COMPSCI 690T Coding Theory and Applications Feb 6, 2017

Lecture 5

Instructor: Arya Mazumdar *Scribe: Names Redacted*

1 Recap

1.1 Asymptotic Bounds

In the previous lecture, we derived various asymptotic bounds on codes. We saw that there is a trade-off between the asymptotic rate, $R(\delta)$, of a code, and its relative distance δ, where $0 \le R(\delta),\ \delta \le 1$. Figure 1 summarizes these results.

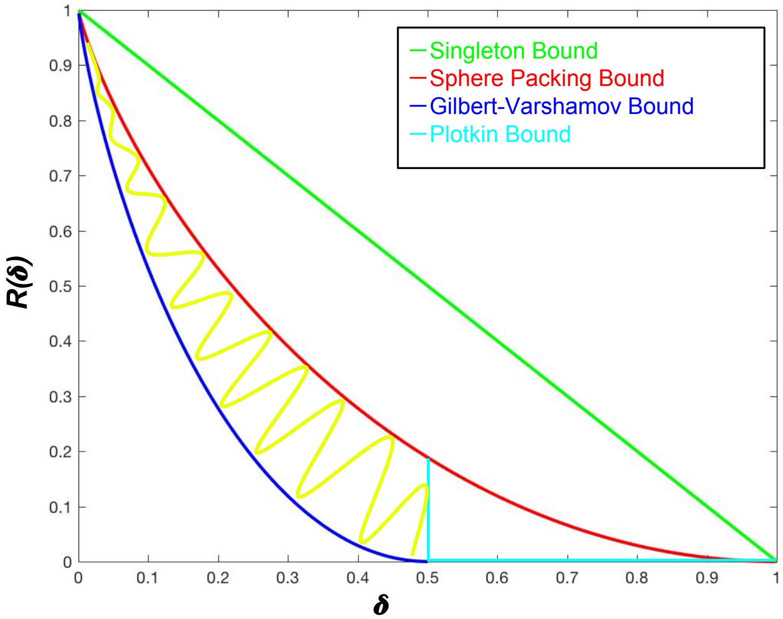

Figure 1: The rate, $R(\delta)$, of an optimal code as a function of δ, relative distance.

Specifically, the Singleton Bound tells us that $R(\delta) \le 1 - \delta$, the Sphere Packing Bound tells us that $R(\delta) \le 1 - h(\delta/2)$, where h is the binary entropy function, the Gilbert-Varshamov Bound tells us that $R(\delta) \ge 1 - h(\delta)$, and the Plotkin Bound tells us that $R(\delta) = 0,\ \delta \ge 1/2$. Recall that the best bound lies in the region between the Gilbert-Varshamov and Plotkin bounds, as illustrated by the yellow shaded region in Figure 1. In this lecture, we will see that there exists a bound better than the Plotkin and Sphere Packing bounds, and it is known as the Bassalygo-Elias (BE) Bound. However, we will first review the Johnson Bound, which will help us prove the BE bound.

1.2 Johnson Bound

The Johnson Bound applies to codes with a constant weight $wt(x) = w,\ \forall\ x \in C$. Let $A(n, d, w)$ be the maximum size of a code of length n, minimum distance d, and codeword weight w. Let $M = A(n, d, w)$. In other words, C has M codewords and length n, as illustrated in Figure 2.

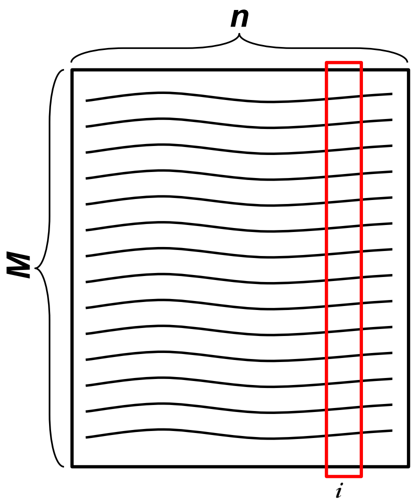

Figure 2: Code C with length n and M codewords.

