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

Erasure List-Decodable Codes From Random and Algebraic Geometry Codes

Ding, Yang; Jin, Lingfei; Xing, Chaoping

2014

Ding, Y., Jin, L., & Xing, C. (2014). Erasure List-Decodable Codes From Random and Algebraic Geometry Codes. IEEE Transactions on Information Theory, 60(7), 3889-3894.

https://hdl.handle.net/10356/81744

https://doi.org/10.1109/TIT.2014.2314468

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [http://dx.doi.org/10.1109/TIT.2014.2314468].

Downloaded on 15 Jun 2024 05:46:39 SGT

Erasure List-Decodable Codes from Random and Algebraic Geometry Codes

Yang Ding, Lingfei Jin and Chaoping Xing

Abstract

Erasure list decoding was introduced to correct a larger number of erasures by outputting a list of possible candidates. In the present paper, we consider both random linear codes and algebraic geometry codes for list decoding from erasures. The contributions of this paper are two-fold. Firstly, for arbitrary $0 < R < 1$ and $\epsilon > 0$ (R and ϵ are independent), we show that with high probability a q-ary random linear code of rate R is an erasure list-decodable code with constant list size $q^{O(1/\epsilon)}$ that can correct a fraction $1 - R - \epsilon$ of erasures, i.e., a random linear code achieves the information-theoretic optimal trade-off between information rate and fraction of erasures. Secondly, we show that algebraic geometry codes are good erasure list-decodable codes. Precisely speaking, a q-ary algebraic geometry code of rate R from the Garcia-Stichtenoth tower can correct $1-R-\frac{1}{\sqrt{q}-1}+\frac{1}{q}-\epsilon$ fraction of erasures with list size $O(1/\epsilon)$. This improves the Johnson bound for erasures applied to algebraic geometry codes. Furthermore, list decoding of these algebraic geometry codes can be implemented in polynomial time. Note that the code alphabet size q in our paper is constant and independent of ϵ.

Index Terms

Erasure codes, List decoding, Algebraic geometry codes, Generalized Hamming weights.

I. Introduction

Erasure codes have received great attention for their wide applications in recovering packet losses in the Internet and storage systems. In the model of erasure channel, errors are described as erasures, namely the receivers are supposed to know the positions where the erasures occurred. Compared with other communication channels such as adversarial noise channel, erasure channel is much simpler. Thus, we can expect better parameters for erasure channel than adversarial noise channel. The notion of list decoding was independently introduced by Elias and Wonzencraft [3], [21]. Instead of the unique decoding, the model of list decoding allows to output a list of possible codewords. The decoding is considered to be successful as long as the correct codeword is included in the list and the list size is not too big.

The problem of list decoding for classical adversarial noise channel has been extensively studied (see [3], [7], [8], [9], [19], [21], [22], for example). A fundamental problem in list decoding is the tradeoff among the information rate, decoding radius (i.e., fraction of errors that can be corrected) and the list size. In other words, if we fix one of these three parameters, then one is interested in optimal tradeoff between the remaining two parameters. For instance, if the list size is fixed to be constant or polynomial in the length of codes, the problem becomes a tradeoff between information rate and decoding radius.

Definition 1.1: ((τ, L)-erasure list decodability) Let Σ be a finite alphabet of size q, $L > 1$ be an integer, and $\tau \in (0, 1)$. A code $C \subseteq \Sigma^n$ is said to be (τ, L)-erasure list-decodable, if for every $\mathbf{r} \in \mathbb{F}_q^{(1-\tau)n}$, and any subset $T \subseteq \{1, 2, \cdots, n\}$ of size $(1 - \tau)n$, one has

$$|\{\mathbf{c} \in C | \mathbf{c}_T = \mathbf{r}\}| \leq L,$$

where $\mathbf{c}_T$ is the projection of $\mathbf{c}$ onto the coordinates indexed by T. In other words, given any received word with at most τn erasures, there are at most L codewords that are consistent with the unerased portion of the received word.

Known results

It is known that, for an erasure channel where the codeword symbols are randomly and independently erased with probability τ, the capacity is $1 - \tau$ [4]. Although erasure list decoding has been considered previously [6], [8], [9], [11], a lot of problems still remain unsolved. Let us summarize some of previous results on erasure list decoding below.

(i) It is well known that algebraic geometry codes from an optimal tower with rate R and alphabet size $q \geq \Omega(1/\epsilon^2)$ are $(1 - R - \epsilon, 1)$-erasure list decodable. In other words, they achieve the list decoding capacity $1 - R$ from erasures for large enough q. However, the results for small q are quite thin.

Y. Ding is with Department of Mathematics, Shanghai Uniersity, Shanghai, China, and School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore (email: dingyang@shu.edu.cn).

L. Jin is with Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China, and School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore.

