Solution of Exercisesheet 3

Exercise 3-1

Exercise 3-2

(a) Is $G_a(s) = G(s)||0$ a secure PRG?
No since the last bit is always 1. This bit is not uniformly at random because the probablitiy of that bit being 1 is 100% instead of 50%.

(b) Is $G_b(s||b) = G(s)||b$ where $|b| = 1$ a secure PRG?
No because

(c) Is $G_c(s) = G(s||0)$ a secure PRG?
Yes

(d) Is $G_d(s) = G(s||0^{|s|}$ a secure PRG?

(e) Is $G_e(s) = G(s) \oplus 1^{l(|s|}$ a secure PRG?

(f) Is $G_f(s) = \textit{trunc}(G(\textit{trunc}(s)))$ a secure PRG?
where *trunc*(x) for a nonempty string x denotes all but the last bit of x.
(For this part, assume that l(n) >n + 2, and ignore the fact that Gf is undefined on input strings of length 1.)