Fall 2006
Coding Theory

Homework 7

(not to be turned in)

Oded Regev
Dept. of Computer Science
Tel Aviv University

1. **Improving the Sudan list-decoding algorithm:** In class we saw how to list decode RS codes from agreements as small as $2\sqrt{kn}$. Improve this to $\sqrt{2kn}$. The best-known algorithm, due to Guruswami and Sudan, needs only $\sqrt{kn}$ agreement and is based on multiplicities. See Sudan's lecture notes or Guruswami's thesis.

2. **Yekhanin's approach to locally decodable codes:** A binary code $C : \{0,1\}^n \to \{0,1\}^N$ is said to be (q, δ, ε)-locally decodable if there exists a randomized decoding algorithm $\mathcal{A}$ that on input $y \in \{0,1\}^N$ and $i \in [n]$ where y satisfies $\delta(y, C(x)) \leq \delta$ for some $x \in \{0,1\}^n$ outputs x_i with probability at least $1 - \varepsilon$ and makes at most q queries to y. In class we saw a simple $(2, \frac{1}{4} - \varepsilon, \frac{1}{2} - 2\varepsilon)$-local decoder for Hadamard codes.

   Definition 1 *Let $N, R, n \geq 1$ be some integers. For each $i \in [n]$, $r \in [R]$, 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 intersecting family *if the following holds:*

   (a) q is odd;

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

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

   (d) For all $i \in [n]$ and $w \in T_i$, $|\{r \in [R] \mid w \in Q_{ir}\}| = Rq/s$ (i.e., T_i is uniformly covered by the Q_{ir});

   (e) For all $i, j \in [n]$, $i \neq j$ and $r \in [R]$, $|Q_{ir} \cap T_j| \equiv 0 \bmod 2$.

   Show how to use a (q, n, N, R, s) regular intersecting family to construct binary linear code encoding n bits into N bits that is $(q, \delta, \delta Nq/s)$ locally decodable for all $\delta > 0$.

3. **One small step in Yekhanin's construction of a regular intersecting family:** Let p be an odd prime number and $m \geq p - 1$ be an integer. Define $n = \binom{m}{p-1}$. Show that there exist two families of vectors $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ in $\mathbb{F}_p^m$ such that

   - for all $i \in [n]$, $\langle u_i, v_i \rangle = 0$;
   - for all $i, j \in [n]$, $i \neq j$, we have $\langle u_i, v_j \rangle \neq 0$.