6.440 Essential Coding Theory March 5, 2008

Lecture 9

Lecturer: Madhu Sudan *Scribe: Shubhangi Saraf*

Today we'll summarize what we've seen so far on the combinatorics of codes and we'll see the proof be Alon for a bound for 'balanced codes'. Next lecture we'll move on to the *algorithmics* of codes. The lecture on March 31^{st} is canceled.

1 Summary of the three basic bounds

Consider the case of the binary alphabet, i.e. $q = 2$. We'll look at families of codes of the form $C_i = (n_i, k_i, d_i)_2$, where $\lim_{i\to\infty} n_i = \infty$, $\lim_{i\to\infty} \frac{d_i}{n_i} = \delta$, and $\lim_{i\to\infty} \frac{k_i}{n_i} = R$. We'll look at the asymptotic bounds that we can prove on rate R of such codes as $\delta \to 0$ and as $\epsilon \to 0$ for when $\delta = 1/2 - \epsilon$. The summary of our results so far is given in the table below.

	R as $\delta \to 0$	R as $\delta = \frac{1}{2} - \epsilon$ and $\epsilon \to 0$
Negative Result	$R \geq 1 - \frac{\delta}{2}\log\frac{1}{\delta}$−(lower order)	$R \leq 1 - 2\delta = 2\epsilon = O(\epsilon)$ (Elias/Plotkin)
Existential Result	$R \geq 1 - \delta\log\frac{1}{\delta}$−(lower order)	$R = \Omega(\epsilon^2)$
Constructive Result	$R \geq 1 - O(\sqrt{\delta}\log\frac{1}{\delta})$−(lower order)	$R = \Omega(\epsilon^3)$

1.1 R as $\delta \to 0$

Observe that for R as $\delta \to 0$, both the negative as well as the existential result are asymptotically the the same function. The growth is right, but they don't have the same constant. We don't know which one of the two bounds is the right answer and it is a question that is well worth examining.

Let us review how we obtained our bound for the constructive result. We had an outer code $[n_1, k_1, d_1]_{2^{k_2}}$, where $\frac{d_1}{n_1} = \delta_1$ and $\frac{k_1}{n_1} = R_1$, and we had an outer code $[n_2, k_2, d_2]_2$ where $\frac{d_2}{n_2} = \delta_2$ and $\frac{k_2}{n_2} = R_2$. We assume $2^{k_2} \geq n_1$. Then we could obtain $R_1 = 1 - \delta_1$. For the inner code we could obtain $R_2 = 1 - \delta_2 \log\frac{1}{\delta_2}$ (which is the best existential result we have). Combining the two, we get $R = R_1 \cdot R_2 \approx 1 - \delta_1 - \delta_2\log\frac{1}{\delta_2}$, and $\delta = \delta_1 \cdot \delta_2$, which is optimized when $\delta_1 = \delta_2 = \sqrt{\delta}$, which gives us $R \geq 1 - O(\sqrt{\delta}\log\frac{1}{\delta})$−(lower order terms). Observe that the gap in the existential and constructive result is embarrassingly large and there is still much to understand.

1.2 R as $\delta = \frac{1}{2} - \epsilon$ and $\epsilon \to 0$

In the other extreme, when $\delta \to 1/2$, by the Plotkin bound we know that $R \leq 1 - 2\delta$. This gives us the best bound we've seen so far for a negative result. For the existential result, we use the probabilistic construction. By an application of the Chernoff bound, we can show that we can get at least $\Omega 2^{\epsilon^2 n}$ codewords, which gives as $R = \Omega(\epsilon^2)$. Again, the gap between the negative and the existential result is huge - $O(\epsilon)$ vs $\Omega(\epsilon^2)$. For a constructive result, we are able to obtain $R = \Omega(\epsilon^3)$. As before, the gap between the existential and constructive result is large.

The negative result (that we obtained by the Plotkin bound) can actually be improved to $R = O(\epsilon^2 \log \frac{1}{\epsilon})$. , but the proof is slightly outside the scope of the class. We'll prove the result for the slightly restricted class of *balanced codes.*

2 Balanced Codes

A code $C \in \{0,1\}^n$ is ϵ-balanced if $\forall x, y \in C$ such that $x \neq y$,

$$(\frac{(1-\epsilon)}{2} \leq \Delta(x,y) \leq (\frac{(1+\epsilon)}{2}.$$

Observe that the first inequality just says that C is a code of relative distance at least $(\frac{(1-\epsilon)}{2}$. The second inequality is a new condition, but many of the codes (Hadamard and dual BCH with a coset containing the all 1s vector removed) we've constructed so far have this property, and it isn't too unreasonable a restriction. For these codes we'll prove the following strong bound.

Theorem 1 *If C is ϵ-balanced, then*

$$Rate(C) = \frac{\log_2 |C|}{n} = O(\epsilon^2 \log \frac{1}{\epsilon}).$$

Proof [Alon] For the proof, we'll use the usual Hamming to Euclid reduction that we'd used earlier. Therefore we assume $C \subseteq \{\frac{-1}{\sqrt{n}}, \frac{+1}{\sqrt{n}}\}$. Also, we'll represent C as a $K \times n$ matrix with entries from $\{\frac{-1}{\sqrt{n}}, \frac{+1}{\sqrt{n}}\}$, where each row of the matrix represents a codeword.

