Folded Algebraic-geometric Codes from Galois Extensions

Ming-Deh Huang and Anand Kumar Narayanan

Abstract. We describe a new class of list decodable codes based on Galois extensions of function fields and present a list decoding algorithm. This work is an extension of Folded Reed Solomon codes to the setting of Algebraic Geometric codes. These codes are obtained as a result of folding the set of rational places of a function field using certain automorphisms from the Galois group of the extension. We discuss two cases based on this framework depending on if the order of the automorphism used to fold the code is large or small compared to the block length. When the automorphism is of large order, the codes have polynomially bounded list size in the worst case. This construction gives codes of rate $R$ that can correct a fraction of $1 - R - \epsilon$ errors. Subject to the existence of asymptotically good towers of function fields with large automorphisms, this error correction performance can be achieved over an alphabet of size independent of block length. The second construction addresses the case when the order of the element used to fold is small compared to the block length. In this case, a heuristic analysis shows that for random errors, the expected list size and the running time of the decoding algorithm are bounded by a polynomial in the block length. When applied to the Garcia-Stichtenoth tower, this yields codes of rate $R$ over an alphabet of size $\left(\frac{1}{\epsilon^6}\right)^{O\left(\frac{1}{\epsilon^2}\right)}$, that can correct a fraction of $1 - R - \epsilon$ errors.

Introduction

Error correction codes are combinatorial objects used in reliable transmission of information. In block error correction, a message which consists of $k$ symbols over an alphabet $S$ is mapped into $N$ symbols over the alphabet. The image of this mapping that is contained in $S^N$ defines a code and an element in the code is called as a codeword. The Hamming distance between two codewords is defined as the number of coordinates where they differ. The codeword is transmitted over a channel that might induce errors. The received word is an arbitrary element in $S^N$ that arises as a corrupted version of the image of a message. A decoder for the code tries to find the message transmitted from the corrupted received word. The integer $N$ is called as the block length of the code and $R = \frac{k}{N}$ the rate of the code.
A list decoder outputs the list of all codewords which have sufficient agreement with the received word. A list decodable code is said to correct \( e \) errors if the number of codewords which are at a Hamming distance of at most \( e \) from any received word is bounded by a polynomial in the block length of the code. There is a tradeoff between the rate and the fraction of errors \( (\delta = \frac{e}{N}) \) corrected. There is first of all the fundamental bound \( R + \delta \leq 1 \). Let \( H_q(x) = x \log_q(\frac{q-1}{x}) + (1-x) \log_q(\frac{1}{1-x}) \), the \( q \)-ary entropy function. Then for codes over an alphabet of size \( q \), we have \( R \leq 1 - H_q(\delta) \). Zyablov and Pinsker \([18]\), showed the existence of list decodable codes whose parameters satisfy the above tradeoff with equality. In particular, \( \forall R, 0 < R < 1 \) and \( \forall q \geq 2 \), there exists list decodable codes of rate \( R \) over an alphabet of size \( q \) that can correct a fraction of \( \delta = H_q^{-1}(1-R) \) errors. When the alphabet size \( q \) is at least \( 2^\frac{1}{\epsilon} \), the fraction of errors corrected turns out to be at least \( 1 - R - \epsilon \). The list decodable codes of Zyablov and Pinsker approach the fundamental bound of \( R + \delta \leq 1 \) as the alphabet size gets large. However the construction uses random coding arguments and the codes are not explicit.

Much progress has been made toward explicit constructions of list decodable codes with bounded worst case list size that approach the fundamental bound of \( R + \delta \leq 1 \) as the alphabet size gets large. Reed Solomon codes with unique decoding (list size bounded by 1) can correct a fraction of \( 1 - R^2 \) errors. The Guruswami-Sudan List Decoding algorithm for Reed Solomon codes improved the bound to \( \delta = 1 - \sqrt{R} \) \([10]\) with polynomially bounded lists. In \([14]\), Parvaresh and Vardy introduced a new class of codes (Parvaresh-Vardy Codes) that could correct a fraction of \( 1 - mR^{\frac{1}{m+1}} \) errors, for an integer \( m \geq 2 \). For certain rates, these can correct more errors than Reed Solomon codes running the Guruswami-Sudan list decoding algorithm. Guruswami and Pathak \([8]\) provide a generalization of the Parvaresh-Vardy code to the Algebraic-Geometric setting thereby reducing the alphabet size. Building on \([14]\), Guruswami and Rudra \([9]\) constructed the first explicit family of codes called Folded Reed Solomon codes that achieve the \( R + \delta \leq 1 - \epsilon \) tradeoff. However, the Folded Reed Solomon codes have an alphabet size requirement of \( (\frac{N}{\epsilon^2})^{O(\frac{1}{\epsilon})} \), which is a large polynomial in the block length. We describe a new class of list decodable codes based on Galois extensions of function fields and present a list decoding algorithm. This work is an extension of Folded Reed Solomon codes to the setting of Algebraic Geometric codes. Independent of this work, Guruswami \([7]\) generalized Folded Reed-Solomon codes to codes from cyclotomic function fields that have an alphabet size that grows logarithmically in the block length. The construction exploits the special structure of cyclotomic function fields and their Artin automorphisms.

By generalizing Folded Reed Solomon codes to Folded Algebraic Geometric codes we present a purely algebraic means towards achieving the rate error correction tradeoff with alphabet size independent of the block length. These codes are obtained as a result of folding the set of rational places of a function field using certain automorphisms from the Galois group of the extension. More precisely, these automorphisms are used to induce an ordering on the places of the function field used in defining the code, and the ordering is used to fold the code and is exploited at the receiver to perform better error correction. Based on this general framework, we present two different constructions depending on if the order of the automorphism
used has order large or small compared to the block length. We present a list decoding algorithm for each case. The decoding algorithms are based on the interpolate and root find strategy common to \[10\][14][9][8]. However, the root finding step turns out to be much more complicated.

When the automorphism has an order comparable to the block length of the code, the list size is bounded by a polynomial in the block length. We present a characterization of the error correction, list and alphabet sizes in terms of function field parameters, namely the number of small degree places and the order of the automorphism used to fold. When applied to Kummer extensions, this gives codes of rate $R$ that can correct a fraction of $1 - R - \epsilon$ errors. The alphabet size required by these codes is lesser than the block length, thus improving on the Folded Reed Solomon codes. When applied to a sequence of asymptotically good function fields that contain a large automorphism, the resulting codes of rate $R$ over an alphabet independent of the block length can correct a fraction of $1 - R - \epsilon$ errors. However it is not known if such a sequence of field extensions exists and we pose an open problem (See § 5).

When the order of the automorphism used is small compared to the block length, the list decoding is much more complicated. We translate the root finding problem over the function field into a root finding problem over the local completion at a place where the automorphism acts as the Frobenius. The interpolated multivariate polynomial is mapped to one of a finite collection of polynomials in the local completion. We present an algorithm to solve the root finding problem over the local completion and a lifting of the solutions to the function field. The root finding algorithm in the local completion only depends on this finite collection of polynomials. If we pick a polynomial from this collection at random, the expected number of roots turns out to be polynomial in the degree of the interpolated polynomial and the size of the residue class field at that place. Under the heuristic that random errors map the received word to a random polynomial in this collection, the expected list size turns out to be bounded by a polynomial in the block length. (See § 3.2 for a discussion on why this heuristic assumption is reasonable.) When applied to the Garcia-Stichtenoth towers, we get codes over an alphabet of size $(\frac{1}{\epsilon})^{O(\frac{1}{\epsilon})}$ that can correct a fraction of $1 - R - \epsilon$ errors. With our heuristic assumptions, the expected list size is bounded by $N^{O(\frac{1}{\epsilon})}$.

1. Folded Algebraic Geometric codes

In this section, we develop the ideas behind the code constructions and present a formal description of Folded Algebraic Geometric codes.

We begin by defining Reed-Solomon codes and then introduce Algebraic Geometric codes as generalizations of Reed-Solomon codes. Let $\mathbb{F}_q$ be the finite field with $q$ elements. Fix a size $N$ subset of the elements of the finite field $\mathbb{F}_q$. Messages are associated with polynomials $\{f \in \mathbb{F}_q[x], \deg(f) < k\}$ with $k \leq N$. Here $\deg(f)$ is the degree of the polynomial $f$. The image of $\{f \in \mathbb{F}_q[x], \deg(f) < k\}$ under evaluation at this subset is the Reed-Solomon code. Observe that the alphabet size $q$ is at least as big as the block length for Reed-Solomon codes. Generalization to Algebraic Geometric codes yields codes of arbitrarily large block length over a
Let $L$ denote a function field that is a finite separable extension of the rational function field $\mathbb{F}_q(x)$, where $x$ is an indeterminate. It is assumed that $L$ has $\mathbb{F}_q$ as the field of constants. A ring $\mathcal{O} \subset L$ is called a valuation ring of the function field $L$ if $\mathbb{F}_q \subset \mathcal{O} \subset L$ and for all $f \in L$, either $f \in \mathcal{O}$ or $f^{-1} \in \mathcal{O}$. A valuation ring is a local ring and hence contains a unique maximal ideal. A place $v$ of the function field $L$ is defined as the maximal ideal of a valuation ring of $L$. If $v$ is a place, then the corresponding valuation ring is determined as $\mathcal{O}_v := \{f \in L : f^{-1} \notin v\}$. The quotient field $\mathbb{F}_v := \mathcal{O}_v/v$ is called the residue class field at $v$. The degree of the place $v$, denoted by $\deg(v)$ is defined as the degree of the extension $\mathbb{F}_v$ over $\mathbb{F}_q$, and $v$ is called a rational place if the degree of $v$ is one. The natural reduction map $\mathcal{O}_v \rightarrow \mathcal{O}_v/v$ is called as evaluation at $v$. Throughout, $f(v)$ denotes the evaluation of $f \in \mathcal{O}_v$ at $v$.

