpha^i) = \{\alpha^i, \alpha^{\lfloor iq \rfloor_n}, \ldots, \alpha^{\lfloor iq^{m_i-1} \rfloor_n}\}$, where m_i is the smallest integer such that $\lfloor iq^{m_i} \rfloor_n = i$.

Together with Lemma 6.1, we conclude that the number of polynomials of degree at most $\frac{q^m-1}{q-1}$ over $\mathbb{F}_{q^m}$ which take on values only in $\mathbb{F}_q$ at every point in $\mathbb{F}_{q^m}$ is precisely q^{2^m}. This is exactly the claim of Theorem 6.1.

Before moving on to state implications of the above result for Reed-Solomon list decoding, we state the following variant of Theorem 6.1.

Theorem 6.2. *Let q be a prime power, and $m \geqslant 1$ be an integer. Then, for each s, $1 \leqslant s \leqslant m$, the number of univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $\sum_{j=1}^{s} q^{m-j}$ which take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$ is at least $q^{\sum_{j=0}^{s}\binom{m}{j}}$. And the number of such polynomials of degree strictly less than q^{m-1} is exactly q (namely just the constant polynomials, so there are no polynomials with this property for degrees between 1 and $q^{m-1}-1$).*

Since the proof of the theorem above is similar to the proof of Theorem 6.1, we will just sketch it here. By Lemmas 6.1 and 6.2, to count the number of univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $q^{m-1} + \cdots + q^{m-s}$ which take values in $\mathbb{F}_q$, we need to count the number of integers $i = i_0 + i_1 q + \cdots + i_{m-1}q^{m-1}$ such that all integers corresponding to cyclic shifts of $(i_0, \ldots, i_{m-1})$ are at most $q^{m-1} + \cdots + q^{m-s}$. It is easy to see all integers i such that $i_j \in \{0, 1\}$ for all j and $i_j = 1$ for at most s values of j, satisfy the required condition. The number of such integers is $\sum_{j=0}^{s}\binom{m}{j}$, which implies the bound claimed in the theorem. The argument when degree is $< q^{m-1}$ is similar. In this case we have to count the number of integers $i_0 + i_1 q + \cdots + i_{m-1}q^{m-1}$ such that all integers corresponding to all cyclic shifts of $(i_0, \ldots, i_{m-1})$ is $< q^{m-1}$. Note that if $i_j \neq 0$ for some $0 \leqslant j \leqslant m-1$, then the $(m-1-j)$th shift with be at least q^{m-1}. Thus, only $i = 0$ satisfies the required condition, which implies claimed bound in the theorem.

6.3.2 Implications for Reed-Solomon List Decoding

In the result of Theorem 6.1, if we imagine keeping $q \geqslant 3$ fixed and letting m grow, then for the choice $n = q^m$ and $k = (q^m-1)/(q-1)$ (so that $\lceil \frac{n}{k} \rceil = q$), Theorem 6.1 immediately gives us the following "negative" result on polynomial reconstruction algorithms and Reed-Solomon list decoding.[4]

Theorem 6.3. *For every prime power $q \geqslant 3$, there exist infinitely many pairs of integers k, n such that $\lceil \frac{n}{k} \rceil = q$ for which there are Reed-Solomon codes of dimension $(k+1)$ and block length n, such that noiselessly list recovering them with input lists of size $\lceil \frac{n}{k} \rceil$ requires super-polynomial (in fact $q^{n^{1/\lg q}}$) output list size.*

The above result is exactly tight in the following sense. It is easy to argue combinatorially (via the "Johnson type" bounds, cf. [64]) that when $\ell < \lceil \frac{n}{k} \rceil$, the number of codewords

[4] We remark that we used the notation $n = q^m - 1$ in the previous subsection, but for this Subsection we will take $n = q^m$.

is polynomially bounded. Moreover [63] presents a polynomial time algorithm to recover all the solution codewords in this case. As was mentioned in the introduction, our results also show the tightness of noiselessly list recovering Reed-Solomon codes in the special setting of Ar, Lipton, Rubinfeld and Sudan [3]. One of the problems considered in [3] is that of noiselessly list recovering Reed-Solomon codes with list size ℓ, when the set S_i at every position i is the set of values of *fixed* ℓ codewords at position i. Note that our lower bound also works in this restricted model if one takes the q fixed codewords to be the q constant codewords.

The algorithm in [63] solves the more general problem of finding all polynomials of degree at most k which agree with at least t out of n' distinct pairs (β_i, γ_i) whenever $t > \sqrt{kn'}$. The following corollary states that, in light of Theorem 6.3, this is essentially the best possible trade-off one can hope for from such a general algorithm. We view this as providing the message that a list-decoding algorithm for Reed-Solomon codes that works with fractional agreement t/n that is less than $\sqrt{R}$ where R is the rate, must exploit the fact that the evaluation points β_i are distinct or almost distinct (by which we mean that no β_i is repeated too many times). Note that for small values of R (close to 0), our result covers even an improvement of the necessary fractional agreement by $O(R)$ which is substantially smaller than $\sqrt{R}$.

Corollary 6.4. *Suppose $\mathcal{A}$ is an algorithm that takes as input n' distinct pairs $(\beta_i, \gamma_i) \in \mathbb{F}^2$ for an arbitrary field $\mathbb{F}$ and outputs a list of all polynomials p of degree at most k for which $p(\beta_i) = \gamma_i$ for more than $\sqrt{kn'} - \frac{k}{2}$ pairs. Then, there exist inputs under which $\mathcal{A}$ must output a list of super-polynomial size.*

Proof. Note that in the list recovery setting of Theorem 6.3, the total number of pairs $n' = n\ell = n\lceil \frac{n}{k} \rceil < n(\frac{n}{k} + 1)$, and the agreement parameter $t = n$. Then

$$\sqrt{kn'} - \frac{k}{2} < \sqrt{kn\Big(\frac{n}{k} + 1\Big)} - \frac{k}{2} = n\sqrt{1 + \frac{k}{n}} - \frac{k}{2}$$

$$\leqslant n\Big(1 + \frac{k}{2n}\Big) - \frac{k}{2} = n = t\,.$$

Therefore there can be super-polynomially many candidate polynomials to output even when the agreement parameter t satisfies $t > \sqrt{kn'} - k/2$. □

6.3.3 Implications for List Recovering Folded Reed-Solomon Codes

In this subsection, we will digress a bit and see what the ideas in Section 6.3.1 imply about list recoverability of folded Reed-Solomon codes. Recall that a folded Reed-Solomon code with folding parameter m is just a Reed-Solomon code with m consecutive evaluation pointsbundled together (see Chapter 3). In particular, if we start with an $[n, k]$ Reed-Solomon code, then we get an $(N = n/m, K = k/m)$ folded Reed-Solomon code.

