Electronic Colloquium on Computational Complexity, Report No. 46 (2013)

Optimal rate list decoding of folded algebraic-geometric codes over constant-sized alphabets

Venkatesan Guruswami[*] Chaoping Xing[†]

March 2013

Abstract

We construct a new list-decodable family of asymptotically good algebraic-geometric (AG) codes over fixed alphabets. The function fields underlying these codes are constructed using class field theory, specifically Drinfeld modules of rank 1, and designed to have an automorphism of large order that is used to "fold" the AG code. This generalizes earlier work by the first author on folded AG codes based on cyclotomic function fields. The recent linear-algebraic approach to list decoding can be applied to our new codes, and crucially, we use the Chebotarev density theorem to establish a polynomial upper bound on the list-size for list decoding up to an error fraction approaching $1 - R$ where R is the rate. The list decoding can be performed in polynomial time given polynomial amount of pre-processed information about the function field.

Our construction yields algebraic codes over constant-sized alphabets that can be list decoded up to the Singleton bound — specifically, for any desired rate $R \in (0,1)$ and constant $\varepsilon > 0$, we get codes over an alphabet size $(1/\varepsilon)^{O(1/\varepsilon^2)}$ that can be list decoded up to error fraction $1-R-\varepsilon$ confining close-by messages to a subspace with $N^{O(1/\varepsilon^2)}$ elements. Previous results for list decoding up to error-fraction $1-R-\varepsilon$ over constant-sized alphabets were either based on concatenation or involved taking a carefully chosen subcode of algebraic-geometric codes. In contrast, our result shows that these folded algebraic-geometric codes *themselves* have the claimed list decoding property. Further, our methods to get function fields with the properties needed for constructing and decoding the code might be of independent algebraic interest.

[*] Computer Science Department, Carnegie Mellon University, Pittsburgh, USA. Research supported in part by a Packard Fellowship and NSF CCF-0963975. Email: guruswami@cmu.edu

[†] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg

ISSN 1433-8092

1 Introduction

Reed-Solomon codes are a classical and widely used family of error-correcting codes. They encode messages, which are viewed as polynomials $f \in \mathbb{F}_q[X]$ of degree $< k$ over a finite field $\mathbb{F}_q$, into *codewords* consisting of the evaluations of f at a sequence of n distinct elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ (this requires a field size $q \geqslant n$). We refer to n as the block lengh of the code. The rate of this code, equal to the ratio of number of message symbols to the number of codeword symbols, equals $R = k/n$. Since two distinct polynomials of degree $< k$ can agree on at most $k-1$ distinct points, every pair of Reed-Solomon codewords differ on more than $n-k$ positions. In other words, the *relative distance* of this code, or the minimum fraction of positions two distinct codewords differ on, is bigger than $(1-R)$. This means that even if up to a fraction $(1-R)/2$ of the n codeword symbols, are corrupted in an *arbitrary* manner, the message polynomial f is still uniquely determined. Moreover, classical algorithms, starting with [14], can recover the message f in such a situation in polynomial time.

For a fraction of errors exceeding $(1-R)/2$, unambiguous decoding of the correct message is not always possible. This holds not just for the Reed-Solomon code but for *every* code. However, if we allow the decoder to output in the worst-case a small list of messages whose encodings are close to the corrupted codeword, then it turns out that one can correct a much larger error fraction. This model is called *list decoding*. Using the probabilistic method, for any $\varepsilon > 0$, one can prove the abundance of codes of rate R which can be list decoded up to an error fraction $(1-R-\varepsilon)$ with a maximum output list size bounded by a constant depending only on ε. This error fraction is twice the classicial $(1-R)/2$ bound, and further is optimal as the message has Rn symbols of information and recovering it up to some small ambiguity is impossible from fewer than a fraction R of correct codeword symbols.

Recent progress in algebraic coding theory has led to the construction of explicit codes which can be efficiently list decoded up to an error fraction approaching the $1-R$ information-theoretic limit. The first such construction, due to Guruswami and Rudra [7], was *folded Reed-Solomon codes*. In the *m-folded* version of this code (where m is a positive integer), the Reed-Solomon (RS) encoding $(f(1), f(\gamma), \cdots, f(\gamma^{n-1}))$ of a low-degree polynomial $f \in \mathbb{F}_q[X]$ is viewed as a codeword of length $N = n/m$ over the alphabet $\mathbb{F}_q^m$ by blocking together successive sets of m symbols. Here γ is a primitive element of the field $\mathbb{F}_q$. The alphabet size of the folded RS codes is $q^m > N^m$. To list decode these codes up to an error fraction $1-R-\varepsilon$, one has to choose $m \approx 1/\varepsilon^2$ which makes the alphabet size a larger polynomial in the block length. In comparison, the probabilistic method shows the existence of such list decodable codes over an alphabet size $\exp(O(1/\varepsilon))$, which is also the best possible asymptotic dependence on ε.

It is possible to bring down the alphabet size of folded RS codes by concatenating them with appropriate optimal codes found by a brute-force search, followed by symbol redistribution using an expander [7]. However, the resulting codes have a large construction and decoding complexity due to the brute-force decoding of the inner codes used in concatenation. Furthermore, these codes lose the nice algebraic nature of folded RS codes which endows them with other useful features like list recovery and soft decoding. It is therefore of interest to find explicitly described algebraic codes over *smaller* alphabets with list decoding properties similar to folded RS codes.

Algebraic-geometric (AG) codes are a generalization of Reed-Solomon codes based on algebraic curves which have $n \gg q$ $\mathbb{F}_q$-rational points. These enable construction of RS-like codes with alphabet size smaller than (and possibly even dependent of) the block length. Thus, they provide a possible avenue to construct the analog of folded RS codes over smaller alphabets.

The algebraic crux in list decoding folded RS codes was the identity $f(\gamma X) \equiv f(X)^q \pmod{E(X)}$ for $E(X) = X^{q-1} - \gamma$ which is an irreducible polynomial over $\mathbb{F}_q$. Extending this to other algebraic-geometric codes requires finding a similar identity in the function field setting. As noted by the first author [6], this can be achieved using Frobenius automorphisms σ in cyclic Galois extensions, and considering the residue of f^σ at a place of high degree in the function field. Using certain subfields of cyclotomic function fields, Guruswami [6] was able to extend the folded RS list decoding result of [7] and obtain folded algebraic-geometric codes of rate R list decodable up to error fraction $1-R-\varepsilon$ over an alphabet size $(\log N)^{O(1/\varepsilon^2)}$. In other words, the alphabet size was reduced to poly-logarithmic in the block length N of the code.

1.1 Our result

The main result in this work is a construction of folded algebraic-geometric codes which brings down the alphabet size to a *constant* depending only on ε. This is based on algebraic function fields constructed via class field theory, utilizing Drinfeld modules of rank 1.

Theorem 1.1 (Main). *Let ℓ be a square prime power and let $q = \ell^2$. For every $R \in (0,1)$, there is an infinite family of $\mathbb{F}_q$-linear algebraic-geometric codes of rate at least R which has relative distance at least $1 - R - 2/(\sqrt{\ell} - 1)$.*

For every pair of integers $m \geqslant s \geqslant 1$, the m-folded version of these codes (which is a code over alphabet $\mathbb{F}_q^m$) can be list decoded from an error fraction

$$\tau = \frac{s}{s+1}\left(1 - \frac{m}{m-s+1}\left(R + \frac{2}{\sqrt{\ell}-1}\right)\right) ,$$

outputting a subspace over $\mathbb{F}_q$ with at most $O(N^{(\sqrt{\ell}-1)s})$ elements that includes all message functions whose encoding is within Hamming distance τN from the input. (Here N denotes the block length of the code.)

Given a polynomial amount of pre-processed information about the code, the algorithm essentially consists of solving two linear systems over $\mathbb{F}_q$, and thus runs in deterministic polynomial time.

Picking suitable parameters in the above theorem, specifically $\ell \approx 1/\varepsilon^2$, $s \approx 1/\varepsilon$, and $m \approx 1/\varepsilon^2$, leads to folded AG codes with alphabet size $(1/\varepsilon)^{O(1/\varepsilon^2)}$ of any desired rate $R \in (0,1)$ that are list decodable up to error fraction $1-R-\varepsilon$ with a maximum output list size bounded by $N^{O(1/\varepsilon^2)}$. In other words, the polylogarithmic alphabet size of cyclotomic function fields is further improved to a constant depending only on ε.

We prove the above theorem by employing the recently developed *linear-algebraic* approach to list decoding, which was first used to an alternate, simpler proof of the list decodability of folded RS codes up to error fractions approaching $1-R$ (see [8]).

One of the simple but key observations that led to this work is the following. In order to apply the linear algebraic list decoder for a folded version of AG codes (such as the cyclotomic function field based codes of [6]), one can use the Frobenius automorphism based argument to just combinatorially *bound* the list size, but such an automorphism is *not* needed in the actual decoding algorithm. In particular, we *don't* need to find high degree places with a specific Galois group element as its Frobenius automorphism (this was one of the several challenges in the cyclotomic function field based construction [6]), but only need the *existence* of such places. This allows us to devise a linear-algebraic list decoder for folded versions of a family of AG codes, once we are able to construct function fields with certain stipulated properties (such as many rational places compared to the genus, and the existence of an automorphism which powers the residue of functions modulo some places). We then construct function fields with these properties over a fixed alphabet using class field theory, which is our main technical contribution.

This gives the first construction of folded AG codes over constant-sized alphabets list decodable up to the optimal $1 - R$ bound, although we are not able to efficiently construct the (natural) representation of the code that is utilized by our polynomial time decoding algorithm. This representation consists of the evaluations of regular functions at the rational places used for encoding (by a regular function at a place, we mean a function having no pole at this place); see Section 4.1 for a precise description.

In our previous works [9, 10], we considered list decoding of folded AG codes and a variant where rational points over a subfield are used for encoding. We were able to show that a *subcode* of these codes can be efficiently list decoded up to the optimal $1 - R - \varepsilon$ error fraction. The subcode is picked based on variants of subspace-evasive sets (subsets of the message space that have small intersection with low-dimensional subspaces) or subspace designs (which are a collection of subspaces with small total intersection with any low-dimensional subspace). In contrast, in this work we are able to list decode the folded AG codes *themselves*, and no pseudorandomly constructed subcode is needed. Further, our methods to construct function fields with the needed properties might be of independent algebraic interest.

1.2 Techniques

Our main techniques can be summarized as follows.

