Problem Sheet 7

1. We have proved in LDC11 that Sudan's algorithm finds all codewords in $B(z, n - 2\sqrt{kn})$ for any z. Show that we can find all codewords in $B(z, n - \sqrt{2kn})$. Moreover the size of the list is bounded by $\sqrt{2n/k}$.
Hint: In Sudan's proof, there is no need to bound separately the degrees in x and in y of $Q(x, y)$. All we need is that for every monomial $c_{i,j}x^i y^j$ of $Q(x, y)$, the quantity $i + (k - 1)j$ is not too large, i.e., it is not bigger than $\sqrt{2n/k}$.

2. In the construction of Trevisan's extractor, we assumed to have a code $C : \{0, 1\}^n \to \{0, 1\}^{\widetilde{n}}$ such that $\forall y \in \{0, 1\}^{\widetilde{n}}$, $|B(y, \frac{1}{2} - \delta) \cap \mathrm{Im}(C)| \leq \frac{1}{\delta^2}$. Verify that replacing the RHS by $\frac{1}{\delta^5}$ has no essential influence on our analysis.

3. Given codes $\mathrm{Enc}_1 : \{1, \ldots, N\} \to \Sigma_1^{n_1}$ and $\mathrm{Enc}_2 : \Sigma_1 \to \Sigma_2^{n_2}$, their concatenation $\mathrm{Enc} : \{1, \ldots, N\} \to \Sigma_2^{n_1 n_2}$ is defined by

$$\mathrm{Enc}(m) = \mathrm{Enc}_2(\mathrm{Enc}_1(m)_1)\mathrm{Enc}_2(\mathrm{Enc}_1(m)_2) \cdots \mathrm{Enc}_2(\mathrm{Enc}_1(m)_{n_1}).$$

Show that if Enc_i has relative minimal distance δ_i, where $i = 1, 2$, then Enc has relative minimal distance $\delta_1\delta_2$.