6.895 Essential Coding Theory October 25, 2004

Lecture 12

Lecturer: Madhu Sudan *Scribe: Kevin Matulef*

1 Overview

Today we will continue talking about achieving good rates with list-decodable codes nonconstructively. Then we will begin talking about trying to achieve these rates constructively, and briefly discuss algebraic geometry codes.

2 Nonconstructive Results on List Decoding

Theorem 1 *There $\exists$ a family of linear binary codes of rate $R = 1 - H_2(p)$ that are (p, n) list-decodable (here p is the fraction of errors corrected, and n is the list size).*

Proof

We construct such a code by choosing linearly independent vectors $b_1, b_2, ..., b_k$ (where $k = R \cdot n$) greedily. At each stage i, we choose the next b_{i+1} so as to minimize the following potential function:

$$\Phi_i = \text{Exp}_x[2^{|C_i \cap B(x,pn)|}] \text{ , where } C_i = span\{b_1...b_i\}$$

From this we can conclude the following:

1. $\Phi_0 = 1 + \frac{|B(0,pn)|}{2^n} \approx 1 + 2^{(H(p)-1)n}$
2. $\forall b_1...b_i, \text{Exp}_{b_{i+1}}[\Phi_{i+1}] \leq \Phi_i^2$.

   Why should this be true? Suppose that we've already chosen $b_1...b_i$. Then by definition, we have

$$\text{Exp}_{b_{i+1}}[\Phi_{i+1}] = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} 2^{|C_{i+1} \cap B(x,pn)|}$$

   Now note that $C_{i+1} \cap B(x, pn) = (C_i \cap B(x, pn)) \cup (C_i \cap B(x - b_{i+1}, pn))$, and thus $|C_{i+1} \cap B(x, pn)| \leq |C_i \cap B(x, pn)| + |C_i \cap B(x - b_{i+1}, pn)|$. Substituting, we get:

$$\text{Exp}_{b_{i+1}}[\Phi_{i+1}] \leq \frac{1}{2^n} \sum_{x \in \{0,1\}^n} 2^{|C_i \cap B(x,pn)|} \cdot 2^{|C_i \cap B(x - b_{i+1},pn)|}$$

$$\leq \frac{1}{4^n} \sum_{x, b_{i+1} \in \{0,1\}^n} 2^{|C_i \cap B(x,pn)|} \cdot 2^{|C_i \cap B(x - b_{i+1},pn)|}$$

$$= \frac{1}{4^n} \sum_{x \in \{0,1\}^n} 2^{|C_i \cap B(x,pn)|} \sum_{z \in \{0,1\}^n} 2^{|C_i \cap B(z,pn)|}$$

$$= \Phi_i^2$$

3. $\Phi_k \leq \Phi_0^{2^k}$.

   This we can see by combining the previous points, and assuming we choose $b_1...b_k$ appropriately.

4. Finally, by combining points 1 and 3 above, and using the approximation that $(1+\epsilon)^n \approx 1+\epsilon n$, we can conclude that $\Phi_k \leq 1+2^{k+(H(p)-1)n}$. When $R < 1-H(p)$, this means $\Phi_k \leq 2$. Looking at the definition of Φ_k, we see that if any ball of radius pn had $n+1$ codewords, then the expected value of $2^{|C_k \cap B(x,pn)|}$ would be greater than 2. Therefore, no ball can have more than n codewords in it.

■

In the above proof, $b_1, ...b_k$ are chosen greedily. It is an open question to see if we get the same result when we pick them completely randomly. In other words, are *most* codes (p,n) list-decodable?

3 Constructive Results vs Nonconstructive Results

We would like to construct a family of $(1/2-\epsilon)$ list-decodable codes of "high" rate. We've seen that the best possible is $1-H(1/2-\epsilon) = \Theta(\epsilon^2)$.

One approach is to construct codes of relative distance $1/2-\epsilon^2$ and use them. We know that these codes are $(1/2-\epsilon, n)$ list decodable.

If we use concatenation codes, what we get is the following:

Outer Code needs large distance $1-\tau \Rightarrow$ rate $\leq \tau$.

