テーマ２：公開鍵暗号と署名の安全性

本日の講義の目的

- ランダムオラクルのもとでの $\mathrm{P} \neq \mathrm{NP}$ の証明

前回までの復習

(1) 記号の準備.

$\mathcal{B}X \;=\;$ 定義域が X である 0,1-値関数の全体
注）たとえば，$\mathcal{B}\{0,1\}^*$ は定義域が $\{0,1\}^*$ である 0,1-値関数の全体
$R \leftarrow \mathcal{B}X \iff R$ を $\mathcal{B}X$ から等確率で 1 つ選ぶ
$\Pr\left[\mathtt{A}^R = f^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^*\right] \;=\; R$ をランダムに選んだとき，
アルゴリズム $\mathtt{A}^R$ が f^R を計算する確率

ここで R を $\mathcal{B}X$ からランダムに選ぶ，ということは，結局は，各 $x \in X$ に対し，$R(x) = 0$ か $= 1$ かを要素ごとに独立に等確率で決める，ということである．

(2) 証明したいこと

ランダムオラクルのもとで $\mathrm{P} \neq \mathrm{NP}$ を証明するには，オラクル X を用いれば NP-的に計算できる関数の中で，ランダムオラクルでは多項式時間で計算できる確率が 0 になるような関数を示せばよい．その関数の候補として次の関数を考えた．

$$f_{\mathrm{ex}}^X(x) \;=\; \begin{cases} 1, & \exists y \in \{0,1\}^n \left[X(y0) = X(y00) = \cdots = X(y0^n) = X(y0^{n+1}) = 1\right], \\ 0, & \text{otherwise}, \end{cases}$$

ただし $n = |x|$.

この関数はオラクル X に対し（それがランダムオラクルでなくても）NP^X-的に計算できる関数である．それに対して，我々はランダムオラクル R のもとでは f_{ex}^R が多項式時間に計算できる確率は 0 であることを示したい．すなわち，証明したいのは次の定理である．

定理 2.1.

$$\Pr\left[f_{\mathrm{ex}}^R \in \mathrm{P}^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^*\right] \;=\; 0. \tag{1}$$

事実 1. 各 n において，すべての $x \in \{0,1\}^n$ で $f_{\mathrm{ex}}^R(x)$ の値は同じである．

事実 2. 各 n で $0.39 \;<\; \Pr\left[f_{\mathrm{ex}}^R(0^n) = 1 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n+1\sim 2n+1}\right] \;<\; 0.5.$

事実 3. 任意の $0 < x < 1$ と自然数 $k \geq 1$ に対して

$$(1-x)^k \ < \ \mathrm{e}^{-kx}$$

3.1. 定理の証明

式 (1) を議論しやすいように変形しよう．

$$\begin{aligned}
\Pr\left[\, f_{\mathrm{ex}}^R \in \mathrm{P}^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \ &= \ \Pr\left[\, \bigvee_{\mathtt{A}:\mathrm{poly.}} \mathtt{A}^R = f_{\mathrm{ex}}^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\leq \ \sum_{\mathtt{A}:\mathrm{poly.}} \Pr\left[\, \mathtt{A}^R = f_{\mathrm{ex}}^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right].
\end{aligned}$$

なので，任意の多項式時間アルゴリズム $\mathtt{A}$ に対して，

$$\Pr\left[\, \mathtt{A}^R = f_{\mathrm{ex}}^R \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \ = \ 0 \tag{2}$$

を示すことができればよい．したがって，以下では $\mathtt{A}$ を，時間計算量がつねに n^c 以下となるアルゴリズムとして，それに対して (2) を示す．なお，c は十分大きくて $n^c \geq 2n+2$ が $n \geq 2$ に対して成り立つものとする．

