CS 860 Topics in Coding Theory Sept. 11, 2025

Lecture 3

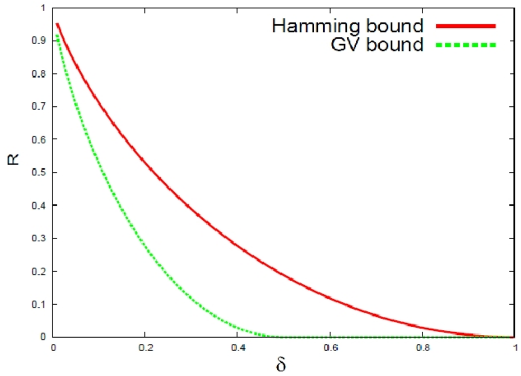
Lecturer: Elena Grigorescu *Scribe: Hanna Derets*

Previous lecture:

- Hamming bound for large distances: $R < 1 - H(\delta/2)$,
- GV bound: $R > 1 - H(\delta)$ - showed existence of codes of large rate by greedy approach in general, and by taking a generator matrix uniformly at random for linear codes.

This lecture:

- Singleton bound: $R \leq 1 - \delta$,
- Plotkin bound: $R \leq 1 - 2\delta$,
- New model – list decoding,
- Elias–Bassalygo bound: $R \leq 1 - H(\rho(\delta))$ (with Johnson bound for ρ).



We are interested in codes of large distance - constant relative distance $\delta = \Delta(C)/n \in (0,1)$ and rate $R = O(1)$. We showed that if we pick a random linear binary code, its rate would approach the GV bound. Can we find such a codes explicitly? Note that it may be tempting to test if the code has good distance –however, computing the distance of a linear code is NP-complete problem, so this approach fails.

Theorem 1 (Singleton bound) *For every code $C \subseteq \Sigma^n$ the dimension is bounded $k = \log|C| \leq n - d + 1$, where $d = \Delta(C)$ is the distance. Asymptotically, for a family of codes of rate R and relative distance δ the rate is bounded $R \leq 1 - \delta$.*

Proof Project the code C to the first $n - d + 1$ coordinates, i.e., $\pi : (c_1, \ldots, c_n) \rightarrow (c_1, \ldots, c_{n-d+1})$, denote the new code $C' = \pi(C)$ of length $n - d + 1$. Note that in the removed suffix of every code word not more than $d - 1$ different positions were discarded, thus $\Delta(C) = d \implies \Delta(C') \geq 1$, moreover π is injective. Therefore, $|C'| = |C| = \Sigma^k \leq \Sigma^{n-d+1} \implies k \leq n - d + 1$.

■

Remark The Singleton bound is independent of the alphabet size. Also, it is worse than the Hamming bound for binary codes, but better for larger alphabet sizes.

For the next theorem, we will need the following helper lemma.

Lemma 2 *If $y_1, y_2, \ldots, y_m \in \mathbb{R}^n$ such that $\forall i,\ y_i \neq \mathbf{0}$ and $\forall i, j,\ \langle y_i, y_j \rangle \leq 0$, then $m \leq 2n$.*

Proof Proving by induction (with a trivial base case), suppose that for all $k < m$ the claim holds, and consider m vectors.

Rotate all vectors such that $y_m = (1, 0, \dots, 0)$, this does not change the inner products. Say, $y_i = (\alpha_i, v_i)$ with $\alpha_i \in \mathbb{R}$, $v_i \in \mathbb{R}^{n-1}$. Then $\langle y_i, y_m \rangle = \alpha_i \leq 0$ for all $1 \leq i < m$. Also, observe that $\langle v_i, v_j \rangle = \langle y_i, y_j \rangle - \alpha_i \alpha_j$, for $i, j \neq m$.

Observe that at most one of v_i for $1 \leq i < m$ is the zero vector (prove by contradiction). Suppose $v_1 = v_2 = \mathbf{0}$, then $\langle y_1, y_2 \rangle = \alpha_1, \alpha_2 + \langle v_1, v_2 \rangle = \alpha_1 \alpha_2 > 0$ as from above $\alpha_i \leq 0$ and as $y_1 \neq \mathbf{0}, y_2 \neq \mathbf{0}$ the product becomes strictly positive $\alpha_1 \alpha_2 > 0$. This contradicts initial assumption $\langle y_i, y_j \rangle \leq 0$.

