# This document is downloaded from DR-NTU (https://dr.ntu.edu.sg) Nanyang Technological University, Singapore. 

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

Guruswami, Venkatesan; Xing, Chaoping

2014

Guruswami, V., \& Xing, C. (2014). Optimal rate list decoding of folded algebraic-geometric codes over constant-sized alphabets. Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, 1858-1866.
https://hdl.handle.net/10356/106724


#### Abstract

© 2014 Society for Industrial and Applied Mathematics. This paper was published in Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms and is made available as an electronic reprint (preprint) with permission of Society for Industrial and Applied Mathematics. The paper can be found at the following URL: [http://epubs.siam.org/doi/abs/10.1137/1.9781611973402.134]. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper is prohibited and is subject to penalties under law.


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

(Extended abstract)

Venkatesan Guruswami ${ }^{\dagger} \quad$ Chaoping Xing ${ }^{\ddagger}$


#### 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 constantsized 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 $(1 / \varepsilon)^{O\left(1 / \varepsilon^{2}\right)}$ that can be list decoded up to error fraction $1-R-\varepsilon$ confining close-by messages to a subspace with $N^{O\left(1 / \varepsilon^{2}\right)}$ 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 algebraicgeometric 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.

[^0]
## 1 Introduction

Reed-Solomon (RS) 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 [16], 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 $\varepsilon$. This error fraction is twice the classicial $(1-R) / 2$ bound, and further is optimal as the message has $R n$ 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 [8], was folded

Reed-Solomon codes. In the $m$-folded version of this code (where $m$ is a positive integer), the Reed-Solomon (RS) encoding $\left(f(1), f(\gamma), \cdots, f\left(\gamma^{n-1}\right)\right.$ ) 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 $\gamma$ 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 $\varepsilon$.

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 [8]. 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 $f(\gamma X) \equiv f(X)^{q}(\bmod E(X))$ 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 $\sigma$ in cyclic Galois extensions, and considering the residue of $f^{\sigma}$ 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 [8] and obtain folded algebraic-geometric codes of rate $R$ list decodable up to error fraction $1-R-\varepsilon$ over an alphabet size $(\log N)^{O\left(1 / \varepsilon^{2}\right)}$. 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 $\varepsilon$. This is based
on algebraic function fields constructed via class field theory, utilizing Drinfeld modules of rank 1.

Theorem 1.1 (Main) Let $\ell$ 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 $O\left(N^{(\sqrt{\ell}-1) s}\right)$ elements that includes all message functions whose encoding is within Hamming distance $\tau N$ 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 $(1 / \varepsilon)^{O\left(1 / \varepsilon^{2}\right)}$ 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 $N^{O\left(1 / \varepsilon^{2}\right)}$. In other words, the polylogarithmic alphabet size of cyclotomic function fields is improved to a constant depending only on $\varepsilon$.

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 [10]).

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 for a precise description.
Comparison to our previous works. In our previous works [11, 12], 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 can be picked in two ways: (i) based on variants of subspaceevasive sets (subsets of the message space that have small intersection with low-dimensional subspaces), yielding randomized constructions with list size a constant, or (ii) based on subspace designs (which are a collection of subspaces with small total intersection with any lowdimensional subspace), yielding constructions with list size say sub-logarithmic in the block length. (The necessary subspace designs were randomly constructed in [12], but a recent work [7] gives an explicit construction with only slightly worse parameters.)

The distinguishing aspect of this work is that we are able to list decode the folded AG codes themselves, and no pseudorandomly constructed subcode is needed. This has certain advantages as we mention now. Our folded AG codes can also be decoded in the stronger "list recovery" model where for each position the input is a set of symbols and one needs to list all codewords whose $i$ 'th symbol belongs to the $i$ 'th set for $\approx R$ fraction of the positions (with $R$ being the code rate). ${ }^{1}$ List recovery is an important primitive for decoding concatenated codes and was also the basis of the application of folded algebraic codes to lossless expanders in [9]. It is also possible that the folded AG codes might be useful to construct subspace codes using the methods of [7]. Finally, the algebraic techniques we use to construct appropriate function fields that enable our list decoding result might be of independent interest.

