擬似ランダム性

廣瀬勝一

擬似ランダムビット生成器

PRBG (Pseudorandom Bit Generator)

Definition 1

以下の条件を満たす関数 $g : \{0,1\}^k \to \{0,1\}^\ell$ は擬似ランダムビット列生成器と呼ばれる.

- $k^{O(1)}$ 時間（入力長の多項式時間）で計算できる.
- $\ell \geq k+1$
- 無作為に選ばれた $s \in \{0,1\}^k$ による $g(s)$ と無作為に選ばれた $r \in \{0,1\}^\ell$ とが識別不可能

PRBG の識別器

Definition 2

以下の条件を満たす確率多項式時間アルゴリズム $\mathcal{D}$ は PRBG g の (q, ε) 識別器と呼ばれる.

$$\Big|\Pr[\mathcal{D}(x_1, \ldots, x_q) = 1 \,|\, (x_1, \ldots, x_q) \leftarrow g(B^k)^q] - \Pr[\mathcal{D}(x_1, \ldots, x_q) = 1 \,|\, (x_1, \ldots, x_q) \leftarrow (B^\ell)^q]\Big| \geq \varepsilon$$

表記法

- $B = \{0, 1\}$
- $g(B^k) = \{g(v) \,|\, v \in B^k\}$（一般的に多重集合）
- $x \leftarrow S$　x が (多重) 集合 S から無作為に選択される

識別不能性 (indistinguishability)

Definition 3

$g : \{0,1\}^k \to \{0,1\}^\ell$ で，$\ell = k^{O(1)}$ とする．任意の正の定数 c について $(1, k^{-c})$ 識別器が存在しないとき，g は識別不能であるという．

Theorem 4

PRBG g について，$(1, \varepsilon)$ 識別器が存在するならば，(q, ε) 識別器が存在する．

証明）明らか． □

Theorem 5

PRBG g について，(q, ε) 識別器が存在するならば，$(1, \varepsilon/q)$ 識別器が存在する．

Th. 5 の証明 (1/3)

$\mathcal{D}$ を g の (q, ε) 識別器とする．以下のアルゴリズム $\mathcal{I}$ が g の $(1, \varepsilon/q)$ 識別器であることを示すことができる．$\mathcal{I}$ は $\mathcal{D}$ をサブルーチンとして利用する．$x \in B^\ell$ を $\mathcal{I}$ への入力とする．

1. $\mathcal{I}$ は $i \in \{1, 2, \ldots, q\}$ を無作為に選び，$(x_1, x_2, \ldots, x_q)$ を以下のように定める．

$$(x_1, \ldots, x_{i-1}) \leftarrow g(B^k)^{i-1}, x_i = x, (x_i, \ldots, x_q) \leftarrow (B^\ell)^{q-i}$$

2. $\mathcal{I}$ は，$\mathcal{D}$ に入力 $(x_1, \ldots, x_q)$ を与えて起動し，$\mathcal{D}(x_1, \ldots, x_q)$ を出力する．

$\mathcal{I}$ が確率多項式時間アルゴリズムであることは容易に確認できる．

$\left|\Pr[\mathcal{I}(x) = 1 \,|\, x \leftarrow g(B^k)] - \Pr[\mathcal{I}(x) = 1 \,|\, x \leftarrow B^\ell]\right|$ を以下で評価する．

Th. 5 の証明 (2/3)

$X = (x_1, \ldots, x_q)$, $\langle X \rangle_i^j = (x_i, \ldots, x_j)$ とする.

$$\Pr[\mathcal{I}(x) = 1 \,|\, x \leftarrow g(B^k)]$$

$$= \sum_{j=1}^{q} \Pr[i = j \wedge \mathcal{I}(x) = 1 \,|\, x \leftarrow g(B^k)]$$

$$= \frac{1}{q} \sum_{j=1}^{q} \Pr[\mathcal{I}(x) = 1 \,|\, i = j \wedge x \leftarrow g(B^k)]$$

$$= \frac{1}{q} \sum_{j=1}^{q} \Pr[\mathcal{D}(X) = 1 \,|\, \langle X \rangle_1^j \leftarrow g(B^k)^j, \langle X \rangle_{j+1}^q \leftarrow (B^\ell)^{q-j}]$$

$$\Pr[\mathcal{I}(x) = 1 \,|\, x \leftarrow B^\ell]$$

$$= \frac{1}{q} \sum_{j=1}^{q} \Pr[\mathcal{D}(X) = 1 \,|\, \langle X \rangle_1^{j-1} \leftarrow g(B^k)^{j-1}, \langle X \rangle_j^q \leftarrow (B^\ell)^{q-j+1}]$$

