CS 229r Essential Coding Theory	Feb 7, 2017

Lecture 5

Instructor: Madhu Sudan — *Scribes: Yueqi Sheng*

In this lecture we will talk about the Elias-Bassalygo bound, which beats both the Hamming and Plotkin bounds. Then we will discuss constructions of code in an attempt to meet those bounds.

1 Recap

In previous lectures, we talked about the rate vs relative distance trade off for binary code ($q = 2$).

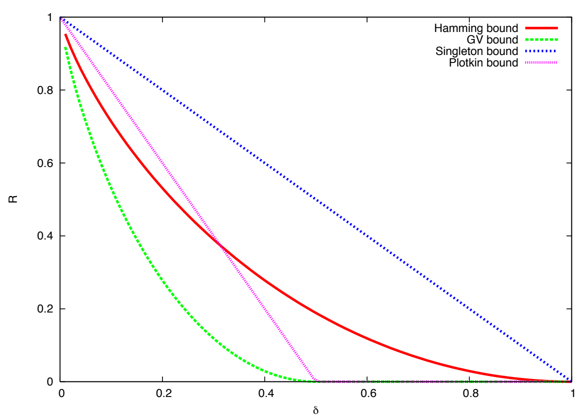
- Hamming bound (packing bound): $R \leq 1 - H(\frac{\delta}{2})$
- Plotkin bound: $R \leq 1 - 2\delta$
- Gilbert-Varshamov bound: $R \geq 1 - H(\delta)$

where $H(\delta) = H_2(\delta) = -(\delta \log \delta + (1 - \delta) \log(1 - \delta))$.

Note that Hamming and plotkin give upper bounds: (R, δ) combination is impossible to achieve above the curve.

A summary plot is given below:

Figure 1: Rate vs Relative distance



2 Elias-Bassalygo bound

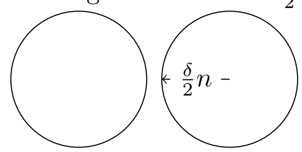
In this section, we will prove the Elias-Bassalygo bound, which is the best known upper bound that could be shown by elementary method.

Notation: For $x, y \in \{0, 1\}^n$,

- Hamming distance: $\Delta(x, y) = |\{i : x_i \neq y_i\}|$ to be the .
- Hamming ball: $B(x, d) = \{y \in \{0, 1\}^n : \Delta(x, y) \leq d\}$
- Volume of Hamming ball: $|B(x, d)|$

Recall the hamming bound (or the packing bound) says that for code with relative distance δ, one can correct $\leq \frac{\delta}{2}$ fraction of error uniquely. Geometrically, let C be the set of codewords with $\min_{x,y\in C} \Delta(x,y) \geq \delta$, then for any $x, y \in C$, $B(x, \frac{\delta}{2}) \cap B(y, \frac{\delta}{2}) = \emptyset$.

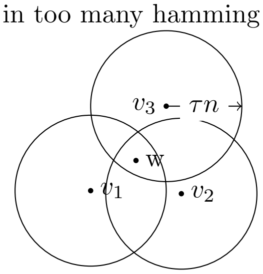
Figure 2: Hamming balls of radius $\frac{\delta}{2}n$ are disjoint



The Elias-Bassalygo bound says given a code with relative distance δ, one can correct $\tau = \frac{1}{2}(1-\sqrt{1-2\delta})$ fraction of error with $L = \text{poly}(n)$ length list. Formally, we have the following lemma:

Lemma 1 (List decoding lemma)**.** *Given C as a code with relateive distance δn, let $\tau = \frac{1}{2}(1-\sqrt{1-2\delta})$. Then $\forall w \in \{0,1\}^n$, there are at most $L = poly(n)$ codewords $v_1, \cdots, v_L \in C$ s.t. $w \in B(v_i, \tau n)$.*

Figure 3: x not in too many hamming balls of radius τn



Theorem 2 (Elias-Bassalygo bound)**.** *If $\mathcal{C}$ is an infinite family of binary code with relative distance δ and rate R, then $R \leq 1 - H(\frac{1}{2}(1-\sqrt{1-2\delta}))$.*

To see lemma 1 implies the theorem: suppose for all $w \in \{0,1\}^n$, $x \in D(w)$ iff $w \in B(x, \tau n)$. Then each w is in at most L such balls.

$$\sum_{x\in C} |B(x,\tau n)| \leq L2^n$$

$|C| = 2^k$. Recall that $|B(x,\tau n)| \sim 2^{H(\tau)n}$. Rerrange the above inequality gives

$$2^k \leq L2^{n(1-H(\tau))}$$

Since $L = poly(n)$, take the log of both side gives $R = \frac{k}{n} \leq 1 - H(\tau) + o(n)$.

Exercise 3. *Prove the list decoding lemma. (Lemma 1)*

Sketch of Proof [of Lemma 1] Embed $w \in \{0,1\}^n$ into $\{\pm 1\}^n$: Define $\phi : \{0,1\} \to \{\pm 1\}$ s.t. $\phi(0) = 1$ and $\phi(1) = 0$. For all $w \in \{0,1\}^n$, denote $w' = [\phi(w_1), \cdots, \phi(w_n)]$.

