Limits to List Decoding Reed-Solomon Codes

Venkatesan Guruswami*
Department of Computer Science & Engineering
University of Washington
Seattle, WA 98195.
venkat@cs.washington.edu

Atri Rudra
Department of Computer Science & Engineering
University of Washington
Seattle, WA 98195.
atri@cs.washington.edu

ABSTRACT

In this paper, we prove the following two results that expose some combinatorial limitations to list decoding Reed-Solomon codes.

1. Given n distinct elements $\alpha_1, \ldots, \alpha_n$ from a field $\mathbb{F}$, and n subsets $S_1, \ldots, S_n$ of $\mathbb{F}$ each of size at most ℓ, the list decoding algorithm of Guruswami and Sudan [7] can in polynomial time output *all* polynomials p of degree at most k which satisfy $p(\alpha_i) \in S_i$ for every i, as long as $\ell < \lceil \frac{n}{k} \rceil$. We show that the performance of this algorithm is the best possible in a strong sense; specifically, we show that when $\ell = \lceil \frac{n}{k} \rceil$, the list of output polynomials can be super-polynomially large in n.
   One way to interpret our result is the following. The algorithm in [7] can, when given as input n' distinct pairs $(\beta_i, \gamma_i) \in \mathbb{F}^2$ (the β_i's need not be distinct), find and output all degree k polynomials p such that $p(\beta_i) = \gamma_i$ for at least t values of i, provided $t > \sqrt{kn'}$. By our result, an improvement to the Reed-Solomon list decoder of [7] that works with slightly smaller agreement, say $t > \sqrt{kn'} - k/2$, can only be obtained by exploiting some property of the β_i's (for example, their (near) distinctness).
2. For Reed-Solomon codes of block length n and dimension k where $k = n^\delta$ for small enough δ, we exhibit an *explicit* received word $\mathbf{r}$ with a super-polynomial number of Reed-Solomon codewords that agree with it on $(2-\varepsilon)k$ locations, for any desired $\varepsilon > 0$ (we note agreement of k is trivial to achieve). Such a bound was known earlier only for a *non-explicit* center. We remark that finding *explicit* bad list decoding configurations is of significant interest — for example the *best* known rate vs. distance trade-off is based on a bad list decoding configuration for algebraic-geometric codes [14] which is unfortunately not explicitly known.

*Research supported in part by NSF Career Award CCF-0343672.

STOC'05, May 22-24, 2005, Baltimore, Maryland, USA.

Categories and Subject Descriptors

E.4 [**Data**]: Coding and Information Theory; F.2.1 [**Theory of Computation**]: Analysis of Algorithms and Problem Complexity; Numerical Algorithms and Problems

General Terms

Algorithms, Theory

Keywords

Reed-Solomon Codes, List Decoding, BCH Codes, List Recovering, Johnson bound

1. INTRODUCTION

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 $\mathbb{F}$. If the degree of the polynomials is at most k, and a polynomial p is encoded as $\langle p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_n)\rangle$, this gives an $[n, k+1, n-k]$ code, i.e., a code of block length n, dimension $k+1$ and distance $n-k$ (the distance property follows from the fact that two distinct degree k polynomials can agree on at most k points). This is optimal in terms of distance to dimension trade-off (meets the so-called "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. The best known polynomial time algorithm today (in terms of number of errors corrected) can, given a received word $\langle y_1, \ldots, y_n\rangle \in \mathbb{F}^n$, find and output a list of all degree k polynomials p which satisfy $p(\alpha_i) = y_i$ for at least t values of $i \in \{1, \ldots, n\}$, provided $t > \sqrt{kn}$ [11, 7]. Note that this is a *list decoding* algorithm that outputs a list of all codewords with the requisite agreement. The performance of the algorithm in [7] matches the so-called Johnson bound (cf. [8]) 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. Our work in this paper is motivated by the question of whether this 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 lower agreement parameter t might lead to super-polynomially large lists as output, which of course will preclude a polynomial time algorithm (at least in the standard model where the list has to be produced

explicitly). While we don't quite show this to be the case in this paper, we give evidence in this direction by demonstrating that in a somewhat more general setting to which also the algorithm of Guruswami and Sudan [7] applies, its performance is indeed the best possible. The details follow.

