Optimal Rate Algebraic List Decoding Using Narrow Ray Class Fields

Xing Chaoping (NTU)

Joint Work with Venkat Guruswami (CMU)

to appear in SODA 2014

Nov 11, 2013

Outline

Outline

Outline

Outline

SECTION 1: BACKGROUND

Coding channel

Channel with adversarial noise, i.e., the channel can arbitrarily corrupt any subset of up to a certain number of symbols of the codeword.

Goal

Correct such errors and recover the original message/codeword efficiently.

Block Code

An error-correcting code C of block length N over a finite alphabet Σ of size q is a subset of Σ^N (one has to establish a bijection between the message set $\mathcal{M}$ and C).

Rate of a block code

Rate of C:

$$R := R(C) := \frac{\log_q |C|}{N} = \frac{\log_q |\mathcal{M}|}{N}.$$

Maximal number of corrupted symbols

Information-theoretically: we need to receive at least $R \times N = \log_q |\mathcal{M}|$ symbols correctly in order to recover the message.

Maximal number of corrupted symbols

In other words, if we assume that the channel allows at most τN errors, we must have $N - \tau N \geq RN$, i.e.,

$$\tau \leq 1 - R. \quad (1)$$

This τ is called the decoding radius.

Maximal number of corrupted symbols

In other words, if we assume that the channel allows at most τN errors, we must have $N - \tau N \geq RN$, i.e.,

$$\tau \leq 1 - R. \tag{1}$$

This τ is called the decoding radius.

Goal

Would like *both* R and τ to be large for a fixed alphabet size

- think of block length $N \to \infty$;
- play a trade-off game between R and τ.

Goal

Would like *both* R and τ to be large for a fixed alphabet size

- think of block length $N \to \infty$;
- play a trade-off game between R and τ.

Decoding strategy

The above trade-off game depends on our decoding strategy.

Communication model

$$\boxed{\mathbf{c}} \quad \longrightarrow \boxed{\quad\text{Channel}\quad} \longrightarrow \quad \boxed{\mathbf{u}}$$

$$\uparrow$$

$$\textit{noise}$$

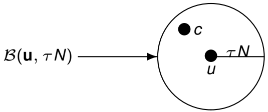
Decoding strategy

To recover **c** from **u**, we consider the intersection of the code C with the following Hamming ball:

$$\mathcal{B}(\mathbf{u}, \tau N) := \{\mathbf{x} \in \Sigma^N : \ d_H(\mathbf{x}, \mathbf{u}) \leq \tau N\}.$$

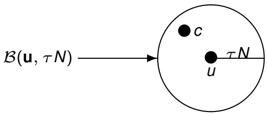
Decoding strategy

Claim: c must belong to this intersection!



Uniquely decodable

A code $C \subseteq \mathbb{F}_q^N$ is called "τ-uniquely decodable" if for every vector $\mathbf{u} \in \mathbb{F}_q^N$, the intersection $C \cap \mathcal{B}(\mathbf{u}, \tau N)$ contains at most one codeword.



Limit of unique decodability

If a code $C \subseteq \mathbb{F}_q^N$ with minimum distance d is "τ-uniquely decodable", then one has

$$\tau \leq (d-1)/2N.$$

Singleton bound

Every τ-uniquely decodable code satisfies

$$\tau \leq \frac{1}{2}(1 - R).$$

This is just half of the limit (1)!

Solution

Question: can we decode up to τN errors with τ close to the limit $1 - R$?

Answer: possible if we consider list-decoding

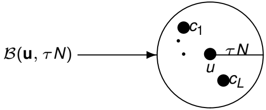
Solution

Question: can we decode up to τN errors with τ close to the limit $1 - R$?

Answer: possible if we consider list-decoding

List-decodable

For a positive integer L and real $0 < \tau < 1$, a code $C \subseteq \mathbb{F}_q^N$ is called "(τ, L)-list decodable" if for every vector $\mathbf{u} \in \mathbb{F}_q^N$, the intersection $C \cap \mathcal{B}(\mathbf{u}, \tau N)$ contains at most L codewords.



Trade-off game

One can image that as the decoding radius increases, the intersection $C \cap \mathcal{B}(\mathbf{u}, \tau N)$ becomes larger, i.e.,the list size L becomes larger.

Trade-off game

Trade-off: Optimize the rate R, decoding radius τ and list size L!

Note that we want large rate R and decoding radius τ, but small list size L.

Trade-off game

Trade-off: Optimize the rate R, decoding radius τ and list size L!

Note that we want large rate R and decoding radius τ, but small list size L.

Additional requirements for list-decodable codes

- small list size L (constant size or polynomial in code length);
- efficient method to find all codewords in the list.

