Exercise 5

February, 2006

1. Consider the r-Hamming code, defined as follows: let H be the $(2^r - 1) \times r$ matrix whose columns contain every possible r-bit string, except for the zero string. The codewords are the bit strings v of length $2^r - 1$ such that $Hv = 0$. (H is called a *parity check matrix* for the code.)

   (a) What is the distance d of the r-Hamming code?

   (b) Show that the 3-Hamming code is perfect, i.e., there is a unique codeword of distance $(d-1)/2$ or less from a bit string of the appropriate length. Is the general r-Hamming code perfect?

2. (a) Let $f : \{0,1\}^n \to \{0,1\}$, and define $f_i(S) = f(S \oplus e_i)$. Express the Fourier coefficients of f_i in terms of the Fourier coefficients of f.

   (b) Let $g = \sum_i f_i$. What condition on $< f, g >$ is equivalent to f being the indicator function for an independent set in the discrete cube? Express this in terms of the Fourier coefficients of f.

   (c) Assume that $\mathbb{E}(f) \geq 1/2$. What can we say about the Fourier coefficients? If f is the indicator function of an independent set, what is f?

   (d) Describe all possible 2-colorings of the discrete cube.

3. For any Boolean function $f : \{-1,1\}^n \to \{1,-1\}$, we say that a polynomial P is a sign-representing polynomial for f if $\forall x : \text{sign} f(x) = \text{sign} P(x)$. The degree of f is defined to be the minimal degree of a sign-representing polynomial of f. Show, using the Fourier expansion of P, that the degree of the parity function is n.

4. The following lemma has been proved by Kahn, Linial and Samorodnitsky, and also by Linial and Nisan:

   Let A_i and B_i be two families of events for $i \in [n]$. For $S \subseteq [n]$, define $a_S = P(\cap_{i \in S} A_i$ and

   $$\alpha_S = P(\cap_{i \in S} \cap \cap_{j \notin S} A_j^c)$$

   and define b_S, β_S similarly for B. If, for every $S \subsetneq [n]$, we have $a_S = b_S$, then there is a real ϵ such that $|\epsilon| \leq 1/2^{n-1}$, and for every $S \subseteq [n]$, the equation $\alpha_S = \beta_S + (-1)^{|S|}\epsilon$ holds.

   Let G and H be a pair of graphs with n vertices and m edges such that the collection of proper edge-subgraphs of G is isomorphic to the collection of proper edge-subgraphs of H. Define $\alpha_{G,S}$ for S an edge subgraph of G to be $P(E(\pi(G)) \setminus E(G)) = S$. Show that there is a real ϵ such that $|\epsilon| < \frac{1}{2^{m-1}}$ and $\alpha_{G,S} - \alpha_{H,S} = (-1)^{|S|}\epsilon$ for every $S \subseteq E(G)$.

   Deduce Müller's Theorem: if G and H are nonisomorphic, then $m \leq \log_2(n!) + 1$.

   If you're feeling adventurous, prove (or look up) the lemma.