Our principal algebraic construction is that of an infinite family of function fields over a fixed base field $\mathbb{F}_q$ with many rational places compared to their genus, together with certain additional properties needed for decoding. Our starting point is a family of function fields $E/\mathbb{F}_\ell$ (where $\ell = \sqrt{q}$) such as those from the Garcia-Stichtenoth towers [4, 5] which attain the Drinfeld-Vlădut bound (the best possible trade-off between number of rational places and genus). We consider the constant field extension $L = \mathbb{F}_q \cdot E$, and take its narrow ray class field of with respect to some high degree place. We descend to a carefully constructed subfield F of this class field in which the $\mathbb{F}_q$-rational places in L split completely, and further the extension F/L has a cyclic Galois group.

A generator σ of this cyclic group $\text{Gal}(F/L)$, which is an automorphism of F of high order, is used to order the evaluation points in the AG code and then to fold this code. This last part is similar to the earlier cyclotomic construction, but there the full extension $F/\mathbb{F}_q(X)$ was cyclic. This was a stringent constraint that in particular ruled out asymptotically good function fields — in fact even abelian extensions must have the ratio of the number of rational places to genus tend to 0 when the genus grows [2]. In our construction, only the portion F/L needs to be cyclic, and this is another insight that we exploit.

Next, using the Chebotarev density theorem, we argue the existence of many large degree places which are inert in the extension F/L and have σ as their Frobenius automorphism. This suffices to argue that the list size is small using previous algebraic techniques. Essentially the values of the candidate message functions at the inert places mentioned above can be found by finding the roots of a univariate polynomial over the residue field, and these values can be combined via Chinese remaindering to identify the message function.

Under the linear-algebraic approach, the above list will in fact be a subspace. Thus knowing that this subspace has only polynomially many elements is enough to list all elements in the subspace in polynomial time by solving a linear system! To solve the linear system, we make use of the local power series expansion of a basis of the Riemann-Roch message space at certain rational places of F.

To summarize, some of the novel aspects of this work are:

1. Decoupling the *proof* of the combinatorial bound on list size from the algorithmic task of *computing* the list. This computational part is tackled by a linear-algebraic decoding algorithm whose efficiency automatically follows from the list size bound.
2. The use of the Chebotarev density theorem to combinatorially bound the list size.
3. The use of class fields based on rank one Drinfeld modules to construct function fields $F/\mathbb{F}_q$ with many $\mathbb{F}_q$-rational places compared to its genus, *and* which have a subfield L such that F/L is a cyclic Galois extension of sufficiently high degree.

1.3 Organization

In Section 2, we show a construction of folded algebraic-geometric codes over arbitrary function fields with many rational places and an automorphism of relatively large order. Then we present a linear-algebraic list decoding of the folded codes. At the end of Section 2, folded Reed-Solomon and cyclotomic codes are used to illustrate our general construction. Section 3 is devoted to discussion of folded algebraic geometric codes based on the function fields which are cyclic extensions of the well-known Garcia-Stichtenoth tower. In Section 4, we discuss the encoding and decoding of our folded codes through local expansion of the candidate functions at a point. The main result of this paper is then stated after discussion of encoding and decoding. In Appendix A, we present and prove the properties of our main algebraic construction, namely cyclic extensions of the Garcia-Stichtenoth tower via class field theory or Drinfeld modules of rank one. A possible approach of finding explicit equations of the base function field used for construction of our folded algebraic geometric codes is discussed in Appendix B.

2 Linear-Algebraic List Decoding of Folded AG Codes

In this section, we first present a construction of folded algebraic geometric codes over arbitrary function fields with certain properties and then give a deterministic list decoding of folded algebraic geometric codes over certain function fields satisfying some conditions.

2.1 Preliminaries on Function Fields

For convenience of the reader, we start with some background on global function fields over finite fields.

For a prime power q, let $\mathbb{F}_q$ be the finite field of q elements. An algebraic function field over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that F is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. The field $\mathbb{F}_q$ is called the full constant field of F if the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself. Such a function field is also called a global function field. From now on, we always denote by $F/\mathbb{F}_q$ a function field F with the full constant field $\mathbb{F}_q$.

Let $\mathbb{P}_F$ denote the set of places of F. The divisor group, denoted by $\mathrm{Div}(F)$, is the free abelian group generated by all places in $\mathbb{P}_F$. An element $G = \sum_{P\in\mathbb{P}_F} n_P P$ of $\mathrm{Div}(F)$ is called a divisor of F, where $n_P = 0$ for almost all $P \in \mathbb{P}_F$. The support, denoted by $\mathrm{Supp}(G)$, of G is the set $\{P \in \mathbb{P}_F : \ n_P \neq 0\}$. For a nonzero function $z \in F$, the principal divisor of z is defined to be $\mathrm{div}(z) = \sum_{P\in\mathbb{P}_F} \nu_P(z)P$, where ν_P denotes the normalized discrete valuation at P. The zero and pole divisors of z are defined to be $\mathrm{div}(z)_0 = \sum_{\nu_P(z)>0} \nu_P(z)P$ and $\mathrm{div}(z)_\infty = -\sum_{\nu_P(z)<0} \nu_P(z)P$, respectively.

For a divisor G of F, we define the Riemann-Roch space associated with G by

$$\mathcal{L}(G) := \{f \in F^* : \ \mathrm{div}(f) + G \geqslant 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite dimensional space over $\mathbb{F}_q$ and its dimension $\ell(G)$ is determined by the Riemann-Roch theorem which gives $\ell(G) = \deg(G)+1-g+\ell(W-G)$, where g is the genus of F and W is a canonical divisor of degree $2g-2$. Therefore, we always have that $\ell(G) \geqslant \deg(G)+1-g$ and the equality holds if $\deg(G) \geqslant 2g-1$.

For a place P, let O_P denote the integral ring at P, i.e., $O_P := \{z \in F : \ \nu_P(x) \geqslant 0\}$. Then the residue ring O_P/P is actually a finite extension of $\mathbb{F}_q$. It is called the residue field of P and denoted by F_P. The degree of P is defined to be the extension degree $[F_P : \mathbb{F}_q]$. For a function f and a place $P \in \mathbb{P}_F$ with $\nu_P(f) \geqslant 0$, we denote by $f(P)$ the residue class of f in the residue class field F_P at P.

For an automorphism $\phi \in \mathrm{Aut}(F/\mathbb{F}_q)$ and a place P, we denote by P^ϕ the place $\{\phi(x) : x \in P\}$. For a function $f \in F$, we denote by f^ϕ the action of ϕ on f. If $\nu_P(f) \geqslant 0$ and $\nu_{P^\phi}(f) \geqslant 0$, then one has that $\nu_P(f^{\phi^{-1}}) \geqslant 0$ and $f(P^\phi) = f^{\phi^{-1}}(P)$. Furthermore, for a divisor $G = \sum_{P\in\mathbb{P}_F} m_P P$ we denote by G^ϕ the divisor $\sum_{P\in\mathbb{P}_F} m_P P^\phi$.

2.2 Folded Algebraic Geometric Codes

Let F be a a global function field F with the full constant field $\mathbb{F}_q$. Fix an automorphism $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ such that F has mN distinct rational places $P_1, P_1^\sigma, \dots, P_1^{\sigma^{m-1}}, P_2, P_2^\sigma, \dots, P_2^{\sigma^{m-1}}, \dots, P_N, P_N^\sigma, \dots, P_N^{\sigma^{m-1}}$. We also choose a divisor D of degree e such that D is fixed under σ, i.e., $D^\sigma = D$; and $P_i^{\sigma^j} \notin \mathrm{Supp}(D)$ for all $1 \leqslant i \leqslant N$ and $0 \leqslant j \leqslant m-1$.

A folded algebraic geometric code can be defined as follows.

Definition 1 (Folded AG codes)**.** The folded code from F with parameters N, l, q, e, m, denoted by $\mathsf{F}(N, l, q, e, m)$, encodes a message function $f \in \mathcal{L}(lD)$ as

$$\pi: \quad f \mapsto \left(\begin{bmatrix} f(P_1) \\ f(P_1^\sigma) \\ \vdots \\ f(P_1^{\sigma^{m-1}}) \end{bmatrix}, \begin{bmatrix} f(P_2) \\ f(P_2^\sigma) \\ \vdots \\ f(P_2^{\sigma^{m-1}}) \end{bmatrix}, \dots, \begin{bmatrix} f(P_N) \\ f(P_N^\sigma) \\ \vdots \\ f(P_N^{\sigma^{m-1}}) \end{bmatrix} \right) \in \left(\mathbb{F}_q^m\right)^N . \tag{1}$$

Note that the folded code $\mathsf{F}(N, l, q, e, m)$ has the alphabet $\mathbb{F}_q^m$ and it is $\mathbb{F}_q$-linear. Furthermore, $\mathsf{F}(N, l, q, e, m)$ has the following parameters.

Lemma 2.1. *If $le < mN$, then the above code $\mathsf{F}(N, l, q, e, m)$ is an $\mathbb{F}_q$-linear code with alphabet size q^m, rate at least $\frac{le-g+1}{Nm}$, and minimum distance at least $N - \frac{le}{m}$.*

Proof. It is clear that the map π in (1) is $\mathbb{F}_q$-linear and the kernel of π is $\mathcal{L}\Big(lD - \sum_{i=1}^{N}\sum_{j=0}^{m-1} P_i^{\sigma^j}\Big)$ which is $\{0\}$ under the condition that $le < mN$. Thus, π is injective. Hence, the rate is at least $\frac{le-g+1}{Nm}$ by the Riemann-Roch theorem. To see the minimum distance, let f be a nonzero function in $\mathcal{L}(lD)$ and assume that I is the support of $\pi(f)$. Then the Hamming weight $\mathrm{wt}_H(\pi(f))$ of $\pi(f)$ is $|I|$ and $f \in \mathcal{L}\left(lD - \sum_{i \notin I}\sum_{j=0}^{m-1} P_i^{\sigma^j}\right)$. Thus, $0 \leqslant \deg\left(lD - \sum_{i \notin I}\sum_{j=0}^{m-1} P_i^{\sigma^j}\right) = le - m(N - |I|)$, i.e., $\mathrm{wt}_H(\pi(f)) = |I| \geqslant N - \frac{le}{m}$. This completes the proof. □

2.3 List Decoding of Folded Algebraic Geometric Codes

Suppose a codeword (1) encoded from $f \in \mathcal{L}(lD)$ was transmitted and received as

$$\mathbf{y} = \begin{pmatrix} y_{1,1} & y_{2,1} & & y_{N,1} \\ y_{1,2} & y_{2,2} & & \vdots \\ & & \ddots & \\ y_{1,m} & \cdots & & y_{N,m} \end{pmatrix}, \tag{2}$$

where some columns are erroneous. Let $s \geqslant 1$ be an integer parameter associated with the decoder.

