CS 229r Essential Coding Theory, Lecture 19 Apr 4, 2017

Lecture 19

Instructor: Madhu Sudan *Scribe: Zhixian Lei*

1 Overview

1. Local Recoverable Codes
2. Multiplicity Codes

2 Local Recoverable Codes

A code over a finite alphabet is called locally recoverable (LRC) if every symbol in the encoding is a function of a small number (at most r) of other symbols. More formally, a (n, k, r) Locally Recoverable Code (LRC) is a code that produces n symbol codeword from message of length k, and for any symbol of the codeword, there exists at most r other symbols such that the value of the symbol can be recovered from them. We say that the code has (r, d) locality if the code has distance $\geq d$ and every message (codeword) symbol can be reconstructed from r other symbols.

Note that here we have weak and strong notions of locally recoverability. For weak local recoverability only the message symbols are locally recoverable by r other codeword symbols. For strong local recoverability for every symbol in codeword we can recover it by r other codeword symbols.

2.1 LRC for weak recovery

Here we show a two-level construction of (r, d) LRC based on systematic Reed-Solomon Code combined with a single parity check $(r+1, r)$ code. Before giving the construction of the code, we introduce the systematic RS code.

Systematic RS code Suppose we want to transmit a message $b_0, b_1, \ldots b_{k-1} \in F_q$. Let $P(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1}$, then usually we encode the message by evaluating $P(x)$ on n different points for example $(P(0), P(1), \ldots, P(n))$. This representation is convenient since it requires no computation to define the polynomial. Let $Q(x) = c_0 + c_1 x_1 + \cdots c_{k-1}x^{k-1}$ such that $Q(0) = b_0, Q(1) = b_1, \ldots Q(k-1) = b_{k-1}$. Then we can also encode the message by evaluating $(Q(0), Q(1), \ldots, Q(n))$. This encoding has the advantage that our original message is actually sent as part of the encoding. A code with this property is called systematic code.

Now we give the construction of a LRC for weak recovery of (r, d) locality. Given message

$$m = m_1 m_2 \cdots m_r m_{r+1} m_{r+2} \cdots m_{2r} \cdots m_k$$

We first encode this message by systematic RS code

$$C_0 = m, RS(m)$$

where $RS(m)$ is the parity check part of systematic RS code. Then we add parity check bit for each r blocks

$$C = m, RS(m), \oplus_{i=1}^{r} m_i, \cdots \oplus_{i=k-r}^{k} m_i$$

In this way we achieve (r, d) locality and we have an upper bound for code length n for weak recovery

$$n \leq \frac{l+1}{l}k + d$$

2.2 Lower bound of message length [GHSY12]

First we recall the Singleton bound

Theorem 1 (Singleton Bound)**.** *For any (n, k, d) code, $d \leq n - k + 1$*

Proof. Let $E : \Sigma^k \to \Sigma^n$ and let $\pi : \Sigma^n \to \Sigma^{k-1}$ be projection to the first $k-1$ coordinates. Then $\pi \circ E : \Sigma^k \to \Sigma^{k-1}$. So there exists $x, x' \in \Sigma^k$ such that $\pi(E(x)) = \pi(E(x'))$ but $x \neq x'$. So $d \leq d(E(x), E(x')) \leq n - k + 1$ □

We can apply Singleton Bound to linear code. Let C be a (n, k, d) linear code and assume that the encoding of x is by the vector

$$C(x) = (c_1 \cdot x, c_2 \cdot x, \ldots, c_n \cdot x)$$

Thus C is specified by the set of n points $C = \{c_1, \ldots, c_n\}$. By the same technique of Singleton bound, we can prove following theorem

Theorem 2. *If a code C has distance d, for every $S \subset C$ such that $Rank(S) \leq k - 1$*

$$|S| \leq n - d$$

Proof. Let $S = \{c'_1, c'_2, \ldots c'_l\}$. Consider the projection $S(x) = (c'_1 \cdot x, c'_2 \cdot x, \ldots c'_l \cdot x)$ from Σ^k to Σ^{k-1}, then there exists $x, x' \in \Sigma^k$ such that $S(x) = S(x')$ and $x \neq x'$. So $d \leq n - |S|$, $|S| \leq n - d$ □