It is easy to check:

$$\langle v_i', v_j' \rangle \leq n - 2\delta n$$

$$\langle v_i', v_i' \rangle = n, \langle w', w' \rangle = n$$

$$\langle v_i', w' \rangle \geq (1-2\tau)n$$

The goal now is to find $\alpha \in [0,1]$ s.t. $\forall v_i', v_j'$,

$$\langle v_i' - \alpha w, v_j' - \alpha \rangle \leq 0$$

By a similar arguement as in that of the hamming bound, we get $L \leq 2n$. $\square$

To see why $\tau = \frac{1}{2}(1 - \sqrt{1-2\delta})$, let's go back to the $\{0,1\}^n$ world. WLOG, assume $w = 0^n$. To obtain $\Delta(w, v_i) \sim \tau n$, choose $v_i \sim Bin(n, \tau)$, i.e set each bit to be 1 w.p. τ and 0 w.p. $1-\tau$. Then

$$\mathbb{E}[\Delta(v_i, v_j)] = 2\tau(1-\tau)n$$

Solve for τ gives $\tau = \frac{1}{2}(1 - \sqrt{1-2\delta})$.

2.1 Compare Elias-Bassalygo with other bounds

Note that since $\frac{\delta}{2} \leq \tau \leq \delta$ and $H(\delta)$ is monotone increasing, Elias-Bassalygo bound stays between GV and hamming bound. As $\delta \to \frac{1}{2}$, $\tau \to \frac{1}{2}$. Thus Elias-Bassalygo is getting close to GV bound when $\delta \to \frac{1}{2}$. However, in the case when δ is small, Elias-Bassalygo is not too much better than Hamming bound. Indeed as $\delta \to 0$, $\sqrt{1-2\delta} \approx 1 - \delta$. A simply calculation shows $1 - H(\tau) \approx 1 - H(\frac{\delta}{2})$.

What about the growth rate when $\delta \to \frac{1}{2}$? say $\delta = \frac{1}{2} - \epsilon$, the GV bound gives $1 - H(\delta) = \Omega(\epsilon^2)$ while Elias-Bassalygo only gives $1 - H(\tau) = \Omega(\epsilon)$.

The Linear Programming bound says GV is the closer to reality. It claims as $\delta \to \frac{1}{2}$, $R \leq O(\epsilon^2 \log(\frac{1}{\epsilon}))$.

3 Reed-Solomon codes

In the previous section we discussed some asymptotic bounds of $[n,k,d]_q$ codes for the rate and relative distance of the code. In this section, we will talk about a explicit construction of linear code in an attempt to meet the bounds from the previous section.

Definition 4 (Reed-Solomon Code). *Given some field $\mathbb{F} = \Sigma$, assume $|\mathbb{F}| \geq n$. Let $\alpha_1, \cdots, \alpha_n$ be the set of distinct elements in $\mathbb{F}$.*
Define $E : \Sigma^k \to \Sigma^n$ as follows: for any $m \in \Sigma^k$, define the degree $k-1$ polynomial given by m be

$$M(x) = \sum_{i}^{k-1} m_i x^{i-1}$$

Then $E(m) = [M(\alpha_1), \cdots, M(\alpha_n)]$ (That is, we treat m as the coefficient of $M(x)$ and evaluate M at $\alpha_1, \cdots, \alpha_n$.)

Claim 5. *The parameter for Reed-Solomon code is $[n, k, n-k+1]_q$.*

Proof of [: claim 5] Given n, k, let E be the encoding function of Reed-Solomon code. Observe that for any $m, m' \in \Sigma^k$, $(M - M')(x) = M(x) - M(x')$. Thus if $M(\alpha_i) = M'(\alpha_i)$, $(M - M')(\alpha_i) = M(\alpha_i) - M'(\alpha_i) = 0$.

$$\Delta(E(M), E(M')) = \Delta(E(M - M'), E(0)) = n - |\{i : (M - M')(\alpha_i) = 0\}|$$

Since $(M - M')(x)$ is a degree $k-1$ polynomial, there are at most $k-1$ roots. $|\{i : (M-M')(\alpha_i) = 0\}| \leq k-1$. Thus we have

$$\Delta(E(M), E(M')) \geq n - (k+1)$$

$\square$

Remark this says Reed-Solomon code matches the singleton bound.

4 Reduce the field size

Note that for Reed-solomon code with parameter $[n, k, n-k+1]_q$, the field size is at least n. It is natural to ask whether one can achieve singleton bound with a smaller field size, in particular, on $\mathbb{F}_2$.