自然数 n_0 を

$$\frac{n_0}{2^{n_0+1}} \ \leq \ \frac{1}{100} \tag{3}$$

となる自然数とする．また，自然数の無限列を $n_1 = n_0^c + 1,\ n_2 = n_1^c + 1,\ \ldots$ と定める．すると

$$\begin{aligned}
&\Pr\left[\, \left[\, \mathtt{A}^R = f_{\mathrm{ex}}^R \,\right] \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\quad \leq \ \Pr\left[\, \bigwedge_{i=0}^{\infty} \mathtt{A}^R(0^{n_i}) = f_{\mathrm{ex}}^R(0^{n_i}) \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\quad \leq \ \Pr\left[\, \mathtt{A}^R(0^{n_0}) = f_{\mathrm{ex}}^R(0^{n_0}) \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\qquad \times \Pr\left[\, \mathtt{A}^R(0^{n_1}) = f_{\mathrm{ex}}^R(0^{n_1}) \,\middle|\, \mathtt{A}^R(0^{n_0}) = f_{\mathrm{ex}}^R(0^{n_0}) \ \wedge \ R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\qquad \times \Pr\left[\, \mathtt{A}^R(0^{n_2}) = f_{\mathrm{ex}}^R(0^{n_2}) \,\middle|\, \bigwedge_{0 \leq i \leq 1} \mathtt{A}^R(0^{n_i}) = f_{\mathrm{ex}}^R(0^{n_i}) \ \wedge \ R \leftarrow \mathcal{B}\{0,1\}^* \,\right] \\
&\qquad \times \ \cdots \\
&\quad = \ \Pr\left[\, \mathtt{A}^R(0^{n_0}) = f_{\mathrm{ex}}^R(0^{n_0}) \,\middle|\, R_0 \leftarrow \mathcal{B}\{0,1\}^{\leq n_0^c},\ R = R_0 \,\right] \\
&\qquad \times \Pr\left[\, \mathtt{A}^R(0^{n_1}) = f_{\mathrm{ex}}^R(0^{n_1}) \,\middle|\, R_0 \leftarrow \mathcal{G}_0,\ R_1 \leftarrow \mathcal{B}\{0,1\}^{n_1 \sim n_1^c},\ R = (R_0, R_1) \,\right] \\
&\qquad \times \Pr\left[\, \mathtt{A}^R(0^{n_2}) = f_{\mathrm{ex}}^R(0^{n_2}) \,\middle|\, (R_0, R_1) \leftarrow \mathcal{G}_1,\ R_2 \leftarrow \mathcal{B}\{0,1\}^{n_2 \sim n_2^c},\ R = (R_0, R_1, R_2) \,\right] \\
&\qquad \times \ \cdots
\end{aligned}$$

となる．ただし，$(R_0, R_1, \ldots, R_i)$ は，定義域が異なるオラクルを張り合わせてできるオラクルを表し，$(R_0, R_1, \ldots, R_k) \leftarrow \mathcal{G}_k$ で，$\bigwedge_{0 \leq i \leq k} \mathtt{A}^{(R_0,\ldots,R_i)}(0^{n_i}) = f_{\mathrm{ex}}^{(R_0,\ldots,R_i)}(0^{n_i})$ を満たすオラクル $(R_0, R_1, \ldots, R_k)$ をランダムに選ぶことを意味する．

したがって，次の補題を示すことができれば，目標の (2) を導くことができる．

補題 3.1. 任意の $n \geq n_0$，任意の $X \subseteq \{0,1\}^{<n}$ に対し，

$$\Pr\left[\, \mathtt{A}^{(X,R)}(0^n) = f_{\mathrm{ex}}^{(X,R)}(0^n) \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n\sim n^c} \,\right] \;\leq\; 0.9. \tag{4}$$

証明： $n \geq n_0$ と $X \subseteq \{0,1\}^{<n}$ を各々 1 つ任意に固定した上で議論しよう．まず，

$$\Pr\left[\, \mathtt{A}^{(X,R)}(0^n) = 1 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n\sim n^c} \,\right] \;\geq\; 0.6$$

の場合を考える．この場合には，事実 2 から

$$\Pr\left[\, f_{\mathrm{ex}}^{R}(0^n) = 0 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n+1\sim 2n+1} \,\right] \;>\; 0.5$$

なので

$$\Pr\left[\, \mathtt{A}^{(X,R)}(0^n) = 1 \,\wedge\, f_{\mathrm{ex}}^{(X,R)}(0^n) = 0 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n\sim n^c} \,\right] \;\geq\; 0.1$$

となり補題が成立する．

そこで，上記の逆の場合，つまり

$$\Pr\left[\, \mathtt{A}^{(X,R)}(0^n) = 0 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n\sim n^c} \,\right] \;\geq\; 0.4$$

