CS 229r Essential Coding Theory Feb 2, 2017

Lecture 4

Instructor: Madhu Sudan *Scribes: Greg Yang*

1 Constructivity

What do we mean by constructivity in coding theory? For example, we say that the Gilbert construction is "nonconstructive" because finding the code takes $\exp(n)$ time.

Ideally, the encoding function $E : \{0,1\}^k \to \{0,1\}^n$ should be polytime for a "constructive" result. But what if, say, we have a linear code, whose generator matrix requires $\exp(n)$ time to find, but the actually matrix multiplication is polytime? Most people would agree this is "constructive." In general, we could have a nonuniform family of encoding functions $E_i : \{0,1\}^{k_i} \to \{0,1\}^{n_i}$, each of which requires $\text{poly}(k_i)$ to compute; another example would be nonuniform families of polysized circuits.

A refresher on notation: For a code $E : \Sigma^k \to \Sigma^n$, the rate R is $\frac{k}{n}$. The distance $\Delta(E) = \min_{u,v \in \text{im } E} \Delta(u,v)$ is often written d. The relative distance δ of $\text{im } E$ is $\frac{d}{n}$.

2 Positive Results

2.1 The GV bound

Last time we established the following Gilbert bound

Theorem 2.1 (Gilbert)**.** *There exists a parity check matrix $H \in \{0,1\}^{n \times (n-k)}$ such that*

$$2^k \geq 2^n / \text{Vol}(n, d-1)$$

such that $C := \{y | yH = 0\}$ has $\Delta C \geq d$.

This implies the corollary

Corollary 2.2 (GV bound)**.** *For the binary alphabet, the following is achievable:*

$$R \geq 1 - H(\delta)$$

Today we sketch the proof of the Varshamov bound, which slightly improves Theorem 2.1.

Theorem 2.3 (Varshamov)**.** *There exists a parity check matrix $H \in \{0,1\}^{n \times (n-k)}$ such that*

$$2^k \geq 2^n / \text{Vol}(n, d-2)$$

such that $C := \{y | yH = 0\}$ has $\Delta C \geq d$.

Proof sketch. Construct the parity check matrix greedily, row by row, such that no $d-1$ rows are linearly dependent. As long as $2^{n-k} > \text{Vol}(n, d-2)$, this is possible. □

Exercise 1. *Complete the proof above.*

Like with the Gilbert bound, we recover Corollary 2.2

2.2 Random construction

We can try constructing codes randomly, which will again recover Corollary 2.2 (asymptotically), by 1) picking 2^{k+1} codewords at random from $\{0,1\}^n$, and 2) remove all nearby pairs of distance $< d$, of which there are $< 2^k$ (exercise!). This is possible, asymptotically, for $\frac{k}{n} \to 1 - H(\frac{d}{n})$ approaching from below.

Here is a simple case illustrating the core of this construction. Suppose we want code of distance $(\frac{1}{2} - \epsilon)n$. Pick $u, v \in \{0,1\}^n$ at random. By Chernoff,

$$\Pr[\Delta(u,v) \leq (\frac{1}{2} - \epsilon)n] \leq 2^{-\epsilon^2 n}.$$

If there are $2^{\frac{1}{2}\epsilon^2 n - 1}$ codewords, then the union bound shows that the probability that all pairs of codewords have distance $> (\frac{1}{2} - \epsilon)$ is nonzero. Therefore as the relative distance $\delta = \frac{d}{n}$ approaches $\frac{1}{2}$ as $\frac{1}{2} - \epsilon$, we can achieve the rate $\Omega(\epsilon^2)$, although nonconstructively.

2.3 Partition proofs

Suppose $C_1, \ldots, C_m$ are all linear codes with $C_i \subseteq \{0,1\}^n$.

Definition 2.4. *We call $C_1, \ldots, C_m$ a **partition** if $C_i \cap C_j = \{\vec{0}\}$, $\bigcup C_i = \{0,1\}^n$, and $|C_i| = |C_j|$.*

Lemma 2.5. *If $C_1, \ldots, C_m$ forms a partition, then for some i, $\Delta(C_i) \geq d$ if $m > \mathrm{Vol}(n, d-1)$.*

Exercise 2. *Prove Lemma 2.5*

Note that $m(|C_i| - 1) = 2^n - 1$ for each i, so that if the above bound on m holds, we get something like the Gilbert bound:

$$\frac{2^n - 1}{\mathrm{Vol}(n, d-1)} > \frac{2^n - 1}{m} = 2^k - 1.$$

3 Negative Results

We have a very simple bound using the pigeonhole principle.