C. Xing is with Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore (email: {dingyang,lfjin,xingcp}@ntu.edu.sg).

The work of all the authors is partially supported by the Singapore Minister of Education under Tier 1 grant RG20/13 and the Singapore A*STAR SERC under Research Grant 1121720011. The first author is also supported by the National Natural Science Foundation of China (11201286) and the First-Class Discipline of University in Shanghai (ZZSD12013).

(ii) Guruswami showed [6] that, for any small $\epsilon > 0$ and $\tau \in (0,1)$, a (τ, L)-erasure list-decodable code of rate $1-\tau-\epsilon$ must satisfy $L \geq \Omega(\frac{1}{\epsilon})$; and on the other hand, there exists a $(\tau, O(\exp(\frac{1}{\epsilon})))$-erasure list-decodable code of rate $1-\tau-\epsilon$.

(iii) In [7, Proposition 10.1], the Johnson bound for erasure decoding radius was derived. It says that, for any given $\epsilon > 0$, every q-ary code of relative distance $\delta < 1-1/q$ is $(\delta + \frac{\delta}{q-1} - \epsilon, O(1/\epsilon))$-erasure list-decodable. This means that, with a constant list size, erasure decoding radius is enlarged by approximately $\frac{\delta}{q-1}$ compared with unique erasure decoding whose decoding radius is only δ. On the other hand, it was shown further in [7, Proposition 10.2] that there exists a q-ary code of length n and relative distance $\delta < 1-1/q$ that is not $(\delta + \frac{\delta}{q-1} + \epsilon, 2^{O(\epsilon^2 \delta n)})$-erasure list-decodable for every small $\epsilon > 0$. This implies that the best bound on erasure list decoding radius of a q-ary code of relative minimum distance δ is $\delta + \frac{\delta}{q-1}$.

(iv) It was shown in [6] that for any small $\epsilon > 0$, with high probability a random binary linear code of rate $R = \Omega(\epsilon/\log(1/\epsilon))$ is $(1-\sigma, O(1/\sigma))$-erasure list-decodable for every σ satisfying $\epsilon \leq \sigma \leq 1$. The main idea for proving this probabilistic result is through counting of submatrices of generator matrix of a random linear code. Furthermore, concatenating such a binary code as an inner code and a code over large field achieving the list decoding capacity as an outer code, Guruswami showed [6] that, for any small $\epsilon > 0$, one can construct a family of concatenated (binary) $(1-\epsilon, O(1/\epsilon))$-erasure list-decodable codes of rate $\Omega(\epsilon^2/\log(1/\epsilon))$ in polynomial time. A slightly better rate was obtained for nonlinear case in [9]. They constructed binary codes with rate $\Omega\left(\epsilon^{1+1/t}/(t^2 \log 1/\epsilon)\right)$ over alphabet of size 2^t for any integer $t \geq 1$. Thus the optimal bound $\Omega(\epsilon)$ can be approached by gradually increasing t. By concatenating a random linear code as an outer code, Rudra and Uurtamo [16] proved that most concatenated binary linear codes with rate $1-\tau-\epsilon$ can be list decoded from τ (a constant) fraction of erasures with a list size $2^{O(1/\epsilon)}$ using some counting and probabilistic arguments.

Our results and comparison

Our contributions of this paper are two-fold.

(i) Firstly, we show that, for arbitrary $0 < R < 1$ and $\epsilon > 0$ (R and ϵ are independent), with high probability a random linear code is $(1-R-\epsilon, q^{O(1/\epsilon)})$-erasure list-decodable, i.e., a random q-ary linear code achieves the information-theoretic optimal tradeoff between information rate and fraction of erasure errors that can be corrected. However, Theorem 2 in [6] which was derived from [12] only shows existence of binary $(1-R-\epsilon, 2^{O(1/\epsilon)})$-erasure list-decodable codes for arbitrary $0 < R < 1$ and $\epsilon > 0$. Furthermore, it is shown in [16] that concatenated codes also yield binary $(1-R-\epsilon, 2^{O(1/\epsilon)})$-erasure list-decodable codes for arbitrary $0 < R < 1$ and $\epsilon > 0$. Hence, our results further strengthen the known results in [6], [16].

(ii) Secondly, we show that algebraic geometry codes are good erasure list-decodable codes. Precisely speaking, for any $0 < \tau < 1$ and $\epsilon > 0$, a q-ary algebraic geometry code from the Garcia-Stichtenoth tower may have rate at least $1-\tau-\frac{1}{\sqrt{q}-1}+\frac{1}{q}-\epsilon$ and is $(\tau, O(1/\epsilon))$-erasure list-decodable. Furthermore, the generator matrices of these algebraic geometry codes can be constructed in polynomial time. Therefore, by the standard erasure list decoding (see [15, Problem 6.11]), the algebraic geometry codes can be list decoded in polynomial time. On the other hand, if we apply the Johnson bound given in [7, Proposition 10.1] to general algebraic geometry codes, we can only claim that a q-ary algebraic geometry code from the Garcia-Stichtenoth tower has rate $1-\tau-\frac{1}{\sqrt{q}-1}+\frac{\tau}{q}-\epsilon$ and is $(\tau, O(1/\epsilon))$-erasure list-decodable. This rate is always smaller than our rate for any $\tau \in (0,1)$. This implies that the Johnson bound could be improved for some special class of codes although it is optimal in general.

