HW 4: Error-correcting codes

(due December 13th, before tutorial)

1. Let $A_q(n,d)$ be the largest k such that a code over alphabet $\{1,\ldots,q\}$ of block length n, dimension k and minimum distance d exists (recall that this corresponds to the notation $(n,k,d)_q$). Determine $A_2(3,d)$ for all integers $d \geq 1$.

2. Suppose C is a $(n,k,d)_2$-code with d odd. Construct using C a code C' that is a $(n+1,k,d+1)_2$-code.

3. By constructing the columns of a parity check matrix in a greedy fashion, show that there exists a binary linear code $[n,k,d]_2$ provided that

$$2^{n-k} > 1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}. \quad (1)$$

   This is a small improvement compared to the general Gilbert-Varshamov bound. In particular, it is tight for the $[7,4,3]_2$ Hamming code.

4. The Hadamard code has a nice property that it can be locally decoded. Let $C_{Had,r} : \{0,1\}^r \to \{0,1\}^{2^r}$ be the encoding function of the Hadamard code. Suppose you are interested only in the i-th bit x_i of the message $x \in \{0,1\}^r$. The challenge is that you only have access to $y \in \{0,1\}^{2^r}$ such that $\Delta(C_{Had,r}(x), y) \leq \frac{2^r}{10}$ and you would like to look only at a few bits of y. Show that by querying only 2 well-chosen positions (the choice will involve some randomization) of y, you can determine x_i correctly with probability $4/5$ (the probability here is over the choice of the queries, in particular x, y and i are fixed).

   Hint: You might want to query y at the position labelled by $u \in \{0,1\}^r$ at random and the position $u + e_i$ where $e_i \in \{0,1\}^r$ is the binary representation of i.