Problem Sheet 5

1. Let $C : \mathbb{F}_q^k \to \mathbb{F}_q^n$ with $k < n$. Show that the minimal distance of $\mathrm{Im}(C)$ is at most $2(n-k)+1$.

2. Let H be an $(n \times n)$-Hadamard matrix ($n = 2^m$). Let $C_H \subseteq \{0,1\}^n$ be the set of vectors obtained from rows of H by replacing each component -1 with 0 (i.e., the *Hadamard* code).

(i) Assume that a codeword h is transmitted with less than $\frac{n}{4}$ errors. Call y the received word, and let $\widetilde{y}$ be the word obtained from y by replacing 0's with -1's. Show that the largest component of $H \cdot \widetilde{y}$ indicates which codeword has been sent.

(ii) Show that we can double the set of codewords by considering the $(2n \times n)$-matrix

$$\begin{pmatrix} H \\ -H \end{pmatrix},$$

with a minor modification of the decoding algorithm. This code scheme is called *punctuated Hadamard code*.

3. For a $l \in \mathbb{N}$ and $\varrho \geq 1$, a family of sets $S_1, \ldots, S_m \subseteq [d] := \{1, \ldots, d\}$ is an (m, l, d, a)- ***design*** if $|S_i| = l$ and $|S_i \cap S_j| \leq a$ for all $1 \leq i < j \leq m$. Similarly, a family of sets $S_1, \ldots, S_m \subseteq [d]$ is a ***weak*** (m, l, d, a)-***design*** if $|S_i| = l$ and

$$\sum_{j=1}^{i-1} 2^{|S_i \cap S_j|} \leq 2^a \cdot (m-1)$$

for all $1 \leq i \leq m$. Prove that every (m, d, l, a) design is also a weak design (with same parameters).

4. Prove that Trevisan's construction still works with a weak design. More specifically, prove the following

Bitte wenden!

Lemma *Let $\mathcal{T} = \{S_1, \ldots, S_m\}$ be a family of m distinct subsets of $[d]$, each having size l. For every $i \in [m]$, there exists a set $\mathcal{F}_i$ of functions from $\{0,1\}^l$ to $\{0,1\}^{d+i-1}$ (depending only on i and $\mathcal{T}$) such that*

1. *For every function $P : \{0,1\}^l \to \{0,1\}$ and every predictor $A : \{0,1\}^{d+i-1} \to \{0,1\}$, there exists a function $f \in \mathcal{F}_i$ such that*

$$\mathbb{P}_x[A(f(x)) = P(x)] \geq \mathbb{P}_y[A(y, P(y_{|S_1}) \cdots P(y_{|S_{i-1}}) = P(y_{|S_i})],$$

   where x is selected uniformly from $\{0,1\}^l$ and y from $\{0,1\}^d$.
2. $\log |F_i| \leq d - l + \sum_{j=1}^{i-1} 2^{|S_i \cap S_j|}$.