Lemma 2.2. *Given a received word as in* (2)*, we can find a nonzero linear polynomial in* $F[Y_1, Y_2, \ldots, Y_s]$ *of the form* $Q(Y_1, Y_2, \ldots, Y_s) = A_0 + A_1Y_1 + A_2Y_2 + \cdots + A_sY_s$ *satisfying*

$$Q(y_{i,j+1}, y_{i,j+2}, \cdots, y_{i,j+s}) = A_0(P_i^{\sigma^j}) + A_1(P_i^{\sigma^j})y_{i,j+1} + \cdots + A_s(P_i^{\sigma^j})y_{i,j+s} = 0 \tag{3}$$

for $i = 1, 2, \ldots, N$ *and* $j = 0, 1, \ldots, m-s$. *The coefficients* A_i *of* Q *satisfy* $A_i \in \mathcal{L}(\kappa D)$ *for* $i = 1, 2, \ldots, s$ *and* $A_0 \in \mathcal{L}((\kappa + l)D)$ *for a "degree" parameter* d *chosen as*

$$\kappa = \left\lfloor \frac{N(m-s+1) - el + (s+1)(g-1) + 1}{e(s+1)} \right\rfloor. \tag{4}$$

Proof. Let u and v be dimensions of $\mathcal{L}(\kappa D)$ and $\mathcal{L}((\kappa+l)D)$, respectively. Let $\{x_1, \ldots, x_u\}$ be an $\mathbb{F}_q$-basis of $\mathcal{L}(\kappa D)$ and extend it to an $\mathbb{F}_q$-basis $\{x_1, \ldots, x_v\}$ of $\mathcal{L}((d+l)D)$. Then A_i is an $\mathbb{F}_q$-linear combination of $\{x_1, \ldots, x_u\}$ for $i = 1, 2, \ldots, s$ and A_0 is an $\mathbb{F}_q$-linear combination of $\{x_1, \ldots, x_v\}$. Determining the functions A_i is equivalent to determining the coefficients in the combinations of A_i. Thus, there are totally $su + v$ freedoms to determine $A_0, A_1, \ldots, A_s$. By the Riemann-Roch theorem, the number of freedoms is at least $s(\kappa e - g + 1) + (\kappa + l)e - g + 1$.

On the other hand, there are totally $N(m - s + 1)$ equations in (3). Thus, there must be one nonzero solution by the condition (4), i.e., $Q(Y_1, Y_2, \ldots, Y_s)$ is a nonzero polynomial. □

Lemma 2.3. *If* f *is a function in* $\mathcal{L}(lD)$ *whose encoding* (1) *agrees with the received word* $\mathbf{y}$ *in at least* t *columns with* $t > \frac{(\kappa+l)e}{m-s+1}$*, then* $Q(f, f^{\sigma^{-1}}, \ldots, f^{\sigma^{-(s-1)}})$ *is the zero function, i.e.,*

$$A_0 + A_1f + A_2f^{\sigma^{-1}} + \cdots + A_sf^{\sigma^{-(s-1)}} = 0. \tag{5}$$

Proof. Since $D = D^{\sigma}$, we have $f^{\sigma^i} \in \mathcal{L}(lD)$ for all $i \in \mathbb{Z}$. Thus, it is clear that $Q(f, f^{\sigma^{-1}}, \ldots, f^{\sigma^{-(s-1)}})$ is a function in $\mathcal{L}((\kappa + l)D)$.

Let us assume that $I \subseteq \{1, 2, \ldots, N\}$ is the index set such that the ith columns of $\mathbf{y}$ and $\pi(f)$ agree if and only if $i \in I$. Then we have $|I| \geqslant t$. For every $i \in I$ and $0 \leqslant j \leqslant m - s$, we have by (3)

$$\begin{aligned} 0 &= A_0(P_i^{\sigma^j}) + A_1(P_i^{\sigma^j})y_{i,j+1} + A_2(P_i^{\sigma^j})y_{i,j+2} + \cdots + A_s(P_i^{\sigma^j})y_{i,j+s} \\ &= A_0(P_i^{\sigma^j}) + A_1(P_i^{\sigma^j})f(P_i^{\sigma^j}) + A_2(P_i^{\sigma^j})f(P_i^{\sigma^{j+1}})) + \cdots + A_s(P_i^{\sigma^j})f(P_i^{\sigma^{j+s-1}}) \\ &= A_0(P_i^{\sigma^j}) + A_1(P_i^{\sigma^j})f(P_i^{\sigma^j}) + A_2(P_i^{\sigma^j})f^{\sigma^{-1}}(P_i^{\sigma^j}) + \cdots + A_s(P_i^{\sigma^j})f^{\sigma^{-s+1}}(P_i^{\sigma^j}) \\ &= \left(A_0 + A_1 f + A_2 f^{\sigma^{-1}} + \cdots + A_s f^{\sigma^{-s+1}}\right)(P_i^{\sigma^j}), \end{aligned}$$

i.e., $P_i^{\sigma^j}$ is a zero of $Q(f, f^{\sigma}, \ldots, f^{\sigma^{s-1}})$. Hence, $Q(f, f^{\sigma^{-1}}, \ldots, f^{\sigma^{-(s-1)}})$ is a function in $\mathcal{L}\left((\kappa + l)D - \sum_{i \in I} \sum_{j=0}^{m-s} P_i^{\sigma^j}\right)$. Our desired result follows from the fact that $\deg\left((\kappa + l)D - \sum_{i \in I} \sum_{j=0}^{m-s} P_i^{\sigma^j}\right) < 0$. □

We first look at the fraction of errors that we can correct from the above list decoding. By taking $t = 1 + \left\lfloor \frac{(\kappa+l)e}{m-s+1} \right\rfloor$ and combining Lemmas 2.3 and 2.2, we conclude the fraction of errors $\tau = 1 - t/N$ satisfies

$$\tau \approx \frac{s}{s+1} - \frac{s}{s+1} \times \frac{m}{m-s+1} \times \frac{k+g}{mN}, \tag{6}$$

where k is the dimension of $\mathcal{L}(lD)$ which is at least $le - g + 1$.

Next we consider the list size. By Lemma 2.3, we know that all candidate functions f in our list must satisfy the equation (5). In other words, we have to study the solution set of the equation (5). In our previous work [9], to upper bound the list size, we analyzed the solutions of the equation (5) by considering local expansions at a certain point. This local expansion method only guarantees a structured list of exponential size. Through precoding by using the structure in the list, we were able to obtain a Monte Carlo construction of subcodes of these codes with polynomial time list decoding. In this paper, we will employ the method used in [7, 6] for list decoding the Reed-Solomon codes and cyclotomic codes to bound the list size. The key part of this method is based on the following result.

Lemma 2.4. *Let $u \geqslant 1$ be an integer. If there is a place P of F with $\deg(P) > le$ such that $z^{\sigma^{-1}}(P) = z^{q^u}(P)$ for all $z \in O_P$, then the solution set of the equation (5) has size at most $q^{u(s-1)}$.*

As Lemma 2.4 is a special case of Lemma 3.2, we refer to the proof of Lemma 3.2.

Lemma 2.4 shows that, to get a small list, it is essential to find a place P of large degree such that $z^{\sigma^{-1}}(P) = z^{q^u}(P)$ for all $z \in O_P$ and a small $u \geqslant 1$. It is fortunate that the Chebotarev Density Theorem (see Theorem A.7) guarantees existence of such a place. Instead of presenting a result on existence of such a place P for arbitrary function field, we will show existence of such a place P for some specific function fields in this and the next sections. The other crucial point that we should keep in mind is that we do not have to use Lemma 2.4 for our decoding as we have an efficient linear-algebraic method to find the list that does not depend on the knowledge of P (see Section 4). Lemma 2.4 is only used to upper bound the list size via the *existence* of such a place P.

In some scenarios, we may not be able to find a single such place P. However, if we are allowed to relax the condition in Lemma 2.4 by using a set of places instead of just one place, we can also upper bound the list size (see Lemma 3.2).

In the next subsection, we use the example of Reed-Solomon and cyclotomic codes considered in [7, 6] to illustrate the above theory.

2.4 Folded Reed-Solomon and Cyclotomic Codes

Folded Reed-Solomon codes. Let us revisit the construction of folded Reed-Solomon codes from [7, 8]. We discuss the construction under the general framework of our folded algebraic geometric codes defined in Subsection 2.2.

Let $F = \mathbb{F}_q(x)$ be the rational function field and let γ be a primitive element of $\mathbb{F}_q$. Consider the automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_q(x)/\mathbb{F}_q)$ sending x to $\gamma^{-1}x$. Let P_i be the zero of $x - \gamma^{m(i-1)}$ for $i = 1, 2, \dots, N$, where $N \leqslant (q-1)/m$. Then $P_i^{\sigma^j}$ is the zero of $x - \gamma^{m(i-1)+j}$ for all $0 \leqslant j \leqslant m-1$. If we take D to be the pole of x, then $\mathcal{L}(kD) = \{f(x) \in \mathbb{F}_q[x] : \deg(f(x)) \leqslant k-1\}$, and our folded algebraic geometric code $\mathsf{F}(N, k, q, 1, m)$ defined in (1) coincides with the folded Reed-Solomon codes defined in [7].

By taking $m \approx 1/\varepsilon^2$ and $s \approx 1/\varepsilon$, the decoding radius given by (6) becomes $\tau \approx 1 - R - \varepsilon$, where $R = k/(mN)$ is the rate of the code (note that the genus g is 0 in the case of rational function field). However, the code alphabet size q (before folding) is about N/ε^2 in this case.

Let P be the place of F corresponding to $x^{q-1} - \gamma$. Then we have $\gamma x \equiv x^q \mod P$, i.e., $x^{\sigma^{-1}} = \gamma x \equiv x^q \mod P$. Thus, one has $z^{\sigma^{-1}}(P) = z^q(P)$ for all $z \in O_P$. By applying Lemma 2.4 (note that the condition that $q - 1 = \deg(P) > le = k + 1$ is satisfied), we conclude that the list size for decoding these folded Reed-Solomon codes is at most q^{s-1}.