Organization

The paper is organized as follows. In Section 2, we introduce some necessary notation and definitions and known results as well. Section 3 is devoted to random codes. In the last section, we show that algebraic geometry codes are good erasure list-decodable codes.

II. Preliminaries

In this paper, we only focus on linear codes. Recall that a q-ary $[n,k]_q$ linear code is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ with dimension k, where $\mathbb{F}_q$ is a finite field with q elements and q is a prime power. We call n the length of the code and k the dimension of the code. The information rate of the code C is defined as $R = k/n$ which represents the efficiency of the code. Another important parameter of the code is the distance which represents the error correcting capability. The distance of a linear code C is defined to be the minimum Hamming weight of nonzero codewords of C, denoted by $d = d(C)$. The relative distance $\delta = \delta(C)$ is defined to be the quotient d/n.

From Definition 1.1, one knows that, in a (τ, L)-erasure list-decodable code C of length n, for every $\mathbf{r} \in \mathbb{F}_q^{(1-\tau)n}$ and $T \subseteq \{1,2,\ldots,n\}$ with $|T| = (1-\tau)n$ the number of the codewords in the output list that are consistent with $\mathbf{r}$ at the coordinates indexed by T is at most L. Thus, if C is linear, it is equivalent to saying that the number of the codewords that are $\mathbf{0}$ at the coordinates indexed by T is at most L, i.e., $|\{\mathbf{c} \in C | \mathbf{c}_T = \mathbf{0}\}| \leq L$. Hence, an $[n,k,d]_q$-linear code is $((d-1)/n, 1)$-erasure list-decodable, but not $(d/n, 1)$-erasure list-decodable.

Definition 2.1: (Erasure list decoding radius (ELDR))

(i) For an integer $L \geq 1$ and a linear code C of length n, we denote

$$\mathrm{Rad}_L(C) := \max\{0 \leq \tau \leq 1 : \ C \text{ is } (\tau, L)\text{-erasure list-decodable}\}.$$

(ii) For an infinite family $\mathcal{C} = \{C_i\}_{i \geq 1}$ of q-ary linear codes with length tending to ∞ and an integer $L \geq 1$, we denote

$$\mathrm{ELDR}_L(\mathcal{C}) := \liminf_i \left\{ \frac{\mathrm{Rad}_L(C_i)}{n_i} \right\},$$

where n_i is the length of C_i.

Definition 2.2: For an integer $L \geq 1$ and $0 \leq \tau \leq 1$, the maximum rate for linear (τ, L)-erasure list-decodable code families is defined to be

$$R_L(\tau) := \sup_{\mathcal{C}:\ \mathrm{ELDR}_L(\mathcal{C}) \geq \tau} R(\mathcal{C}).$$

The notation of erasure list decoding for linear codes actually had already been studied in the form of generalized Hamming weight [20]. However, the explicit relationship between erasure list decoding and generalized Hamming weight had not been made clear until the work in [6]. The concept of generalized Hamming weight was initially introduced in [20] and later received great attention due to applications in cryptography, design of codes, t-resilient functions and so on [1].

Definition 2.3: (Generalized Hamming Weight) The r-th generalized Hamming weight of a code C, denoted by $d_r(C)$, is defined to be the size of the smallest support of an r-dimensional subcode of C, i.e.,

$$d_r(C) = \min\{|\mathrm{Supp}(D)| : \ D \text{ is a subspace of } C \text{ of dimension } r\},$$

where $\mathrm{Supp}(D) = \{i : \ \exists (c_1, \ldots, c_n) \in D, c_i \neq 0\}$.

Note that $d_1(C)$ is exactly the minimum distance d of C. The characterization of erasure list decodability through generalized Hamming weight is given below.

Lemma 2.4: ([6]) A q-ary linear code C of length n is $(s/n, L)$-erasure list-decodable if and only if $d_r(C) > s$, where $r = \lfloor \log_q L \rfloor + 1$.

The above characterization is quite straightforward since all codewords in the list with fixed positions equal to 0 form a vector space.

The link stated in Lemma 2.4 establishes a two-way bridge. Results for erasure list decoding can be derived directly from the existing results on generalized Hamming weight, and thus the applications of generalized Hamming weight are inherited. In the meanwhile, some new properties for generalized Hamming wight can be obtained as well if one can develop some fresh ideas on erasure list decoding.