1.1 Limitations to "list recovering"

The algorithm in [7] in fact solves the following more general *polynomial reconstruction* problem in polynomial time: Given n' distinct pairs $(\beta_i, \gamma_i) \in \mathbb{F}^2$ (we stress that the β_i's need **not** be distinct), output a list of all polynomials p of degree k which satisfy $p(\beta_i) = \gamma_i$ for more than $\sqrt{kn'}$ values of $i \in \{1, 2, \ldots, n'\}$. In particular, the algorithm can solve the following "list recovering" problem[1] for an $[n, k+1, n-k]_q$ Reed-Solomon code as long as the parameter ℓ satisfies $\ell < \lceil \frac{n}{k} \rceil$:

DEFINITION 1 (LIST RECOVERING). *For a q-ary code C of block length n, the list recovering 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, $1 \leq i \leq n$, 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 list recovering with input lists of size ℓ.*

In other words, given n distinct elements $\alpha_1, \ldots, \alpha_n$ from a field $\mathbb{F}$, and n subsets $S_1, \ldots, S_n$ of $\mathbb{F}$ each of size at most ℓ, one can output all degree $\leq k$ polynomials p which satisfy $p(\alpha_i) \in S_i$ for every i in polynomial time. In Section 2, 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 3).

As a corollary, this rules out an efficient solution to the polynomial reconstruction algorithm that works even under the slightly weaker condition $t > \sqrt{kn'} - k/2$.[2] In this respect, the "square root" bound achieved by [7] is optimal, and any improvement to their list decoding algorithm which works with agreement fraction $t/n < \sqrt{r}$ where $r = k/n$ is the rate of the code, or in other words which works beyond the Johnson bound, must exploit the fact that the evaluation points β_i are distinct (or "almost distinct"). We are tempted to view this as evidence that the $\sqrt{r}$ bound is the minimum agreement under which list decoding is possible for the RS code, and hope that this work paves the way towards eventual resolution of this question.

While this part on tightness of Johnson bound remains speculatory at this stage, for the problem of list recovering itself, our work proves that RS codes are indeed sub-optimal, as we describe below. Guruswami and Indyk [6] prove that there exists a fixed $R > 0$ 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). On the other hand, by our work Reed-Solomon codes for list recovering with input lists of size ℓ must have rate at most $1/\ell$. Thus, despite the fact that most of the initial success in efficient list decoding has been for algebraic codes like Reed-Solomon codes, one needs to look for new codes in other domains in order to make progress towards the construction of and algorithms for near-optimal list-decodable codes.

[1]The terminology "list recovering" was coined in [6] though the problem was considered in many guises before, including for example in [12].

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

1.2 Explicit "bad" list decoding configurations

The result mentioned above presents an explicit bad list recovering configuration, i.e., an input instance to the list recovering 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 (or center) $\mathbf{r}$ with super-polynomially many codewords that agree with $\mathbf{r}$ at t or more places. A simple counting argument establishes the *existence* of such received words for certain settings of parameters n, k, t [10, 2]– in particular for $n = k^\delta$, one can get $t = \frac{k}{\delta}$ for any $\delta > 0$. In Section 3, 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 $\varepsilon > 0$. Note that such a construction is trivial for $t = k$ since we can interpolate degree k polynomials through any set of k points.

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 [3]. 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 $\rho < 1$. While we get the former, we only achieve $\rho = 1 - o(1)$.

As another motivation, we point out that the current *best* trade-off between rate and relative distance is achieved by a non-linear code comprising of precisely a bad list decoding configuration in certain algebraic-geometric codes [14]. Unfortunately the associated center is only shown to exist by a counting argument and its explicit specification will be required to get explicit codes with these parameters.

1.3 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 about q^{m-1} that take values in $\mathbb{F}_q$ at every point in $\mathbb{F}_{q^m}$, for any prime power q. Note that this implies that there can be a super-polynomial number of solutions to list recovering 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 center with several RS codewords with non-trivial agreement with it is obtained using ideas from [2] relating to representations of elements in an extension finite field by products of distinct linear factors.

1.4 Related Work

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 [5] which also exhibited limits to list recoverability of codes. One of the simple yet powerful ideas used in [5], and also in the work on extractor codes [12], 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 [12, 5] yields roughly $n^{\frac{\ell k}{n}}$ codewords for list recovering where ℓ is the size of the S_i's in Definition 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 uses techniques that are new to this line of study.