Folded cyclotomic codes. Next we consider the cyclotomic codes discussed in [6]. We refer to the paper [6] without detailed explanation on cyclotomic function fields. Let $F/\mathbb{F}_q(x)$ be the subfield of a cyclotomic function field constructed in [6], where $q = \ell^2$ for a prime power ℓ. Then $F/\mathbb{F}_q(x)$ is a cyclic extension of degree $n = (\ell^d + 1)/(\ell + 1)$ for some parameter d. Let σ be a generator of the cyclic group $\mathrm{Gal}(F/\mathbb{F}_q(x))$. Then for each $\alpha \in \mathbb{F}_\ell$, there are n rational places of F lying over $x - \alpha$ that can be written as $P, P^{\sigma}, \dots, P^{\sigma^{n-1}}$. Thus, there are at least ℓn rational places and they can be arranged in the following way: $P_1, P_1^{\sigma}, \dots, P_1^{\sigma^{m-1}}, \dots, P_N, P_N^{\sigma}, \dots, P_N^{\sigma^{m-1}}$, where m is a positive integer less than n and N satisfies $N = \ell\lfloor n/m \rfloor$. Choose D to be the unique ramified place of F (which has degree d) to form the Riemann-Roch space $\mathcal{L}(lD)$. Then our folded algebraic geometric code $\mathsf{F}(N, l, q, d, m)$ defined in (1) coincides with the folded cyclotomic codes defined in [6].

The genus of the cyclotomic field F is $g = 1 + (d - 2)(\ell^d + 1)/(2\ell + 2) - d/2$. By taking $m \approx 1/\varepsilon^2$, $s \approx 1/\varepsilon$, $d \approx \ell\varepsilon$. Then the decoding radius given by (6) becomes $\tau \approx 1 - R - \varepsilon$, where $R = (ln - g + 1)/N$ is the rate of the code. The code alphabet size q (before folding) is $O(\log N/\varepsilon)$ in this case. This already improves the code alphabet size of folded RS codes.

By the Chebotarev Density Theorem (see Theorem A.7), we know that there exists a place P of F such that P has degree ℓn and $z^{\sigma^{-1}}(P) = z^{q^\ell}(P)$ for all $z \in O_P$. By applying Lemma 2.4, we conclude that the list size for decoding these folded cyclotomic codes is at most $q^{\ell(s-1)} = O(N^{1/\varepsilon^2})$.

We note that in [6], the place P is identified using the precise knowledge of the splitting behavior of places in cyclotomic extensions, and this was needed for the efficiency of the algorithm. Here, on the other hand, we only require the *existence* of such P (which we can guarantee by invoking the Chebotarev density theorem) to bound the list size, and the linear-algebraic algorithm itself is oblivious of P. As mentioned earlier, the realization of this power offered by using a linear interpolation polynomial (instead of the higher degree interpolation polynomial Q adopted in [6]) is a simple but key insight in this work.

3 Folded AG Codes over Constant-Sized Alphabets

The main disadvantage of the folded Reed-Solomon and cyclotomic codes is that the code alphabet size has to grow to ∞ as the code length N tends to ∞. To solve this problem, one can imagine that function fields with many rational places should be employed. Lemma 2.4 requires that there be a place P of large degree in F such that σ^{-1} maps every z to z^{q^u} in the residie field F_P for a relatively small u. To achieve this, one can use the the Chebotarev Density Theorem as in the case of cyclotomic codes. One condition of applying the Chebotarev Density Theorem is to construct a function field $F/\mathbb{F}_q$ with many rational places and a cyclic extension F/L such that the extension degree $[F:L]$ is sufficiently large. However, the current available function fields such as the Garcia-Stichtenoth tower [4] do not provide such an example. After careful analysis, we realize that certain finite cyclic extension of the Garcia-Stichtenoth tower is exactly what we need. Such an example can be constructed though class field theory or Drinfeld module of rank one. We state the result below and leave the detailed proof to Appendix A.

Theorem 3.1. *Let ℓ be a square prime power and let $q=\ell^2$. Let $\{E/\mathbb{F}_\ell\}$ be the Garcia-Stichtenoth tower given in* [4]. *Denote by $n := N(E/\mathbb{F}_\ell)$ the number of $\mathbb{F}_\ell$-rational places of E. Put $r = 2\lceil n/(\sqrt{\ell}-1)\rceil + 1$ and $h = 3r$. Then there exists a family $\{F/\mathbb{F}_q\}$ of function fields indexed by n satisfying that for each $F/\mathbb{F}_q$ in this family, F/L is a cyclic extension of degree $e := (\ell^r+1)/(\ell+1)$ with $L = \mathbb{F}_q \cdot E$ and a set U of places of F such that*

(i) *$|U| \geqslant q^r$ and $\deg(P) = eh$ for all places P in U.*

(ii) *For every place P in U, we have $z^{\sigma^{-1}}(P) = z^{q^h}(P)$ for all $z \in O_P$, where σ is a generator of* $\mathrm{Gal}(F/L)$.

(iii) *Every rational place of E can be regarded as a rational place of L and there are e places of F lying over such a place. Furthermore* $\liminf N(F/\mathbb{F}_q)/g(F) \geqslant (\sqrt{\ell}-1)/2 = (q^{1/4}-1)/2$.

If we choose one place P from the set U in Theorem 3.1 and apply Lemma 2.4, we find that the condition $\deg(P) = eh > le$ is not satisfied since le can be as large as $N(F/\mathbb{F}_q) \approx ne$. The idea is to choose a subset T of U in Theorem 3.1 and consider the congruence equation $z^{\sigma^{-1}} \equiv z^{q^u} \mod P$ for every $P \in T$ and $z \in O_P$. Finally applying the Chinese Remainder Theorem gives a upper bound for list size.

Lemma 3.2. *Let T be a set of places of F such that $\sum_{P\in T}\deg(P) > le$. Let $u \geqslant 1$ be an integer. Assume that for every $P \in T$ and any $z \in O_P$, one has $z^{\sigma^{-1}}(P) = z^{q^u}(P)$, then the solution set of the equation* (5) *has size at most $q^{u(s-1)|T|}$.*

Proof. Consider the map $\psi:\ \mathcal{L}(lD) \to \prod_{P\in T} F_P$ by sending z to $\psi(z) = (z(P))_{P\in T}$. It is clear that ψ is $\mathbb{F}_q$-linear. Furthermore, ψ is injective. Indeed, if $\psi(y) = \psi(z)$ for some $y, z \in \mathcal{L}(lD)$, then $\psi(y-z) = 0$, i.e., $(y-z)(P) = 0$ for all $P \in T$. Hence, $y - z$ belongs to $\mathcal{L}(lD - \sum_{P\in T} P)$. So, we must have $y - z = 0$ since $\deg(lD - \sum_{P\in T} P) = le - \sum_{P\in T}\deg(P) < 0$.

Let W be the solution set of (5). Then for every $P \in T$ and $f \in W$, we have

$$\begin{aligned} 0 &= A_0(P) + A_1(P)f(P) + A_2(P)f^{\sigma^{-1}}(P) + \cdots + A_s(P)f^{\sigma^{-(s-1)}}(P) \\ &= A_0(R) + A_1(P)f(P) + A_2(P)f^{q^u}(P) + \cdots + A_s(P)f^{q^{u(s-1)}}(P) \in F_P. \end{aligned}$$

The above equation has at most $q^{u(s-1)}$ solutions in F_P. This implies that the set $W_P := \{f(P) : f \in W\} \subseteq F_P$ has size at most $q^{u(s-1)}$. Moreover, it is clear that $\psi(W) \subseteq \prod_{P\in T} W_P$. Thus, our desired result follows from $|W| = |\psi(W)| \leqslant \left|\prod_{P\in T} W_P\right| = \prod_{P\in T} |W_P| \leqslant q^{u(s-1)|T|}$. This completes the proof. □

We are now ready to state our main result on list decoding of folded algebraic geometric codes.

Theorem 3.3. *Let ℓ be a square prime power and let $q = \ell^2$. For every $R \in (0,1)$, there is an infinite family of folded codes given in* (1) *of rate at least R which has relative distance at least $1 - R - 2/(\sqrt{\ell} - 1)$.*

For every pair of integers $m \geqslant s \geqslant 1$, these codes can be list decoded from an error fraction

$$\tau = \frac{s}{s+1}\left(1 - \frac{m}{m-s+1}\left(R + \frac{2}{\sqrt{\ell}-1}\right)\right) ,$$

outputting a subspace over $\mathbb{F}_q$ with at most $O(N^{(\sqrt{\ell}-1)s})$ elements that includes all message functions whose encoding is within Hamming distance τN from the input. (Here N denotes the block length of the code.)

Proof. Let $\{F/\mathbb{F}_q\}$ be a family of function fields given in Theorem 3.1. Choose a rational place ∞ of E and regard it as a rational place of L. Define the divisor $D := l\sum_{P_\infty|\infty, P_\infty \in \mathbb{P}_F} P_\infty$. Then it is easy to see that $D^\sigma = D$. For every rational place R of E, there are exactly e rational places of F lying over R and they can be represented as $P, P^\sigma, \dots, P^{\sigma^{e-1}}$. By taking away those rational places lying over ∞, we have at least $e(n-1)$ rational places of F, where $n = N(E/\mathbb{F}_\ell)$. Thus, for an integer m with $1 \leqslant m < e$, we can label Nm distinct places $P_1, P_1^\sigma, \dots, P_1^{\sigma^{m-1}}, \dots, P_N, P_N^\sigma, \dots, P_N^{\sigma^{m-1}}$ of F such that none of them lies over ∞, as long as $N \leqslant (n-1)\lfloor \frac{e}{m} \rfloor = (N(E/\mathbb{F}_\ell) - 1)\lfloor \frac{e}{m} \rfloor$.

Consider the folded algebraic geometric code $\mathsf{F}(N, l, q, e, m)$ defined in Definition 1 with σ being a generator of $\mathrm{Gal}(F/L)$. We choose l to satisfy the condition $le < Nm$. Choose a subset T of U with $|T| = \lceil \sqrt{\ell} - 1 \rceil$. Then we have

$$\sum_{R\in T} \deg(R) \geqslant 3re(\sqrt{\ell}-1) \geqslant 6N(E/\mathbb{F}_\ell)e = 6mN(E/\mathbb{F}_\ell)\frac{e}{m} > Nm > le.$$

This implies that the condition in Lemma 3.2 is satisfied. Hence, the code $\mathsf{F}(N, l, q, e, m)$ is deterministically list decodable with list size at most $q^{3r(s-1)\lceil\sqrt{\ell}-1\rceil} = O(q^{sn})$. Note that the code length is N which is approximately $en/m = O(n\ell^{2n/(\sqrt{\ell}-1)}/\ell m)$. Thus, the list size is $O(N^{(\sqrt{\ell}-1)s})$.

