Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 14: List Decoding Capacity

October 2, 2007

Lecturer: Atri Rudra *Scribe: Thanh-Nhan Nguyen*

In the last lecture, we stated a theorem for list decoding capacity, which we restate here:

Theorem 0.1 (List-Decoding Capacity). *Let $q \geq 2$ be an integer, and $0 < \rho < 1 - \frac{1}{q}$ be a real.*

(i) Let $L \geq 1$ be an integer, there exists an (ρ, L)-list decodable code with rate

$$R \leq 1 - H_q(\rho) - \frac{1}{L}$$

(ii) For every (ρ, L) code of rate $1 - H_q(\rho) + \varepsilon$, L needs to be exponential in block length of the code.

In this lecture, we will prove this theorem.

1 Proof of Theorem 0.1

Proof. We start with the proof of (i). Pick a code C at random where

$$|C| = q^k, k \leq (1 - H_q(\rho) - \frac{1}{L})n.$$

That is, as in Shannon's proof, for every message $\mathbf{m}$, pick $C(\mathbf{m})$ uniformly at random from $[q]^n$.

Definition 1.1. *Given $\mathbf{y} \in [q]^n$, and $\mathbf{m}_0, \cdots, \mathbf{m}_L \in [q]^k$, tuple $(\mathbf{y}, \mathbf{m}_0, \cdots, \mathbf{m}_L)$ defines a "bad event" if*

$$C(\mathbf{m}_i) \in B(\mathbf{y}, \rho n), 0 \leq i \leq L$$

where recall that $B(\mathbf{x}, e) = \{\mathbf{z} | \Delta(\mathbf{x}, \mathbf{z}) \leq e\}$

Fix $\mathbf{y} \in [q]^n$, $\mathbf{m}_0, \cdots, \mathbf{m}_L \in [q]^k$.
Note that for fixed i, by the choice of C, we have:

$$Pr[C(\mathbf{m}_i) \in B(\mathbf{y}, \rho n)] = \frac{Vol_q(\mathbf{y}, \rho n)}{q^n} \leq q^{-n(1-H_q(\rho))}, \tag{1}$$

where the inequality follows from the upper bound on the volume of a Hamming ball that we have already seen. Now the probability of a bad event given $(\mathbf{y}, \mathbf{m}_0, \cdots, \mathbf{m}_L)$ is

$$Pr\left[\bigwedge_{i=0}^{L} C(\mathbf{m}_i) \in B(\mathbf{y}, \rho n)\right] = \prod_{0}^{L} Pr[C(\mathbf{m}_i) \in B(\mathbf{y}, \rho n)] \leq q^{-n(L+1)(1-H_q(\rho))},$$

where the equality follows from the fact that the random choice of codewords for distinct messages are independent and the inequality follows from (1). Then,

$$\begin{aligned}
Pr[\text{ any bad event}] &\leq q^n \binom{q^k}{L+1} q^{-n(L+1)(1-H_q(\rho))} && (2)\\
&\leq q^n q^{Rn(L+1)} q^{-n(L+1)(1-H_q(\rho))} && (3)\\
&= q^{-n(L+1)[1-H_q(\rho)-\frac{1}{L+1}-R]} \\
&\leq q^{-n(L+1)[1-H_q(\rho)-\frac{1}{L+1}-1+H_q(\rho)+\frac{1}{L}]} && (4)\\
&= q^{-\frac{n}{L}} \\
&< 1
\end{aligned}$$

In the above, (2) follows by counting the number of $\mathbf{y}$'s , and the number of $L+1$ tuples. (3) follows from the fact that $\binom{a}{b} \leq a^b$, and $k = Rn$. (4) follows by assumption $R \leq 1 - H_q(\rho) - \frac{1}{L}$. Rest of the steps follow from rearranging and canceling the terms. Therefore, by probabilistic method, there exists C such that it is (ρ, L)-list decodable.

Now we turn to the proof of part (ii). For this part, we need to show the existence of a $\mathbf{y} \in [q]^n$ such that $|C \cap B(\mathbf{y}, \rho n)|$ is super-polynomially large for every C of $R \geq 1 - H_q(\rho) + \varepsilon$.
Pick $\mathbf{y} \in [q]^n$ at random. Fix $\mathbf{c} \in C$. Then

$$\begin{aligned}
Pr[\mathbf{c} \in B(\mathbf{y}, \rho n)] &= Pr[\mathbf{y} \in B(\mathbf{c}, \rho n)] \\
&= \frac{Vol(\mathbf{y}, \rho n)}{q^n} && (5)\\
&\geq q^{-n(1-H_q(\rho))-o(n)}, && (6)
\end{aligned}$$

where (5) follows from the fact that $\mathbf{y}$ is chosen uniformly at random from $[q]^n$ and (6) follows by the lower bound on the volume of the Hamming ball that we have seen earlier. We define

$$X_{\mathbf{c}} = \begin{cases} 1 & \text{if } \mathbf{c} \in B(\mathbf{y}, \rho n) \\ 0 & \text{otherwise} \end{cases}$$

We have

$$\begin{aligned}
E[|B(\mathbf{y}, \rho n)|] &= \sum_{\mathbf{c} \in C} E[X_{\mathbf{c}}] && (7)\\
&= \sum_{\mathbf{c} \in C} Pr[X_{\mathbf{c}} = 1] \\
&\geq \sum_{\mathbf{c} \in C} q^{-n(1-H_q(\rho)+o(n))} && (8)\\
&= q^{n[R-1+H_q(\rho)-o(1)]} \\
&\geq q^{\Omega(n)} \\
& && (9)
\end{aligned}$$

In the above, (7) follows by the linearity of expectation, (8) follows from (6), and (9) follows by choice of R. Hence, by probabilistic method, there exists $\mathbf{y}$ such that $|B(\mathbf{y}, \rho n) \cap C|$ is $q^{\Omega(n)}$, as desired. $\square$

Remark 1.2. *The proof above can be modified to work for random linear codes. In particular, one can show that with high probability, a random linear code is* (ρ, L)*-list decodable code as long as*

$$R \leq 1 - H_q(\rho) - \frac{1}{\lceil \log_q(L+1) \rceil}.$$

The details are left as an exercise. This means that there exists linear codes with rate $1 - H_q(\rho) - \varepsilon$ *that are* $\left(\rho, q^{O(1/\varepsilon)}\right)$*-list decodable. However, just for* $q = 2$*, one can show the* existence *of* $(\rho, O(1/\varepsilon))$*-list decodable codes [2] (though it is not a high probability result).*

The following questions are still open:

1. Is a random linear binary code of rate $1 - H(\rho) - \varepsilon$ with high probability $(\rho, O(1/\varepsilon))$-list decodable?
2. Does there exist a q-ary linear code (for $q > 2$) of rate $1 - H_q(\rho) - \varepsilon$ that is $\left(\rho, q^{o(1/\varepsilon)}\right)$ list-decodable?

It has been conjectured that the answer to both of these questions is positive [1].
Update: Jan 2010 Guruswami, Håstad and Kopparty have solved the open questions above by showing that random linear codes of rate $1 - H_q(\rho) - \varepsilon$ are $(\rho, O(1/\varepsilon))$-list decodable.

References

[1] Venkatesan Guruswami. *List decoding of error-correcting codes*. Number 3282 in Lecture Notes in Computer Science. Springer, 2004. (Winning Thesis of the 2002 ACM Doctoral Dissertation Competition).

[2] Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1035, 2002.