Using above theorem, we can prove the lower bound of n for linear code of locality (r, d)

Theorem 3. *For any (n, k, d) linear code of locality (r, d)*

$$(k-1)\frac{r+1}{r} \leq n - d$$

Proof. Our lower bound proceeds by constructing a large set $S \subset C$ where $Rank(S) \leq k - 1$ and apply Theorem 2. Initially $S = \emptyset$, For i from 1 to $\frac{k-1}{r}$, we pick $c_i \in C \backslash S$. Since every symbol can be reconstructed from r other symbols, c_i is linear dependent on other r elements in C. We call the set of these $r+1$ elements T_i, $Rank(T_i) \leq r$. Ad we let $S \leftarrow S \cup T_i$. In the end, the $Rank(S) \leq k - 1$ and $|S| \leq (k-1)\frac{r+1}{r}$. By Theorem 2, $(k-1)\frac{r+1}{r} \leq n - d$ □

2.3 Tamo-Barg Construction [TB14]

Now we give the Tamo-Barg construction for (r, d) LRC. Suppose $r + 1 | q - 1$, then there exists $w \in F_q$ such that $\{1, w, w^2, \ldots, w^r\}$ are distinct elements and $w^{r+1} = 1$. The code is defined as the subcode of RS code

$$C = \{(f(x))_{x \in F_q^*} | f(x) = \sum_{i \leq k} \alpha_i x^i, \alpha_i = 0 \text{ if } i = -1 \bmod r + 1\}$$

The dimension of this code is $k\frac{r}{r+1}$ since every $r + 1$ coefficients there is one of them to be 0. And the distance of this code is $n - k$ by standard argument.

Next we show the locality of this construction.

Theorem 4. *Tamo-Barg Construction achieves locality (r, d)*

Proof. Suppose some polynomial $f(x)$ satisfying that $f(x) = \sum_{i \leq k} \alpha_i x^i, \alpha_i = 0$ if $i = -1 \bmod r + 1$, then $f(x) \bmod (x^{r+1} - c)$ is a degree $r - 1$ polynomial. In addition, the evaluation of $f(x)$ on set $S_a = \{a, aw, \ldots aw^r\}$ for some element a is the same as the evaluation of $f(x) \bmod (x^{r+1} - a^{r+1})$ on the same set. But $f(x) \bmod (x^{r+1} - a^{r+1})$ is a degree $r - 1$ polynomial. So $f(a)$ is determined by $\{f(aw), \ldots f(aw^r)\}$ which achieves (r, d) locality. S_a is called a local set because for any element $x \in S_a$, $f(x)$ is determined by $f(y)$ for $y \in S_a \backslash x$ □

3 Multiplicity Code [KSY14]

In this section we study multiplicity codes which generalize the Reed-Muller codes and improve upon them in the regime of high rate. Recall the definition of (ϵ, l) local decoder. D is defined to be an (ϵ, l) local decoder for a given code C if $D^x(i)$ is a l local algorithm and $\forall x$ such that $\delta(x, E(m)) \leq \epsilon\delta(C)$ we have for all i, $\Pr[D^x(i) = E(m_i)] \leq 2/3$. Here we consider the regime of high rate with rate $R = 1 - \delta - o(1)$, locality $L = n^{o(1)}$ and we want to correct $\delta/2$ fraction of errors. For $\alpha > 0$ and $\beta > 0$, multiplicity codes can achieve $R \geq 1 - \alpha$ and $L \geq n^{\beta}$ and $\epsilon = \frac{\alpha\beta}{2}$

Recall locally decoding Reed-Muller codes $RM(m, d, q)$ for $m \geq 2$ and $n = q^m$. The locality $L = q = n^{\frac{1}{m}}$. When $d \to q$, the dimension of the code gives

$$\binom{m+d}{m} \approx \binom{m+q}{m} \approx \frac{q^m}{m!} = \frac{n}{m!}$$

So rate $R \leq \frac{1}{m!} \leq 1/2$. To improve this $1/2$ barrier, we use multiplicity codes which encode polynomial by its values and derivatives.