The technique behind our results in Section 3 is closely related to that of the recent result of Cheng and Wan [2] on connections between Reed-Solomon list decoding and the discrete logarithm problem over finite fields.

2. BCH CODES AND LIST RECOVERING REED-SOLOMON CODES

2.1 Main Result

We will work with polynomials over $\mathbb{F}_{q^m}$ of characteristic p where q is a power of p, and $m \geq 1$. We will denote by $\mathbb{F}_{q^m}^*$ the set of nonzero elements in the field $\mathbb{F}_{q^m}$. Our goal in this section is to prove the following result, and in Section 2.2 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 2.3 to give a precise characterization of the concerned polynomials.)

THEOREM 1. *Let q be a prime power, and $m \geq 1$ 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,*

$$\left|\{P(z) \in \mathbb{F}_{q^m}[z] \mid \ deg(P) \leq \frac{q^m-1}{q-1} \ \text{and} \ \forall \alpha \in \mathbb{F}_{q^m}, \right.$$

$$\left. P(\alpha) \in \mathbb{F}_q\}\right| = q^{2^m} \ .$$

In the rest of this section, we prove Theorem 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. We begin with the definition of BCH codes, (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 point the reader to [9], Ch. 7, Sec. 6, and Ch. 9, Secs. 1-3, for detailed background information on BCH codes.

DEFINITION 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:*

$$\mathrm{BCH}_{q,m,d,\alpha} = \{ \ \langle c_0, c_1, \ldots, c_{n-1}\rangle \in \mathbb{F}_q^n \mid$$

$$c(\alpha^i) = 0 \ \textit{for} \ i = 1, 2, \ldots, d-1,$$

$$\textit{where} \ c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x] \ \} \ .$$

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.*

Our interest in BCH codes is due to the following folklore result, which presents an alternate view of BCH codes as what are called subfield subcodes (cf. [9, Ch. 7, Sec. 7]) of Reed-Solomon codes. (It is our opinion that this alternate view, despite being much easier to state, does not get the mention it deserves in the standard coding textbooks. For sake of completeness, and since we view our work as a good opportunity to do so, we present a proof in Appendix A.)

LEMMA 1 (BCH CODES ARE SUBFIELD SUBCODES OF RS CODES). *Let q be a prime power and $m \geq 1$ 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 codewords of* $\mathrm{BCH}_{q,m,d,\alpha}$ *are in one-one correspondence with elements of the set*

$$\{\langle P(\alpha^0), P(\alpha^1), \ldots, P(\alpha^{n-1})\rangle \in \mathbb{F}_q^n \mid P \in \mathbb{F}_{q^m}[z],$$

$$\deg(P) \leq n - d, \ \textit{and} \ P(\gamma) \in \mathbb{F}_q \ \forall \gamma \in \mathbb{F}_{q^m}\} \ .$$

In light of the above lemma, in order to prove Theorem 1, we have to prove that $|\mathrm{BCH}_{q,m,d,\alpha}| = q^{2^m}$ 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 [1, Ch. 12], and give a sketch of its proof for the sake of completeness.

LEMMA 2 (DIMENSION OF BCH CODES). *For integer i, n, define $\lfloor i \rfloor_n$ by the conditions $i = \lfloor i \rfloor_n \mod n$ and $0 \leq \lfloor i \rfloor_n \leq n-1$. Then $|\mathrm{BCH}_{q,m,d,\alpha}| = q^{|I(q,m,d)|}$ where*

$$I(q,m,d) = \{i \mid 0 \leq i \leq n-1, \ \lfloor iq^j \rfloor_n \leq n - d$$

$$\textit{for all} \ j, \ 0 \leq j \leq m-1\} \qquad (1)$$

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 2 that the BCH codewords are simply polynomials $c(x)$ over $\mathbb{F}_q$ of degree at most $(n-1)$ which vanish at α^i for $1 \leq i < d$. 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. Therefore there is a unique monic polynomial $g(x) \in \mathbb{F}_q[x]$ such that

