Cryptography--ENEE/CMSC/MATH 456 PRG
Class Exercise 2/7/24

Let G be a pseudorandom generator where $|G(s)| = |s| + 1$

1. Define $G'(s) = G(s||\overline{s})$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?

2. Define $G'(s) = G(s)||G(\overline{s})$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?

3. Define $G'(s) = G(s)_1||G(G(s)_2, \dots, G(s)_{|s|+1})$, where $G(s)_i$ denotes the i-th output bit of $G(s)$. Is G' necessarily a pseudorandom generator?