### 1.2 Summary of main techniques

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 de-

[^1]coding. Our starting point is a family of function fields $E / \mathbb{F}_{\ell}$ (where $\ell=\sqrt{q}$ ) such as those from the GarciaStichtenoth towers $[4,5]$ which attain the DrinfeldVlădut 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 $\sigma$ of this cyclic group $\operatorname{Gal}(F / L)$, 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 $\sigma$ 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 linearalgebraic 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.

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.

## 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 $\operatorname{Div}(F)$, 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 $\operatorname{Div}(F)$ is called a divisor of $F$, where $n_{P}=0$ for almost all $P \in \mathbb{P}_{F}$. The support, denoted by $\operatorname{Supp}(G)$, of $G$ is the set $\left\{P \in \mathbb{P}_{F}: n_{P} \neq 0\right\}$. For a nonzero function $z \in F$, the principal divisor of $z$ is defined to be $\operatorname{div}(z)=\sum_{P \in \mathbb{P}_{F}} \nu_{P}(z) P$, where $\nu_{P}$ denotes the normalized discrete valuation at $P$. The zero and pole divisors of $z$ are defined to be $\operatorname{div}(z)_{0}=\sum_{\nu_{P}(z)>0} \nu_{P}(z) P$ and $\operatorname{div}(z)_{\infty}=-\sum_{\nu_{P}(z)<0} \nu_{P}(z) P$, respectively.

For a divisor $G$ of $F$, we define the Riemann-Roch space associated with $G$ by $\mathcal{L}(G):=\left\{f \in F^{*}: \operatorname{div}(f)+\right.$ $G \geqslant 0\} \cup\{0\}$. 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 $\ell(G)=\operatorname{deg}(G)+$ $1-g+\ell(W-G)$, where $g$ is the genus of $F$ and $W$ is a canonical divisor of degree $2 g-2$. Therefore, we always
have that $\ell(G) \geqslant \operatorname{deg}(G)+1-g$ and the equality holds if $\operatorname{deg}(G) \geqslant 2 g-1$.

For a place $P$, let $O_{P}$ denote the integral ring at $P$, i.e., $O_{P}:=\left\{z \in F: \nu_{P}(x) \geqslant 0\right\}$. 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 $\left[F_{P}: \mathbb{F}_{q}\right]$. 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 $\phi \in \operatorname{Aut}\left(F / \mathbb{F}_{q}\right)$ and a place $P$, we denote by $P^{\phi}$ the place $\{\phi(x): x \in P\}$. For a function $f \in F$, we denote by $f^{\phi}$ the action of $\phi$ on $f$. If $\nu_{P}(f) \geqslant 0$ and $\nu_{P^{\phi}}(f) \geqslant 0$, then one has that $\nu_{P}\left(f^{\phi^{-1}}\right) \geqslant 0$ and $f\left(P^{\phi}\right)=f^{\phi^{-1}}(P)$. Furthermore, for a divisor $G=\sum_{P \in \mathbb{P}_{F}} m_{P} P$ we denote by $G^{\phi}$ 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 with the full constant field $\mathbb{F}_{q}$. Fix an automorphism $\sigma \in$ $\operatorname{Aut}\left(F / \mathbb{F}_{q}\right)$ such that $F$ has $m N$ distinct rational places $P_{1}, P_{1}^{\sigma}, \ldots, P_{1}^{\sigma^{m-1}}, P_{2}, P_{2}^{\sigma}, \ldots, P_{2}^{\sigma^{m-1}}, \ldots$, $P_{N}, P_{N}^{\sigma}, \ldots, P_{N}^{\sigma^{m-1}}$. We also choose a divisor $D$ of degree $e$ such that $D$ is fixed under $\sigma$, i.e., $D^{\sigma}=D$; and $P_{i}^{\sigma^{j}} \notin \operatorname{Supp}(D)$ 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 $\mathrm{F}(N, l, q, e, m)$, encodes a message function $f \in \mathcal{L}(l D)$ to the following element
(1)