Inner Code has $1/2-\tau/2$ relative distance $\Rightarrow$ rate $= \Theta(\tau^2)$.

The combined code has relative distance $(1-\tau)\cdot(1/2-\tau/2) = \frac{(1-\tau)^2}{2} \geq 1/2-\tau$, while the rate is $\Theta(\tau^3)$. So this approach gives a rate of $\Theta(\tau^3)$, but we know that codes exist with rate $\Theta(\tau^2)$. This is a good illustration of the gap between current constructive and nonconstructive results.

Actually, the gap is even worse than this, since if we are shooting for relative distance $1/2-\epsilon^2$, using the above approach with concatenation codes we get a rate of $\Theta(\epsilon^6)$.

Further, there is still a problem with decoding. Suppose that a $1/2-\delta$ fraction of errors has occured overall. The inner code is able to correct $1/2-\epsilon$ fraction of errors. We can analyze to show that a $\delta-\epsilon$ fraction of the blocks must have less than $1/2-\epsilon$ fraction of errors. The distance comes out to be roughly $1/2-\delta^2$ and rate roughly δ^4.

Putting this together, we see that the decoding algorithm constructed has rate $\leq O(\epsilon^8)$. Although it is known how to reduce this to $O(\epsilon^4)$ using more sophisticated decoding techniques, nobody has been able to achieve $O(\epsilon^3)$ or $O(\epsilon^2)$. Doing so would be an important accomplishment.

We have already discussed the case when $\delta = 1/2-\epsilon$ as $\epsilon \to 0$, and said that the gap in the rate is $O(\epsilon^3)$ for constructive results, and $O(\epsilon^2)$ for nonconstructive. We can also consider the gap in terms of relative distance. Let $R = 1-\delta\log\frac{1}{\delta}$ so if $\epsilon = \delta\log\frac{1}{\delta}$ we can approximate $\delta \approx \frac{\epsilon}{\log 1/\epsilon}$. The nonconstructive result then gives us $\delta = \frac{\epsilon}{\log 1/\epsilon}$, while the constructive result involves concatenating a code of relative distance $\frac{\epsilon}{2}$ with one of relative distance $\frac{\epsilon}{2\log 1/\epsilon}$ for a total relative distance of $\delta = \frac{\epsilon^2}{\log 1/\epsilon}$.

Early in coding theory, theorists were generally converging on the thesis "random codes are the best codes." Slowly though, a series of codes such as the RS codes, BCH codes, and Hadamard codes were observed to have properties that made them better than random codes. For example, when $q \geq n$, the RS codes are $[n,k,n-k]_q$ while random codes are $[n,k,n-k-\frac{n}{\log q}]_q$. This led to a refined version of the thesis: "asymptotically, for any *fixed* alphabet, random codes are the best (when $R, \delta > 0, q < \infty, n \to \infty$)."

4 Algebraic Geometry Codes

These codes were conceived of by V.D. Goppa ('79), and finally developed and proved by Tsfasman, Vladuts, Zink ('82).

Goppa looked at the RM codes, consisting of multivariate polynomials evaluated at many points, but instead of evaluating the polynomials on all points in the space, he considered evaluating the polynomials on a subset of points.

- Set of messages=$\{$set of polynomials in m variables$\}$.
- Code=evaluation of polynomials on a subset $S \subset \mathbb{F}_q^m$

Tsfasman, Vladuts, and Zink used a subset S of size approximately $q^{m/2}$, yielding the following result:

Theorem 2 *$\forall q$ st q is a prime power and q is a square, there $\exists$ $[n, k, n-k-\frac{n}{\sqrt{q}-1}]_q$ codes.*

Note that a random code has distance roughly $n-k-\frac{n}{\log q}$, which is slightly worse than the result above. The constants turn out to be such that the algebraic geometry codes outperform random codes for $q \geq 49$.

This has led to a new version of the refined thesis: that random codes are still the best when $q = 2$ or 3. The truth of this new conjecture is still very much up for debate.