Th. 5 の証明 (3/3)

$$
\begin{aligned}
&\left|\Pr[\mathcal{I}(x)=1 \,|\, x \leftarrow g(B^k)] - \Pr[\mathcal{I}(x)=1 \,|\, x \leftarrow B^\ell]\right| \\
&= \left| \frac{1}{q}\sum_{j=1}^{q} \Pr[\mathcal{D}(X)=1 \,|\, \langle X\rangle_1^j \leftarrow g(B^k)^j, \langle X\rangle_{j+1}^q \leftarrow (B^\ell)^{q-j}] - \right. \\
&\qquad \left. \frac{1}{q}\sum_{j=1}^{q} \Pr[\mathcal{D}(X)=1 \,|\, \langle X\rangle_1^{j-1} \leftarrow g(B^k)^{j-1}, \langle X\rangle_j^q \leftarrow (B^\ell)^{q-j+1}] \right| \\
&= \frac{1}{q}\left|\Pr[\mathcal{D}(X)=1 \,|\, X \leftarrow g(B^k)^q] - \Pr[\mathcal{D}(X)=1 \,|\, X \leftarrow (B^\ell)^q]\right| \\
&\geq \varepsilon/q
\end{aligned}
$$

Blum-Blum-Shub PRBG

p, q を $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$ を満たす相異なる素数とする．p, q は秘密情報である．

$n = pq$.

n と互いに素な $s \in \mathbb{Z}_n$ を無作為に選ぶ.

$z_0 = s^2 \bmod n$;
for $i = 1$ *to* ℓ {
  $z_i = {z_{i-1}}^2 \bmod n$;
  $x_i = z_i \bmod 2$; /* the least significant bit */
}
return $(x_1, \ldots, x_\ell)$;

上のように計算される $(x_1, x_2, \ldots, x_\ell) = g_{\mathrm{BBS}}(s)$ は PRBG である．

擬似ランダム関数 (PRF: Pseudorandom Function)

Definition 6

以下の条件を満たす関数 $f : \{0,1\}^k \times \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$ は
擬似ランダム関数と呼ばれる.

- $\ell_1 = k^{O(1)}$ かつ $\ell_2 = k^{O(1)}$ である.
- $k^{O(1)}$（入力長の多項式）時間で計算できる.
- 無作為に選択された $s \in \{0,1\}^k$ による $f(s,\cdot)$ と，無作為に選択された $r : \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$ とが識別不可能である.

擬似ランダム関数 $f(s,\cdot)$ はしばしば $f_s(\cdot)$ と表記される.

擬似ランダム関数の識別器 (I)