$$
\left(\left[\begin{array}{c}
f\left(P_{1}\right) \\
f\left(P_{1}^{\sigma}\right) \\
\vdots \\
f\left(P_{1}^{\sigma^{m-1}}\right)
\end{array}\right],\left[\begin{array}{c}
f\left(P_{2}\right) \\
f\left(P_{2}^{\sigma}\right) \\
\vdots \\
f\left(P_{2}^{\sigma^{m-1}}\right)
\end{array}\right], \ldots,\left[\begin{array}{c}
f\left(P_{N}\right) \\
f\left(P_{N}^{\sigma}\right) \\
\vdots \\
f\left(P_{N}^{\sigma^{m-1}}\right)
\end{array}\right]\right)
$$

in $\left(\mathbb{F}_{q}^{m}\right)^{N}$. Note that the folded code $\mathrm{F}(N, l, q, e, m)$ has the alphabet $\mathbb{F}_{q}^{m}$ and it is $\mathbb{F}_{q}$-linear. Furthermore, it is straightforward to verify that $\mathrm{F}(N, l, q, e, m)$ has the following parameters.

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

### 2.3 List Decoding of Folded Algebraic Geometric Codes

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

$$
\mathbf{y}=\left(\begin{array}{cccc}
y_{1,1} & y_{2,1} & & y_{N, 1}  \tag{2}\\
y_{1,2} & y_{2,2} & & \vdots \\
& & \ddots & \\
y_{1, m} & \cdots & & y_{N, m}
\end{array}\right)
$$

where some columns are erroneous. Let $s \geqslant 1$ be an integer parameter associated with the decoder. Then we have the following two lemmas (see [11, 12]).

Lemma 2.2 Given a received word as in (2), we can find a nonzero linear polynomial in $F\left[Y_{1}, Y_{2}, \ldots, Y_{s}\right]$ of the form $Q\left(Y_{1}, Y_{2}, \ldots, Y_{s}\right)=A_{0}+A_{1} Y_{1}+A_{2} Y_{2}+\cdots+$ $A_{s} Y_{s}$ satisfying

$$
\begin{align*}
& Q\left(y_{i, j+1}, y_{i, j+2}, \cdots, y_{i, j+s}\right)=A_{0}\left(P_{i}^{\sigma^{j}}\right)+ \\
& A_{1}\left(P_{i}^{\sigma^{j}}\right) y_{i, j+1}+\cdots+A_{s}\left(P_{i}^{\sigma^{j}}\right) y_{i, j+s}=0 \tag{3}
\end{align*}
$$

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 $\kappa$ chosen as

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

Lemma 2.3 If $f$ is a function in $\mathcal{L}(l D)$ 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 $Q\left(f, f^{\sigma^{-1}}, \ldots, f^{\sigma^{-(s-1)}}\right)$ is the zero function, i.e.,

$$
\begin{equation*}
A_{0}+A_{1} f+A_{2} f^{\sigma^{-1}}+\cdots+A_{s} f^{\sigma^{-(s-1)}}=0 \tag{5}
\end{equation*}
$$

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

$$
\begin{equation*}
\tau \approx \frac{s}{s+1}-\frac{s}{s+1} \times \frac{m}{m-s+1} \times \frac{k+g}{m N} \tag{6}
\end{equation*}
$$

where $k$ is the dimension of $\mathcal{L}(l D)$ 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 [11], 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 $[8,6]$ 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 $\operatorname{deg}(P)>l e$ 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 $q^{u(s-1)}$.

Note that Lemma 2.4 is a special case 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 [ 3,14$]$ ) 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 [8, 6] to illustrate the above theory.

### 2.4 Folded RS and Cyclotomic Codes

Folded Reed-Solomon codes. Let us revisit the construction of folded Reed-Solomon codes from [8, 10]. 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 $\gamma$ be a primitive element of $\mathbb{F}_{q}$. Consider the automorphism $\sigma \in \operatorname{Aut}\left(\mathbb{F}_{q}(x) / \mathbb{F}_{q}\right)$ sending $x$ to $\gamma^{-1} x$. Let $P_{i}$ be the zero of $x-\gamma^{m(i-1)}$ for $i=1,2, \ldots, N$, 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 $\mathcal{L}(k D)=\left\{f(x) \in \mathbb{F}_{q}[x]: \operatorname{deg}(f(x)) \leqslant k-1\right\}$, and our folded algebraic geometric code $\mathrm{F}(N, k, q, 1, m)$ defined in (1) coincides with the folded Reed-Solomon codes defined in [8].