Additional requirements for list-decodable codes

- small list size L (constant size or polynomial in code length);
- efficient method to find all codewords in the list.

Performance of random codes (Peter Elias, 1991)

For given small $\epsilon > 0$ and rate $R \in (0, 1)$, with high probability a random code over alphabet with size $\exp(O(1/\epsilon))$ has the following parameters:

Code length N:	arbitrarily large and independent of ϵ
Decoding radius:	$1 - R - \epsilon$ (close to the limit $1 - R$)
List size:	$O(1/\epsilon)$ (constant)

Problem for random codes

It is not known how to construct or even randomly sample such a code for which the associated algorithmic task of list decoding can be performed efficiently!

Problem to be solved

Construct codes with efficient list decoding and good parameters as random codes have!

SECTION 2: KNOWN RESULTS

Sudan's list decoding of Reed-Solomon (RS) codes

Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1-R)/2$ and $1-R$;

(ii) Length N is at most alphabet size.

Sudan's list decoding of Reed-Solomon (RS) codes

Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1-R)/2$ and $1-R$;

(ii) Length N is at most alphabet size.

Sudan's list decoding of Reed-Solomon (RS) codes

Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1-R)/2$ and $1-R$;

(ii) Length N is at most alphabet size.

Guruswami-Sudan's list decoding of algebraic-geometry (AG) codes

Guruswami-Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1-R)/2$ and $1-R$;

(ii) Length N is arbitrarily large.

Guruswami-Sudan's list decoding of algebraic-geometry (AG) codes

Guruswami-Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1-R)/2$ and $1-R$;

(ii) Length N is arbitrarily large.

Guruswami-Sudan's list decoding of algebraic-geometry (AG) codes

Guruswami-Sudan

$$\tau = 1 - \sqrt{R}$$

Remark:

(i) It is between $(1 - R)/2$ and $1 - R$;

(ii) Length N is arbitrarily large.

Guruswami-Rudra's list decoding of folded RS codes

Guruswami-Rudra

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(N^{1/\epsilon})$;

(ii) Length N is at most alphabet size.

Guruswami-Rudra's list decoding of folded RS codes

Guruswami-Rudra

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(N^{1/\epsilon})$;

(ii) Length N is at most alphabet size.

Guruswami-Rudra's list decoding of folded RS codes

Guruswami-Rudra

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(N^{1/\epsilon})$;

(ii) Length N is at most alphabet size.

Guruswami-Rudra's list decoding of folded RS codes

After pre-encoding (i.e., choose some subset of polynomials with bounded degree), the list size can be reduced to $O(1/\epsilon)$.

Guruswami-X.'s list decoding of AG subcodes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding + Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of AG subcodes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding + Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of AG subcodes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding + Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of AG subcodes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding + Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of AG subcodes

As a result, Guruswami-X.'s list decoding of AG subcodes achieves the performance of a random codes except for

(i) it is Monte-Carlo;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-X.'s list decoding of AG subcodes

As a result, Guruswami-X.'s list decoding of AG subcodes achieves the performance of a random codes except for

(i) it is Monte-Carlo;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-X.'s list decoding of AG subcodes

As a result, Guruswami-X.'s list decoding of AG subcodes achieves the performance of a random codes except for

(i) it is Monte-Carlo;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-Kopparty's deterministic version

By removing random sampling in Guruswami-X.'s list decoding of AG subcodes, Guruswami-Kopparty got a deterministic version of list decoding of algebraic geometry codes with

Guruswami-Kopparty's list decoding of AG subcodes

Guruswami-Kopparty.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is polynomial in length.

Guruswami-Kopparty's list decoding of AG subcodes

Guruswami-Kopparty.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is polynomial in length.

Guruswami-Kopparty's list decoding of AG subcodes

Guruswami-Kopparty.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is polynomial in length.

Guruswami-Kopparty's list decoding of AG subcodes

Guruswami-Kopparty.

$$\tau = 1 - R - \epsilon$$

Remark:

(i) List size is $O(1/\epsilon)$ (pre-encoding);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is polynomial in length.

SECTION 3: MAIN RESULT

Guruswami-X.'s list decoding of folded AG codes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

(i) List size is polynomial in length N (no pre-encoding, no Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of folded AG codes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

(i) List size is polynomial in length N (no pre-encoding, no Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of folded AG codes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

(i) List size is polynomial in length N (no pre-encoding, no Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of folded AG codes

Guruswami-X.

$$\tau = 1 - R - \epsilon$$

(i) List size is polynomial in length N (no pre-encoding, no Monte-Carlo);

(ii) Length N is arbitrarily large.

(iii) Alphabet size is $\tilde{O}(\exp(1/\epsilon^2))$.