By above, $v_1, \dots, v_{m-2} \neq \mathbf{0}$ and such that $\langle v_i, v_j \rangle = \langle y_i, y_j \rangle - \alpha_i, \alpha_j \leq 0$, thus by induction hypothesis, $(m-2) \leq 2(n-1) \implies m \leq 2n$. ■

Theorem 3 (Plotkin bound) *(i) If a binary code $C \subseteq \mathbb{F}_2^n$ has distance $d \geq n/2$ (i.e., $\delta \geq 1/2$), then C has at most $|C| \leq 2n$ codewords, i.e., $k = \log |C| \leq \log(2n)$. (ii) For any binary code $C \subseteq \mathbb{F}_2^n$ we have $k = \log |C| \leq n - 2d + \log(4d)$. Asymptotically, for any family of linear codes of rate r and relative distance δ we have $R \leq 1 - 2\delta$.*

Proof (i) The argument is based on geometry in Euclidean space. Consider "embedding"

$$\psi : \mathbb{F}_2^n \to \mathbb{R}^n, \ \psi(c_1, \dots, c_n) = ((-1)^{c_1}, (-1)^{c_2}, \dots, (-1)^{c_n}).$$

Consider the inner product in $\mathbb{R}^n$:

$$\langle \psi(x), \psi(y) \rangle = \sum_{i=1}^{n} (-1)^{x_i + y_i} = \#\text{of agreements between } (x, y) - \#\text{disagreements} =$$

$$= n - 2 \cdot (\#\text{ disagreements}) \ \leq \ n - 2\Delta(C) \leq 0,$$

since $\Delta(C) \geq n/2$. Also the mapping ψ is injective, thus $|Im(\psi)| = |C|$. So, we obtained a collection of $|C|$ vectors in $\mathbb{R}^n$, such that all pairwise angles are $\geq 90°$($\Leftrightarrow \forall x, y \in C$, $\langle \psi(x), \psi(y) \rangle \leq 0$). The Lemma 2 finishes the proof of part (i).

(ii) Project the code C onto first $n - 2d$ coordiantes to obtain C' (as a multiset, as the projection is not injective). Let c_{spec} be the most common string among those in C' (or tied with) and define

$$C'' = \{c_2 \in \mathbb{F}_2^{2d} \,|\, (c_{spec}, c_2) \in C\}.$$

Note that codeword length of C'' is $2d$ and $|C''| \geq |C|/2^{n-2d}$. Also, the distance is $\Delta(C'') \geq d$ since $\Delta(C) = d$ and the distance is on the first of $n - 2d$ coordinates. So, in C'': $\Delta(C'') = \delta n$ length $N = 2\delta n$ and by part (i) $|C''| \leq 2 \cdot 2\delta n = 4\delta n \implies |C| \leq 2^{n - 2\delta n} \cdot 4\delta n$ so $k \leq n - 2\delta n + \log(4\delta n)$. ■

The Plotkin bound shows that there are no codes of positive rate $R > 0$ and large distance $\delta > 1 - 1/|\Sigma|$. Also, the Plotkin bound is tight for Hadamard code - space orthogonal to the Hamming code $Had = \{y \mid y \cdot c = 0, \ c \in Ham\}$, $|Had| = n + 1 = 2^t$ (more details next lecture).

Remark The Plotkin and Hamming upper bounds are each better than the Singleton bound as a function of δ. But there is even a better upper bound that combines ideas from both: sphere packing and geometry over R.

What if we draw balls of radius $> d/2$ around vectors and have more than one codeword in some of them? Then decoding of the message is ambiguous. However, in practice, with some side-information, it is conceivable that if the number of possible messages is small, the actual transmitted message can be disambiguated. In the 1960s Elias and Wozencraft introduced the list decoding model, to reflect the possibility of decoding beyond the unique decoding radius.

Definition 4 *A code $C \subseteq \Sigma^n$ is (e, L)list decodable if $\forall x \in \Sigma^n$ the ball $B(x, e)$ contains at most L many codewords of C.*

So far, we have discussed $(\frac{d-1}{2}, 1)$-list decodability. As L is the worst-case list size, we want it to be small for an efficient list-decoding algorithm to exist: thus, L should be a polynomial in the block length n, as otherwise, the algorithm will have to output a super-polynomial number of codewords and hence, cannot have a polynomial running time. The Johnson bound below gives bounds the list size at the particular distance $\rho = (1 - \sqrt{1 - 2\delta})/2$ (the Johnson radius).

Theorem 5 (Johnson bound) *If a binary code $C \subseteq \mathbb{F}_2^n$ with length n has a relative distance δ, then C is $(\rho n, poly(n))$-list-decodable for $\rho = (1 - \sqrt{1 - 2\delta})/2$.*

We first show how to use Theorem 5 to prove a new upper bound on the rate of any binary code, namely the Elias-Bassalygo bound.

Theorem 6 (Elias-Bassalygo bound) *Every binary code of rate R, relative distance δ and large enough block length satisfies $R \leq 1 - H(\rho(\delta))$ where $\rho(\delta) = (1 - \sqrt{1 - 2\delta})/2$.*

Proof Let $L = poly(n)$ to be the maximum list size at $\rho(\delta)$ as given by the Johnson bound. Observe that if we place balls of radius ρn around each codeword, every $w \in \{0, 1\}^n$ belongs to $\leq L$ many balls (covering argument as in Hamming bound). So (using the Johnson bound)

$$\sum_{x \in C} (Ball(x, \rho_{JS} n)) = 2^k \cdot B_n(\rho n) \leq L \cdot 2^n = poly(n) \cdot 2^n \implies 2^k \cdot 2^{H(\rho)n} \leq 2^{n + O(\log n)}$$

so $k/n + H(\rho) \leq 1 + O(1)$ and $R \leq 1 - H(\rho)$. ■

Remark Elias-Bassalygo bound is better than Hamming and Plotkin. But later, we will also see an LP bound that is even better.

