| **Error Correcting Codes: Combinatorics, Algorithms and Applications** | **(Fall 2007)** |

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 lemmas which we will prove in this lecture.

1   Geometric Lemma

The proof of the Plotkin bound needed the existence of a map from codewords to real vectors with certain properties, which the next lemma guarantees.

Lemma 1.1. *Let $C \subseteq [q]^n$. Then there exists a function $f : C \longrightarrow \mathbb{R}^{nq}$ such that*

1. *For every $\mathbf{c} \in C, \|f(\mathbf{c})\| = 1$.*

2. *For every $\mathbf{c}_1 \neq \mathbf{c}_2 \in C, \langle f(\mathbf{c}_1), f(\mathbf{c}_2)\rangle = 1 - \left(\frac{q}{q-1}\right)\left(\frac{\Delta(\mathbf{c}_1,\mathbf{c}_2)}{n}\right).$*

We also used the following lemma, which gives a bound on the number of vectors that can exists such that every pair is at an obtuse angle with each other.

Lemma 1.2 (Geometric Lemma). *Let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$.*

1. *If $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ are all non-zero and $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle \leq 0$ for all $i \neq j$, then $m \leq 2n$.*

2. *If $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ are unit vectors and $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle \leq -\varepsilon < 0$ for every $i \neq j$, then $m \leq 1 + 1/\varepsilon$.*

Next, we prove the two lemmas above.

Proof of Lemma 1.1.   We begin by picking a map $\phi : [q] \to \mathbb{R}^q$ with certain properties. Then we apply ϕ to all the coordinates of a codeword to define the map $f : C \to \mathbb{R}^{nq}$ that satisfies the claimed properties. We now fill in the details.

We begin by defining the map $\phi : [q] \to \mathbb{R}^q$. For every $i \in [q]$, define

$$\phi(i) = \left\langle \frac{1}{q}, \frac{1}{q}, \ldots, \underbrace{\frac{-(q-1)}{q}}_{i^{\text{th}}\text{position}}, \ldots \frac{1}{q} \right\rangle,$$

that is all but the ith position in $\phi(i) \in \mathbb{R}^q$ has a value of $1/q$ and the ith position has value $-(q-1)/q$.

Next, we record two properties of ϕ that follow immediately from its definition. For every $i \in [q]$,

$$||\phi(i)||^2 = \frac{(q-1)}{q^2} + \frac{(q-1)^2}{q^2} = \frac{(q-1)}{q}. \tag{1}$$

Also for every $i \neq j \in [q]$,

$$\langle \phi(i), \phi(j) \rangle = \frac{(q-2)}{q^2} - \frac{2(q-1)}{q^2} = -\frac{1}{q} \tag{2}$$

We are now ready to define our final map $f : C \to \mathbb{R}^{nq}$. For every $\mathbf{c} = (c_1, \ldots, c_n) \in C$, define

$$f(\mathbf{c}) = \sqrt{\frac{q}{n(q-1)}} \cdot \langle \phi(c_1), \phi(c_2), \ldots, \phi(c_n) \rangle.$$

To complete the proof, we will show that f satisfies the claimed properties. We begin with condition 1. Note that

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

where the first equality follows from the definition of f and the second equality follows from (1).

We now turn to the second condition. We claim

$$\langle f(\mathbf{c}_1), f(\mathbf{c}_2) \rangle = \left[\Delta(\mathbf{c}_1, \mathbf{c}_2) \left(\frac{-1}{q} \right) + (n - \Delta(\mathbf{c}_1, \mathbf{c}_2)) \left(\frac{q-1}{q} \right) \right] \cdot \left(\frac{q}{n(q-1)} \right) \tag{3}$$

$$= 1 - \Delta(\mathbf{c}_1, \mathbf{c}_2) \left(\frac{q}{n(q-1)} \right) \left[\frac{-1}{q} - \frac{q-1}{q} \right]$$

$$= 1 - \left(\frac{q}{q-1} \right) \left(\frac{\Delta(\mathbf{c}_1, \mathbf{c}_2)}{n} \right),$$

as desired. In the above, (3) is obtained using (2), (1) and the definition of the Hamming distance. $\square$

Proof of Lemma 1.2. We begin with a proof of the first result. The proof is by induction on n. Note that in the base case of $n = 0$, we have $m = 0$, which satisfies the claimed inequality $m \leq 2n$.