Observe that the matrix $M = C \cdot C^T$ is a $K \times K$ matrix with the following properties:

1. The diagonals of M are all 1's.
2. The off diagonal entries of M are at most ϵ in absolute value.
3. Rank$(M) \leq n$.

2.1 Linear Algebra Review

If M is a real and symmetric $K \times K$ matrix then

- It has K eigenvalues (not necessarily distinct), say $\lambda_1, \lambda_2, \ldots, \lambda_K$.
- $\text{Rank}(M) = K - \#\{i | \lambda_i = 0\}$.
- The trace of M, $\text{Tr}(M) := \sum_{i=1}^{K} M_{i_i} = \sum_{i=1}^{K} \lambda_i$
- $M \cdot M$ has eigenvalues $\lambda_1^2, \lambda_2^2, \ldots, \lambda_K^2$.

Lemma 2 (1) *If M is a real, symmetric $K \times K$ matrix with all its diagonal entries being 1 and its off diagonal entries being at most ϵ in absolute value, then*

$$\textit{Rank}(M) \geq \frac{K}{1 + (K-1)\epsilon^2}.$$

Proof Let $\lambda_1, \lambda_2, \ldots, \lambda_K$ be the eigenvalues of M. Then

$$\sum_{i=1}^{K} \lambda_i = K.$$

Say $\lambda_1, \lambda_2, \ldots, \lambda_r \neq 0$ and $\lambda_{r+1}, \ldots \lambda_K = 0$. By the Cauchy-Schwartz inequality, this implies that

$$\sum_{i=1}^{K} \lambda_i^2 \geq \frac{K^2}{r} = \frac{K^2}{\text{Rank}(M)}.$$

Also,

$$\sum_{i=1}^{K} \lambda_i^2 = \sum_{i=1}^{K} (M \cdot M)_{i_i} = \sum_{i,j} M_{i_j} \cdot M_{i_j} = \sum_{i} (\sum_{j} M_{i_j}^2) \leq K + K(K-1)\epsilon^2.$$

Putting both equations together we conclude that

$$\text{Rank}(M) \geq \frac{K}{1 + (K-1)\epsilon^2}.$$

■

Observe that in the statement of the above lemma, if we assume ϵ is a constant and we let K grow arbitrarily large, then we get that $\text{Rank}(M) \geq 1/\epsilon^2$. It doesn't grow with large with K and hence it doesn't quite give us what we want for the theorem. We'll apply the lemma to a different matrix to get out result.

Lemma 3 (2) *Let $M^{(t)}$ be the matrix whose (i,j)'th entry is $M_{i_j}^t$. Let $r = \textit{Rank}(M)$. Then*

$$\textit{Rank}(M^{(t)}) \leq \binom{r+t}{t}.$$

Proof Let $V_i, \ldots V_r$ span the columns of M. Consider a column of the form $\sum_{i=1}^{r} \alpha_i V_i$. In $M^{(t)}$, we get columns that are vectors whose j'th entry is of the form $(\sum_{i=1}^{r} \alpha_i V_{i_j})^t$. We want to show that the columns of $M^{(t)}$ are spanned by few vectors. Let

$$V^{(k_1,\ldots,k_r)} := V_j^{(k_1,\ldots,k_r)} := V_{1,j}^{k_1} \cdot V_{2,j}^{k_2} \cdots V_{r,j}^{k_r}, j \in \{1, \ldots k\}.$$

Then the set of vectors

$$V^{(0,0,\ldots,0)}, V^{(0,0,\ldots,1)}, \ldots, V^{(t,0,\ldots,0)},$$

i.e. the set of vectors $V^{(k_1,k_2,\ldots,k_r)}$ where $\sum k_i = t$, span all vectors of the form $(\sum_{i=1}^{r} \alpha_i V_{i_j})^t$. ■

Lemma 4 (3) *If M is a real, symmetric $K \times K$ matrix with all its diagonal entries being 1 and its off diagonal entries being at most ϵ in absolute value,then Rank$(M) \geq \Omega(\frac{1}{\epsilon^2} \cdot \frac{1}{\log 1/\epsilon} \cdot \log K)$.*

Observe that the above lemma implies that when ϵ is a constant, the rank grows with K as K goes to ∞, which is what we're looking for.

Proof Pick t so that $(\epsilon^t)^2 = \epsilon^{2t} \approx \frac{1}{K}$. Hence $t = \frac{\log K}{\log \frac{1}{\epsilon^2}}$. By Lemma 1 we get that

$$\text{Rank}(M^{(t)}) \geq \frac{K}{2}.$$

However we also know that

$$\text{Rank}(M^{(t)}) \leq \binom{r+t}{t} \approx (\frac{r}{t})^t.$$

Thus

$$\frac{r}{t} \geq K^{1/t} \approx \frac{1}{\epsilon^2} \Rightarrow r \geq \frac{t}{\epsilon^2} = \Omega(\frac{1}{\epsilon^2} \cdot \frac{1}{\log 1/\epsilon} \cdot \log K).$$

■

The proof of Theorem 1 immediately follows from the above lemma. ■

Even for general codes, it has been shown that $R = O(\epsilon^2 \log \frac{1}{\epsilon})$. This is known as the MRRW bound or the linear programming bound. There are recent proofs of this result by [Navon, Samorodnitsky] and [Friedman, Tillich] that give some geometric insight.