Electronic Colloquium on Computational Complexity, Report No. 1 (2009)

ARTIN AUTOMORPHISMS, CYCLOTOMIC FUNCTION FIELDS, AND FOLDED LIST-DECODABLE CODES

VENKATESAN GURUSWAMI

ABSTRACT. Algebraic codes that achieve list decoding capacity were recently constructed by a careful "folding" of the Reed-Solomon code. The "low-degree" nature of this folding operation was crucial to the list decoding algorithm. We show how such folding schemes conducive to list decoding arise out of the Artin-Frobenius automorphism at primes in Galois extensions. Using this approach, we construct new folded algebraic-geometric codes for list decoding based on cyclotomic function fields with a cyclic Galois group. Such function fields are obtained by adjoining torsion points of the Carlitz action of an irreducible $M \in \mathbb{F}_q[T]$. The Reed-Solomon case corresponds to the simplest such extension (corresponding to the case $M = T$). In the general case, we need to descend to the fixed field of a suitable Galois subgroup in order to ensure the existence of many degree one places that can be used for encoding.

Our methods shed new light on algebraic codes and their list decoding, and lead to new codes achieving list decoding capacity. Quantitatively, these codes provide list decoding (and list recovery/soft decoding) guarantees similar to folded Reed-Solomon codes but with an alphabet size that is only polylogarithmic in the block length. In comparison, for folded RS codes, the alphabet size is a large polynomial in the block length. This has applications to fully explicit (with no brute-force search) binary concatenated codes for list decoding up to the Zyablov radius.

CONTENTS

Research supported in part by NSF CCF-0343672, a David and Lucile Packard Fellowship, and NSF grant CCR-0324906 to the IAS.

ISSN 1433-8092

1. Introduction

1.1. **Context and Motivation.** Recent progress in algebraic coding theory [16, 6] has led to the construction of explicit codes over large alphabets that achieve list decoding capacity — namely, they admit efficient algorithms to correct close to the optimal fraction $1-R$ of errors with rate R. The algebraic codes constructed in [6] are *folded* Reed-Solomon codes, where the Reed-Solomon (RS) encoding $(f(1), f(\gamma), \cdots, f(\gamma^{n-1}))$ of a low-degree polynomial $f \in \mathbb{F}_q[T]$ is viewed as a codeword of length $N = n/m$ over the alphabet $\mathbb{F}_q^m$ by identifying successive blocks of m symbols. Here γ is a primitive element of the field $\mathbb{F}_q$.

Simplifying matters somewhat, the principal algebraic engine behind the list decoding algorithm in [6] was the identity $f(\gamma T) \equiv f(T)^q \pmod{(T^{q-1}-\gamma)}$, and the fact that $(T^{q-1}-\gamma)$ is irreducible over $\mathbb{F}_q$. This gave a low-degree algebraic relation between $f(T)$ and $f(\gamma T)$ in the residue field $\mathbb{F}_q[T]/(T^{q-1}-\gamma)$. This together with an algebraic relation found by the "interpolation step" of the decoding enabled finding the list of all relevant message polynomials $f(T)$ efficiently.

One of the main motivations of this work is to gain a deeper understanding of the general algebraic principles underlying the above folding, with the hope of extending it to more general algebraic-geometric (AG) codes. The latter question is an interesting algebraic question in its own right, but is also important for potentially improving the alphabet size of the codes, as well as the decoding complexity and output list size of the decoding algorithm. (The large complexity and list size of the folded RS decoding algorithm in [6] are a direct consequence of the large degree q in the identity relating $f(\gamma T)$ and $f(T)$.)

An extension of the Parvaresh-Vardy codes [16] (which were the precursor to the folded RS codes) to arbitrary algebraic-geometric codes was achieved in [5]. But in these codes the encoding includes the evaluations of an additional function explicitly picked to satisfy a low-degree relation over some residue field. This leads to a substantial loss in rate. The crucial insight in the construction of folded RS codes was the fact that this additional function could just be the closely related function $f(\gamma T)$ — the image of $f(T)$ under the automorphism $T \mapsto \gamma T$ of $\mathbb{F}_q(T)$.

1.2. **Summary of our contributions.** We explain how folding schemes conducive to list decoding (such as the above relation between $f(\gamma T)$ and $f(T)$) arise out of the *Artin-Frobenius automorphism* at primes in Galois extensions. With the benefit of hindsight, the role of such automorphisms in folding algebraic codes is quite natural. In terms of technical contributions, we use this approach to construct new list-decodable folded algebraic-geometric codes based on *cyclotomic function fields* with a cyclic Galois group. Cyclotomic function fields [1, 9] are obtained by adjoining torsion points of the Carlitz action of an irreducible $M \in \mathbb{F}_q[T]$. The Reed-Solomon case corresponds to the simplest such extension (corresponding to the case $M = T$). In the general case, we need to descend to the fixed field of a suitable Galois subgroup in order to ensure the existence of many degree one places that can be used for encoding. We establish some key algebraic lemmas that characterize the desired subfield in terms of the appropriate generator μ in the algebraic closure of $\mathbb{F}_q(T)$ and its minimal polynomial over $\mathbb{F}_q(T)$. We then tackle the computational algebra challenge of computing a representation of the subfield and its rational places, and the message space, that is conducive for efficient encoding and decoding of the associated algebraic-geometric code.

Our constructions lead to some substantial quantitative improvements in the alphabet size which we discuss below in Section 1.4. We also make some simplifications in the list decoding algorithm and avoid the need of a zero-increasing basis at each code place (Lemma 6.2). This, together with several other ideas, lets us implement the list decoding algorithm in polynomial time assuming *only* the natural representation of the code needed for efficient encoding, namely a basis for the message space. Computing such a basis remains an interesting question in computational function field theory. Our description and analysis of the list decoding algorithm in this work is self-contained, though it builds strongly on the framework of the algorithms in [23, 16, 5, 6].

1.3. **Galois extensions and Artin automorphisms.** We now briefly discuss how and why Artin-Frobenius automorphisms arise in the seemingly distant world of list decoding. In order to generalize the Reed-Solomon case, we are after function fields whose automorphisms we have a reasonable understanding of. Galois extensions are a natural subclass of function fields to consider, with the hope that some automorphism in the Galois group will give a low-degree relation over some residue field. Unfortunately, the explicit constructions of good AG codes are typically based on a tower of function fields [3, 4], where each step is Galois, but the whole extension is not. (Stichtenoth [22] recently showed the existence of a Galois extension with the optimal trade-off between genus and number of rational places, but this extension is not, and cannot be, cyclic, as we require.)

In Galois extensions K/F, for each place A' in the extension field K, there is a special and important automorphism called the Artin-Frobenius automorphism (see, eg. [13, Chap. 4]) that simply powers the residue of any (regular) function at that place. The exponent or degree of this map is the norm of the place A of F lying below A'. Since the degree dictates the complexity of decoding, we would like this norm to be small. On the other hand, the residue field at A' needs to be large enough so that the message functions can be uniquely identified by their residue modulo A'. The most appealing way to realize this is if the place A is inert, i.e., has a unique A' lying above it. However, this condition can only hold if the Galois group is cyclic, a rather strong restriction. For example, it is known [2] that even abelian extensions must be *asymptotically bad*.

In order to construct AG codes, we also need to have a good control of how certain primes split in the extension. For cyclotomic function fields, and of course their better known number-theoretic counterparts $\mathbb{Q}(\omega)$ obtained by adjoining a root of unity ω, this theory is well developed. As mentioned earlier, the cyclotomic function field we use itself has very few rational places. So we need to descend to an appropriate subfield where many degree one places of $\mathbb{F}_q(T)$ split completely, and develop some underlying theory concerning the structure of this subfield.

The Artin-Frobenius automorphism[1] is a fundamental notion in algebraic number theory, playing a role in Chebatorev density theorem and Dirichlet's theorem on infinitude of primes in arithmetic progressions, as well as quadratic and more general reciprocity laws. We find

[1]Following Rosen [18], we will henceforth refer to the Artin-Frobenius automorphisms as simply Artin automorphisms. Many texts (eg. [13]) actually refer to these as Frobenius automorphisms. Since the latter term is most commonly associated with automorphism $x \mapsto x^q$ of $\mathbb{F}_{q^m}$, we prefer the term Artin automorphism to refer to the general notion that applies to all Galois extensions. The association of a place with its Artin-Frobenius automorphism is called the Artin map.

it rather intriguing that this notion ends up playing an important role in algorithmic coding theory as well.

1.4. **Long codes achieving list decoding capacity and explicit binary concatenated codes.** Quantitatively, our cyclotomic function field codes achieve list decoding (and list recovery) guarantees similar to folded RS codes but with an alphabet size that is only *polylogarithmic* in the block length. In comparison, for folded RS codes, the alphabet size is a large polynomial in the block length. We note that Guruswami and Rudra [6] also present capacity-achieving codes of rate R for list decoding a fraction $(1 - R - \varepsilon)$ of errors with alphabet size $|\Sigma| = 2^{(1/\varepsilon)^{O(1)}}$, a fixed constant depending only on ε. But these codes do not have the strong "list recovery" (or more generally, soft decoding) property of folded RS codes.

Our codes inherit the powerful list recovery property of folded RS codes, which makes them very useful as outer codes in concatenation schemes. In fact, due to their small alphabet size, they are even better in this role. Indeed, they can serve as outer codes for a family of concatenated codes list-decodable up to the Zyablov radius, *with no brute-force search* for the inner codes. This is the first such construction for list decoding. It is similar to the "Justesen-style" explicit constructions for rate vs. distance from [11, 20], except even easier, as one can use the ensemble of *all linear codes* instead of the succinct Wozencraft ensemble at the inner level of the concatenated scheme.

1.5. **Related work.** Codes based on cyclotomic function fields have been considered previously in the literature. Some specific (non-asymptotic) constructions of function fields with many rational places over small fields $\mathbb{F}_q$ $(q \leqslant 5)$ appear in [14, 15]. Cyclotomic codes based on the action of polynomials T^a for small a appear in [17], but decoding algorithms are not discussed for these codes, nor are these extensions cyclic as we require. Our approach is more general and works based on the action of an arbitrary irreducible polynomial. Exploiting the Artin automorphism of cyclotomic fields for an algorithmic purpose is also new to this work.

Independent of our work, Huang and Narayanan [10] also consider AG codes constructed from Galois extensions, and observe how automorphisms of large order can be used for folding such codes. To our knowledge, the only instantiation of this approach that improves on folded RS codes is the one based on cyclotomic function fields from our work. As an alternate approach, they also propose a decoding method that works with folding via automorphisms of small order. This involves computing several coefficients of the power series expansion of the message function at a low-degree place. Unfortunately, piecing together these coefficients into a function could lead to an exponential list size bound. The authors suggest a heuristic assumption under which they can show that for a *random* received word, the expected list size and running time are polynomially bounded.

2. Background on Cyclotomic function fields

Some basic preliminaries on function fields, valuations and places, Galois extensions, decomposition of primes, Artin-Frobenius automorphism, etc. are discussed in Appendix B. In this section, we will focus on background material concerning cyclotomic function fields. These are the function-field analog of the classic cyclotomic number fields from algebraic number theory. This theory was developed by Hayes [9] in 1974 building upon ideas due to Carlitz [1] from the late 1930's. The objective was to develop an explicit class field theory classifying all abelian extensions of the rational function field $\mathbb{F}_q(T)$, analogous to classic results for $\mathbb{Q}$ and imaginary quadratic extensions of $\mathbb{Q}$. The common idea in these results is to allow a ring of "integers" in the ground field to act on part of its algebraic closure, and obtain abelian extensions by adjoining torsion points of this action. We will now describe these extensions of $\mathbb{F}_q(T)$.