It is not too hard to check that the one can generalize Theorem 6.1 to show the following. Let $a \geqslant 1$ be an integer and q be a prime power. Then there are q^{2^a} codewords from an $\left(\frac{q^a}{m}, \frac{q^a-1}{m(q-1)}\right)$ folded Reed-Solomon code such that every symbol of such a codeword takes a value in $(\mathbb{F}_q)^m$. The set of q^{2^a} folded Reed-Solomon codewords are just the q^{2^a} BCH codewords from Theorem 6.1, with m consecutive positions in the BCH codeword "folded" into one symbol. Thus, this shows that an (N, K) folded Reed-Solomon code (with folding parameter m) cannot be noiselessly list recovered with input lists of size $\left(\frac{N}{K}\right)^m$.

Let us now recall the algorithmic results for (noiselessly) list recovering folded Reed-Solomon codes. From (3.6) it follows that an (N, K) folded Reed-Solomon code (with folding parameter m) can be noiselessly list recovered with input lists of size ℓ if

$$N \geqslant \left(1+\frac{s}{r}\right)\left(\frac{m}{m-s+1}\right)\sqrt[s+1]{NK^s\ell},$$

where $1 \leqslant s \leqslant m$, and $r \geqslant s$ are parameters that we can choose. Thus for any $\varepsilon > 0$ if $r = \frac{s}{\varepsilon}$, then we can satisfy the above condition if

$$\ell \leqslant (1-\varepsilon)^{s+1}\left(\frac{N}{K}\right)^s\left(\frac{m-s+1}{m}\right)^{s+1}. \tag{6.3}$$

The bound above unfortunately is much smaller than the bound of $(N/K)^m$, unlike the case of Reed-Solomon codes where the two bounds were (surprisingly) tight. For the case when $K = o(N)$, however one can show that for any $\delta > 0$, the bound in (6.3) is at least $(N/K)^{m(1-\delta)}$. Indeed, one can choose $s = m(1-\delta/2)$, in which case the bound in (6.3) is $(N/K)^{m(1-\delta)} \cdot (N/K)^{m\delta/2}(\delta/2)^{m(1-\delta/2)+1}(1-\varepsilon)^{m(1-\delta/2)+1}$. The claimed expression follows by noting that $N/K = \omega(1)$ while δ, ε and m are all $O(1)$.

6.3.4 A Precise Description of Polynomials with Values in Base Field

We proved in Section 6.3.1, for $Q = \frac{q^m-1}{q-1}$, there are exactly q^{2^m} polynomials over $\mathbb{F}_{q^m}$ of degree Q or less that evaluate to a value in $\mathbb{F}_q$ at every point in $\mathbb{F}_{q^m}$. The proof of this obtains the coefficients of such polynomials using a "Fourier transform" of codewords of an associated BCH code, and as such gives little insight into the structure of these polynomials. One of the natural questions to ask is: Can we say something more concrete about the structure of these q^{2^m} polynomials? In this section, we answer this question by giving an exact description of the set of all these q^{2^m} polynomials.

We begin with the following well-known fact which simply states that the "Norm" function of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ takes only values in $\mathbb{F}_q$.

Lemma 6.3. *For all $x \in \mathbb{F}_{q^m}$, $x^{\frac{q^m-1}{q-1}} \in \mathbb{F}_q$.*

Theorem 6.5. *Let q be a prime power, and let $m \geqslant 1$. Let α be a primitive element of $\mathbb{F}_{q^m}$. Then, there are exactly q^{2^m} univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $Q = \frac{q^m-1}{q-1}$*

that take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$, and these are precisely the polynomials in the set

$$N = \{ \sum_{i=0}^{2^m-1} \beta_i (z+\alpha^i)^Q \ \mid \ \beta_0, \beta_1, \ldots, \beta_{2^m-1} \in \mathbb{F}_q \} \,.$$

Proof. By Lemma 6.3, clearly every polynomial P in the set N satisfies $P(\gamma) \in \mathbb{F}_q$ for all $\gamma \in \mathbb{F}_{q^m}$. The claim that there are exactly q^{2^m} polynomials over $\mathbb{F}_{q^m}$ of degree Q or less that take values only in $\mathbb{F}_q$ was already established in Theorem 6.1. So the claimed result that N precisely describes the set of all these polynomials follows if we show that $|N| = q^{2^m}$.

Note that by definition, $|N| \leqslant q^{2^m}$. To show that $|N| \geqslant q^{2^m}$, it clearly suffices to show (by linearity) that if

$$\sum_{i=0}^{2^m-1} \beta_i (z+\alpha^i)^Q = 0 \tag{6.4}$$

as polynomials in $\mathbb{F}_{q^m}[z]$, then $\beta_0 = \beta_1 = \cdots = \beta_{2^m-1} = 0$. We will prove this by setting up a full rank homogeneous linear system of equations that the β_i's must satisfy. For this we need Lucas' theorem, stated below.

Lemma 6.4 (Lucas' Theorem, cf. [47]). *Let p be a prime. Let a and b be positive integers with p-ary expansions $a_0 + a_1 p + \cdots + a_r p^r$ and $b_0 + b_1 p + \cdots + b_r p^r$ respectively. Then $\binom{a}{b} = \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_r}{b_r} \mod p$, which gives us $\binom{a}{b} \neq 0 \mod p$ if and only if $a_j \geqslant b_j$ for all $j \in \{0, 1, \cdots, r\}$.*

Define the set

$$T = \{ \ \sum_{j \in S} q^j \ \mid \ S \subseteq \{0, \cdots, m-1\} \ \} \,.$$

Applying Lemma 6.4 with p being the characteristic of the field $\mathbb{F}_q$, we note that when operating in the field $\mathbb{F}_{q^m}$, the binomial coefficient of z^j in the expansion of $(z+\alpha^i)^Q$ is 1 if $j \in T$ and 0 otherwise. It follows that (6.4) holds if and only if $\sum_{i=0}^{2^m-1} (\alpha^i)^{Q-j}\beta_i = 0$ for all $j \in T$, which by the definition of T and the fact that $Q = 1 + q + q^2 + \cdots + q^{m-1}$ is equivalent to

$$\sum_{i=0}^{2^m-1} (\alpha^j)^i \beta_i = 0 \ \text{ for all } j \in T. \tag{6.5}$$