The claimed error fraction follows from (6) and the fact that $g/Nm \to (\sqrt{\ell}-1)/2$. □

4 Encoding and Decoding

We have not considered encoding and decoding of the folded algebraic geometric codes constructed in Sections 2 and 3. This section is devoted to the computational aspects of encoding and decoding of our folded codes.

4.1 Encoding

Let us consider the folded algebraic geometric code given in the proof of Theorem 3.3, where the divisor D is $l\sum_{P_\infty|\infty, P_\infty\in\mathbb{P}_F} P_\infty$ and the Riemann-Roch space is $\mathcal{L}(lD)$. To encode, we assume that $le > 2g-1$ and there is an algorithm to find a basis $\{z_1, z_2, \dots, z_k\}$ of $\mathcal{L}(lD)$ with $k = le - g + 1$.

Furthermore, we assume that, for every point $P_i^{\sigma^j}$ and each function f with $\nu_{P_i^{\sigma^j}}(f) \geqslant 0$, there is an efficient algorithm to evaluate f at $P_i^{\sigma^j}$, i.e., find $f(P_i^{\sigma^j})$. For a function f and a rational place P with $\nu_{\mathsf{P}}(f) \geqslant 0$, the algorithm of evaluating f at P consists of

(i) Finding a local parameter t at P (recall that a function t is called a local parameter at P if $\nu_{\mathsf{P}}(t) = 1$).

(ii) Finding the unique element $\alpha \in \mathbb{F}_q$ such that $\nu_{\mathsf{P}}\left(\frac{f-\alpha}{t}\right) \geqslant 0$ (note that this unique element α is equal to $f(\mathsf{P})$).

4.2 Decoding

As we have seen, encoding is easy as long as we have an efficient algorithm to compute a basis of the Riemann-Roch space and evaluations at rational places. However, we need some further work for decoding.

The idea of decoding is to solve the equation (5) through local expansions at a point. Let us briefly introduce local expansions first. The reader may refer to [13, pages 5-6] for the detailed result on local expansions. Let $F/\mathbb{F}_q$ be a function field and let P be a rational place. For a nonzero function $f \in F$ with $\nu_{\mathsf{P}}(f) \geqslant v$, we have $\nu_{\mathsf{P}}\left(\frac{f}{t^v}\right) \geqslant 0$. Put $a_v = \left(\frac{f}{t^v}\right)(\mathsf{P})$, i.e., a_v is the value of the function f/t^v at P. Note that the function $f/t^v - a_v$ satisfies $\nu_{\mathsf{P}}\left(\frac{f}{t^v} - a_v\right) \geqslant 1$, hence we know that $\nu_{\mathsf{P}}\left(\frac{f-a_vt^v}{t^{v+1}}\right) \geqslant 0$. Put $a_{v+1} = \left(\frac{f-a_vt^v}{t^{v+1}}\right)(\mathsf{P})$. Then $\nu_{\mathsf{P}}(f - a_vt^v - a_{v+1}t^{v+1}) \geqslant v+2$.

Assume that we have obtained a sequence $\{a_r\}_{r=v}^m$ $(m > v)$ of elements of $\mathbb{F}_q$ such that $\nu_{\mathsf{P}}(f - \sum_{r=v}^k a_rt^r) \geqslant k+1$ for all $v \leqslant k \leqslant m$. Put $a_{m+1} = \left(\frac{f-\sum_{r=v}^m a_rt^r}{t^{m+1}}\right)(\mathsf{P})$. Then $\nu_{\mathsf{P}}(f - \sum_{r=v}^{m+1} a_rt^r) \geqslant m+2$. In this way we continue our construction of the a_r. Then we obtain an infinite sequence $\{a_r\}_{r=v}^\infty$ of elements of $\mathbb{F}_q$ such that $\nu_{\mathsf{P}}(f - \sum_{r=v}^m a_rt^r) \geqslant m+1$ for all $m \geqslant v$. We summarize the above construction in the formal expansion

$$f = \sum_{r=v}^{\infty} a_rt^r, \tag{7}$$

which is called the local expansion of f at P.

It is clear that local expansions of a function depend on choice of the local parameters t. Note that if a power series $\sum_{i=v}^\infty a_it^i$ satisfies $\nu_{\mathsf{P}}(f - \sum_{i=v}^m a_it^i) \geqslant m+1$ for all $m \geqslant v$, then it is a local expansion of f. The above procedure shows that finding a local expansion at a rational place is very efficient as long as the computation of evaluations of functions at this place is easy.

The following fact plays an important role in our decoding.

Lemma 4.1. *Let $F/\mathbb{F}_q$ be a function field and let $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ be an automorphism. Let $\mathsf{P}, \mathsf{P}^{\sigma^{-1}}$ be two distinct rational places. Assume that t is a common local parameter of P and P^σ,* *i.e.,* $\nu_{\mathsf{P}}(t) = \nu_{\mathsf{P}^\sigma}(t) = 1$ *such that* $t^\sigma = t$. *Suppose that* $f \in F$ *has a local expansion* $\sum_{i=0}^\infty a_i t^i$ *at* P^σ *for some* $a_i \in \mathbb{F}_q$, *then the local expansion of* $f^{\sigma^{-1}}$ *at* P *is* $\sum_{i=0}^\infty a_i t^i$.

Proof. By the definition of local expansion, we have $\nu_{\mathsf{P}^\sigma}\left(f - \sum_{i=0}^m a_i t^i\right) \geqslant m+1$ for all $m \geqslant 0$. This gives $\nu_{(\mathsf{P}^\sigma)^{\sigma^{-1}}}\left((f - \sum_{i=0}^m a_i t^i)^{\sigma^{-1}}\right) = \nu_{\mathsf{P}}\left(f^{\sigma^{-1}} - \sum_{i=0}^m a_i t^i\right) \geqslant m+1$ for all $m \geqslant 0$. The desired result follows. □

Now let F be the function field constructed in Theorem 3.1. Assume that $R \neq \infty$ is a rational place of E and $t \in E$ is a local parameter at R. Then R can be viewed as an $\mathbb{F}_q$-rational point of $L = \mathbb{F}_q \cdot E$. Moreover, R splits completely in F/L. We may assume that all rational places of F lying over R are $\mathsf{P}, \mathsf{P}^\sigma, \ldots, \mathsf{P}^{\sigma^{\mathsf{e}-1}}$, where σ is a generator of $\mathrm{Gal}(F/L)$. It is clear that t is a common local parameter of $\mathsf{P}, \mathsf{P}^\sigma, \ldots, \mathsf{P}^{\sigma^{\mathsf{e}-1}}$. Furthermore, we have $t^\sigma = t$ since $t \in E \subset L$.

To solve for the functions f that satisfy the algebraic equation (5), let us assume that $f = \sum_{i=1}^k f_i z_i$ for some $f_i \in \mathbb{F}_q$, where $k = le - g + 1$ is the dimension of $\mathcal{L}(lD)$. Solving for f in (5) is equivalent to finding $\{f_i\}_{i=1}^k$. Assume that the local expansion of z_i at $\mathsf{P}^{\sigma^{\mathsf{j}}}$ is given by $\sum_{h=0}^\infty \alpha_{ijh} t^h$. Then by Lemma 4.1, $z_i^{\sigma^{-j}}$ have the local expansion $\sum_{h=0}^\infty \alpha_{ijh} t^h$ at P. Thus, $f^{\sigma^{-j}}$ has the local expansion $\sum_{i=1}^k \sum_{h=0}^\infty \alpha_{ijh} t^h$ at P. Furthermore assume that A_i have local expansions $\sum_{j=0}^\infty a_{ij} t^j$ at P for $0 \leqslant i \leqslant s$. Substitute these local expansions in Equation (5), we obtain an equation

$$c_0(f_1, f_2, \ldots, f_k) + c_1(f_1, f_2, \ldots, f_k)t + \cdots + c_i(f_1, f_2, \ldots, f_k)t^i + \cdots = 0, \tag{8}$$

where $c_i(f_1, f_2, \ldots, f_k)$ is a linear combination of $f_1, f_2, \ldots, f_k$ for all $i \geqslant 0$. Thus, each of the coefficients of the above power series (8) must be zero. This produces infinitely many linear equations $c_i(f_1, f_2, \ldots, f_k) = 0$ for $i \geqslant 0$ in variables $f_1, f_2, \ldots, f_k$. This system of infinitely many linear equations is equivalent to the system

$$c_i(f_1, f_2, \ldots, f_k) = 0 \qquad \text{for } i = 0, 1, \ldots, le \tag{9}$$

due to the fact that $A_0 + A_1 f + \cdots + A_s f^{\sigma^{-(s-1)}} \in \mathcal{L}(lD)$ and the following simple claim.

Lemma 4.2. *If* x *is an element in* $\mathcal{L}(lD)$ *and has a local expansion* $\sum_{i=0}^\infty \lambda_i t^i$ *for some* $\lambda_i \in \mathbb{F}_q$, *then* x *is identical to* 0 *if* $\lambda_i = 0$ *for all* $i \leqslant le$.

Proof. By the local expansion of x at P, we know that x belongs to $\mathcal{L}(lD - (le+1)\mathsf{P})$. The desired result follows from the fact that $\deg(lD - (le+1)\mathsf{P}) = \mathsf{-1} < \mathsf{0}$. □

The equation system (9) has $le+1$ equations and contains $k = le - g + 1$ variables. Theorem 3.3 guarantees that this system has at most $O(N^{(\sqrt{\ell}-1)s})$ solutions.

Given the discussion of encoding and decoding, we rewrite Theorem 3.3 as the main result of this paper.

Theorem 4.3 (Main)**.** *For any small* $\varepsilon > 0$ *and a real* $0 < R < 1$, *one can construct a folded algebraic geometric code over alphabet size* $(1/\varepsilon)^{O(1/\varepsilon^2)}$ *with rate* R *and decoding radius* $\tau = 1 - R - \varepsilon$ *such that the length of the code tends to* ∞ *and is independent of* ε. *Moreover, the code is deterministically list decodable with a list size* $O(N^{1/\varepsilon^2})$.

