Coding Theory Spring 2009

Problem Set # 3

Due: July 9th, 2009 *Lecturer: Irit Dinur*

General Instructions:

- Please submit the exercise in the mailbox of Or Meir.
- Try to solve each problem first without consulting references. If you need references, please indicate clearly which reference you used.
- Team work: Allowed, but please limit yourself to groups of at most 3. Each person must submit the entire exercise.

Questions:

1. **Distance amplification.** Here is another nice application of expanders for constructing codes. A bipartite graph G is a (γ, δ)-weak expander if every set of size at least δn has at least $\gamma \delta n$ neighbors.
   (a) Given an $(n, k, \delta n)$ binary code C, and a (c, c)-regular (γ, δ)-weak expander $G = ([n], [n], E)$, we can construct an $(n, k/c, d)_{2^c}$ code C' by first encoding k bits via C and then placing the symbols on the left hand side of G and reading them off from the right. Give a formal definition of C', and show that the alphabet and rate are as claimed.
   (b) Prove that the distance of C' is $d \geq \gamma \delta n$.
   Remark: Although always $\gamma \leq c$ it is possible to have $\gamma\delta = 1 - O(1/c)$ which gives a relative distance $\to 1$ as c grows (and with it the alphabet size of C').
2. **Expanders from codes.** We have seen how to construct codes from expanders. In this exercise we will see the reverse direction. This will be done by constructing a graph with small second-largest eigenvalue (in absolute value), which implies it is a good expander, although we have not seen this in class.
   For a group G and a set of group elements $S = \{s_1, \ldots, s_n\}$ the Cayley graph $CG[G, S]$ has a vertex per element $x \in G$ and an edge (x, y) if $xy^{-1} \in S$ or $yx^{-1} \in S$.
   Let C be an $[n, k, d]$-code generated by an n-by-k matrix B whose rows are $b_1, \ldots, b_n$. Consider the additive group $\mathbb{F}_2^k$ generated by $S = \{b_1, \ldots, b_n\}$, and let us analyze the graph $H = CG[\mathbb{F}_2^k, S]$.
   (a) A character of a group G is a function $\chi : G \to \mathbb{C}$ such that $\chi(xy) = \chi(x)\chi(y)$. Let H' be some Cayley graph on G, and let A be its adjacency matrix. Prove that each character of G gives rise to an eigenvector of A, i.e. to a vector χ such that $A\chi = \lambda\chi$.
   (b) Prove that $\chi_a : \mathbb{F}_2^k \to \mathbb{C}$ defined by $\chi(x) = (-1)^{x \cdot a}$ for $x, a \in \mathbb{F}_2^k$ is a character of $\mathbb{F}_2^k$. Use this to find all eigenvalues of the graph $H = CG[\mathbb{F}_2^k, S]$ defined above.
   (c) Deduce that if C is a code whose pairwise distances are always between $(\frac{1}{2} - \varepsilon)n$ and $(\frac{1}{2} + \varepsilon)n$ then the second largest eigenvalue of H is at most $2\varepsilon n$.
   Remark: Codes C with such distance bounds are called ε-biased codes, and can be obtained by concatenating a Reed-Solomon code with a Hadamard code.
3. 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 $a_1, \ldots, a_n \geq 0$, $\sum a_i^2 \geq (\sum a_i)^2/n$ which can be proven using the Cauchy-Schwartz inequality.

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

(c) Show that if we only assume $t > 0.99\sqrt{mn}$ in (3b) 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 $f : F_q \to F_q$ be some arbitrary function. Show that the number of polynomials $p \in F_q[x]$ of degree at most $q/9$ that agree with f on at least $0.34q$ elements of F_q is bounded by a constant.