In [6], Guruswami made use of the connection between generalized Hamming weight and erasure list decoding to establish some bounds for rate $R_L(\tau)$ through the existing bounds on generalized Hamming weight.

Lemma 2.5: ([6]) One has

(i) For every integer $L \geq 1$ and every τ, $0 \leq \tau \leq 1$,

$$R_L(\tau) \geq 1 - \frac{\tau}{r} \log_q \frac{q^r - 1}{q - 1} - \frac{H_q(\tau)}{r}$$

where $r = \lfloor \log_q L \rfloor + 1$. In particular, for any small $\epsilon > 0$ and $\tau \in (0, 1)$, there exists a $(\tau, O(\exp(\frac{1}{\epsilon})))$-erasure list-decodable code of rate $1 - \tau - \epsilon$.

(ii) For small $\epsilon > 0$ and τ with $0 < \tau < 1$, a (τ, L)-erasure list-decodable code of rate $1 - \tau - \epsilon$ must satisfy $L \geq \Omega(\frac{1}{\epsilon})$.

III. Random List Decodable Erasure Codes

Random $(1 - \epsilon, O(1/\epsilon))$-erasure list-decodable codes of rate $R = \Omega(\epsilon / \log(1/\epsilon))$ were discussed in [6] by using a characterization of generator matrices of erasure list-decodable codes. However, the rate is quite small and actually is dependent on ϵ. In this section, we are going to show that for any $0 \leq R \leq 1$ (R is independent of ϵ), with probability $1 - q^{-\Omega(n)}$ a random linear code C of length n and rate R is $(1 - R - \epsilon, q^{O(1/\epsilon)})$-erasure list-decodable. Our approach is through a characterization of parity-check matrices of erasure list-decodable codes.

The following result is useful in the proof of Theorem 3.3. The reader may refer to [15, pp. 135, Problem 4.33] for the proof.

Proposition 3.1: If $k/n \to R > 0$ when n tends to ∞, then for a random matrix H over $\mathbb{F}_q$ of size $(n - k) \times n$, the probability that H is full-rank is approaching 1 when n tends to ∞.

Lemma 3.2: Let s be a positive integer, then an $[n, k]_q$ code C is $(s/n, L)$-erasure-list-decodable if and only if any submatrix $H'_{(n-k)\times s}$ of the parity check matrix $H_{(n-k)\times n}$ of C has rank at least $s - \lfloor \log_q L \rfloor$.

Proof: By Definition 1.1 and the fact that C is a linear code, C is $(s/n, L)$-erasure-list-decodable if and only if

$$|\{\mathbf{c} \in C | \mathbf{c}_T = \mathbf{0}\}| \leq L$$

for arbitrary $T \subseteq \{1, 2, \ldots, n\}$ with size $n - s$. This implies that C is $(s/n, L)$-erasure-list-decodable if and only if for any submatrix $H'_{(n-k)\times s}$ of $H_{(n-k)\times n}$,

$$|\{\mathbf{x} \in \mathbb{F}_q^s | H'_{(n-k)\times s} \cdot \mathbf{x} = \mathbf{0}\}| \leq L,$$

i.e., the solution space of $H'_{(n-k)\times s}\mathbf{x} = \mathbf{0}$ has dimension at most $\lfloor \log_q L \rfloor$. Therefore, $H'_{(n-k)\times s}$ has rank at least $s - \lfloor \log_q L \rfloor$. ■

Theorem 3.3: For every small $\epsilon > 0$, a real $0 < R < 1$ and sufficiently large n, with probability at least $1 - q^{-\Omega(n)}$, a random linear code over $\mathbb{F}_q$ of length n and rate R is $(1 - R - \epsilon, q^{O(\frac{1}{\epsilon})})$-erasure list-decodable.

Proof: Put $\ell = \lceil \frac{1}{\epsilon}((2 - R)\log_q 2 + 1) \rceil$ and $L = q^\ell$. Thus, $L = q^{O(\frac{1}{\epsilon})}$. We randomly pick a matrix $H_{(n-k)\times n}$. Then with probability approaching 1, $H_{(n-k)\times n}$ is full rank from Proposition 3.1. Let such a full rank matric $H_{(n-k)\times n}$ be the parity check matrix of our linear code C. Then we are going to prove that with probability at most $q^{-\Omega(n)}$, C is not (s, L)-erasure list-decodable for $s = \lfloor n - k - \epsilon n \rfloor$. By Lemma 3.2, this happens only if some $(n - k) \times s$ submatrix of H has rank less than $s - \lfloor \log_q L \rfloor$.