Definition 7

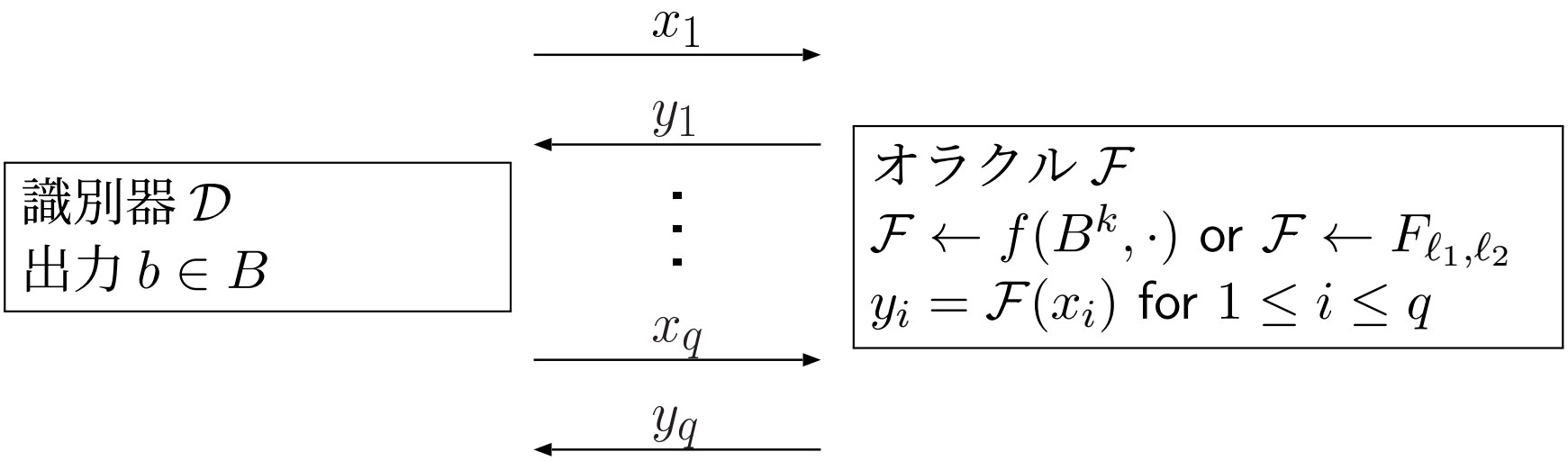
以下の条件を満たす確率多項式時間アルゴリズム $\mathcal{D}$ は擬似ランダム関数 $f : \{0,1\}^k \times \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$ の (q, ε) 識別器と呼ばれる.

- $\mathcal{D}$ は関数 $\mathcal{F} : \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$ をオラクルとする. $\mathcal{D}$ によるオラクルへの質問の個数は高々qである.
- $\left| \Pr[\mathcal{D}^{\mathcal{F}}(1^k) = 1 \,|\, \mathcal{F} \leftarrow f(B^k, \cdot)] - \Pr[\mathcal{D}^{\mathcal{F}}(1^k) = 1 \,|\, \mathcal{F} \leftarrow F_{\ell_1,\ell_2}] \right| \geq \varepsilon$

表記法

- F_{ℓ_1,ℓ_2} は $\{0,1\}^{\ell_1}$ から $\{0,1\}^{\ell_2}$ への関数の集合である.

擬似ランダム関数の識別器と識別不能性



$\mathcal{D}$ は y_i を得た後で x_{i+1} を質問する.

Definition 8

$f : \{0,1\}^k \times \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$ で，$\ell_1 = k^{O(1)}$, $\ell_2 = k^{O(1)}$ とする．任意の正の定数 c_1, c_2 について (k^{c_1}, k^{-c_2}) 識別器が存在しないとき，f は識別不能であるという.

