

Problem Sheet 8

1. Does Sudan's list decoding algorithm need to be modified if in the list of the n given points (x_i, y_i) , the first coordinates are not all distinct? (see LDC9)
2. Let X be a distribution on $\{0, 1\}^n$ which is 2^{-k} -close to a distribution Y with minimal entropy k , and Z be a distribution on $\{0, 1\}^n$ with minimal entropy $k - 1$. Comment on the difference between X and Z .
3. View the Hadamard encoding as a pseudorandom generator $H : \{0, 1\}^n \rightarrow \{0, 1\}^{2^n}$. Prove that $H(U_n)$ is a distribution which is pairwise independent (i.e., for every pair of coordinates of the output, the probability of being any $(a, b) \in \{0, 1\}^2$ is $1/4$).