Proof [Proof of Theorem5] We have to show that at distance $\rho = (1 - \sqrt{1 - 2\delta})/2$ there are at most $L = 2n$ codewords around any received word in $\{0, 1\}^n$. Let w be the received word in $\mathbb{F}_2^n$. Let $c_1, c_2, \ldots, c_{i+1}$ be such that $\Delta(c_i, w) \leq \rho n$ and $\Delta(c_i, c_j) \geq d = \delta n$.

As before, consider mapping $\psi(x) = 1/\sqrt{n}((-1)^{x_1}, (-1)^{x_2}, \ldots, (-1)^{x_n})$, then

- for $c_i \neq c_j$ angles are larger than $\pi/2$

$$\langle \psi(c_i), \psi(c_j) \rangle \leq \frac{n - 2\Delta(c_i, c_j)}{n} \leq 1 - 2\delta \leq 0$$

- $\forall i$ angles of $\psi(c_i)$ with $\psi(w)$ are smaller than $\pi/2 : \langle \psi(c_i), \psi(w) \rangle \geq 1 - 2\rho \geq 0$
- $\langle \psi(c_i), \psi(c_i) \rangle = 1 = \langle \psi(w), \psi(w) \rangle$

We'll show that there can't be too many vectors with small angles to $\psi(w)$ but large pairwise angles, by scaling $\psi(w)$ as $\alpha\psi(w)$ to get

$$\langle \psi(c_i) - \alpha\psi(w), \psi(c_j) - \alpha\psi(w) \rangle \leq 0 \;\; \forall i, j$$

and apply Plotkin bound to show that there are only $L = 2n$ such vectors. As in the proof of Plotkin bound, without loss of generality, suppose $\psi(w) = (1, 0, \ldots, 0)$. When can we find α such that $\langle \psi(c_i) - \alpha\psi(w), \psi(c_j) - \alpha\psi(w) \rangle \leq 0$? It requires

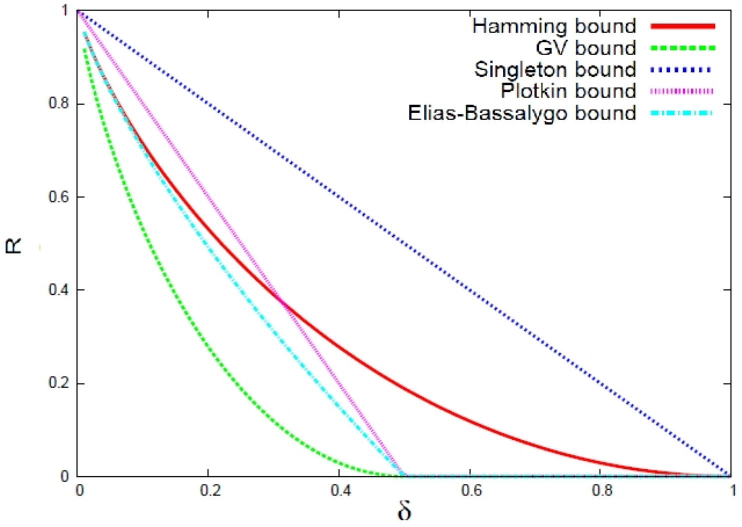
$$\langle \psi(c_i) - \alpha\psi(w), \psi(c_j) - \alpha\psi(w) \rangle =$$
$$\langle \psi(c_i), \psi(c_j) \rangle - \alpha\langle \psi(w), \psi(c_j) \rangle - \alpha\langle \psi(c_i), \psi(w) \rangle + \alpha^2$$
$$\leq 1 - 2\delta - 2\alpha(1 - 2\rho) + \alpha^2$$

to be negative. It is not obvious that such scaling exists. Homework: to verify that for $\delta \in [0, 1], \rho = (1 - \sqrt{1 - 2\delta})/2$ there $\exists \alpha \in [0, 1]$ that $1 - 2\delta - 2\alpha(1 - 2\rho) + \alpha^2 \leq 0$. ■

Remark The Johnson bound is interesting for codes with large relative distance, as $\forall\delta, \;\; \rho \geq \delta/2$, and when δ is small, then $\rho \approx \delta/2$.

Remark The Johnson bound is tight: there are codes such that at distance $> \rho(\delta)n$ there are received words with superpoly many codewords withih ρn distance. An important followup question is to design an efficient list decoding algorithms that can decode up to the Johnson bound

The visualization of all the considered so far bounds is shown below.


Hamming bound
GV bound
Singleton bound
Plotkin bound
Elias-Bassalygo bound
R
δ