Let us label the 2^m elements $\{\alpha^j \mid j \in T\}$ as $\alpha_0, \alpha_1, \ldots, \alpha_{2^m-1}$ (note that these are *distinct* elements of $\mathbb{F}_{q^m}$ since α is primitive in $\mathbb{F}_{q^m}$). The coefficient matrix of the homogeneous system of equations (6.5) with unknowns $\beta_0, \ldots, \beta_{2^m-1}$ is then the Vandermonde matrix

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^{2^m-1} \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{2^m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{2^m-1} & \alpha_{2^m-1}^2 & \cdots & \alpha_{2^m-1}^{2^m-1} \end{pmatrix},$$

which has full rank. Therefore, the only solution to the system (6.5) is $\beta_0 = \beta_1 = \cdots = \beta_{2^m-1} = 0$, as desired. □

6.3.5 Some Further Facts on BCH Codes

The results in the previous subsections show that a large number (q^{2^m}) of polynomials over $\mathbb{F}_{q^m}$ take on values in $\mathbb{F}_q$ at every evaluation point, and this proved the tightness of the "square-root" bound for agreement $t = n = q^m$ and total number of points $n' = nq$ (recall Corollary 6.4). It is a natural question whether similarly large list size can be shown at other points (t, n'), specifically for slightly smaller n' and t. For example, what if $n' = n(q-1)$ and we consider list recovery from lists of size $q-1$. In particular, how many polynomials of degree at most $Q = (q^m - 1)/(q-1)$ take on values in $\mathbb{F}_q \setminus \{0\}$ at t points in $\mathbb{F}_{q^m}$. It is easily seen that when $t = n = q^m$, there are precisely $(q-1)$ such polynomials, namely the constant polynomials that equal an element of $\mathbb{F}_q^*$. Indeed, by the Johnson bound, since $t > \sqrt{Qn'}$ for the choice $t = n$ and $n' = n(q-1)$, we should not expect a large list size. However, even for the slightly smaller amount of agreement $t = n - 1 = \lfloor \sqrt{Qn'} \rfloor$, there are only about a linear in n number of codewords, as Lemma 6.5 below shows. Hence obtaining super-polynomial number of codewords at other points on the square-root bound when the agreement t is less than the block length remains an interesting question, which perhaps the BCH code connection just by itself cannot resolve.

Lemma 6.5. *Let q be a prime power and let $m > 1$. For any polynomial $P(z)$ over $\mathbb{F}_{q^m}[z]$, let its Hamming weight be defined as $|\{\beta \in \mathbb{F}_{q^m} | P(\beta) \neq 0\}|$. Then, there are exactly $(q-1)q^m$ univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $Q = \frac{(q^m-1)}{q-1}$ that take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$ and that have Hamming weight $(q^m - 1)$. Furthermore, these are precisely the polynomials in the set $W = \{\lambda(z+\beta)^Q \mid \beta \in \mathbb{F}_{q^m}, \lambda \in \mathbb{F}_q^*\}$.*

Proof. It is obvious that all the polynomials in W satisfy the required property and are distinct polynomials. We next show that any polynomial of degree at most Q that satisfies the required properties belongs to W completing the proof.

Let $P(z)$ be a polynomial of degree at most Q that satisfies the required properties. We must show that $P(z) \in W$. Let $\gamma \in \mathbb{F}_{q^m}$ be such that $P(\gamma) = 0$. Clearly, for each $\beta \in (\mathbb{F}_{q^m} \setminus \{\gamma\})$, $P(\beta)/(\beta - \gamma)^Q \in \mathbb{F}_q^*$. By a pigeonhole argument, there must exist some $\lambda \in \mathbb{F}_q^*$ such that $P(\beta) = \lambda(\beta - \gamma)^Q$ for at least $\frac{q^m-1}{q-1} = Q$ values of β in $\mathbb{F}_{q^m} \setminus \{\gamma\}$. Since $P(\gamma) = 0$, we have that the degree Q polynomials $P(z)$ and $\lambda(z-\gamma)^Q$ agree on at least $Q+1$ field elements, which means that they must be equal to each other. Thus the polynomial $P(z)$ belongs to W and the proof is complete. □

6.4 Explicit Hamming Balls with Several Reed-Solomon Codewords

Throughout this section, we will be concerned with an $[q, k+1]$ Reed-Solomon code $\mathrm{RS}[q, k+1]$ over $\mathbb{F}_q$. We will be interested in a received word $\mathbf{y} \in \mathbb{F}_q^q$ such that a super-polynomial number of codewords of $\mathrm{RS}[q, k+1]$ agree with $\mathbf{y}$ on t or more positions, and the aim would be to prove such a result for t non-trivially larger than k. We start with the existential result.

6.4.1 Existence of Bad List Decoding Configurations

It is easy to prove the *existence* of a received word $\mathbf{y}$ with at least $\binom{q}{t}/q^{t-k}$ codewords with agreement at least t with $\mathbf{y}$. One way to see this is that this quantity is the expected number of such codewords for a received word that is the evaluation of a *random* polynomial of degree t [70].[5]

We have the following lower bound on $\binom{q}{t}/q^{t-k}$:

$$\frac{\binom{q}{t}}{q^{t-k}} \geqslant \frac{q^t}{t^t q^{t-k}} = \frac{q^k}{t^t} = 2^{k\log q - t\log t}.$$

Now when $k = q^\delta$ for some $\delta > 0$ and $t = \frac{q^\delta}{2\delta}$, then $k\log q - t\log t$ is $\Omega(q^\delta \log q)$, which implies that the number of RS codewords with agreement t with the received word $\mathbf{r}$ is $q^{\Omega(q^\delta)}$.

On the other hand, if $k = \Omega(q)$ let $t = k + \Delta$, where $\Delta = \frac{k}{2\log q}$ (we also assume $t \leqslant q/2$). Now, $k\log q - t\log t \geqslant k\log q - (k+\Delta)(\log q - 1) = k + \Delta - \Delta\log q \geqslant k/2$. Thus, we get $2^{\Omega(q)}$ RS codewords with agreement $t = k + O\left(\frac{q}{\log q}\right)$ with the received word $\mathbf{r}$.