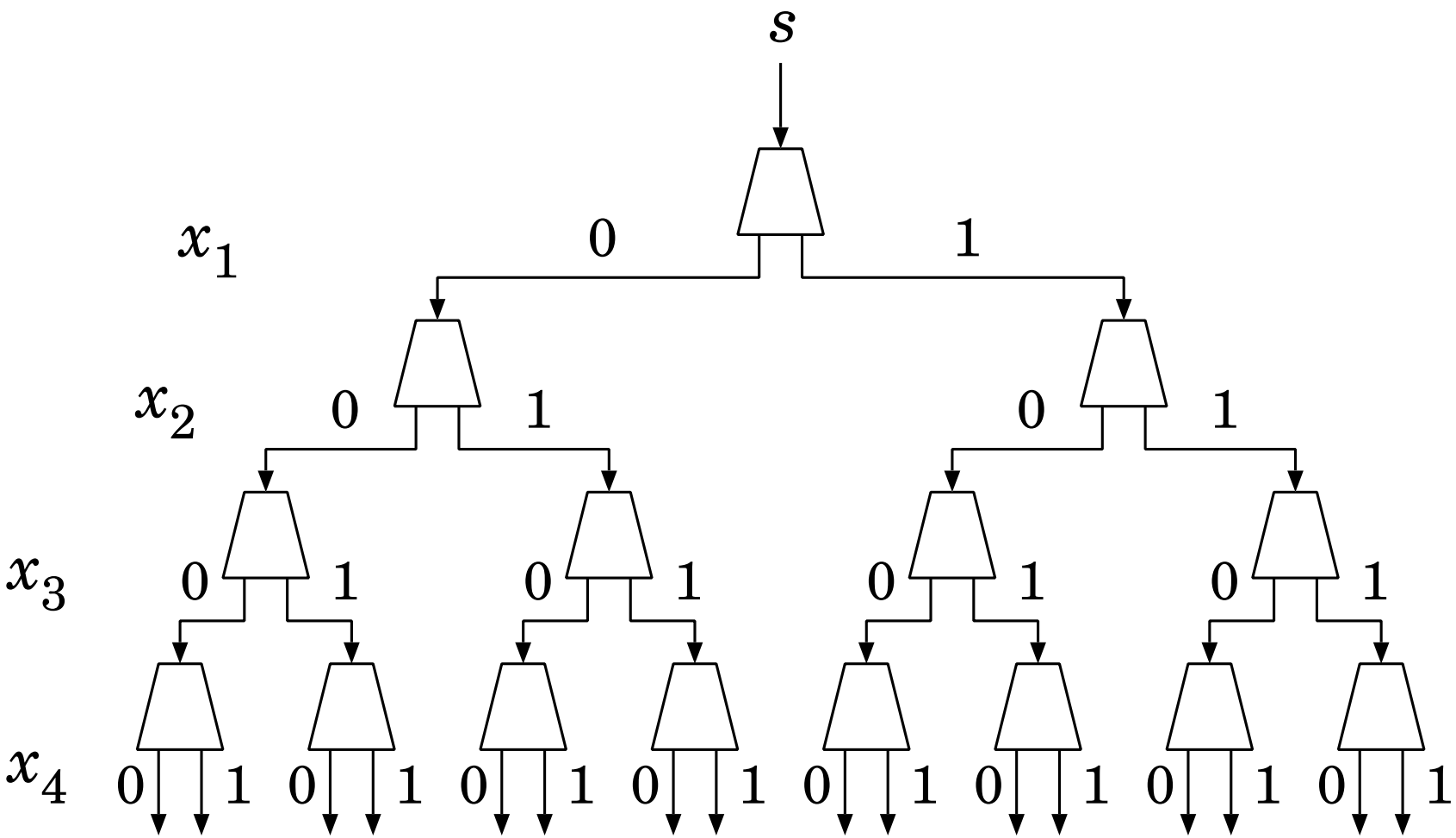
PRBG を用いた PRF の構成法

$g : \{0,1\}^k \to \{0,1\}^{2k}$ を PRBG とする．
$g(s) = (u_0, u_1)$ と表記し，$i = 0, 1$ について，$g_i(s) = u_i$ と表記する．ここで，$u_i \in \{0,1\}^k$ である．
g を用いて PRF は以下のように構成される．

$$f_s(x) = g_{x_\ell}(g_{x_{\ell-1}}(\cdots(g_{x_2}(g_{x_1}(s)))\cdots))$$

ここで，$x = (x_1, x_2, \ldots, x_\ell) \in \{0,1\}^\ell$ である．
また，$f_s : \{0,1\}^\ell \to \{0,1\}^k$ である．

PRBG を用いた PRF の構成法



PRBG を用いた PRF の識別不能性

Theorem 9

$g : \{0,1\}^k \to \{0,1\}^{2k}$ とし，$g(s) = (g_0(s), g_1(s))$ と表記する．ここで，$b \in \{0,1\}$ について，$g_b : \{0,1\}^k \to \{0,1\}^k$ である．
$f : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^k$ を以下のように定義する．

$$f_s(x) = g_{x_\ell}(g_{x_{\ell-1}}(\cdots(g_{x_2}(g_{x_1}(s)))\cdots))$$

このとき，f の (q,ε) 識別器が存在するならば，g の $(q,\varepsilon/\ell)$ 識別器が存在する．

$0 \le i \le \ell$ について

$$f^{(i)}(x) = g_{x_\ell}(\cdots(g_{x_{i+2}}(g_{x_{i+1}}(s_{(x_1,\ldots,x_i)})))\cdots)$$