Let $V_v(f)$ denote the valuation of $f$ at $v$ defined as follows. Let $t \in \mathcal{O}_v$ generate the ideal $v \langle t \rangle$. Any $f \in L$ can be written as $f = t^b f', b \in \mathbb{Z}$, where $f'$ is a unit in $\mathcal{O}_v$. The integer $b$ is independent of the choice of $t$ and is defined as $V_v(f)$ [16][I.1.11]. Let $S$ denote the set of places in $L$. The group of divisors is the additive free abelian group $\mathcal{D}$ generated by the places of $L$. The elements of $\mathcal{D}$ are called as divisors. In particular, a divisor $D$ is of the form $D = \sum_{v \in S} n_v v$, where $n_v \in \mathbb{Z}$ and $n_v = 0$ for all but a finite set. The degree of the divisor is $\deg(D) = \sum_{v \in S} n_v \deg(v)$. A divisor of a function $f \in L$ is defined as $\text{div}(f) := \sum_{v \in S} V_v(f) v$. Let 

$$\mathcal{L}(D) = \{f \in L : \text{div}(f) + D \geq 0\} \cup \{0\}$$

 denote the Riemann-Roch space associated with the divisor $D$. The dimension of the Riemann-Roch space is lower bounded as $\dim(\mathcal{L}(D)) \geq \deg(D) - g + 1$. Here $g$ is the genus of the function field. Further, if $\deg(D) \geq 2g - 1$, then $\dim(\mathcal{L}(D)) = \deg(D) - g + 1$.

Let $S_r$ denote the set of rational places of $L$. Let $S_D \subseteq S_r$ be a subset of the rational places not including $P_\infty$, where $P_\infty \in S$ is a point at infinity. Without loss of generality, assume that the degree of $P_\infty$ is 1. Algebraic Geometric codes were introduced by Goppa [5] and are defined as follows. Let $\alpha \leq |S_D|$ be a positive integer parameter. Messages are associated with functions in $\mathcal{L}((\alpha - 1) P_\infty)$ and the code is the image of the evaluation of $\mathcal{L}((\alpha - 1) P_\infty)$ at the places of $S_D$ (Refer to [5] and [16] for a detailed description).

The block length $|S_D|$ is upper bounded by the number of rational points in $L$. The number of rational points $N_L$ of a function field $L$ satisfies $\frac{N_L}{q} \leq \sqrt{q} - 1$ (Drinfeld-Vladut Bound). If $q$ is a perfect square, then there exists an explicit family of function fields for which the number of rational points attains the upper bound [4]. By taking all rational places as places of evaluation, one can construct Algebraic Geometric codes on these function fields of arbitrarily large block length $N_L$ over a constant alphabet $q$. A fraction of $1 - \sqrt{R + \frac{q}{N_L}} = 1 - \sqrt{R + \frac{1}{\sqrt{q-1}}}$ errors can
be corrected with polynomial lists [10]. We thus obtain codes of arbitrary large block length over a constant alphabet with similar error correction performance compared to Reed-Solomon codes.

1.1. Folded Algebraic Geometric Codes. In Folded Reed-Solomon codes [9], the ordering of places was exploited by the decoder to perform error correction up to the list decoding capacity. However, it was not apparent as to whether these techniques generalized to the case of Algebraic Geometric codes. We present such a folding scheme for Algebraic Geometric codes defined over certain Galois extensions. Consider Reed-Solomon codes where all the elements of the multiplicative group of \( F_q \) are used for evaluation. The multiplicative group of a finite field is cyclic. Let \( \gamma \in F_q^* \) be a generator. In Folded Reed-Solomon codes the places of evaluation are enumerated as \( 1, \gamma, \gamma^2, \ldots, \gamma^{q−1} \). The evaluation of a polynomial \( f \) at \( \gamma^i \), gives us some information about the evaluation of \( f \) at \( \gamma^{i+1} \). This is exploited at the decoder [9]. We use the action of an element of the Galois group to induce an ordering of the places. First, we build some notation regarding Galois groups.

From now on, we assume that \( L/K \) is a finite Galois extension, where \( K \) is a finite separable extension of \( F_q(x) \). Further assume that \( L \) and \( K \) both have \( F_q \) as the field of contents. Let \( \text{Gal}(L/K) \) denote the Galois group of the extension. For a place \( v \in S \) and \( \sigma \in \text{Gal}(L/K) \), let \( \sigma(v) = \{ \sigma(f) : f \in \mathcal{O}_v \} \). Then \( \sigma(v) \) is also a place in \( L \) [16][Lem III 5.2]. Thus \( \text{Gal}(L/K) \) acts on the places of \( L \). This action can be naturally extended to divisors, so that the action of \( \sigma \in \text{Gal}(L/K) \) on a divisor \( D = \sum_{v \in S} a_v v \) is defined by \( \sigma(D) = \sum_{v \in S} a_v \sigma(v) \). An element \( \sigma \in \text{Gal}(L/K) \) induces an isomorphism on the residue fields of \( v \) and \( \sigma(v) \), given by \( \sigma(f(v)) := \sigma(f)(\sigma(v)) \). Thus \( \deg(v) = \deg(\sigma(v)) \). If \( \sigma \) fixes the divisors \( \sum_{v \in S \setminus P} v \) and \( P_{\infty} \), then \( \sigma \) defines an automorphism on the Algebraic Geometric code [16][VIII.3].

Let \( v \) and \( v' \) denote two places in \( L \) such that \( \sigma^{-1}(v) = v' \). Let \( f \in \mathcal{O}_v \).

\[
\sigma(f(v')) = \sigma(f)\sigma(v') = \sigma(f)\sigma(\sigma^{-1}(v)) = \sigma(f)(v)
\]

Thus from the evaluation of \( f \) at \( v' \) we can infer the evaluation of \( \sigma(f) \) at \( v \). We now order the places of evaluation of the code so that this can be exploited at the decoder.

For a place \( v \in L \), an automorphism \( \sigma \in \text{Gal}(L/K) \) and a positive integer \( c \), define \( \Gamma_v^c(\sigma) \) to be the ordered set \( \langle v, \sigma^{-1}(v), \ldots, \sigma^{-c+1}(v) \rangle \). The evaluation of a function \( f \in L \) at \( \Gamma_v^c(\sigma) \) is defined as \( f(\Gamma_v^c(\sigma)) := \langle f(v), f(\sigma^{-1}(v)), \ldots, f(\sigma^{-c+1}(v)) \rangle \). Thus \( f(\Gamma_v^c(\sigma)) \in \bigoplus_{i=0}^{c-1} F_{\sigma^{-i}(v)} \).

1.2. Code Definition, Encoding and Parameters. The set of places used to define the code is restricted to the set of rational places that resulted out of complete splitting in the extension. These are ordered using an automorphism \( \sigma \in \text{Gal}(L/K) \) of order \( b \). Let \( u \) be a place in \( K \) that splits completely in the extension \( L/K \). Then for every place \( v \) above \( u \), \( \sigma^{-i}(v) \) are all distinct for \( i = 0, \ldots, b−1 \). Thus \( \Gamma_v^b(\sigma) \) consists of distinct places. Hence the set of places lying above
u in L can be partitioned into \( \frac{[L-K]}{b} \) cycles under the action of \( \sigma^{-1} \) with each cycle of length \( b \).

We now formally describe the encoding process with folding parameter \( m \). We assume without loss of generality that \( m \) divides \( b \). Let \( S_{sp} \) denote the set of rational places in \( L \) that resulted out of complete splitting and with support disjoint from points at infinity. Denote the cardinality of \( S_{sp} \) by \( n \). Observe that as \( v \) resulted out of splitting, \( \Gamma^m_\sigma(v) \) represents a cycle of distinct places under the action of \( \sigma^{-1} \). The set \( \Gamma^m_\sigma(v) \) can be further partitioned into sub blocks of size \( m \) as \( \Gamma^m_\sigma(v) = \{ \Gamma^m_\sigma(v), \Gamma^m_\sigma(\sigma^{-m}(v)), \ldots, \Gamma^m_\sigma(\sigma^{-b+m}(v)) \} \). Thus \( S_{sp} \) can be partitioned into \( N := \frac{n}{m} \) sub blocks of size \( m \) under the action of \( \sigma^{-1} \). In particular, there exists a set \( S_{rep} := \{ v_1, v_2, \ldots, v_N \} \subseteq S_{sp} \) such that \( \{ \Gamma^m_\sigma(v_1), \Gamma^m_\sigma(v_2), \ldots, \Gamma^m_\sigma(v_N) \} \) is an ordered set with \( S_{sp} \) being the disjoint union of \( \Gamma^m_\sigma(v), v \in S_{rep} \).

