Problem Sheet 3

1. (i) A mapping $f : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k,ε)-**disperser** if for all $A \subset \{0,1\}^n$ with $|A| \geq 2^k$ we have $|f(A \times \{0,1\}^d)| \geq (1-\varepsilon)2^m$. Verify that every (k,ε)-extractor is a (k,ε)-disperser.

(ii) Give an interpretation for the definition of disperser in the probabilistic setting. (Hint: If P is an (n,k)-source, what can you say about the support of $\mathcal{P}_{f,P\times\mathbb{U}_d}$?)

(iii) Let $G_f = (V_1, V_2, E)$ be the bipartite multigraph obtained from f (Recall exercise 3 in Sheet 1), where $V_1 = \{0,1\}^n$, $V_2 = \{0,1\}^m$. Which graph property does G_f possess when f is a (k,ε)-disperser?

2. Let $G : \{0,1\}^3 \to \{0,1\}^6$ be defined by

$$\begin{array}{ll} 000 \mapsto 001101 & 100 \mapsto 101100 \\ 001 \mapsto 001011 & 101 \mapsto 100110 \\ 010 \mapsto 011010 & 110 \mapsto 110100 \\ 011 \mapsto 010110 & 111 \mapsto 110010 \end{array}$$

Let $T_1, T_2 : \{0,1\}^6 \to \{0,1\}$ be defined by $T_1(x) = 1$ if and only if x has exactly 3 components equal to 1, and $T_2(x) = 1$ if and only if $x_4 = \text{minority}\{x_1, x_2, x_3\}$ (i.e., the value appearing less in $\{x_1, x_2, x_3\}$). Evaluate for $i = 1, 2$

$$|\mathbb{P}_{x\sim \mathrm{U}_6}[T_i(x) = 1] - \mathbb{P}_{y\sim \mathrm{U}_3}[T_i(G(y)) = 1]|.$$

3. (i) In affine geometry, two distinct lines have at most one point in common. Use this fact to construct a $(q^2+q, q^2, q, 1)$-design for every prime power $q = p^n$.

(ii) Compare your construction with the probabilistic design discussed in class.

4. (Exercise on page HA-3) Let $T : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}^m$ be two binary functions, and let $r_{l+1}, \ldots, r_m \in \{0,1\}$ be fixed bits, where $l \leq m$. Prove that

$$\mathbb{P}_{x,b}[T(g(x)_{\leq l-1}, b, r_{l+1}, \ldots, r_m) = 1 \,|\, b = g(x)_l]$$
$$= \mathbb{P}_x[T(g(x)_{\leq l}, r_{l+1}, \ldots, r_m) = 1],$$

where $x \sim \mathbb{U}_n$ and $b \sim \mathbb{U}_1$ are two independent uniformly distributed variables.