の場合を考える．

いま，R を $\mathcal{B}\{0,1\}^{n\sim n^c}$ の 1 つで，$\mathtt{A}^{(X,R)}(0^n) = 0$ となるようなオラクルとする．ここで $\mathtt{A}^{(X,R)}(0^n)$ の計算を追ってみると，オラクルに何回か質問をしているはずである．とくに長さ n の y に対して，$R(y0^k)$ という質問をしている場合に注目し，そのような質問が行われた y の集合を Y とする．そうすると $\mathtt{A}^{(X,R)}(0^n)$ の計算には，

$$W \;=\; \{\, w0^k \,|\, w \in \{0,1\}^n - Y,\, 1 \leq k \leq n+1 \,\}$$

の要素に対するオラクルの値は影響しない．つまり，任意の $R' \in \mathcal{B}W$ で R を上書きしたオラクル R/R' を使ったとしても，$\mathtt{A}^{(X,R/R')}(0^n) = 0$ のままである．ちなみに $|Y| \leq n^c$ なので $|\{0,1\}^n - Y| \geq 2^n - n^c$ である．

しかし，事実 2 の証明と同様の議論で

$$\begin{aligned}
&\Pr\left[\, f_{\mathrm{ex}}^{(X,R/R')}(0^n) = 1 \,\middle|\, R' \leftarrow \mathcal{B}W \,\right] \\
&\quad\geq\; 1 - \left(1 - \frac{1}{2^{n+1}}\right)^{2^n - n^c} \;\geq\; 1 - \mathrm{e}^{-2^n/2^{n+1}} \cdot \mathrm{e}^{n^c/2^{n+1}} \\
&\quad\geq\; 1 - \frac{1}{\sqrt{\mathrm{e}}} \cdot \mathrm{e}^{1/100} \;\geq\; 1 - \frac{1}{\sqrt{\mathrm{e}}} \cdot 1.01 \;\geq\; 1 - 0.61 \cdot 1.01 \;\geq\; 1 - 0.62 \;=\; 0.38
\end{aligned}$$

を示すことができる．つまり，

$$\Pr\left[\, \mathtt{A}^{(X,R)} = 0 \,\wedge\, f_{\mathrm{ex}}^{(X,R)}(0^n) = 1 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^{n\sim n^c} \,\right] \;\geq\; 0.4 \cdot 0.38 \;\geq\; 0.15$$

したがって，この場合も補題が成り立つ． □

テーマ＃２での課題（〆切：原則として６月１１日（金））

ランダムオラクルのもとでは一方向関数を構成できる．もしかすると落とし戸関数も構成可能かもしれない．実際に一方向関数が存在することを証明しよう．

採点のレベル（Ｃレベル以上が合格）

Ｂレベル（議論が曖昧の場合にはＣレベルの場合もある）：
以下に定義する関数が最悪時一方向関数であることを示す．

任意の $x, y \in \{0,1\}^n$ に対し

$$f^X(xy) \;=\; \begin{cases} x0^n, & \text{if } X(xy0) = X(xy0^2) = \cdots = X(xy0^{n+1}) = 1, \\ xy, & \text{otherwise.} \end{cases}$$

ランダムオラクルのもとで「最悪時一方向関数」ことを示すには，すべての多項式時間アルゴリズム A に対し，

$$\Pr\left[\forall x0^n \in \mathrm{Range}(f)\ \left[\mathtt{A}^R(x0^n) \in f^{-1}(x0^n)\right] \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^*\right] \;=\; 0$$

を示せばよい．なお，$\mathrm{Range}(f)$ は f の値域である．

Ａレベル： 上記の関数が平均的にもある程度の一方向性を持つことを示す．つまり，すべての多項式時間アルゴリズム A に対し，

$$\Pr\left[\Pr\left[\mathtt{A}^R(x0^n) \notin f^{-1}(x0^n) \,|\, x0^n \leftarrow \mathrm{Range}(f)\right] \;<\; 0.1 \,\middle|\, R \leftarrow \mathcal{B}\{0,1\}^*\right] \;=\; 0$$

を示せばよい（誤り率の上界 0.1 は適当な定数であれば，もっと小さくてもよい）．

特Ａレベル： 上で考えた関数では，ある程度の正解率（たとえば 0.5）で逆像を得るアルゴリズムを作ることもできる．では，正解率が，たとえば 0.01 を超えられないような強い一方向性を持つ関数を構成してみよう．あるいは落とし戸関数は構成できるだろうか？