Recall that \( P_\infty \) is a rational point at infinity in \( L \). We assume that \( P_\infty \) is fixed by \( \sigma \). Again, the Riemann-Roch space \( \mathcal{L}(\alpha - 1)P_\infty \) constitutes the message space. The codeword corresponding to message \( f \in \mathcal{L}(\alpha - 1)P_\infty \) is the evaluation of \( f \) at \( S_{sp} \). The folded code is viewed as a code over an alphabet of size \( q^m \).

In particular, the codeword is \( \{ f(\Gamma^m_\sigma(v_1)), f(\Gamma^m_\sigma(v_2)), \ldots, f(\Gamma^m_\sigma(v_N)) \} \). The block length of the code is \( N = \frac{n}{m} \). The rate depends on the dimension \( k := \dim(\mathcal{L}(\alpha - 1)P_\infty) \). The rate of the code \( R = \frac{k}{mN} = \frac{k}{n} \). This process of breaking an ordered set of places into blocks and looking at evaluations at these blocks as a code over a larger alphabet is called as folding.

2. List Decoding Folded Algebraic Geometric Codes

We describe a list decoding algorithm for the Folded Algebraic Geometric codes in this section.

Let \( \{ Y_j, v_j \in S_{rep} \} \) denote the received word. Here \( Y_j \in \bigoplus_{i=0}^{m} \mathbb{F}_{\sigma^{-i}(v_j)} \). Let \( \{ y_v, v \in S_{sp} \} \) where \( y_v \in \mathbb{F}_q \) denote the corresponding unfolded received word. The decoding algorithm proceeds by first interpolating a polynomial in \( s \) variables based on the received word. Here \( s \leq m \) is a positive integer parameter determined later. The interpolation step involves finding a non zero multivariate polynomial \( Q \in L[z_1, z_2, \ldots, z_s] \), such that

- \( \forall f_1, f_2, \ldots, f_s \in \mathcal{L}(\alpha - 1)P_\infty \), we require \( Q(f_1, f_2, \ldots, f_s) \in \mathcal{L}(lP_\infty) \)
- \( \forall v \in S_{sp}, \forall f_1, f_2, \ldots, f_s \in \mathcal{L}(\alpha - 1)P_\infty \) such that \( f_1(v) = y_v, f_2(v) = y_{s-1}(v), \ldots, f_s(v) = y_{s-r+1}(v) \), we require \( \nu_v(Q(f_1, f_2, \ldots, f_s)) \geq r \)

where \( l \) and \( r \) are integer parameters determined later. Here, \( r \) is the multiplicity parameter and \( \nu_v \) denotes the valuation at \( v \).

The received symbol corresponding to a place \( v \in S_{rep} \) is said to be in agreement if the received symbol at \( v \), \( \langle y_v, y_{\sigma^{-1}(v)}, \ldots, y_{\sigma^{-m}(v)} \rangle \), is the actual transmitted symbol. The agreement parameter \( T \) is defined as the number of locations (places in \( S_{rep} \)) at which there is an agreement. The interpolation algorithm is easily adapted from and similar to the second decoding algorithm presented in [8]. The reader is referred to the original paper [8] for details regarding the construction of \( Q \) and a discussion relating to representation needed to efficiently compute \( Q \). The
interpolation problem can be reduced to solving a linear system over $\mathbb{F}_q$ that can be solved in time polynomial in the block length. In particular, for an agreement parameter $T \geq \left\lfloor \frac{m}{m-s+1} \cdot \frac{q}{N} \right\rfloor$, there exists $r, l$ with $l := rT(m-s+1) - 1$ such that $Q$ satisfying the conditions exists and can be constructed in polynomial time [8]. Moreover the degree $d$ of the multivariate polynomial $Q$ is upper bounded by $d \leq \frac{l-q}{\alpha}$ which at worst grows linearly in the block length. [8]

The connection of the interpolation problem to list decoding is seen in the following lemma.

**Lemma 2.1.** Let $rT(m-s+1) > l$. If $f \in \mathcal{L}((\alpha-1)P_\infty)$ satisfies $f(v) = y_{v}, f(\sigma^{-1}(v)) = y_{\sigma^{-1}(v)}, \ldots, f(\sigma^{-m+1}(v)) = y_{\sigma^{-m+1}(v)}$ for at least $T$ of the places $v \in S_{rep}$, then $Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0.$

**Proof:** Let $S_T \subseteq S_{rep}$ denote the set of places in $S_{rep}$ such that $f(v) = y_v, f(\sigma^{-1}(v)) = y_{\sigma^{-1}(v)}, \ldots, f(\sigma^{-m+1}(v)) = y_{\sigma^{-m+1}(v)}$. By construction, if $v \in S_T$, then $f(v') = y_{v'}, f(\sigma^{-1}(v')) = y_{\sigma^{-1}(v')}, \ldots, f(\sigma^{-s+1}(v')) = y_{\sigma^{-s+1}(v')}$ for $v' \in \{v, \sigma^{-1}, \ldots, \sigma^{-m+1}\}$. Observe that for $v' \in S_{sp}$,

$$f(v') = y_{v'}, f(\sigma^{-1}(v')) = y_{\sigma^{-1}(v')}, \ldots, f(\sigma^{-s+1}(v')) = y_{\sigma^{-s+1}(v')}$$

$$\Rightarrow f(v') = y_{v'}, (\sigma(f)(v')) = y_{\sigma^{-1}(v')}, \ldots, (\sigma^{-s+1}(f)(v')) = y_{\sigma^{-s+1}(v')}$$

$$\Rightarrow \mathcal{V}_v(Q(f, \sigma(f), \ldots, \sigma^{s-1}(f))) \geq r$$

$$|S_T| \geq T \Rightarrow \sum_{v' \in S_{sp}} \mathcal{V}_v(Q(f, \sigma(f), \ldots, \sigma^{s-1}(f))) \geq r T (m-s+1) > l$$

But $Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) \in \mathcal{L}(P_\infty)$. This is because $\sigma$ fixes $P_\infty$ and thus $\sigma^{-1}(f) \in \mathcal{L}((\alpha-1)P_\infty) \forall f \in \mathcal{L}((\alpha-1)P_\infty)$ and $j \in \mathbb{Z}$. Thus $Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0$. □

For the special case of $m = b$, more is true. If $v \in S_T$, then $f(v') = y_{v'}, f(\sigma^{-1}(v')) = y_{\sigma^{-1}(v')}, \ldots, f(\sigma^{-s+1}(v')) = y_{\sigma^{-s+1}(v')}$ for $v' \in \{v, \sigma^{-1}, \ldots, \sigma^{-m+1}\}$. Thus

$$\sum_{v' \in S_{sp}} \mathcal{V}_v(Q(f, \sigma(f), \ldots, \sigma^{s-1}(f))) \geq r T m$$

For the special case of $m = b$, the agreement parameter in the interpolation algorithm can be improved to $T \geq \frac{rT}{\sqrt{N(\alpha-1)}}$ and $l = r T m - 1$. By setting $r T m > l$, we get $Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0$. Thus any function (message) $f \in \mathcal{L}((\alpha-1)P_\infty)$ whose evaluation (codeword) has an agreement of at least $T$ with the received word, where $rT(m-s+1) > l$ or $r T m > l$ in the case $m = b$, satisfies $Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0$. Thus we can find all the messages in the list if we could enumerate all $f \in \mathcal{L}((\alpha-1)P_\infty)$ that satisfy $Q(f, \sigma(f), \sigma^2(f), \ldots, \sigma^{s-1}(f)) = 0$. We are thus interested in solving the following root finding problem.