Denote $n - k$ by K. Let A denote the number of full-rank matrices $H_{(n-k)\times n}$ in which there exists $s = n - k - \epsilon n$ columns with rank at most $s - \ell$. Note that the total number of matrices of size $K \times s$ over $\mathbb{F}_q$ with rank at most $s - \ell$ is equal to $\sum_{i=0}^{s-\ell} \binom{K}{i}(q^s - 1)\cdots(q^s - q^{i-1})q^{(K-i)i}$. For the remaining $n - s$ columns, we have $q^{K(n-s)}$ choices. Thus, we have

$$\begin{aligned}
A &\leq \binom{n}{s} q^{K(n-s)} \sum_{i=0}^{s-\ell} \binom{K}{i} (q^s - 1)\cdots(q^s - q^{i-1}) q^{(K-i)i} \\
&< 2^n \sum_{i=0}^{s-\ell} \binom{K}{i} q^{(si+Ki-i^2)+K(n-s)} \\
&\leq 2^n \times q^{(s+K)(s-\ell)-(s-\ell)^2+K(n-s)} \sum_{i=0}^{s-\ell} \binom{K}{i} \\
&\leq 2^{n+K} \times q^{(s+K)(s-\ell)-(s-\ell)^2+K(n-s)} \\
&\leq q^{(n+K)\log_q 2} \times q^{(2K-\epsilon n)(K-\epsilon n-\ell)-(K-\epsilon n-\ell)^2+K(n-K+\epsilon n)} \\
&< q^{n((2-R)\log_q 2-\epsilon\ell)+Kn}.
\end{aligned}$$

Substituting the value of ℓ to the above equation, we have

$$\limsup_{n\to\infty} \frac{A}{(q^n - 1)(q^n - q)\cdots(q^n - q^{n-k-1})} \leq \limsup_{n\to\infty} \frac{A}{q^{(n-k)n}} \times \lim_{n\to\infty} \frac{q^{(n-k)n}}{(q^n - 1)(q^n - q)\cdots(q^n - q^{n-k-1})} \leq \lim_{n\to\infty} q^{-n} = 0.$$

This implies that with probability at most q^{-n}, a random matrix $H_{(n-k)\times n}$ has full rank and a submatrix of size $(n-k)\times s$ of rank at most $s - \ell$. The claimed result follows from setting of our parameters. ■

IV. Algebraic Geometry Codes are Good Erasure List-Decodable Codes

In the previous section, we proved that random codes are good erasure list-decodable codes. There is still a lack of constructive results on erasure list decoding. Though Guruswami [6] presented a constructive result from concatenated codes, the rate is extremely small. In this section, we show that algebraic geometry (AG for short) codes are good erasure list-decodable codes and furthermore they can be list decoded in polynomial-time. As a preparation, we recall some basic results on AG codes first. Readers may refer to [18] for more details.

Let $\mathcal{X}$ be a smooth, projective, absolutely irreducible curve of genus $g(\mathcal{X})$ (we will use g instead of $g(\mathcal{X})$ if there is no confusion in the context) defined over $\mathbb{F}_q$. We denote by $\mathbb{F}_q(\mathcal{X})$ the function field of $\mathcal{X}$. Denote by $N(\mathcal{X})$ the number of rational points of $\mathcal{X}$. Let $\mathcal{P} = \{P_1, ..., P_n\}$ be a set of n distinct rational points over $\mathbb{F}_q$. Let G be a divisor such that $\mathrm{Supp}(G) \cap \{P_1, ..., P_n\} = \emptyset$. Define $\mathcal{L}(G)$ as the Riemann-Roch space associated to G and denote $\dim \mathcal{L}(G) = \ell(G)$. The algebraic geometry code $C(G, \mathcal{P})$ is defined as the image of $\mathcal{L}(G)$ in $\mathbb{F}_q^n$ under the following evaluation map

$$C : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n, \quad f \mapsto (f(P_1), ..., f(P_n)).$$

If $n > \deg(G)$, then $C(G, \mathcal{P})$ is an $[n, \geq \deg(G) - g + 1, \geq n - \deg(G)]_q$-AG code. Throughout this section, we always assume that n is bigger than $\deg(G)$.

The gonality of a curve $\mathcal{X}$ was introduced in [14]. It is defined to be the smallest degree of a nonconstant map from $\mathcal{X}$ to the projective line. We denote the gonality of $\mathcal{X}$ by $t(\mathcal{X})$. More specifically, if $\mathcal{X}$ is defined over a field $\mathbb{F}_q$ and $\mathbb{F}_q(\mathcal{X})$ is the function field of $\mathcal{X}$, then $t(\mathcal{X})$ is the minimum degree of the field extensions of $\mathbb{F}_q(\mathcal{X})$ over a rational function field. It is easy to see that if $g(\mathcal{X}) = 0$, then $t(\mathcal{X}) = 1$. If $g(\mathcal{X}) = 1$ or 2, then $t(\mathcal{X}) = 2$. However, for general g, the gonality is no longer determined by genus. In general, we have the following lower bound for $t(\mathcal{X})$.