Let T be an indeterminate over the finite field $\mathbb{F}_q$. Let $R_T = \mathbb{F}_q[T]$ denote the polynomial ring, and $F = \mathbb{F}_q(T)$ the field of rational functions. Let F^{ac} be a fixed algebraic closure of F. Let $\mathrm{End}_{\mathbb{F}_q}(F^{\mathrm{ac}})$ be the ring of $\mathbb{F}_q$-endomorphisms of F^{ac}, thought of as a $\mathbb{F}_q$-vector space. We consider two special elements of $\mathrm{End}_{\mathbb{F}_q}(F^{\mathrm{ac}})$: (i) the Frobenius automorphism τ defined by $\tau(z) = z^q$ for all $z \in F^{\mathrm{ac}}$, and (ii) the map μ_T defined by $\mu_T(z) = Tz$ for all $z \in F^{\mathrm{ac}}$. The substitution $T \to \tau + \mu_T$ yields a ring homomorphism from R_T to $\mathrm{End}_{\mathbb{F}_q}(F^{\mathrm{ac}})$ given by: $f(T) \mapsto f(\tau + \mu_T)$. Using this, we can define the *Carlitz action* of R_T on F^{ac} as follows: For $M \in R_T$,

$$C_M(z) = M(\tau + \mu_T)(z) \qquad \text{for all } z \in F^{\mathrm{ac}} \ .$$

This action endows F^{ac} the structure of an R_T-module, which is called the Carlitz module. For a nonzero polynomial $M \in R_T$, define the set

$$\Lambda_M = \{z \in F^{\mathrm{ac}} \mid C_M(z) = 0\} \ ,$$

to consist of the M-torsion points of F^{ac}, i.e., the elements annihilated by the Carlitz action of M (this is also the set of zeroes of the polynomial $C_M(Z) \in R_T[Z]$). Since R_T is commutative, Λ_M is in fact an R_T-submodule of F^{ac}. It is in fact a cyclic R_T-module, naturally isomorphic to $R_T/(M)$.

The cyclotomic function field $F(\Lambda_M)$ is obtained by adjoining the set Λ_M of M-torsion points to F. [2] The following result from [9] summarizes some fundamental facts about cyclotomic function fields, stated for the special case when M is irreducible (we will only use such extensions). Proofs can also be found in the graduate texts [18, Chap. 12] or [19, Chap. 12]. In what follows, we will often use the convention that an irreducible polynomial $P \in R_T$ is identified with the place of F which is the zero of P, and also denote this place by P. Recall that these are all the places of F, with the exception of the place P_∞, which is the unique pole of T.

Proposition 2.1. *Let $M \in R_T$ be a nonzero degree d monic polynomial that is irreducible over $\mathbb{F}_q$. Let $K = F(\Lambda_M)$. Then*

(i) *$C_M(Z)$ is a separable polynomial in Z of degree q^d over R_T, of the form $\sum_{i=0}^{d}[M,i]Z^{q^i}$ where the degree of $[M,i]$ as a polynomial in T is $q^i(d-i)$. The polynomial $\psi_M(Z) = C_M(Z)/Z$ is irreducible in $R_T[Z]$. The field K is equal to the splitting field of $\psi_M(Z)$, and is generated by any nonzero element $\lambda \in \Lambda_M$, i.e., $K = F(\lambda)$.*

(ii) *K/F is a Galois extension of degree (q^d-1) and $\mathrm{Gal}(K/F)$ is isomorphic to $(R_T/(M))^*$, the cyclic multiplicative group of units of the field $R_T/(M)$. The Galois automorphism σ_N associated with $\bar{N} \in (R_T/(M))^*$ is given by $\sigma_N(\lambda) = C_N(\lambda)$.*

[2] It is instructive to compare this with the more familiar setting of cyclotomic number fields. There, one lets $\mathbb{Z}$ act on the multiplicative group $(\mathbb{Q}^{\mathrm{ac}})^*$ with the endomorphism corresponding to $n \in \mathbb{Z}$ sending $\zeta \mapsto \zeta^n$ for $\zeta \in \mathbb{Q}^{\mathrm{ac}}$. The n-torsion points now equal $\{\zeta \in \mathbb{Q}^{\mathrm{ac}} \mid \zeta^n = 1\}$, i.e., the n'th roots of unity. Adjoining these gives the various cyclotomic number fields.

The Galois automorphisms commute with the Carlitz action: for any $\sigma \in \mathrm{Gal}(K/F)$ *and* $A \in R_T$, $\sigma(C_A(x)) = C_A(\sigma(x))$ *for all* $x \in K$.

(iii) *If* $P \in R_T$ *is a monic irreducible polynomial different from* M*, then the Artin automorphism at the place* P *is equal to* σ_P.

(iv) *The integral closure of* R_T *in* $F(\lambda)$ *equals* $R_T[\lambda]$.

(v) *The genus* g_M *of* $F(\Lambda_M)$ *satisfies* $2g_M - 2 = d(q^d - 2) - \frac{q}{q-1}(q^d - 1)$.

The splitting behavior of primes in the extension $F(\Lambda_M)/F$ will be crucial for our construction. We record this as a separate proposition below.

Proposition 2.2. *Let* $M \in R_T$, $M \neq 0$, *be a monic, irreducible polynomial of degree* d.

(i) *(Ramification at* M*) The place* M *is totally ramified in the extension* $F(\Lambda_M)/F$*. If* $\lambda \in \Lambda_M$ *is a root of* $C_M(z)/z$ *and* $\tilde{M}$ *is the unique place of* $F(\Lambda_M)$ *lying above* M*, then* λ *is a* $\tilde{M}$*-prime element, i.e.,* $v_{\tilde{M}}(\lambda) = 1$.

(ii) *(Ramification at* P_∞*) The infinite place* P_∞ *of* F*, i.e., the pole of* T*, splits into* $(q^d-1)/(q-1)$ *places of degree one in* $F(\Lambda_M)/F$*, each with ramification index* $(q-1)$*. Its decomposition group equals* $\mathbb{F}_q^*$.

(iii) *(Splitting at other places) If* $P \in R_T$ *is a monic irreducible polynomial different from* M*, then* P *is unramified in* $F(\Lambda_M)/F$*, and splits into* $(q^d - 1)/f$ *primes of degree* $f \cdot \deg(P)$ *where* f *is the order of* P *modulo* M *(i.e., the smallest positive integer* e *such that* $P^e \equiv 1 \pmod{M}$*).*

3. Reed-Solomon codes as cyclotomic function field codes

We now discuss how Reed-Solomon codes arise out of the simplest cyclotomic extension $F(\Lambda_T)/F$. This serves both as a warm-up for our later results, and as a method to illustrate that one can view the folding employed by Guruswami and Rudra [6] as arising naturally from the Artin automorphism at a certain prime in the extension $F(\Lambda_T)/F$.

We have $\Lambda_T = \{u \in F^{\mathrm{ac}} \mid u^q + Tu = 0\}$. Pick a nonzero $\lambda \in \Lambda_T$. By Proposition 2.2, the only ramified places in $F(\Lambda_T)/F$ are T, and the pole P_∞ of T. Both of these are totally ramified and have a unique place above them in $F(\Lambda_T)$. Denote by Q_∞ the place above P_∞ in $F(\Lambda_T)$.

We have $\lambda^{q-1} = -T$, so λ has a pole of order one at Q_∞, and no poles elsewhere. The place $T+1$ splits completely into $n = q-1$ places of degree one in $F(\Lambda_T)$. The evaluation of λ at these places correspond to the roots of $x^{q-1} = 1$, i.e., to nonzero elements of $\mathbb{F}_q$. Thus the places above $T+1$ can be described as $P_1, P_\gamma, \cdots, P_{\gamma^{q-2}}$ where γ is a primitive element of $\mathbb{F}_q$ and $\lambda(P_{\gamma^i}) = \gamma^i$ for $i = 0, 1, \ldots, q-2$.

For $k < q-1$, define $\mathcal{M}_k = \{\sum_{i=0}^{k-1} \beta_i \lambda^i \mid \beta_i \in \mathbb{F}_q\}$. $\mathcal{M}_k$ has q^k elements, each with at most $(k-1)$ poles at Q_∞ and no poles elsewhere. Consider the $\mathbb{F}_q$-linear map $E_{\mathrm{RS}} : \mathcal{M}_k \to \mathbb{F}_q^n$ defined as

$$E_{\mathrm{RS}}(f) = \Big(f(P_1), f(P_\gamma), \cdots, f(P_{\gamma^{q-2}})\Big) .$$

Clearly the above just defines an $[n,k]_q$ Reed-Solomon code, consisting of evaluations of polynomials of degree $< k$ at elements of $\mathbb{F}_q^*$.

Consider the place $T+\gamma$ of F. The condition $(T+\gamma)^f \equiv 1 \pmod{T}$ is satisfied iff $\gamma^f = 1$, which happens iff $(q-1)|f$. Therefore, the place $T+\gamma$ remains inert in $F(\Lambda_T)/F$. Let A denote the unique place above $T+\gamma$ in $F(\Lambda_T)$. The degree of A equals $q-1$.

The Artin automorphism at A, σ_A, is given by $\sigma_A(\lambda) = C_{T+\gamma}(\lambda) = C_\gamma(\lambda) = \gamma\lambda$. Note that this implies $f(P_{\gamma^{i+1}}) = \sigma_A(f)(P_{\gamma^i})$ for $0 \leqslant i < q-2$. By the property of the Artin automorphism, we have $\sigma_A(f) \equiv f^q \pmod{A}$ for all $f \in R_T[\lambda]$. Note that this is same as the condition $f(\gamma\lambda) \equiv f(\lambda)^q \pmod{(\lambda^{q-1}-\gamma)}$ treating f as a polynomial in λ. This corresponds to the algebraic relation between $f(X)$ and $f(\gamma X)$ in the ring $\mathbb{F}_q[X]$ that was used by Guruswami and Rudra [6] in their decoding algorithm, specifically in the task of finding all $f(X)$ of degree less than k satisfying $Q(X, f(X), f(\gamma X)) = 0$ for a given $Q \in \mathbb{F}_q[X,Y,Z]$. In the cyclotomic language, this corresponds to finding all $f \in R_T[\lambda]$ with $< k$ poles at Q_∞ satisfying $Q(f, \sigma_A(f)) = 0$ for $Q \in R_T[\lambda](Y,Z)$. Since $\deg(A) = q-1 \geqslant k$, f is determined by its residue at A, and we know $\sigma_A(f) \equiv f^q \pmod{A}$. Therefore, we can find all such f by finding the roots of the univariate polynomial $Q(Y, Y^q) \mod A$ over the residue field $\mathcal{O}_A/A$.

4. Subfield construction from cyclic cyclotomic function fields

In this section, we will construct the function field construction that will be used for our algebraic-geometric codes, and establish the key algebraic facts concerning it. The approach will be to take cyclotomic field $K = F(\Lambda_M)$ where M is an irreducible of degree $d > 1$ and get a code over $\mathbb{F}_q$. But the only places of degree 1 in $F(\Lambda_M)$ are the ones above the pole P_∞ of T. There are only $(q^d-1)/(q-1)$ such places above P_∞, which is much smaller than the genus. So we descend to a subfield where many degree 1 places split completely. This is done by taking a subgroup H of $(\mathbb{F}_q[T]/(M))^*$ with many degree 1 polynomials and considering the fixed field $E = K^H$. For every irreducible $N \in R_T$ such that $\bar{N} = N \mod M \in H$, the place N splits completely in the extension E/F (this follows from the fact that C_N is the Artin automorphism at the place N). This technique has also been used in the previous works [17, 14, 15] mentioned in Section 1.5, though our approach is more general and works with any irreducible M. The study of algorithms for cyclotomic codes and the role played by the Artin automorphism in their list decoding is also novel to our work.

4.1. **Table of parameters.** Since there is an unavoidable surfeit of notation and parameters used in this section and Section 5, we summarize them for easy reference in Appendix A.