*Given a polynomial $Q \in L(z_1, z_2, \ldots, z_m)$ such that for every $h_1, h_2, \ldots, h_m \in \mathcal{L}((\alpha-1)P_\infty), Q(h_1, h_2, \ldots, h_m) \in \mathcal{L}(P_\infty)$ and an automorphism $\sigma \in \text{Gal}(L/K)$, enumerate $f \in \mathcal{L}((\alpha-1)P_\infty)$ that satisfy $Q(f, \sigma(f), \sigma^2(f), \ldots, \sigma^{s-1}(f)) = 0$.*
2.1. Frobenius Elements and Ramification Groups. Here we describe certain concepts in Galois extensions on which the decoding algorithms depend. Let \( v \) be an arbitrary place in \( L \) that is above a place \( u \) in \( K \). The decomposition group of \( v \) is defined as \( D_v := \{ \sigma \in \text{Gal}(L/K) : \sigma(v) = v \} \). For \( \sigma \in D_v \), the action of \( \sigma \) on the residue class field \( \mathbb{F}_v \) is well defined. That is \( \sigma(f(v)) = \sigma(f)\sigma(v) = \sigma(f)(v) \). Thus, there is a natural homomorphism \( \phi : D_v \rightarrow \text{Gal}(\mathbb{F}_v/\mathbb{F}_u) \). If \( v \) is unramified then \( \phi \) is an isomorphism, and there is a unique element \( \sigma_v \in \text{Gal}(L/K) \), called the Frobenius element at \( v \), such that \( \sigma_v(f) = f^{\#(\mathcal{O}_v/u)} \mod v \) for all \( f \in \mathcal{O}_L \). Let \( w \) be an unramified place in \( L \) above a place \( u \) in \( K \). Denote by \( \mathbb{H}_u := \{ \sigma_w, w \) is a place above \( u \} \). Let \( \Psi \subseteq \text{Gal}(L/K) \) be the conjugacy class of an arbitrary element in \( \text{Gal}(L/K) \). Tchebotarev Density Theorem ([13],[15][Thm 9.13B]) states that,

\[
\left| \{ u \in K : \mathbb{H}_u = \Psi \} \right| - \frac{|\Psi| q^{\deg(u)}}{|\text{Gal}(L/K)| \deg(u)} \leq 2g(K) \left| \Psi \right| \frac{q^{\deg(u)}}{|\text{Gal}(L/K)|} + \sum_{u' \in K \text{ ramified}} \deg(u')
\]

Here \( g(K) \) denotes the genus of \( K \).

3. Root Finding Step of the Decoding Algorithm

We now describe algorithms to solve the root finding problem. Two cases depending on if \( b \) is large or small are addressed. We begin by describing some techniques common to both cases. Let \( w \) (unramified) be a place in \( L \) lying above \( u \) in \( K \) such that \( \sigma \) is the Frobenius element at \( w \). Further assume that the degree of \( u \) is \( \eta = C \log_q(n) \), where \( C \) is a positive constant. As \( \sigma \) has order \( b \) in \( \text{Gal}(L/K) \), the degree of \( w \) is \( b\eta \). We recall that the action of \( \sigma \) at \( w \) is given by \( \sigma(f) = f^{\#(\mathcal{O}_u/u)} \mod w \). That is \( \sigma(f) = f^{\eta} \mod w \).

We now establish the existence of a place \( w \) of degree \( b\eta \) such that \( \sigma \) is the Frobenius element at \( w \). The existence follows from the Tchebotarev Density Theorem for function fields. The number of \( w \) of degree \( b\eta \) such that \( \sigma \) is the Frobenius at \( w \) is lower bounded by, \( \#\{ u \in K : \text{there is some } w \text{ over } u \text{ where } \sigma_w = \sigma, \deg(w) = b\eta \} \geq \frac{1}{b} \frac{q^{\eta}}{\eta} + O(q^{\frac{\eta}{2}}) \). Thus for large enough \( \eta \), such a place \( w \) always exists. In fact, roughly speaking, \( \frac{1}{b} \) fraction of all unramified places of degree \( \eta \) in \( K \) have a place \( w \) above it such that \( \sigma \) is the Frobenius element at \( w \). We are only interested in function fields where \( n > g \). In this case, the choice of \( \eta = C \log_q(n) \) with \( C \) a large enough absolute constant, guarantees the existence of such a \( w \). Moreover, such a place can be found in time polynomial in \( n \) as follows. Exhaustively search through each place of degree \( \eta \) in \( K \), if there exists a place above it where \( \sigma \) acts as the Frobenius. We can enumerate all places of degree at most \( C \log_q(n) \) of the separable extension \( K/\mathbb{F}_q(x) \). Given an element that generates \( L \) over \( K \) and the action of \( \sigma \) on that element, we can test if \( \sigma \) acts a Frobenius at a place above \( \eta \).

3.1. The large automorphism case : \( m \neq b \) and \( b \) large. The root finding problem is solved for the case where the automorphism used to fold has an order \( b \), that is at least a constant fraction of \( \frac{N}{\log_q(N)} \). Further we assume that \( m < b \) is small and independent of the blocklength.

Let \( w \in L \) be place of degree \( b\eta \), where \( \eta \) is the smallest integer such that \( b\eta \geq \alpha \).
LEMMA 3.1. The evaluation map \( \mathcal{L}((\alpha - 1)P_\infty) \hookrightarrow F_w \) is an injection.

Proof: The kernel of the map is the Riemann-Roch space \( \mathcal{L}((\alpha - 1)P_\infty - w) \). The degree of the divisor associated with the kernel is \( \deg(\alpha - 1 - \deg(w)) = \alpha - 1 - \deg(w) < 0 \). Since the dimension of the Riemann-Roch space associated with any divisor of negative degree is zero, the kernel is zero dimensional and the map is injective. \( \square \)

In addition, assume that \( \sigma \) is the Frobenius element at \( w \).

LEMMA 3.2. The number of \( f \in \mathcal{L} \) that satisfy \( Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0 \) is upper bounded by \( d.q^{(s-1)\eta} \).

Proof: Clearly, \( Q(f, \sigma(f), \ldots, \sigma^{s}(f))(w) = Q(f, f^\eta, \ldots, f^{(s-1)\eta})(w) \) because \( \sigma \) acts at \( w \) as \( \sigma(f) \equiv f^\eta \pmod{w} \), \( \forall f \in \mathcal{O}_w \).

Let \( Q = \sum_i q_i z_1^{a_{i1}} z_2^{a_{i2}} \ldots z_s^{a_{is}} \in L[z_1, z_2, \ldots, z_s] \) be the interpolated multivariate polynomial. We define \( Q_w := \sum_i q_i(w) z_1^{a_{i1}} z_2^{a_{i2}} \ldots z_s^{a_{is}} \) as the reduction of \( Q \) at \( w \).

If \( f \in \mathcal{O}_w \) satisfies \( Q(f, \sigma(f), \ldots, \sigma^{s-1}(f)) = 0 \), then \( Q(f, f^\eta, \ldots, f^{(s-1)\eta})(w) = 0 \). Thus \( f(w) \) is a root of \( Q_w(z, z^\eta, \ldots, z^{(s-1)\eta}) \) over \( F_w \). The degree of the univariate polynomial \( Q_w(z, z^\eta, \ldots, z^{(s-1)\eta}) \) is bounded by \( d.q^{(s-1)\eta} \). The number of roots of \( Q_w(z, z^\eta, \ldots, z^{(s-1)\eta}) \) in \( F_w \) is bounded by \( d.q^{(s-1)\eta} \). As \( \mathcal{L}((\alpha - 1)P_\infty) \hookrightarrow F_w \) is an injection, the roots \( f(w) \in F_w \) lift to a unique \( f \in \mathcal{L}((\alpha - 1)P_\infty) \). \( \square \)

Thus \( d.q^{(s-1)\eta} \) gives an upper bound on the number of solutions of the root finding problem. Observe that \( d.q^{(s-1)\eta} \) is polynomial in the block length \( N = \frac{n}{m} \). This is because \( b \) is at least a constant fraction of \( \frac{N}{\log_q(n)} \) and \( \alpha \leq n \). Hence the inequality \( b \eta \geq \alpha \) holds for an \( \eta = C \log_q(n) \) for a large enough constant \( C \).

We can extend the framework to use places of a small degree \( \mu \) for evaluation. This would result in codes over an alphabet of size \( q^{m\mu} \) and the worst case list size is polynomially bounded if the order of the automorphism \( b \) is comparable to the block length. A description follows.

Consider the composite function fields \( L' := F_w L \) and \( K' := F_w K \). Clearly, \( Gal(L'/K') \cong Gal(L/K) \). Thus \( Gal(L'/K') \) has an element (say \( \sigma' \)) of order \( b \). Further, \( L \) and \( L' \) have the same genus as \( F_w \) is perfect [15][Chap 10]. The rational places in \( L' \) that result out of splitting (in their entirety or a subset) are used as the places of evaluation. Using \( \sigma' \) to fold, we get folded codes over \( L' \). Let \( N' \) denote the number of places used for evaluation (block length). The alphabet size is \( q^{m\mu} \). From Lemma 3.2, we get the following result.

THEOREM 3.3. The codes constructed from \( L' \) are of block length \( N' \), rate \( R \) over an alphabet of size \( q^{m\mu} \) and can correct \( N' - N'((\frac{m}{m - s + 1}(R + \frac{m\eta}{N}))^{1/s}) \) errors with a list size bounded by \( d.q^{\mu(s-1)\eta} \).

