応用数学６ 2010 年 12 月 9 日

第 3 回小テスト

講師: 安永憲司

問題 1.

一方向性関数 $f : \{0,1\}^n \to \{0,1\}^n$ に対して，関数 $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ を以下のように定義する．

$$g(x_1, x_2) = (f(x_1), x_2).$$

ただし，$x_1, x_2 \in \{0,1\}^n$ である．関数 g が一方向性関数であることを証明せよ．

ヒント: 関数 g が一方向性関数でないと仮定すると，f が一方向性関数でないことを示せばよい．つまり，f の逆計算ができる PPT アルゴリズム A が存在したとすると，g の逆計算ができる PPT アルゴリズム B が存在することを示せばよい．

関数 f が一方向性関数であるとは，

1. $f(x)$ を計算する PPT アルゴリズムが存在．
2. 任意の PPT アルゴリズム A に対して，無視できる関数 ε が存在して，すべての $n \in \mathbb{N}$ に対して，

$$\Pr[f(x') = y \mid x \stackrel{R}{\leftarrow} \{0,1\}^n, y = f(x), x' \leftarrow A(1^n, y)] \le \varepsilon(n).$$

を満たすときである．逆に，関数 f が一方向性関数でないときは，

1. $f(x)$ を計算する PPT アルゴリズムが存在しない．
2. ある PPT アルゴリズム A と，多項式 $p(\cdot)$ が存在して，無限に多くの $n \in \mathbb{N}$ に対して，

$$\Pr[f(x') = y \mid x \stackrel{R}{\leftarrow} \{0,1\}^n, y = f(x), x' \leftarrow A(1^n, y)] \ge 1/p(n).$$

の少なくとも一方を満たしているときである．

問題 2.

効率的に計算可能な関数 $G : \{0,1\}^n \to \{0,1\}^{n+1}$ を考える．アルゴリズム D に対して，

$$\mathsf{Adv}(D) = \left|\Pr[D(y) = 1 \mid x \leftarrow \{0,1\}^n, y = G(x)] - \Pr[D(y) = 1 \mid y \leftarrow \{0,1\}^{n+1}]\right|$$

と定義する．G が擬似乱数生成器 (PRG) であるとは，任意の PPT アルゴリズム D に対して，$\mathsf{Adv}(D)$ が無視できる関数で上から抑えられるときである．

PRG の定義を，任意のアルゴリズム D に対して $\mathsf{Adv}(D)$ が無視できる関数で上から抑えられるときであると変更する．つまり，アルゴリズムの計算時間を，多項式時間に制限せず，どのようなアルゴリズムに対しても成り立つときに PRG と呼ぶことにする．このとき，PRG は存在しないことを示せ．つまり，計算時間を多項式時間に制限しなければ，どのような関数 G に対しても，$\mathsf{Adv}(D)$ が無視できない関数となるようなアルゴリズム D が存在することを示せ．