4.2. **Function field construction.** Let $\mathbb{F}_r$ be a subfield of $\mathbb{F}_q$. Let $M \in \mathbb{F}_r[T]$ be a monic polynomial that is irreducible over $\mathbb{F}_q$ (note that we require $M(T)$ to have coefficients in the smaller field $\mathbb{F}_r$, but demand irreducibility in the ring $\mathbb{F}_q[T]$). The following lemma follows from the general characterization of when binomials $T^m - \alpha$ are irreducible in $\mathbb{F}_q[T]$ [12, Chap. 3].

Lemma 4.1. *Let $d \geqslant 1$ be an odd integer such that every prime factor of d divides $(r-1)$ and $\gcd(d, (q-1)/(r-1)) = 1$. Let γ be a primitive element of $\mathbb{F}_r$. Then $T^d - \gamma \in \mathbb{F}_r[T]$ is irreducible in $\mathbb{F}_q[T]$.*

A simple choice for which the above conditions are met is $r = 2^a$, $q = r^2$, and $d = r-1$ (we will need a more complicated choice for our list decoding result in Theorem 7.1). For the sake of generality as well as clarity of exposition, we will develop the theory without making specific choices for the parameters, a somewhat intricate task we will undertake in Section 7.

For the rest of this section, fix $M(T) = T^d - \gamma$ as guaranteed by the above lemma. We continue with the notation $F = \mathbb{F}_q(T)$, $R_T = \mathbb{F}_q[T]$, and $K = F(\Lambda_M)$. Fix a generator $\lambda \in \Lambda_M$ of K/F so that $K = F(\lambda)$.

Let G be the Galois group of K/F, which is isomorphic to the cyclic multiplicative group $(\mathbb{F}_q[T]/(M))^*$. Let $H \subset G$ be the subgroup $\mathbb{F}_q^* \cdot (\mathbb{F}_r[T]/(M))^*$. The cardinality of H is $(r^d - 1) \cdot \frac{q-1}{r-1}$. Note that since G is cyclic there is a unique subgroup H of this size. Indeed, if $\Gamma \in G$ is an arbitrary generator of G, then $H = \{1, \Gamma^b, \Gamma^{2b}, \ldots, \Gamma^{q^d-1-b}\}$ where

$$b = \frac{|G|}{|H|} = \frac{q^d - 1}{r^d - 1} \cdot \frac{r-1}{q-1} \; . \tag{4.1}$$

Let $A \in R_T$ be an arbitrary polynomial such that $A \mod M$ is a generator of $(\mathbb{F}_q[T]/(M))^*$. We can then take Γ so that $\Gamma(\lambda) = C_A(\lambda)$. (We fix a choice of A in the sequel and assume that A is pre-computed and known. We will later, in Section 5.3, pick such an A of appropriately large degree.) Note that by part (2) of Proposition 2.1, the Galois action commutes with the Carlitz action and therefore $\Gamma^j(\lambda) = C_{A^j}(\lambda)$ for all $j \geqslant 1$. Thus knowing the polynomial A lets us compute the action of the automorphisms of H on any desired element of $K = F(\lambda)$.

Let $E \subset K$ be the subfield of K fixed by the subgroup H, i.e., $E = \{x \in K \mid \sigma(x) = x \; \forall \sigma \in H\}$. The field E will be the one used to construct our codes. We first record some basic properties of the extension E/F, and how certain places decompose in this extension.

Proposition 4.2. *For $E = F(\Lambda_M)^H$, the following properties hold:*

- (i) *E/F is a Galois extension of degree $[E : F] = b$.*
- (ii) *The place M is the only ramified place in E/F, and it is totally ramified with a unique place (call it M') above it in E.*
- (iii) *The infinite place P_∞ of F, i.e., the pole of T, splits completely into b degree one places in E.*
- (iv) *The genus g_E of E equals $\frac{d(b-1)}{2} + 1$.*
- (v) *For each $\beta \in \mathbb{F}_r$, the place $T - \beta$ of F splits completely into b degree one places in E.*
- (vi) *If $A \in R_T$ is irreducible of degree $\ell \geqslant 1$ and $A \mod M$ is a primitive element of $R_T/(M)$, then the place A is inert in E/F. The Artin automorphism σ_A at A satisfies*

$$\sigma_A(x) \equiv x^{q^\ell} \pmod{A'} \tag{4.2}$$

for all $x \in \mathcal{O}_{A'}$, where A' is the unique place of E lying above A.

Proof. By Galois theory, $[E : F] = |G|/|H| = b$. Since G is abelian, E/F is Galois with Galois group isomorphic to G/H. Since $E \subset K$, and M is totally ramified in K, it must also be totally ramified in E. The only other place ramified in K is P_∞, and since H contains the decomposition group $\mathbb{F}_q^*$ of P_∞, P_∞ must split completely in E/F.

The genus of E is easily computed since E/F is a tamely ramified extension [21, Sec. III.5]. Since only the place M of degree d is ramified, we have $2g_E - 2 = d(b-1)$.

Since $H \supset \mathbb{F}_r[T]$, for $\beta \in \mathbb{F}_r$, the Artin automorphism $\sigma_{T-\beta}$ of the place $T-\beta$ in K/F belongs to H. The Artin automorphism of $T-\beta$ in the extension E/F is the restriction of $\sigma_{T-\beta}$ to E, which is trivial since H fixes E. It follows that $T-\beta$ splits completely in E.

For an irreducible polynomial $A \in R_T$ which has order $q^d - 1$ modulo M, by part (3) of Proposition 2.2, the place A remains inert in the extension K/F, and therefore also in the sub-extension E/F. Since the degree of the place A equals ℓ, (4.2) follows from the definition of the Artin automorphism at A. □

4.3. **A generator for E and its properties.** We would like to represent elements of E and be able to evaluate them at the places above $T-\beta$. To this end, we will exhibit a $\mu \in F^{\mathrm{ac}}$ such that $E = F(\mu)$ along with defining equation for μ (which will then aid in the evaluations of μ at the requisite places).

Theorem 4.3. *Let λ be an arbitrary nonzero element of Λ_M (so that $K = F(\lambda)$). Define*

$$\mu \stackrel{def}{=} \prod_{\sigma \in H} \sigma(\lambda) = C_{A^b}(\lambda) C_{A^{2b}}(\lambda) \cdots C_{A^{q^d-1}}(\lambda) \ . \tag{4.3}$$

Then, the fixed field K^H equals $E = F(\mu)$. The minimal polynomial $h(Z) \in R_T[Z]$ of μ over F is given by

$$h(Z) = \prod_{j=0}^{b-1} (Z - \Gamma^j(\mu)) \ .$$

Further, the polynomial $h(Z)$ can be computed in $q^{O(d)}$ time.

Proof. By definition μ is fixed by each $\pi \in H$ and so $\mu \in E$. Therefore $F(\mu) \subseteq E$.

To show $E = F(\mu)$, we will argue that $[F(\mu) : F] = b$, which in turn follows if we show that $h(Z)$ has coefficients in F and is irreducible over F. Since $\Gamma^b(\mu) = \mu$ and thus $\Gamma^j(\mu)$ only depends on $j \mod b$, all symmetric functions of $\{\Gamma^j(\mu)\}_{j=0}^{b-1}$ are fixed by Γ, and thus also by all of $\mathrm{Gal}(K/F)$. The coefficients of $h(Z)$ must therefore belong to F. The lemma actually claims that the coefficients lie in R_T. To see this, note that for $j = 0, 1, \ldots, b-1$,

$$\Gamma^j(\mu) = \prod_{\substack{0 \leqslant i < q^d - 1 \\ i \mod b = j}} \Gamma^i(\lambda) = \prod_{\substack{0 \leqslant i < q^d - 1 \\ i \mod b = j}} C_{A^i}(\lambda) \ . \tag{4.4}$$

Since λ and all its Galois conjugates $C_{A^i}(\lambda)$ are integral over F, each $\Gamma^j(\mu)$ is integral over F, and thus so is each coefficient of $h(Z)$. But since we already know they belong to F, the coefficients must in fact lie in R_T.

We will prove $h(Z)$ is irreducible over F by showing that it is an Eisenstein polynomial with respect to the place M. Since $\mu = \lambda \times \prod_{\sigma \in H, \sigma \neq 1} \sigma(\lambda)$, for each j, $0 \leqslant j < b$, $\Gamma^j(\mu)$ is divisible by $\Gamma^j(\lambda)$ in the ring $R_T[\lambda]$. Now $\Gamma^j(\lambda) = C_{A^j}(\lambda)$ which is divisible by λ. By Proposition 2.2, $\lambda \in \tilde{M}$, and hence each coefficient of $h(Z)$ belongs to the ideal $F \cap \tilde{M} = M$. (A reminder that we are using M to denote both the polynomial in R_T and its associated place.) Therefore, all coefficients of $h(Z)$ except the leading coefficient are divisible by M.

The constant term of $h(Z)$ equals

$$\prod_{j=0}^{b-1} \Gamma^j(\mu) = \prod_{j=0}^{b-1} \prod_{\sigma\in H} \Gamma^j(\sigma(\lambda)) = \prod_{j=0}^{b-1} \prod_{0\leqslant i<(q^d-1)/b} \Gamma^{bi+j}(\lambda) = \prod_{\pi\in G} \pi(\lambda) = M \tag{4.5}$$

where the last step follows since the minimal polynomial of λ over F is $\prod_{\pi\in G}(Z-\pi(\lambda))$, but the minimal polynomial is also $C_M(Z)/Z$ which has M as the constant term. Thus the constant term of $h(Z)$ is not divisible by M^2. By Eisenstein's criterion, we conclude that $h(Z)$ must be irreducible over F.

Finally, we turn to how the coefficients of $h(Z)$ can be computed efficiently. By the expression (4.4), we can compute $\Gamma^j(\mu)$ for $0 \leqslant j \leqslant b-1$ as a formal polynomial in λ with coefficients from R_T. We can divide this polynomial by the monic polynomial $C_M(\lambda)/\lambda$ (formally, over the polynomial ring $R_T[\lambda]$) and represent $\Gamma^j(\mu)$ as a polynomial of degree less than (q^d-1) in λ. Using this representation, we can compute the polynomials $h^{(i)}(Z) = \prod_{j=0}^{i}(Z-\Gamma^j(\mu))$ for $1 \leqslant i \leqslant b-1$ iteratively, as an element of $R_T[\lambda][Z]$, with all coefficients having degree less than (q^d-1) in λ. When $i = b-1$, we would have computed $h(Z)$ — we know at the end all the coefficients will have degree 0 in λ and belong to R_T. □

By Equation (4.5) in the above argument, and the fact that $v_{M'}(\Gamma^j(\mu)) = v_{M'}(\mu)$, we conclude that $v_{M'}(\mu) = 1$, i.e. μ (as well as each of its Galois conjugates $\Gamma^j(\mu)$) is M'-prime. We record this fact below. It will be used to prove that the integral closure of R_T in E equals $R_T[\mu]$ (Proposition 5.2), en route characterizing the message space in Theorem 5.1.

Lemma 4.4. *The element μ has a simple zero at M', i.e., $v_{M'}(\mu) = 1$.*

With the minimal polynomial $h(Z)$ of μ at our disposal, we turn to computing the evaluations of μ at the b places above $T-\beta$, call them $P_j^{(\beta)}$ for $j = 0, 1, \ldots, b-1$, for each $\beta \in \mathbb{F}_r$. (Recall that the place $T-\beta$ splits completely in E/F by Proposition 4.2, Part (v).) The following lemma identifies the set of evaluations of μ at these places. This method is related to Kummer's theorem on splitting of primes [21, Sec. III.3].