By picking \( \mu \) large enough such that \( \frac{m\eta}{N} < 1 \), the fraction of errors corrected approaches \( 1 - R - \epsilon \) with the choice of \( m = \Theta(\frac{1}{\epsilon}) \) and \( s = \Theta(\frac{1}{\epsilon} \log(\frac{1}{\epsilon})) \) for any

\(^1\)Note that for the proof of Lemma 3.2 to be complete, we need to ensure that \( Q_w(z, z^{\eta}, \ldots, z^{(s-1)\eta}) \) does not go to zero. Such situations are overcome through a procedure analogous to [8][Lem 6.7] by using the fact that \( q^{\eta} > d \).
Given a field extension $L$ with an automorphism of order $b = o(\frac{g}{\log_q(g)})$, the above theorem gives a lower bound on the alphabet size to achieve the optimal error correction with polynomially bounded worst case list sizes. This can be seen by picking $\mu$ large enough such that $\frac{g}{\mu} < 1$ and picking only a subset of the places so that $b$ is at least a constant fraction of $\frac{N'}{\log_q(N')}$. This would achieve the optimal error correction trade off for an $\epsilon^3 > \frac{q}{N'}$. An example that improves on Folded Reed-Solomon Codes follows.

**Example 3.4. Codes from Kummer Extensions**

We use a special case of Kummer Extensions to give an example. A description of Kummer extensions can be found in [16]. Let $q$ be prime and $h(x)$ an irreducible polynomial in $K = \mathbb{F}_q(x)$. Consider $L = K(\nu)$, where $\nu$ is a root of the polynomial $y^{q-1} - h(x)$ which is irreducible in $K[y]$. The extension $L/K$ is cyclic of degree $q - 1$, say $Gal(L/K) = \langle \sigma \rangle$. The genus of $L$ is $\frac{(\deg(h)-1)(q-1)}{2}$. The point at infinity is totally ramified and all other rational places in $K$ away from zero are split. The number of rational places in $L$, that resulted out of splitting is $(q - 1)^2$.

Pick $g \log_q(g^D)$ of these places for evaluation for some constant $D$. Let the degree of $h$ be a small fixed constant, say $\deg(h) = 2$. Applying Theorem 3.3 to this case with $\mu = 1$ and $N' = g \log_q(g^D)$ yields codes over an alphabet size of $q^m$. For $\epsilon^3 > \frac{1}{\log_q(g^m)}$, setting $m = \Theta(\frac{1}{\epsilon})$, $s = \Theta(\frac{1}{\epsilon} \log(\frac{1}{R}))$ we can correct $1 - R - \epsilon$ errors with worst case list size bounded by $dg \frac{2^s}{\epsilon}$. Thus, the worst case list size is bounded by a polynomial in the block length. The alphabet size required $q^{\Theta(\frac{1}{\epsilon})}$ is lesser than the block length and thus improves on the alphabet size of Folded Reed-Solomon codes.

**3.2. Lifting algorithm to solve the Root Finding Problem:** We describe an algorithm to solve the root finding problem when the order of the automorphism $\sigma$ is small. In this case however the algorithm is much more complicated. We only describe the algorithm for the special case of $s = m = b$. The generalization to $s < m < b$ is straightforward and only this special case will be used in the explicit constructions.

We begin by developing some notation about local completions. Let $L_w$ denote the local completion of $L$ at $w$. Let $t$ be a local parameter at $w$. That is $t \in L$ such that $tO_w = wO_w$. Every $f \in O_w$ has an expansion at $w$ of the form $f = \sum_{c \in \mathbb{Z}} f_c t^c \in L_w$. Here $f_c \in O_w/wO_w \cong \mathbb{F}_w$. Thus $O_w$ can be thought of as the ring of infinite power series in $t$, $\mathbb{F}_w[[t]]$. Let $C_{f_c}(f)$ be an alternate notation for the coefficient $f_c$.

The interpolated polynomial $Q(z_1, z_2, \ldots, z_m)$ has degree $d$ and hence can be written as $\sum_{\beta} a_{\beta} z_1^{\beta_1} z_2^{\beta_2} \cdots z_m^{\beta_m}$, where $\beta_j \leq d$, $0 \leq j \leq m - 1$ and $a_{\beta} \in L$. Here $\beta$
The linear reduction map

We now set $a = 0$ the coefficients that the received word and the interpolation algorithm induce a distribution where $\phi$ takes uniformly random elements from variables in $\mathcal{O}_w$. For simplicity of presentation in the discussion below, we will assume that $\sigma(t) = t$. Since $\sigma$ acts on $\gamma \in \mathbb{F}_w$ as $\gamma : \gamma \rightarrow \gamma^\eta$ and fixes $t$, $\sigma$ acts on $\mathcal{O}_w \cong \mathbb{F}_w[[t]]$ as

$$
\sigma\left(\sum_{c=0}^{\infty} f_c t^c\right) = \sum_{c=0}^{\infty} \sigma(f_c) t^c = \sum_{c=0}^{\infty} f_c^\eta t^c
$$

LEMMA 3.5. The linear reduction map $\phi : \mathcal{L}((\alpha - 1)P_\infty) \hookrightarrow \mathbb{F}_w[[t]]/ < t^e >$ that takes $f \in \mathcal{L}((\alpha - 1)P_\infty) \subset \mathcal{O}_w$ to $\sum_{c=0}^{e} f_c t^c$ is injective for $e > \left\lceil\frac{m}{\eta}\right\rceil$.

**Proof:** Let $h \in \mathcal{L}((\alpha - 1)P_\infty)$ be in the kernel of the map. Then $h_e = 0$ for $e = 0, \ldots, e - 1$, hence $h$ has a zero of multiplicity at least $e$ at $w$. It follows that $h \in \mathcal{L}((\alpha - 1)P_\infty - ew)$. But $\deg((\alpha - 1)P_\infty - ew) = \alpha - 1 - em\eta < 0$, so $\mathcal{L}((\alpha - 1)P_\infty - ew)$ has dimension 0, and it follows that $h = 0$. \(\Box\)

We now set $e = \left\lceil\frac{m}{\eta}\right\rceil$. Thus $f \in \mathcal{L}((\alpha - 1)P_\infty)$ can be determined from its truncated expansion $\phi(f) = \sum_{c=0}^{e} f_c t^c$. From the above lemma it is clear that to find the list of messages with sufficient agreement, it suffices to solve the following problem in the local completion.

Find all $\phi(f) \in \mathbb{F}_w[[t]]/ < t^e >$ such that $Q(f, \sigma(f), \ldots, \sigma^{m-1}(f)) = 0$ in $\mathbb{F}_w[[t]]$

An algorithm is described in the next section to solve the above problem from which the below result follows. The algorithm depends only on the coefficients $a_{\beta}$. Let $\phi(a_{\beta}) = \sum_{c=0}^{e} a_{\beta,c} t^c$ be the truncated expansion of $a_{\beta}$. Under the assumption that the received word and the interpolation algorithm induce a distribution where the coefficients $a_{\beta,0}, a_{\beta,1}, \ldots, a_{\beta,e}$ are independent uniformly distributed random variables in $\mathbb{F}_w$, we have the below result.

**Theorem 3.6.** If $\{a_{\beta,c}, 0 \leq c \leq e, \beta \in B\}$ constitute a set of independent, uniformly random elements from $\mathbb{F}_w$, then the expected list size is bounded by $d q^{(m-1)\eta}$.

A proof of the above theorem is given in the next section.

**Heuristic Assumption:** We assume that when a random error occurs on the transmitted codeword, the interpolation algorithm maps the received word into $\{a_{\beta,c}, 0 \leq c \leq e, \beta \in B\}$ thereby inducing a distribution wherein $a_{\beta,c}$ are independent, uniformly random elements from $\mathbb{F}_w$.

The heuristic assumption is a natural one because the coefficients of $Q$, $a_{\beta} \in \mathcal{L}((\alpha - 1)P_\infty)$ are determined as the solution of a linear system that depends on the received word. The linear system is usually close to full rank. This is followed by the reduction of $a_{\beta,c}$ modulo $t^e$.

With this assumption, for a random received word, the expected list size is bounded by $d q^{(m-1)\eta}$, which is a polynomial in the block length.
4. Root finding in the Local Completion

We describe an algorithm to determine $\phi(f) \in \mathbb{F}_w[[t]]/ < t^e >$ corresponding to $f \in \mathcal{L}((\alpha - 1)\mathcal{P}_\infty) \subset \mathbb{F}_w[[t]]$ such that $Q(f, \sigma(f), \ldots, \sigma^{m-1}(f)) = 0$ in $\mathbb{F}_w[[t]]$. As a consequence we have an algorithm that solves the root finding problem for the case of expected number of roots is bounded by a polynomial in the degree of $Q$ and the size of the residue class field $\mathbb{F}_w$ when the coefficients of $Q$ modulo $t^e$ is drawn at random.

We begin by writing down the constraints that $\{f_c\}_{c=0}^e$ corresponding to $\phi(f) = \sum_{c=0}^e f_c t^c$ must satisfy.