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

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 (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, $1 \leq i < d$, as roots. Now comes the simple but crucial property: since $g(x)$ has coefficients in $\mathbb{F}_q$, and q is a power of the characteristic of the field, $g(x^q) = g(x)^q$ identically as polynomials, and in particular for every $\gamma \in \mathbb{F}_{q^m}$

$$g(\gamma) = 0 \text{ if and only if } g(\gamma^q) = 0.$$

Recalling the way $\lfloor i \rfloor_n$ was defined and that $\gamma^n = 1$ for all $\gamma \in \mathbb{F}_{q^m}^*$, the above implies that for every i, $0 \leq i \leq n-1$, and every j, $0 \leq j \leq m-1$,

$$g(\alpha^{-i}) = 0 \text{ if and only if } g(\alpha^{-\lfloor iq^j \rfloor_n}) = 0. \tag{2}$$

Using the above we claim that for $0 \leq i \leq n-1$, if $i \notin I(q,m,d)$, then $g(\alpha^{-i}) = 0$. This immediately gives us the lower bound $\deg(g) \geq n - |I(q,m,d)|$, as g has at least $n - |I(q,m,d)|$ distinct roots. Indeed, suppose $i \notin I(q,m,d)$. Then there must exist some j, $0 \leq j \leq m-1$ such that $\lfloor iq^j \rfloor_n > n-d$, or equivalently $i' = n - \lfloor iq^j \rfloor_n \leq d-1$. Since $g(x)$ belongs to the BCH code, $g(\alpha^{i'}) = g(\alpha^{-\lfloor iq^j \rfloor_n}) = 0$, which by (2) implies $g(\alpha^{-i}) = 0$.

For the other direction, define the polynomial $h(x) \in \mathbb{F}_{q^m}[x]$ as

$$h(x) = \prod_{\substack{i \notin I(q,m,d) \\ 0 \leq i \leq n-1}} (x - \alpha^{-i})\ .$$

By definition of h and $I(q,m,d)$, it is easily seen that γ is a root of h if and only if γ^q is a root of h. By a well-known algebra fact (cf. [13, Thm. 1.1.22]), this implies that the coefficients of h lie in $\mathbb{F}_q$, i.e., $h(x) \in \mathbb{F}_q[x]$. Also note that if $n-d < i \leq n-1$, then clearly $i \notin I(q,m,d)$, and therefore $h(\alpha^{-i}) = 0$ for $n-d < i \leq n-1$, or equivalently $h(\alpha^i) = 0$ for $1 \leq i < d$. Thus $h(x)$ belongs to the BCH code and therefore must be divisible by $g(x)$. Hence $\deg(g) \leq \deg(h) = n - |I(q,m,d)|$, which combined with our earlier lower bound gives $\deg(g) = n - |I(q,m,d)|$. □

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, $0 \leq i < q^m - 1$ such that $\lfloor iq^j \rfloor_{q^m-1} \leq \frac{q^m-1}{q-1} = 1 + q + \cdots + q^{m-1}$ 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 at most $1+q+\cdots+q^{m-1}$. Clearly, this condition is satisfied if and only if that 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 $d = (q^m - 1) - \frac{q^m-1}{q-1}$.

Together with Lemma 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 1.

Before moving on to state implications of above result for Reed-Solomon list decoding, we state the following generalization of Theorem 1 which can proved in the same manner (the result of Theorem 1 is the case when parameter $k = m$):

THEOREM 2. *Let q be a prime power, and $m \geq 1$ be an integer. Then, for each k, $1 \leq k \leq m$, the number of univariate polynomials in $\mathbb{F}_{q^m}[z]$ of degree at most $\sum_{j=1}^{k} q^{m-j}$ which take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$ is exactly $q^{\sum_{j=0}^{k}\binom{m}{j}}$. 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 $q^{m-1}-1$).*

2.2 Implications for Reed-Solomon List Decoding

In the result of Theorem 1, if we imagine keeping $q \geq 3$ fixed and let 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 1 immediately gives us the following "negative" result on polynomial reconstruction algorithms and Reed-Solomon list decoding.[3]

THEOREM 3. *For every prime power $q \geq 3$, 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 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. [8]) that when $\ell < \lceil \frac{n}{k} \rceil$, the number of codewords is polynomially bounded. Moreover [7] presents a polynomial time algorithm to recover all the solution codewords in this case.

