Problem Sheet 9

1. For a distribution Q on a set $\mathcal{F}$, we define its *collision probability* as

$$\mathrm{cp}(Q) = \sum_{x \in \mathcal{F}} Q(x)^2.$$

Note that $\mathrm{cp}(Q)$ is essentially the probability that two independent random variables X, Y with distributions $P_X = P_Y = Q$ output the same value. Prove the following. For independent random variables $X, Y : \Omega \to \mathcal{F}$, $|\mathcal{F}| < \infty$, it holds that

$$\mathbb{P}[X = Y] \leq \sqrt{\mathrm{cp}(X)\mathrm{cp}(Y)} \leq \max\{\mathrm{cp}(X), \mathrm{cp}(Y)\}.$$

2. Let Q be a convex combination of the distributions $Q_1, \ldots, Q_m$. Prove that

$$\mathrm{cp}(Q) \leq \max\{\mathrm{cp}(Q_1), \ldots, \mathrm{cp}(Q_m)\}.$$

3. Let $A, B : \Omega \to \mathcal{F}$ be independent random variables, and $\mathcal{F}$ a finite group. Prove that

$$\mathrm{cp}(A + B) \leq \min\{\mathrm{cp}(A), \mathrm{cp}(B)\}.$$

Hint. Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets, $A_1, \ldots, A_n : \Omega \to \mathcal{A}$ independent random variables and $f : \mathcal{A}^n \to \mathcal{B}$ be any function. Then the distribution of $f(A_1, \ldots, A_n)$ is a convex combination of the distributions $f(A_1, \ldots, A_{n-1}, a)$ for $a \in \mathcal{A}$.

4. Let $A, B : \Omega \to \mathcal{F}$ be independent random variables, $U_{\mathcal{F}}$ the uniform distribution on $\mathcal{F}$ and $\mathcal{F}$ a finite group. Prove that

$$\mathrm{dist}(A + B, U_{\mathcal{F}}) \leq \min\{\mathrm{dist}(A, U_{\mathcal{F}}), \mathrm{dist}(B, U_{\mathcal{F}})\}.$$