Lemma 4.5. *Consider the polynomial $\bar{h}^{(\beta)}(Z) \in \mathbb{F}_q[Z]$ obtained by evaluating the coefficients of $h(Z)$, which are polynomials in T, at β. Then $\bar{h}^{(\beta)}(Z) = \prod_{j=0}^{b-1}(Z-\mu(P_j^{(\beta)}))$. In particular, the set of evaluations of μ at the places above $(T-\beta)$ equals the roots of $\bar{h}^{(\beta)}$ in $\mathbb{F}_q$, and can be computed in $b^{O(1)}$ time given $h \in R_T[Z]$.*

Proof. We know $h(Z) = \prod_{j=0}^{b-1}(Z-\Gamma^j(\mu))$. Therefore

$$\bar{h}^{(\beta)}(Z) = \prod_{j=0}^{b-1}(Z-\Gamma^j(\mu)(P_0^{(\beta)})) = \prod_{j=0}^{b-1}\Big(Z-\mu\big(\Gamma^{-j}(P_0^{(\beta)})\big)\Big) = \prod_{j=0}^{b-1}(Z-\mu(P_j^{(\beta)}))$$

where the last step uses the fact that $\Gamma^{-j}(P_0^{(\beta)})$ for $j = 0, 1, \ldots, b-1$ is precisely the set of places above $T-\beta$. □

5. Code construction from cyclotomic function field

We will now describe the algebraic-geometric codes based on the function field E. A tempting choice for the message space is perhaps $\{\sum_{i=0}^{b-1} a_i(T)\mu^i\} \subset R_T[\mu]$ where $a_i(T)$ are polynomials of some bounded degree. This is certainly a $\mathbb{F}_q$-linear space and messages in this space have no poles outside the places lying above P_∞. However, the valuations of μ at these places is complicated (one needs the Newton polygon method to estimate these [19, Sec. 12.4]), and since μ has both zeroes and poles amongst these places, it is hard to get good bounds on the total pole order of such messages at each of the places above P_∞.

5.1. **Message space.** Let M' be the unique totally ramified place M' in E lying above M; $\deg(M') = \deg(M) = d$. We will use as message space elements of $R_T[\mu]$ that have no more than a certain number ℓ of poles at the place M' and no poles elsewhere. These can equivalently be thought of (via a natural correspondence) as elements of E that have bounded (depending on ℓ) pole order at each place above P_∞, and no poles elsewhere, and we can develop our codes and algorithms in this equivalent setting. Since the literature on AG codes typically focuses on one-point codes where the messages have poles at a unique place, we work with functions with poles restricted to M'.

Formally, for an integer $\ell \geqslant 1$, let $\mathcal{L}(\ell M')$ be the space of functions in E that have no poles outside M' and at most ℓ poles at M'. $\mathcal{L}(\ell M')$ is an $\mathbb{F}_q$-vector space, and by the Riemann-Roch theorem, $\dim(\mathcal{L}(\ell M')) \geqslant \ell d - g + 1$, where $g = d(b-1)/2 + 1$ is the genus of E. We will assume that $\ell \geqslant b$, in which case $\dim(\mathcal{L}(\ell M')) = \ell d - g + 1$.

We will represent the code by a basis of $\mathcal{L}(\ell M')$ over $\mathbb{F}_q$. Of course, we first need to understand how to represent a single function in $\mathcal{L}(\ell M')$. The following lemma suggest a representation for elements of $\mathcal{L}(\ell M')$ that we can use.

Theorem 5.1. *A function f in E with poles only at M' has a unique representation of the form*

$$f = \frac{\sum_{i=0}^{b-1} a_i \mu^i}{M^e} \tag{5.1}$$

where $e \geqslant 0$ is an integer, each $a_i \in R_T$, and not all the a_i's are divisible by M (as polynomials in T).

Proof. If f has poles only at M', there must be a smallest integer $e \geqslant 0$ such that $M^e f$ has no poles outside the places above P_∞. This means that $M^e f$ must be in the integral closure ("ring of integers") of R_T in E, i.e., the minimal polynomial of $M^e f$ over R_T is monic. The claim will follow once we establish that the integral closure of R_T in E equals $R_T[\mu]$, which we show next in Proposition 5.2. The uniqueness follows since $\{1, \mu, \ldots, \mu^{b-1}\}$ forms a basis of E over F. ∎

Proposition 5.2. *The integral closure of R_T in E equals* $R_T[\mu] = \left\{\sum_{i=0}^{b-1} a_i \mu^i \;\mid\; a_i \in R_T\right\}$.

Proof. The minimal polynomial $h(Z)$ of μ over R_T is monic (Theorem 4.3). Thus μ is integral over R_T, and so $R_T[\mu]$ is contained in the integral closure of R_T in E. We turn to proving the reverse inclusion. The proof follows along the lines of a similar argument used to prove that the integral closure of R_T in $K = F(\lambda)$ equals $R_T[\lambda]$ [18, Prop. 12.9]. Let $\omega \in E$ be integral over R_T. We know that $\{1, \mu, \mu^2, \dots, \mu^{b-1}\}$ is a basis for E over F. Also μ, and therefore each μ^i, is integral over F. By virtue of these facts, it is known (see, for example, [13, Chap. 2]) that there exist $a_i \in R_T$ such that $\omega = \frac{1}{\Delta}\sum_{i=0}^{b-1} a_i\mu^i$ where $\Delta \in R_T$ is the *discriminant* of the extension E/F. As M is the only ramified place in the extension E/F, the discriminant Δ is a power of M up to units, and by assuming wlog that Δ is monic, we can conclude that $\Delta = M^{e'}$ for some exponent $e' \geqslant 0$. Thus we have

$$M^{e'}\omega = \sum_{i=0}^{b-1} a_i\mu^i \tag{5.2}$$

with $a_i \in R_T$, and not all the a_i's are divisible by M.

Our goal is to show that $e' = 0$. We will do this by comparing the valuations $v_{M'}$ of the both sides of (5.2). We have

$$v_{M'}(M^{e'}\omega) = v_{M'}(M^{e'}) + v_M(\omega) = be' + v_M(\omega) \geqslant be' \ . \tag{5.3}$$

Let i_0, $0 \leqslant i_0 < b$, be the smallest value of i such that $v_M(a_i) = 0$. Such an i_0 must exist since not all the a_i's are divisible by M. By Lemma 4.4, $v_{M'}(\mu) = 1$, and so

$$v_{M'}(a_i\mu^i) = v_{M'}(a_i) + i = bv_M(a_i) + i \ .$$

For $i = i_0$, $v_{M'}(a_{i_0}\mu^{i_0}) = i_0$. For $i < i_0$, $v_{M'}(a_i\mu^i) \geqslant bv_M(a_i) \geqslant b > i_0$ (since $v_M(a_i) \geqslant 1$ for $i < i_0$). For $i > i_0$, $v_{M'}(a_i\mu^i) \geqslant v_{M'}(\mu^i) = i > i_0$. It follows that

$$v_{M'}\Big(\sum_{i=0}^{b-1} a_i\mu^i\Big) = \min_{0\leqslant i\leqslant b-1} v_{M'}(a_i\mu^i) = i_0 \tag{5.4}$$

Combining (5.3) and (5.4), we conclude $b > i_0 \geqslant be'$ which implies $e' = 0$. □

5.2. **Succinctness of representation.** In order to be able to efficiently compute with the representation (5.1) of functions in $\mathcal{L}(\ell M')$, we need the guarantee that the representation will be *succinct*, i.e., of size polynomial in the code length. We show that this will be the case by obtaining an upper bound on the degree of the coefficients $a_i \in R_T$ in Lemma 5.3 below. This is not as straightforward as one might hope, and we thank G. Anderson and D. Thakur for help with its proof. For the choice of parameters we will make (in Theorems 6.10 and 7.1), this upper bound will be polynomially bounded in the code length. Therefore, the assumed representation of the basis functions is of polynomial size.

Lemma 5.3. *Suppose $f \in \mathcal{L}(\ell M')$ is given by $f = \frac{1}{M^e}\sum_{i=0}^{b-1} a_i\mu^i$ for $a_i \in R_T$ (not all divisible by M) and $e \geqslant 0$. Then the degree of each a_i is at most $\ell + q^d b$.*

Proof. Let $g = M^e f = \sum_{i=0}^{b-1} a_i\mu^i$. We know that g has at most eb poles at each place of E that lies above P_∞ (since f has no poles at these places). Using the fact that f has at most ℓ poles at M', and the uniqueness of the representation $f = \frac{1}{M^e}\sum_{i=0}^{b-1} a_i\mu^i$, it is easy to argue that $eb \leqslant \ell + b$. So, g has at most $\ell + b$ poles at each place of E lying above P_∞.

Let $\sigma = \sigma_A$; we know that σ is a generator of $\mathrm{Gal}(E/F)$. For $j = 0, 1, \dots, b-1$, we have $\sigma^j(g) = \sum_{i=0}^{b-1} a_i\sigma^j(\mu^i)$. Let $\mathbf{a} = (a_0, a_1, \dots, a_{b-1})^T$ be the (column) vector of coefficients, and let $\mathbf{g} = (g, \sigma(g), \ldots, \sigma^{b-1}(g))^T$. Denoting by Φ the $b \times b$ matrix with $\Phi_{ji} = \sigma^j(\mu^i)$ for $0 \leqslant i, j \leqslant b-1$, we have the system of equations $\Phi\mathbf{a} = \mathbf{b}$.

We can thus determine the coefficients a_i by solving this linear system. By Cramer's rule, $a_i = \det(\Phi_i)/\det(\Phi)$ where Φ_i is obtained by replacing the i'th column of Φ by the column vector $\mathbf{g}$. The square of the denominator $\det(\Phi)$ is the discriminant of the field extension E/F, and belongs to R_T. Thus the degree of a_i is at most the pole order of $\det(\Phi_i)$ at an arbitrary place, say $\tilde{P}$, above P_∞. By the definition (4.3) of μ, and the fact that λ and its conjugates have at most one pole at the places above P_∞ in $F(\Lambda_M)$, it follows that μ has at most $(q^d-1)/b$ poles at $\tilde{P}$. The same holds for all its conjugates $\sigma^j(\mu)$. The function g and its conjugates $\sigma^j(g)$ have at most $\ell + b$ poles at $\tilde{P}$. In all, this yields a crude upper bound of

$$\frac{q^d-1}{b}\frac{(b-1)b}{2} + \ell + b \leqslant \ell + q^d b$$

for the pole order of $\det(\Phi_i)$ at $\tilde{P}$, and hence also the degree of the polynomial $a_i \in R_T$. $\square$

5.3. **Rational places for encoding and their ordering.** So far, the polynomial $A \in R_T$ was any monic irreducible polynomial that was a primitive element modulo M, so that its Artin automorphism σ_A generates $\mathrm{Gal}(E/F)$. We will now pick A to have degree D satisfying $D > \frac{\ell d}{b}$. This can be done by a Las Vegas algorithm in $(Dq^d)^{O(1)}$ time by picking a random polynomial and checking that it works, or deterministically by brute force in $q^{O(d+D)}$ time. Either of these lies within the decoding time claimed in Theorem 6.10, and will be polynomial in the block length for our parameter choices in Theorem 7.1. By Proposition 2.1, A remains inert in E/F, and let us denote by A' the unique place of E that lies over A. The degree of A' equals Db.

For each $\beta \in \mathbb{F}_r$, fix an arbitrary place $P_0^{(\beta)}$ lying above $T - \beta$ in E. For $j = 0, 1, \ldots, b-1$, define

$$P_j^{(\beta)} = \sigma_A^{-j}(P_0^{(\beta)}) \; . \tag{5.5}$$

Since $\mathrm{Gal}(E/F)$ acts transitively on the set of primes above a prime, and σ_A generates $\mathrm{Gal}(E/F)$, these constitute all the places above $T - \beta$. Lemma 4.5 already tells us the *set* of evaluations of μ at these places, but not which evaluation corresponds to which point. We have $\mu(\sigma_A^{-j}(P_0^{(\beta)})) = \sigma_A^j(\mu)(P_0^{(\beta)})$; hence, to compute the evaluations of μ at all these b places as per the ordering (5.5), it suffices to know

(i) the value at $\mu(P_0^{(\beta)})$, which we can find by simply picking one one of the roots from Lemma 4.5 arbitrarily, and
(ii) a representation of $\sigma_A(\mu)$ as an element of $R_T[\mu]$ (since $\sigma_A(\mu)$ is integral over R_T, it belongs to $R_T[\mu]$ by virtue of Proposition 5.2). Note that $T(P_0^{(\beta)}) = \beta$, so once we know $\mu(P_0^{(\beta)})$, we can evaluate any element of $R_T[\mu]$ at $P_0^{(\beta)}$.