Given a polynomial amount of pre-processed information about the code, the algorithm essentially consists of solving two linear systems over $\mathbb{F}_q$, *and thus runs in deterministic polynomial time.*

Proof. In Theorem 3.3, choose $s \approx 1/\varepsilon$ and $m \approx 1/\varepsilon^2$ and $q \approx 1/\varepsilon^4$, the error fraction τ given in Theorem 3.3 is $1 - R - \varepsilon$. The alphabet size of the folded code is q^m, which is $(1/\varepsilon)^{O(1/\varepsilon^2)}$ and the list size is $O(N^{(\sqrt{\ell}-1)s}) = O(N^{1/\varepsilon^2})$. □

References

[1] Virgile Ducet and Claus Fieker, *Computing equations of curves with many points*, (2012), preprint. 21

[2] Gerhard Frey, Marc Perret, and Henning Stichtenoth, *On the different of abelian extensions of global fields*, Coding theory and algebraic geometry, Lecture Notes in Mathematics, vol. 1518, Springer Berlin/Heidelberg, 1992, pp. 26–32. 3

[3] M. D. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin, 2008. 19

[4] Arnaldo Garcia and Henning Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound*, Inventiones Mathematicae **121** (1995), 211–222. 3, 9, 20

[5] ———, *On the asymptotic behavior of some towers of function fields over finite fields*, Journal of Number Theory **61** (1996), no. 2, 248–273. 3

[6] Venkatesan Guruswami, *Cyclotomic function fields, Artin-Frobenius automorphisms, and list error-correction with optimal rate*, Algebra and Number Theory **4** (2010), no. 4, 433–463. Extended abstract appeared in the Proceedings of the 41th ACM Symposium on Theory of Computing (STOC'09). 2, 7, 8, 9

[7] Venkatesan Guruswami and Atri Rudra, *Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy*, IEEE Transactions on Information Theory **54** (2008), no. 1, 135–150. Extended abstract appeared in the Proceedings of the 38th ACM Symposium on Theory of Computing (STOC'06). 1, 2, 7, 8

[8] Venkatesan Guruswami and Carol Wang, *Linear-algebraic list decoding for variants of Reed-Solomon codes*, Electronic Colloquium on Computational Complexity (ECCC) **19** (2012), 73, To appear in *IEEE Trans. Info. Theory.* 2, 8

[9] Venkatesan Guruswami and Chaoping Xing, *Folded codes from function field towers and improved optimal rate list decoding*, CoRR **abs/1204.4209** (2012), Extended abstract appeared in the Proceedings of the 44th ACM Symposium on Theory of Computing (STOC'12). 3, 7

[10] ———, *List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound*, Electronic Colloquium on Computational Complexity (ECCC) **19** (2012), 146, Extended abstract will appear in the Proceedings of the 45th ACM Symposium on Theory of Computing (STOC'13). 3

[11] Florian Hess, *Computing riemann-roch spaces in algebraic function felds and related topics*, J. Symbolic Computation **33** (2002), no. 4, 425–445. 20

[12] V. Kumar Murty and J. Scherk, *Effective versions of the chebotarev density theorem for function elds*, C. R. Acad. Sci. (Paris) **319** (1994), 523–528. 19

[13] Harald Niederreiter and Chaoping Xing, *Rational points on curves over finite fields–theory and applications*, Cambridge University Press, 2000. 11, 14, 15, 17

[14] W. Wesley Peterson, *Encoding and error-correction procedures for Bose-Chaudhuri codes*, IEEE Transactions on Information Theory **6** (1960), 459–470. 1

[15] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. 19

Appendix

A Proof of Theorem 3.1

In view of Theorem 3.3, it is essential to construct a family of function fields given in Theorem 3.1. In this section, we use class field theory and the Chebotarev Density Theorem to show the existence of such a family.

A.1 Narrow-ray class fields and Drinfeld module of rank one

Throughout this subsection, we fix a function field F over $\mathbb{F}_q$ and a rational place ∞. Denote by A the ring

$$A := \{x \in F : \ \nu_P(x) \geqslant 0 \text{ for all } P \neq \infty\}.$$

Let Fr and Prin denote the fractional ideal group and the principal ideal group of A, respectively. Then the fractional idea class group $\mathrm{Cl}(A) = \mathrm{Fr}/\mathrm{Prin}$ of A is actually isomorphic to the zero degree divisor class group of F.

Let $D = \sum_P \nu_P(D)P$ be a positive divisor of F with $\infty \notin \mathrm{supp(D)}$. For $x \in F^*$, $x \equiv 1 \pmod{D}$ means that x satisfies the following condition:

if $P \in \mathrm{supp}(D)$, then $\nu_P(x-1) \geqslant \nu_P(D)$.

Let Fr_D be the subgroup of Fr consisting of the fractional ideals of A that are relatively prime to D, that is,

$$\mathrm{Fr}_D = \{\Re \in \mathrm{Fr} : \nu_P(\Re) = 0 \text{ for all } P \in \mathrm{supp(D)}\}.$$

Define the subgroup Prin_D of Fr_D by

$$\mathrm{Prin}_D = \{xA : x \in F^*, \, x \equiv 1 \pmod{D}\}.$$

The factor group $\mathrm{Fr}_D/\mathrm{Prin}_D$ is called the ∞-ray class group modulo D. It is a finite group and denoted by $\mathrm{Cl}_D(A)$. If $D = 0$, then we obtain the fractional ideal class group $\mathrm{Cl}(A)$.

Choose a local parameter $t \in F$ at P, i.e., $\nu_P(t) = 1$. Then the ∞-adic completion $\mathbb{F}_\infty$ of F consists of all power series of the form $\sum_{i=v}^{\infty} a_i t^i$, where $v \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$ for all $i \geqslant v$. We can define a sign function sgn from $\mathbb{F}_\infty^*$ to $\mathbb{F}_q^*$ by sending $\sum_{i=v}^{\infty} a_i t^i$ to a_v if $a_v \neq 0$ (see [13, pages 50-51]). Define

$$\mathrm{Prin}_D^+ = \{xA : \ x \in F^*, \ \mathrm{sgn}(x) = 1, \, x \equiv 1 \pmod{D}\}.$$

Definition 2 (Narrow ray class group). *The factor group*

$$\mathrm{Cl}_D^+(A) = \mathrm{Fr}_D/\mathrm{Prin}_D^+$$

is called the narrow ray class group of A modulo D (with respect to the sgn). *When D is supported on a single place Q, i.e., $D = 1 \cdot Q$, we denote $\mathrm{Cl}_D(A)$ (resp. $\mathrm{Cl}_D^+(A)$) as simply $\mathrm{Cl}_Q(A)$ (resp. $\mathrm{Cl}_Q^+(A)$).*

We have the following result [13, Proposition 2.6.4] concerning narrow ray and ideal class groups.

Lemma A.1. (i) Prin_D^+ *is a subgroup of* $\mathrm{Prin}(D)$ *and* $\mathrm{Prin}_D/\mathrm{Prin}_D^+ \simeq \mathbb{F}_q^*$.

(ii) *We have the isomorphisms*

$$\mathrm{Cl}_D^+(A)/\mathbb{F}_q^* \backsimeq \mathrm{Cl}_D^+(A)/(\mathrm{Prin}_D/\mathrm{Prin}_D^+) \backsimeq \mathrm{Cl}_D(A).$$

(iii) *We have*

$$\mathrm{Cl}_D^+(A)/(A/\mathcal{D})^* \backsimeq \mathrm{Cl}(A),$$

where $\mathcal{D}$ is the ideal of A corresponding to the divisor D, i.e., $\mathcal{D} = \prod \wp^{n_P}$ if $D = \sum n_P P$ with $\wp$ being the prime ideal of A corresponding to the place P.

Let H_A denote the Hilbert class field of F with respect to the place ∞, i.e, H_A is the maximal abelian extension in a fixed algebraic closure of F such that ∞ splits completely. Then we have $\mathrm{Gal}(H_A/F) \backsimeq \mathrm{Cl}(A)$.

We will use the following result from class field theory (see [13, Sections 2.5-2.6]).

Proposition A.2. *Now let Q be a place of degree $d > 1$ in a function field $F/\mathbb{F}_q$. Then there exists an abelian extension F^Q of F (called a narrow ray class field) with the following properties:*

(i) $\mathrm{Gal}(F^Q/F) \simeq \mathrm{Cl}_Q^+(A)$ *and the extension degree of F^Q/F is $|\mathrm{Cl}_Q^+(A)| = (q^d-1)|\mathrm{Cl}(A)| = (q^d-1)h_F$, where $h_F := |\mathrm{Cl}(A)|$ is the zero degree divisor class number of F.*

(ii) The Hilbert class field H_A of F is a subfield of F^Q and the Galois group $\mathrm{Gal}(F^Q/H_A)$ *is isomorphic to $(A/\mathcal{Q})^* \backsimeq \mathbb{F}_{q^d}^*$, where $\mathcal{Q}$ is the ideal of A corresponding to the place Q.*

(iii) ∞ and Q are only ramified places in F^Q/F. The inertia group of Q in F^Q/F is $(A/\mathcal{Q})^*$ and the inertia group of ∞ is $\mathbb{F}_q^*$. In particular, the ramification index of Q is $e_Q = q^d - 1$ and the ramification index of ∞ is $q-1$. Furthermore, ∞ splits into rational places in F^Q.

(iv) In the Galois extension F^Q/F, the Frobenius automorphism of a place P that is different from ∞ and Q is P itself when P is viewed as an element in $\mathrm{Cl}_Q^+(A)$.

From the above, we can easily compute the genus of F^Q by the Hurwitz genus formula, i.e.,

$$2g(F^Q) - 2 = (2g(F)-2)h_F(q^d-1) + (q-2)h_F\frac{q^d-1}{q-1} + d(q^d-2)h_F\ .$$

Next, we give a more explicit description of the narrow ray class field F^Q in terms of a Drinfeld module of rank one.

Let p be the characteristic of $\mathbb{F}_q$ and let $\pi : c \mapsto c^p$ be the Frobenius endomorphism of H_A. Consider the left twisted polynomial ring $H_A[\pi]$ whose elements are polynomials in π with coefficients from H_A written on the left; but multiplication in $H_A[\pi]$ is twisted by the rule

$$\pi u = u^p \pi \qquad \text{for all } u \in H_A.$$

Let $\tilde{D} : H_A[\pi] \longrightarrow H_A$ be the map which assigns to each polynomial in $H_A[\pi]$ its constant term.

Definition 3. A Drinfeld A-module of rank 1 over H_A is a ring homomorphism $\phi : A \longrightarrow H_A[\pi]$, $a \mapsto \phi_a$, such that:

(i) not all elements of $H_A[\pi]$ in the image of ϕ are constant polynomials;

(ii) $\tilde{D} \circ \phi$ is the identity on A;

(iii) There exists a positive integer λ such that $\deg(\phi_a) = -\lambda\nu_\infty(a)$ for all nonzero $a \in A$, where $\deg(\phi_a)$ is the degree of ϕ_a as a polynomial in π.

