Spectral Graph Theory and its Applications Lecture 14

Distances in Point Sets

Lecturer: Daniel A. Spielman October 21, 2004

14.1 Distances in Point Sets

In this lecture, we will prove two theorems relating distances in point sets to the Gram matrices of eigenspaces. The first will be an upper bound on the number of points in a distance-2 set. This provides a lower bound on the dimensions of the eigenspaces of strongly-regular graphs.

The second theorem will be a reformulation of the linear programming bound of Delsarte. The LP bound enables us to upper bound the number of codewords in an error-correcting code of high minimum distance. We will prove this bound by examining the Gram matrices of the eigenspaces of the hypercube. We will merely apply the LP bound to prove the Plotkin bound. However, the best bounds on error-correcting codes can also be proved this way.

14.2 Distance-two sets

Let $x_1, \ldots, x_n$ be a set of points in $\mathbb{R}^f$ such that there are three values α, β and γ such that

$$\langle x_i, x_j \rangle = \begin{cases} \alpha & \text{if } i = j, \\ \beta \text{ or } \gamma & \text{otherwise.} \end{cases}$$

We remark that if all the points are distinct, then we must have $\beta, \gamma < \alpha$. We will now prove an upper bound on n in terms of f.

The key to our proof is to define an f-variate polynomial for each point. In particular, we set

$$p_i(y) = (\langle y, x_i \rangle - \beta)(\langle y, x_i \rangle - \gamma).$$

We first note that each polynomial p_i is an f-variate polynomial of degree 2. As each f-variate polynomial of degree 2 can be expressed in the form

$$a + \sum_i b_i y_i + \sum_{i \leq k} c_{i,j} y_i y_j,$$

we see that the vector space of degree-2 polynomials in f variables has dimension

$$1 + 2f + \binom{f}{2}.$$

To prove an upper bound on n, we will show that these polynomials are linearly independent. Assume by way of contradiction that they are not. Then, without loss of generality, there exist coefficients $\alpha_1, \ldots, \alpha_n$ with $\alpha_1 \neq 0$ and

$$\sum_i \alpha_i p_i(y) = 0.$$

To obtain a contradiction, plug in $y = x_1$, to find

$$\sum_i \alpha_i p_i(x_1) = \alpha_1 p_1(x_1) \neq 0.$$

Thus, we may conclude

$$n \leq 1 + 2f + \binom{f}{2}.$$

14.3 The Linear Programming Bound

We now explain a version of Delsarte's linear programming bound. Let $\mathcal{C} \subset \{0,1\}^n$ be an error-correcting code of minimum distance Δ. Delsarte's linear programming bound enables us to prove upper bounds on $|\mathcal{C}|$ in terms of n and Δ. The tool we will use in these bounds is an analysis of the Gram matrix of the eigenspaces of the hypercube H_n.

Recall that the adjacency matrix of H_n has eigenvalues $n - 2k$ for $k = 0, \ldots, n$, and that the kth eigenspace is spanned by the vectors χ_w where $w \in \{0,1\}^n$, $|w| = k$, and we recall

$$\chi_w(x) = (-1)^{\langle w,x \rangle}.$$

Let U_k denote the 2^n-by-$\binom{n}{k}$ matrix whose columns are the eigenvectors of the kth eigenspace, and let

$$E_k = U_k U_k^T.$$

Then, the (x, y) entry of E_k equals

$$\begin{aligned}
E_k(x,y) &= \sum_{w:|w|=k} \chi_w(x)\chi_w(y) \\
&= \sum_{w:|w|=k} (-1)^{\langle w,x \rangle}(-1)^{\langle w,y \rangle} \\
&= \sum_{w:|w|=k} (-1)^{\langle w,x \oplus y \rangle} \\
&= \sum_{w:|w|=k} \chi_w(x \oplus y).
\end{aligned}$$

So, this entry only depends upon $x \oplus y$.

Here is Delsarte's linear programming bound.

Theorem 14.3.1. *Let $\alpha_1, \ldots, \alpha_n \geq 0$, $\alpha_0 = 1$, and let*

$$A = \sum_{k=0}^{n} \alpha_k E_k.$$

If for all x and y that differ in at least Δ coordinates, $A(x,y) \leq 0$, then every code $\mathcal{C} \subset \{0,1\}^n$ of minimum distance Δ satisfies

$$|\mathcal{C}| \leq A(\mathbf{0}, \mathbf{0}).$$

Proof. Let $C \in \mathbb{R}^{2^n}$ be the characteristic vector of $\mathcal{C}$. Recall that $E_0 = J$, the all-1's matrix. We now compute

$$C^T J C = \sum_{x \in \mathcal{C}} \sum_{y \in \mathcal{C}} 1 = |\mathcal{C}|^2 .$$

We also note that each matrix E_k is positive semi-definite, so

$$C^T E_k C \geq 0$$

One can also see that by observing

$$C^T E_k C = C_T U_k U_k^T C = (U_k^T C)^T (U_k^T C) \geq 0.$$

Finally, as $A(x,y) \leq 0$ for each x and y that differ in at least Δ coordinates,

$$C^T A C \leq C^T \mathtt{diag}(A) C,$$

where by $\mathtt{diag}(A)$ we mean the matrix containing just the diagonal elements of A. Putting these inequalities together, we find

$$\begin{aligned}
|\mathcal{C}|^2 &\leq C^T J C \\
&\leq C^T J C + \sum_{k \geq 1} \alpha_k C^T E_k C \\
&= C^T A C \\
&\leq C^T \mathtt{diag}(A) C \\
&= |\mathcal{C}| \, A(\mathbf{0}, \mathbf{0}).
\end{aligned}$$

□

To actually apply this theorem, we must find linear combinations of the E_k matrices that have negative entries for all far apart x and y. Let's begin by examining E_1. In our analysis, I will let e_i denote the elementary unit vector that is 1 in the ith coordinate. We have

$$\begin{aligned}
E(x,y) &= \sum_{|w|=1} \chi_w(x \oplus y) \\
&= \sum_{1 \leq i \leq n} \chi_{e_i}(x \oplus y) \\
&= (n - |x \oplus y|) - |x \oplus y| \\
&= n - 2\,|x \oplus y|).
\end{aligned}$$

So, consider the polynomial

$$A = E_0 + E_1.$$

We have $A(x, y) \leq 0$ for $|x \oplus y| \geq n/2$. We will use this to prove the Plotkin bound.

Theorem 14.3.2. *Let $n = 2l + 1$ and $\Delta = l + 1$. Then, every code $\mathcal{C}$ of minimum distance Δ has at most $n + 1$ codewords.*

Proof. The matrix A satisfies the conditions of Theorem 14.3.1, so

$$|\mathcal{C}| \leq A(\mathbf{0}, \mathbf{0}) = 1 + n,$$

as $E_1(\mathbf{0}, \mathbf{0}) = n$. □

14.4 An almost-matching point set

To show that we can come very close to the bound of Theorem 14.3.2, consider the following set of 2^d points in $\mathbb{R}^{2^d}$. Each point will be represented as a vector indexed by entries of $x \in \{0,1\}^d$. For $w \in \{0,1\}^d$, the point p_w will have coordinates

$$p_w(x) = (1 + \chi_w(x))/2.$$

From our proof a few lectures ago that the characteristic vectors were orthogonal, we can see that each of these points differ in half their coordinates. Morover, we can double the size of the point set by taking every point p_w and its complement. We thereby obtain $2n$ points in $\{0,1\}^n$ that each differ in at least $n/2$ coordinates.