HW 5: More error correcting codes

(due Wednesday December 18th, before tutorial)

We use the notation introduced in class for Reed-Solomon codes.

1. Consider a $[4,2]_5$ Reed-Solomon code over $\mathbb{F}_5$ with $\alpha_i = 2^{i-1}$. Compute a generator matrix and a parity check matrix for this code (you may use an exercise from the tutorial for that, but you can also do it without). What is the minimum distance of this code? Check that your answer is consistent with the parity check matrix.

2. A well-studied family of codes is called cyclic codes. Their defining property is that if $(c_0, \ldots, c_{n-1}) \in C$ then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Show that if β is a generator of $\mathbb{F}_q^*$ and $\alpha_i = \beta^{i-1}$ with $n = q-1$, then the $[n,k]_q$ Reed-Solomon code is cyclic.

3. 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