

Определение $\{f_n\}$, $f_n : \{0, 1\}^{l(n)} \rightarrow \{0, 1\}^{m(n)}$ - семейство односторонних функций, если:

- $\{f_n\}$ - полиномиально вычислимо относительно n ;
- $\forall \{C_n\}$ - последовательности схем полиномиального размера

$$P[C_n(f_n(x)) \in f_n^{-1}(f_n(x))] \sim 0$$

- $\mapsto \text{Dom } f_n$ - доступно.

Определение $d(\alpha_n, \beta_n) = \sum_{x \in \text{Dom}} \frac{|\alpha_n(x) - \beta_n(x)|}{2}$

Определение Последовательность $\{\alpha_n\}$ называется пренебрежимо малой, если $\forall \text{poly}(n) \exists N : \forall n > N |\alpha_n| < \frac{1}{\text{poly}(n)}$.

Определение Распределение μ_n называется полиномиально моделируемым, если существует (вероятностный) алгоритм A , получающий на вход Un $p(n)$ и $\forall x \in \text{Dom } \mu_n$ $P[A = x] = \mu_n(x)$.

Определение Распределение μ_n называется доступным, если существует полиномиально моделируемое распределение η_n такое, что $d(\mu_n, \eta_n) \sim 0$.

Свойства

1) $\alpha_n \sim \beta_n, \beta_n \sim \gamma_n \Rightarrow \alpha_n \sim \gamma_n$

2) $\alpha_n \sim \beta_n$, и γ_n независима от α_n и β_n . Тогда $\alpha_n \gamma_n \sim \beta_n \gamma_n$ (конкатенация).

Δ Пусть это не так. Тогда существует $\{C_n\}$ полиномиального размера, такие, что $|P[C_n(\alpha_n \gamma_n) = 1] - P[C_n(\beta_n \gamma_n) = 1]|$ - не пренебрежимо малая последовательность. Заметим, что $|P[C_n(\alpha_n \gamma_n) = 1] - P[C_n(\beta_n \gamma_n) = 1]| \leq |E_{\gamma_n}(P[C_n(\alpha_n \gamma_n) = 1] - P[C_n(\beta_n \gamma_n) = 1])| \leq E_{\gamma_n}(|P[C_n(\alpha_n \gamma_n) = 1] - P[C_n(\beta_n \gamma_n) = 1]|) \leq |P[C_n(\alpha_n \gamma_{\max}) = 1] - P[C_n(\beta_n \gamma_{\max}) = 1]|$, то есть $\alpha_n \not\sim \beta_n$. Противоречие. \square

3) Пусть $\{T_n\}$ - последовательность схем полиномиального размера, и $\alpha_n \sim \beta_n$. Тогда $T_n(\alpha_n) \sim T_n(\beta_n)$

Определение $h_n(x)$ называется трудным битом для односторонней $f_n(x)$, если $h_n(x)$ полиномиально вычислима, и $\forall \{C_n\}$ - схем полиномиального размера $P[C_n(f_n(x)) = h_n(x)] \sim \frac{1}{2}$.

Определение Две последовательности α_n, β_n называются вычислимыми и неотличимыми, если $\forall \{C_n\}$ - схем полиномиального размера $P[C_n(\alpha_n) = 1] \sim P[C_n(\beta_n) = 1]$.

Лемма Пусть $\{f_n\}$ - семейство односторонних функций, являющихся перестановками, а $\{h_n\}$ - ее трудный бит. Тогда

$$h_n(x)f_n(x) \sim r_nf_n(x) \sim r_nx$$

где r_n - чистый случайный бит.

\triangle Докажем правую эквивалентность. Поскольку $P[C_n(x) = 1] = P[C_n(f_n(x)) = 1]$, и используем свойство III.

Докажем левую эквивалентность. От противного. Пусть $\exists\{C_n\}$ - схем полиномиального размера таких, что $\exists s(n) = \text{poly}(n)$, и $\forall N \exists n > N$:

$$|P[C_n(h_n(x)f_n(x)) = 1] - P[C_n(r_nf_n(x)) = 1]| > \frac{1}{s(n)}$$

Построим $\{R_n\}$:

- I $R_n(r_n, f_n(x)) = r_n$, если $C_n(0f_n(x)) = C_n(1f_n(x))$;
- II $R_n(r_n, f_n(x)) = 0$, если $C_n(0f_n(x)) = 1, C_n(1f_n(x)) = 0$;
- III $R_n(r_n, f_n(x)) = 1$, если $C_n(1f_n(x)) = 1, C_n(0f_n(x)) = 0$;

Тогда легко проверить, что

$$|R_n(r_n, x)| = |P[C_n(h_n(x)f_n(x)) = 1] - P[C_n(r_nf_n(x)) = 1]| > \frac{1}{s(n)}$$

Это значит, что $\{R_n\}$ обращает функцию f_n . Противоречие. \square

Лемма (о сглаживании) Пусть H - универсальное семейство хэш-функций с параметрами (m, s) , $h = Un(H)$, x - случайная величина в $\{0, 1\}^m$, $H_1(x) \geq k$, $r = Un(\{0, 1\}^s)$ (!!!! почему и там и там s), $L_1(\alpha, \beta) = \sum_y |P[\alpha = y] - P[\beta = y]|$.

Тогда

$$(h(x), h) \sim_{2^{\frac{s-k}{2}}} (r, h)$$

$(h(x), h) \sim_{2^{\frac{s-k}{2}}} (r, h)$ где \sim понимается в смысле L_1 расстояния.

\triangle Пусть $|H| = 2^l$. Одно из неравенств далее следует из того, что $E\xi^2 \geq (E\xi)^2$.

$$L_1 = \sum_{h,a} |2^{-l} P_x[h(x) = a] - 2^{-l-s}| \leq$$

$$E_{h,a} |P_x[h(x) = a] 2^s - 1| \leq \sqrt{E_{h,a} (P_x[h(x) = a] 2^s - 1)^2} \leq$$

$$\sqrt{E_{h,a} (2^s \sum_x P(x) \mathbb{I}[h(x) = a] - 1)^2} \leq$$

$$\sqrt{E_{h,a} (2^s \sum_{x_1} P(x_1) \mathbb{I}[h(x_1) = a] - 1) \sqrt{E_{h,a} (2^s \sum_{x_2} P(x_2) \mathbb{I}[h(x_2) = a] - 1)}} =$$

$$\sqrt{E_{h,a} (\sum_{x_1, x_2} 2^{2s} P(x_1) P(x_2) \mathbb{I}[h(x_1) = h(x_2) = a]) + Q} = (*)$$

$$Q - \text{остаток, и } Q = E_{h,a} (1 - 2^{s+1} \sum_x P(x) \mathbb{I}[h(x) = a]) = 1 + (-2) = -1.$$

$E_h(\mathbb{I}[h(x_1) = h(x_2) = a]) = 2^{-2s}$, если $x_1 \neq x_2$, и 2^{-s} в другом случае. Для того, чтобы посчитать сумму в $(*)$, прибавим и вычтем этот член.

Из условия $H_1(x) \geq k$ вытекает, что $\sum_x P^2(x) \leq 2^{-k}$ (используется в последнем неравенстве).

$$(*) = \sqrt{1 - \left(\sum_{(x,x)} P^2(x) - \sum_{(x,x)} 2^s P^2(x) \right) - 1} = \sqrt{\sum_x (2^s - 1) P^2(x)} = \sqrt{(2^s - 1) \sum_x P^2(x)} \leq \sqrt{2^s 2^{-k}} = 2^{\frac{s-k}{2}}$$

□