3.1 Example for $m = 2$ and first order derivatives

Consider polynomial $f(x, y)$. Let f_x be the derivative with respect to x and f_y be the derivative with respect to y. Then the encoding of f gives

$$E(f) = (f(\alpha, \beta), f_x(\alpha, \beta), f_y(\alpha, \beta))_{\alpha,\beta \in F_q}$$

The codes is over $\Sigma = F_q^3$, the code maps $\binom{d+2}{2}$ coefficients in F_q to q^2 elements of $\Sigma = F_q^3$. Let's consider the case when $d = (1 - \epsilon)2q$, the number of coefficients is close to $\frac{d^2}{2} \approx 2q^2$ when $\epsilon \to 0$. So the encoding is a map from $F_q^{2q^2} \to F_q^{3q^2}$, the rate is approaching $2/3$. We can also consider the case when $m = 1$ and the first order multiplicity code has distance $\geq \epsilon$ Then $d = (1 - \epsilon)2q$, the message is in space $F_q^{(1-\epsilon)2q} = \Sigma^{(1-\epsilon)q}$ where $\Sigma = F_q^2$ and codewords are in space Σ^q which gives rate close to $1 - \epsilon$

3.2 Locally decoding multiplicity codes

Similar to locally decoding Reed-Muller code, if we want to locally decode for point (b_1, b_2), we can try to pick a random line going through (b_1, b_2). For example, we randomly pick a line $x = a_1t + b_1$ and $y = a_2t + b_2$. Then the evaluations of the polynomial $f(x, y)$ on this line l can be reduced to

$$h(t) = f(a_1t + b_1, a_2t + b_2)$$

The degree of h is $\leq d$ and we can also get the derivative of h on t

$$h'(t) = a_1f_x(a_1t + b_1) + a_2f_y(a_2t + b_2)$$

Then we do the univariate multiplicity codes decoding by the result in previous exercise. The problem now is how to recover $f_x(b_1)$ and $f_x(b_2)$ from $h'(t)$. To have this, we need two random lines $h_1(t)$ and $h_2(t)$ and do the univariate multiplicity codes decoding. Then we can transform $h_1'(0)$ and $h_2'(0)$ to $f_x(b_1)$ and $f_y(b_2)$

The conclusion is that for $m = 2$ and first order derivatives, if $d = (1 - \epsilon)2q$, then Rate $R = \frac{2}{3}(1 - \epsilon)^2$ if we want to corrects $\Omega(\epsilon)$ fraction of errors with $O(q) = O(\sqrt{n})$ locality. We can also generalize this result to general multiplicity code (m, d, q, s) where s denotes the multiplicity. Then encoding of polynomial f of degree $\leq d$ gives

$$\left\{(f_{e_1,e_2,\ldots,e_m}(x)) \,|\, \sum e_i \leq S\right\}_{x \in F_q^m}$$

The alphabet $\Sigma = F_q^{\binom{m+s}{s}}$, $n = q^m$, the locality is still $O(q) = O(n^{\frac{1}{m}} = n^{\beta}$ if we let $m = \frac{1}{\beta}$. $d = (1-\epsilon)sq$, the rate becomes

$$R = \frac{\binom{m+d}{m}}{\binom{m+s}{m}q^m} \approx \frac{d^m m!}{m! s^m q^m} \approx (\frac{d}{sq})^m$$

where we assume $s \approx m^2$. In general let $m = \frac{1}{\beta}$ and $s = \frac{1}{\alpha\beta}$ we have $\epsilon = \alpha\beta$

Further we can think of using Hasse derivatives which is defined as: the ith Hasse derivatives of polynomial $f(x)$ is the coefficient of z^i in the polynomial $f(x+z)$. Thus $f(x+z) = \sum f^{(i)}(x)z^i$ there are some properties for Hasse derivatives but we will not discuss them in detail.

References

[GHSY12] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information Theory*, 58(11):6925–6934, 2012.

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM (JACM)*, 61(5):28, 2014.

[TB14] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.