

## Lecture 17: Proof of a Geometric Lemma

October 5, 2007

Lecturer: Atri Rudra

Scribe: Sandipan Kundu & Atri Rudra

In the last lecture, we proved the Plotkin bound, except for a couple of geometric lemmas which we will prove in this lecture.

### 1 Geometric Lemma

Claim : Let  $C \subseteq [q]^n$ . There exists a function  $f : C \rightarrow \mathbb{R}^{nq}$  s.t.

1.  $\forall \mathbf{c} \in C, \|f(\mathbf{c})\| = 1$ .
2.  $\forall \mathbf{c}_1 \neq \mathbf{c}_2 \in C, \langle f(\mathbf{c}_1), f(\mathbf{c}_2) \rangle = 1 - \frac{\Delta(\mathbf{c}_1, \mathbf{c}_2)q}{(q-1)n}$

**Lemma 1.1.** Let  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m \in \mathbb{R}^n$ .

1. If  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$  are all non-zero and  $\langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq 0$  for all  $i \neq j, m \leq 2n$ .
2. If  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$  are unit vectors and  $\langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq -\varepsilon (\varepsilon > 0), \forall i \neq j$ , then  $m \leq 1 + 1/\varepsilon$ .

We are going to proof the claim and then the lemma. In the proof of the claim we show that there is function with the stated properties. Initially we pick a  $\phi : [q] \rightarrow \mathbb{R}^q$  with certain properties. Then we use  $\phi$  to define a  $f : \mathbb{R}^q \rightarrow \mathbb{R}^{nq}$  which satisfies the claimed properties.

*Proof.* of the claim

$$\phi : [q] \rightarrow \mathbb{R}^q.$$

$$\phi(i) = \left\langle \frac{1}{q}, \frac{1}{q}, \dots, \frac{-(q-1)}{q}, \dots, \frac{1}{q} \right\rangle \quad (1)$$

$i^{\text{th}}$  position

$$\forall i, \phi(i)^2 = \frac{(q-1)}{q^2} + \frac{(q-1)^2}{q^2} = \frac{(q-1)}{q} \quad (2)$$

$$\forall i \neq j, \langle \phi(i), \phi(j) \rangle = \frac{(q-2)}{q^2} - \frac{2(q-1)}{q^2} = \frac{(-1)}{q} \quad (3)$$

$$f(\mathbf{c}) \triangleq \sqrt{\frac{q}{(q-1)n}} \langle \phi(\mathbf{c}_1), \phi(\mathbf{c}_2), \dots, \phi(\mathbf{c}_n) \rangle \quad (4)$$

Now we will show the defined function satisfies the claim.

$$\|f(\mathbf{c})\|^2 = \frac{q}{(q-1)n} \sum_i \|\phi(i)\|^2 = 1 \quad (5)$$

$$\langle f(\mathbf{c}_1), f(\mathbf{c}_2) \rangle = [\Delta(\mathbf{c}_1, \mathbf{c}_2) \left(\frac{-1}{q}\right) + (n - \Delta(\mathbf{c}_1, \mathbf{c}_2)) \left(\frac{q-1}{q}\right)] \left(\frac{q}{q-1}\right) \left(\frac{1}{n}\right) \quad (6)$$

$$\begin{aligned} &= 1 - \Delta(\mathbf{c}_1, \mathbf{c}_2) \left(\frac{q}{q-1}\right) \left(\frac{1}{n}\right) \left[\frac{-1}{q} - \frac{q-1}{q}\right] \\ &= 1 - \left(\frac{q}{q-1}\right) \end{aligned} \quad (7)$$

(6) is obtained using (3),(2). □

*Proof.* of (i) of the lemma.

By induction on  $n$ . When  $n = 0$ . We have non-zero  $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbb{R}^n$  such that

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq 0 \quad \forall i \neq j \quad (8)$$

Without loss of generality  $\mathbf{v}_m = \langle 1, 0, \dots, 0 \rangle$ . For  $1 \leq i \leq m-1$

$$\mathbf{v}_i = [\alpha_i y_i], \alpha_i \in \mathbb{R}, \mathbf{y}_i \in \mathbb{R}^{n-1} \quad (9)$$

By (8)  $\alpha_i \leq 0$ . Reduce from  $m$  vectors over  $\mathbb{R}^n \rightarrow (m-1)$  vectors in  $\mathbb{R}^{n-1}$

Mini-Claim: At most one of  $\mathbf{y}_1, \dots, \mathbf{y}_{m-1}$  is not all zero.

If not say  $\mathbf{y}_1 = \mathbf{y}_2 = \vec{0} \implies \alpha_1, \alpha_2 < 0$

$$\implies \langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \alpha_1 \cdot \alpha_2 > 0 \text{ This is a contradiction.}$$

$$\langle \mathbf{y}_i, \mathbf{y}_j \rangle = \langle \mathbf{v}_i, \mathbf{v}_j \rangle - \alpha_i \cdot \alpha_j \leq \langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq 0$$

Reduced problem to  $\geq m-2$  vectors on dimension  $n-1$ . Continuing the process we can conclude that every loss in dimension of the vector results in twice in loss in the numbers of the vectors in the set. Hence, claim 1 of the lemma is being proved. □

*Proof.* of (ii) of the lemma

$$\mathbf{z} = \mathbf{v}_1 + \dots + \mathbf{v}_m \quad (10)$$

$$0 \leq \|\mathbf{z}\|^2 = \sum_{i=1}^m \|\mathbf{v}_i\|^2 + 2 \sum_{i < j} \langle \mathbf{v}_i, \mathbf{v}_j \rangle \quad (11)$$

$$\leq m + 2 \cdot \frac{m}{(m-1)} \cdot (-\varepsilon) \quad (12)$$

$$= m(1 - \varepsilon m + \varepsilon)$$

$$\therefore m(1 - \varepsilon m + \varepsilon) \geq 0$$

$$\text{This implies } m \leq 1 + \frac{1}{\varepsilon} \quad (13)$$

$$(14)$$

(12) is true as  $\mathbf{v}_i$  are unit vectors and using the fact  $\langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq -\varepsilon$

□

## 2 Johnson Bound

$J(n, d, e) = \max$  number of codewords in a Hamming radius  $e$  for any code distance,  $d$  and block length,  $n$ .

$0 \leq e \leq n$ ,  $J(n, d, \lfloor \frac{d-1}{2} \rfloor) = 1$

Say for some  $e > \lfloor \frac{d-1}{2} \rfloor$ ,  $0 \leq e \leq n$ ,  $J(n, d, e)$  is  $n^{o(1)}$ , then list decoding is possible for any code (atleast combinatorial).