We start from a simple fact about finite field

Fact 6. *$\mathbb{F}_q$ is a field iff q is a prime power.*

Exercise 7. *Prove fact 6.*

Definition 8. *For $t \geq \log(|\mathbb{F}_q|)$, let $\phi : \mathbb{F}_q \to \{0,1\}^t$ be an 1-1, onto map. For $x \in \mathbb{F}_q^m$, denote $\phi(x) = [\phi(x_1), \cdots, \phi(x_m)]$.*

Here we take $n = q = 2^t$.

Claim 9. *If C is a Reed-Solomon code with parameter $[n, k, n-k+1]_q$, then $\phi(C)$ is a $[tn, tk, n-k+1]_2$ code, where*

$$\phi(C) = \{\phi(x) : x \in C\}$$

Proof of [: Claim 9] By construction, for $m \geq 1$ and $x \in \mathbb{F}_q^m$, $\phi(x) \in (\{0,1\}^t)^m$. Thus the block length and message length for $\phi(C)$ tn, tk.

To lower bound $\Delta(\phi(C))]_2$: For all $x, y \in \mathbb{F}_q^n$ and $i \in \{1, \cdots, n\}$. If $x(i) \neq y(i)$, then since ϕ is 1-1, $\Delta(\phi(x(i)), \phi(y(i))) \geq 1$. This gives

$$\Delta(\phi(x), \phi(y)) = \sum_i \Delta(\phi(x(i)), \phi(y(i))) \geq D(x, y) \geq n - k + 1$$

where the last inequality follows from the definition of Reed-Solomon code. Thus $\Delta(\phi(C)) \geq n - k + 1$. Thus the parameter for $\phi(C)$ is $[tn, tk, n-k+1]_2$. $\square$

Let $N = n \log n$, as $n \to \infty$, $n \approx \frac{N}{\log N}$. Let $R = \frac{k}{n}$ be the rate, the above parameters becomes $[N, RN, (1-R)\frac{N}{\log N}]_2$.

If we change d: say $d = 15$, we get $n - k = 14$ from Reed-Solomon code. Then the rate becomes $R = 1 - \frac{14}{n}$ and we get a code with parameter $[N, N - 14 \log N - o(\log N), 15]$. Here we no longer meet the singleton bound.

One could argue that we only get one bit distance from every block of t bits, indeed we can look for better map ϕ.

4.1 Code concatenation

By taking ϕ in the previous section to be some encoding function, we can obtained better parameters. This is the Concatenated code.

Definition 10 (concatenation code)**.** *Let $\Sigma = \mathbb{F}_q$ be a field. $E_{outer} : \Sigma^k \to \Sigma^n$, $E_{inner} : \Sigma \to \{0,1\}^t$ with $t = O(\log n)$. Let $\delta_0 = \Delta(E_{inner})$, i.e. $\forall a, b \in \Sigma$, $\Delta(E_{inner}(a), E_{inner}(b)) \geq \delta_0$. Then the concatenated code $E_{outer} \circ E_{inner} : \Sigma^k \to (\{0,1\}^t)^n$ is defined as*

$$E_{outer} \circ E_{inner}(m) = [E_{inner}(x_1), \cdots, E_{inner}(x_n)]$$

where $E_{outer}(m) = [x_1, \cdots, x_n]$.

What are the parameters of the concatenation code? Suppose the parameter of E_{outter} is $[n_1, k_1, d_1]_{q_1}$ and the parameter of E_{inner} is $[n_2, k_2, d_2]_{q_2}$.

- Observe that by construction, $n_2 = \log_{q_2}(q_1)$

- The parameter of $E_{outer} \circ E_{inner}$ is $[n_1 n_2, k_1 k_2, d_1 d_2]_{q_2}$.

  Sketch of Proof The proof of block length and message length follows directly from that of Claim 9. To get the relative distance: If $x_i \neq y_i$, then $\Delta(E_{inner}(x_i), E_{inner}(y_i)) \geq d_2 n_2$. If x, y are encoding given by E_{outter}, there are at least $d_1 n_1$ such i. Therefore $\Delta(E_{outer} \circ E_{inner}) \geq d_1 n_1 (d_2 n_2)$. Thus the relative distance is $\frac{d_1 n_1 (d_2 n_2)}{n_1 n_2} = d_1 d_2$.

- The rate $R = \frac{k_1 k_2}{n_1 n_2} = R_1 R_2$. The relative distance is $\delta = \delta_1 \delta_2$. □

If we let E_{outter} be Reed-Solomon code, $R_1 \approx 1 - \delta_1$. Suppose $R_2 = 1 - H(\delta_2)$, then the for $\Delta(E_{outer} \circ E_{inner})$, $R_1 R_2 \approx (1 - \delta_1)(1 - H(\delta_2))$. This is a bit weaker than GV since given the distance $\delta_1 \delta_2$, we could have achieve the rate $1 - H(\delta_1 \delta_2)$.

Exercise 11. *Assume E_{inner} is the linear binary code with parameter $[R_2 \log n, \log n, \delta]$, show that there exists such E_{inner} with $R_2 \geq 1 - H(\delta)$ and there exists an algorithm that find the E_{inner} in $O(poly(n))$ time.*

References