Theorem 3.1 (Singleton Bound)**.** *For any code over any alphabet Σ, $R \leq 1 - \delta$.*

Proof. Let $E : \Sigma^k \to \Sigma^n$ be the encoding function, and $\pi : \Sigma^n \to \Sigma^{k-1}$ be projection to the first $k-1$ coordinates. By pigeonhole applied to $\pi \circ E : \Sigma^k \to \Sigma^{k-1}$, there are $x, x' \in \Sigma^k$, distinct, s.t., $\pi(E(x)) = \pi(E(x'))$. Thus $\Delta(C) \leq \Delta(E(x), E(x')) \leq n - k + 1$, where $C = \mathrm{im}\, E$ is the set of codewords. Dividing by n and taking $n \to \infty$ gives the desired bound. □

Using the familiar packing arguments, we can also show the following.

Theorem 3.2 (Hamming (Packing) Bound)**.** *For any code in the binary alphabet, $R \leq 1 - H(\delta/2)$.*

Proof. Each code of distance d corrects $\leq \frac{d-1}{2}$ errors. By packing arguments, (over binary alphabet)

$$\begin{aligned} |C|\,\mathrm{Vol}(n, \frac{d-1}{2}) &\leq 2^n \\ 2^k 2^{H(\delta/2)n - o(n)} &\leq 2^n \\ k &\leq n - H(\delta/2)n + o(n) \\ R &\leq 1 - H(\delta/2) \end{aligned}$$

□

Let's now work with $\{-1,1\} \cong \{1,0\}$. For $x \in \{1,-1\}^n$,

$$\langle x, x\rangle = n$$
$$\langle x, y\rangle = n - 2\Delta(x,y)$$

Suppose $C = (V_1, \ldots, V_K) \subseteq \{-1,1\}^n$ and $\Delta(C) > \frac{1}{2}$. Then $\langle V_i, V_j\rangle < 0$ for $i \neq j$. We claim that the number of such vectors can be at most $n+1$. If instead of strict inequality, we have $\Delta(C) \geq \frac{1}{2}$, then we claim that the number of such vectors can be at most $2n$. If $\Delta(C) = \frac{1}{2}$, then V_i have to be multiples of coordinate vectors in $\mathbb{R}^n$, so there are at most n of them.

Let's prove one of these claims.

Lemma 3.3. *If $\langle V_i, V_j\rangle < 0$ for $i \neq j$, then $K \leq n+1$.*

Proof. Suppose $K = n+2$. Then there is a nontrivial linear dependence

$$\sum_{i=1}^{n+1} \lambda_i V_i = 0.$$

If $\lambda_i \geq 0$ for all i, then

$$\begin{aligned} 0 &= \langle V_{n+2}, \sum_{i=1}^{n+1} \lambda_i V_i\rangle \\ &= \sum_{i=1}^{n+1} \lambda_i \langle V_{n+2}, V_i\rangle \\ &< 0, \end{aligned}$$

a contradiction. We reach a similar contradiction if all $\lambda_i \leq 0$.

Therefore, if $I = \{i : \lambda_i > 0\}$ and $J = \{j : \lambda_j < 0\}$, then neither I nor J is empty. We can therefore write

$$\sum_{i\in I} \lambda_i V_i = \sum_{j\in J} -\lambda_j V_j.$$

But then

$$0 \leq \|\sum_{i\in I} \lambda_i V_i\|^2 = \langle \sum_{i\in I} \lambda_i V_i, \sum_{j\in J} -\lambda_j V_j\rangle < 0,$$

a contradiction again. Therefore $K < n+2$. □

Exercise 3. *Show that if $\langle V_i, V_j\rangle \leq 0$, then $K \leq 2n$.*

We have shown the following

Theorem 3.4 (Plotkin)**.** *Over a binary alphabet, if the relative distance of the code is $> \frac{1}{2}$, then the rate is $O(\log n/n)$ which goes to 0 as $n \to \infty$.*

Exercise 4. *Show that if the distance of the code is $\frac{1}{2} + \epsilon$, then the rate is $\leq \frac{1}{n}\log(1 + \frac{1}{2\epsilon})$.*

Suppose we have a $(n,k,d)_q$ code. We can obtain a $(n-1,k,d-1)_q$ code by "puncturing the code", i.e. chopping off the last coordinate. We can also obtain a $(n-1,k-1,d)_q$ code by finding the most popular letter in the first coordinate, taking the codewords that start with this letter, and removing this coordinate. In the first case, we get slightly better rate at the cost of some relative distance; in the second case, we get slightly better relative distance at the cost of some rate.

Exercise 5. *Show $R \leq 1 - 2\delta$ given our observations above.*

References