Let λ_i be the number of 1's in the ith column of C. Recall from Lecture 4 that

$$\sum_{c,c' \in C} d(c,c') = \sum_{i=1}^{n} \lambda_i (M - \lambda_i)$$
$$\binom{M}{2} d \leq \sum_{i=1}^{n} \lambda_i (M - \lambda_i)$$
$$\frac{M(M-1)}{2} d \leq M \sum_{i=1}^{n} \lambda_i - \sum_{i=1}^{n} \lambda_i^2 = MMw - n\left(\frac{1}{n}\sum_{i=1}^{n} \lambda_i^2\right)$$

By Jensen's Inequality, we know that $E[X^2] \geq (E[X])^2$ for a variable X. Therefore,

$$n\left(\frac{1}{n}\sum_{i=1}^{n} \lambda_i^2\right) \geq n\left(\frac{1}{n}\sum_{i=1}^{n} \lambda_i\right)^2 = \frac{1}{n}\left(\sum_{i=1}^{n} \lambda_i\right)^2 = \frac{1}{n} M^2 w^2$$

Using this fact, we have:

$$\frac{M(M-1)}{2} d \leq M^2 w - \frac{1}{n} M^2 w^2$$
$$\frac{M(M-1)}{2} d \leq M^2 w \left(1 - \frac{w}{n}\right)$$
$$1 - \frac{1}{M} \leq \frac{2w}{d}\left(1 - \frac{w}{n}\right) = \frac{2wn - 2w^2}{nd}$$
$$\frac{1}{M} \geq 1 - \frac{2wn - 2w^2}{nd} = \frac{nd - 2wn + 2w^2}{nd}$$
$$M = A(n,d,w) \leq \frac{nd}{nd - 2wn + 2w^2}$$

This is the Johnson Bound. Note that it is valid only if the denominator above is > 0.

$$nd - 2wn + 2w^2 > 0$$

In general, this is a rule of thumb for constant-weight codes.

2 Bassalygo-Elias Bound

First, we define a useful shorthand notation. For a set $C \subseteq \{0,1\}^n$ and for any $x \in \{0,1\}^n$, define $x+C = \{x+c : c \in C\}$. For example, let $C = \{000, 010, 011\}$ and $x = 100$. Then $x+C = \{100, 110, 111\}$.

To derive the Bassalygo-Elias Bound, we need the following lemma.

Bassalygo-Elias Lemma: For any two sets $C,\ A\ \subseteq \{0,1\}^n$,

$$\sum_{x \in \{0,1\}^n} |(x+C) \cap A| = |C||A|$$

Proof: Consider the sum on the left-hand side. It can be rewritten as follows:

$$\begin{aligned}\sum_{x \in \{0,1\}^n} |(x+C) \cap A| &= \sum_{x \in \{0,1\}^n} \sum_{c \in C} \sum_{a \in A} \mathbb{1}(x+c=a) \\ &= \sum_{c \in C} \sum_{a \in A} \sum_{x \in \{0,1\}^n} \mathbb{1}(x=a-c) \\ &= \sum_{c \in C} \sum_{a \in A} 1 \\ &= |C||A|\end{aligned}$$

Above, $\mathbb{1}$ is the indicator function. ■

Due to this lemma, we know that there exists an $x \in \{0,1\}^n$ such that

$$|(x+C) \cap A| \geq \frac{1}{2^n}|C||A|$$

This follows from the fact that the right-hand side of the inequality is simply the average size of a set $(x'+C) \cap A$, $x' \in \{0,1\}^n$.

Now, let A be the set of all vectors of fixed weight w. Then all vectors in the set $(x+C) \cap A$ have weight w. Let C be a code of length n and distance d. Note that $x+C$ is also a code of length n and distance d. Then it follows that $(x+C) \cap A$ is a code with fixed weight w, length n, and minimum distance d. We know that

$$|(x+C) \cap A| \leq A(n,d,w)$$

Using the Johnson Bound,

$$\begin{aligned}\frac{1}{2^n}|C||A| &\leq \frac{nd}{nd-2wn+2w^2} \\ |C| &\leq \frac{2^n}{|A|}\frac{nd}{nd-2wn+2w^2}\end{aligned}$$

Recall that A is the set of all possible vectors with weight w. Then the size of A is

$$\begin{aligned}|A| &= \binom{n}{w} \\ \implies |C| &\leq \frac{2^n}{\binom{n}{w}}\frac{nd}{nd-2wn+2w^2}\end{aligned}$$

