Cryptography: Homework 3

(Deadline: 10am, 2022/10/7)

1. (20 points) Let X_n be a random variable over $\{0,1\}^n$. Let $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a PRG. Show that if $\{X_n\} \equiv_{\text{c.i.}} \{U_n\}$, then $\{G(X_n)\} \equiv_{\text{c.i.}} \{U_{\ell(n)}\}$.

2. (30 points) Prove that if f is a one-way function, then the function g defined by $g(x_1, x_2) = (f(x_1), x_2)$, where $|x_1| = |x_2|$, is also a one-way function.