Example A.3. Consider the rational function field $F = \mathbb{F}_q(T)$ with ∞ being the pole place of T. Then we have $A = \mathbb{F}_q[T]$ and $H_A = F = \mathbb{F}_q(T)$. A Drinfeld A-module ϕ of rank 1 over F is uniquely determined by the image ϕ_T of T. By Definition 3 we must have

$$\tilde{D}(\phi_T) = (\tilde{D} \circ \phi)(T) = T,$$

i.e., ϕ_T is a nonconstant polynomial in π with the constant term T. Since $\deg(\phi_T) = -\lambda\nu_\infty(T) = \lambda$, we know that ϕ_T is of the form $T + f(\pi)\pi + x\pi^\lambda$ for an element $x \in F^*$ and $f(\pi) \in F[\pi]$ with $\deg(f(\pi)) \leqslant \lambda - 2$. Taking $x = 1$ and $f(\pi) = 0$ gives the so-called Carlitz module, which yields the construction of cyclotomic function fields.

Definition 4. We fix a sign function sgn. We say that a Drinfeld A-module ϕ of rank 1 over H_A is sgn-normalized if $\mathrm{sgn}(a)$ is equal to the leading coefficient of ϕ_a for all $a \in A$. In particular, the leading coefficient of ϕ_a must belong to $\mathbb{F}_q^*$.

Definition 5 (Twisted polynomials corresponding to an ideal)**.** *Given a Drinfeld A-module ϕ of rank 1 over H_A and a prime ideal $\mathcal{Q}$ of A, let $I_{\mathcal{Q},\phi}$ be the left ideal generated in $H_A[\pi]$ by the twisted polynomials ϕ_a, $a \in \mathcal{Q}$. As left ideals are principal, $I_{\mathcal{Q},\phi} = H_A[\pi]\phi_{\mathcal{Q}}$ for a unique monic twisted polynomial $\phi_{\mathcal{Q}} \in H_A[\pi]$.*

Let K be any H_A-algebra. Then for a polynomial $f(\pi) = \sum_{i=0}^{k} b_i\pi^i \in H_A[\pi]$ the action of $f(\pi)$ on K is defined by

$$f(\pi)(t) = \sum_{i=0}^{k} b_i t^{p^i} \quad \text{for all } t \in K\ .$$

Let $\overline{H_A}$ denote a fixed algebraic closure of H_A whose additive group $(\overline{H_A}, +)$ is equipped with an A-module structure under the action of ϕ.

Definition 6. Let ϕ be a sgn-normalized Drinfeld A-module of rank 1 over H_A and $\mathcal{Q}$ be a nonzero ideal of A. The $\mathcal{Q}$-torsion module $\Lambda_\phi(\mathcal{Q})$ associated with ϕ is defined by

$$\Lambda_\phi(\mathcal{Q}) = \{t \in (\overline{H_A}, +) : \phi_{\mathcal{Q}}(t) = 0\}.$$

The following are a few basic facts about $\Lambda_\phi(\mathcal{Q})$:

(i) $\Lambda_\phi(\mathcal{Q})$ is a finite set of cardinality $|\Lambda_\phi(\mathcal{Q})| = p^{\deg(\phi_\mathcal{Q})}$;

(ii) $\Lambda_\phi(\mathcal{Q})$ is an A-submodule of $(\overline{H_A}, +)$ and a cyclic A-module isomorphic to $A/\mathcal{Q}$;

(iii) $\Lambda_\phi(\mathcal{Q})$ has $\Phi(\mathcal{Q}) := |(A/\mathcal{Q})^*|$ generators as a cyclic A-module, where $(A/\mathcal{Q})^*$ is the group of units of the ring $A/\mathcal{Q}$.

The elements of $\Lambda_\phi(\mathcal{Q})$ are also called the $\mathcal{Q}$- torsion elements in $(\overline{H_A}, +)$. The following gives an explicit description of narrow ray class fields in terms of extension fields obtained by adjoining these torsion elements.

Proposition A.4. *The extension field $H_A(\Lambda_\phi(\mathcal{Q}))$ obtained by adjoining these $\mathcal{Q}$-torsion elements to H_A is isomorphic to the narrow ray class field F^Q from Proposition* A.2*, where Q is the place corresponding to the ideal $\mathcal{Q}$.*

In the case where F is the rational function field and ϕ is the Carlitz module in Example A.3, the field F^Q is the cyclotomic function field over F with modulus $\mathcal{Q}$.

A.2 A family of function fields

In this subsection, we assume that ℓ is a prime power and $q = \ell^2$. The following is the key technical component of our construction of the function fields needed for our list-decodable code construction.

Lemma A.5. *Let $E/\mathbb{F}_\ell$ be a function field with at least one rational point ∞ and a place Q of degree r, where $r > 1$ is an odd integer. Then there exists a function field $F/\mathbb{F}_q$ such that*

(i) *$F/(\mathbb{F}_q \cdot E)$ is a cyclic abelian extension with $[F : \mathbb{F}_q \cdot E] = \frac{\ell^r+1}{\ell+1}$.*

(ii) *$N(F/\mathbb{F}_q) \geqslant \frac{\ell^r+1}{\ell+1} N(E/\mathbb{F}_\ell)$.*

(iii) *$g(F) \leqslant (g(E) - 1)\frac{\ell^r+1}{\ell+1} + \frac{r}{2}\left(\frac{\ell^r+1}{\ell+1} - 1\right) + 1$.*

Proof. Let us outline the idea behind the proof. First we choose a place Q of E of odd degree r and consider the constant extension $\mathbb{F}_q \cdot E$. Then Q remains a place of degree r in $\mathbb{F}_q \cdot E$ since r is odd (see [13, Theorem 1.5.2(iii)(a)]). We take the narrow ray class field of $\mathbb{F}_q \cdot E$ modulo Q and then descend to a subfield K which is the fixed field of a certain subgroup of the Galois group. This is done to ensure that the rational places of E which can be regarded as rational places of $\mathbb{F}_q \cdot E$ split completely in $K/\mathbb{F}_q \cdot E$ (note that K may not be a cyclic extension over $\mathbb{F}_q \cdot E$). To obtain a cyclic extension over $\mathbb{F}_q \cdot E$, we need to descend to a further subfield of K, which will be our claimed function field F. The reason why we use a place Q of odd degree is that, in the case of odd r, the narrow ray class group of $\mathbb{F}_q \cdot E$ modulo Q is a cyclic Galois extension over its Hilbert class field. In the end, we can construct our desired function field such that it is a cyclic extension over $\mathbb{F}_q \cdot E$.

Put $E_1 := E$ and consider the constant field extension $E_2 := \mathbb{F}_q \cdot E_1$. Then ∞ remains a rational place in E_2 and Q remains a place of degree r in E_2 as well.

Let A_i be the ring in E_i defined by

$$A_i := \{x \in E_i : \ \nu_P(x) \geqslant 0 \ \text{ for all } P \neq \infty\}$$

and let H_i be the Hilbert class field of A_i of E_i with respect to ∞. Consider the narrow-ray class field $E_i^Q = H_i(\Lambda_\phi(\mathcal{Q}))$ where $\mathcal{Q}$ is the ideal corresponding to place Q. Then we can identify $\mathrm{Gal}(E_i^Q/E_i)$ with $\mathrm{Cl}_Q^+(A_i)$.

Now let K be the subfield of the extension E_2^Q/E_2 fixed by the subgroup $G = \mathbb{F}_q^* \cdot \mathrm{Cl}_Q^+(A_1)$ of $\mathrm{Cl}_Q^+(A_2)$. We have

$$|G| = \frac{|\mathbb{F}_q^*| \cdot |\mathrm{Cl}_Q^+(A_1)|}{|\mathbb{F}_q^* \cap \mathrm{Cl}_Q^+(A_1)|} = \frac{(\ell^2-1)\cdot(\ell^r-1)h_{E_1}}{\ell-1} = (\ell+1)(\ell^r-1)h_{E_1}$$

and so

$$[K:E_2] = \frac{|\mathrm{Cl}_D^+(A_2)|}{|G|} = \frac{(q^r-1)h_{E_2}}{|G|} = \frac{\ell^r+1}{\ell+1} \times \frac{h_{E_2}}{h_{E_1}}. \tag{10}$$

Let P_∞ be a place of K lying over ∞. Then the inertia group of P_∞ in the extension E_2^Q/K is $\mathbb{F}_q^* \cap G$, and so the ramification index $e(P_\infty|\infty)$ of P_∞ over ∞ is given by

$$e(P_\infty|\infty) = \frac{|\mathbb{F}_q^*|}{|\mathbb{F}_q^* \cap G|} = \frac{|\mathbb{F}_q^* \cdot G|}{|G|} = \frac{|\mathbb{F}_q^* \cdot \mathrm{Cl}_Q^+(A)|}{|G|} = 1,$$

i.e., ∞ is unramified in K/E_2.

Let R be a place of K lying over Q. Since the inertia group of Q in E_2^Q/E_2 is $(A_2/\mathcal{Q})^*$ by the theory of narrow ray class fields, the inertia group of R in E_2^Q/K is $(A_2/\mathcal{Q})^* \cap G = \mathbb{F}_q^* \cdot (A/\mathcal{Q})^*$. Thus, the ramification index $e(R|Q)$ of R over Q is given by

$$e(R|Q) = \frac{|(A_2/\mathcal{Q})^*|}{|\mathbb{F}_q^* \cdot (A_1/\mathcal{Q})^*|} = \frac{|(A_2/\mathcal{Q})^*| \cdot |\mathbb{F}_q^* \cap (A_1/\mathcal{Q})^*|}{|\mathbb{F}_q^*| \cdot |(A_1/\mathcal{Q})^*|} = \frac{(q^r-1)(\ell-1)}{(q-1)(\ell^r-1)} = \frac{\ell^r+1}{\ell+1}. \tag{11}$$

Since ∞, Q are the only ramified places in E_2^Q/E_2, and ∞ is unramified in K/E_2, we conclude that the place Q is the only ramified place in K/E_2 with ramification index $(\ell^r+1)/(\ell+1)$.