The algorithm in [7] 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 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 1. *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 recovering setting of Theorem 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

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

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

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

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

2.3 A precise description of polynomials with values in base field

We proved in Section 2.1, 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 3. *For all $x\in\mathbb{F}_{q^m}$, $x^{\frac{q^m-1}{q-1}}\in\mathbb{F}_q$.*

THEOREM 4. *Let q be a prime power, and let $m\geq 1$. 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 $Q=\frac{q^m-1}{q-1}$ which 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*

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

PROOF. By Lemma 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 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, $|N|\leq q^{2^m}$. To show that $|N|\geq q^{2^m}$, it clearly suffices to show (by linearity) that if

$$\sum_{i=0}^{2^m-1}\beta_i(z+\alpha^i)^Q=0 \qquad (3)$$

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 4 (LUCAS' THEOREM, CF. [4]). *Let p be a prime. Let a and b be positive integers with p-ary expansions $a_0+a_1p+\cdots+a_rp^r$ and $b_0+b_1p+\cdots+b_rp^r$ 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 $a_j\geq b_j$ for all $j\in\{0,1,\cdots,r\}$.*

Define the set

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

Applying Lemma 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 (3) 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

$$\sum_{i=0}^{2^m-1}(\alpha^j)^i\beta_i=0\ \ \text{for all } j\in T. \qquad (4)$$

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 (4) 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 (4) is $\beta_0=\beta_1=\cdots=\beta_{2^m-1}=0$, as desired. $\square$

2.4 Some further facts on the BCH code and list recovering associated RS code

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 1). 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 recovering from lists of size $q-1$. In particular, how many polynomials of degree $Q=(q^m-1)/(q-1)$ 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 which 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 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 5. *Let q be a prime power and let $m>1$. For any polynomial $P(z)$ over $\mathbb{F}_{q^m}[z]$, let it's 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 $Q=\frac{(q^m-1)}{q-1}$ which take values in $\mathbb{F}_q$ when evaluated at every point in $\mathbb{F}_{q^m}$ and which have Hamming weight (q^m-1). Furthermore, these are precisely the polynomials in the set $W=\{\lambda(z+\beta)^Q\ \ |\ \ \beta\in\mathbb{F}_{q^m},\lambda\in\mathbb{F}_q^*\}$.*

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 which satisfies the required properties belongs to W completing the proof.

Let $P(z)$ be a polynomial of degree at most Q which 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 $\beta \in (\mathbb{F}_{q^m} - \{\gamma\})$, $P(\beta)/(\beta-\gamma)^Q \in \mathbb{F}_q^*$. 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 $\mathbb{F}_{q^m} - \{\gamma\}$. 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. □

3. EXPLICIT HAMMING BALLS WITH SEVERAL REED-SOLOMON CODEWORDS

Throughout this section, we will be concerned with an $[q, k+1]$ Reed-Solomon code RS$[q,k]$ over $\mathbb{F}_q$. We will be interested in a center $\mathbf{r} \in \mathbb{F}_q^q$ such that a super-polynomial number of codewords of RS$[q,k]$ agree with $\mathbf{r}$ on t or more positions, and the aim would be to prove such a result for t non-trivially larger than k. It is easy to prove the *existence* of such an $\mathbf{r}$ with at least $\binom{q}{t}/q^{t-k}$ codewords with agreement at least t with $\mathbf{r}$. 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 [10].[4] A related way is suggested in [2] 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 fact 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 (see Theorem 5 below), and thereby get an *explicit center* $\mathbf{r}$ with several close-by codewords from RS$[q,k]$.

THEOREM 5. *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 $t \geq (\frac{4}{\epsilon}+2)(h+1)$ and[5] $q \geq \max(t^2, (h-1)^{\frac{(2+\epsilon)t}{t-(2+\epsilon)}})$, then for all $\beta \in \mathbb{F}_{q^h}^*$, $N_t(\beta) > (t-1)q^{t-h-1}$.*

PROOF. From the proof of Theorem 4 in [2], we obtain $N_t(\beta) \geq E_1 - E_2$, 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, $\binom{t}{2} = \frac{t^2}{2} - \frac{t}{2} \leq \frac{q-t}{2}$.

We first give a lower bound on E_1. Indeed, using $\binom{t}{2} \leq \frac{q-t}{2}$ 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 $t > (\frac{4}{\epsilon}+2)h$, that is, $t-h > (\frac{4+\epsilon}{4+2\epsilon})t$. Further, from our choice of q, $(h-1)^t \leq q^{\frac{t}{2+\epsilon}-1}$. We now bound E_2 from above. From our bounds on $\binom{t}{2}$ and $(h-1)^t$, we have $E_2 \leq (1+\frac{q-t}{2})q^{(\frac{4+\epsilon}{4+2\epsilon})t-1} < (1+\frac{q-t}{2})q^{t-h-1} = \frac{q^{t-h}}{2} - (\frac{t}{2}-1)q^{t-h-1}$, where the second inequality comes from our bound on $t-h$.