In the remainder of the chapter, we will try to match these parameters with *explicit* received words. We will refer to Reed-Solomon codes with constant rate as *high* rate Reed-Solomon codes and to Reed-Solomon codes with inverse polynomial rate as *low* rate Reed-Solomon codes.

6.4.2 Low Rate Reed-Solomon Codes

Another argument for the existence of a bad list-decoding configuration (from the previous subsection), as suggested in [25], is based on an element β in $\mathbb{F}_{q^h} = \mathbb{F}_q(\alpha)$, for some positive integer h, that can be written as a product $\prod_{a\in T}(\alpha + a)$ for at least $\binom{q}{t}/q^h$ subsets $T \subset \mathbb{F}_q$ with $|T| = t$ — the *existence* of such a β again follows by a trivial counting argument. Here we use the result due to Cheng and Wan [25] that for certain settings of parameters and fields such a β can be explicitly specified with only a slight loss in the number of subsets T, and thereby get an *explicit received word* $\mathbf{y}$ with several close-by codewords from $\mathrm{RS}[q, k+1]$.

[5] The bound can be improved slightly to $\binom{q}{t}/q^{t-1-k}$ by using a random *monic* polynomial.

Theorem 6.6 ([25]). *Let $\varepsilon > 0$ be arbitrary. Let q be a prime power, h be a positive integer and α be such that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^h}$. For any $\beta \in \mathbb{F}^*_{q^h}$, let $N_t(\beta)$ denote the number of t-tuples $\langle a_1, a_2, \ldots, a_t \rangle$ of distinct $a_i \in \mathbb{F}_q$ such that $\beta = \prod_{i=1}^{t}(\alpha + a_i)$. If $t \geqslant (\frac{4}{\varepsilon} + 2)(h+1)$, $\varepsilon < t - 2$ and $q \geqslant \max(t^2, (h-1)^{\frac{(2+\varepsilon)t}{t-(2+\varepsilon)}})$, then for all $\beta \in \mathbb{F}^*_{q^h}$, $N_t(\beta) > (t-1)q^{t-h-1}$.*

Proof. From the proof of Theorem 3 in [25], we obtain $N_t(\beta) \geqslant E_1 - E_2$, where $E_1 = \frac{q^t - \binom{t}{2}q^{t-1}}{q^h - 1}$ and $E_2 = (1 + \binom{t}{2})(h-1)^t q^{\frac{t}{2}}$. Observe that from the choice of q, $\binom{t}{2} = \frac{t^2}{2} - \frac{t}{2} \leqslant \frac{q-t}{2}$.

We first give a lower bound on E_1. Indeed, using $\binom{t}{2} \leqslant \frac{q-t}{2}$ and $q^h - 1 < q^h$, we have $E_1 > \frac{2q^t - (q-t)q^{t-1}}{2q^h} = \frac{q^{t-h}}{2} + \frac{t}{2}q^{t-h-1}$.

Note that from our choice of t, we have $t > (\frac{4}{\varepsilon} + 2)h$, that is, $t - h > (\frac{4+\varepsilon}{4+2\varepsilon})t$. Further, from our choice of q, $(h-1)^t \leqslant q^{\frac{t}{2+\varepsilon}-1}$. We now bound E_2 from above. From our bounds on $\binom{t}{2}$ and $(h-1)^t$, we have $E_2 \leqslant (1 + \frac{q-t}{2})q^{(\frac{4+\varepsilon}{4+2\varepsilon})t-1} < (1 + \frac{q-t}{2})q^{t-h-1} = \frac{q^{t-h}}{2} - (\frac{t}{2} - 1)q^{t-h-1}$, where the second inequality comes from our bound on $t - h$.

Combining the bounds on E_1 and E_2 proves the theorem. □

We now state the main result of this section concerning Reed-Solomon codes:

Theorem 6.7. *Let $\varepsilon > 0$ be arbitrary real, q a prime power, and h any positive integer. If $t \geqslant (\frac{4}{\varepsilon} + 2)(h+1)$ and $q \geqslant \max(t^2, (h-1)^{\frac{(2+\varepsilon)t}{t-(2+\varepsilon)}})$ then for every k in the range $t - h \leqslant k \leqslant t - 1$, there exists an explicit received word $\mathbf{y} \in \mathbb{F}_q^q$ such that there are at least $\frac{q^k}{t!\binom{k+h}{t}}$ codewords of $\mathrm{RS}[q, k+1]$ that agree with $\mathbf{y}$ in at least t positions.*

We will prove the above theorem at the end of this section. As $\varepsilon \to 0$, and $q, k, h \to \infty$ in the above, we can get super-polynomially many codewords with agreement $(1+\delta)k$ for some $\delta = \delta(\varepsilon) > 0$ for a Reed-Solomon code of dimension tending to $q^{1/2}$. As $\varepsilon \to \infty$, we can get super-polynomially many codewords with agreement tending to $2k$ with dimension still being $q^{\Omega(1)}$. We record these as two corollaries below (for the sake of completeness, we sketch the proofs). We note that the non-explicit bound $\binom{q}{t}/q^{t-k}$ gives a super-polynomial number of codewords for agreement $t \geqslant k/\delta$ for dimension about $k = q^{\delta - o(1)}$, where as our explicit construction can give agreement at most $2k$ (or dimension at most $\sqrt{q}$).

Corollary 6.8. *For all $0 < \gamma < 1$, and primes p, there exists $\delta > 0$ such that for any power of p (call it q) that is large enough, there exists an explicit $\mathbf{y} \in \mathbb{F}_q^q$ such that the Reed-Solomon code $\mathrm{RS}[q, k+1 = q^\delta + 1]$ contains a super-polynomial (in q) number of codewords with agreement at least $(2-\gamma)k$ with $\mathbf{y}$.*