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 $R=k /(m N)$ 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 $N / \varepsilon^{2}$ in this case.

Let $P$ be the place of $F$ corresponding to $x^{q-1}-\gamma$. Then we have $\gamma x \equiv x^{q} \bmod P$, i.e., $x^{\sigma^{-1}}=\gamma x \equiv x^{q}$ $\bmod P$. 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 $q-1=\operatorname{deg}(P)>l e=k+1$ 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 $\ell$. Then $F / \mathbb{F}_{q}(x)$ is a cyclic extension of degree $n=\left(\ell^{d}+1\right) /(\ell+1)$ for some parameter $d$. Let $\sigma$ be a generator of the cyclic group $\operatorname{Gal}\left(F / \mathbb{F}_{q}(x)\right)$. Then for each $\alpha \in \mathbb{F}_{\ell}$, there are $n$ rational places of $F$ lying over $x-\alpha$ that can be written as $P, P^{\sigma}, \ldots, P^{\sigma^{n-1}}$. Thus, there are at least $\ell n$ rational places and they can be arranged in the following way: $P_{1}, P_{1}^{\sigma}, \ldots, P_{1}^{\sigma^{m-1}}, \ldots, P_{N}, P_{N}^{\sigma}, \ldots, P_{N}^{\sigma^{m-1}}$, 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 $\mathcal{L}(l D)$. Then our folded algebraic geometric code $\mathrm{F}(N, l, q, d, m)$ defined in (1) coincides with the folded cyclotomic codes defined in [6].

The genus of the cyclotomic field $F$ is $g=1+(d-$ $2)\left(\ell^{d}+1\right) /(2 \ell+2)-d / 2$. 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 [3, 14]), we know that there exists a place $P$ of $F$ such that $P$ has degree $\ell n$ 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 $q^{\ell(s-1)}=O\left(N^{1 / \varepsilon^{2}}\right)$.

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 $\infty$ as the code length $N$ tends to $\infty$. 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 $\sigma^{-1}$ maps every $z$ to $z^{q^{u}}$ in the residue 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 skip the detailed proof, which can be found in the full version.

Theorem 3.1 Let $\ell$ be a square prime power and let $q=$ $\ell^{2}$. Let $\left\{E / \mathbb{F}_{\ell}\right\}$ be the Garcia-Stichtenoth tower given in [4]. Denote by $n:=N\left(E / \mathbb{F}_{\ell}\right)$ the number of $\mathbb{F}_{\ell}$-rational places of $E$. Put $r=2\lceil n /(\sqrt{\ell}-1)\rceil+1$ and $h=3 r$. Then there exists a family $\left\{F / \mathbb{F}_{q}\right\}$ 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 $e:=\left(\ell^{r}+1\right) /(\ell+1)$ with $L=\mathbb{F}_{q} \cdot E$ and a set $U$ of places of $F$ such that
(i) $|U| \geqslant q^{r}$ and $\operatorname{deg}(P)=$ 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 $\sigma$ is a generator of $\operatorname{Gal}(F / L)$.
(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 $\lim \inf N\left(F / \mathbb{F}_{q}\right) / g(F) \geqslant$ $(\sqrt{\ell}-1) / 2=\left(q^{1 / 4}-1\right) / 2$.

If we choose one place $P$ from the set $U$ in Theorem 3.1 and apply Lemma 2.4, we find that the condition $\operatorname{deg}(P)=e h>l e$ is not satisfied since $l e$ can be as large as $N\left(F / \mathbb{F}_{q}\right) \approx n e$. The idea is to choose a subset $T$ of $U$ in Theorem 3.1 and consider the congruence equation $z^{\sigma^{-1}} \equiv z^{q^{u}} \bmod P$ 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 $\sum_{P \in T} \operatorname{deg}(P)>$ 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 $q^{u(s-1)|T|}$.