とする．ここで，各 $(x_1,\ldots,x_i) \in \{0,1\}^i$ について，$s_{(x_1,\ldots,x_i)} \in \{0,1\}^k$ を決める．
$F_{\ell,k}^{(i)}$ を $f^{(i)}$ の集合とする．このとき，$F_{\ell,k}^{(0)} = f(\{0,1\}^k, \cdot)$ であり，$F_{\ell,k}^{(\ell)} = F_{\ell,k}$ である．

Th. 9 の証明 (I)

$\mathcal{D}$ を f の (q, ε) 識別器とする．このとき，以下のアルゴリズム $\mathcal{I}$ が g の $(q, \varepsilon/\ell)$ 識別器であることが証明できる．$\mathcal{I}$ は $\mathcal{D}$ をサブルーチンとして利用する．$z_1, \ldots, z_q$ を $\mathcal{I}$ への入力とする．$b \in \{0,1\}$ について $z_{j,b} \in \{0,1\}^k$ と表記し，$z_j = (z_{j,0}, z_{j,1})$ と表記する．

1. $\mathcal{I}$ は $i \in \{1, 2, \ldots, \ell\}$ を無作為に選択し，$\hat{f}^{(i)}$ を以下のように定義する．

$$\hat{f}^{(i)}(x) \stackrel{\text{def}}{=} g_{x_\ell}(\cdots(g_{x_{i+2}}(g_{x_{i+1}}(\hat{s}_{(x_1,\ldots,x_i)})))\cdots)$$

2. $\mathcal{I}$ は 1^k を入力として $\mathcal{D}$ を起動する．$\mathcal{D}$ からの各質問 x について，$\mathcal{I}$ は $\hat{f}^{(i)}(x)$ を返す．
3. $\mathcal{I}$ は $\mathcal{D}$ の出力を出力する．

Th. 9 の証明 (II)

上に挙げた手続きで，$\mathcal{I}$ は $\hat{s}_{(x_1,\ldots,x_i)}$ を以下のように定める．

$L = \emptyset;\ j = 1;$
while $\mathcal{D}$ *asks queries*
  if the new query from $\mathcal{D}$ *is* x *then* $\{$
    if $((x_1, \ldots, x_{i-1}), j') \in L$ *then* $\hat{s}_{(x_1,\ldots,x_i)} = z_{j',x_i}$;
    else $\{$
      $\hat{s}_{(x_1,\ldots,x_i)} = z_{j,x_i}$;
      $L = L \cup \{((x_1, \ldots, x_{i-1}), j)\}$;
      $j = j + 1$;
    $\}$
  $\}$

Th. 9 の証明 (III)

$X = (x_1, \ldots, x_q)$ とする.
$\left|\Pr[\mathcal{I}(X) = 1 \,|\, X \leftarrow g(B^k)^q] - \Pr[\mathcal{I}(X) = 1 \,|\, X \leftarrow (B^\ell)^q]\right|$ は以下のように評価できる.

$$\Pr[\mathcal{I}(X) = 1 \,|\, X \leftarrow g(B^k)^q] = \sum_{j=1}^{\ell} \Pr[i = j \wedge \mathcal{I}(X) = 1 \,|\, X \leftarrow g(B^k)^q]$$

$$= \frac{1}{\ell} \sum_{j=1}^{\ell} \Pr[\mathcal{I}(X) = 1 \,|\, i = j \wedge X \leftarrow g(B^k)^q]$$

$$= \frac{1}{\ell} \sum_{j=1}^{\ell} \Pr[\mathcal{D}^{\mathcal{F}}(X) = 1 \,|\, \mathcal{F} \leftarrow F_{\ell,k}^{(j-1)}]$$

$$\Pr[\mathcal{I}(X) = 1 \,|\, X \leftarrow (B^\ell)^q] = \frac{1}{\ell} \sum_{j=1}^{\ell} \Pr[\mathcal{D}^{\mathcal{F}}(X) = 1 \,|\, \mathcal{F} \leftarrow F_{\ell,k}^{(j)}]$$

Th. 9 の証明 (IV)