Proof. For any integer h, choose ε, t and k such that $t = (\frac{4}{\varepsilon} + 2)(h+1)$, $k = t - h + 1$ and $t = (2-\gamma)k$. These relations imply that

$$\varepsilon = \frac{4}{(\frac{2-\gamma}{1-\gamma})(\frac{h-1}{h+1}) - 2}.$$

Note that in the limit as h goes to infinity, $\varepsilon = \frac{4(1-\gamma)}{\gamma}$. Further, choose q to be a prime power such that $pq_0 \geqslant q \geqslant q_0$, where $q_0 = (h-1)^{\frac{2+\varepsilon}{1-(2+\varepsilon)/t}}$. Finally note that as t goes to infinity, $q_0 = (h-1)^{\frac{2(2-\gamma)}{\gamma}}$. For the rest of the proof we will assume that h is large enough so that $\varepsilon \simeq \frac{4(1-\gamma)}{\gamma}$, $q_0 \simeq (h-1)^{\frac{2(2-\gamma)}{\gamma}}$ and $(h-1)^{\frac{2(2-\gamma)}{\gamma}} \geqslant t^2$. Note that now $\delta = \log_q(h-1) - \log_q(1-\gamma) \geqslant \frac{2(2-\gamma)}{\gamma} - \log_q p - \log_q(1-\gamma) > 0$. As all conditions of Theorem 6.7 are satisfied, we have that the relevant number of codewords is at least $\mathcal{B} = \frac{q^k}{(t+1)!}$. Now as $t \simeq \left(\frac{2-\gamma}{1-\gamma}\right)(h+1)$ and h is large enough, we can assume that $t \leqslant \left(\frac{2-\gamma}{1-\gamma}\right)(2h)$. Thus, $t^t \leqslant (2h)^{(\frac{2-\gamma}{1-\gamma})(2h)} \cdot (\frac{2-\gamma}{1-\gamma})^{(\frac{2-\gamma}{1-\gamma})(2h)}$. To finish the proof we will show that $\mathcal{B} \geqslant \frac{q^{ch}}{2^{dh}}$ where c and d are constants which depend on γ. Indeed as $(t+1)! \leqslant t^t$, and $k \geqslant h$, we have

$$\frac{q^k}{(t+1)!} \geqslant \frac{q^h}{(2h)^{(\frac{2-\gamma}{1-\gamma})(2h)} \cdot (\frac{2-\gamma}{1-\gamma})^{(\frac{2-\gamma}{1-\gamma})(2h)}}.$$

Since h is large enough, $q \geqslant (h/2)^{\frac{2(2-\gamma)}{\gamma}}$, which along with the above inequality implies that

$$\mathcal{B} \geqslant \frac{h^{h\left(\frac{2(2-\gamma)}{\gamma}\right)}}{h^{(\frac{2-\gamma}{1-\gamma})(2h)}} \cdot \frac{1}{2^{\frac{2(2-\gamma)h}{\gamma}} 2^{(\frac{2-\gamma}{1-\gamma})(2h)} (\frac{2-\gamma}{1-\gamma})^{(\frac{2-\gamma}{1-\gamma})(2h)}} \geqslant \frac{h^{h\left(\frac{2(2-\gamma)}{\gamma}\right)\left(1-\frac{\gamma}{1-\gamma}\right)}}{2^{dh}},$$

where d is chosen such that $2^{dh} \geqslant 2^{\frac{2(2-\gamma)h}{\gamma}} 2^{(\frac{2-\gamma}{1-\gamma})(2h)} (\frac{2-\gamma}{1-\gamma})^{(\frac{2-\gamma}{1-\gamma})(2h)}$. Note that such d exists and it only depends on γ. Finally, if $\gamma < 1/2$, then there exists a value c that depends only on γ such that $h^{h\left(\frac{2(2-\gamma)}{\gamma}\right)\left(1-\frac{\gamma}{1-\gamma}\right)} \geqslant q^{ch}$. Thus, we have proved the theorem for $0 < \gamma < 1/2$. Since having an agreement of $2-\gamma$ implies an agreement of $2-\gamma'$ for any $\gamma' \geqslant \gamma$, the proof of the theorem for $0 < \gamma < 1$ follows. □

Corollary 6.9. *For all* $0 < \gamma < \frac{1}{2}$ *and primes p, there exists* $\delta > 0$*, such that for any power of p (call it q) that is large enough, there is an explicit* $\mathbf{y} \in \mathbb{F}_q^q$ *such that the Reed-Solomon code* $\mathrm{RS}[q, k+1 = q^{1/2-\gamma}+1]$ *contains a super-polynomial (in q) number of codewords with agreement at least* $(1+\delta)k$ *with* $\mathbf{y}$.

Proof. The proof is similar to the proof of Corollary 6.8 and hence, most details are skipped. Choose t and k such that $t = (\frac{4}{\varepsilon}+3)(h-1)$ and $k = t-h+1$. Note that for $h > \frac{8}{\varepsilon}+5$, $t > (\frac{4}{\varepsilon}+2)(h+1)$. Also let q be a prime power such that $q_0 \leqslant q \leqslant pq_0$, where $q_0 = (h-1)^{\frac{2+\varepsilon}{1-(2+\varepsilon)/t}}$. As in Corollary 6.8, we consider h to be very large and we have $q_0 \simeq (h-1)^{\frac{2}{1-2\gamma}}$, $t \simeq \frac{1+\gamma}{\gamma}(h-1)$ and $k \simeq \frac{h-1}{\gamma}$. Recalling that $t = (1+\delta)k$, we have $\delta \simeq \gamma$. Again using arguments as in the proof of Corollary 6.8, we have a lower bound of $\Omega(\frac{q^h}{2^{dh}})$ where d is a constant which depends on γ. □

(**Proof of Theorem 6.7**). In what follows, we fix $E(x)$ to be a polynomial of degree h that is irreducible over $\mathbb{F}_q$. For the rest of this proof we will denote $\mathbb{F}_q[x]/(E(x))$ by $\mathbb{F}_{q^h}$. Also note that for any root α of E, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^h}$.

Pick any ℓ where $0 \leqslant \ell \leqslant h-1$ and note that q and t satisfy the conditions of Theorem 6.6. For any $B = (b_0, b_1, \cdots, b_\ell)$, where $b_i \in \mathbb{F}_q$ with at least one non zero b_j; define $L_B(x) \overset{\text{def}}{=} \sum_{i=0}^{\ell} b_i x^i$. Fix $r(x)$ to be an arbitrary non-zero polynomial of degree at most $h-1$. By their definitions, $r(\alpha)$ and $L_B(\alpha)$ are elements of $\mathbb{F}^*_{q^h}$.

We will set the received word $\mathbf{y}$ to be $\langle \frac{r(a)}{E(a)} \rangle_{a \in \mathbb{F}_q}$. Note that since $E(x)$ is an irreducible polynomial, $E(a) \neq 0$ for all $a \in \mathbb{F}_q$, and $\mathbf{y}$ is a well-defined element of $\mathbb{F}_q^q$.