Guruswami-X.'s list decoding of folded AG codes

As a result, Guruswami-X.'s list decoding of folded AG codes achieves the performance of a random codes except for

(i) efficient encoding is needed;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-X.'s list decoding of folded AG codes

As a result, Guruswami-X.'s list decoding of folded AG codes achieves the performance of a random codes except for

(i) efficient encoding is needed;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-X.'s list decoding of folded AG codes

As a result, Guruswami-X.'s list decoding of folded AG codes achieves the performance of a random codes except for

(i) efficient encoding is needed;

(ii) Alphabet size is slightly bigger than $O(\exp(1/\epsilon))$.

Guruswami-X.'s list decoding of folded AG codes

Remark:

(i) The underlying function field is constructed through class field theory, need to get an efficient encoding.

(ii) As long as encoding is efficient, decoding is efficient as well!

Guruswami-X.'s list decoding of folded AG codes

Remark:

(i) The underlying function field is constructed through class field theory, need to get an efficient encoding.

(ii) As long as encoding is efficient, decoding is efficient as well!

Folded AG codes by Guruswami-X.

Let $F/\mathbb{F}_q$ be a function field and let σ be an automorphism of $F/\mathbb{F}_q$. Assume that we have mN rational places

$$P_1, P_1^{\sigma}, \dots, P_1^{\sigma^{m-1}}, \dots, P_N, P_N^{\sigma}, \dots, P_N^{\sigma^{m-1}}$$

with $m \approx \Theta(1/\epsilon^2)$ and $mN = N(F/\mathbb{F}_q)$.

Folded AG codes by Guruswami-X.

Let D be a divisor of F such that $D^\sigma = D$. Consider the Riemann-Roch space $\mathcal{L}(D)$. Then

$$f^{\sigma^i} \in \mathcal{L}(D)$$

for any $f \in \mathcal{L}(D)$.

Folded AG codes by Guruswami-X.

A function $f \in \mathcal{L}(D)$ is encoded to

$$\pi(f) := \left(\begin{bmatrix} f(P_1) \\ f(P_1^{\sigma}) \\ \vdots \\ f(P_1^{\sigma^{m-1}}) \end{bmatrix}, \ldots, \begin{bmatrix} f(P_N) \\ f(P_N^{\sigma}) \\ \vdots \\ f(P_N^{\sigma^{m-1}}) \end{bmatrix} \right). \qquad (2)$$

Interpolation equation

Assume that $\pi(f)$ is sent out, then f satisfies an equation

$$A_0 + A_1 f + A_2 f^{\sigma} + \cdots + A_s f^{\sigma^{s-1}} = 0, \qquad (3)$$

where $s \approx \Theta(1/\epsilon)$ and A_i are functions determined by $\pi(f)$.

List size

Thus, the list size is the number of solutions of (3).

Conversion through Frobenius

Consider a cyclic extension F/L and assume that σ fixes L, i.e., $\sigma \in \mathrm{Gal}(F/L)$. Furthermore, assume

(i) $Q_1, \dots, Q_t$ are places of F of degree $r[F : L]$ that are completely insert in F/L;

(ii) σ is the Frobebius of Q_i for all $1 \leq i \leq t$.

Conversion through Frobenius

Equation (3) becomes

$$A_0 + A_1 f + A_2 f^{q^r} + \cdots + A_s f^{q^{r(s-1)}} \equiv 0 \mod Q_i \quad (4)$$

for $i = 1, 2, \ldots, t$.

Conversion through Frobenius

By the Chinese Remainder Theorem, the list size is at most

$$q^{rt(s-1)}$$

if $rt[F:L] > mN = N(F) \geq \deg(D)$.

List size

Conclusion: If rt is $O(\log N)$, then the list size is polynomial in N!

Decoding radius

The decoding radius satisfies

$$\tau = 1 - R - \epsilon - \frac{g(F)}{N(F)},$$

where R is the rate of the folded code.

Decoding radius

Assume that $\frac{g(F)}{N(F)} \to 1/q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

Conclusion: The decoding radius satisfies

$$\tau = 1 - R - \epsilon$$

if we let $q = (1/\epsilon)^{1/\lambda}$.

Code alphabet size

Conclusion: The code alphabet size is now

$$q^m = q^{1/\epsilon^2} = (1/\epsilon)^{O(1/\epsilon^2)} = \tilde{O}(\exp(1/\epsilon^2)).$$

Construction of function fields

Thus, we need a function field $F/\mathbb{F}_q$ satisfying

(a) $N(F)/g(F) \to 1/q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

(b) There exists a subfield $L/\mathbb{F}_q$ such that F/L is a cyclic extension and $[F : L] \approx N/\Theta(\log N)$.