We now show that $\sigma_A(\mu) \in R_T[\mu]$ can be computed efficiently.

Lemma 5.4. (i) *The values of $\sigma_A^j(\mu)$ for $0 \leqslant j \leqslant b-1$ as elements of $R_T[\mu]$ can be computed in $q^{O(d)}$ time.*

(ii) *The values $\mu(P_j^{(\beta)})$ for $\beta \in \mathbb{F}_r$ and $j = 0, 1, \ldots, b-1$ can be computed in $q^{O(d)}$ time. Knowing these values, we can compute any function in the message space $\mathcal{L}(\ell M')$ represented in the form (5.1) at the places $P_j^{(\beta)}$ in $\mathrm{poly}(\ell, q^d)$ time.*

Proof. Part (ii) follows from Part (i) and the discussion above. To prove Part (i), note that once we compute $\sigma_A(\mu)$, we can recursively compute $\sigma_A^j(\mu)$ for $j \geqslant 2$, using the relation $h(\mu) = 0$ to replace μ^b and higher powers of μ in terms of $1, \mu, \ldots, \mu^{b-1}$. By definition (4.3), we have $\mu = \prod_{0 \leqslant i < (q^d-1)/b} C_{A^{ib} \bmod M}(\lambda)$. Thus one can compute an expression $\mu = \sum_{i=0}^{q^d-2} e_i \lambda^i \in R_T[\lambda]$ with coefficients $e_i \in R_T$ in $q^{O(d)}$ time. By successive multiplication in the ring $R_T[\lambda]$ (using the relation $C_M(\lambda) = 0$ to express λ^{q^d-1} and higher powers in terms of $1, \lambda, \ldots, \lambda^{q^d-2}$), we can compute, for $l = 0, 1, \ldots, b-1$, expressions $\mu^l = \sum_{i=0}^{q^d-2} e_{il} \lambda^i$ with $e_{il} \in R_T$ in $q^{O(d)}$ time.

We have $\sigma_A(\mu) = \sum_{i=0}^{q^d-2} e_i \sigma_A(\lambda)^i = \sum_{i=0}^{q^d-2} e_i C_{A \bmod M}(\lambda)^i$. So one can likewise compute an expression $\sigma_A(\mu) = \sum_{i=0}^{q^d-2} f_i \lambda^i$ with $f_i \in R_T$ in $q^{O(d)}$ time. The task now is to re-express this expression for $\sigma_A(\mu)$ as an element of $R_T[\mu]$, of the form $\sum_{l=0}^{b-1} a_l \mu^l$, for "unknowns" $a_l \in R_T$ that are to be determined. We will argue that this can be accomplished by solving a linear system.

Indeed, using the above expressions $\mu^l = \sum_{i=0}^{q^d-2} e_{il} \lambda^i$, the coefficients a_l satisfy the following system of linear equations over R_T:

$$\sum_{l=0}^{b-1} e_{il} a_l = f_i \quad \text{for} \quad i = 0, 1, \ldots, q^d - 2 \;. \tag{5.6}$$

Since the representation $\sigma_A(\mu) = \sum_{l=0}^{b-1} a_l \mu^l$ is unique, the system has a unique solution. By Cramer's rule, the degree of each a_l is at most $q^{O(d)}$. Therefore, we can express the system (5.6) as a linear system of size $q^{O(d)}$ over $\mathbb{F}_q$ in unknowns the coefficients of all the polynomials $a_l \in R_T$. By solving this system in $q^{O(d)}$ time, we can compute the representation of $\sigma_A(\mu)$ as an element of $R_T[\mu]$. $\square$

5.4. **The basic cyclotomic AG code.** The basic AG code $\mathcal{C}^0$ based on subfield E of the cyclotomic function field $F(\Lambda_M)$ is defined as

$$\mathcal{C}^0 = \left\{ \left(f(P_j^{(\beta)}) \right)_{\beta \in F_r, 0 \leqslant j < b} \;\middle|\; f \in \mathcal{L}(\ell M') \right\} \tag{5.7}$$

where the ordering of the places $P_j^{(\beta)}$ above $T - \beta$ is as in (5.5). We record the standard parameters of the above algebraic-geometric code, which follows from Riemann-Roch, the genus of E from Proposition 4.2, and the fact a nonzero $f \in \mathcal{L}(\ell M')$ can have at most $\ell \cdot \deg(M') = \ell d$ zeroes.

Lemma 5.5. *Let $\ell \geqslant b$. $\mathcal{C}^0$ is an $\mathbb{F}_q$-linear code of block length $n = rb$, dimension $k = \ell d - d(b-1)/2$, and distance at least $n - \ell d$.*

Lemma 5.4, Part (ii), implies the following.

Lemma 5.6 (Efficient encoding)**.** *Given a basis for the message space $\mathcal{L}(\ell M')$ represented in the form (5.1), the generator matrix of the cyclotomic code $\mathcal{C}^0$ can be computed in* $\mathrm{poly}(\ell, q^d, q^D)$ *time.*

5.5. **The folded cyclotomic code.** Let $m \geqslant 1$ be an integer. For convenience, we assume $m|b$ (though this is not really necessary). Analogous to the construction of folded Reed-Solomon codes [6], the folded cyclotomic code $\mathcal{C}$ is obtained from $\mathcal{C}^0$ by bundling together successive m-tuples of symbols into a single symbol to give a code of length $N = n/m$ over $\mathbb{F}_q^m$. Formally,

$$\mathcal{C} = \left\{ \left(f(P^{(\beta)}_{m\imath}), f(P^{(\beta)}_{m\imath+1}), \cdots, f(P^{(\beta)}_{m\imath+m-1}) \right)_{\beta \in F_r, 0 \leqslant \imath < b/m} \;\mid\; f \in \mathcal{L}(\ell M') \right\} \tag{5.8}$$

We will index the N positions of codewords in $\mathcal{C}$ by pairs $(\beta, \imath)$ for $\beta \in \mathbb{F}_r$ and $\imath \in \{0, 1, \ldots, \frac{b}{m} - 1\}$.

The generator matrix of unfolded code $\mathcal{C}^0$, which can be computed given a basis for $\mathcal{L}(\ell M')$ as per Lemma 5.6, obviously suffices for encoding. We will later on argue that the *same representation* also suffices for polynomial time list decoding.

5.6. **Folding and Artin-Frobenius automorphism.** The unique place A' lying above A has degree $D' \stackrel{\text{def}}{=} Db$. The residue field at A', denote it $K_{A'}$, is isomorphic to $\mathbb{F}_{q^{D'}}$. By our choice $Db > \ell d$. This immediately implies a message in $\mathcal{L}(\ell M')$ is uniquely determined by its evaluation at A'.

Lemma 5.7. *The map $\mathsf{ev}_{A'} : \mathcal{L}(\ell M') \to K_{A'}$ given by $\mathsf{ev}_{A'}(f) = f(A')$ is one-one.*

The key algebraic property of our folding is the following.

Lemma 5.8. *For every $f \in \mathcal{L}(\ell M')$:*

(i) *For every $\beta \in \mathbb{F}_r$ and $0 \leqslant j < b - 1$, $\sigma_A(f)(P^{(\beta)}_j) = f(P^{(\beta)}_{j+1})$.*
(ii) $\sigma_A(f)(A') = f(A')^{q^D}$.

Proof. The first part follows since we ordered the places above $T - \beta$ such that $P^{(\beta)}_{j+1} = \sigma_A^{-1}(P^{(\beta)}_j)$.

The second part follows from the property of the Artin automorphism at A, since the norm of the place A equals $q^{\deg(A)} = q^D$. (A nice discussion of the Artin-Frobenius automorphism, albeit in the setting of number fields, appears in [13, Chap. 4].) □

6. List decoding algorithm

We now turn to list decoding the folded cyclotomic code $\mathcal{C}$ defined in (5.8). The underlying approach is similar to that of the algorithm for list decoding folded RS codes [6] and algebraic-geometric generalizations of Parvaresh-Vardy codes [16, 5]. We will therefore not repeat the entire rationale and motivation behind the algorithm development. But our technical presentation and analysis is self-contained. In fact, our presentation here does offer some simplifications over previous descriptions of AG list decoding algorithms from [7, 8, 5]. A principal strength of the new description is that it *avoids the use of zero-increasing bases* at each code place $P_j^{(\beta)}$. This simplifies the algorithm as well as the representation of the code needed for decoding.

The list decoding problem for $\mathcal{C}$ up to e errors corresponds to solving the following function reconstruction problem. Recall that the length of the code is $N = n/m = rb/m$, and the codeword positions are indexed by $\mathbb{F}_r \times \{0, 1, \ldots, \frac{b}{m} - 1\}$.

Input: Collection $\mathcal{T}$ of N tuples $\left(y_{m\imath}^{(\beta)}, y_{m\imath+1}^{(\beta)}, \cdots, y_{m\imath+m-1}^{(\beta)}\right) \in \mathbb{F}_q^m$ for $\beta \in \mathbb{F}_r$ and $0 \leqslant \imath < b/m$

Output: A list of all $f \in \mathcal{L}(\ell M')$ whose encoding as per $\mathcal{C}$ agrees with the $(\beta, \imath)$'th tuple for at least $N - e$ codeword positions.

6.1. **Algorithm description.** We describe the algorithm at a high level below and later justify how the individual steps can be implemented efficiently, and under what condition the decoding will succeed. We stress that regardless of complexity considerations, even the *combinatorial* list-decodability property "proved" by the algorithm is non-trivial.

Algorithm List-Decode($\mathcal{C}$): (uses the following parameters):

- an integer parameter s, $2 \leqslant s \leqslant m$, for s-variate interpolation
- an integer parameter $w \geqslant 1$ that governs the zero order (multiplicity) guaranteed by interpolation
- an integer parameter $\Delta \geqslant 1$ which is the total degree of the interpolated s-variate polynomial

Step 1: (Interpolation) Find a nonzero polynomial $Q(Z_1, Z_2, \ldots, Z_s)$ of total degree at most Δ with coefficients in $\mathcal{L}(\ell M')$ such that for each $\beta \in \mathbb{F}_r$, $0 \leqslant \imath < b/m$, and $j' \in \{0, 1, \ldots, m - s\}$, the shifted polynomial

$$Q\big(Z_1 + y_{m\imath+j'}^{(\beta)}, Z_2 + y_{m\imath+j'+1}^{(\beta)}, \cdots, Z_s + y_{m\imath+j'+s-1}^{(\beta)}\big) \tag{6.1}$$

has the property that the coefficient of the monomial $Z_i^{n_1} Z_2^{n_2} \cdots Z_s^{n_s}$ vanishes at $P_{m\imath+j'}^{(\beta)}$ whenever its total degree $n_1 + n_2 + \cdots + n_s < w$.

Step 2: (Root-finding) Find a list of all $f \in \mathcal{L}(\ell M')$ satisfying

$$Q(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f)) = 0 \ .$$

Output those whose encoding as per the code $\mathcal{C}$ agrees with at least $N - e$ of the m-tuples in $\mathcal{T}$.

6.2. **Analysis of error-correction radius.**

Lemma 6.1. *If $k(\Delta + 1)^s \geqslant N(m - s + 1)(w + s - 1)^s$ (where, recall, $k = \ell d - d(b-1)/2$ is the dimension of $\mathcal{L}(\ell M')$), then a nonzero polynomial Q with the stated properties exists. If we know the evaluations of the functions in a basis $\{\phi_1, \phi_2, \ldots, \phi_k\}$ of $\mathcal{L}(\ell M')$ at the places*

$P_j^{(\beta)}$, then such a Q can be found by solving a homogeneous system of linear equations over $\mathbb{F}_q$ with at most $Nm(w+s)^s$ equations and unknowns.