**Lemma 4.1.** For all $f \in \mathbb{F}_w[[t]]$ such that $Q(f, \sigma(f), \ldots, \sigma^{m-1}(f)) = 0$ in $\mathbb{F}_w[[t]]$ and $i \geq 0$, 

$$Q(\sum_{c=0}^{i-1} f_c t^c, \sum_{c=0}^{i-1} f^q_c t^c, \ldots, \sum_{c=0}^{i-1} f^{q^{(m-1)}}_c t^c) \equiv 0 \pmod{t^i}$$

**Proof:** For all $i \geq 0$, we have

$$Q(f, \sigma(f), \sigma^2(f), \ldots, \sigma^{m-1}(f)) = Q(\sum_{c=0}^\infty f_c t^c, \sigma(\sum_{c=0}^\infty f_c t^c), \ldots, \sigma^{m-1}(\sum_{c=0}^\infty f_c t^c))$$

$$= Q(\sum_{c=0}^{i-1} f_c t^c, \sigma(\sum_{c=0}^{i-1} f_c t^c), \ldots, \sigma^{m-1}(\sum_{c=0}^{i-1} f_c t^c)) \pmod{t^i}$$

$$= Q(\sum_{c=0}^{i-1} f_c t^c, \sum_{c=0}^{i-1} f^q_c t^c, \ldots, \sum_{c=0}^{i-1} f^{q^{(m-1)}}_c t^c) \pmod{t^i}$$

$$\Rightarrow Q(\sum_{c=0}^{i-1} f_c t^c, \sum_{c=0}^{i-1} f^q_c t^c, \ldots, \sum_{c=0}^{i-1} f^{q^{(m-1)}}_c t^c) \equiv 0 \pmod{t^i}$$

By Lemma 3.5 $f \in \mathcal{L}((\alpha - 1)\mathcal{P}_\infty)$ is determined by $f \pmod{t^e}$. Hence it suffices to determine $\{f_c\}_{c=0}^e$ such that $Q(\sum_{c=0}^{i-1} f_c t^c, \sum_{c=0}^{i-1} f^q_c t^c, \ldots, \sum_{c=0}^{i-1} f^{q^{(m-1)}}_c t^c) \equiv 0 \pmod{t^e}$. These equations only depend on the coefficients of $Q$ modulo $t^e$.

We begin by determining the list of possible $f_0$. We have $Q(f_0, f_0^q, \ldots, f_0^{q^{(m-1)}}) = 0 \pmod{t}$. Thus $f_0$ is a root of $Q_w(z, z^q, \ldots, z^{q^{(m-1)}})$ in $\mathbb{F}_w$. Hence a list of possible $f_0$ can be enumerated by finding the roots of $Q_w(z, z^q, \ldots, z^{q^{(m-1)}})$ whose degree gives an upper bound of $d q^{(m-1)}$ on the number of possible $f_0$.

For every fixed $f_0$, $f_1, \ldots, f_{i-1}$ such that

$$Q(\sum_{c=0}^{i-1} f_c t^c, \sum_{c=0}^{i-1} f^q_c t^c, \ldots, \sum_{c=0}^{i-1} f^{q^{(m-1)}}_c t^c) \equiv 0 \pmod{t^i},$$

we have

$$Q(\sum_{c=0}^{i} f_c t^c, \sum_{c=0}^{i} f^q_c t^c, \ldots, \sum_{c=0}^{i} f^{q^{(m-1)}}_c t^c) \equiv \mu_i t^i \pmod{t^{i+1}}$$

where $\mu_i = C_{t^i}(Q(\sum_{c=0}^{i} f_c t^c, \sum_{c=0}^{i} f^q_c t^c, \ldots, \sum_{c=0}^{i} f^{q^{(m-1)}}_c t^c)).$
Again the set of valid $f_i$ is contained in the set of $f_i$ that satisfy $\mu_i = 0$. Observe that $\mu_i = 0$ is a polynomial equation in $f_0, f_1, \ldots, f_i$. Given that $f_0, f_1, \ldots, f_{i-1}$ are already determined, we can break $\mu_i$ into a polynomial in $f_i$ and a polynomial that does not contain $f_i$. The polynomial in $f_i$ turns out to be very special. It is an additive polynomial whose coefficients depend only on $f_0$ and $a_{\beta,0}$. We now proceed to illustrate this fact and show how this can be exploited to determine $f_i$.

Consider the term

\[
\left( \sum_{c=0}^{\infty} a_{\beta,c} t^c \right) \left( \sum_{c=0}^{\infty} f_{q^c} t^c \right) \cdots \left( \sum_{c=0}^{\infty} f_{q^{(m-1)}t^c} \right)
\]

corresponding to the monomial $a_{\beta} z_1^{\beta_1} z_2^{\beta_2} \cdots z_m^{\beta_m}$.

The coefficient of $t^i$ that arises from this monomial is

\[
a_{\beta,0} \sum_{j=1, \beta_j \neq 0}^m f_0^{\lambda_0 \beta - q(j-1)\eta} f_i^{(j-1)\eta} + a_{\beta,i} f_0^{\lambda_0} + H_{\beta,i}
\]

Here $H_{\beta,i}$ depends on \{ $a_{\beta,0}, a_{\beta,1}, \ldots, a_{\beta,i-1}, f_0, f_1, \ldots, f_{i-1}$ \} and $H_i := \sum_{\beta} H_{\beta,i}$, and $\lambda_{\beta} := \sum_{j=1}^m \beta_j q(j-1)\eta$.

By taking the sum over all monomials, we get

\[
\mu_i = \sum_{\beta} a_{\beta,0} \sum_{j=0, \beta_j \neq 0}^m f_0^{\lambda_0 \beta - q(j-1)\eta} f_i^{(j-1)\eta} + \sum_{\beta} a_{\beta,i} f_0^{\lambda_0} + H_i
\]

The term depending on $f_i$ can be rewritten as

\[
\sum_{\beta} a_{\beta,0} \sum_{j=0, \beta_j \neq 0}^m f_0^{\lambda_0 \beta - q(j-1)\eta} f_i^{(j-1)\eta} = \sum_{j=1}^m \left( \sum_{\beta, \beta_j \neq 0} a_{\beta,0} f_0^{\lambda_0 \beta - q(j-1)\eta} f_i^{(j-1)\eta} \right)
\]

Define $F(z) := \sum_{j=1}^m \left( \sum_{\beta, \beta_j \neq 0} a_{\beta,0} f_0^{\lambda_0 \beta - q(j-1)\eta} \right) z^{q(j-1)\eta}$. Clearly, $F$ is a fixed polynomial independent of $i$ and depends only on $a_{\beta,0}$ and $f_0$.

Now $\mu_i = 0 \Rightarrow F(f_i) + \sum_{\beta} a_{\beta,i} f_0^{\lambda_0} + H_i = 0$. As $f_0, f_1, \ldots, f_{i-1}$ are fixed, we can solve for $f_i$ by finding the roots in $F_w$ of the polynomial $F(z) + \sum_{\beta} a_{\beta,i} f_0^{\lambda_0} + H_i = 0$.

Observe that the polynomial $F(z) \in F_w[z]$ is an additive polynomial $\langle q \rangle$-polynomial [6][12] and is $F_u$-linear. The roots of $F(z)$ in $F_w$ thus forms an $F_u$-linear space. The polynomial $F(z) + \sum_{\beta} a_{\beta,i} f_0^{\lambda_0} + H_i = 0$ is the sum of the additive polynomial $F(z)$ and the constant term $\sum_{\beta} a_{\beta,i} f_0^{\lambda_0}$. For each $i$, the constant term $\sum_{\beta} a_{\beta,i} f_0^{\lambda_0} + H_i$ is fixed given that $f_0, f_1, \ldots, f_{i-1}$ is fixed. We now state a useful lemma on the structure of the roots polynomial that are the sum of an additive polynomial and a constant.

Let $P(z) \in F_w[z]$ be an additive polynomial that is $F_u$-linear. In particular $P$ is of the form $P(z) = \sum_{j=0}^{\deg(P)} p_j z^{q^j}$, where $p_j \in F_w$. Let $U_P$ denote the $F_u$-linear
space of the roots of $P$ in $\mathbb{F}_w$. Let $\delta \in \mathbb{F}_w$ be an arbitrary field element.

**Lemma 4.2.** If $\gamma_1, \gamma_2 \in \mathbb{F}_w^*$ are two roots of the polynomial $W(z) := P(z) - \delta$, then $\gamma_2 \in \gamma_1 + U_p$.

**Proof:** The elements $\gamma_1, \gamma_2 \in \mathbb{F}$ are roots of $W$. Thus $P(\gamma_1) = \delta$ and $P(\gamma_2) = \delta \Rightarrow P(\gamma_1) = P(\gamma_2)$. But $P$ is an additive polynomial. Thus $P(\gamma_1) - P(\gamma_2) = 0 \Rightarrow P(\gamma_1 - \gamma_2) = 0 \Rightarrow \gamma_2 \in \gamma_1 + U_p$.