In the general case, we have $m \geq 1$ non-zero vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$ such that for every $i \neq j$,

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq 0 \tag{4}$$

By a change of basis, we can assume that $\mathbf{v}_m = \langle 1, 0, \ldots, 0 \rangle$. For $1 \leq i \leq m - 1$, denote the vectors as $\mathbf{v}_i = \langle \alpha_i, \mathbf{y}_i \rangle$, for some $\alpha_i \in \mathbb{R}$ and $\mathbf{y}_i \in \mathbb{R}^{n-1}$. Note that by (4), $\alpha_i \leq 0$.

Next, we claim that at most one of $\mathbf{y}_1, \ldots, \mathbf{y}_{m-1}$ can be the all zero vector, $\mathbf{0}$. If not, assume w.l.o.g., that $\mathbf{y}_1 = \mathbf{y}_2 = \mathbf{0}$. As $\mathbf{v}_1$ and $\mathbf{v}_2$ are non-zero, $\alpha_1, \alpha_2 < 0$. This in turn implies that

$$\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \alpha_1 \cdot \alpha_2 > 0,$$

2

which is a contradiction. W.l.o.g., assume that $\mathbf{v}_1, \ldots, \mathbf{v}_{m-2}$ are all non-zero vectors. Further, note that for every $i \neq j \in [m-2]$, $\langle \mathbf{y}_i, \mathbf{y}_j \rangle = \langle \mathbf{v}_i, \mathbf{v}_j \rangle - \alpha_i \cdot \alpha_j \leq \langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq 0$. Thus, we have reduced problem on m vectors with dimension n to an equivalent problem on $m-2$ vectors with dimension $n-1$.[1] If we continue this 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. Induction completes the proof.

We now move on to the proof of the second part. Towards that end, define $\mathbf{z} = \mathbf{v}_1 + \ldots + \mathbf{v}_m$. Now consider the following sequence of relationships:

$$\|\mathbf{z}\|^2 = \sum_{i=1}^{m} \|\mathbf{v}_i\|^2 + 2\sum_{i<j} \langle \mathbf{v}_i, \mathbf{v}_j \rangle \leq m + 2 \cdot \binom{m}{2} \cdot (-\varepsilon) = m(1 - \varepsilon m + \varepsilon).$$

The inequality follows from the facts that each $\mathbf{v}_i$ is a unit vector and the assumption that for every $i \neq j$, $\langle \mathbf{v}_i.\mathbf{v}_j \rangle \leq -\varepsilon$. As $\|\mathbf{z}\|^2 \geq 0$,

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

Thus, we have $m \leq 1 + \frac{1}{\varepsilon}$, as desired. □

2 Johnson Bound

Next lecture, we will look at another bound called Johnson bound. To get the ball rolling, let us fix an important notation. Define $J(n, d, e)$ to be the maximum number of codewords in a Hamming ball of radius e for any code with distance d and block length n. As a warm up, we have already seen that for every $0 \leq d \leq n$, $J\left(n, d, \lfloor \frac{d-1}{2} \rfloor\right) = 1$. Note that if we can show that for some $e > \lfloor \frac{d-1}{2} \rfloor, 0 \leq e \leq n$, $J(n, d, e)$ is $n^{O(1)}$, then it will imply that (at least combinatorially) list decoding is possible for any code beyond the "traditional" half the distance bound. The Johnson bound shows the existence of such an e.

---

[1]It could be the case that all of $\mathbf{y}_1, \ldots, \mathbf{y}_{m-1}$ are non-zero in which case we go down from m vectors to $m-1$ vectors. However, by throwing away two vectors, we only get a "weaker" upper bound. Actually it is not too hard to see that if the original set of vectors are the $2n$ vectors, one along each dimension (and its negation) then in each step of the induction m will go down by exactly 2.