We now proceed to bound from below the number of polynomials of degree $k \overset{\text{def}}{=} t + \ell - h$ that agree with $\mathbf{y}$ on t positions. For each non-zero tuple $B \in \mathbb{F}_q^{\ell+1}$, define $Q_B(x) = -\frac{r(x)}{L_B(x)}$. Clearly, $Q_B(\alpha) \in \mathbb{F}^*_{q^h}$. For notational convenience we will use N_B to denote $N_t(Q_B(\alpha))$. Then, for $j = 1, \cdots, N_B$ there exist $\mathcal{A}_{(B,j)}$ where $\mathcal{A}_{(B,j)} \subset \mathbb{F}_q$ and $|\mathcal{A}_{(B,j)}| = t$ such that $P_B^{(j)}(\alpha) \overset{\text{def}}{=} \prod_{a \in \mathcal{A}_{(B,j)}} (\alpha + a) = Q_B(\alpha)$. By Theorem 6.6, we have $N_B \geqslant (t-1)q^{t-h-1}$ for every B — let us denote by N this latter quantity. Recalling the definition of Q_B, we have that for any (B, j), $\frac{r(\alpha)}{L_B(\alpha)} = -P_B^{(j)}(\alpha)$, or equivalently $r(\alpha) + P_B^{(j)}(\alpha) L_B(\alpha) = 0$. Since E is the irreducible polynomial of α over $\mathbb{F}_q$, this implies that $E(x)$ divides $P_B^{(j)}(x) L_B(x) + r(x)$ in $\mathbb{F}_q[x]$.

Finally we define $T_B^{(j)}(x)$ to be a polynomial of degree $k = t + \ell - h$ such that

$$T_B^{(j)}(x) E(x) = P_B^{(j)}(x) L_B(x) + r(x). \tag{6.6}$$

Clearly $T_B^{(j)}(-a)$ equals $r(-a)/E(-a)$ for each $a \in \mathcal{A}_{(B,j)}$ and thus the polynomial $T_B^{(j)}$ agrees with $\mathbf{y}$ on at least t positions. To complete the proof we will give a lower bound on the number of *distinct* polynomials in the collection $\{T_B^{(j)}\}$. For a fixed B, out of the N_B choices for $P_B^{(j)}$, $t!$ choices of j would lead to the same[6] polynomial of degree t. Since $N_B \geqslant N$, there are at least $\frac{(q^{\ell+1}-1)N}{t!}$ choices of pairs (B, j). Clearly for $j_1 \neq j_2$ the polynomials $P_B^{(j_1)}(x)$ and $P_B^{(j_2)}(x)$ are distinct, however we could have $P_{B_1}^{(j_1)}(x) L_{B_1}(x) = P_{B_2}^{(j_2)}(x) L_{B_2}(x)$ (both are equal to say $S(x)$) leading to $T_{B_1}^{(j_1)}(x) = T_{B_2}^{(j_2)}(x)$. However the degree of S is at most $t + \ell = k + h$, and hence S can have at most $k + h$ roots, and therefore at most $\binom{k+h}{t}$ factors of the form $\prod_{a \in T}(x + a)$ with $|T| = t$. It follows that no single degree k polynomial is counted more than $\binom{k+h}{t}$ times in the collection $\{T_B^{(j)}\}$, and hence there must be at least

$$\frac{(q^{\ell+1}-1)N}{t!\binom{k+h}{t}} \geqslant \frac{q^k}{t!\binom{k+h}{t}}$$

distinct polynomials among them, where we used $N = (t-1)q^{t-h-1}$ and $(q^{\ell+1}-1)(t-1) \geqslant q^{\ell+1} = q^{k-t+h+1}$ since $k = t + \ell - h$. □

[6] If $\langle a_1, \cdots, a_t \rangle$ is a solution of the equation $\beta = \prod_{i=1}^{t}(\alpha + a_i)$ then so is $\langle a_{\sigma(1)}, \cdots, a_{\sigma(t)} \rangle$ for any permutation σ on $\{1, \cdots, t\}$.

6.4.3 High Rate Reed-Solomon Codes

We now consider the case of constant rate Reed-Solomon codes. We start with the main result of this subsection.

Theorem 6.10. *Let $L \geqslant 2$ be an integer. Let $p = aL + 1$ be a prime and define $t = bL$ for any $1 < b < a - 1$. Let the received word $\mathbf{r}$ be the evaluation of $R(X) = X^t$ over $\mathbb{F}_p^*$. Then there are $\binom{a}{b}$ many codewords in $RS[n = p, k = (b-1)L + 1]_{\mathbb{F}_p}$ that agree with $\mathbf{r}$ in at least t places.*

To get some interesting numbers, let's instantiate the parameters in the above theorem. First we need the following result (we will prove this later in the subsection):

Lemma 6.6. *For every $0 < \varepsilon \leqslant 1/(c_L - 1)$, where $1 < c_L < 6$, there exists infinitely many L with prime $p = aL + 1$ such that a is $\Theta(L^\varepsilon)$.*

Corollary 6.11. *Let p be a prime that satisfies Lemma 6.6 for some ε. Then there exists at least $2^{\Omega(n^{\varepsilon/(1+\varepsilon)})}$ codewords in $RS[n = p, k = \Omega(n), d = n - k + 1]_{\mathbb{F}_p}$ with agreement $t = k + \Theta(n^{1/(1+\varepsilon)})$.*

Proof. Set $b = \lfloor (1-\delta)a \rfloor + 1$ for some $\delta > 0$. Thus, $k = (b-1)L \geqslant \lfloor (1-\delta)aL \rfloor = \Theta(aL) = \Theta(n)$. Further, $t = bL = k + L = k + \Theta(n^{1/(1+\varepsilon)})$. The last part follows from the fact that $n = \Theta(L^{1+\varepsilon})$. Finally, the number of codewords is at least $\left(\frac{a}{b-1}\right)^{b-1} = 2^{\Omega(a)} = 2^{\Omega(n^{\varepsilon/(1+\varepsilon)})}$. □

If one is satisfied with super polynomially many codewords, say $2^{w(n)}$ for some $w(n) = \omega(\log n)$, then choosing $\varepsilon = \frac{c \log w(n)}{\log n - c \log w(n)}$ (for some suitable constant c), gives an agreement $t = k + \Theta\left(\frac{n}{(w(n))^c}\right)$.