The converse holds as well. That is, if $\gamma_1$ is a root of $W$, then all the elements of $\gamma_1 + U_p$ are roots of $W$. Thus the polynomial $W$ either has no roots in $\mathbb{F}_w$ or has exactly $\#U_p$ roots. Further, $W$ has a root say $\gamma \in \mathbb{F}_w$ if and only if $P(\gamma) = \delta$.

Consider the space of $\mathbb{F}_w$-linear maps from $\mathbb{F}_w$ to $\mathbb{F}_w$. Every such map arises out of the evaluation map of an additive polynomial $[6]$. Let $P(\mathbb{F}_w)$ denote the image of $\mathbb{F}_w$ under the linear map associated with $P$. From the above argument, it is clear that the polynomial $W$ has a root in $\mathbb{F}_w$ if and only if $\delta \in P(\mathbb{F}_w)$.

Define $\delta_i := -\sum_{\beta} a_{\beta,i} f_0^{\lambda_\beta} - H_i$. The polynomial $F(z) - \delta_i$ has roots in $\mathbb{F}_w$ if and only if $\delta_i \in F(\mathbb{F}_w)$.

This prompts at an iterative procedure that can be used to exhaust the list of all coefficients $\{f_c\}, 0 \leq c \leq e$ that correspond to the messages $f$ in question. We now present the algorithm. Consider a rooted tree with root $r$ and nodes corresponding to elements from $\mathbb{F}_w$.

**The Decoding Algorithm**

- Set of roots of $Q_w(z, z^q, \ldots, z^{q^{(m-1)}})$ in $\mathbb{F}_w$ as the children of the root.
- Compute $U_F$, the space of roots of $F(z)$ in $\mathbb{F}_w$ and $F(\mathbb{F}_w)$.
- For $i = 1$ to $e$,
  - For every path $(r, f_0, f_1, \ldots, f_{i-1})$ do
    - If $\delta_i \in F(\mathbb{F}_w)$ with $F(\gamma) = \delta_i$, then set $\gamma + U_F$ as the children of $f_{i-1}$.
  - Lift every $f_0 + f_1 t + \ldots + f_e t^e$ corresponding to a path $(r, f_0, f_1, \ldots, f_e)$ to a function $f \in L((\alpha - 1)P_\infty)$.
- Output the list of all such functions that have sufficient agreement.

The root finding in the first step can be performed efficiently in time polynomial in the degree of $Q_w(z, z^q, \ldots, z^{q^{(m-1)}})$. The root finding in the second step can be done efficiently by solving a linear system as described in [12][Eqn 3.16]. Hence the total running time of the algorithm is polynomially bounded by the number of nodes in the tree.

**4.1. List Size and Running Time of the Algorithm.** In this section we present a heuristic argument that shows that the running time of the algorithm as well as the list size grow polynomially in the block length with very high probability.

The list size is clearly upper bounded by the number of leaf nodes at the level $e$ in the tree. The number of choices for $f_0$ is upper bounded by $d q^{(m-1)\eta}$, which
is the degree of the polynomial \( Q_w(z, z^{\eta}, \ldots, z^{\eta^{(m-1)}}) \). For a fixed \( f_0 \), we now analyse the number of leaf nodes at level \( e \) that are descendents of \( f_0 \).

From the algorithm description, it is clear that the algorithm depends only on \( a_{\beta,0}, a_{\beta,1}, \ldots, a_{\beta,e} \), the coefficients of \( Q \) modulo \( t^e \). Consider the set of coefficients \( \{a_{\beta,c}, 0 \leq c \leq e, \beta \in B\} \). This can be regarded as an element in \( \bigoplus_{0 \leq c \leq e, \beta \in B} \mathbb{F}_w \). The interpolation algorithm followed by reduction modulo \( t^e \), maps the received word to an element in the finite set \( \bigoplus_{0 \leq c \leq e, \beta \in B} \mathbb{F}_w \).

We now present a lemma that relates the distribution of \( \{a_{\beta,c}, 0 \leq c \leq e, \beta \in B\} \) to the distribution they induce on \( \delta_i \).

**Lemma 4.3.** For any \( 0 < i \leq e \), if \( \{a_{\beta,i}, \beta \in B\} \) are independent and uniformly random then \( \delta_i \) is a uniformly random variable in \( \mathbb{F}_w \) given that \( f_0, \ldots, f_{i-1} \) are fixed.

**Proof:** By definition, \( \delta_i = -\sum_\beta a_{\beta,i} f_0^\lambda \beta - H_i \). Here \( H_i \) is an element in \( \mathbb{F}_w \) determined completely by \( a_{\beta,0}, \ldots, a_{\beta,i-1} \), and \( f_0, \ldots, f_{i-1} \). Over a finite field a finite linear combination of independent uniformly distributed variables plus a fixed element induces the uniform distribution. Thus \( \delta_i \) is a uniformly random element in \( \mathbb{F}_w \).\( \square \)

Let \( U = U_F \). Assume that \( f_0, \ldots, f_{i-1} \) and \( a_{\beta,0}, \ldots, a_{\beta,i-1} \) are fixed. The node \( f_{i-1} \) has children if and only if \( \delta_i \in F(\mathbb{F}_w) \). The image \( F(\mathbb{F}_w) \) is an \( \mathbb{F}_w \) linear space of dimension \( m - \dim(U) \), where \( \dim(U) \) is the dimension of \( U \). We reiterate that the linear spaces \( U \) and \( F(\mathbb{F}_w) \) are fixed once \( f_0 \) is fixed.

The probability that \( \delta_i \), considered as a random element in \( \mathbb{F}_w \), is in \( F(\mathbb{F}_w) \) is

\[
\text{Prob}\{\delta_i \in F(\mathbb{F}_w)\} = \frac{\#F(\mathbb{F}_w)}{\#\mathbb{F}_w} = \frac{q^{\eta(m - \dim(U))}}{q^{\eta m}} = q^{-\eta \dim(U)}.
\]

The expected number of \( f_i \) given \( \{f_0, f_1, \ldots, f_{i-1}\} \) is, by Lemma 4.3,

\[
E(\#f_i|\{f_0, f_1, \ldots, f_{i-1}\}) = \#U \text{Prob}\{\delta_i \in F(\mathbb{F}_w)\} = q^{\eta \dim(U)} q^{-\eta \dim(U)} = 1
\]

**Lemma 4.4.** The expected number of nodes at level \( i \) that are descendents of a fixed \( f_0 \) is bounded by 1.

**Proof:** We prove the above claim by induction. Again, fix \( f_0 \). Assume inductively that the expected number of \( f_{i-1} \) that are descendents of \( f_0 \) is 1.

For \( f_1, \ldots, f_i \in \mathbb{F}_w \), let \( Pr(f_0, \ldots, f_i) \) denote the probability that \( f_0, f_1, \ldots, f_i \) is a path; that is \( f_j \) is a descendent of \( f_{j-1} \) for \( j = 1, \ldots, i \). Then for fixed \( f_0 \) the
expected number of descendents of \( f_0 \) at level \( i \) is

\[
\sum_{f_1, \ldots, f_i \in F_w} \Pr(f_1, \ldots, f_i) = \sum_{f_i} \sum_{f_1, \ldots, f_{i-1}} \Pr(f_i|f_1, \ldots, f_{i-1}) \Pr(f_1, \ldots, f_{i-1}) \\
= \sum_{f_i} \sum_{f_1, \ldots, f_{i-1}} \Pr(f_i|f_1, \ldots, f_{i-1}) \Pr(f_1, \ldots, f_{i-1}) \\
= \Pr(f_1, \ldots, f_{i-1}) \sum_{f_i} \Pr(f_i|f_1, \ldots, f_{i-1}) \\
= \Pr(f_1, \ldots, f_{i-1}) \mathbb{E}(\#f_1, \ldots, f_{i-1}) \\
= \Pr(f_1, \ldots, f_{i-1}).
\]

The last equality is the expected number of descendents of \( f_0 \) at level \( i - 1 \), and by induction that is \( 1^2 \square \)

From the lemma it follows that under the assumption that \( \delta_i \) are random elements in \( F_w \), the number of \( f_e \) that are descendents of \( f_0 \) is bounded by 1. Hence the total number of \( f_e \) is bounded by the number of \( f_0 \). Thus the list size is upper bounded by the number of \( f_0 \). Thus the list size is bounded by \( d q^{(m-1)n} \).

Consider the case when \( \{a_{\beta,c}, 0 \leq c \leq e, \beta \in B\} \) are independent, uniformly random elements from \( F_w \). In this case the constraint that \( \{a_{\beta,c}, \beta \in B\} \) are independent uniformly random is clearly satisfied. Finally, Theorem 3.6 follows from Lemma 4.3, Lemma 4.4 and the fact that the list size is bounded by the number of leaf nodes at level \( e \) in the tree.