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

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

[5]We also need $\epsilon < t-2$, but this will be satisfied since we will think of ϵ as a fixed constant and let q, h and t grow.

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

THEOREM 6. *Let $\epsilon > 0$ be arbitrary, q a prime power, and h any positive integer. If $t \geq (\frac{4}{\epsilon}+2)(h+1)$ and $q \geq \max(t^2, (h-1)^{\frac{(2+\epsilon)t}{t-(2+\epsilon)}})$ then for every k in the range $t-h \leq k \leq t-1$, there exists an explicit received word $\mathbf{r} \in \mathbb{F}_q^q$ such that there are at least $\frac{q^k}{t!\binom{k+h}{t}}$ codewords of RS$[q,k]$ which agree with $\mathbf{r}$ in at least t positions.*

We will prove the above theorem at the end of this section. As $\epsilon \to 0$, and $q, g, h \to \infty$ 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 $\epsilon \to \infty$, 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. We note that the non-explicit bound $\binom{q}{t}/q^{t-k}$ gives a super-polynomial number of codewords for agreement $t \geq k/\delta$ 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 2. *For all $0 < \gamma < 1$, there exists $\delta > 0$ such that for all large enough prime powers q, there exists an explicit $\mathbf{r} \in \mathbb{F}_q^q$ such that the Reed-Solomon code RS$[q, k = q^\delta]$ contains a super-polynomial (in q) number of codewords with agreement at least $(2-\gamma)k$ with $\mathbf{r}$.*

COROLLARY 3. *For all $0 < \gamma < \frac{1}{2}$, there exists $\delta > 0$, such that for all large enough prime powers q, there is an explicit $\mathbf{r} \in \mathbb{F}_q^q$ such that the Reed-Solomon code RS$[q, k = q^{1/2-\gamma}]$ contains a super-polynomial (in q) number of codewords with agreement at least $(1+\delta)k$ with $\mathbf{r}$.*

Proof of Theorem 6. In what follows, we fix $H(x)$ to be a polynomial of degree h that is irreducible over $\mathbb{F}_q$. For the rest of this proof we will denote $\mathbb{F}_q[x]/(H(x))$ by $\mathbb{F}_{q^h}$. Also note that for any root α of H, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^h}$.

Pick any ℓ where $0 \leq \ell \leq h-1$ and note that q and t satisfy the conditions of Theorem 5. 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 $L_B(x) \stackrel{\text{def}}{=} \sum_{i=0}^{\ell} b_i x^i$. 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 center $\mathbf{r}$ to be $\langle \frac{r(a)}{H(a)}\rangle_{a\in\mathbb{F}_q}$. Note that since $H(x)$ is an irreducible polynomial, $H(a) \neq 0$ for all $a \in \mathbb{F}_q$, and $\mathbf{r}$ is a well-defined element of $\mathbb{F}_q^q$.

We now proceed to bound from below the number of polynomials of degree $k \stackrel{\text{def}}{=} t + \ell - h$ which agree with $\mathbf{r}$ 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 $P_B^{(j)}(\alpha) \stackrel{\text{def}}{=} \prod_{a\in\mathcal{A}_{(B,j)}}(\alpha+a) = Q_B(\alpha)$. By Theorem 5, we have $N_B \geq (t-1)q^{t-h-1}$ 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 H is the irreducible polynomial of α over $\mathbb{F}_q$, this implies that $H(x)$ 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 $k = t + l - h$ such that

$$T_B^{(j)}(x)H(x) = P_B^{(j)}(x)L_B(x) + r(x). \quad (5)$$

Clearly $T_B^{(j)}(-a)$ equals $r(-a)/H(-a)$ for each $a \in \mathcal{A}_{(B,j)}$ and thus the polynomial $T_B^{(j)}$ agrees with $\mathbf{r}$ 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 $N_B \geq N$, 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

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

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

Comparison with the Cheng-Wan paper [2]

Our results in this subsection build upon the results in [2]– 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 5, we get an estimate on $N_t(\beta)$ while Cheng and Wan only require $N_t(\beta) > 0$. Also Cheng and Wan consider equation (5) only with the choice $L_B(x) = 1$.