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

Theorem 3.3 Let $\ell$ 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 $O\left(N^{(\sqrt{\ell}-1) s}\right)$ elements that includes all message functions whose encoding is within Hamming distance $\tau N$ from the input. (Here $N$ denotes the block length of the code.)

Proof. Let $\left\{F / \mathbb{F}_{q}\right\}$ be a family of function fields given in Theorem 3.1. Choose a rational place $\infty$ of $E$ and regard it as a rational place of $L$. Define the divisor $D:=l \sum_{P_{\infty} \mid \infty, P_{\infty} \in \mathbb{P}_{F}} P_{\infty}$. 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 $P, P^{\sigma}, \ldots, P^{\sigma^{e-1}}$. By taking away those rational places lying over $\infty$, we have at least $e(n-1)$ rational places of $F$, where $n=N\left(E / \mathbb{F}_{\ell}\right)$. Thus, for an integer $m$ with $1 \leqslant m<e$, we can label $N m$ distinct places $P_{1}, P_{1}^{\sigma}, \ldots, P_{1}^{\sigma^{m-1}}, \ldots, P_{N}, P_{N}^{\sigma}, \ldots, P_{N}^{\sigma^{m-1}}$ of F such that none of them lies over $\infty$, as long as $N \leqslant(n-1)\left\lfloor\frac{e}{m}\right\rfloor=\left(N\left(E / \mathbb{F}_{\ell}\right)-1\right)\left\lfloor\frac{e}{m}\right\rfloor$.

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

$$
\begin{aligned}
\sum_{R \in T} \operatorname{deg}(R) & \geqslant 3 r e(\sqrt{\ell}-1) \geqslant 6 N\left(E / \mathbb{F}_{\ell}\right) e \\
& =6 m N\left(E / \mathbb{F}_{\ell}\right) \frac{e}{m}>N m>l e
\end{aligned}
$$

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

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

## 4 Encoding and Decoding

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

Encoding. Let us consider the folded algebraic geometric code given in the proof of Theorem 3.3, where the divisor $D$ is $l \sum_{P_{\infty} \mid \infty, P_{\infty} \in \mathbb{P}_{F}} P_{\infty}$ and the Riemann-Roch space is $\mathcal{L}(l D)$. To encode, we assume that $l e>2 g-1$ and there is an algorithm to find a basis $\left\{z_{1}, z_{2}, \ldots, z_{k}\right\}$ of $\mathcal{L}(l D)$ with $k=l e-g+1$.

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 $f\left(P_{i}^{\sigma^{j}}\right)$. For a function $f$ and a rational place P with $\nu_{\mathrm{P}}(f) \geqslant 0$, 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 $\nu_{\mathrm{P}}(t)=1$ ); and (ii) finding the unique element $\alpha \in \mathbb{F}_{q}$ such that $\nu_{\mathrm{P}}\left(\frac{f-\alpha}{t}\right) \geqslant 0$ (note that this unique element $\alpha$ is equal to $f(\mathrm{P}))$.

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. 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 [15, 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 $\nu_{\mathrm{P}}(f) \geqslant v$, we have $\nu_{\mathrm{P}}\left(\frac{f}{t^{v}}\right) \geqslant 0$. Put $a_{v}=\left(\frac{f}{t^{v}}\right)$ (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 $\nu_{\mathrm{P}}\left(\frac{f}{t^{v}}-a_{v}\right) \geqslant 1$, hence we know that $\nu_{\mathrm{P}}\left(\frac{f-a_{v} t^{v}}{t^{v+1}}\right) \geqslant 0$. Put $a_{v+1}=\left(\frac{f-a_{v} t^{v}}{t^{v+1}}\right)$ (P). Then $\nu_{\mathrm{P}}\left(f-a_{v} t^{v}-a_{v+1} t^{v+1}\right) \geqslant v+2$.

