Solutions 3

1. (i) Proof by contradiction. Assume that $f : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is not a (k,ε)-disperser. This means we can find some $A \subseteq \{0,1\}^n$ with $|A| \geq 2^k$ and

$$|f(A \times \{0,1\}^d| < (1-\varepsilon)2^m.$$

To show that f is not a (k,ε)-extractor we let P be the uniform (n,k)-source supported on A, i.e. $P(x) = |A|^{-1}$ if $x \in A$ and $P(x) = 0$ otherwise. Define $S := \{0,1\}^m \setminus f(A \times \{0,1\}^d)$. We have

$$\mathcal{P}_{f,P\times\mathbb{U}_d}(S) = (P \times \mathbb{U}_d)(f^{-1}(S)) = 0$$

since P is supported on A, and

$$\mathbb{U}_m(S) = 2^{-m}|S| = 2^{-m}(2^m - |f(A \times \{0,1\}^d)|) > \varepsilon.$$

Hence,

$$\delta(\mathcal{P}_{f,P\times\mathbb{U}_d}, \mathbb{U}_m) = \max_{S\subseteq\{0,1\}^m} |\mathcal{P}_{f,P\times\mathbb{U}_d}(S) - \mathbb{U}_m(S)| > \varepsilon,$$

which means that f is not a (k,ε)-extractor.

(ii) For any (n,k)-source distribution P, the support of $\mathcal{P}_{f,P\times\mathbb{U}_d}$ has size at least $(1-\varepsilon)2^m$.

(iii) For any subset $X \subseteq V_1$ of size $|X| \geq 2^k$, there are at least $(1-\epsilon)2^m$ neighbors of X in G_f.

2. The values are $\frac{11}{16}$ for $i = 1$ and $\frac{1}{8}$ for $i = 2$.

3. (i) We consider the affine plane $P := \mathbb{F}_q^2$ over the field $\mathbb{F}_q$. The affine lines in P are subsets of the form

$$\ell_{a,b,c} = \{(x,y) \in P \,|\, ax + by = c\}, \qquad a,b,c \in \mathbb{F}_q$$

The number of lines is equal to $q^2 + q$, as there are q parallels to each of the $q+1$ lines running through the origin. Now we have our design, since the plane P has q^2 points and contains $q^2 + q$ lines, each line contains q points and two distinct lines intersect in at most one point.

Bitte wenden!

(ii) The probabilistic design has the parameters (m, r, l, a) where $r \approx \frac{l^2}{a}\exp(1 + \frac{\ln m}{a})$. Our construction has $m = q^2+q$, $l = q$ and $a = 1$. For these parameters, the underlying set of the probabilistic design has $r = q^2\exp(1+\ln(q^2+q)) = O(q^4)$ elements. Hence, our construction with $r = q^2$ is more efficient.

4. For the ease of notation, let $T'(x, b) := T(g(x)_{\leq l-1}, b, r_{l+1}, \ldots, r_m)$. Since x and b are independent random variables, we have

$$\begin{aligned}
\mathbb{P}_{x,b}[T'(x,b) = 1 \mid b = g(x)_l] &= \frac{\mathbb{P}_{x,b}[T'(x,b) = 1 \text{ and } b = g(x)_l]}{\mathbb{P}_b[b = g(x)_l]} \\
&= 2 \cdot \mathbb{P}_{x,b}[T'(x,b) = 1 \text{ and } b = g(x)_l] \\
&= 2 \cdot \mathbb{P}_{x,b}[T'(x,g(x)_l) = 1 \text{ and } b = g(x)_l] \\
&= 2 \cdot \mathbb{P}_x[T'(x,g(x)_l) = 1] \cdot \mathbb{P}_b[b = g(x)_l] \\
&= \mathbb{P}_x[T'(x,g(x)_l) = 1],
\end{aligned}$$

finishing the proof.