Math 2^8: The Theory of Error-Correcting Codes
Problem Set #1

1. (Continuity of $\mathcal{R}$ and $\mathcal{R}_{\text{lin}}$) Fix q. For $\delta \in [0,1]$ define $\mathcal{R}(\delta) = \limsup_C \frac{\log_q M}{n}$ over all $(n, M, d)_q$ codes with $d \geq \delta n$, and if q is a prime power then define $\mathcal{R}_{\text{lin}}(\delta) = \limsup_C k/n$ over all $[n, k, \geq \delta n]_q$ codes. Thus the asymptotic Singleton, sphere-packing, and Gilbert-Varshamov bounds are

$$\mathcal{R}(\delta) \leq 1 - \delta, \quad \mathcal{R}(\delta) \leq 1 - \frac{H_q(\delta/2)}{\log q}, \quad \mathcal{R}(\delta) \geq 1 - \frac{H_q(\delta)}{\log q}$$

respectively, with the Gilbert-Varshamov bound assuming $\delta \leq (q-1)/q$. Prove that $\mathcal{R}$ and $\mathcal{R}_{\text{lin}}$ are continuous by showing that if $0 < e < d$ then an $(n, M, d)_q$ code yields an $(n, M', d')_q$ code with $M' \geq M/q^e$ and $d' \geq d$, and an $[n, k, d]_q$ code yields an $[n, k', \geq d]_q$ code with $k' \geq k - e$. (For continuity at $\delta = 0$ use Gilbert-Varshamov.)

2. (A bound on spherical codes[1]) Fix $t \in (0,1)$. Suppose S is a set of unit vectors in some Euclidean space such that $\langle x, y \rangle \leq -t$ for all distinct $x, y \in S$. Prove that $\#S \leq t^{-1} + 1$, with equality iff $\langle x, y \rangle = -t$ for all distinct $x, y \in S$. (Hint: this condition implies that $\sum_{x \in S} x = 0$.)

3. (A bound on binary codes) A binary code C of length n can be identified with a subset of the vertex set $\{1, -1\}^n$ of the hypercube in $\mathbf{R}^n$. Express the Hamming distance between two words w, w' in terms of the inner product between the corresponding vertices $(-1)^w, (-1)^{w'}$. Use this and the inequality in Problem 1 to deduce that if C is an (n, M, d) code with $2d > n$ then $M \leq 2d/(2d-n)$. It follows that asymptotically $\delta > 1/2 \Longrightarrow R = 0$, so at least for $\delta > 1/2$ we cannot do asymptotically better than the Gilbert-Varshamov bound (nor even for $\delta = 1/2$ by Problem 1). Can you generalize this to codes over an arbitrary finite alphabet, where the threshold $1/2$ becomes $(q-1)/q$?

4. (Optimality and uniqueness of the binary $(7, 8, 4)$ code) As a special case of Problem 2, the dual Hamming code has the largest number of words possible for a code with $q = 2$, $n = 7$, and $d = 4$. Suppose a $(7, 8, 4)_2$ code C contains 0000000. Prove that the seven nonzero words are line complements in a Fano plane of order 2, and thus that C is isomorphic with the dual Hamming code.

[1] A "spherical code" is the analog of an error-correcting code with Hamming space replaced by a Euclidean sphere. A spherical code is a subset C of the unit sphere in some (usually finite-dimensional) Euclidean space; the aim is to make C large while keeping distinct points far, which is measured by keeping their inner product bounded away from 1.