5. Polynomial List Sizes and A Question on the Existence of Certain Field Extensions

We apply the Folded Algebraic Geometric Code construction (the case of \( m \neq b \) and \( b \) large) to certain field extensions that have large order automorphisms.

Let \( L_a \) be a finite Galois extension of \( \mathbb{F}_q(x) \). Assume that we have a sequence of such function fields \( L_a, a \in \mathbb{Z}^+ \) with genus \( g(L_a) \) tending to infinity as \( a \) grows. The function field sequence \( L_a \) is called as asymptotically good if the ratio of the number of rational places in \( L_a \) to the genus \( g(L_a) \) is bounded away from zero as the genus \( g \) grows. This is an informal definition. For a formal definition see [16][V.3.6]. In our context we pose a further restriction and say that \( L_a \) is asymptotically good if the ratio of the number of rational places in \( L_a \) that resulted out of splitting in the extension (call \( n \)) to the genus of \( L_a \) is greater than 1. In addition we require that \( L_a \) also have a large order automorphism \( \tau \in \text{Gal}(L_a/\mathbb{F}_q(x)) \).

**Question 5.1:** Does there exist an asymptotically good sequence of function fields \( L_a \) such that there exists an element \( \tau \in \text{Gal}(L_a/\mathbb{F}_q(x)) \) whose order \( b \) is a constant

---

\(^2\)We have to address the case where \( F(z) \) is identically zero. In this case any \( f_e \in F_w \) satisfies \( F(f_e) = 0 \). However \( F(F_w) = 0 \). The probability that \( \delta_i = 0 \) is \( \frac{1}{\#F_w} \). Thus the expected number of \( f_i \) given \( f_0, f_1, \ldots, f_{i-1} \) is \( \frac{1}{\#F_w} \cdot \#F_w = 1 \)
times \frac{[L_a:F_q(x)]}{\log_q([L_a:F_q(x)])} \gamma

If such an extension exists, the number of rational places in \( L_a \) is upper bounded by \( q |L_a : F_q(x)| = q \# Gal(L_a/F_q(x)) \). Thus \( b \) is a constant fraction of \( \frac{N}{\log_q(N)} \).

From section 3.1, we have the following result.

**The codes constructed from** \( L_a \) **are of block length** \( N \), **rate** \( R \) over an alphabet of size \( q \), that can correct \( N - N \left( \frac{m}{m-s+1} (R + \frac{m8}{N}) \right) \) errors with a list size bounded by a polynomial in \( N \).

The fraction of errors corrected approaches \( 1 - R - \epsilon \) for the choice of \( m = \Theta(\frac{1}{x^2}) \) and \( s = \Theta(\frac{1}{x} \log(\frac{1}{x})) \) for any \( \epsilon > \frac{2}{8} \). A discussion on the existence of asymptotically good towers of function fields with large automorphism follows.

We begin by considering towers where the field at the top is Galois over the rational functional field. The Galois closure of the Garcia-Stichtenoth is one such example. It is interesting to note that the Galois Closure of the Garcia-Stichtenoth towers are optimal as well [17]. Thus in that case the function field on the top of the tower (call \( L_a \)) is a Galois extension of \( F_{q^2}(x) \). Thus we can hope to use elements of \( Gal(L_a/F_{q^2}(x)) \) to fold the code. But it is not clear if there exists an element of order comparable to the degree of the extension. In fact, when \( q \) is prime, the Galois group is \( \bigoplus_{a=0}^{x} \mathbb{Z}/2\mathbb{Z} \). In this case no such large order automorphisms exist and all elements have order at most \( q \).

There certainly exists geometric extensions with large automorphisms. For instance, there exists cyclic extensions (Galois Group is cyclic) over \( F_q(x) \) of arbitrarily large degree, when the degree of the extension is a power of \( q \). These are special cases of cyclotomic function fields [15][chap 12],[6][chap 3] and are generated by adjoining to \( F_q(x) \), a torsion submodule of the division points of a Carlitz module. However, such extensions do not possess enough places of small degree [11]. As a consequence, folded codes defined on theses cyclic extensions do not improve on Folded Reed Solomon codes in terms of alphabet size. Recently, Guruswami [7] by considering certain special subfields of the cyclomatic fields, constructed codes that achieve the list decoding capacity with an alphabet size that is logarithmic in the block length.

### 6. Folded Codes from Garcia-Stichtenoth Towers

Garcia and Stichtenoth described [4] function field towers that are asymptotically optimal. We apply the construction with \( s = m = b \) to these towers of function fields. We state the below theorems quantifying the error correction performance of these codes.

**Theorem 6.1.** The folded codes from Garcia-Stichtenoth towers of rate \( R \), block length \( N \) over an alphabet of size \( q^{2m} \) can correct \( N(1 - (R + \frac{m}{q-1}) \frac{1}{m}) \) errors.

The expected list size bounded by \( N^{O(m)} \) under the heuristic assumption
The Folded codes from Garcia-Stichtenoth towers of rate $R$ can correct up to a fraction of $1 - R - \epsilon$ errors over an alphabet of size $(\frac{1}{2m})^{O(\frac{1}{\epsilon})}$ independent of the size of the block length.

The expected list size is bounded by $N^{O(\frac{1}{\epsilon})}$ under the heuristic assumption.

These are towers defined as a sequence of Artin-Schreier extensions. The base field is the finite field $F_{q^2}$, where $q$ is a prime power. $F_0$ is the rational function field $F_0 = F_{q^2}(x)$.

$$F_i = F_{i-1}(x_n)$$

$$x_i^q + x_i = \frac{x_{i-1}^q}{x_{i-1}^2 + 1}, \quad 1 \leq i \leq a.$$ 

The automorphism $\sigma$ is used to fold the places $S_{sp}$. By evaluating $L((\alpha - 1)P_\infty)$ at $P_\infty$, we get a folded algebraic geometric code with $n = q^k(q^2 - q)$ and a folding parameter of $m$. Observe that by increasing $a$ we can make $n$ arbitrarily large compared to $m$.

Thus the block length of the resulting code is $N = \frac{q^a(q^2 - q)}{m}$. The dimension of the code $k = \text{dim}(L((\alpha - 1)P_\infty))$. If $\alpha - 1 \geq 2g - 2$, then $k = \alpha - g$. The code is over an alphabet of $q^{2m}$ and under our heuristic can be decoded if the agreement $T$ is at least $\frac{m-1}{\sqrt{N(\alpha - 1)^m}}$ with expected list size bounded by $d,q^{2(m-1)n}$. Thus the number of errors that can be corrected is $N - \frac{m-1}{\sqrt{N(\alpha - 1)^m}} = N(1 - (\frac{k+g}{N})^{\frac{m}{m+1}})$

Observe that $n/g$ tends to $q - 1$ as $g$ grows. Here $m$ equals $p$, the characteristic of the finite field $F_{q^2}$. Theorem 6.1 follows

The expected list size bounded by $N^{O(m)}$ under the heuristic assumption.

Observe that the Folded codes from Garcia-Stichtenoth towers of rate $R$ can correct
up to a fraction of $1 - R - \epsilon$ errors when $p = o\left(\frac{1}{\epsilon^2}\right)$, $m = p^2$ and $q = p^b, b > 2$. This is the optimum tradeoff in terms of rate and error correction \cite{1}. Thus if $q = p^2$, we can achieve the optimum rate-error correction tradeoff over an alphabet of size $(\frac{1}{p^2})^{O\left(\frac{1}{\epsilon^4}\right)}$ independent of the size of the block length. Theorem 6.2 follows.

References

\cite{1} Aleshnikov, I., Kumar, P.V., Shum, K.W., Stichtenoth, H. “On the splitting of places in a tower of function fields meeting the Drinfeld-Vladut bound”, IEEE Transactions on Information Theory, Volume 47, Issue 4, May 2001 Page(s):1613 - 1619


\cite{5} V D Goppa “Geometry and Codes” in Mathematics and its Applications. Kluwer Academic Press


\cite{7} Venkatesan Guruswami, “Artin automorphisms, Cyclotomic function fields, and Folded list-decodable codes”, ACM Symposium on Theory of Computing (STOC) 2009


\cite{10} Venkatesan Guruswami, Madhu Sudan, “Improved decoding of Reed-Solomon and algebraic-geometric codes ” IEEE Trans. on Info. Theory

\cite{11} Ming-Deh Huang and Anand Kumar Narayanan, “Folded Algebraic Geometric Codes from Galois Extensions” http://arxiv.org/abs/0901.1162


\cite{14} Farzad Parvaresh, Alexander Vardy, “Correcting errors beyond the Guruswami-Sudan radius in polynomial time” IEEE Symposium on Foundation of Computer Science (FOCS) 2005

\cite{15} Michael Rosen, “Number Theory in Function Fields”. Graduate Texts in Mathematics


Computer Science Department, University of Southern California, Los Angeles 90089

E-mail address: huang@usc.edu

Computer Science Department, University of Southern California, Los Angeles 90089

E-mail address: anandnarayanan@usc.edu