ハイブリッド論法

定義（アンサンブル）

- I を可算な添数集合とする。
- I を添え字とするアンサンブルとは、I を添え字とする確率変数の列のことである。
- すなわち、X_i が確率変数であるとき、$\{X_i\}_{i \in I}$ は I を添え字とするアンサンブル。

定義（多項式時間識別不能性）

- $X = \{X_n\}_{n\in\mathbf{N}}$ と $Y = \{Y_n\}_{n\in\mathbf{N}}$ を、自然数の集合 $\mathbf{N}$ を添え字とする二つのアンサンブルとする。
- X と Y が多項式時間識別不能であるとは、任意の確率的多項式時間アルゴリズム D、任意の多項式 $p(\cdot)$、十分に大きな n に対して、

$$|\Pr[D(X_n,1^n)=1] - \Pr[D(Y_n,1^n)=1]| < 1/p(n)$$

- 「十分に大きな n に対して」とは、「ある N が存在して、任意の $n>N$ に対して」ということ。

定義（サンプリングによる識別不能性）

- $X = \{X_n\}_{n\in\mathbf{N}}$ と $Y = \{Y_n\}_{n\in\mathbf{N}}$ を二つのアンサンブルとする。
- X と Y が多項式時間サンプリングにより識別不能であるとは、任意の確率的多項式時間アルゴリズム D、任意の多項式 $p(\cdot)$ と $m(\cdot)$、十分に大きな n に対して、

$$\left| \Pr[D(X_n^{(1)}, \ldots, X_n^{(m(n))}) = 1] - \Pr[D(Y_n^{(1)}, \ldots, Y_n^{(m(n))}) = 1] \right| < 1/p(n)$$

- $X_n^{(1)}$ から $X_n^{(m(n))}$ までは X_n のコピー。
- $Y_n^{(1)}$ から $Y_n^{(m(n))}$ までは Y_n のコピー。

定義（効率的に構成可能なアンサンブル）

- アンサンブル $X = \{X_n\}_{n \in \mathbf{N}}$ が効率的に構成可能であるとは、確率的多項式時間アルゴリズム S が存在して、任意の n に対して、確率変数 $S(1^n)$ と X_n が同一の分布を持つ。

定理

- $X = \{X_n\}_{n \in \mathbf{N}}$ と $Y = \{Y_n\}_{n \in \mathbf{N}}$ を二つの効率的に構成可能なアンサンブルとする。
- X と Y は多項式時間識別不能であると仮定する。
- このとき、X と Y は多項式時間サンプリングにより識別不能である。

証明（1/4）

- 還元論法（reducibility argument）による。
- 背理法による。確率的多項式時間アルゴリズム D と 多項式 $m(\cdot)$ と $p(\cdot)$ が存在して、無限個の n に対して、

$$\Delta(n) := |\ \Pr[D(X_n^{(1)}, \ldots, X_n^{(m(n))}) = 1] - \Pr[D(Y_n^{(1)}, \ldots, Y_n^{(m(n))}) = 1]\ | > 1/p(n)$$

と仮定する。

補足

- ある N が存在して、任意の $n>N$ に対して …
- これを否定すると、
- 任意の N に対して、ある $n>N$ が存在して、… でない
- ということは、
- 無限個の n に対して … でない

証明（2/4）

- 以下、背理法の仮定のもとで、アンサンブル X と Y を識別する確率的多項式時間アルゴリズム D' を構成する。
- そのために、$0 \leq k \leq m$ に対して、ハイブリッド確率変数 H_n^k を導入。

$$H_n^k := (X_n^{(1)}, \ldots, X_n^{(k)}, Y_n^{(k+1)}, \ldots, Y_n^{(m)})$$

補足

- ハイブリッド確率変数 H_n^k :

$$H_n^k := (X_n^{(1)}, \ldots, X_n^{(k)}, Y_n^{(k+1)}, \ldots, Y_n^{(m)})$$

- 要するに、k 回目までのサンプリングでは、X_n を用いて、k+1 回目以降は Y_n を用いる。
- H_n^m は $(X_n^{(1)}, \ldots, X_n^{(m)})$
- H_n^0 は $(Y_n^{(1)}, \ldots, Y_n^{(m)})$