したがって

$$\left|\Pr[\mathcal{I}(X)=1 \mid X \leftarrow g(B^k)^q] - \Pr[\mathcal{I}(X)=1 \mid X \leftarrow (B^\ell)^q]\right|$$

$$= \frac{1}{\ell}\left|\sum_{j=1}^{\ell} \Pr[\mathcal{D}^{\mathcal{F}}(X)=1 \mid \mathcal{F} \leftarrow F_{\ell,k}^{(j-1)}] - \sum_{j=1}^{\ell} \Pr[\mathcal{D}^{\mathcal{F}}(X)=1 \mid \mathcal{F} \leftarrow F_{\ell,k}^{(j)}]\right|$$

$$= \frac{1}{\ell}\left|\Pr[\mathcal{D}^{\mathcal{F}}(X)=1 \mid \mathcal{F} \leftarrow F_{\ell,k}^{(0)}] - \Pr[\mathcal{D}^{\mathcal{F}}(X)=1 \mid \mathcal{F} \leftarrow F_{\ell,k}^{(\ell)}]\right|$$

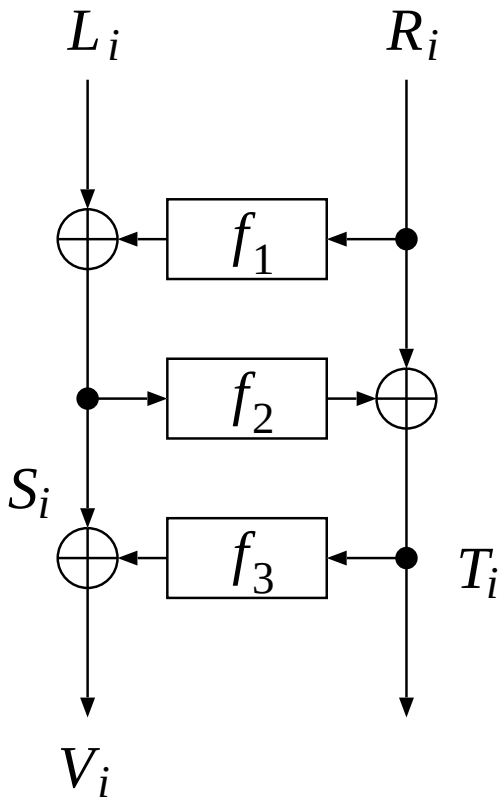
$$\geq \frac{\varepsilon}{\ell}$$

$\mathcal{I}$ は g の $(q, \varepsilon/\ell)$ 識別器である. □

PRF を用いた擬似ランダム置換 (PRP)

Luby & Rackoff, 1988 年

$\psi(f_1, f_2, f_3) \stackrel{\text{def}}{=}$



$\psi(f_1, f_2, f_3)$ の識別不能性

Lemma 10

任意の $h : (\{0,1\}^{2\ell})^q \to \{0,1\}$ と任意の $x_1, \ldots, x_q \in \{0,1\}^{2\ell}$ について

$$\Big|\Pr[h(f(x_1), \ldots, f(x_q)) = 1 \,|\, f \leftarrow \psi(F_{\ell,\ell}, F_{\ell,\ell}, F_{\ell,\ell})] - \Pr[h(f(x_1), \ldots, f(x_q)) = 1 \,|\, f \leftarrow F_{2\ell,2\ell}]\Big| \leq \frac{q^2}{2^\ell}$$

上の式で

$$\begin{aligned}\Pr[h(f(x_1), \ldots, f(x_q)) = 1 \,|\, f \leftarrow F_{2\ell,2\ell}] \\ = \Pr[h(r_1, \ldots, r_q) = 1 \,|\, (r_1, \ldots, r_q) \leftarrow (B^{2\ell})^q]\end{aligned}$$

Lem. 10 の証明 (I)

一般性を失うことなく，$x_1, \ldots, x_q$ はすべて互いに異なると仮定できる．
$S_1, \ldots, S_q$ がすべて互いに異なるという事象を E_S で表す．$T_1, \ldots, T_q$ がすべて互いに異なるという事象を E_T で表す．
$T_i = R_i \oplus f_2(S_i)$ で f_2 はランダムだから，E_S が生じると $T_1, \ldots, T_q$ はランダムである．同様に E_T が生じると $V_1, \ldots, V_q$ はランダムである．
以上より，E_S と E_T の両方が生じると，$\psi(F_{\ell,\ell}, F_{\ell,\ell}, F_{\ell,\ell})$ は $F_{2\ell,2\ell}$ と完全に識別不能である．したがって，以下の不等式が成立する．

$$\Big|\Pr[h(f(x_1), \ldots, f(x_q)) = 1 \,|\, f \leftarrow \psi(F_{\ell,\ell}, F_{\ell,\ell}, F_{\ell,\ell})] - \Pr[h(f(x_1), \ldots, f(x_q)) = 1 \,|\, f \leftarrow F_{2\ell,2\ell}]\Big| \leq 1 - \Pr[E_S \wedge E_T]$$