Proof of Theorem 6.10. The basic idea is to find a "lot" of t-tuples $(y_1, y_2, \ldots, y_t) \in \mathbb{F}_p^t$, (where for every $i \neq j$, $y_i \neq y_j$) such that the polynomial $P_{(y_1,\ldots,y_t)}(X) = \prod_{i=1}^t (X - y_i)$ is actually of the form

$$X^t + \sum_{j=1}^{t-L} c_j X^j$$

where c_{t-L} can be 0.[7] The above is equivalent to showing that $(y_1, \ldots, y_t)$ satisfy the following equations

$$y_1^s + y_2^s + \cdots y_t^s \;= 0 \quad s = 1, 2, \ldots L - 1 \tag{6.7}$$

We give an "explicit" description of at least $\binom{a}{b}$ distinct $(y_1, \ldots, y_t)$ such tuples.

[7] Then $R(X) - P_{(y_1,\ldots,y_t)}(X)$ is of degree $t - L = k - 1$ as needed.

Let $\mathbb{F}_p^*$ be generated by γ and set $\alpha = \gamma^a$. Note that the order of α is exactly L. Now consider the "orbits" in $\mathbb{F}_p^*$ under the action of α. It is not too hard to see that for $0 \leqslant i < a$, the i^{th} orbit is the set $\gamma^i\mathcal{A}$, where $\mathcal{A} = \{1, \alpha, \alpha^2, \ldots, \alpha^{L-1}\}$. We will call γ^i the "representative" of the i^{th} orbit. Consider all subsets $\{i_0, \ldots, i_{b-1}\} \subseteq \{0, 1, \ldots, a-1\}$ of size b. Each such subset corresponds to a tuple $(y_1, \ldots, y_t)$ in the following manner (recall that $t = bL$). For subset $\{i_0, \ldots, i_{b-1}\}$, define $y_{dL+r} = \gamma^{i_d}\alpha^r$, where $0 \leqslant d < b$ and $0 \leqslant r < L$. Note that each such subset $\{i_0, \ldots, i_{b-1}\}$ implies a distinct tuple $(y_1, \ldots, y_t)$. Thus, there are $\binom{a}{b}$ such distinct tuples.

To complete the proof, we will now verify that (6.7) holds for every such tuple $(y_1, \ldots, y_t)$. Indeed by construction, for $s = 1, \ldots, L-1$:

$$\sum_{j=1}^{t} y_j^s = \sum_{d=0}^{b-1} \gamma^{i_d s} \left(\sum_{r=0}^{L-1} \alpha^{sr} \right) = \sum_{d=0}^{b-1} \gamma^{i_d s} \left(\frac{\alpha^{Ls} - 1}{\alpha^s - 1} \right) = 0,$$

where the last inequality follows from the the fact that the order of α is L. □

We now turn to the proof of Lemma 6.6. First we need the following result, which is a special case of Linnik's theorem:

Theorem 6.12 ([78]). *There exists a constant c_L, $1 < c_L < 6$, such that for all sufficiently large d, there exists a prime p such that $p < d^{c_L}$ and $p \equiv 1 \mod d$.*

Proof of Lemma 6.6. Fix any $0 < \varepsilon \leqslant \frac{1}{c_L - 1}$. The basic idea of the proof is to "redistribute" the product bd as aL, where $a = \Theta(L^\varepsilon)$.

Let $d = 2^r$ be sufficiently large so that it satisfies the condition of Theorem 6.12. Thus, by Theorem 6.12, $p = bd + 1$ is prime for some $1 \leqslant b < 2^{r(c_L - 1)}$. Let $2^i \leqslant b < 2^{i+1}$ for some $i \in [0, r(c_L - 1) - 1]$. Now we consider two cases depending on whether $i \leqslant i_0 = \lfloor r\varepsilon \rfloor$ or not.

First consider the case when $i \leqslant i_0$. Here define $x_i = \lfloor \frac{r\varepsilon - i}{1+\varepsilon} \rfloor$. Finally, let $a = b2^{x_i}$ and $L = 2^{r - x_i}$. First note that $0 \leqslant x_i \leqslant r$ and thus, a and L are well defined. Also note that

$$\frac{a}{L^\varepsilon} = \frac{b2^{x_i}}{2^{\varepsilon(r - x_i)}} = b2^{(1+\varepsilon)x_i - r\varepsilon} \geqslant 2^i 2^{(1+\varepsilon)(\frac{r\varepsilon - i}{1+\varepsilon}) - r\varepsilon - 1} = \frac{1}{2},$$

where the inequality follows from the fact that for all positive reals $\lfloor y \rfloor \geqslant y - 1$ and $b \geqslant 2^i$. Similarly, one can show that $a/L^\varepsilon < 4$ and thus, $a = \Theta(L^\varepsilon)$ as required.

Now we consider the case when $i > i_0$. In this case define $x_i = \lfloor \frac{r - \varepsilon(i+1)}{1+\varepsilon} \rfloor$. Finally, let $a = 2^{r - x_i}$ and $L = b2^{x_i}$. Note that $x_i \leqslant r$. Also note that as $i + 1 < r(c_L - 1)$, $x_i \geqslant 0$ and thus, a and L are well defined. As before, we first lower bound

$$\frac{a}{L^\varepsilon} = \frac{2^{r - x_i}}{b^\varepsilon 2^{\varepsilon x_i}} > \frac{2^{r - x_i}}{2^{\varepsilon(i+1) + \varepsilon x_i}} = 2^{r - (1+\varepsilon)x_i - \varepsilon(i+1)} \geqslant 1,$$

where the first inequality follows from $b < 2^{i+1}$ and the second follows from the fact that for all positive y, $\lfloor y \rfloor \leqslant y$. Similarly one can show that $\frac{a}{L^\varepsilon} \leqslant 4$, which implies that $a = \Theta(L^\varepsilon)$ as required. □

Smooth Variation of the Agreement

In this section, we will see how to get rid of the "restriction" that t has to be a multiple of L in Theorem 6.10.

Theorem 6.13. *Let $L \geqslant 2$ and $0 \leqslant e < L$ be integers. Let $p = aL+1$ be a prime and define $t = bL+e$ for any $1 < b < a-1$. Let the received word $\mathbf{r}$ be the evaluation of $R(X) = X^t$ over $\mathbb{F}_p^*$. Then there are $\binom{a-1}{b}$ many codewords in $RS[n = p, k = (b-1)L+1+e]_{\mathbb{F}_p}$ that agree with $\mathbf{r}$ in at least t places.*

Since the proof is very similar to that of Theorem 6.10, we will just sketch the main ideas here. The basic argument used earlier was that every t-tuple $(y_1, y_2, \ldots, y_t)$ was chosen such that the polynomials $P_{(y_1,\ldots,y_t)}(X)$ and $R(X)$ agreed on the first $t-k$ co-efficients and the RS codewords were simply the polynomials $R(X) - P_{(y_1,\ldots,y_t)}(X)$. Now the simple observation is that for any fixed polynomial $D(X)$ of degree e we can get RS codewords of dimension $k' = k+e$ by considering the polynomials $D(X)\left(R(X) - P_{(y_1,\ldots,y_t)}(X)\right)$. The new agreement t' is with the new received word $R'(X) = R(X)D(X)$. Now $t'-t$ is the number of roots of $D(X)$ that are not in the set $\{y_1, \ldots, y_t\}$.