証明（3/4）

- D' への入力を α とする。
- D' は、まず、$0 \le k \le m-1$ を満たす k を等確率で選ぶ。
- 次に D' は、X_n の k 個の独立したコピー $x^1,\ldots,x^k$ を作る。X_n は効率的に構成可能。
- 同様に Y_n の $n-k-1$ 個の独立したコピー $y^{k+2},\ldots,y^m$ を作る。
- D' は $D(x^1, \ldots, x^k, \alpha, y^{k+2}, \ldots, y^m)$ を呼び出す。

主張 1

- $\mathrm{Pr}[D'(X_n) = 1] = (1/m) \sum_{k=0}^{m-1} \mathrm{Pr}[D(H_n^{k+1}) = 1]$

(証明)

- $D'(\alpha) = D(X_n^{(1)}, \ldots, X_n^{(k)}, \alpha, Y_n^{(k+2)}, \ldots, Y_n^{(m)})$
- $\mathrm{Pr}[D'(X_n) = 1]$

$= (1/m) \sum \mathrm{Pr}[D(X_n^{(1)}, \ldots, X_n^{(k)}, X_n, Y_n^{(k+2)}, \ldots, Y_n^{(m)}) = 1]$

$= (1/m) \sum \mathrm{Pr}[D(H_n^{k+1}) = 1]$

同様に

- $\mathrm{Pr}[D'(Y_n) = 1] = (1/m) \sum \mathrm{Pr}[D(H_n^{k}) = 1]$

主張 2

- $|\Pr[D'(X_n) = 1] - \Pr[D'(Y_n) = 1]| = \Delta(n)/m(n)$

（証明）

- 左辺

$= (1/m) |\sum \Pr[D(H_n^{k+1}) = 1] - \sum \Pr[D(H_n^{k}) = 1]|$

$= (1/m) |\Pr[D(H_n^{m}) = 1] - \Pr[D(H_n^{0}) = 1]|$

$= (1/m) |\Pr[D(X_n^{(1)}, \ldots, X_n^{(m)})=1] -$

$\Pr[D(Y_n^{(1)}, \ldots, Y_n^{(m)})=1]|$

$= \Delta(n)/m$

証明（4/4）

- 仮定により、無限個の n に対して、

  $\Delta(n) > 1/p(n)$
- $| \Pr[D'(X_n)=1] - \Pr[D'(Y_n)=1] | > 1/p(n)m(n)$
- これは、X と Y は多項式時間識別不能であるという仮定に反する。

m が n に依存しない場合

- $\Delta(n) := |\ \mathrm{Pr}[D(X_n^{(1)}, \ldots, X_n^{(m(n))}) = 1] -$
  $\mathrm{Pr}[D(Y_n^{(1)}, \ldots, Y_n^{(m(n))}) = 1]\ |$
  $= |\ \mathrm{Pr}[D(H_n^{m})=1] - \mathrm{Pr}[D(H_n^{0})=1]\ |$
  $= |\ \sum \mathrm{Pr}[D(H_n^{k+1})=1] - \sum \mathrm{Pr}[D(H_n^{k})=1]\ |$
  $= |\ \sum (\mathrm{Pr}[D(H_n^{k+1})=1] - \mathrm{Pr}[D(H_n^{k})=1])\ |$
  $\leq \sum |\ \mathrm{Pr}[D(H_n^{k+1})=1] - \mathrm{Pr}[D(H_n^{k})=1]\ |$
- 無限個の n に対して $\Delta(n) > 1/p(n)$ ならば、ある k が存在して、無限個の n に対して、
  $|\ \mathrm{Pr}[D(H_n^{k+1})=1] - \mathrm{Pr}[D(H_n^{k})=1]\ | > 1/p(n)m$

ハイブリッド論法（hybrid argument)

- 基本的なアンサンブルから作られた二つの複合的なアンサンブル
- 両者を混合したハイブリッド・アンサンブル
- 極端なハイブリッドは、複合的なハイブリッドに一致する。
- 隣り合うハイブリッドは、基本的なアンサンブルに簡単に関連づけられる。
- ハイブリッドの数は小さい（多項式）。