To get the tightest possible bound, we should take the max over all w in the denominator. This final step yields the Bassalygo-Elias Bound:

$$A(n,d) \leq \frac{2^n nd}{\max\limits_{w} \binom{n}{w}(nd-2wn+2w^2)}$$

Note that we must keep $2w^2 - 2wn + nd > 0$. This is a quadratic equation, and its roots $w_1,\ w_2$ are:

$$w_{1,2} = \frac{2n \pm \sqrt{4n^2 - 8nd}}{4} = \frac{n \pm \sqrt{n^2 - 2nd}}{2}$$

To avoid a trivial bound, we should pick

$$w \leq \frac{n - \sqrt{n^2 - 2nd}}{2}$$

Our bound then becomes:

$$A(n, d) \leq \frac{2^n nd}{\binom{n}{\frac{n-\sqrt{n^2-2nd}}{2}}}$$

Next, we look at the asymptotic bound:

$$R(\delta) \leq \lim_{n\to\infty} \frac{1}{n}\left(n - \log\binom{n}{\frac{n-\sqrt{n^2-2nd}}{2}}\right) = \lim_{n\to\infty} 1 - \frac{1}{n}\log\binom{n}{\frac{n-\sqrt{n^2-2nd}}{2}}$$

By definition, $d = \delta n$, and we know that

$$\frac{1}{n}\log\binom{n}{\delta n} \to h(\delta)$$

In our case,

$$\begin{aligned} \delta n &= \frac{n - \sqrt{n^2 - 2nd}}{2} \\ \delta &= \frac{1 - \sqrt{1 - 2d/n}}{2} = \frac{1 - \sqrt{1 - 2\delta}}{2} \end{aligned}$$

Therefore,

$$R(\delta) \leq 1 - h\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}\right)$$

This is the Asymptotic BE Bound. We update the graphic in Figure 1 to reflect the location of the BE bound with respect to the other bounds. This is shown in Figure 3. As before, the region with the yellow curve represents the gap between the best upper and lower bounds, and the best bound lies somewhere in that region.

Q: Why is the BE Bound better than the Hamming Bound?

A: Recall that for the Hamming Bound, $R(\delta) \leq 1 - h(\delta/2)$. We will show that

$$\begin{gathered} h\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}\right) \geq h(\delta/2) \\ \frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta} \geq \frac{\delta}{2} \end{gathered}$$

This inequality holds for any $\delta > 0$ (note that for $\delta > 1/2$, $R(\delta) \leq 0$ for the BE Bound).

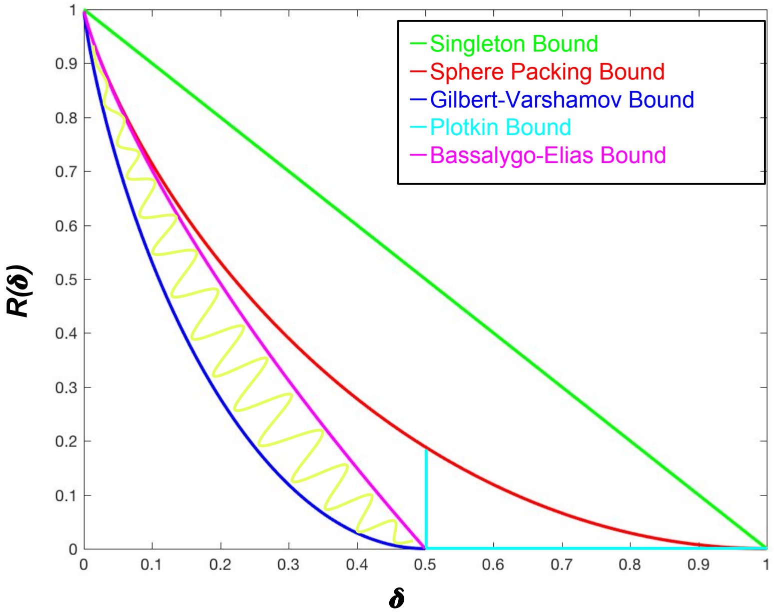

Figure 3: Rate, $R(\delta)$, of an optimal code as a function of δ, relative distance.

3 Randomized Code Construction

Recall that from the Gilbert-Varshamov Bound, we know that $R(\delta) \geq 1 - h(\delta)$.