Lemma 4.1: ([14]) Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$ of genus g with N rational points. Then $t(\mathcal{X}) \geq N/(q + 1)$.

By using the lower bound on $t(\mathcal{X})$, one has the following proposition.

Proposition 4.2: $C(G,\mathcal{P})$ is $\left(\frac{1}{n}\left(n-\deg(G)+\lceil\frac{n}{q+1}\rceil-1\right),q\right)$-erasure list-decodable.

Proof: Let s be a positive integer with $s\le n-\deg(G)+\lceil\frac{n}{q+1}\rceil-1$. For any subset $T\subseteq\{1,2,\cdots,n\}$ of size $n-s$, we claim that

$$|\{\mathbf{c}\in C(G,\mathcal{P})|\mathbf{c}_T=\mathbf{0}\}|\le q.$$

This is equivalent to proving that

$$\dim\mathcal{L}\left(G-\sum_{i\in T}P_i\right)\le 1.$$

Suppose $\dim\mathcal{L}\left(G-\sum_{i\in T}P_i\right)\ge 2$, then one can choose a nonconstant function $f\in\mathcal{L}\left(G-\sum_{i\in T}P_i\right)$, i.e.,

$$(f)+G-\sum_{i\in T}P_i\ge 0.$$

Let $H=(f)+G-\sum_{i\in T}P_i\ge 0$. Then it is clear that

$$\deg(H)=\deg\left(G-\sum_{i\in T}P_i\right)=\deg(G)+s-n\le\left\lceil\frac{n}{q+1}\right\rceil-1\quad\text{and}\quad\dim\mathcal{L}(H)=\dim\mathcal{L}\left(G-\sum_{i\in T}P_i\right)\ge 2.$$

Choose a function $z\in\mathcal{L}(H)\setminus\mathbb{F}_q$, then $[\mathbb{F}_q(\mathcal{X}):\mathbb{F}_q(z)]$ is at most $\deg(H)\le\lceil\frac{n}{q+1}\rceil-1<\frac{N}{q+1}$. This contradicts Lemma 4.1.

Our desired result follows from Definition 1.1. ■

Proposition 4.2 can be extended by the Griesmer bound through the following lemma.

Lemma 4.3: If a divisor G satisfies $\ell(G)\ge t\ge 1$ and $\deg G<N$, then $\deg(G)\ge N\cdot\frac{q^{t-1}-1}{q^t-1}$, where N stands for the number of rational points on $\mathcal{X}$.

Proof: Suppose $P_1,\ldots,P_N$ are N distinct rational points on $\mathcal{X}$. By the strong approximation theorem, there exists $x\in\mathbb{F}_q(\mathcal{X})$ such that $\mathrm{Supp}((x)+G)\cap\{P_1,\ldots,P_N\}=\emptyset$. Then $\ell((x)+G)=\ell(G)$ and $\deg((x)+G)=\deg(G)$. Thus, we can obtain an algebraic geometry code $C((x)+G,\{P_1,\ldots,P_N\})$ with parameters $[N,\ell(G),d\ge N-\deg(G)]_q$. By the Griesmer bound [13], we have

$$N\ge\sum_{i=0}^{\ell(G)-1}\left\lceil\frac{d}{q^i}\right\rceil\ge\sum_{i=0}^{t-1}\left\lceil\frac{d}{q^i}\right\rceil\ge(N-\deg(G))\sum_{i=0}^{t-1}\frac{1}{q^i}.$$

Thus, the desired result follows from the above inequality. ■

Theorem 4.4: If G satisfies $\ell(G)\ge t\ge 1$ and $\deg(G)<n$, then $C(G,\mathcal{P})$ is $\left(\frac{1}{n}\left(n-\deg(G)+\lceil\frac{q^{t-1}-1}{q^t-1}n\rceil-1\right),q^{t-1}\right)$-erasure list-decodable.

Proof: Let s be an integer satisfying $s\le n-\deg(G)+\lceil\frac{q^{t-1}-1}{q^t-1}n\rceil-1$. For any $T\subseteq\{1,2,\cdots,n\}$ of size $n-s$, we have

$$\deg\left(G-\sum_{i\in T}P_i\right)=\deg(G)-|T|=\deg(G)-n+s\le\left\lceil\frac{q^{t-1}-1}{q^t-1}n\right\rceil-1<N\cdot\frac{q^{t-1}-1}{q^t-1}.$$

By Lemma 4.3, we have

$$\ell\left(G-\sum_{i\in T}P_i\right)\le t-1.$$

Our desired result follows from Definition 1.1. ■

Remark 4.5: When $t=1$, Theorem 4.4 shows that $C(G,\mathcal{P})$ is $\left(\frac{1}{n}\left(n-\deg(G)-1\right),1\right)$-erasure list-decodable. For $t=2$, we obtain the result of Proposition 4.2.