Now, all $\mathbb{F}_\ell$-rational places of E_1 can be viewed as $\mathbb{F}_q$-rational places of E_2 and furthermore they split completely in K. This is because for a rational place P of E_1 with $P \neq \infty, Q$, from Proposition A.2 and our construction, it follows that the Frobenius automorphism of P is contained in the subgroup $\mathrm{Gal}(E_2^Q/K)$. Therefore, the Frobenius automorphism of P in the extension K/E_2 is the identity, and therefore P must split completely in K/E_2.

Since the decomposition group of Q in E_2^Q/E_2 is isomorphic to the cyclic group $(A/\mathcal{Q})^*$, the decomposition group of Q in K/E_2 is cyclic as well. The inertia group of Q, which is a subgroup of the decomposition group of Q, has order $\frac{\ell^r+1}{\ell+1}$ by (11). Thus, the Galois group $\mathrm{Gal}(K/E_2)$ contains a cyclic subgroup of order $\frac{\ell^r+1}{\ell+1}$. This implies that there exists a subfield F of K/E_2 such that $\mathrm{Gal}(F/E_2)$ is a cyclic group of order $\frac{\ell^r+1}{\ell+1}$. It is clear that all $\mathbb{F}_\ell$-rational places of E_1 split completely in F as well. Hence

$$N(F/\mathbb{F}_q) \geqslant [F:E_2]N(E_1/\mathbb{F}_\ell) = \frac{\ell^r+1}{\ell+1}N(E_1/\mathbb{F}_\ell)\ .$$

Moreover, the place Q is the only ramified place in F/E_2 (since it is the only ramified place in K/E_2) and it is tamely ramified with the ramification index at most $[F:E_2]$. Hence, we can apply the Hurwitz genus formula to the extension F/E_2 and get

$$2g(F) - 2 \leqslant (2g(E_2)-2)[F:E_2] + r([F:E_2]-1).$$

The desired result follows from the fact that $g(E_2) = g(E_1)$. □

The following theorem provides the family of function fields that we required to construct our folded algebraic geometric codes in Theorem 3.3.

Theorem A.6. *Let ℓ be a prime power and let $q = \ell^2$. Assume that there is a family $\{E/\mathbb{F}_\ell\}$ of function fields such that $g(E) \to \infty$ and $N(E/\mathbb{F}_\ell)/g(E) \to A$ for a positive real A. Then for any odd integer r with $r > \log(2 + 7g(E))/\log(\ell)$, there exists a function field $F/\mathbb{F}_q$ such that F is a finite extension of $\mathbb{F}_q \cdot E$ of degree $e := (\ell^r + 1)/(\ell + 1)$ and*

(i) *$g(F) \to \infty$ and $g(F) \leqslant (g(E) - 1)e + r(e - 1)/2 + 1$.*

(ii) *$N(F/\mathbb{F}_q) \geqslant eN(E/\mathbb{F}_\ell)$.*

(iii) *$F/(\mathbb{F}_q \cdot E)$ is a cyclic Galois extension of degree e.*

In particular, we have $\liminf_{g(F)\to\infty} N(F/\mathbb{F}_q)/g(F) \geqslant A/(1 + c)$ if $r/g(E) \to 2c$ for a constant $c \geqslant 0$.

Proof. The result follows directly from Lemma A.5 and the fact that there exists a place of degree r in E as long as $r > \log(2 + 7g(E))/\log(\ell)$ (see [15, Corollary 5.2.10]). This completes the proof. □

A.3 Chebotarev Density Theorem

Given Theorem A.6, to show that the family of function fields with property (P3) exists, it remains to find a large set S of places of $\mathbb{P}_F$ satisfying (P3)(ii). In order to accomplish this task, we need the explicit form of the Chebotarev Density Theorem.

For an automorphism $\phi \in \mathrm{Aut}(F/\mathbb{F}_q)$, it induces a canonical automorphism in $\mathrm{Aut}(F_P/\mathbb{F}_q)$, denoted by ϕ_P. If ϕ_P is the Frobenius of $\mathrm{Aut}(F_P/\mathbb{F}_q)$, i.e., $x^{\phi_P} = x^q \mod P$ for any $x \in O_P$, then ϕ is called a Frobenius automorphism of P.

If F/L is a Galois extension and $L/\mathbb{F}_q$ is a global function field, we consider the place Q of L lying under P. Then an automorphism $\phi \in \mathrm{Gal}(F/L)$ belongs to $\mathrm{Aut}(F/\mathbb{F}_q)$. Furthermore, ϕ induces a canonical automorphism in $\mathrm{Aut}(F_P/L_Q)$. If L_Q is isomorphic to $\mathbb{F}_{q^u}$ for some integer $u \geqslant 1$ and $z^\phi \equiv z^{q^u} \mod P$ for all $z \in_P$, then ϕ is called the Frobenius automorphism of F/L at P. In particular, in case F/L is abelian, a Frobenius automorphism is also called an Artin automorphism.

Let F/L be a Galois extension of degree e of function fields over $\mathbb{F}_q$. Assume that $\mathbb{F}_q$ is the full constant field of both F and L. Let t be a separating transcendence element over $\mathbb{F}_q$. Let $d = [L : \mathbb{F}_q(t)]$.

For a place P of F lying over Q of L, let $\left[\frac{F/L}{P}\right]$ be the Frobenius of P. Then for any $\phi \in \mathrm{Gal}(F/L)$, the Frobenius of P^ϕ is $\phi \left[\frac{F/L}{P}\right] \phi^{-1}$. Thus, the conjugacy class $\left\{\phi \left[\frac{F/L}{P}\right] \phi^{-1} : \phi \in \mathrm{Gal}(F/L)\right\}$ is determined by Q. We denote this conjugacy class by $\left[\frac{F/L}{Q}\right]$.

Fix a conjugacy class C of $\mathrm{Gal}(F/L)$, let $M_h(C)$ denote the number of places Q of degree h in L that are unramified in both F/L and $L/\mathbb{F}_q(t)$ such that $\left[\frac{F/L}{P}\right] = C$. Then we have the following result [3, Proposition 6.4.8] and [12].

Theorem A.7 (Chebotarev Density Theorem)**.** *One has*

$$\left| M_h(C) - \frac{|C|}{eh} q^h \right| \leqslant \frac{2|C|}{eh}(e + g_F)q^{h/2} + e(2g_L + 1)q^{h/4} + g_F + de, \tag{12}$$

where g_F and g_L denote the genera of F and L, respectively.

Finally, we are able to show existence of a family of function fields given in Theorem 3.1.

Proof of Theorem 3.1: Let $\{E/\mathbb{F}_\ell\}$ be the well-known Garcia-Stichtenoth tower [4] and put $L = \mathbb{F}_q \cdot E$. Then one has $N(E/\mathbb{F}_\ell)/g(E) \to \sqrt{\ell} - 1$ with $g(E) \to \infty$ and $[E : \mathbb{F}_\ell(t)] \leqslant g(E)$ for a separating transcendence element over $\mathbb{F}_\ell$. Thus, $d = [L : \mathbb{F}_q(t)] \leqslant g(E) = g(L)$. By our choice of parameters h, r, we find that

$$\frac{1}{eh} q^h - \left(\frac{2}{eh}(e + g_F)q^{h/2} + e(2g_L + 1)q^{h/4} + g_F + de \right) \geqslant q^r.$$

By Theorem A.7, there exists a set S of places of L with $|S| \geqslant q^r$ such that $\deg(R) = h$ and $\left[\frac{F/L}{R}\right] = \sigma^{-1}$ for every place R in S. Let P be a place of F lying over R. The Frobenius σ^{-1} of P belongs to $\mathrm{Gal}(F/Z)$, where Z is the decomposition field of P in F/L. Since the order of σ^{-1} is $e = [F : L]$, we must have $Z = L$ and hence the relative degree $f(P|R)$ is e. So P is the only place of F lying over R. Let U be the set of places lying over those in S.

Since $r/g(E) \to 2$, we have $\liminf N(F/\mathbb{F}_q)/g(F) \geqslant (\sqrt{\ell} - 1)/2$ by Theorem A.6.

B Computing A Basis of Riemann-Roch Space

Both encoding and decoding described in Section 4 depend on an algorithm to find a basis of the Riemann-Roch space $\mathcal{L}(lD)$. We divide this job into two steps. The first step is to find an explicit equation defining our function field F constructed earlier through class field method. The second step is to find a basis of our Riemann-Roch space based on the equation form Step 1.

In [11], a polynomial algorithm of finding a basis of a Riemann-Roch space is given based on an explicit equations of the associated function field. If F is of the form $\mathbb{F}_q(x, y)$ with a defining equation

$$y^h + a_1(x)y^{h-1} + \cdots + a_{h-1}(x)y + a_h(x) = 0 \tag{13}$$

with $a_i(x) \in \mathbb{F}_q[x]$, then [11] describes an algorithm with polynomial time in h, the divisor degree le and Δ, where Δ is the largest degree of $a_1(x), a_2(x), \ldots, a_h(x)$ in (13). Thus, if we can find an equation defining the field F with Δ being a polynomial in the code length N, then [11] provides an polynomial algorithm in the code length N to determine a basis of $\mathcal{L}(lD)$.

Thus, to get a polynomial time encoding and decoding for our folded algebraic code, it is sufficient to obtain polynomial time algorithms for

(i) finding a defining equation (13) of F such that Δ is a polynomial in code length N;

(ii) computing evaluations of functions at rational places.

Part (ii) is usually easier. The key part is to find a defining equation of the underlying function field. To see this, we start with the function field E defined by the Garcia-Stichtenoth tower. Then one has $[E : \mathbb{F}_\ell(x)] \leqslant N(E/\mathbb{F}_\ell)$. Moreover, $E/\mathbb{F}_\ell(x)$ is a separable extension, thus there exists $\beta \in E$ such that $E = \mathbb{F}_\ell(x, \beta)$. Consequently, we have $L = \mathbb{F}_q \cdot E = \mathbb{F}_q(x, \beta)$.

The paper [1] describes a method to find an element α of F such that $F = L(\alpha)$. Thus, $F = \mathbb{F}_q(x, \alpha, \beta)$. Now the problem is how to find an element $y \in F$ such that $F = \mathbb{F}_q(x, \alpha, \beta) = \mathbb{F}_q(x, y)$ with the defining equation given in (13) and the maximum degree Δ is a polynomial in N.

We summarize what we discussed above into an open problem.

Open Problem. *Find a polynomial time algorithm to construct an explicit equation* (13) *of the function field F given in Theorem* 3.1 *and compute a basis of the Riemann-Roch space efficiently.*

ECCC ISSN 1433-8092

http://eccc.hpi-web.de