Fall 2006
Coding Theory

Homework 5
Due 2006/12/21

Oded Regev
Dept. of Computer Science
Tel Aviv University

1. **LP bound:** By using the LP bound, show that no $(n, *, d)_2$ code with $d \geq n/2$ can have more than $2n$ codewords (we already proved this as part of the Plotkin bound; this shows the optimality of Hadamard codes). Hint: use the polynomial $K_0 + K_1 + \frac{2}{n} K_2$.

2. **The q-ary Johnson bound:**

   (a) (Not to be turned in) Show that for any $q \geq 2$ there exists a set of unit vectors $v_1, \ldots, v_q \in \mathbb{R}^{q-1}$ such that for all $i \neq j$, $\langle v_i, v_j \rangle = -\frac{1}{q-1}$. Hint: use the vertices of the simplex. One way to define them is to take the q elementary vectors $e_1, \ldots, e_q \in \mathbb{R}^q$ and to notice that they all lie in a $q-1$-dimensional affine subspace.

   (b) Show that for any $q \geq 2$, $0 < \delta < \frac{q-1}{q}$, and $\tau < \frac{q-1}{q}(1 - \sqrt{1 - \frac{q}{q-1}\delta})$, there exists a constant c such that any $(n, *, \delta n)_q$ code is also $(\tau n, c)$-list-decodable. Notice that it is always enough to assume $\tau < 1 - \sqrt{1-\delta}$ and that for large q this almost matches the previous assumption (see figure).

   (c) (Not to be turned in) Deduce the q-ary Elias-Bassalygo bound.

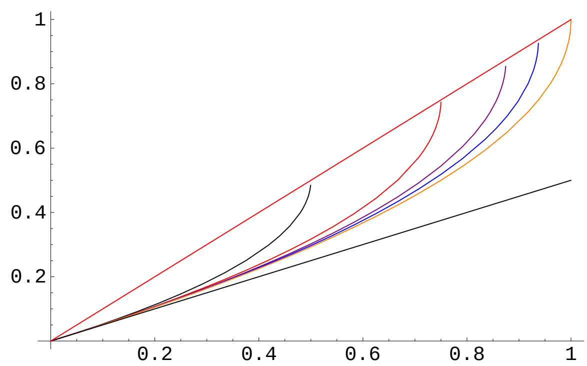

Figure 1: A plot of τ as a function of δ for $q = 2, 4, 8, 16, \infty$ with the lines δ and $\delta/2$

3. **Alternative proof of the Johnson bound for large alphabets:**

   (a) Let $m \leq t \leq n$ and ℓ be integers such that $t > \sqrt{mn}$. Consider a bipartite graph with n vertices on the left and ℓ vertices on the right with all right degrees equal to t, and the property that for any two different vertices on the right, the intersection of their neighbor sets is of size at most m (i.e., it contains no $K_{m+1,2}$). Show that

$$\ell \leq \frac{n(t-m)}{t^2 - mn}.$$

   Hint: bound in two different ways the number of paths (v_1, v_2, v_3) in which v_1, v_3 are vertices on the right and v_2 is on the left. You will probably want to use that for any $a_1, \ldots, a_n \geq 0$, $\sum_{i=1}^{n} a_i^2 \geq (\sum_{i=1}^{n} a_i)^2/n$ which you can prove using the Cauchy-Schwartz inequality.

(b) Deduce that any $(n, *, d)_q$ code is $(e, O(n^2))$-list-decodable for any $e < n - \sqrt{n(n-d)}$.

(c) Show that if we only assume $t \geq 0.99\sqrt{mn}$ in (3a) then ℓ can be exponential in n. What does this imply for the Johnson bound? Hint: take, say, $m = n/4$ and use a probabilistic argument.

4. **Agreement:** Let q be a prime power and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be some arbitrary function. Show that the number of polynomials $p \in \mathbb{F}_q[x]$ of degree at most $q/9$ that agree with f on at least $0.34q$ elements of $\mathbb{F}_q$ is bounded by a constant.