Combing Lemma 2.4 and Theorem 4.4, we immediately obtain the following lower bound on generalized Hamming weight of algebraic geometry codes.

Corollary 4.6: For $1\le t\le\deg(G)-g+1$, the t-th generalized Hamming weight of $C(G,\mathcal{P})$ satisfies

$$d_t(C(G,\mathcal{P}))\ge n-\deg(G)+\left\lceil\frac{q^{t-1}-1}{q^t-1}n\right\rceil.$$

Now we come to the main result of this section.

Theorem 4.7: Let q be a square. For any small $\epsilon>0$ and τ with $0<\tau<1-\frac{1}{\sqrt{q}-1}+\frac{1}{q}-\epsilon$ where q and ϵ are independent, there exists a family $\{C(G,\mathcal{P})\}$ of algebraic geometry codes with length tending to ∞ such that $C(G,\mathcal{P})$ have rate at least $1-\tau-\frac{1}{\sqrt{q}-1}+\frac{1}{q}-\epsilon$ and are $(\tau,O(\frac{1}{\epsilon}))$-erasure list-decodable. Furthermore, it can be list decoded in $O((n\log_q n)^3)$ time, where n is the length of the code.

Proof: Choose a curve $\mathcal{X}/\mathbb{F}_q$ in the Garcia-Stichtenoth tower [5]. Then $N(\mathcal{X})/g(\mathcal{X}) \to \sqrt{q}-1$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ with $n = N(\mathcal{X}) - 1$. Choose the last rational point P of $\mathcal{X}$ such that $P \notin \mathcal{P}$. Put

$$m := n - \lceil \tau n \rceil + \left\lceil \frac{q^{t-1}-1}{q^t-1} n \right\rceil - 1$$

and $G = mP$. By Theorem 4.4, $C(G, \mathcal{P})$ is $\left(\frac{1}{n}\left(n - m + \lceil \frac{q^{t-1}-1}{q^t-1} n \rceil - 1\right), q^{t-1}\right)$-erasure list-decodable for any constant $t \geq 1$. Hence, $C(G, \mathcal{P})$ is (τ, q^{t-1})-erasure list-decodable. Pick $\epsilon = \frac{1}{q} - \frac{q^{t-1}-1}{q^t-1} = \frac{q-1}{q(q^t-1)}$, then $q^{t-1} = O(\frac{1}{\epsilon})$. Moreover, the rate of $C(G, \mathcal{P})$ is at least

$$\frac{1}{n}(m - g + 1) \to 1 - \tau - \frac{1}{\sqrt{q}-1} + \frac{q^{t-1}-1}{q^t-1} = 1 - \tau - \frac{1}{\sqrt{q}-1} + \frac{1}{q} - \epsilon.$$

This proves the first statement of the theorem.

Finally by [17], we know that a basis of $\mathcal{L}(G)$ can be found in $O((n \log_q n)^3)$ time, where n is the length of the code. Thus, the generator matrix of the desired algebraic geometry codes can be found in polynomial time. The list decoding algorithm is equivalent to solving a linear system of k unknowns and $(1-\tau)n$ equations, which can be solved in $O(n^3)$ time [15, Problem 6.11]. This completes the proof. ■

OPEN PROBLEMS

For adversarial error channel, it has been shown that, given decoding radius $0 < \tau < 1$, the optimal rate for list decoding is $R = 1 - H_q(\tau)$, where $H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$ is the q-ary entropy function. More precisely speaking, for any small $\epsilon > 0$ and τ with $0 < \tau < 1 - 1/q$, with high probability a random code is $(1 - H_q(\tau) - \epsilon, O(\frac{1}{\epsilon}))$-list decodable. Furthermore, every q-ary $(1 - H_q(\tau) - \epsilon, L)$-list-decodable code has list size at least $\Omega(\log 1/\epsilon)$. Using probabilistic arguments, it is shown that with high probability a list size of $\Omega(1/\epsilon)$ is needed for list decoding random linear codes from random errors [10]. Under the situation of erasure list decoding, the optimal rate R that one could achieve is $R = 1 - \tau$. If we denote $L_{\tau,q}(\epsilon)$ to be the smallest integer L for which there are q-ary (τ, L)-erasure list-decodable codes of rate at least $1 - \tau - \epsilon$ for infinitely many lengths n, then it follows from Theorem 3.3 and Lemma 2.5 (ii) that $\Omega(\frac{1}{\epsilon}) \leq L_{\tau,q}(\epsilon) \leq q^{O(1/\epsilon)}$ and this upper bound was proved to be tight for random linear codes [10]. Now the first open problem is

Open Problem 1: Determine $L_{\tau,q}(\epsilon)$ for arbitrary codes.