Assume that we have obtained a sequence $\left\{a_{r}\right\}_{r=v}^{m}$ $(m>v)$ of elements of $\mathbb{F}_{q}$ such that $\nu_{\mathrm{P}}\left(f-\sum_{r=v}^{k} a_{r} t^{r}\right) \geqslant$ $k+1$ for all $v \leqslant k \leqslant m$. Put $a_{m+1}=\left(\frac{f-\sum_{r=v}^{m} a_{r} t^{r}}{t^{m+1}}\right)(\mathrm{P})$. Then $\nu_{\mathrm{P}}\left(f-\sum_{r=v}^{m+1} a_{r} t^{r}\right) \geqslant m+2$. In this way we continue our construction of the $a_{r}$. Then we obtain an infinite sequence $\left\{a_{r}\right\}_{r=v}^{\infty}$ of elements of $\mathbb{F}_{q}$ such that $\nu_{\mathrm{P}}\left(f-\sum_{r=v}^{m} a_{r} t^{r}\right) \geqslant m+1$ for all $m \geqslant v$. We summarize the above construction in the formal expansion $f=\sum_{r=v}^{\infty} a_{r} t^{r}$, 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 $\sum_{i=v}^{\infty} a_{i} t^{i}$ satisfies $\nu_{\mathrm{P}}\left(f-\sum_{i=v}^{m} a_{i} t^{i}\right) \geqslant m+1$ 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 can be easily proved, but it plays an important role in our decoding.

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

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 $\mathrm{P}, \mathrm{P}^{\sigma}, \ldots, \mathrm{P}^{\sigma^{e-1}}$, where $\sigma$ is a generator of $\operatorname{Gal}(F / L)$. It is clear that $t$ is a common local parameter of $\mathrm{P}, \mathrm{P}^{\sigma}, \ldots, \mathrm{P}^{\sigma^{\mathrm{e}-1}}$. 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 $k=l e-g+1$ is the dimension of $\mathcal{L}(l D)$. Solving for $f$ in (5) is equivalent to finding $\left\{f_{i}\right\}_{i=1}^{k}$. Assume that the local expansion of $z_{i}$ at $\mathrm{P}^{\sigma^{j}}$ is given by $\sum_{h=0}^{\infty} \alpha_{i j h} t^{h}$. Then by Lemma 4.1, $z_{i}^{\sigma^{-j}}$ have the local expansion $\sum_{h=0}^{\infty} \alpha_{i j h} t^{h}$ at P . Thus, $f^{\sigma^{-j}}$ has the local expansion $\sum_{i=1}^{k} \sum_{h=0}^{\infty} \alpha_{i j h} t^{h}$ at P . Furthermore assume that $A_{i}$ have local expansions $\sum_{j=0}^{\infty} a_{i j} t^{j}$ at P for $0 \leqslant i \leqslant s$. Substitute these local expansions in Equation (5), we obtain an equation

$$
\begin{align*}
& c_{0}\left(f_{1}, f_{2}, \ldots, f_{k}\right)+c_{1}\left(f_{1}, f_{2}, \ldots, f_{k}\right) t \\
& +\cdots+c_{i}\left(f_{1}, f_{2}, \ldots, f_{k}\right) t^{i}+\cdots=0 \tag{7}
\end{align*}
$$

where $c_{i}\left(f_{1}, f_{2}, \ldots, f_{k}\right)$ 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 (7) must be zero. This produces infinitely many linear equations $c_{i}\left(f_{1}, f_{2}, \ldots, f_{k}\right)=0$ 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

$$
\begin{equation*}
c_{i}\left(f_{1}, f_{2}, \ldots, f_{k}\right)=0 \quad \text { for } i=0,1, \ldots, l e \tag{8}
\end{equation*}
$$

due to the fact that $A_{0}+A_{1} f+\cdots+A_{s} f^{\sigma^{-(s-1)}} \in \mathcal{L}(l D)$ and the following simple claim which follows because a function with pole order at most $l e$ can be have at most $l e$ zeroes at P .

Lemma 4.2 If $x$ is an element in $\mathcal{L}(l D)$ 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 $i \leqslant l e$.