Lem. 10 の証明 (II)

$$1 - \Pr[E_S \wedge E_T] = \Pr[\,\overline{E_S} \vee \overline{E_T}\,] \le \Pr[\,\overline{E_S}\,] + \Pr[\,\overline{E_T}\,]$$
$$\le \sum_{1 \le i < j \le q} \Pr[S_i = S_j] + \sum_{1 \le i < j \le q} \Pr[T_i = T_j]$$

$$\begin{aligned}\Pr[S_i = S_j] &= \Pr[R_i = R_j \wedge S_i = S_j] + \Pr[R_i \neq R_j \wedge S_i = S_j] \\ &= \Pr[R_i \neq R_j \wedge S_i = S_j] \\ &= \Pr[R_i \neq R_j] \Pr[S_i = S_j \mid R_i \neq R_j] \\ &= 2^{-\ell} \Pr[R_i \neq R_j] \le 2^{-\ell}\end{aligned}$$

上の式で，$R_i = R_j$ のときは $L_i \neq L_j$ なので，
$\Pr[R_i = R_j \wedge S_i = S_j] = 0$ である．

Lem. 10 の証明 (III)

$$\begin{aligned}\Pr[T_i = T_j] &= \Pr[S_i = S_j \wedge T_i = T_j] + \Pr[S_i \neq S_j \wedge T_i = T_j] \\ &= \Pr[S_i = S_j \wedge R_i = R_j] + \Pr[S_i \neq S_j \wedge T_i = T_j] \\ &\leq 2^{-\ell}\end{aligned}$$

したがって，$1 - \Pr[E_S \wedge E_T] \leq q(q-1)2^{-\ell} \leq q^2\, 2^{-\ell}$ である．

□

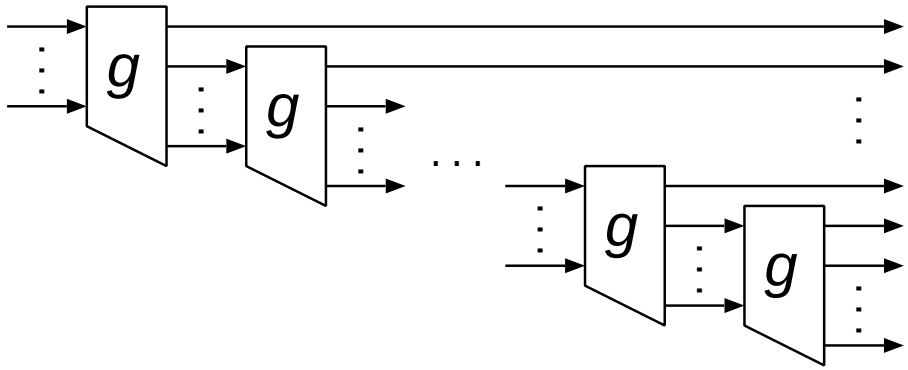
$\psi(f_1, f_2, f_3)$ の擬似ランダム性

Theorem 11

$f : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ とする．
$\psi(f(\{0,1\}^k, \cdot), f(\{0,1\}^k, \cdot), f(\{0,1\}^k, \cdot))$ の (q, ε) 識別器が存在するならば，f の $(q, \frac{1}{3}(\varepsilon - \frac{q^2}{2^\ell}))$ 識別器が存在する．

演習問題

1. $g : \{0,1\}^k \to \{0,1\}^{k+1}$ を PRBG とする．このとき，下図の関数が PRBG であることを証明せよ．



2. $\psi(F_{\ell,\ell}, F_{\ell,\ell})$ が擬似ランダムでないことを示せ．
3. Th. 11 を証明せよ．