Proof. The proof is standard and follows by counting degrees of freedom vs. number of constraints. One can express the desired polynomial as $\sum_{n_1,n_2,\dots,n_s} q_{(n_1,\dots,n_s)} Z_1^{n_1}\cdots Z_s^{n_s}$ with unknowns $q_{(n_1,\dots,n_s)} \in \mathbb{F}_q$. The number of coefficients is $k\binom{\Delta+s}{s} > k(\Delta+1)^s/s!$. For each place $P_{m\imath+j'}^{(\beta)}$, one can express the required condition at that place by $\binom{w+s-1}{s}$ linear conditions (this quantity is the number of monomials of total degree $< w$), for a total of

$$N(m-s+1)\binom{w+s-1}{s} < N(m-s+1)\frac{(w+s-1)^s}{s!}$$

constraints. When the number of unknowns exceeds the number of constraints, a nonzero solution must exist. A solution can also be found efficiently once the linear system is set up, which can clearly be done if we know the evaluations of ϕ_i's at the code places (i.e., a "generator matrix" of the code). $\square$

Lemma 6.2. *Let Q be the polynomial found in Step 1. If the encoding of some f as per $\mathcal{C}$ agrees with $\big(y_{m\imath}^{(\beta)}, y_{m\imath+1}^{(\beta)}, \cdots, y_{m\imath+m-1}^{(\beta)}\big)$ for some position $(\beta,\imath)$, then $Q(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f))$ has at least w zeroes at each of the $(m-s+1)$ places $P_{m\imath+j'}^{(\beta)}$ for $j'=0,1,\dots,m-s$.*

Proof. The proof differs slightly from earlier proofs of similar statements (eg., [5, Lemma 6.6]) in that it avoids the use of zero-increasing bases and is thus simpler. We will prove the claim for $j'=0$, and the same proof works for any $j' \leqslant m-s$. Note that agreement on the m-tuple at position $(b,\imath)$ implies that

$$f(P_{m\imath}^{(\beta)}) = y_{m\imath}^{(\beta)},\ f(P_{m\imath+1}^{(\beta)}) = y_{m\imath+1}^{(\beta)},\ \cdots,\ f(P_{m\imath+s-1}^{(\beta)}) = y_{m\imath+s-1}^{(\beta)}\ .$$

By Lemma 5.8, Part (i), this implies

$$f(P_{m\imath}^{(\beta)}) = y_{m\imath}^{(\beta)},\ \sigma_A(f)(P_{m\imath}^{(\beta)}) = y_{m\imath+1}^{(\beta)},\ \cdots,\ \sigma_{A^{s-1}}(f)(P_{m\imath}^{(\beta)}) = y_{m\imath+s-1}^{(\beta)}\ .$$

Denote by Q^* the shifted polynomial (6.1) for the triple $(\beta,\imath,0)$. We have

$$\begin{aligned} Q\big(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f)\big) =\ & Q^*\big(f-y_{m\imath}^{(\beta)}, \sigma_A(f)-y_{m\imath+1}^{(\beta)}, \cdots, \sigma_A^{s-1}(f)-y_{m\imath+s-1}^{(\beta)}\big) \\ = \sum_{\substack{n_1,n_2,\dots,n_s \\ w\leqslant n_1+\cdots+n_s\leqslant\Delta}} & q^*_{(n_1,\dots,n_s)}\big(f-f(P_{m\imath}^{(\beta)})\big)^{n_1}\big(\sigma_A(f)-\sigma_A(f)(P_{m\imath}^{(\beta)})\big)^{n_2}\cdots\big(\sigma_{A^{s-1}}(f)-\sigma_{A^{s-1}}(f)(P_{m\imath}^{(\beta)})\big)^{n_s}\ . \end{aligned}$$

for some coefficients $q^*_{(n_1,\dots,n_s)} \in \mathbb{F}_q$. Each term of the function in the last expression clearly has valuation at least w at $P_{m\imath}^{(\beta)}$, and hence so does $Q\big(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f)\big)$. $\square$

Lemma 6.3. *If the encoding of $f \in \mathcal{L}(\ell M')$ has at least $N-e$ agreements with the input tuples $\mathcal{T}$, and $(N-e)(m-s+1)w > d\ell(\Delta+1)$, then $Q(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f)) = 0$.*

Proof. Since f has no poles outside M', neither do $\sigma_{A^i}(f)$ for $1 \leqslant i < s$. Moreover, $v_{M'}(\sigma_A(f)) = v_{\sigma_A^{-1}(M')}(f) = v_{M'}(f)$ (since M' is the unique place above M and is thus fixed by every Galois automorphism). Since $f \in \mathcal{L}(\ell M')$, this implies $\sigma_{A^i}(f) \in \mathcal{L}(\ell M')$ for every i. Since each coefficient of Q also belongs to $\mathcal{L}(\ell M')$, we conclude that $Q(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f)) \in \mathcal{L}((\ell+\ell\Delta)M')$. On the other hand, by Lemma 6.2, $Q(f,\sigma_A(f),\dots,\sigma_{A^{s-1}}(f))$ has at least

$(N-e)(m-s+1)w$ zeroes. If $(N-e)(m-s+1)w > \ell(\Delta+1)d$, then $Q(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f))$ has more zeroes than poles and must thus equal 0. $\square$

Putting together the above lemmas, we can conclude the following about the list decoding radius guaranteed by the algorithm. Note that we have not yet discussed how Step 2 may be implemented, or why it implies a reasonable bound on the output list size. We will do this in Section 6.3.

Theorem 6.4. *For every s, $2 \leqslant s \leqslant m$, and any $\zeta > 0$, for the choice $w = \lceil s/\zeta \rceil$ and a suitable choice of the parameter Δ, the algorithm* List-Decode($\mathcal{C}$) *successfully list decodes up to e errors whenever*

$$e < (N-1) - (1+\zeta)\left(\frac{k}{m-s+1}\right)^{1-1/s} N^{1/s}\left(1 + \frac{d(b-1)}{2k}\right) . \tag{6.2}$$

Proof. Picking $w = \lceil s/\zeta \rceil$ and $\Delta + 1 = \left\lceil \left(\frac{N(m-s+1)}{k}\right)^{1/s}(w+s-1)\right\rceil$, the requirement of Lemma 6.1 is met. By Lemma 5.5, the dimension k satisfies $\ell d = k + d(b-1)/2$. A straightforward computation reveals that for this choice, the bound (6.2) implies the decoding condition $(N-e)(m-s+1)w > \ell d(\Delta+1)$ under which Lemma 6.3 guarantees successful decoding. $\square$

Remark 6.5. The above error-correction radius is non-trivial only when $s \geqslant 2$. We will see later how to pick parameters so that the error fraction approaches $1 - R^{1-1/s}$. For AG codes, even $s = 1$ led to a non-trivial guarantee of about $1 - \sqrt{R}$ in [7], and for folded Reed-Solomon codes the error fraction with s-variate interpolation was $1 - R^{s/(s+1)}$. The weaker bound we get is due to restricting the pole order of coefficients of Q to at most ℓ, the number of poles allowed for messages. This is similar to the algorithm in [5, Sec. 5]. Since we let grow s anyway, this does not hurt us. It also avoids some difficult technical complications that would arise otherwise (discussed, eg. in [5]), and allows implementing the interpolation step just using the natural generator matrix of the code.

6.3. **Root-finding using the Artin automorphism.** So far we have not discussed how Step 2 of decoding can be performed, and why in particular it implies a reasonably small upper bound on the number of solutions $f \in \mathcal{L}(\ell M')$ that it may find in the worst-case. We address this now. This is where the properties of the Artin automorphism σ_A will play a crucial role. Recall (i) $K_{A'} = \mathcal{O}_{A'}/A'$ denotes the residue field at the place A' of E lying above A, and (ii) we picked A so that $D = \deg(A)$ obeyed $Db > \ell d$.

Lemma 6.6. *Suppose $f \in \mathcal{O}_{A'}$ satisfies*

$$Q(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f)) = 0$$

for some $Q \in \mathcal{O}_{A'}[Z_1, Z_2, \ldots, Z_s]$. Let $\overline{Q} \in K_{A'}[Z_1, Z_2, \ldots, Z_s]$ be the polynomial obtained by reducing the coefficients of Q modulo A'. Then $f(A') \in K_{A'}$ obeys

$$\overline{Q}\big(f(A'), f(A')^{q^D}, f(A')^{q^{2D}}, \cdots, f(A')^{q^{D(s-1)}}\big) = 0 . \tag{6.3}$$

Proof. If $Q(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f)) = 0$, then surely $\overline{Q}\big(f(A'), \sigma_A(f)(A'), \cdots, \sigma_{A^{s-1}}(f)(A')\big) = 0$. The claim (6.3) now follows immediately from Lemma 5.8, Part (ii). $\square$

Lemma 6.7. *If $Q(Z_1, \ldots, Z_s)$ is a* nonzero *polynomial of total degree at most $\Delta < q^D$ all of whose coefficients belong to $\mathcal{L}(\ell M')$, then the polynomial $\Phi \in K_{A'}[Y]$ defined as*

$$\Phi(Y) \stackrel{def}{=} \overline{Q}\big(Y, Y^{q^D}, \cdots, Y^{q^{D(s-1)}}\big)$$

is a nonzero *polynomial of degree at most $\Delta \cdot q^{D(s-1)}$.*

Proof. If $\psi \in \mathcal{L}(\ell M')$ is nonzero, then $\psi(A') \neq 0$. (Otherwise, the degree of zero divisor of ψ will be at least $\deg(A') = bD > \ell d$, and thus exceed the degree of the pole divisor of ψ.) It follows that if $Q \neq 0$, then $\overline{Q}(Z_1, \ldots, Z_s)$ obtained by reducing coefficients of Q modulo A' is also nonzero.[3] Since the degree of $\overline{Q}$ in each Z_i is at most $\Delta < q^D$, it is easy to see that $\Phi(Y) = \overline{Q}\big(Y, Y^{q^D}, \cdots, Y^{q^{D(s-1)}}\big)$ is also nonzero. The degree of Φ is at $q^{D(s-1)}$ times the total degree of $\overline{Q}$, which is at most Δ. $\square$

By the above two lemmas, we see that one can compute the set of residues $f(A')$ of all f satisfying $Q(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f)) = 0$ by computing the roots in $K_{A'}$ of $\Phi(Y)$. Since $\mathsf{ev}_{A'}$ is injective on $\mathcal{L}(\ell M')$ (Lemma 5.7), this also lets us recover the message $f \in \mathcal{L}(\ell M')$.

Lemma 6.8. *Given a nonzero polynomial $Q(Z_1, \ldots, Z_s)$ with coefficients from $\mathcal{L}(\ell M')$ and degree $\Delta < q^D$, the set of functions*

$$\mathcal{S} = \{f \in \mathcal{L}(\ell M') \mid Q\big(f, \sigma_A(f), \ldots, \sigma_{A^{s-1}}(f)\big) = 0\}$$

has cardinality at most q^{Ds}.

Moreover, knowing the evaluations of a basis $\mathcal{B} = \{\phi_1, \phi_2, \ldots, \phi_k\}$ of $\mathcal{L}(\ell M')$ at the place A', one can compute the coefficients expressing each $f \in \mathcal{S}$ in the basis $\mathcal{B}$ in $q^{O(Ds)}$ time.