Thus, we can now vary the values of k by picking the polynomial $D(X)$ of different degrees. However, the difference $t'-k'$ might go down (as an arbitrary polynomial $D(X)$ of degree e might not have e roots and even then, some of them might be in the set $\{y_1, \ldots, y_t\}$). To get around this, while choosing the tuples $(y_1, \ldots, y_t)$, we will not pick any elements from one of the a cosets (recall that the tuples $(y_1, \ldots, y_t)$ are just a collection of b out of the a cosets formed by the orbits of $\alpha = \gamma^a$, where γ generates $\mathbb{F}_p^*$). This reduces the number of tuples from $\binom{a}{b}$ to $\binom{a-1}{b}$. Now we pick an arbitrary subset of that coset of size $0 \leqslant e < L$– say the subset is $\{z_1, \ldots, z_e\}$. Finally, pick $D(X) = \prod_{i=1}^{e}(X - z_i)$. Note that this implies that $t' = t+e$ as desired.

6.5 Bibliographic Notes and Open Questions

Results in Section 6.3 and Section 6.4.2 appeared in [59] while those in Section 6.4.3 are from [62].

Our work, specifically the part that deals with precisely describing the collection of polynomials that take values only in $\mathbb{F}_q$, bears some similarity to [51] which also exhibited limits to list recoverability of codes. One of the simple yet powerful ideas used in [51], and also in the work on extractor codes [101], is that polynomials which are r'th powers of a lower degree polynomial take only values in a multiplicative subgroup consisting of the r'th powers in the field. Specifically, the construction in [101, 51] yields roughly $n^{\frac{\ell k}{n}}$ codewords for list recovery where ℓ is the size of the S_i's in Definition 6.1. Note that this gives super-polynomially many codewords only when the input lists are asymptotically bigger than n/k.

In our work, we also use r'th powers, but the value of r is such that the r'th powers form a subfield of the field. Therefore, one can also freely add polynomials which are r'th powers and the sum still takes on values in the subfield. This lets us demonstrate a much larger collection of polynomials which take on only a small possible number of values at every point in the field. Proving bounds on the size of this collection of polynomials used techniques that were new to this line of study.

The technique behind our results in Section 6.4.2 is closely related to that of the result of Cheng and Wan [25] on connections between Reed-Solomon list decoding and the discrete logarithm problem over finite fields. However, our aim is slightly different compared to theirs in that we want to get a large collection of codewords close by to a received word. In particular in Theorem 6.6, we get an estimate on $N_t(\beta)$ while Cheng and Wan only require $N_t(\beta) > 0$. Also Cheng and Wan consider equation (6.6) only with the choice $L_B(x) = 1$.

Ben-Sasson, Kopparty and Radhakrishnan in [12], exploiting the sparsity of *linearized polynomials*, have shown the following. For every $\delta \in (0, 1)$ there exits Reed-Solomon code of block length n and dimension $n^\delta + 1$, which contains super-polynomial many codewords that agree with a received word in at least $n^{\sqrt{\delta}}$ positions. Also they show for constant rate Reed-Solomon codes (where the rate is $R > 0$), there exists a received word that has agreement $R'N$ (where $R' > R$) with roughly $N^{\Omega(\log(1/R)}$ codewords. The received word in the above constructions, however, is not explicit. Ben-Sasson et al. also construct an explicit received word that agrees with super-polynomially many Reed-Solomon codewords in $\omega(k)$ many places, where $k = n^\delta + 1$ is the dimension of the code. However, their results do not give an explicit bad list decoding configurations for constant rate Reed-Solomon codes. The results in [12] do not work for prime fields while the results on explicit received words in this chapter do work for prime fields.

We conclude with some open questions.

Open Question 6.1. *We have shown that RS codes of rate $1/\ell$ cannot be list recovered with input lists of size ℓ in polynomial time when ℓ is a prime power. Can one show a similar result for other values of ℓ?*

Using the density of primes and our work, we can bound the rate by $O(1/\ell)$, but if it is true it will be nice to show it is at most $1/\ell$ for every ℓ.

We have shown that the $\sqrt{kn'}$ bound for polynomial reconstruction is the best possible given n' general pairs $(\beta_i, \gamma_i) \in \mathbb{F}^2$ as input. It remains a big challenge to determine whether this is the case also when the β_i's are all distinct, or equivalently

Open Question 6.2. *Is the Johnson bound is the true list decoding radius of RS codes?*

We conjecture this to be the case in the following sense: there exists a field $\mathbb{F}$ and a subset of evaluations points S such that for the Reed-Solomon code defined over $\mathbb{F}$ and S, the answer to the question above is yes. One approach that might give at least partial results would be to use some of our ideas (in particular those using the norm function, possibly extended to other symmetric functions of the automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$) together with ideas in the work of Justesen and Hoholdt [70] who used the Trace function to demonstrate that a linear number of codewords could occur at the Johnson bound. Further, the work of

Ben-Sasson et al. [12] gives evidence for this for RS codes of rate $n^{-\varepsilon}$ for constant ε close to 0.

Open Question 6.3. *Can one show an analog of Theorem 6.6 on products of linear factors for the case when t is linear in the field size q (the currently known results work only for t up to $q^{1/2}$)?*

This is an interesting field theory question in itself, and furthermore might help towards showing the existence of super-polynomial number of Reed-Solomon codewords with agreement $t \geqslant (1+\varepsilon)k$ for some $\varepsilon > 0$ for constant rate (i.e. when k is linear in n)? It is important for the latter, however, that we show that $N_t(\beta)$ is very large for some *special* field element β in an extension field, since by a trivial counting argument it follows that there exist $\beta \in \mathbb{F}_{q^h}^*$ for which $N_t(\beta) \leqslant \binom{q}{t}/(q^h - 1)$.