Q: Can we construct a code better than that of the GV greedy construction?

A: Consider the following construction: pick up vectors uniformly and at random until we have M vectors. All M vectors must be distance d apart.

Suppose that we picked vectors $x_1,\ x_2,\ \ldots,\ x_M$.

Definition: A pair of codewords (x_i, x_j) is *bad* if $d(x_i, x_j) < d$.

What is $P(d(x_i, x_j) < d)$, the probability that a pair of codewords is bad? To answer this question, suppose that we picked a codeword x_i. Imagine a sphere of radius $d-1$ around x_i. We are interested in the probability that the next codeword we pick, x_j, lies within this sphere. Recall that the volume of the sphere is

$$\sum_{i=0}^{d-1} \binom{n}{i}$$

and the number of all possible codewords is 2^n, so taking the ratio of these two quantities will give us the probability of a bad event:

$$P(d(x_i, x_j) < d) = \frac{\sum_{i=0}^{d-1} \binom{n}{i}}{2^n}$$

Next, we are interested in the probability that any pair of codewords that we picked are bad. Using the union bound, we obtain:

$$P(\exists\ (i,j) : (x_i, x_j) \text{ is bad}) \leq \binom{M}{2} \frac{\sum_{i=0}^{d-1} \binom{n}{i}}{2^n}$$

Suppose that we want this probability to be less than a constant ϵ. Then, with probability $1 - \epsilon$, all pairs of codewords are good. For example, let $\epsilon = 1/100$.

$$\begin{aligned}
\binom{M}{2} \frac{\sum_{i=0}^{d-1} \binom{n}{i}}{2^n} &< \frac{1}{100} \\
\binom{M}{2} &< \frac{1}{100} \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}} \\
\frac{M^2}{2} &< \frac{1}{100} \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}} \\
\text{let } M &= \frac{1}{10} \frac{2^{n/2}}{\sqrt{\sum_{i=0}^{d-1} \binom{n}{i}}} \\
\text{then } R &= \frac{\log M}{n} = \frac{1}{2} - \frac{1}{2} h(\delta) = \frac{1}{2}(1 - h(\delta))
\end{aligned}$$

This rate achieves half of the GV bound. This means that our construction is not very efficient. However, we can get rid of the 1/2 factor using expurgation.

4 Expurgation

Let's pick M vectors, where

$$M = \frac{1}{2} \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}$$

A codeword x_i is bad if $\exists\ j : (x_i, x_j)$ is bad.

$$P(x_i \text{ is bad}) \leq M \frac{\sum_{i=0}^{d-1} \binom{n}{i}}{2^n} = \frac{1}{2}$$

The expected number of bad codewords is:

$$\begin{aligned}
E[\#\text{ bad codewords}] &\leq \frac{M}{2} \\
\rightarrow E[\#\text{ good codewords}] &\geq \frac{M}{2}
\end{aligned}$$

If we get rid of approximately $M/2$ codewords that are bad, then

$$|C| = \frac{1}{4} \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}$$

This code satisfies the asymptotic GV Bound, as expected.

5 Random Linear Code

Consider an $(n-k) \times n$ parity check matrix H where each bit is picked according to $Ber(1/2)$. Recall that all vectors x in the nullspace of H are codewords, so that $Hx = 0$. We will show that this code has a high distance.

Let the random variable A_w be the number of codewords with weight w. The probability that the product of one row of H and any nonzero codeword x is equal to 0 is 1/2. Since we have $n-k$ rows, and they are independent,

$$P(Hx = 0) = \frac{1}{2^{n-k}} = P(A_w)$$

$$\text{then } E(A_w) = \binom{n}{w}\frac{1}{2^{n-k}}$$

$$E\left[\sum_{w=1}^{d-1} A_w\right] = \sum_{i=1}^{d-1}\binom{n}{i}\frac{1}{2^{n-k}}$$

If

$$\sum_{i=1}^{d-1}\binom{n}{i}\frac{1}{2^{n-k}} < 1$$

then there are no bad codewords. This means that if we let

$$2^k = \frac{2^n}{\sum_{i=1}^{d-1}\binom{n}{i}} - 1$$

then this code achieves the GV Bound (more on this in the next lecture).