Proof. As argued above, any desired $f \in \mathcal{L}(\ell M')$ has the property that $\Phi(f(A')) = 0$, so the evaluations of functions in $\mathcal{S}$ take at most degree$(\Phi) \leqslant \Delta q^{D(s-1)} \leqslant q^{Ds}$ values. Since $\mathsf{ev}_{A'}$ is injective on $\mathcal{S}$, this implies $|\mathcal{S}| \leqslant q^{Ds}$. The second part follows since we can compute the roots of Φ in $K_{A'}$ in time poly$(q^{Ds}, \log |K_{A'}|) \leqslant q^{O(Ds)}$. Knowing $f(A')$, we can recover f (in terms of the basis $\mathcal{B}$) by solving a linear system if we know the evaluations of the functions in the basis $\mathcal{B}$ at A'. The next section discusses a convenient representation for computations in $K_{A'}$. $\square$

6.3.1. *Representation of the residue field $K_{A'}$.* The following gives a convenient representation for elements of $K_{A'}$ which can be used in computations involving this field.

Lemma 6.9. *The elements $\{1, \mu(A), \ldots, \mu(A)^{b-1}\}$ form a basis for $K_{A'}$ over the field $R_T/(A) \simeq \mathbb{F}_{q^D}$. In other words, elements of $K_{A'}$ can be expressed in a unique way as*

$$\sum_{i=0}^{b-1} b_i(T) \mu(A)^i$$

where each $b_i \in R_T$ has degree less than D.

[3] This is simplicity we gain by restricting the coefficients of Q to also belong to $\mathcal{L}(\ell M')$.

Proof. Since A is inert in E/F, the minimal polynomial $h(Z)$ of μ over F has the property that $\overline{h}(Z)$, obtained by reducing the coefficients of h modulo A, is irreducible over the residue field $R_T/(A)$. Thus $\mu(A)$ generates $K_{A'}$ over $R_T/(A)$, and in fact minimal polynomial of $\mu(A)$ w.r.t to K_A equals $\overline{h}(Z)$. Note that the coefficients of $\overline{h}$, which belong to $R_T/(A)$, have a natural representation as a polynomial in R_T of degree $< \deg(A) = D$. ☐

We note that given the representation of the basis $\mathcal{B} = \{\phi_1, \phi_2, \ldots, \phi_k\}$ in the form guaranteed by Theorem 5.1, one can trivially compute the evaluations of $\phi_i(A')$ in the above form. There is no need to explicitly compute $\mu(A) \in \mathcal{O}_A/A$. Therefore, the decoding algorithm requires no additional pre-processed information beyond a basis for the message space $\mathcal{L}(\ell M')$ — the rest can all be computed efficiently from the basis alone.

6.4. **Wrap-up.** We are now ready to state our final decoding claim.

Theorem 6.10. *For any s, $2 \leqslant s \leqslant m$, and $\zeta > 0$, the folded cyclotomic code $\mathcal{C} \subseteq (\mathbb{F}_q^m)^N$ defined in (5.8) can be list decoded in time $(Nm)^{O(1)}(s/\zeta)^{O(s)} + q^{O(Ds)}$ from a fraction ρ of errors*

$$\rho = 1 - (1+\zeta)\left(\frac{R_0 m}{m-s+1}\right)^{1-1/s}\left(1 + \frac{d}{2R_0 r}\right), \tag{6.4}$$

where $R_0 = k/n$ is the rate of the code. The size of the output list is at most q^{Ds}. The decoding algorithm assumes polynomial amount of pre-processed information consisting of basis functions $\{\phi_1, \ldots, \phi_k\}$ for the message space $\mathcal{L}(\ell M')$ represented in the form (5.1). (Note that this is the same *representation used for encoding, and it is succinct by Lemma 5.3.)*

Proof. We first note that bound on fraction of errors follows from Theorem 6.4, and the fact that $k = R_0 n = R_0 N m = R_0 b r$. By Lemma 6.1 and its proof, in Step 1 of the algorithm we can find a nonzero polynomial Q (of degree $< q^D$) such that for any $f \in \mathcal{L}(\ell M')$ that needs to be output by the list decoder, we must have $Q(f, \sigma_A(f), \cdots, \sigma_{A^{s-1}}(f)) = 0$. We can evaluate the basis functions ϕ_i at $P_j^{(\beta)}$ in $(\ell q^d)^{O(1)}$ time by Lemma 5.4, and with this information, the running time of this interpolation step can be bounded by $(Nm)^{O(1)}(w+s)^{O(s)} = (Nm)^{O(1)}(s/\zeta)^{O(s)}$ (since $w = O(s/\zeta)$). We can also efficiently compute the evaluations of ϕ_i at A' in the representation suggested by Lemma 6.9. Therefore, by Lemma 6.8, we can then find a list of the at most q^{Ds} functions f satisfying $Q(f, \sigma_A(f), \cdots, \sigma_{A^{s-1}}(f)) = 0$ in $q^{O(Ds)}$ time. ☐

Remark 6.11 (List Recovery)**.** A similar claim holds for the more general *list recovery* problem, where for each position we are given as input a set of up to l elements of $\mathbb{F}_q^m$, and the goal is to find all codewords which agree with some element of the input sets for at least a fraction $(1-\rho)$ of positions. In this case, $1-\rho$ only needs to be only a factor $l^{1/s}$ larger than the bound (6.4). By picking $s \gg l$, the effect of l can be made negligible. This feature is very useful in concatenation schemes; see Section 7.1 and [6] for further details.

7. Long codes achieving list decoding capacity

We now describe the parameter choices which leads to capacity-achieving list-decodable codes, i.e., codes of rate R_0 that can correct a fraction $1-R_0-\varepsilon$ of errors (for any desired $0 < R_0 < 1$), and whose alphabet size is polylogarithmic in the block length; the formal statement appears in Theorem 7.1 below. (Recall that for folded RS codes, the alphabet size is a large polynomial in the block length.) Using concatenation and expander-based ideas, Guruswami and Rudra [6] also present capacity-achieving codes over a fixed alphabet size (that depends on the distance ε to capacity alone). The advantage of our codes is that they inherit strong list recovery properties similar to the folded RS codes (Remark 6.11). This is very useful in concatenation schemes, and indeed our codes can be used as outer codes for an explicit family of binary concatenated codes list-decodable up to the Zyablov radius, *with no brute-force search* for the inner code (see Section 7.1 below).

We now describe our main result on how to obtain the desired codes from the construction $\mathcal{C}$ and Theorem 6.10. The underlying parameter choices to achieve this require a fair bit of care.

Theorem 7.1 (Main)**.** *For every R_0, $0 < R_0 < 1$, and every constant $\varepsilon > 0$, the following holds for infinitely many integers $\mathbf{q}$ which are powers of two. There is a code of rate at least R_0 over an alphabet of size $\mathbf{q}$ with block length $N \geqslant 2^{\mathbf{q}^{\Omega(\varepsilon^2/\log(1/R_0))}}$ that can be list decoded up to a fraction $1 - R_0 - \varepsilon$ of errors in time bounded by $(N \log(1/R_0)/\varepsilon^2)^{O(1/(R_0\varepsilon)^2)}$.*

Proof. Suppose R_0, $0 < R_0 < 1$, and $\varepsilon > 0$ are given. Let $c = 2\lfloor \frac{10}{R_0\varepsilon} \rfloor + 1$, and $\phi(c)$ denote the Euler's totient function of c.

Let $u \geqslant 1$ be an arbitrary integer; we will get a family of codes by varying u. The code we construct will be a folded cyclotomic code $\mathcal{C}$ defined in Eq. (5.8). Let $x = \phi(c)u$. Note that $2^x \equiv 1 \pmod{c}$. We first pick q, r, d as follows: $r = 2^x$, $q = r^2$, and $d = (2^x - 1)/c$. For this choice, $d|r-1$ and $(q-1)/(r-1) = r+1$ is coprime to d, as required in Lemma 4.1. So we can take $M(T) = T^d - \gamma \in \mathbb{F}_r[T]$ for γ primitive in $\mathbb{F}_r$ as the irreducible polynomial over $\mathbb{F}_q$.

For the above choice $d/r < 1/c \leqslant \varepsilon R_0/20$, so that $\frac{d}{2R_0 r} < \frac{\varepsilon}{10}$. By picking

$$s = \Theta(\varepsilon^{-1}\log(1/R_0)), \quad m = \Theta(s/\varepsilon) \ ,$$

and $\zeta = \varepsilon/20$, we can ensure that the decoding radius ρ guaranteed in Eq. (6.4) by Theorem 6.10 is at least $1 - (1+\varepsilon)R_0$.

The degree b of the extension E/F (Eq. (4.1)) is given by $b = \frac{r^d+1}{r+1}$. The length of the unfolded cyclotomic code $\mathcal{C}^0$ (defined in (5.7)) equals $n = rb > r^d/2$. We need to ensure that the rate of $\mathcal{C}^0$, which is equal to the rate of the folded cyclotomic code $\mathcal{C}$, is at least R_0. To this end, we will pick

$$\ell = \left\lceil \frac{b}{2} + \frac{R_0 r b}{d} \right\rceil \ . \tag{7.1}$$

It is easily checked that for our choice of parameters $\ell \geqslant b$. By Lemma 5.5, the rate of $\mathcal{C}^0$ equals $\frac{d(\ell-(b-1)/2)}{rb}$, which is at least R_0 for the above choice of ℓ.

We next pick the value of D, the degree of the irreducible A, which is the key quantity governing the list size and decoding complexity. We need $D > \ell d/b$. For the ℓ chosen above, this condition is surely met if $D > 2r$. But there must also be an irreducible A of degree D that is a primitive root modulo M. Since we know the Riemann hypothesis for function fields, there is an effective Dirichlet theorem on the density of irreducibles in arithmetic progressions (see [18, Thm 4.8]). This implies that when $D \gg 2d$, such a polynomial A must exist (in fact about a $\frac{\phi(q^d-1)}{D(q^d-1)}$ fraction of degree D polynomials satisfy the needed property). We can thus pick

$$D = \Theta(r) = \Theta(dc) = \Theta(d/(R_0\varepsilon)) \ .$$

The running time of the list decoding algorithm is dominated by the $q^{O(Ds)}$ term, and for the above choice of parameters can be bounded by $q^{O(d/(R_0\varepsilon)^2)}$. The block length of the code N satisfies

$$N = \frac{n}{m} > \frac{r^d}{2m} = \frac{q^{d/2}}{2m} = \Omega\left(\frac{\varepsilon^2 q^{d/2}}{\log(1/R_0)}\right) \ .$$

As a function of N, the decoding complexity is therefore bounded by $(N\log(1/R_0)/\varepsilon^2)^{O(1/(R_0\varepsilon)^2)}$. The alphabet size of the folded cyclotomic code is $\mathbf{q} = q^m$, and we can bound the block length N from below as a function of $\mathbf{q}$ as:

$$\begin{aligned} N &\geqslant \frac{q^{d/2}}{2m} \geqslant \frac{q^{\Omega(r/c)}}{2m} \geqslant \frac{q^{\Omega(\varepsilon R_0\sqrt{q})}}{2m} \\ &\geqslant 2^{\sqrt{q}} \qquad \text{(for large enough } q \text{ compared to } 1/R_0,\ 1/\varepsilon) \\ &= 2^{\mathbf{q}^{1/(2m)}} \geqslant 2^{\mathbf{q}^{\Omega(\varepsilon^2/\log(1/R_0)))}} \ . \end{aligned}$$

This establishes the claimed lower bound on block length, and completes the proof of the theorem. □

7.1. **Concatenated codes list-decodable up to Zyablov radius.** Using the strong list recovery property of folded RS codes, a polynomial time construction of binary codes list-decodable up to the Zyablov radius was given in [6, Thm 5.3]. The construction used folded RS codes as outer codes in a concatenation scheme, and involved an undesirable brute-force search to find a binary inner code that achieves list decoding capacity. The time to construct the code grew faster than $N^{\Omega(1/\varepsilon)}$ where ε is the distance of the decoding radius to the Zyablov radius. This result as well as our result below hold not only for binary codes but also codes over any fixed alphabet; for sake of clarity, we state results only for binary codes.

Since the folded cyclotomic codes from Theorem 7.1 are much longer than the alphabet size, by using them as outer codes, it is possible to achieve a similar result without having to search for an inner code, by using as inner codes *all possible binary linear codes* of a certain rate!