4. CONCLUSIONS AND OPEN QUESTIONS

Our work exposes limitations to the kind of trade-offs for list recovering achievable using Reed-Solomon codes, and in particular demonstrates that RS codes are quite far from the best possible in this regard. Specifically, they can have rate at most $1/\ell$ for list recovering with input lists of size ℓ when the best, albeit non-explicit, codes can achieve constant rate. It is interesting that the result is exactly tight: list recovering for input lists of size ℓ when $\ell < \lceil \frac{n}{k} \rceil$ is possible in polynomial time, while at $\ell = \lceil \frac{n}{k} \rceil$ we might have to confront super-polynomial number of solution codewords. Our work raises several interesting questions for future work; we list some of them below:

- 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 whether the Johnson bound is the true list decoding radius of RS codes. We conjecture this to be the case. 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 Høholdt [10] who used the Trace function to demonstrate that a linear number of codewords could occur at the Johnson bound.

- Can one show an analog of Theorem 5 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 $t \geq (1 + \varepsilon)k$ 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 $N_t(\beta) \leq \binom{q}{t}/(q^h - 1)$.

[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 $\{1, \cdots, t\}$.

5. REFERENCES

[1] Elwyn Berlekamp. *Algebraic Coding Theory.* McGraw-Hill Series in Systems Science, 1968.

[2] Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. In *Proceedings of the 45th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 335–341, October 2004.

[3] Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a code. *IEEE Transactions on Information Theory*, 49(1):22–37, January 2003.

[4] Andrew Granville. The arithmetic properties of binomial coefficients. In `http://www.cecm.sfu.ca/organics/papers/granville/`, 1996.

[5] Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48:1021–1035, May 2002.

[6] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 658–667, 2001.

[7] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, 1999.

[8] Venkatesan Guruswami and Madhu Sudan. Extensions to the Johnson Bound. *Manuscript; available from http://theory.lcs.mit.edu/ madhu/papers.html*, 2000.

[9] F. J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier/North-Holland, Amsterdam, 1981.

[10] Jørn Justesen and Tom Høholdt. Bounds on list decoding of MDS codes. *IEEE Transactions on Information Theory*, 47(4):1604–1609, May 2001.

[11] Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.

[12] Amnon Ta-Shma and David Zuckerman. Extractor Codes. *IEEE Transactions on Information Theory*, 50(12):3015–3025, 2004.

[13] J. H. van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics **86**, (Third Edition) Springer-Verlag, Berlin, 1999.

[14] Chaoping Xing. Nonlinear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound. *IEEE Transactions on Information Theory*, 49(7):1653–1657, 2003.

APPENDIX

A. BCH CODES ARE SUBFIELD SUBCODES

Lemma 2 *Let q be a prime power and $m \geq 1$ 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 codewords of $\mathrm{BCH}_{q,m,d,\alpha}$ are in one-one correspondence with elements of the set*

$$\{\langle P(\alpha^0), P(\alpha^1), \ldots, P(\alpha^{n-1})\rangle \mid P \in \mathbb{F}_{q^m}[z],\ \deg(P) \leq n-d,$$

$$\text{and } P(\gamma) \in \mathbb{F}_q\ \forall \gamma \in \mathbb{F}_{q^m}\}\ .$$

PROOF. Our goal is to prove that the two sets

$$S_1 = \{\ \langle c_0, c_1, \ldots, c_{n-1}\rangle \mid$$

$$c(\alpha^i) = 0 \text{ for } i = 1, 2, \ldots, d-1,$$

$$\text{where } c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]\ \}\ ,$$

$$S_2 = \{\langle P(\alpha^0), P(\alpha^1), \ldots, P(\alpha^{n-1})\rangle \mid P \in \mathbb{F}_{q^m}[z],$$

$$\deg(P) \leq n-d,\ \text{and } P(\gamma) \in \mathbb{F}_q\ \forall \gamma \in \mathbb{F}_{q^m}\}\ ,$$

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 $r = 1, 2, \ldots, d-1$, 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 $1 \leq r+j \leq n-1$ and α is primitive. Therefore, $\langle P(\alpha^0), P(\alpha^1), \ldots, P(\alpha^{n-1})\rangle \in S_1$.

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 $0 \leq j \leq n-1$, 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 $0 \leq s \leq n-1$. Indeed,

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

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. □