(c) Let $rt = O(\log N)$. There exist places $Q_1, \dots, Q_t$ of F of degree $r[F : L]$ that are completely insert in F/L such that σ is the Frobebius of Q_i for all $1 \le i \le t$;

Construction of function fields

Thus, we need a function field $F/\mathbb{F}_q$ satisfying

(a) $N(F)/g(F) \to 1/q^\lambda$ for some $\lambda \in (0, 1/2]$.

(b) There exists a subfield $L/\mathbb{F}_q$ such that F/L is a cyclic extension and $[F : L] \approx N/\Theta(\log N)$.

(c) Let $rt = O(\log N)$. There exist places $Q_1, \ldots, Q_t$ of F of degree $r[F : L]$ that are completely insert in F/L such that σ is the Frobebius of Q_i for all $1 \le i \le t$;

Construction of function fields

Thus, we need a function field $F/\mathbb{F}_q$ satisfying

(a) $N(F)/g(F) \to 1/q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

(b) There exists a subfield $L/\mathbb{F}_q$ such that F/L is a cyclic extension and $[F : L] \approx N/\Theta(\log N)$.

(c) Let $rt = O(\log N)$. There exist places $Q_1, \dots, Q_t$ of F of degree $r[F : L]$ that are completely insert in F/L such that σ is the Frobebius of Q_i for all $1 \le i \le t$;

Construction of function fields

Thus, we need a function field $F/\mathbb{F}_q$ satisfying

(a) $N(F)/g(F) \to 1/q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

(b) There exists a subfield $L/\mathbb{F}_q$ such that F/L is a cyclic extension and $[F : L] \approx N/\Theta(\log N)$.

(c) Let $rt = O(\log N)$. There exist places $Q_1, \dots, Q_t$ of F of degree $r[F : L]$ that are completely insert in F/L such that σ is the Frobebius of Q_i for all $1 \leq i \leq t$;

Construction of function fields

Part (c) is easily satisfied by the Chebotarev density theorem which says:

> *The number of unramified places of L of degree r with Frobenius equal to the generator of $\mathrm{Gal}(F/L)$ is roughly $q^r/r[F:L]$.*

Construction of function fields

Question: How to construct a function field $F/\mathbb{F}_q$ satisfying

(a) $N(F)/g(F) \to 1/q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

(b) There exists a subfield $L/\mathbb{F}_q$ such that F/L is a cyclic extension and $[F : L] \approx N/\Theta(\log N)$.

SECTION 4: FUNCTION FIELDS FROM CLASS FIELDS

Currently available function fields

All currently available function field towers are not suitable:

(i) Garcia-Stichtenoth towers and their Galois closures;

(ii) Modular curves;

(iii) Class field towers.

Currently available function fields

All currently available function field towers are not suitable:

(i) Garcia-Stichtenoth towers and their Galois closures;

(ii) Modular curves;

(iii) Class field towers.

Currently available function fields

All currently available function field towers are not suitable:

(i) Garcia-Stichtenoth towers and their Galois closures;

(ii) Modular curves;

(iii) Class field towers.

Currently available function fields

All currently available function field towers are not suitable:

(i) Garcia-Stichtenoth towers and their Galois closures;

(ii) Modular curves;

(iii) Class field towers.

Construction

(i) Starting with any good tower or family $\{E/\mathbb{F}_\ell\}$ such that $N(E)/g(E) \to \sqrt{\ell} - 1$. Put $q = \ell^2$.

Construction

(ii) Choose a place Q of degree $e = \Theta(N(E))$ and consider the narrow ray class field $K/(\mathbb{F}_q \cdot E)$ with conductor Q. Then K/H is a cyclic extension of degree $q^e - 1$, where H is the Hilbert class field of $K/(\mathbb{F}_q \cdot E)$.

Construction

(iii) Take a subgroup G of $\mathrm{Gal}(K/(\mathbb{F}_q \cdot E))$ such that $\mathrm{Gal}(K/(\mathbb{F}_q \cdot E))/G$ is a cyclic group of order $(\ell^e - 1)/(\ell - 1)$ such that G contains all places of E. Then all place of E split completely in F, where $F = K^G$.

Construction

(iv) It can be easily shown that if $e/g(E) \to 2c$, then

$$N(F)/g(F) \to \frac{\sqrt{\ell}-1}{1+c} = \frac{q^{0.25}-1}{1+c}.$$

Construction

Conclusion: we have a function field family $\{F/\mathbb{F}_q\}$ such that

(i) $N(F)/g(F) \to q^{\lambda}$ for some $\lambda \in (0, 1/2]$.

(ii) Let $L = \mathbb{F}_q \cdot E$. Let $N = \epsilon^2 N(F) = \Theta(e[F : L])$ be our code length. Then F/L is a cyclic extension and $[F : L] = N/\Theta(\log N)$.

THANKS!