Theorem 7.2. *Let $0 < R_0, r < 1$ and $\varepsilon > 0$. Let $\mathcal{C}$ be a folded cyclotomic code guaranteed by Theorem 7.1 with rate at least R_0 and a large enough block length N. Let $\mathcal{C}^*$ be a binary code obtained by concatenating $\mathcal{C}$ with all possible binary linear maps of rate r (each one used a roughly equal number of times). Then $\mathcal{C}^*$ is binary linear code of rate at least $R_0 \cdot r$ that can be list decoded from a fraction $(1-R_0)H^{-1}(1-r) - \varepsilon$ of errors in $N^{(1/\varepsilon)^{O(1)}}$ time.*

We briefly discuss the idea behind proving the above claim. As the alphabet size of folded cyclotomic codes is polylogarithmic in N, each outer codeword symbol can be expressed using $O_\varepsilon(\log\log N)$ bits. Hence the total number of such inner codes S will be at most $2^{O_\varepsilon((\log\log N)^2)} \ll N$ for large enough N. The N outer codeword positions will be partitioned into S (roughly) equal parts in an arbitrary way, and each inner code used to encode all the outer codeword symbols in one of the parts. Most of the inner codes achieve list decoding capacity — if their rate is r, they can list decode $H^{-1}(1-r)-\varepsilon$ fraction of errors with constant sized lists (of size $2^{O(1/\varepsilon)}$). This suffices for analyzing the standard algorithm for decoding concatenated codes (namely, list decode the inner codes to produce a small set of candidate symbols for each position, and then list recover the outer code based on these sets). Arguing as in [6, Thm 5.3], we can thus prove Theorem 7.2.

Acknowledgments

Many thanks to Dinesh Thakur for several illuminating discussions about Carlitz-Hayes theory and cyclotomic function fields. I thank Dinesh Thakur and Greg Anderson for helping me with the proof of Lemma 5.3. Thanks to Andrew Granville for pointing me to Dirichlet's theorem for polynomials.

References

[1] L. Carlitz. A class of polynomials. *Trans. Amer. Math. Soc.*, 43:167–182, 1938.

[2] G. Frey, M. Perret, and H. 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] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

[4] A. Garcia and H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[5] V. Guruswami and A. Patthak. Correlated Algebraic-Geometric codes: Improved list decoding over bounded alphabets. *Mathematics of Computation*, 77(261):447–473, 2008.

[6] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.

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

[8] V. Guruswami and M. Sudan. On representations of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 47(4):1610–1613, 2001.

[9] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, March 1974.

[10] M.-D. Huang and A. K. Narayanan. Folded algebraic geometric codes from Galois extensions. Personal communication, 2008.

[11] J. Justesen. A class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18:652–656, 1972.

[12] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their applications*. Cambridge University Press, Cambridge, MA, 1986.

[13] D. A. Marcus. *Number Fields*. Springer-Verlag, New York Inc., 1977.

[14] H. Niederreiter and C. P. Xing. Explicit global function fields over the binary field with many rational places. *Acta Arithmetica*, 75:383–396, 1996.

[15] H. Niederreiter and C. P. Xing. Cyclotomic function fields, Hilbert class fields and global function fields with many rational places. *Acta Arithmetica*, 79:59–76, 1997.

[16] F. Parvaresh and A. Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *Proceedings of the 43nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 285–294, 2005.

[17] H.-G. Quebbemann. Cyclotomic Goppa codes. *IEEE Trans. Info. Theory*, 34:1317–1320, 1988.

[18] M. Rosen. *Number Theory in Function Fields*. Springer-Verlag New York, Inc., 2002.

[19] G. D. V. Salvador. *Topics in the theory of algebraic function fields*. Birkhauser, Boston, 2006.

[20] B.-Z. Shen. A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate. *IEEE Transactions on Information Theory*, 39(1):239–241, 1993.

[21] H. Stichtenoth. *Algebraic function fields and codes.* Springer, Berlin, 1993.
[22] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound. *IEEE Transactions on Information Theory*, 52(5):2218–2224, 2006.
[23] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.

Appendix A. Table of parameters used

Since the construction of the cyclotomic function field and the associated error-correcting code used a large number of parameters, we summarize them below for easy reference.

We begin by recalling the parameters concerning the function field construction:

q	size of the ground finite field
r	size of the subfield $\mathbb{F}_r \subset \mathbb{F}_q$
F	the field $\mathbb{F}_q(T)$ of rational functions
R_T	the ring of polynomials $\mathbb{F}_q[T]$
P_∞	the place of F that is the unique pole of T
M	polynomial $T^d - \gamma \in \mathbb{F}_r[T]$, irreducible over $\mathbb{F}_q$
d	degree of the irreducible polynomial M
C_M	the Carlitz action corresponding to M
Λ_M	the M-torsion points in F^{ac} under the action C_M
K	the cyclotomic function field $F(\Lambda_M)$
λ	nonzero element of Λ_M that generates K over F; $K = F(\lambda)$
G	the Galois group of K/F, naturally isomorphic to $(R_T/(M))^*$
H	the subgroup $\mathbb{F}_q^* \cdot \mathbb{F}_r[T]$ of G
E	the fixed field K^H of H
μ	primitive element for E/F; $E = F(\mu)$
b	the degree $[E : F]$ of the extension E/F
g	the genus of E/F, equals $d(b-1)/2 + 1$

The construction of the code $\mathcal{C}^0$ (Eqn. (5.7)) and its folded version $\mathcal{C}$ (Eqn. (5.8)) used further parameters, listed below:

M'	the unique place of E lying above M
ℓ	maximum pole order at M' of message functions; $\ell \geqslant b$
$\mathcal{L}(\ell M')$	$\mathbb{F}_q$-linear space of messages of the codes
n	block length of $\mathcal{C}^0$, $n = br$
k	dimension of the $\mathbb{F}_q$-linear code $\mathcal{C}$, $k = \ell d - g + 1$
m	folding parameter
N	block length of folded code $\mathcal{C}$, $N = n/m$
$P_j^{(\beta)}$	for $\beta \in \mathbb{F}_r$ and $0 \leqslant j < b$, these are the rational places lying above $T - \beta$ in E
A	an irreducible polynomial (place of F) that remains inert in E/F
D	the degree of the polynomial A; satisfies $Db > \ell d$
σ_A	the Artin automorphism of the extension E/F at A
A'	the unique place of E lying above A

Appendix B. Algebraic preliminaries

We review some basic background material concerning global fields and their extensions. The term global field refers to either a number field, i.e., a finite extension of $\mathbb{Q}$, or the function field L of an algebraic curve over a finite field, i.e., a finite extension of $F = \mathbb{F}_q(T)$. While we are only interested in the latter, much of the theory applies in a unified way to both settings. Good references for this material are the texts by Marcus [13] and Stichtenoth [21].

B.1. **Valuations and Places.** A subring X of L is said to be a *valuation ring* if for every $z \in L$, either $z \in X$ or $z^{-1} \in X$. Each valuation ring is a *local ring*, i.e., it has a unique maximal ideal. The set of *places* of L, denoted $\mathbb{P}_L$, is the set of maximal ideals of all the valuation rings of L. Geometrically, this corresponds to the set of all (non-singular) points on the algebraic curve corresponding to L. The valuation ring corresponding to a place P is called the ring of *regular functions* at P and is denoted $\mathcal{O}_P$.

Associated with a place P is a *valuation* $v_P : L \to \mathbb{Z} \cup \{\infty\}$, that measures the order of zeroes or poles of a function at P, a negative valuation implies the function has a pole at P (by convention we set $v_P(0) = \infty$). In terms of v_P, we have $\mathcal{O}_P = \{x \in L \mid v_P(x) \geqslant 0\}$ and $P = \{x \in L \mid v_P(x) > 0\}$. The valuation v_P satisfies $v_P(xy) = v_P(x) + v_P(y)$ and the triangle inequality $v_P(x + y) \geqslant \min\{v_P(x), v_P(y)\}$ (and equality holds if $v_P(x) \neq v_P(y)$).

The quotient $\mathcal{O}_P/P$ is a field since P is a maximal ideal and it is called the *residue field* at P. The residue field $\mathcal{O}_P/P$ is a finite extension field of $\mathbb{F}_q$; the degree of this extension is called the *degree* of P. We will also sometimes use the terminology *primes* to refer to places — the terms primes and places will be used interchangeably.

B.2. **Decomposition of primes in Galois extensions.** We now discuss how primes decompose in field extensions. Let K/L be a finite, separable extension of global fields of degree $[K : L] = n$. We will restrict our attention of Galois extensions. Let P be a place of L. Let $\mathcal{O}'_P$ be the integral closure of $\mathcal{O}_P$ in K, i.e., the set of all $z \in K$ which satisfy a monic polynomial equation with coefficients in $\mathcal{O}_P$. The ideal $P\mathcal{O}'_P$ can be written as the product of prime ideals of $\mathcal{O}'_P$ as $P\mathcal{O}'_P = (P_1 P_2 \ldots P_r)^e$. Here $P_1, P_2, \ldots, P_r$ are said to be the places of K lying above P (and P is said to be lie below each P_i). One has the equality $P_i \cap L = P$ for every i. The ring $\mathcal{O}'_P$ is the fact the intersection of $\mathcal{O}_{P_i}$ for $i = 1, 2, \ldots, r$. The quantity e is called the *ramification index*, and when $e = 1$, P (as well as the P_i) are said to be *unramified*. For $x \in L$, one has $v_{P_i}(x) = e \cdot v_P(x)$. The residue field $\mathcal{O}_{P_i}/P_i$ is a finite extension of $\mathcal{O}_P/P$; the degree f of this extension is called the inertia degree of P. The ramification index e, inertia degree f, and number r of primes above P satisfy $efr = n = [K : L]$.

If $e = n$ and $f = r = 1$, the prime P is said to be *totally ramified*. If $r = n$ and $e = f = 1$, the prime P is said to *split completely*. If $f = n$ and $e = r = 1$, the prime P is said to be *inert*.

B.3. **Galois action on primes and the Artin automorphism.** The Galois group $G = \mathrm{Gal}(K/L)$ acts transitively on the primes $P_1, P_2, \ldots, P_r$ of K lying above $P \in \mathbb{P}_L$. For each P_i, there is a subgroup $D(P_i|P) \subseteq G$ that fixes P_i; this is called the *decomposition group* of P_i. It is known that the decomposition is isomorphic to the Galois group of the finite field extension $(\mathcal{O}_{P_i}/P_i)/(\mathcal{O}_P/P)$ of the residue fields. Note that the latter group is cyclic and generated by the Frobenius automorphism Frob mapping $x \mapsto x^q$. The element of $D(P_i|P)$ corresponding to Frob is called the Artin automorphism $\mathcal{A}(P_i|P)$ of P_i over P.

When G is abelian (which covers the cases we are interested in), the decomposition group $D(P_i|P)$ and the Artin automorphism $\mathcal{A}(P_i|P)$ are the same for every P_i, and they depend only on the prime P below. Denote the Artin automorphism at P by $\mathcal{A}_P$. This has the following important property:

$$\mathcal{A}_P(x) \equiv x^{\|P\|} \pmod{P_i}$$

for every $x \in \mathcal{O}'_P$ and every prime P_i lying above P. If P is unramified, then $\mathcal{A}_P$ is the only element of G with this property. In the unramified case, by Chinese Remaindering the above also implies

$$\mathcal{A}_P(x) \equiv x^{\|P\|} \pmod{P\mathcal{O}'_P}$$

for every $x \in \mathcal{O}'_P$.

Note that if P is inert with a unique prime P' lying above it, then $D(P'|P) = G$, and thus G must be cyclic. Thus, only cyclic extensions can have an inert prime.

Department of Computer Science and Engineering, University of Washington. Currently visiting the Computer Science Dept., Carnegie Mellon University. Some of this work was done when the author was a member in the School of Mathematics, Institute for Advanced Study.

E-mail address: venkat@cs.washington.edu

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/