ハイブリッド論法の応用

- LR オラクル
  - IND-CPA や IND-CCA における暗号化オラクルを、$m(n)$ 個のメッセージ対を受け取って、同じビット b で選んで暗号化するオラクルに拡張。
  - $\mathrm{LR}(b, x_0, x_1)$ は x_b を暗号化した結果を返す。
- ハイブリッド・オラクル
  - $\mathrm{LR}_k(b, x_0, x_1)$ は、k 回目に呼び出されたとき、x_b を暗号化して返す。それまでは常に x_0 を暗号化して返し、それ以後は常に x_1 を暗号化して返す。
  - $\mathrm{LR}_1(1, x_0, x_1)$ は $\mathrm{LR}(1, x_0, x_1)$ と同じ結果になる。
  - $\mathrm{LR}_m(0, x_0, x_1)$ は $\mathrm{LR}(0, x_0, x_1)$ と同じ結果になる。

$\mathrm{LR}_k(b, x_0, x_1)$

- $\mathrm{LR}_{\mathrm{once}}(b, x_0, x_1)$ を、一回だけ呼び出せる LR オラクルとする。
- $\mathrm{LR}_k(b, x_0, x_1)$ を $\mathrm{LR}_{\mathrm{once}}(b, x_0, x_1)$ を用いて実現。
  - $1 \sim k-1$ 回目に呼び出されたとき、$E_{pk}(x_0)$ を返す。
  - k 回目に呼び出されたとき、$\mathrm{LR}_{\mathrm{once}}(b, x_0, x_1)$ を返す。
  - $k+1$ 回目以降に呼び出されたとき、$E_{pk}(x_1)$ を返す。
- 性質
  - $\mathrm{LR}_1(1, x_0, x_1) = \mathrm{LR}(1, x_0, x_1)$
  - $\mathrm{LR}_m(0, x_0, x_1) = \mathrm{LR}(0, x_0, x_1)$
  - $\mathrm{LR}_k(0, x_0, x_1) = \mathrm{LR}_{k+1}(1, x_0, x_1)$

ハイブリッド論法の適用

- $A(\mathrm{LR}(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$ を、LR オラクルを用いて IND-CPA 等に勝つ攻撃者とする。

  $|\ \Pr[b = A(b)] - 1/2\ |$: negligible でない

  where $A(b) = A(\mathrm{LR}(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$

  $|\ \Pr[A(0) = 1] - \Pr[A(1) = 1]\ |$: negligible でない

- A を用いて $A'(\mathrm{LR}_{\mathrm{once}}(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$ を構成する。

  $A'(b) = A'(\mathrm{LR}_{\mathrm{once}}(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$ とおく。

  – まず、1〜m の値 k を等確率で選ぶ。

  – そして、$A(\mathrm{LR}_k(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$ を呼び出す。

  $A'(k, b) = A(\mathrm{LR}_k(b,\cdot,\cdot), E_{pk}(\cdot), D_{sk}(\cdot))$ とおく。

導出

- $\Pr[A'(b) = 1] = (1/m)\sum_{k=1}^{m} \Pr[A'(k, b) = 1]$
- $\Pr[A'(m, 0) = 1] = \Pr[A(0) = 1]$
- $\Pr[A'(1, 0) = 1] = \Pr[A(1) = 1]$
- $\Pr[A'(k, 0) = 1] = \Pr[A'(k+1, 1) = 1]$
- $\Pr[A'(0) = 1] - \Pr[A'(1) = 1]$

$= (1/m)\sum (\Pr[A'(k, 0) = 1] - \Pr[A'(k, 1) = 1])$

$= (1/m)(\Pr[A'(m, 0) = 1] - \Pr[A'(1, 1) = 1])$

$= (1/m)(\Pr[A(0) = 1] - \Pr[A(1) = 1])$

補足

- IND-CPA では、暗号化オラクルが必要。
- IND-CCA では、LR オラクルが返した暗号文を復号してはならないが、この性質は LR_k にも継承される。
- さらに、鍵を多重化することも可能。