The equation system (8) has $l e+1$ equations and contains $k=l e-g+1$ variables. Theorem 3.3 guarantees that this system has at most $O\left(N^{(\sqrt{\ell}-1) s}\right)$ 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 $(1 / \varepsilon)^{O\left(1 / \varepsilon^{2}\right)}$ with rate $R$ and
decoding radius $\tau=1-R-\varepsilon$ such that the length of the code tends to $\infty$ and is independent of $\varepsilon$. Moreover, the code is deterministically list decodable with a list size $O\left(N^{1 / \varepsilon^{2}}\right)$.

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 $\tau$ given in Theorem 3.3 is $1-R-\varepsilon$. The alphabet size of the folded code is $q^{m}$, which is $(1 / \varepsilon)^{O\left(1 / \varepsilon^{2}\right)}$ and the list size is $O\left(N^{(\sqrt{\ell}-1) s}\right)=O\left(N^{1 / \varepsilon^{2}}\right)$.

## References

[1] Virgile Ducet and Claus Fieker. Computing equations of curves with many points. In Proceedings of the ANTS X conference, 2012.
[2] Gerhard Frey, Marc Perret, and Henning Stichtenoth. On the different of abelian extensions of global fields. In Coding theory and algebraic geometry, volume 1518 of Lecture Notes in Mathematics, pages 26-32. Springer Berlin/Heidelberg, 1992.
[3] M. D. Fried and M. Jarden. Field Arithmetic. Springer-Verlag, Berlin, 2008.
[4] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound. Inventiones Mathematicae, 121:211-222, 1995.
[5] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. Journal of Number Theory, 61(2):248-273, 1996.
[6] Venkatesan Guruswami. Cyclotomic function fields, Artin-Frobenius automorphisms, and list errorcorrection with optimal rate. Algebra and Number Theory, 4(4):433-463, 2010.
[7] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. In Proceedings of the 54th Annual Symposium on Foundations of Computer Science, October 2013. To appear. Available at http://eccc.hpi-web.de/report/2013/060/.
[8] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Errorcorrection with optimal redundancy. IEEE Transactions on Information Theory, 54(1):135-150, 2008.
[9] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. Journal of the ACM, 56(4), 2009.
[10] Venkatesan Guruswami and Carol Wang. Linearalgebraic list decoding for variants of Reed-Solomon codes. IEEE Transactions on Information Theory, 59(6):3257-3268, 2013.
[11] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. CoRR, abs/1204.4209, 2012. Extended abstract in STOC 2012.
[12] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound. Electronic Colloquium on Computational Complexity (ECCC), 19:146, 2012. Extended abstract in STOC 2013.
[13] Florian Hess. Computing Riemann-Roch spaces in algebraic function felds and related topics. J. Symbolic Computation, 33(4):425-445, 2002.
[14] V. Kumar Murty and J. Scherk. Effective versions of the Chebotarev density theorem for function elds. C. R. Acad. Sci. (Paris), 319:523-528, 1994.
[15] Harald Niederreiter and Chaoping Xing. Rational Points on Curves over Finite Fields-Theory and Applications. Cambridge University Press, 2000.
[16] W. Wesley Peterson. Encoding and error-correction procedures for Bose-Chaudhuri codes. IEEE Transactions on Information Theory, 6:459-470, 1960.
[17] Henning Stichtenoth. Algebraic Function Fields and Codes. Universitext, Springer-Verlag, Berlin, 1993.


[^0]:    *An expanded version of this paper is available at http://eccc.hpi-web.de/report/2013/046/
    ${ }^{\dagger}$ Computer Science Department, Carnegie Mellon University, Pittsburgh, USA. Research supported in part by a Packard Fellowship and NSF CCF-0963975. Email: guruswami@cmu.edu
    ${ }^{\ddagger}$ Division of Mathematical Sciences, School of Physical \& Mathematical Sciences, Nanyang Technological University, Singapore. Research supported in part by the Singapore A*STAR SERC under Research Grant 1121720011 and the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. Email: xingcp@ntu.edu.sg

[^1]:    ${ }^{1}$ See [8, Sec. 5] or [10, Sec. 2.4] for an explanation of how to extend the algebraic list decoders for folded codes to the list recovery setting; the details for our codes will be identical.

