Problem Set 2

Due in class on Thursday, March 4, 2004.

Problem 4: Density of invertible strings

[Textbook, Chapter 2, Exercise 5.]

Problem 5: Range of one-way functions

[Textbook, Chapter 2, Exercise 10.]

Problem 6: Hard-core predicate and one-way functions

[Textbook, Chapter 2, Exercise 25, part 1.]

Problem 7: Pairwise independence

Let $p_1, p_2, p_3 \in [0, 1]$. Let $s^1, s^2, s^3$ be independent random variables over $\{0, 1\}$ such that

\[ \Pr[s^i = 1] = p_i \]

for $i = 1, 2, 3$. Consider the random variables $\zeta_1 = s^1 \oplus s^2$ and $\zeta_2 = s^1 \oplus s^3$.

(a) Assume $p_1 = p_2 = p_3 = \frac{2}{3}$. For each $a_1, a_2 \in \{0, 1\}$, calculate $\Pr[\zeta_1 = a_1]$, $\Pr[\zeta_2 = a_2]$, and $\Pr[\zeta_1 = a_1 \land \zeta_2 = a_2]$. Argue that $\zeta_1$ and $\zeta_2$ are independent. Show your work.

(b) Do part (a) again, except now assume $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{2}$, and $p_3 = \frac{2}{7}$. Are $\zeta_1$ and $\zeta_2$ still independent? Why or why not?