CSC 2414H - Assignment 4

Due Apr 24 , 2008

General rules : In solving this you may consult books and you may also consult with each other, but you must each write your own solution. In each problem list the people you consulted. This list will not affect your grade.

1. In class we discussed locally-testable-codes and locally-tecodable codes. The purpose of this exercies is to show how a certain combinatorial construct gives rise to a locally-decodable code.

   Definition: A binary code $C : \{0,1\}^n \mapsto \{0,1\}^N$ is (q, d, ϵ)-locally decodable if there exists a randomized decoding algoritm $\mathcal{A}$ that on input $i \in [n]$, and $y \in \{0,1\}^N$ such that for some $x \in \{0,1\}^n$, $d_H(y, C(x)) \leq d$ outputs x_i with probability at least $1 - \epsilon$ and makes at most q queries to y. In class we saw that using the linearity testing algorithm we can $(2, (\mathbf{1/4} - \epsilon)\mathbf{N}, 1/2 - 2\epsilon)$-locally decode Hadamard codes.

   Consider a set system as follows. Let $N, R, n \geq 1$ be some integers. For $i \in [n]$ and $r \in [R]$, let T_i and Q_{ir} be subsets of $[N]$. We say that T_i and Q_{ir} form a (q, n, N, R, s) regular family if the folloiwng holds:

   (a) q is odd;

   (b) $|T_i| = s$ for all $i \in [n]$;

   (c) for all $i \in [n], r \in [R]$, $Q_{ir} \subset T_i$ and $|Q_{ir}| = q$

   (d) for all $i \in [n]$ and $w \in T_i$,

   $$|\{r \in [R] : w \in Q_{ir}\}| = Rq/s$$

   (in other words, T_i is uniformly covered by the Q_{ir}.);

   (e) for all $i \neq j \in [n]$, and $r \in R$, $|Q_{ir} \cap T_j|$ is even.

   Show how to construct, for every d, a binary linear code that encodes n bits into N bits that is $(q, d, dq/s)$ locally-decodable using a (q, n, N, R, s) regular family. You should describe the decoding algorithm as well.

2. An $n \times n$ matrix H with entries ± 1 is a Hadamard matrix if $HH^t = nI$ (where the product is over the real field).

(a) Let C is a binary $[n, \log n, n/2]$ code **such that all nonzero codewords Have weight** $n/2$. Show how to construct an Hadamard matrix using C. Deduce that there is an $n \times n$ Hadamard matrix for any n which is a power of 2.

(b) Given an $n \times n$ Hadamard matrix H_n and an $m \times m$ Hadamard matrix H_m construct an $nm \times nm$ hadamrd matrix. Notice that this, too, gives a construction of Hadamard matrices of dimension that is a power of 2.

(c) Show that if an $n \times n$ exists then n is either 1 or 2 or a multiple of 4.

(d) Show that the absolute value of the determinant of an $n \times n$ Hadamard matrix is $n^{n/2}$.

3. (a) For a boolean function f on $\{0,1\}^n$, let ρ_f be the probability that linearity test of BLR fails. In other words

$$\rho_f = \mathrm{Pr}_{\mathrm{x,y} \in \{0,1\}^{\mathrm{n}}}[\mathrm{f(x)} + \mathrm{f(y)} \neq \mathrm{f(x+y)}].$$

(Here addition is done mod 2.) Now let g be a random boolean function. In other words, for every $x \in \{0,1\}^n$, $g(x)$ takes values 0/1 uniformly and independently. Consider ρ_g (notice this is a random variable). Give a lower bound to ρ_g that holds with high probability. Also, give a lower bound (that holds with high probability) on the distance of g from the class of linear boolean functions.

(b) Show that local testability must use randomness. More precisely, consider the following saetting. Let C be a binary code of distance d and let T be a deterministic test that makes q queries on its input $w \in \{0,1\}^n$ **and answers**

- **YES if** $w \in C$
- **NO if dist**$(w, C) \geq d/3$

(there is no requirement for other inputs)