In the literature, there are not many results on constructive bounds on erasure list decoding except for sufficiently large q or small rate [6], [11]. The second open problem would be

Open Problem 2: Narrow the rate gap between $1 - \tau - \frac{1}{\sqrt{q}-1} + \frac{1}{q}$ and $1 - \tau$ by constructing erasure list-decodable codes explicitly, i.e., construct a q-ary (τ, L)-erasure list-decodable codes of rate $R > 1 - \tau - \frac{1}{\sqrt{q}-1} + \frac{1}{q}$ such that the list size L is either a constant or a polynomial in length. The alphabet size q considered here is a relatively small constant.

REFERENCES

[1] A. Ashikhmin, A. Barg and S. Litsyn, "New upper bounds on generalized weights", *IEEE. Trans. Inform. Theory,* **45**, pp. 1258-1263, 1999.
[2] G. D. Cohen, S. N. Litsyn and G. Zémor, "Upper bounds on generalized distances", *IEEE. Trans. Inform. Theory,* **40**, pp. 2090-2092, 1994.
[3] P. Elias, "List-decoding for noisy channels", MIT, Res. Lab. Electron., Cambridge, MA, Tech. Rep. 335, 1957.
[4] P. Elias, "Coding for two noisy channels", Information Theory, Third London Symposium, pp. 61-76, 1995.
[5] A. Garcia, H. Stichenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound", Inventiones Mathematicae, **121**, pp.211–222, 1995.
[6] V. Guruswami, "List decoding from erasure: Bounds and code constructions," *IEEE. Trans. Inform. Theory,* **49**, pp.2826-2833, 2003.
[7] V. Guruswami, "List decoding of error correcting codes", Number 3282 in Lecture Notes in Computer Science. Springer, 2004.
[8] V. Guruswami and P. Indyk, "Linear-time list decoding in error-free settings", Lecture Notes in Computer Science. **3142**, PP. 695-707, 2004.
[9] V. Guruswami and P. Indyk, "Near-optimal linear time codes for unique decoding and new list-decodable codes over small alphabets", In Proceedings of the 34nd Annual ACM Symposium on Theory of Computing, pp.812-821, 2002.
[10] V. Guruswami, S. Narayanan, "Combinatorial Limitations of Average-Radius List Decoding", Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques Lecture Notes in Computer Science Volume **8096**, 2013, pp 591-606
[11] V. Guruswami and M. Sudan, "List decoding algorithms for certain concatenated codes", In Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, pp.181-190, 2000.
[12] T. Helleseth, T. Kløve, V. I. Levenshtein and Ø. Ytrehus, "Bounds on minimum support weights", *IEEE. Trans. Inform. Theory,* **41**, pp.432-440, 1995.
[13] S. Ling and C. P. Xing, *Coding Theory – A First Course,* Cambridge University Press, 2004.
[14] R. Pellikaan, "On the gonality of curves, abundant codes and decoding", Lecture notes in Math., **1518**, 132-144, Springer, Berlin, 1992.
[15] R. Roth, *Introduction to coding theory*, Cambridge University Press, 2006.
[16] A. Rudra and S. Uurtamo, "Two theorem in list decoding", APPROX/RANDOM'10 Proceedings of the 13th international conference on Approximation, and 14 the International conference on Randomization, and combinatorial optimization: algorithms and techniques Pages 696-709, 2010.
[17] K. W. Shum, I. Aleshnikov, P. V. Kummer, H. Stichtenoth and V. Deolalikar, "A low-complexity algorithm for the construction of algebraic-geometry codes better than the Gilbert-Varshamov bound," *IEEE. Trans. Inform. Theory,* **47**, pp.2225-2241, 2001.
[18] H. Stichtenoth, *Algebraic Function Fields and Codes,* Springer Verlag, 1993.
[19] M. Sudan, "List decoding: Algorithms and applications", *SIGACT news*, **31**, pp.16-27, 2000.
[20] V. Wei, "Generalized Hamming weight for linear codes," *IEEE. Trans. Inform. Theory,* **37**, pp.1412-1418, 1991.
[21] J. M. Wozencraft, "List decoding", Quarterly Progress Report MIT, Res. Lab. Electron., Cambridge, MA, **48**, 1958.
[22] V. V. Zyablov and M. S. Pinsker, "List cascade decoding"(in Russian), *Probl. Inf. Transm.,* **17**, pp.29-34, 1981.

Yang DING received her Ph. D degree from Southeast University, China in 2010. Since then, she has been with Shanghai University as a Lecturer. Her interests include coding theory and cryptography.

Lingfei JIN received her Ph.D degree in mathematics from Nanyang Technological University, Singapore in 2013. She is currently an associate professor in Fudan University, China. Her research interests include classical and quantum coding.

Chaoping XING received his Ph.D. degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore. Since December of 2007, he has been with Nanyang Technological University and currently is a full Professor. Dr. Xing has been working on the areas of algebraic curves over finite fields, coding theory, cryptography and quasi-Monte Carlo methods, etc.